VERTIV™

Smart InfraSight™

User Manual

Version 4.0.1

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.

Visit https://www.vertiv.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

This page intentionally left blank

1 Activation

1.1 Overview

1.1.1 Appliance

Open a supported browser and enter the default server IP address in the address bar: https://192.168.0.251 The user will be presented with an activation page for Smart InfraSight™. After Smart InfraSight™ is successfully activated, users can continue to use the relevant features of Smart InfraSight™.

1.1.2 Virtual Machine

Open a supported browser and enter the default IP address of the Virtual Machine host in the address bar. The user will be presented with an activation page for Smart InfraSight™. After Smart InfraSight™ is successfully activated, users can continue to use the relevant features of Smart InfraSight™.

1.1.3 Functional Modules

For more information about activating the function, refer to Onboarding Process .

1.1.4 Recommended Configurations and Precautions

Recommended configuration for client hardware

Refer to AV-50015 Vertiv™ Smart InfraSight™ v4.0 Quick Installation Guide on Hardware Requirements and Monitoring Scale table.

Browser Requirements and Language Settings

Google Chrome 73 and above (recommended: 109.0.5414.75 and above), Firefox 66 and above. Edge 87 and above (recommended: 109.0.5414.75 and above).

In the Edge browser, the software display language is the same as the current system language, and other browsers can set it in the browser settings.

Recommended configuration for clients using the Power Train feature:

RAM: 16GB

CPU: i5-10500 or higher

Recommended resolution: 1920x1080, minimum supported resolution: 1600x900

NOTE: You need to check the firewall configuration information of the network environment to prevent the following ports from being disabled, resulting in Smart InfraSight™ not being able to obtain data correctly, as shown in the following table.

Network port	Host	Remark
8443(http)/443(https)/13054	Smart InfraSight™	Smart InfraSight™ server
80(http)/7681	NVR	80: The port requested by the NVR command RESTful 7681/7682 (ws/wss): Websocket video communication port
4001/4002	Newbell Access Control	Newbell access control and fingerprint reader
UPD 161/162	SNMP Trap	
80(http)/13392/5657(udp)	RDU 501	Communicate with RDU

1.2 Quick Start

1.2.1 Quick Deployment Procedure

1. Get the activation code.
2. Enter the correct activation code to activate Smart Infrasight.
3. Set the e-mail address of the system administrator (Username: admin).
4. Set the login password of the system administrator (Username: admin).
5. Configure the mail server.

1.3 Onboarding Process

1.3.1 Activating the Smart InfraSight™

Getting an Activation Code

When accessing the Smart InfraSight™ system for the first time, this screen is presented to the user as part of the onboarding process. The user contacts Vertiv to get a feature code for the Smart InfraSight™ instance. After verifying the user's identity, Vertiv will provide the user the activation code to be entered into the Activation Code field. Figure 1.1 on the facing page shows the activation page.

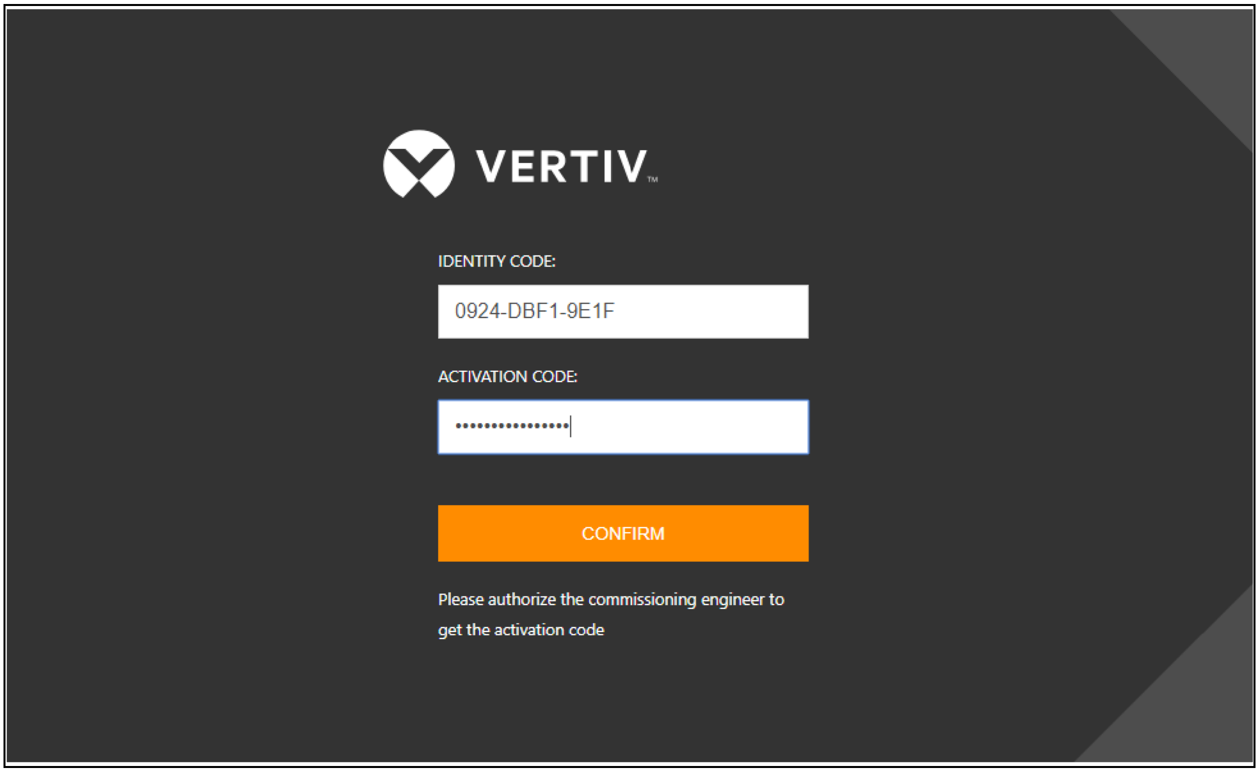
Figure 1.1 Activation Page

NOTE: The Activation code is unique to each Smart InfraSight™.

Activation

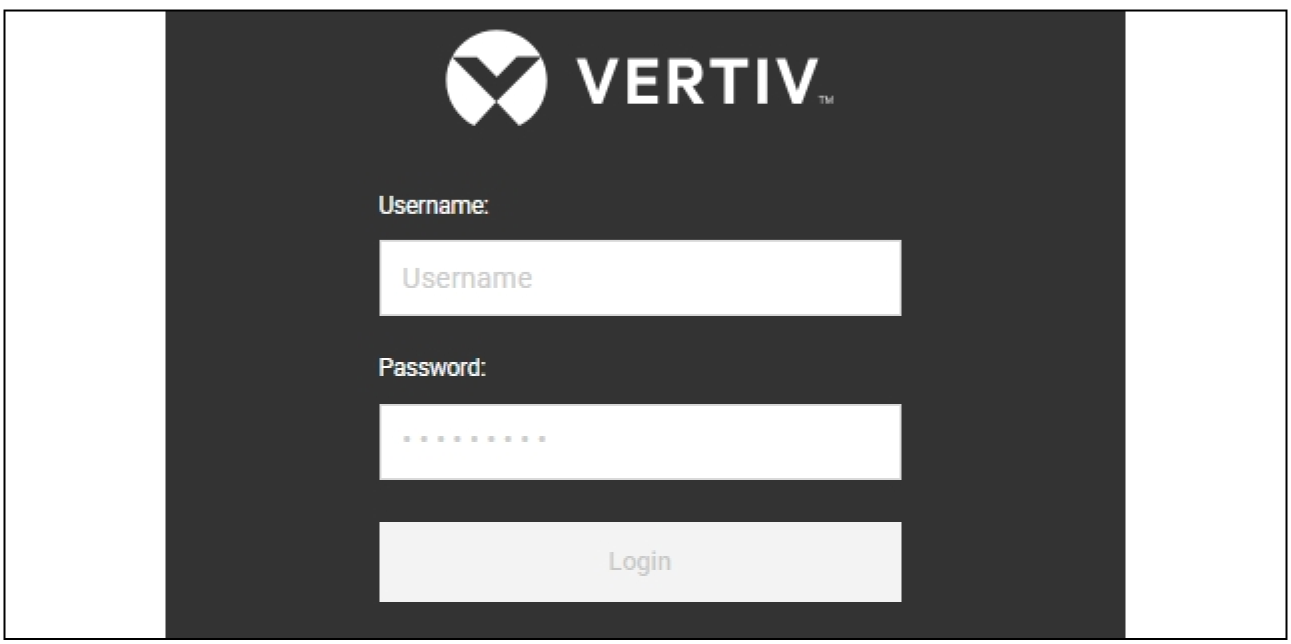
1. Enter the activation code and click the *Confirm* button as shown in Figure 1.2 on the next page .

Figure 1.2 Activation Screen



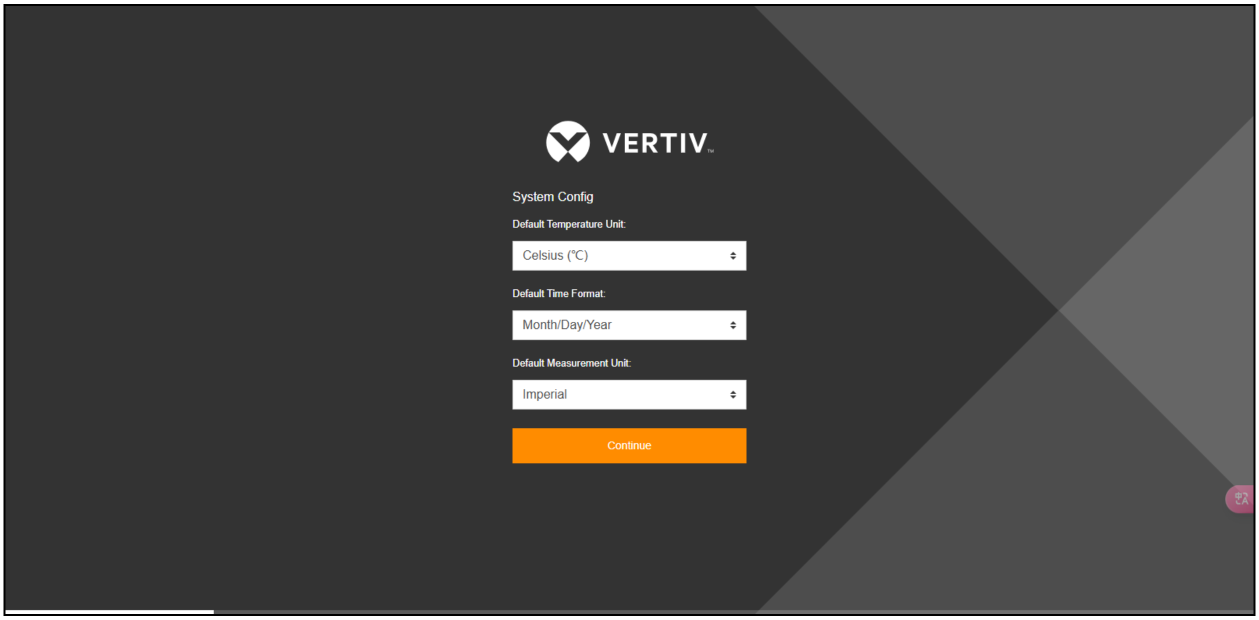
2. If the activation code is entered correctly, the activation operation will be completed, and the page will be redirected to the User login Screen as shown in Figure 1.3 below .

Figure 1.3 User Login Screen



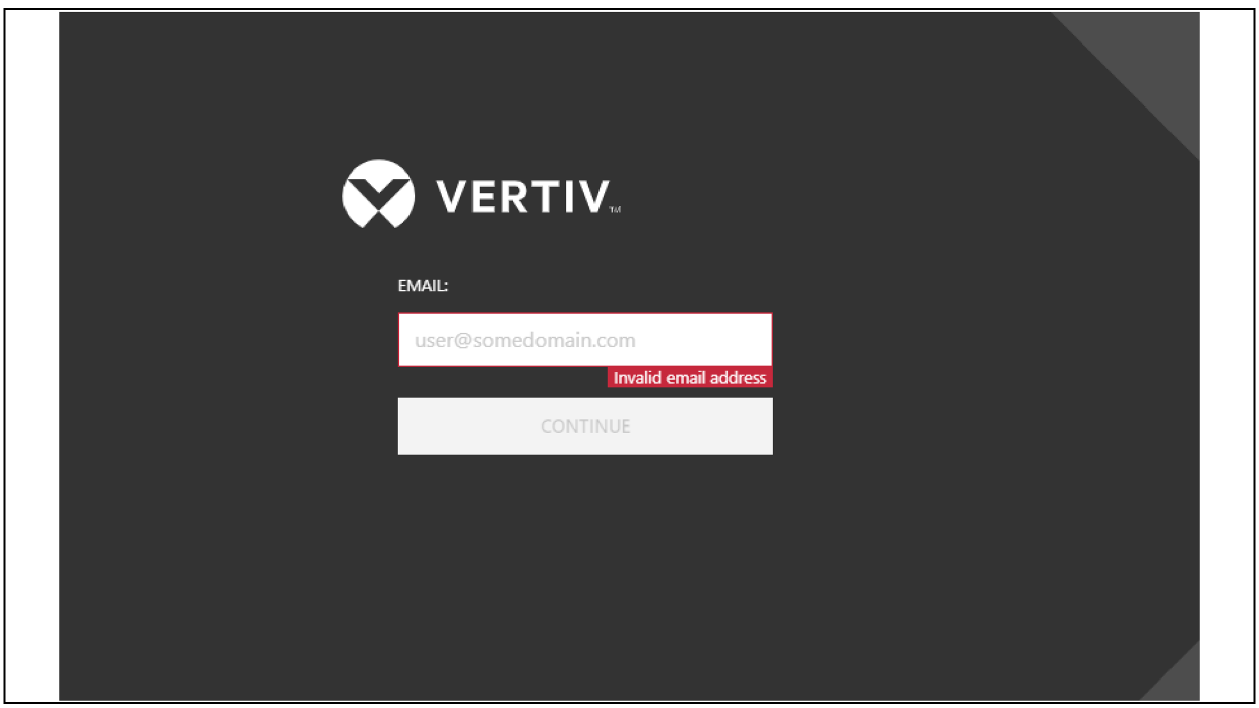
3. Use the preset account default **username** is: **admin**, and **password**: **Passw0rd123** to log in, if the password is correct, the page will jump to the system localization configuration interface as shown in **Figure 1.4** below .

Figure 1.4 System Configuration



4. After the localization configuration is completed, click the Continue button, and the page will jump to the interface of setting the system administrator's email address as shown in **Figure 1.5** below .

Figure 1.5 Setting up an Administrator's Email Address

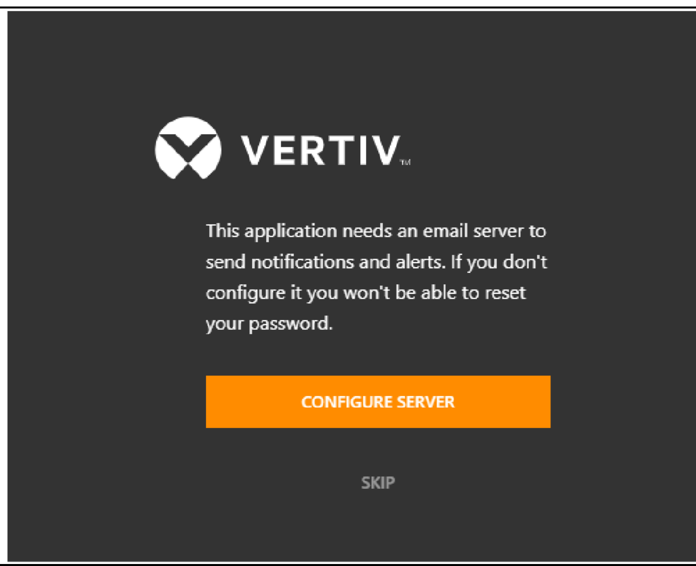


5. After entering the correct administrator email address the page will jump to the interface of setting the system administrator (Username: admin) login password as shown in Figure 1.6 below .

Figure 1.6 Setting up the Login Password for the System Administrator (Admin)

6. After setting the login password of the system administrator that meets the set necessary conditions, the page will automatically jump to the configuration page of the mail server as shown in Figure 1.7 below . The user can configure the mail server now, or click the skip button to add the mail server configuration later in the system settings - notification settings.

Figure 1.7 Server Configuration—Skip Option

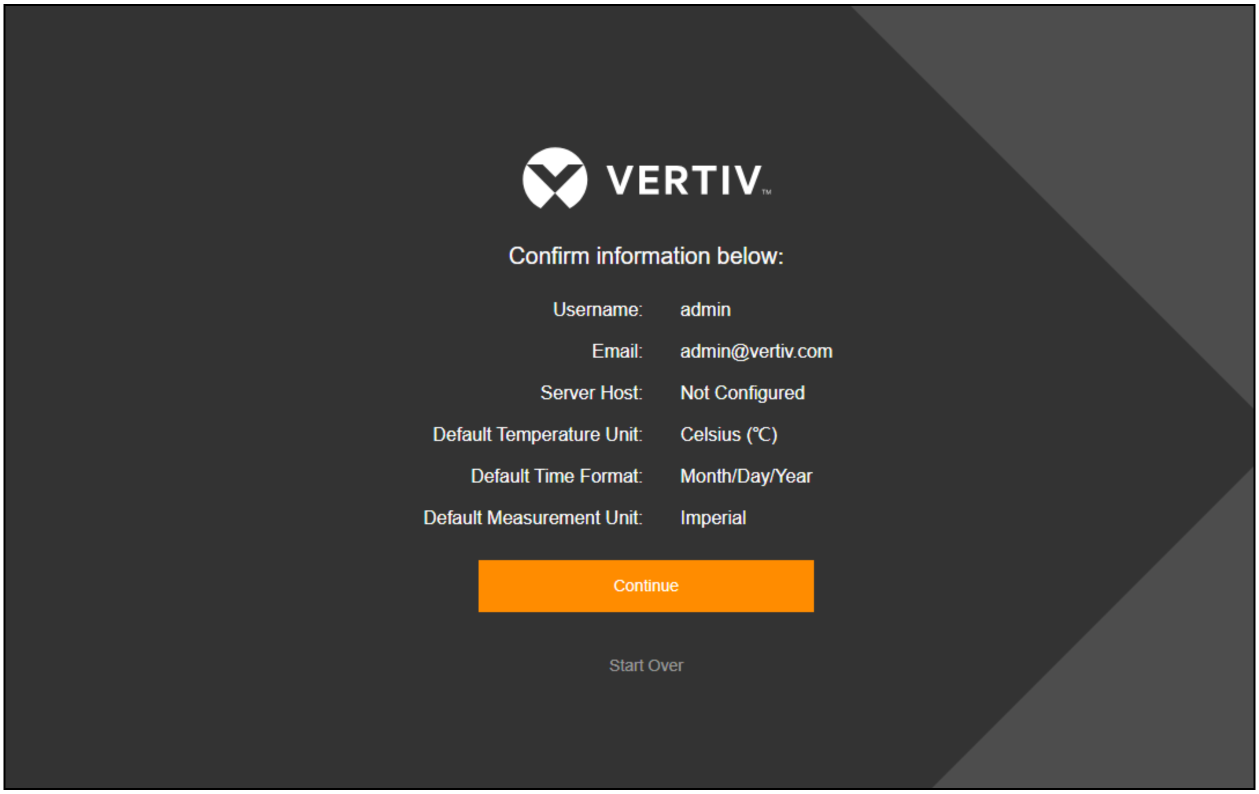


If you select Configure, you will be redirected to the Configure Mail Server page, as shown in Figure 1.8 below . After entering the email server host name, host port number, mail server login user name, mail server login password, and whether to use TLS, the mail server configuration is complete.

Figure 1.8 Configuring the Mail Server

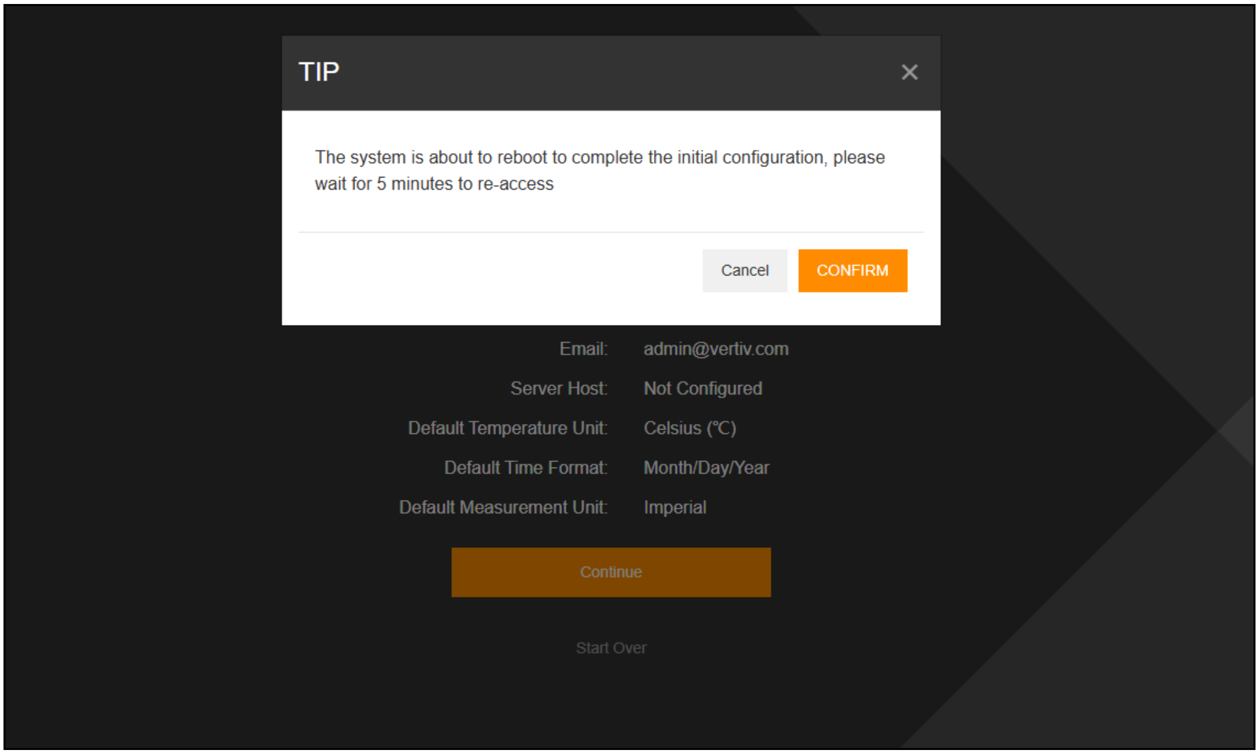
Finally, confirm that the system initialization configuration information is correct, and click Continue as shown in Figure 1.9 on the next page , and you can start using Smart InfraSight™. The username is the default username admin (the default username of the system administrator cannot be modified), and use the password you have just set to login.

Figure 1.9 System Configuration Interface



Click the confirm button as shown in Figure 1.10 on the facing page , the system will restart to complete the initial configuration, please wait for 5 min and then refresh the page.

Figure 1.10 Confirmation Window



This page intentionally left blank

2 User Login

2.1 General

2.1.1 Overview

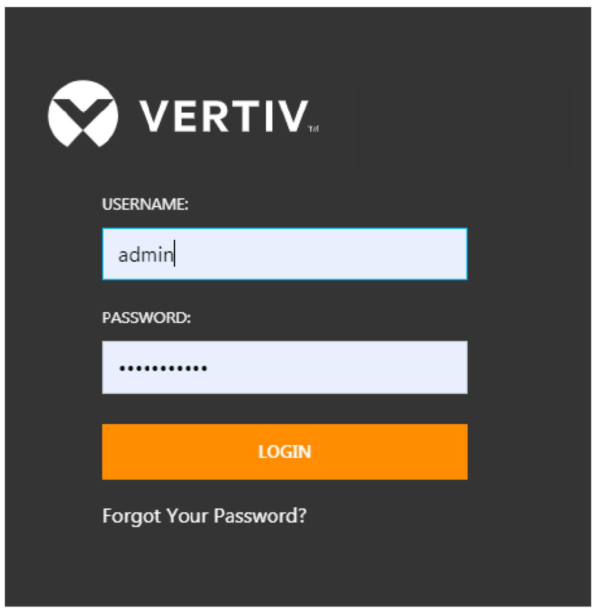
After Smart InfraSight™ is activated and the initialization information is configured, users can now login to the Smart Infrasight system.

2.2 Detailed Functions

2.2.1 User Login

Enter your Username and password and click the *Login*, as shown in **Figure 2.1** below .

Figure 2.1 User Login

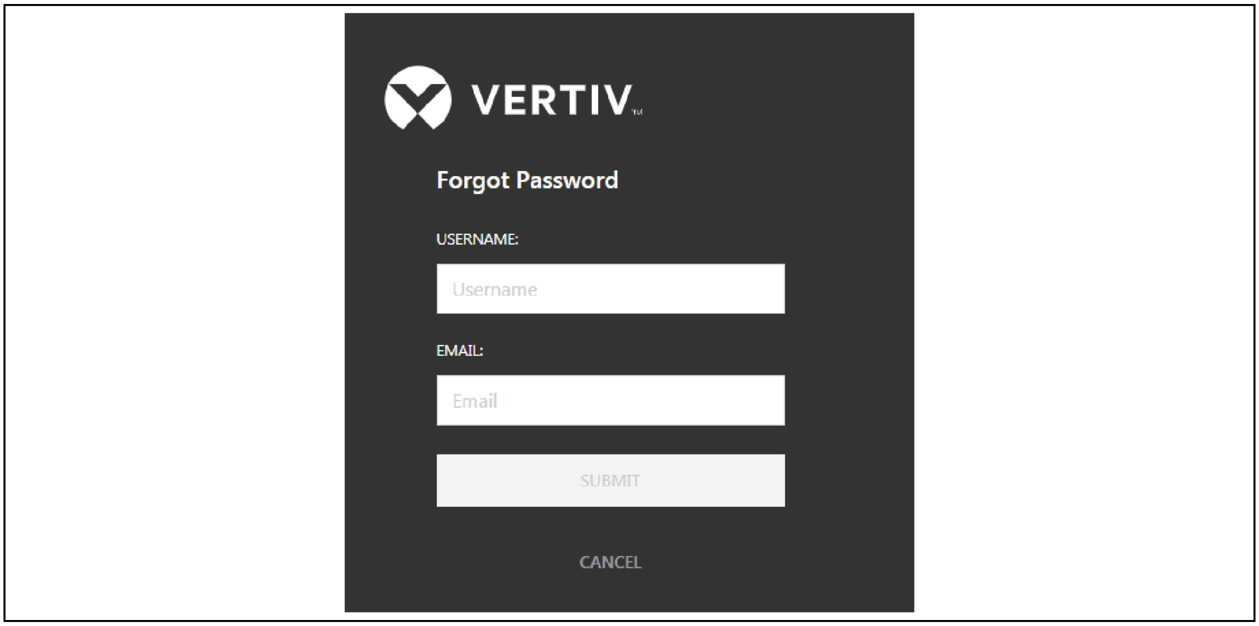


Forgot Password

Click *Forgot Password* on the login page, then enter your Username and email address on the Forgot Password page, and click the *Submit*, as shown in **Figure 2.2** on the next page .

NOTE: After entering the username or password incorrectly for 5 times, the account will be locked for 2 hours.

Figure 2.2 Forgot Password Window



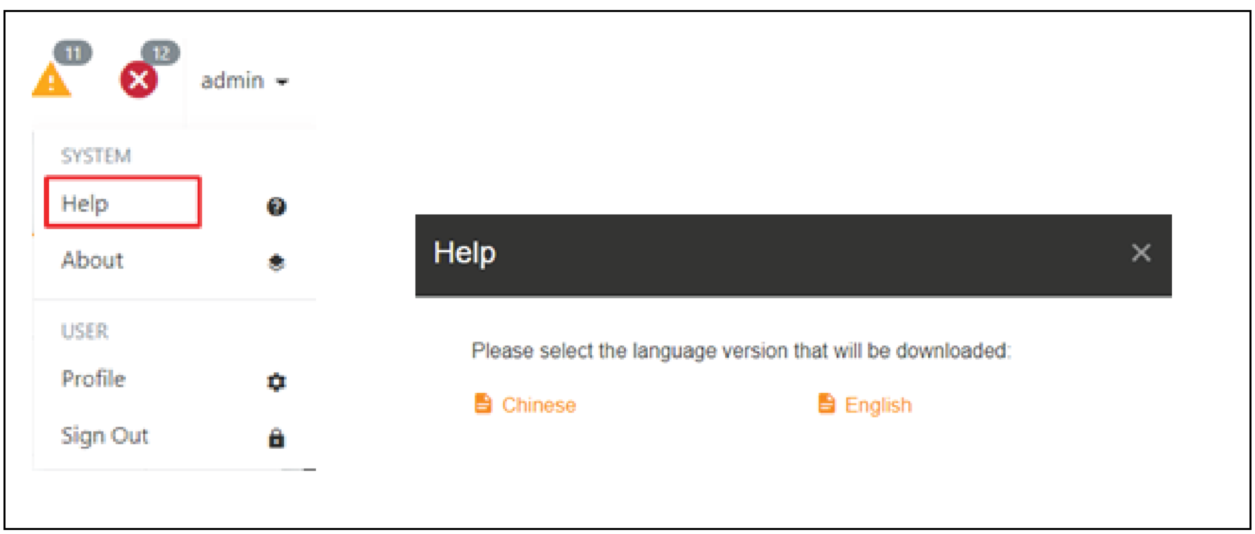
NOTE: You need to enter a correct username and the corresponding email address or the verification code email will not actually be sent.

2.2.2 User Profiles and Help Information

Help

After logging in, click the drop-down menu on the right side of the Username in the upper right corner (admin example is shown in Figure 2.3 below), and then click the *Help* menu to pop up the User Manual download links and select the Chinese or English version User Manual.

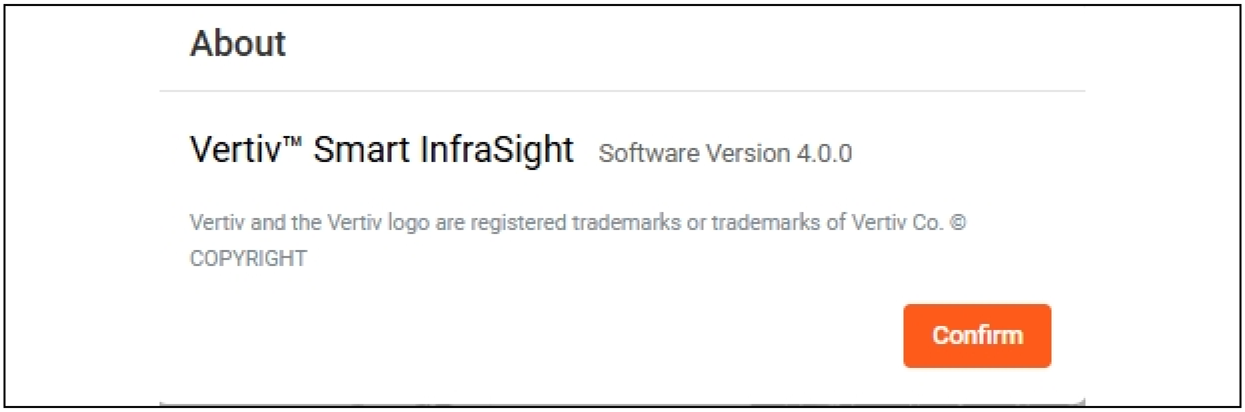
Figure 2.3 Help Page



About Page

After logging in, click the drop-down menu button on the right side of the Username in the upper right corner (admin example is shown in **Figure 2.4** below), and then click the *About* menu to view the software information.

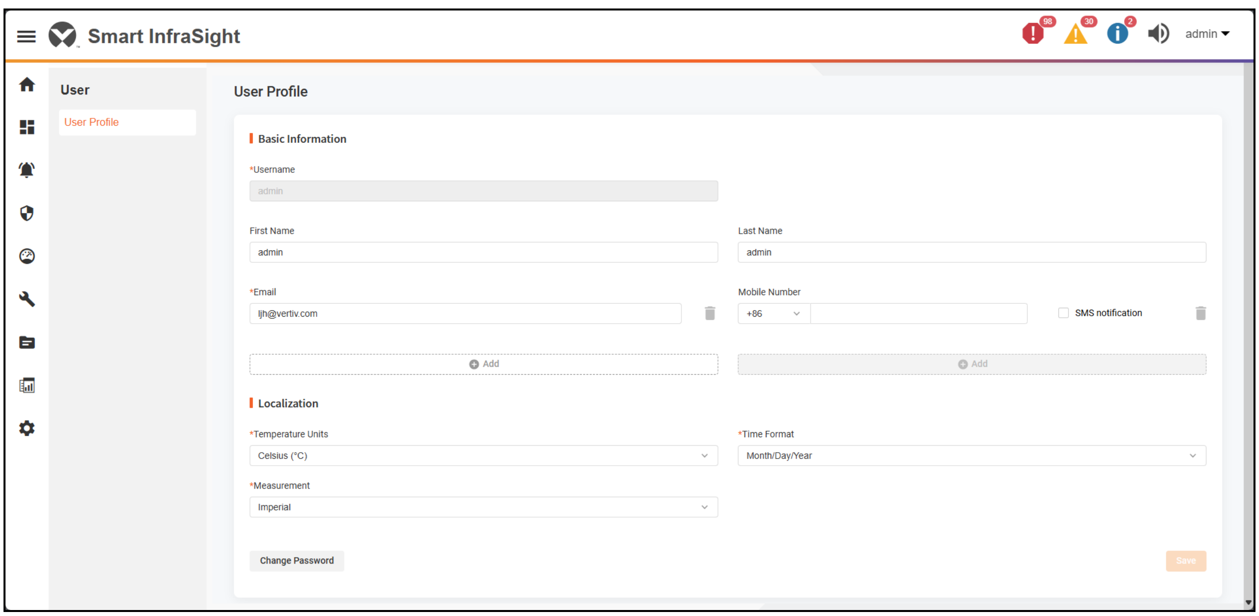
Figure 2.4 About Page



User Profiles

After logging in, click the drop-down menu button on the right side of the Username (admin) in the upper right corner, and click *Profile* to jump to the user profile interface, as shown in **Figure 2.5** below .

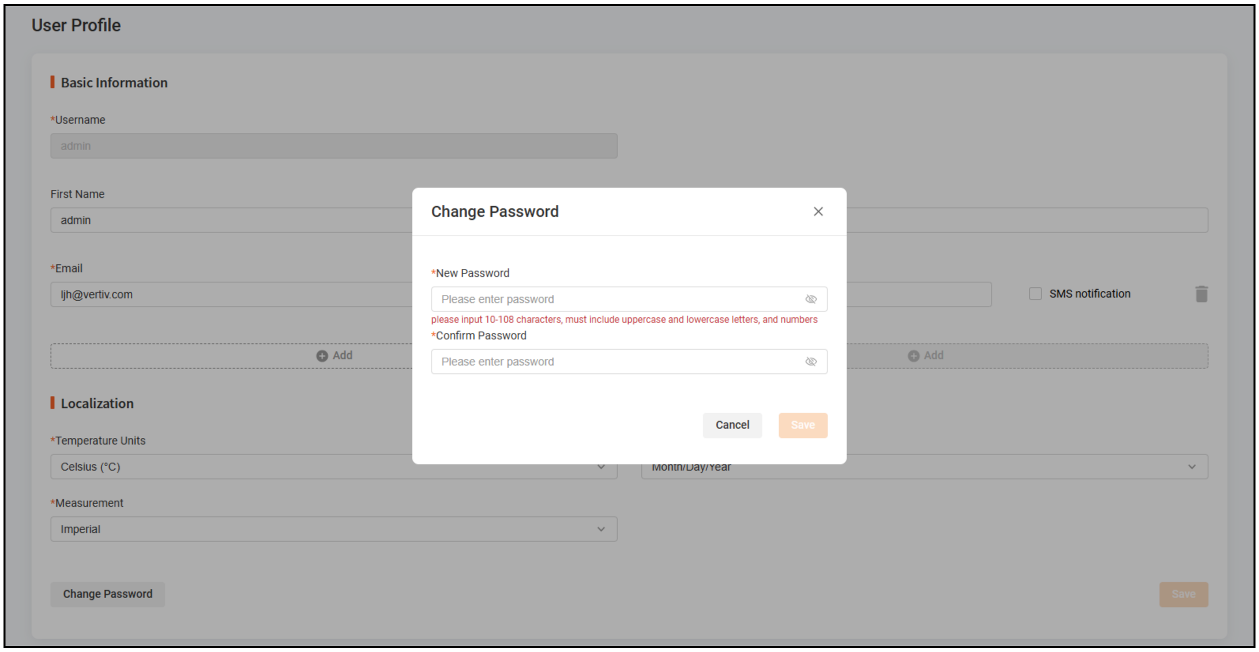
Figure 2.5 User Profile



Changing the User Password

Click the *Change Password* icon in the lower-left corner of the profile page, enter and confirm the new password in the pop-up window as shown in **Figure 2.6** on the next page , then click *Save* to apply the change. You will be logged out and redirected to the login page.

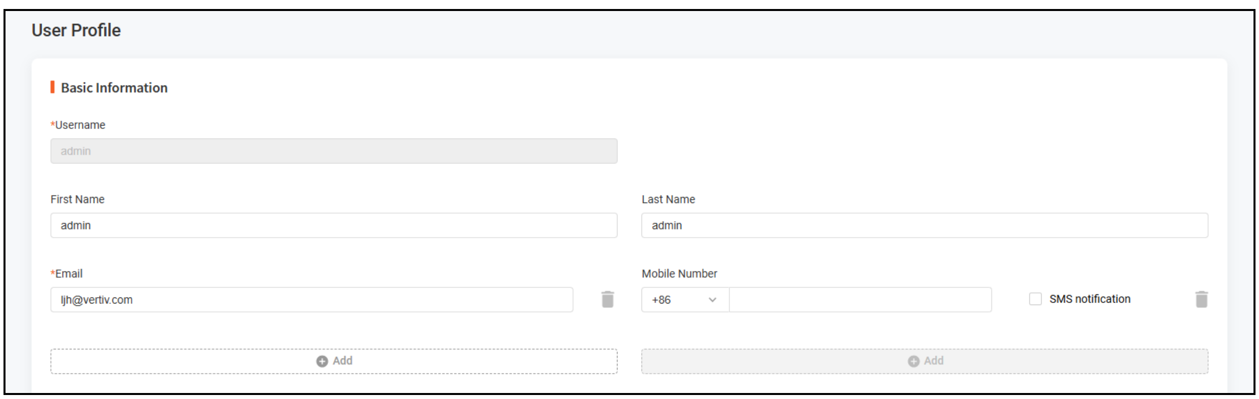
Figure 2.6 Changing the User Password



Modifying the Contact Information

In the user profile, you can modify the contact information in the basic information field, including email address (required) and mobile phone number (optional) enter the email address and phone number in the input box as shown in **Figure 2.7** below , and click Save to modify the contact information.

Figure 2.7 Modifying the Contact Information

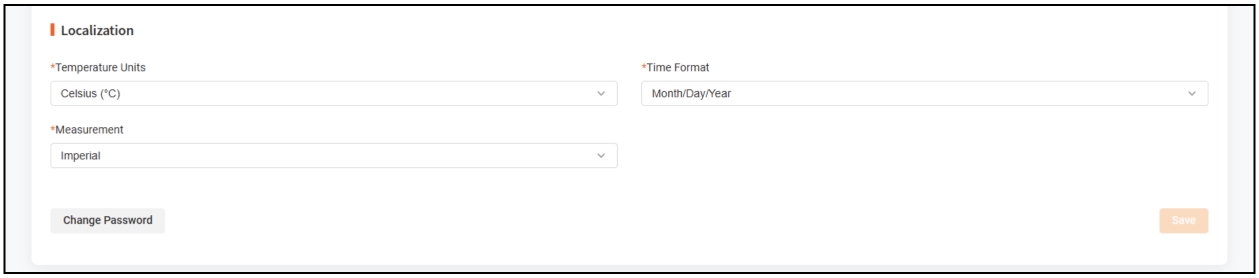


NOTE: 1. For the Phone number, select the International Country Code first, and then enter the phone number.

Modify the Localization Configuration

In the user profile, as shown in **Figure 2.8** on the facing page , Every user can modify his/her own localization configuration, including temperature units (Fahrenheit, Celsius), time format (month/day/year, day/month/year), and unit of measurement (imperial, metric). After saving the configuration, the system will display the units or time formats accordingly.

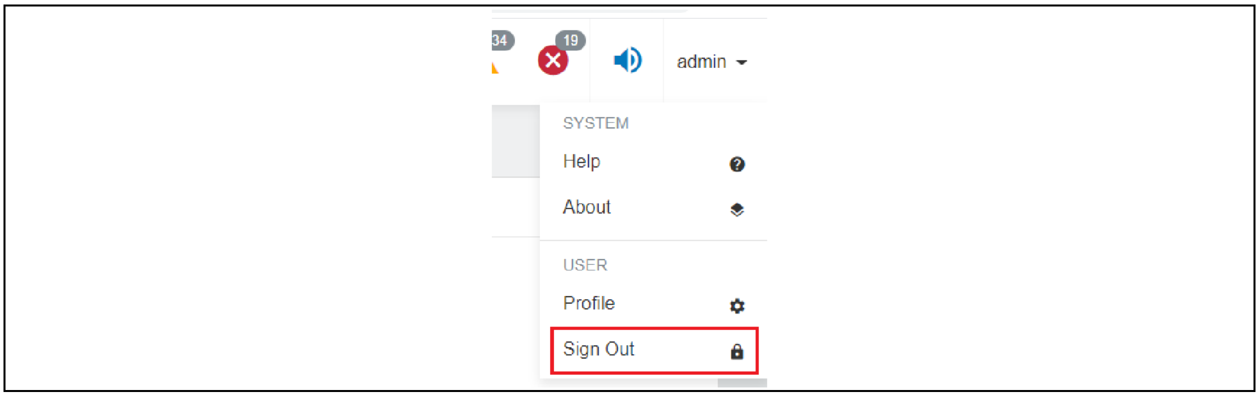
Figure 2.8 Modifying the Localization Configuration



Signing Out

Click the *Sign Out* option from the drop-down menu to the right of your Username, as shown in **Figure 2.9** below , and the system will log you out of the current user.

Figure 2.9 Signing Out



This page intentionally left blank

3 Monitoring

3.1 Overview

The monitoring home page is where you can start to monitor Smart Solution modules or SNMP devices. The home page is a module used to display the primary monitoring data of each site or location in the Smart InfraSight system. The main interface is a configuration tree. Click on the site nodes under each location to enter the monitoring home page of different sites. There are currently five supported sites: Smart Aisle sites, Smart Row sites, Smart Cabinet sites, CREMS sites and general sites.

3.1.1 Functional Modules

- Monitoring Tree
- Location
- Site
- Location: Map Navigation
- Location: 3D
- Site: Monitoring Center
- Site: Monitoring Battery Devices

3.2 Quick Start

3.2.1 SNMP Site Rapid Deployment Steps

To monitor and display SNMP devices on the SNMP site homepage:

1. Navigate to Configuration Tool > Device Management and click the *Add* button on the SNMP Device page.
2. Add devices individually or in batches.
3. At first, all SNMP devices will be added to the Default Site. Return to the Monitoring to create different sites and move SNMP devices into different sites as needed.
4. Configure widgets in SNMP sites' homepage.

You can refer to chapter Configuration Tool on page 293 for instruction on adding SNMP devices.

3.2.2 RDU Rapid Deployment Steps

To enable the RDU sites to display data properly, perform the following steps:

1. Discover the RDU device and add the RDU to the monitoring.
2. Move the added RDU site to the target location in Monitoring Tree.
3. Configure the site's monitoring homepage.

To add an RDU site, refer to Chapter 15 of the Configuration Tool for instructions on discovering and adding sites. The system supports four types of RDU sites: Smart Aisle, Smart Row, Smart Cabinet, and CREMS (Computer Room Environmental Monitoring System).

3.3 Detailed Features

3.3.1 Monitoring Tree

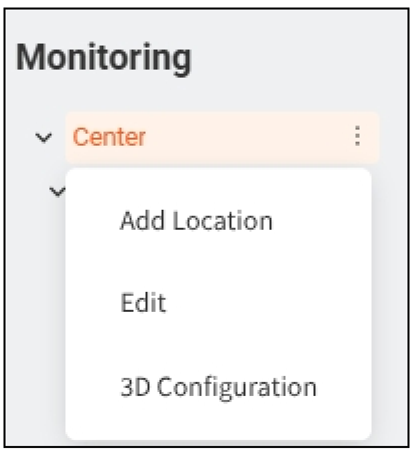
The monitoring tree consists of two levels: locations and sites. Locations form the upper level and can be nested up to seven layers deep. Sites, on the other hand, can only be attached to the lowest-level locations. A location cannot contain both sub-locations and sites; it must have one or the other.

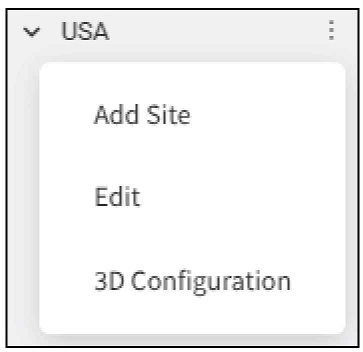
3.3.2 Location

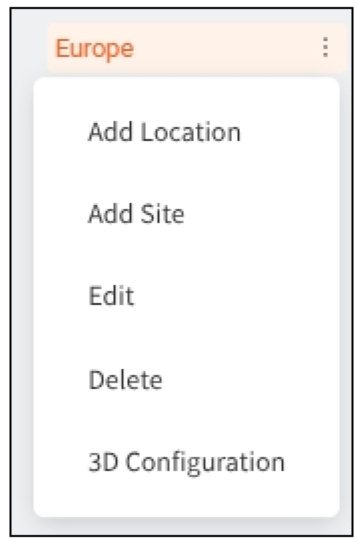
In the Monitoring Tree, there is by default a Center node, with a Default Location shown beneath it. This Default Location cannot be deleted. When an RDU site is added for monitoring, it's automatically attached to the Default Location. On the other hand, adding SNMP devices for the first time will create a Default Site under the Default Location, which includes the SNMP devices for monitoring. The Default Site also cannot be deleted.

For a Center node or a location node with only other locations beneath it, open the menu to add a new location. For a location with sites, the menu allows you to add only a new site. If a location is empty, you can add either a new site or a new location from its menu. (You can nest up to 7 layers of locations.)

Figure 3.1 Adding the Location







A pop-up window in the Center section	Pop-up window under a location that has sites	Pop-up window under a location that is empty

1. Adding a location

1. Click the *ellipsis* icon the right side of Center, click *Add Location*, as shown in Figure 3.2 on the facing page .

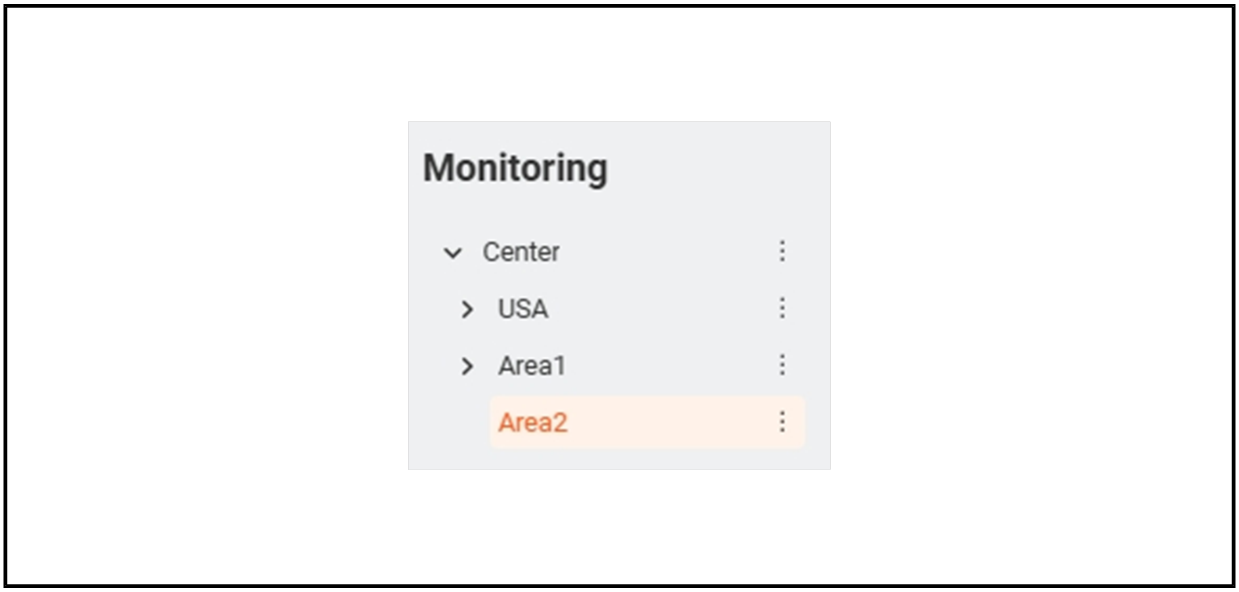
Figure 3.2 Adding a Location

2. Enter the name of the Location you want to add, for example: Area2. As shown in Figure 3.3 below .

Figure 3.3 Editing Location

3. Click *Save* to return to the home page. The added location will appear in the drop down menu, as shown in Figure 3.4 on the next page .

Figure 3.4 Newly Added Location in the Location Management Interface



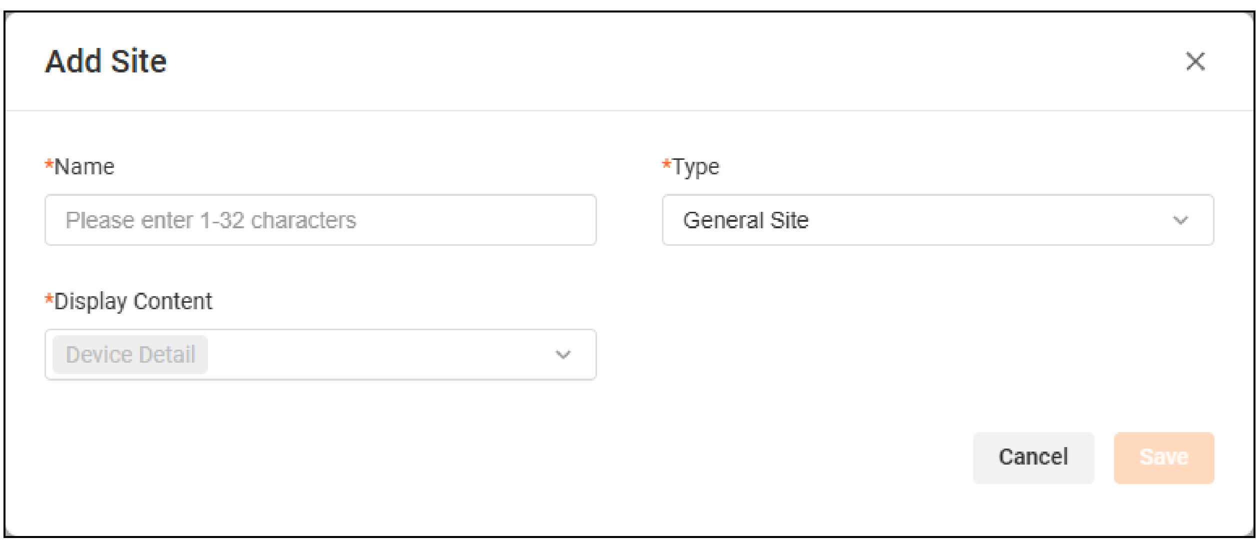
If you need to add a location under location Area2, click on the *ellipsis* on the right side of location name and repeat steps 1 to 3 .

2. Adding a Site

2.1 Adding a General Site

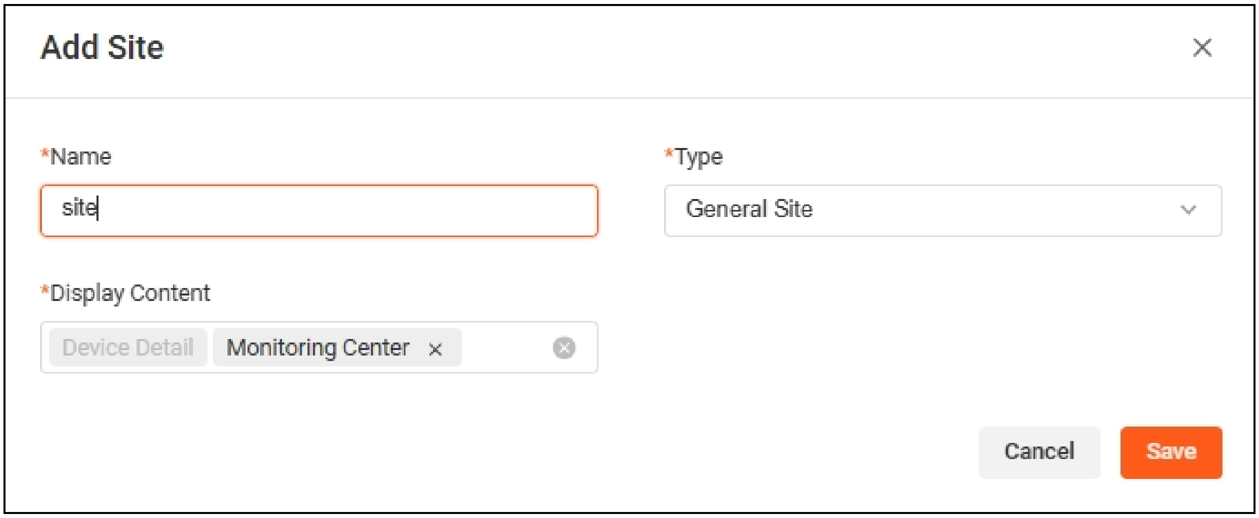
1. Take the Area2 Location as an example, click on the *ellipsis* on the right side, and select Add Site, the default selected site type is **General Site**. The General Site can be used to manage SNMP devices, as shown in **Figure 3.5** below .

Figure 3.5 Adding a General Site



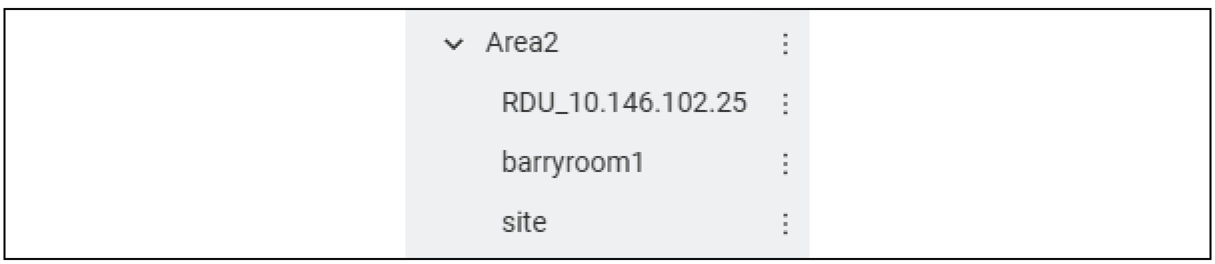
2. Enter the name of the site you want to add, for example, enter the name as **Site**. The display content controls the displaying tab in this site. You can select to display Monitoring Center, as shown in **Figure 3.6** on the facing page .

Figure 3.6 Completing the Site Addition



In Display Content drop down box, you can choose to display Monitoring Center in this site. Click *Save* to create the new site.

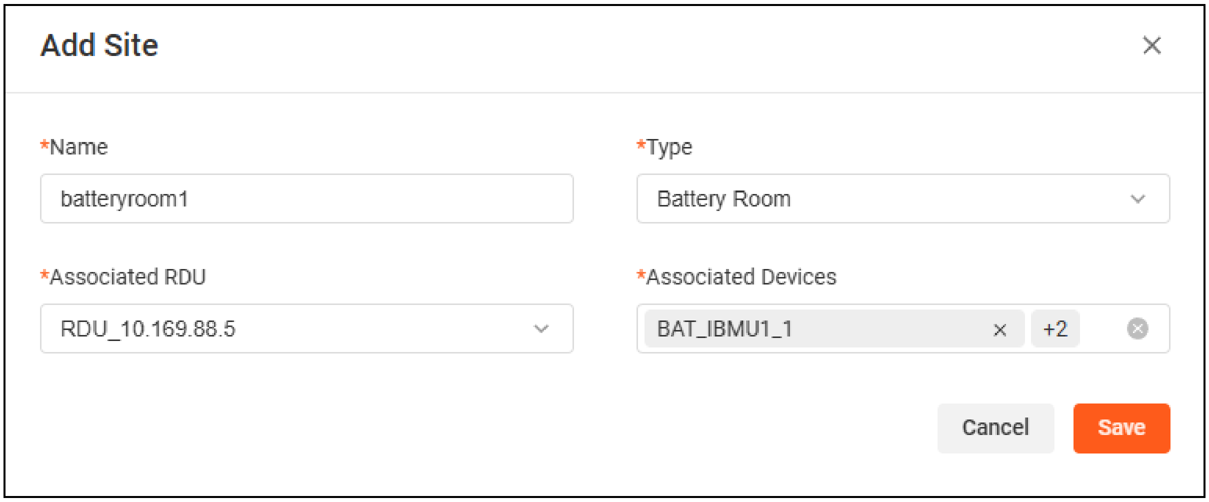
Figure 3.7 New Added Site under Area2



2.2 Adding Battery Room Sites

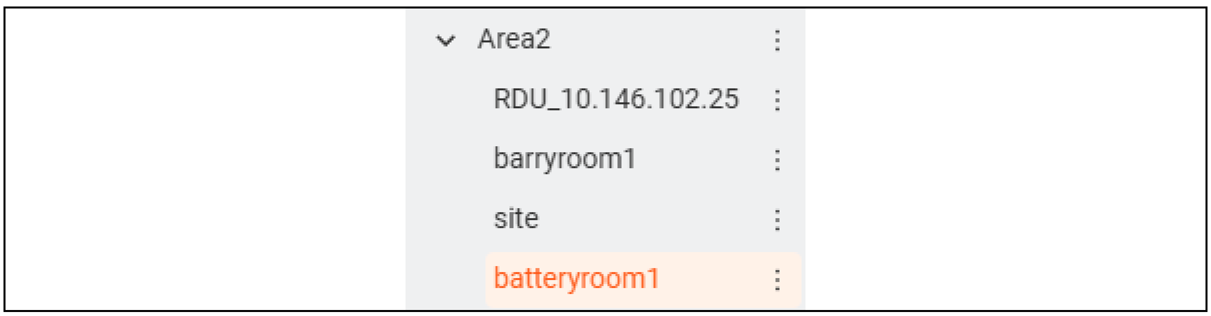
1. To add a new battery room site, select Battery Room for the site type in the Add Site pop-up window, and select the associated RDU and device. When you select the associated devices, you can move lithium battery devices, lead-acid battery devices, UPS and power meter devices from the RDU site to the new battery room site, as shown in Figure 3.8 on the next page .

Figure 3.8 Added Battery Room Type Site



2. Click *Save* to return to the home page. As shown **Figure 3.9** below .

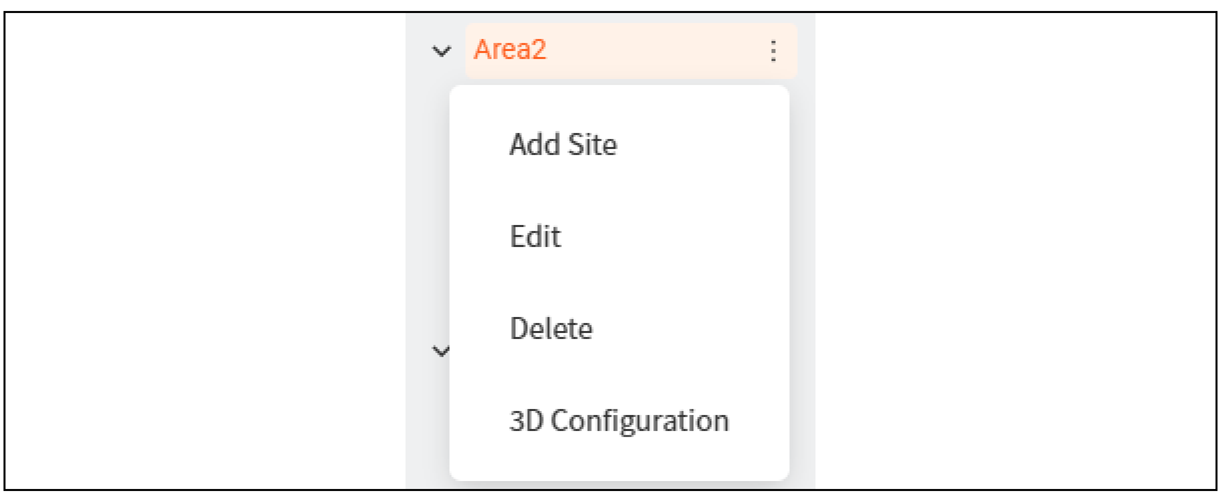
Figure 3.9 The Newly Added Battery Room Site



3. Editing Location:

3. Open the menu of the location and click the *Edit* button, as shown **Figure 3.10** below .

Figure 3.10 Action Menu

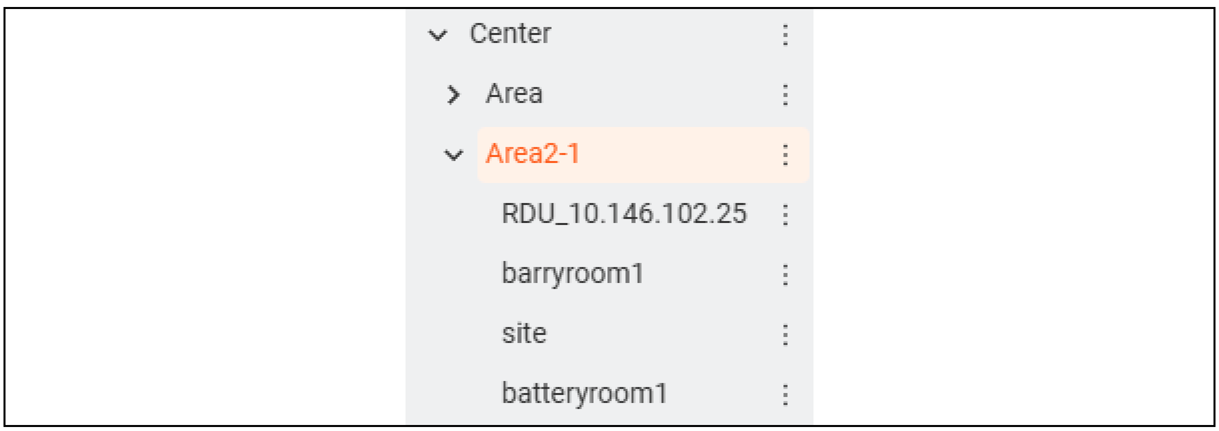


You can modify the name of the location, as shown in **Figure 3.11** below .

Figure 3.11 Edit Location

Click *save*, as shown in **Figure 3.12** below .

Figure 3.12 Location Management Page



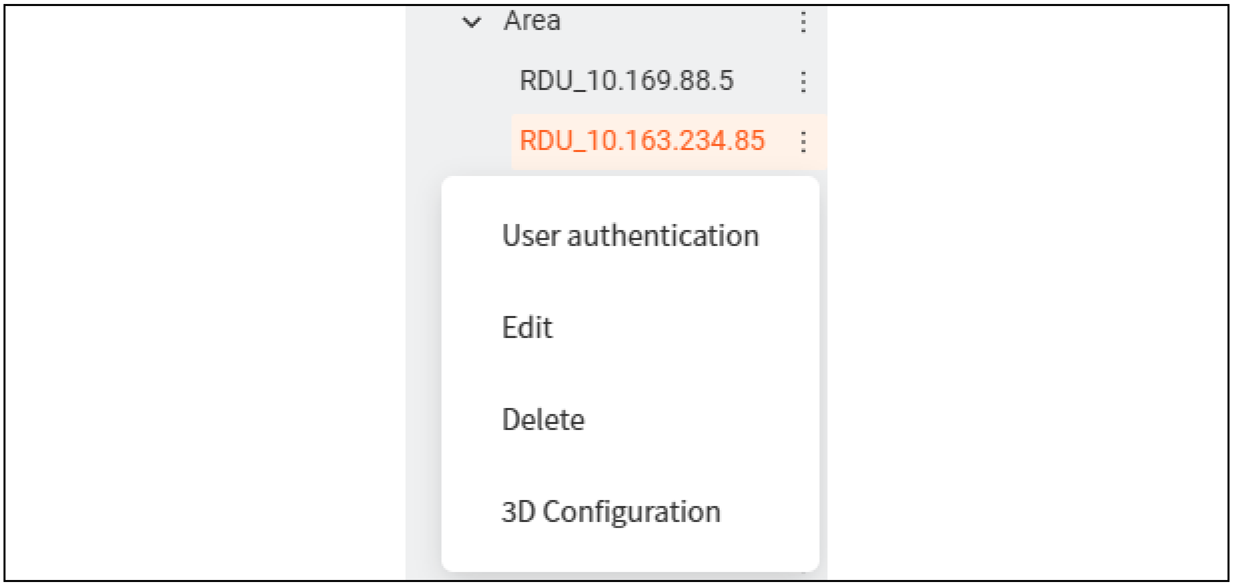
3.3.3 Site

Site types available: RDU site, General Site, Battery Room site.

1. RDU Site

There are several types of RDU sites: Smart Aisle, Smart Row, Smart Cabinet, CREMS (CREMS site is a site using an independent RDU for device monitoring which is not installed in a Smart Solutions product). Different types of RDU sites differ only in 3D configuration. The user can click on the *ellipsis* on the right side of the site to operate the site, and there is user authentication, editing, deleting, and 3D configuration operations. As shown in **Figure 3.13** on the next page .

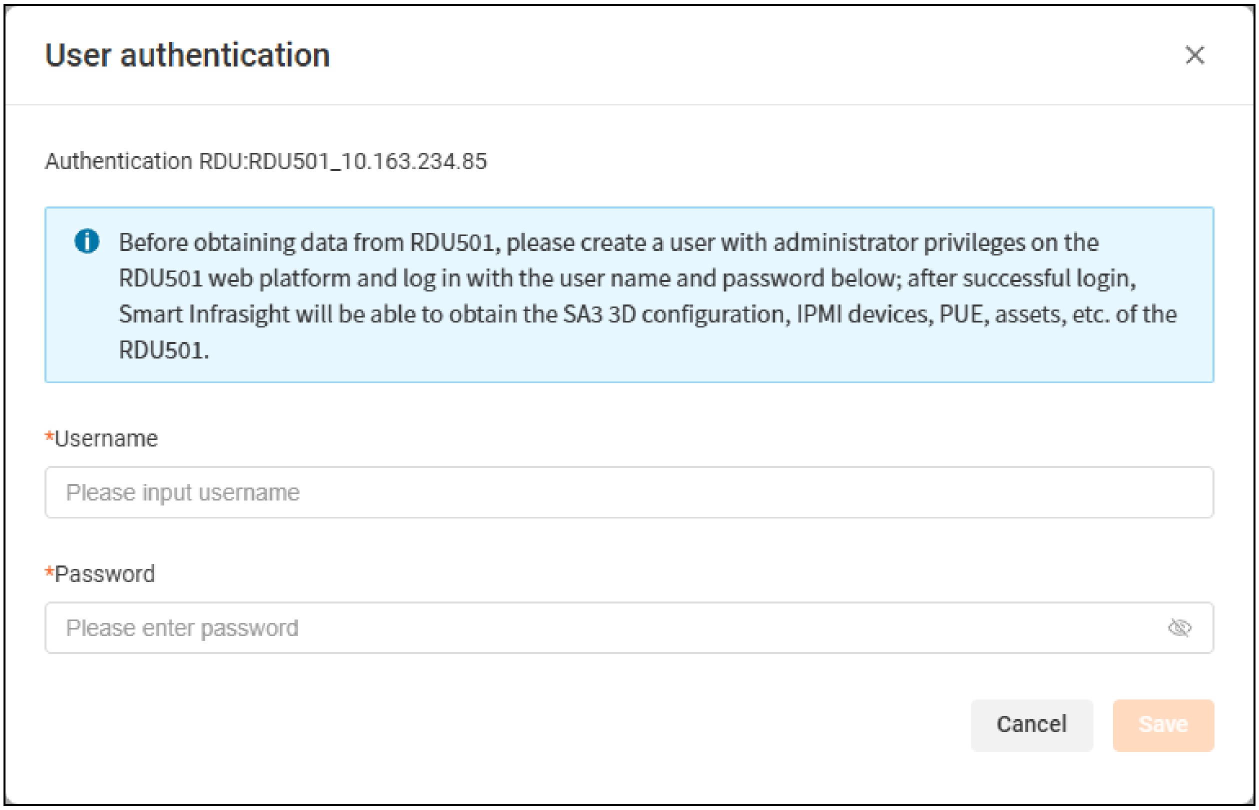
Figure 3.13 RDU Site Action Menu



By clicking the User authentication button, you can enter the administrator account and password for the corresponding RDU. Once authentication is successful, Smart Infrasight can retrieve data from the RDU, including the 3D layout of Smart Aisle, Smart Row, Smart Cabinet, IPMI device information, PUE, and more. As shown in Figure 3.14 on the facing page .

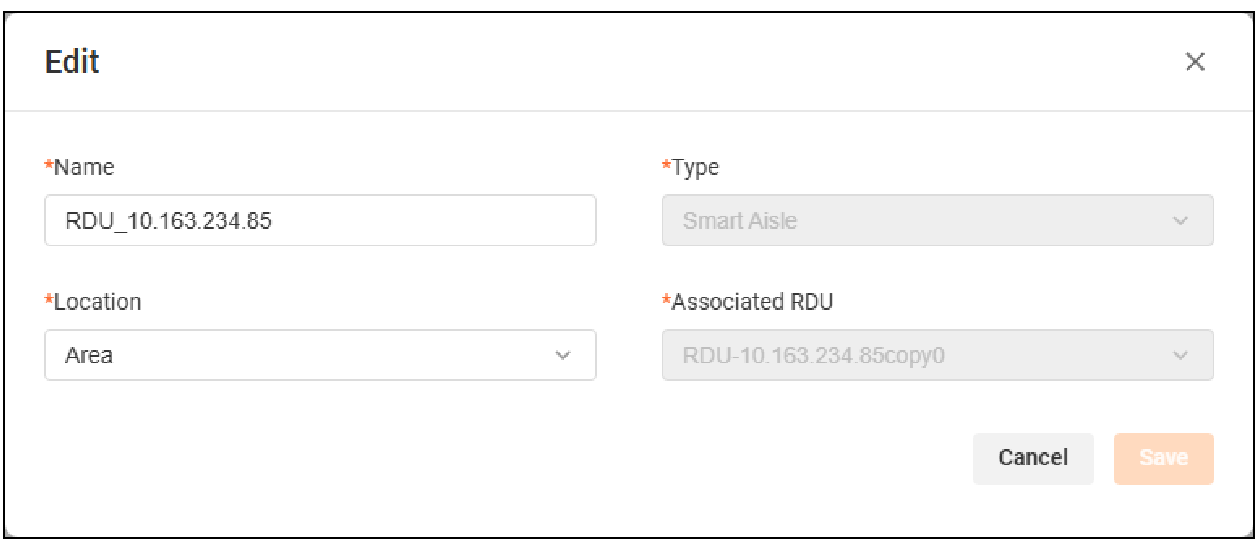
NOTE: It is recommended to not user the default RDU admin account here as Smart Infrasight will log out the RDU admin user out constantly. We recommend you create a second admin account in the RDU and enter those details here.

Figure 3.14 Pop-up interface — User Authentication



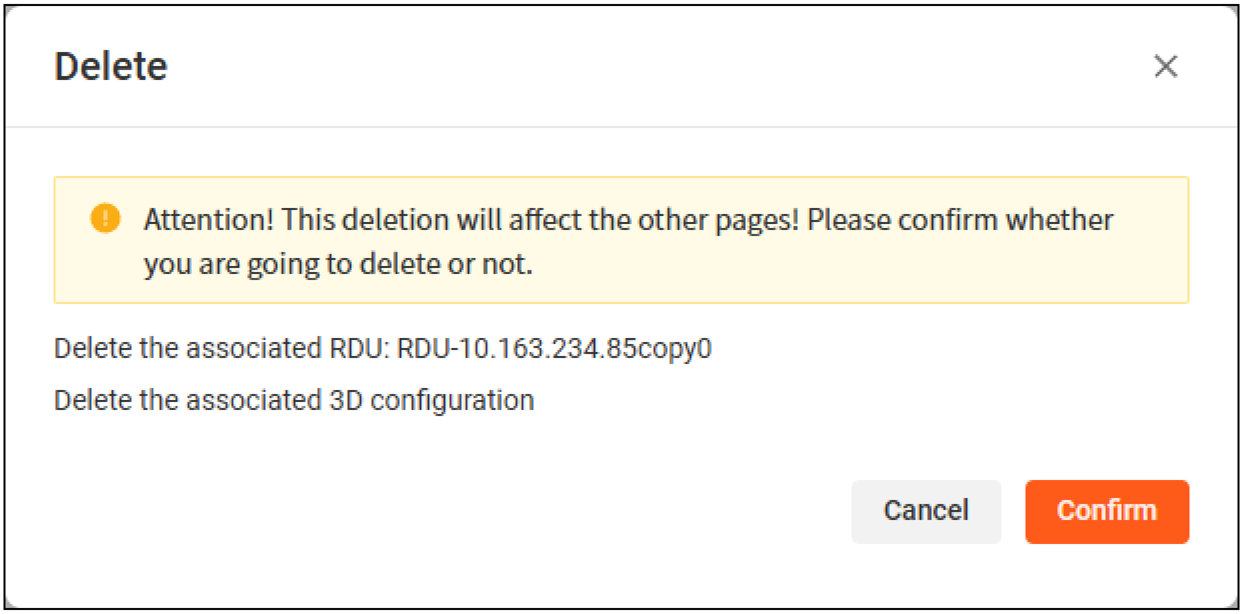
Click the *Edit* button, you can modify the current site name, location, and you can also see the site type of the current site and the RDU bound to the site, as shown in **Figure 3.15** below .

Figure 3.15 Editing the Site



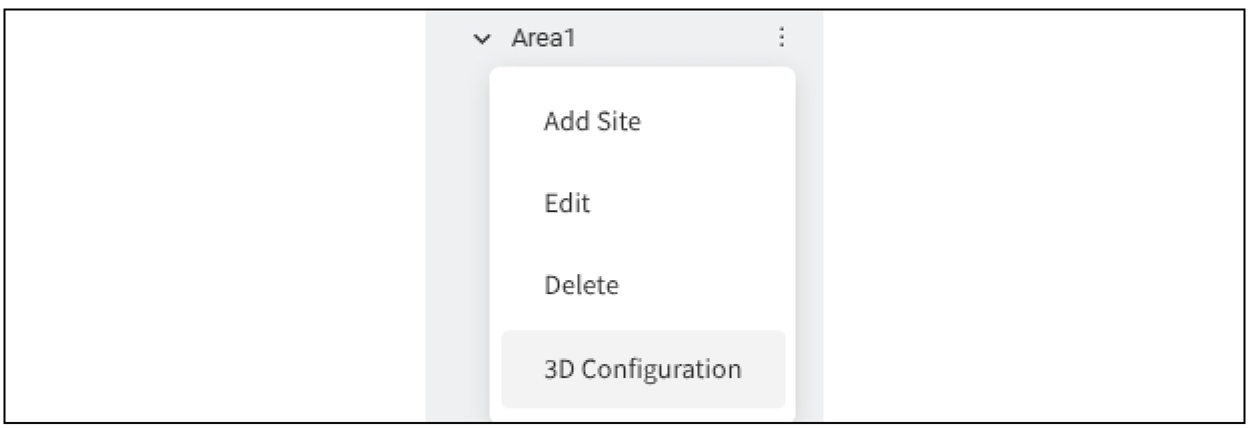
Click the *delete* icon to delete the site as follows **Figure 3.16** on the next page .

Figure 3.16 Site Deletion Popup Box



Click the *3D configuration* button to enter the 3D configuration interface of the current site as shown in Figure 3.17 below , refer to Chapter 4 3D Configuration for details.

Figure 3.17 3D Configuration Interface Selection

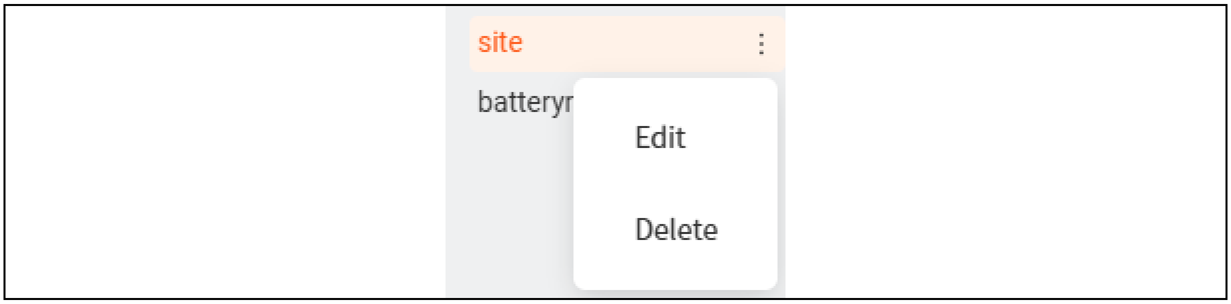


NOTE: 3D configuration currently supports Smart Aisle2, Smart Aisle3, Smart Row2 and CREMS RDU Site, Battery Room Site.

2. General Site

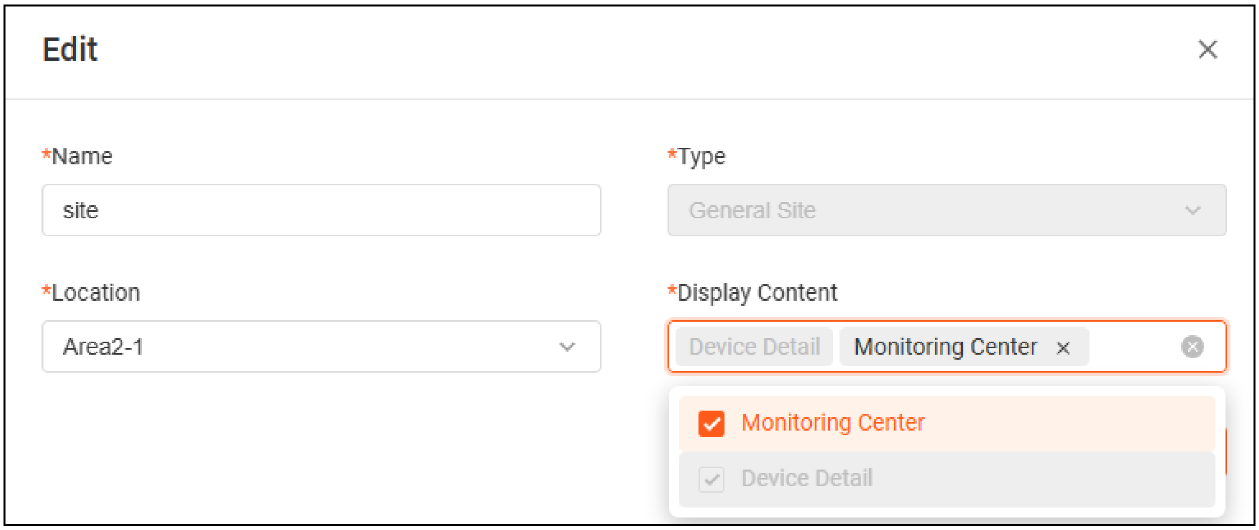
Click the *Edit* button, to modify the current site name, location and display content. By modifying the display content, you can display or hide the Monitoring Center of the site, as shown in Figure 3.18 on the facing page .

Figure 3.18 General Site Action Menu



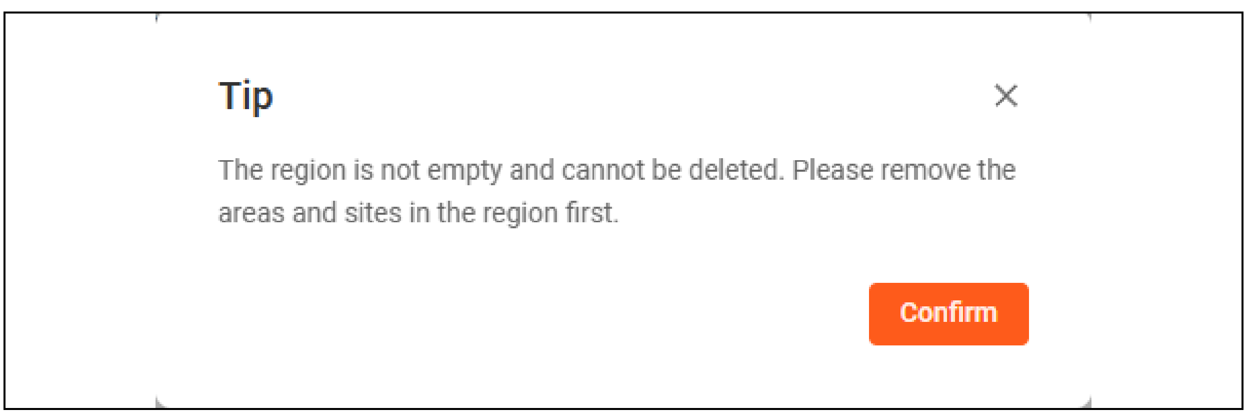
Click the *Edit* button to modify the current site name, location, and display content. By changing the Display Content, you can display or hide the Monitoring Center of the site, as shown in Figure 3.19 below

Figure 3.19 The General Site Edit Popup Box



Click on the *delete* , if there is a monitoring device under the site, it will prompt that it cannot be deleted, and the device in the site needs to be removed to allow the deletion, as shown Figure 3.20 below .

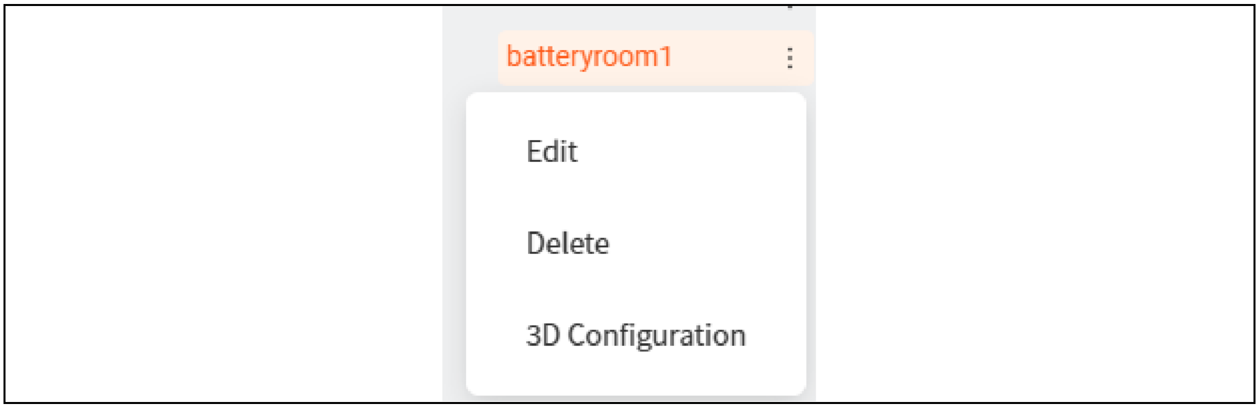
Figure 3.20 The Device Deletion Popup Box



3. Battery Room Site

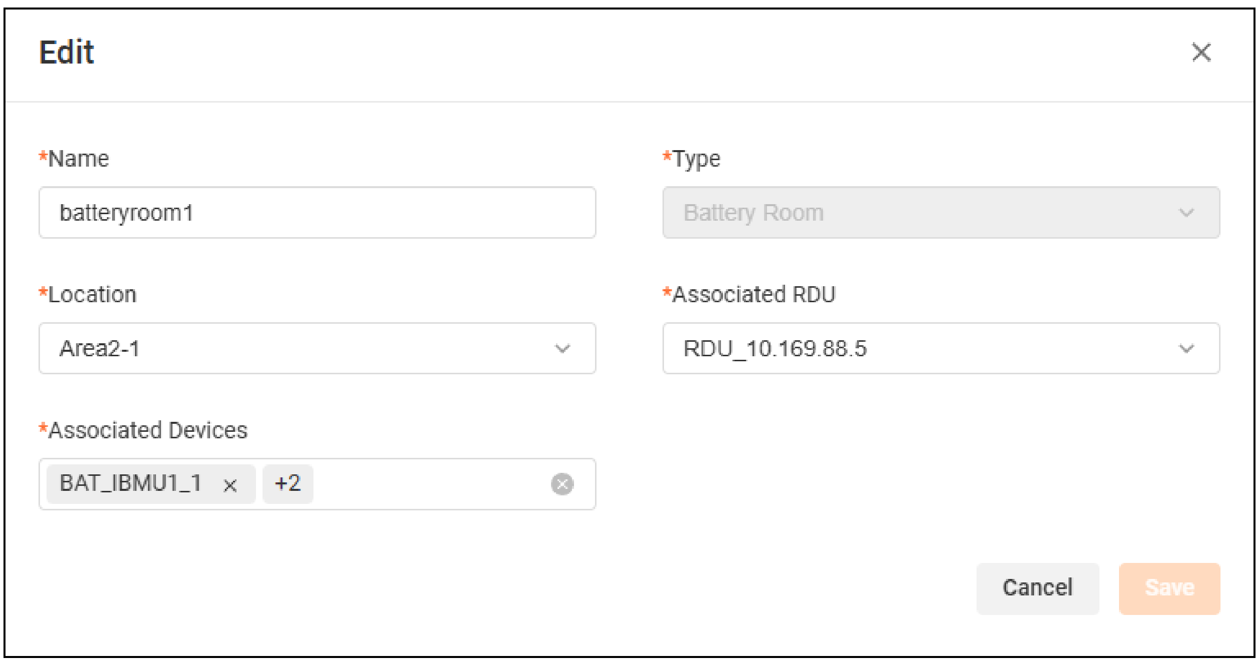
The user-created battery room site can be associated with the corresponding RDU site. Battery and other devices can then be moved from the RDU site to be managed under the battery room site. Take a battery room site as an example, click the *ellipsis* on the right to pop up the action menu. As shown in Figure 3.21 below .

Figure 3.21 Battery Room Site Action Menu



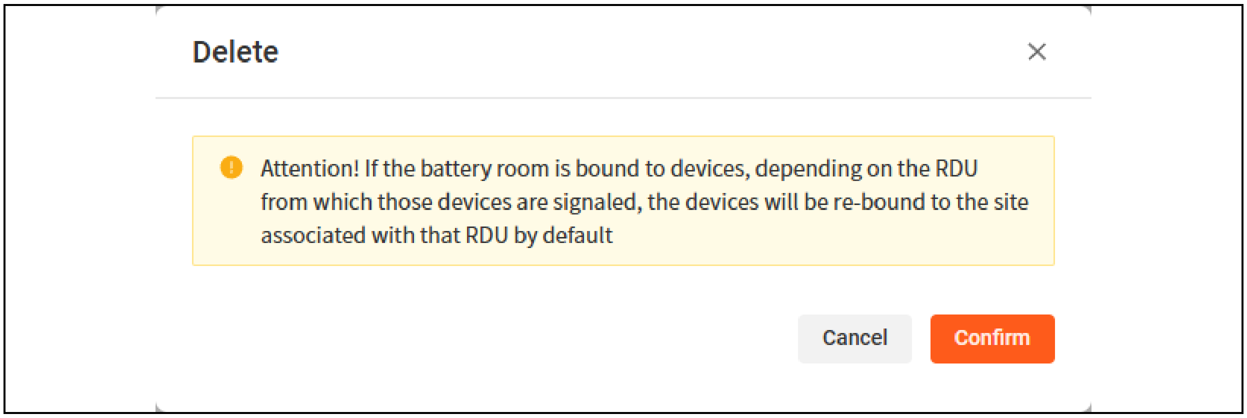
Click the *Edit* button to modify the battery room's name, location, and associated RDU. Then, select the devices within Associated Devices to be placed in the battery room site, including lithium batteries, lead-acid batteries, UPS units, and power meters. as shown in Figure 3.22 below .

Figure 3.22 Editing Battery Room Site



Click the *delete* button, once the battery room site has been deleted, the device bound to the battery room will be re-bound to the RDU site where the devices are originally monitored, as shown below Figure 3.23 on the facing page .

Figure 3.23 Delete the Popup Box for the Battery Room



3.3.4 Location: Map Navigation

When you click on any location (or Center) nodes in the Monitoring Tree, you will be directed to the Map Navigation page. Here, you can customize the background map image and adjust the positions of sites within that location. This allows you to visualize the geographical relationships between different sites under the selected location node.

1. Customizing the Background Image

In the location's Map Navigation page,, click on the settings icon in the right corner of the Map Navigation area, and click *Edit Background*. As shown in the **Figure 3.24** below .

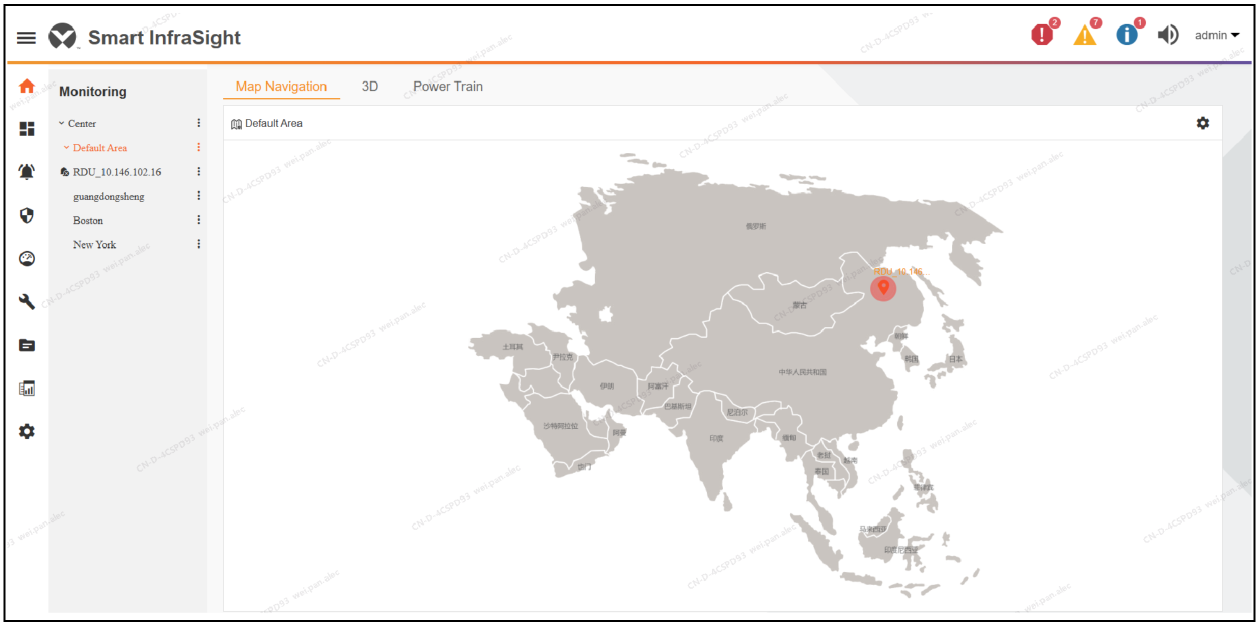
Figure 3.24 Editing Background Image

Select a background image and click *Save* to set the background image.

2. Editing the Site Location

In the location's Map Navigation page, click on the settings icon in the right corner of the Map Navigation area, and click *Edit* Location. As shown in **Figure 3.25** on the next page .

Figure 3.25 Editing the Site Position

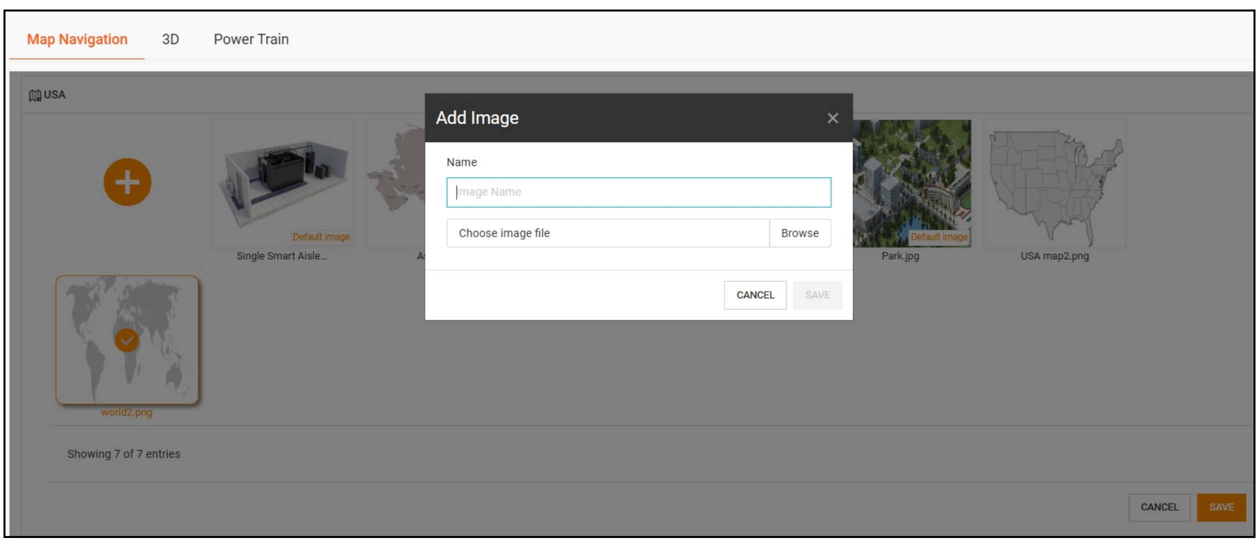


Drag the site icon to a target position and click *Save* in the bottom right corner.

3. Uploading a custom Background Image

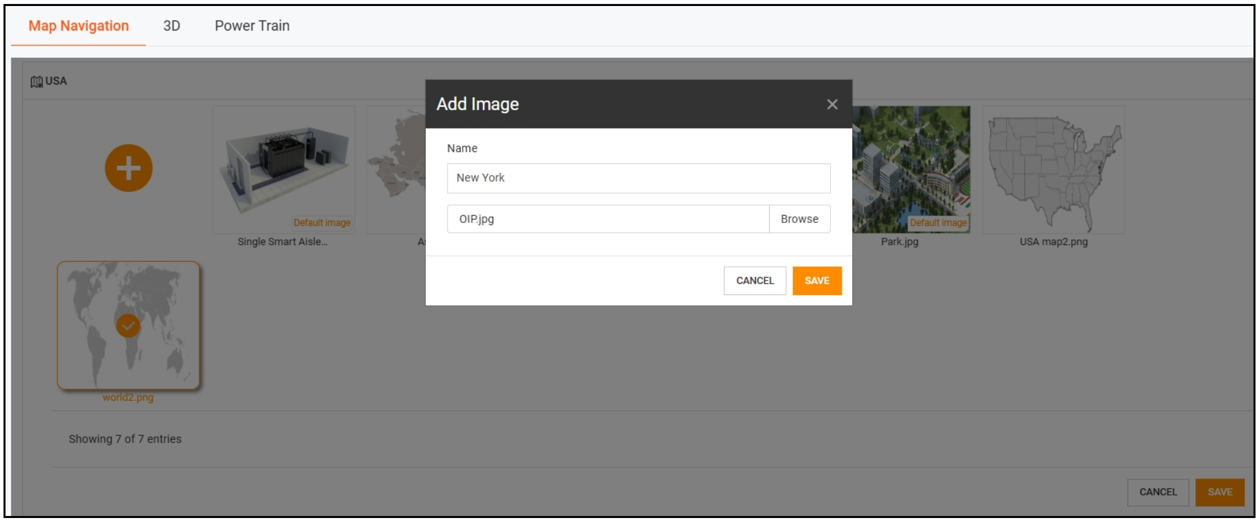
Go to the Edit Background page, click on the *Add Image button*, as shown in **Figure 3.26** below .

Figure 3.26 Adding Image Popup Window



Enter a name for the image, select a path for the image as shown in **Figure 3.27** on the facing page , and click *Save*. (You cannot upload a picture with the same name, and the size of the picture cannot exceed 10MB).

Figure 3.27 Uploading a Custom Background Image

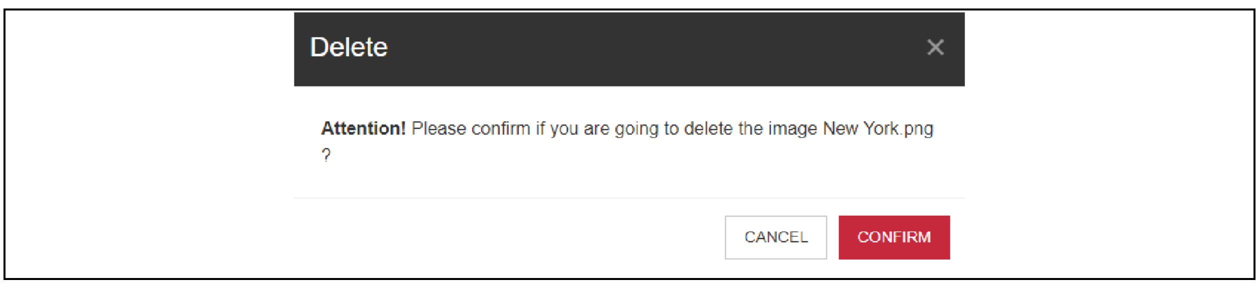


NOTE: Only PNG, JPG, and GIF formats are supported.

4. Deleting the Background Image

Go to the list of background images and click the *X* in the upper right corner of the image and confirm deletion as shown in Figure 3.28 below .

Figure 3.28 Deleting the Background Image



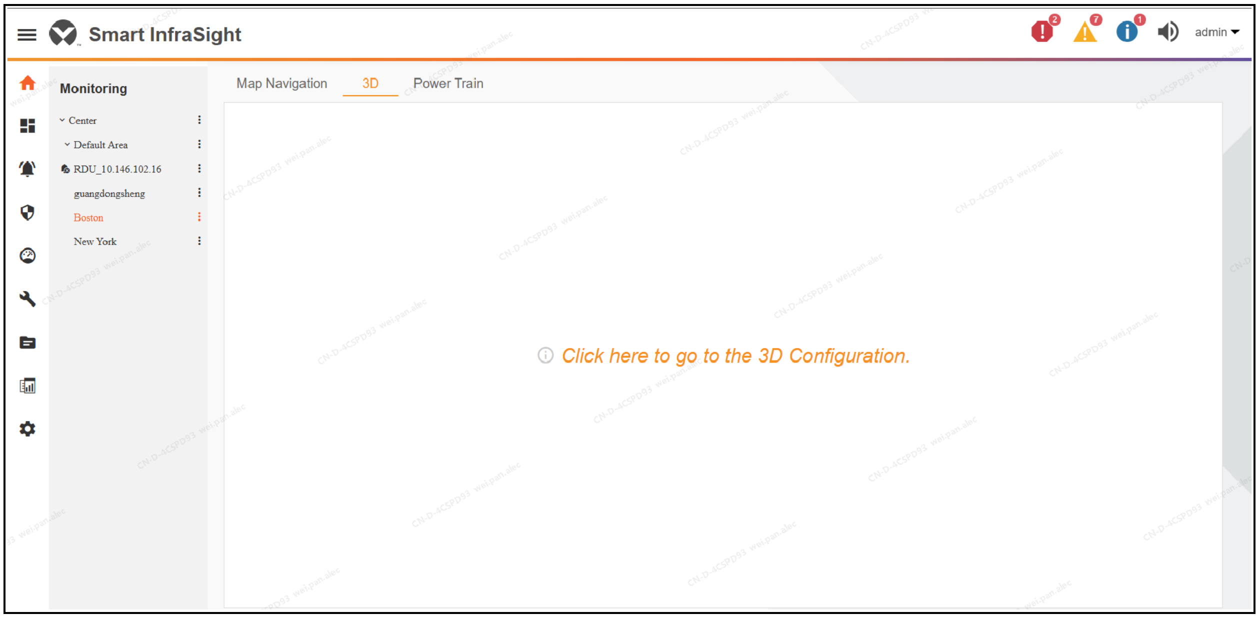
NOTE: The default image cannot be deleted.

3.3.5 Location: 3D

There are two ways to enter the 3D configuration.

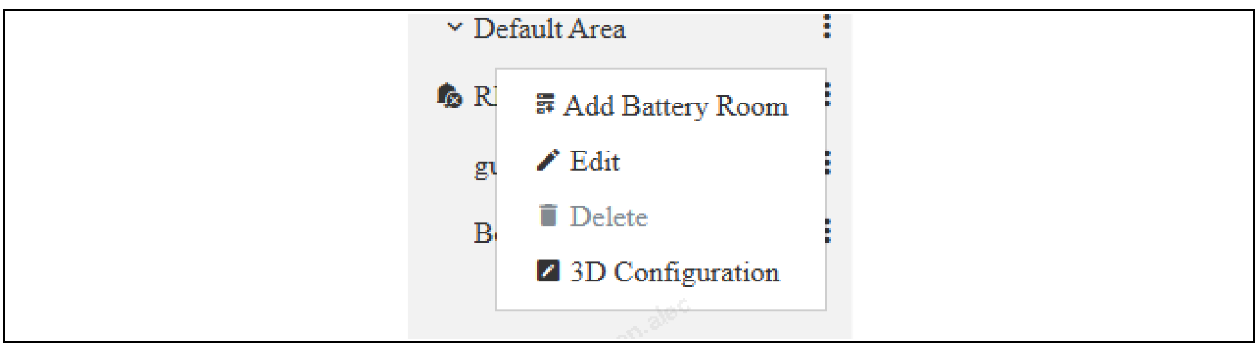
1. After adding a Smart Solutions site for the first time the user will need to configure the 3D image. Click the *3D link* on the page which will jump to 3D configuration area, as shown in Figure 3.29 on the next page .

Figure 3.29 Entering Location 3D Configuration Path 1



2. Click the *ellipsis* button on the right side of the location node in Monitoring Tree, and select the 3D configuration, as shown in **Figure 3.30** below .

Figure 3.30 Location 3D Configuration Path 2



For more instructions about how to configure the 3D location, refer to Chapter 4.3 3D Configuration Detailed Functions .

3.3.6 Site: Monitoring Center

The site monitoring home page at most includes 5 parts:

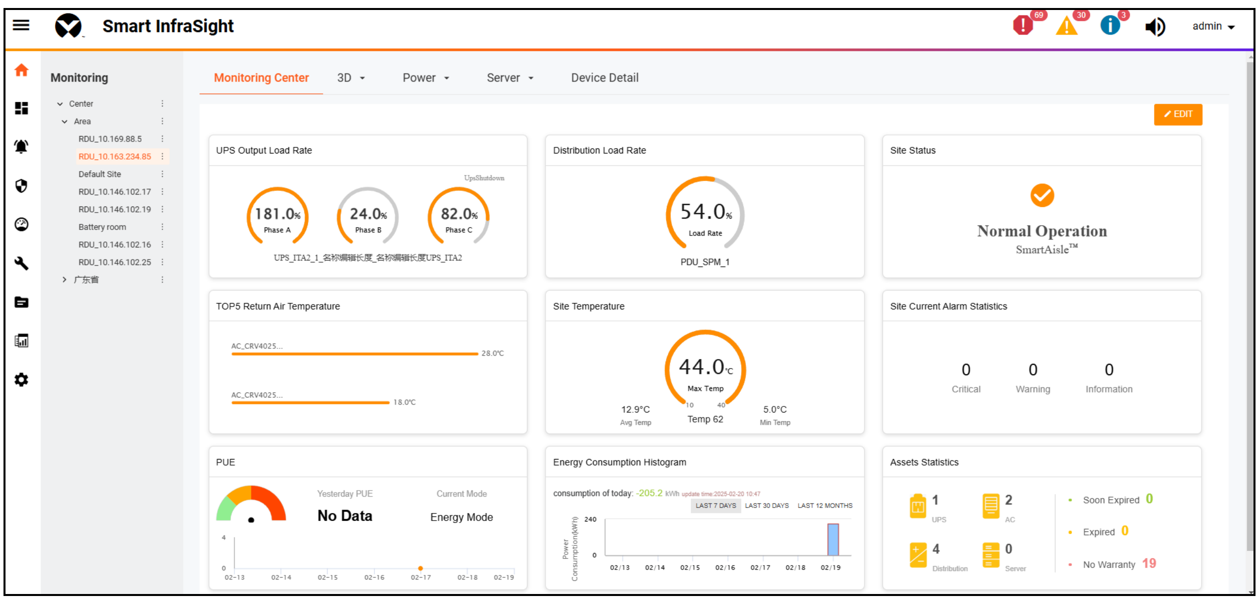
- Monitoring Center
- 3D
- Power
- Server
- Device Details

For SNMP sites, Monitoring Center can be edited in the same way as Dashboard, you can freely add widgets, change the size and position of the widgets, and customize the key signals you want to display in the widgets, you can refer to chapter9 Dashboard for more details on the configuration.

For RDU sites, there are 9 default widgets in the monitoring center, displaying information including as shown in **Figure 3.31** below .

- UPS Output Load Rate
- Distribution Load Rate
- Site Status
- Top 5 Return Air Temperature
- Site Temperature
- Site Current Alarm Statistics
- PUE
- Energy Consumption Bar Charts
- Asset Statistics

Figure 3.31 Monitoring Home Page

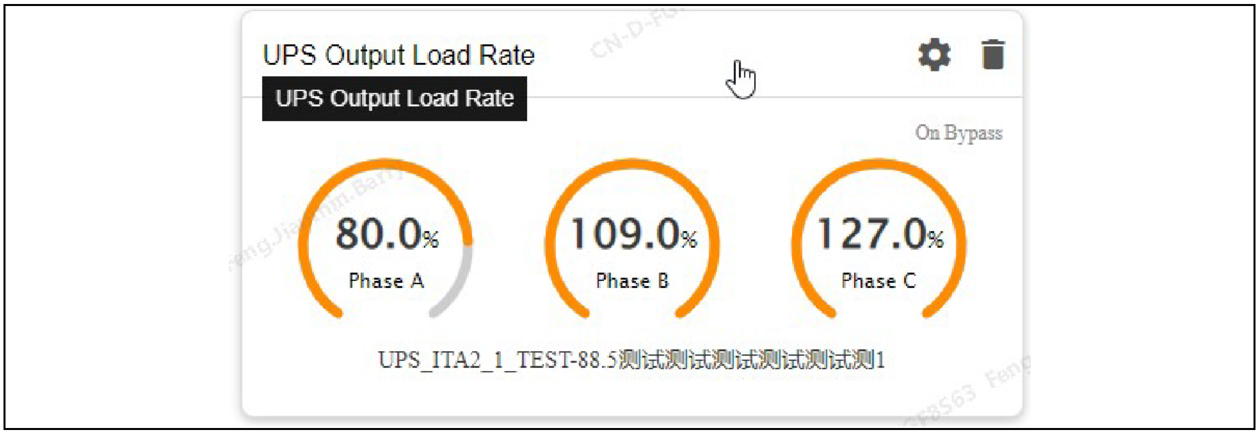


By default, the monitoring home page displays the 9 widgets of the current site, and the user can delete, edit, add, and drag the 9 widgets by selecting the Edit button in the upper right corner.

1. Deleting the Widgets

1. Hover over the widgets header to see the setting button and delete button, as shown in **Figure 3.32** on the next page .

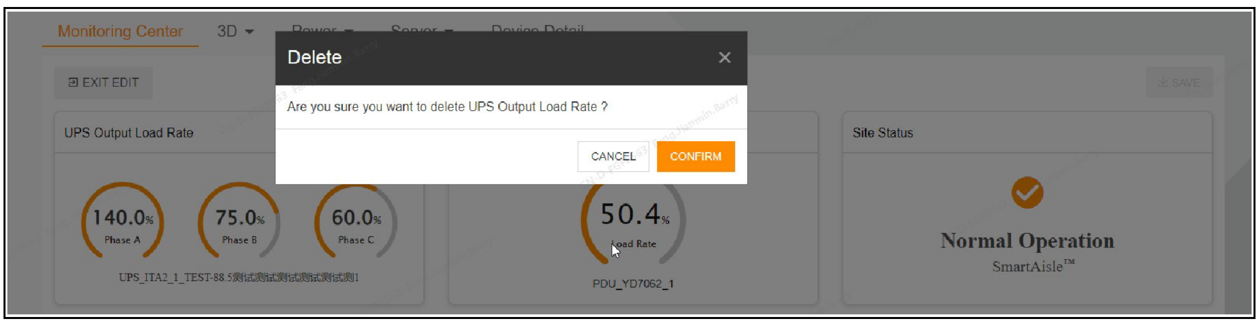
Figure 3.32 Deleting the Widget



Click the *Delete* icon, and a pop-up box prompts the user to decide whether to delete the widgets.

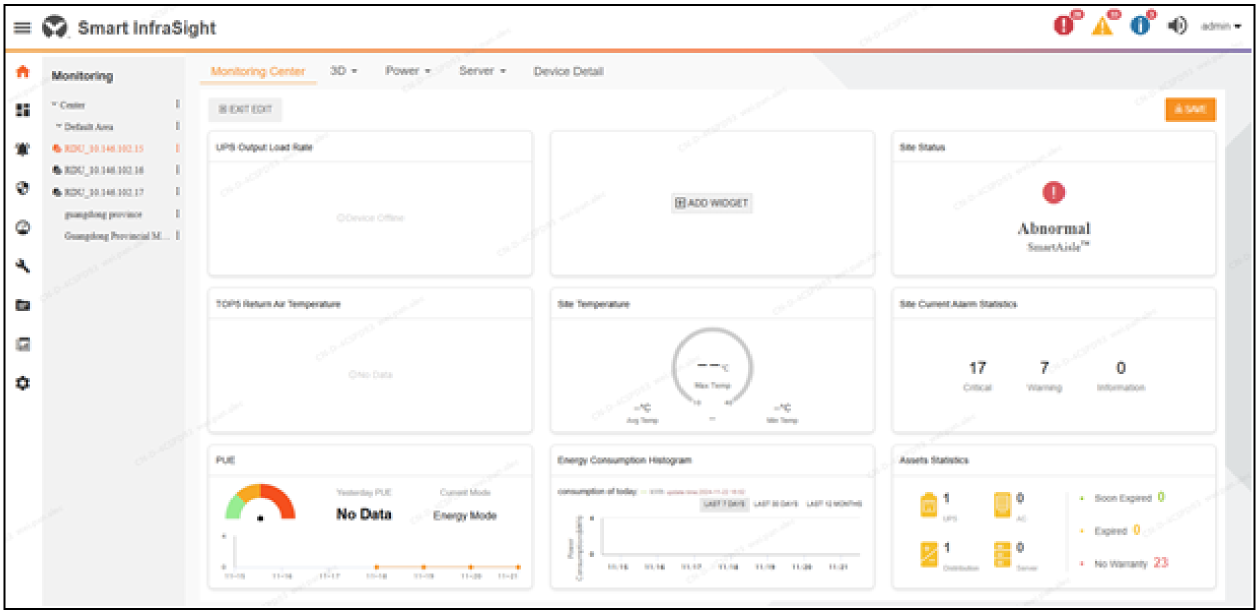
Click *Confirm* to delete the current widgets, as shown in Figure 3.33 below .

Figure 3.33 Deletion Popup Window



After the modification is completed, click *save* in the upper right corner to save the current editing status and to confirm the deletion operation.

Figure 3.34 The Monitoring Home page after Deletion



2. Editing the Widgets

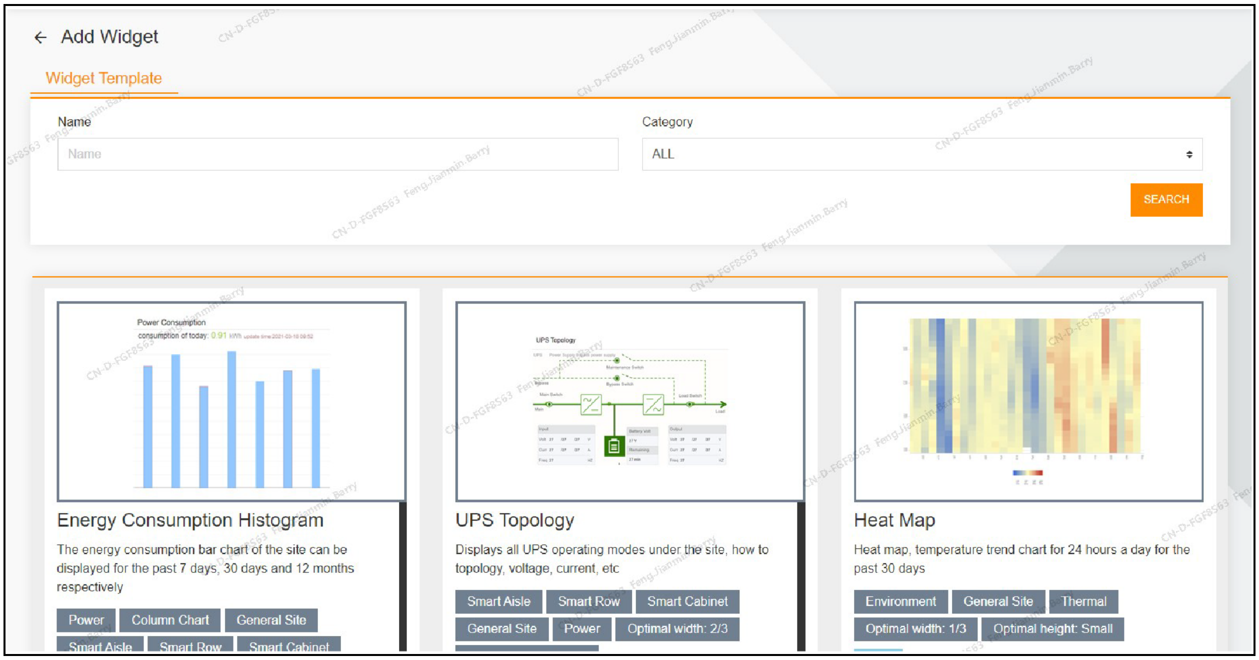
After entering the edit state, click the edit button of the widget, and the config pop-up window will appear as shown in **Figure 3.35** below .

Figure 3.35 Editing a Widget

3. Adding New Widgets

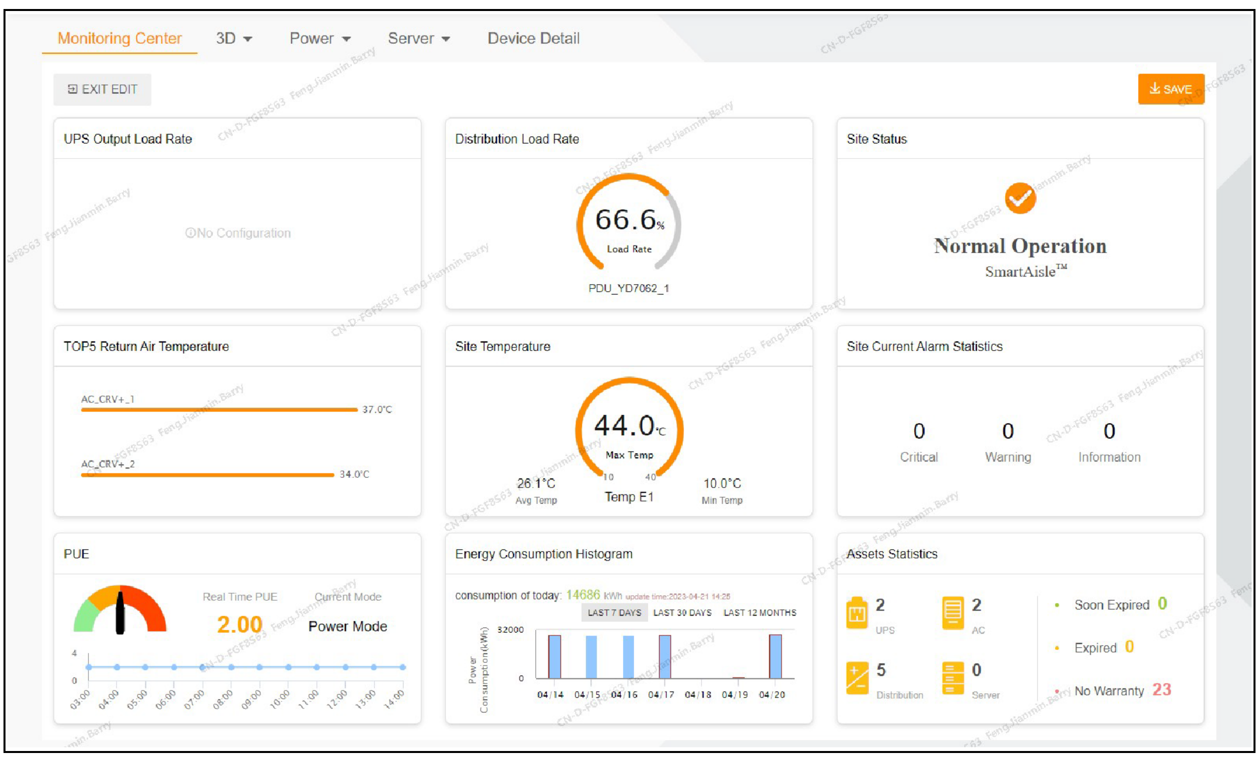
Enter Edit mode by clicking the *Edit* button on the upper right corner of the monitoring homepage, clicking on the *Add Widget* button of the blank widget, and you will be redirected to the Add Widget page, as shown in **Figure 3.36** on the next page .

Figure 3.36 Adding Widgets Page



You can select the target widget. Click *Add* to complete the addition in the edit state. As shown in **Figure 3.37** below .

Figure 3.37 After Adding the Widgets



The new widget is unconfigured by default. You can edit the widget name and detailed configuration in the Config pop-up window. After finishing editing the monitoring homepage, click the save button in the upper right corner.

4. Dragging and Dropping Widgets

Click the *edit* icon in the upper right corner, enter the editing state, hover the mouse over the head of the widgets. The mouse cursor changes to a small hand, allowing you to drag and move the widget to the desired position.

Power Distribution and Thermal Monitoring

For details on configuring the third tab of the monitoring home page, please refer to Single-Site Power Distribution and Thermal on page 157.

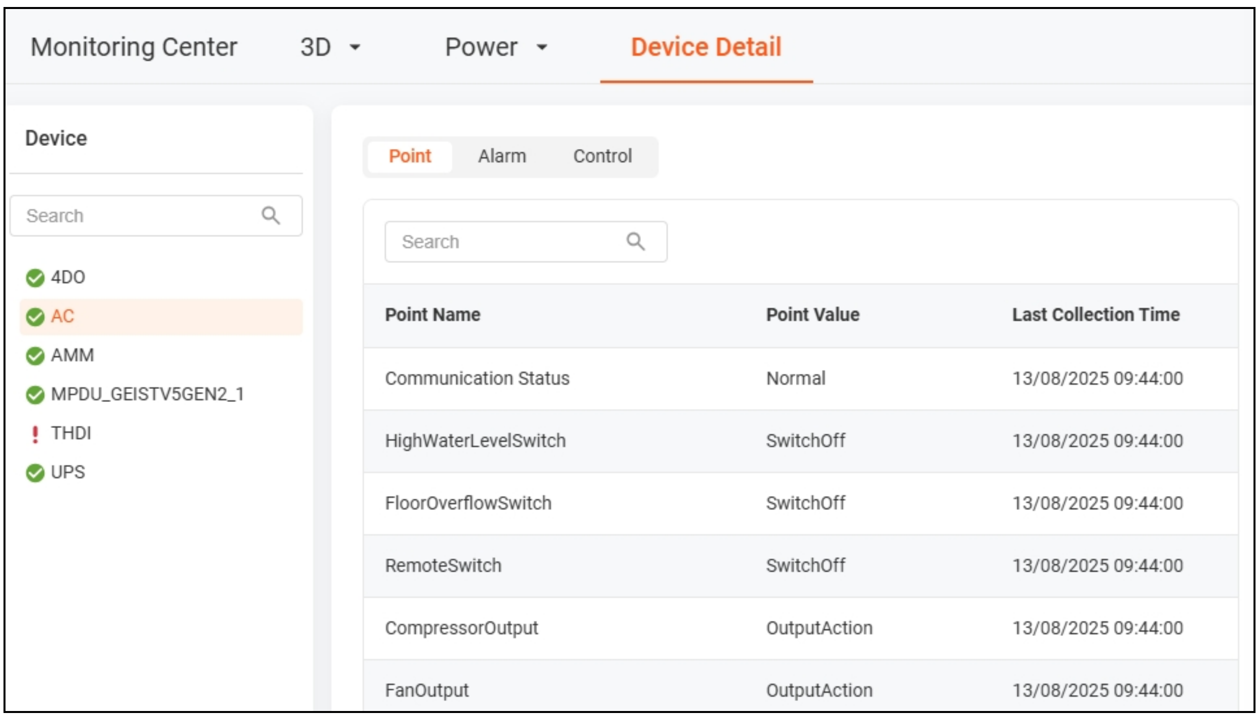
Server

At the RDU501 site, IPMI devices such as servers and switches can be monitored using Smart Infrasight via RDU501. For more information on monitoring IPMI devices, please refer to IT Management on page 165.

Device Details

The Device Details section displays all monitored devices at the current site, including their signal points, alarms, and control points, and the page is displayed as shown in Figure 3.38 below .

Figure 3.38 Device Details Page



Select a device to display its real-time data on the right side. This information updates every minute. For hourly stored numeric points, you can click on the point to view its historical line chart, as shown in Figure 3.39 on the next page .

Figure 3.39 Device Point Page

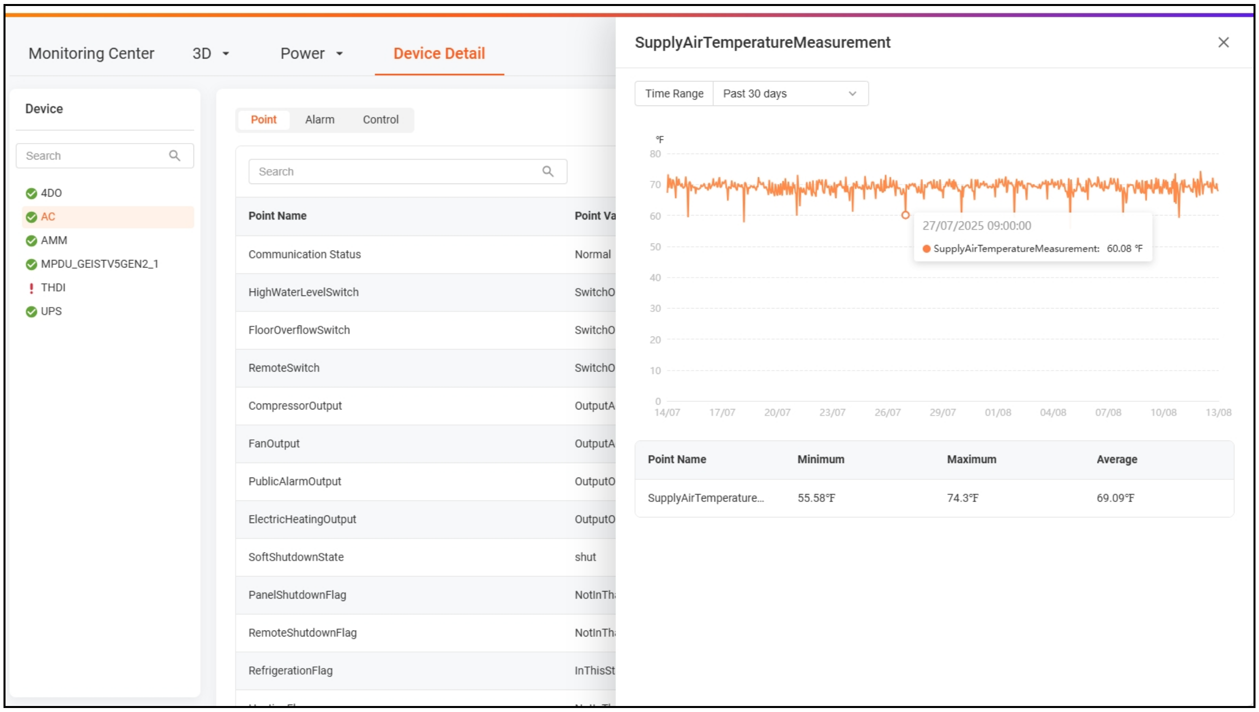


Figure 3.40 Device Alarm Page

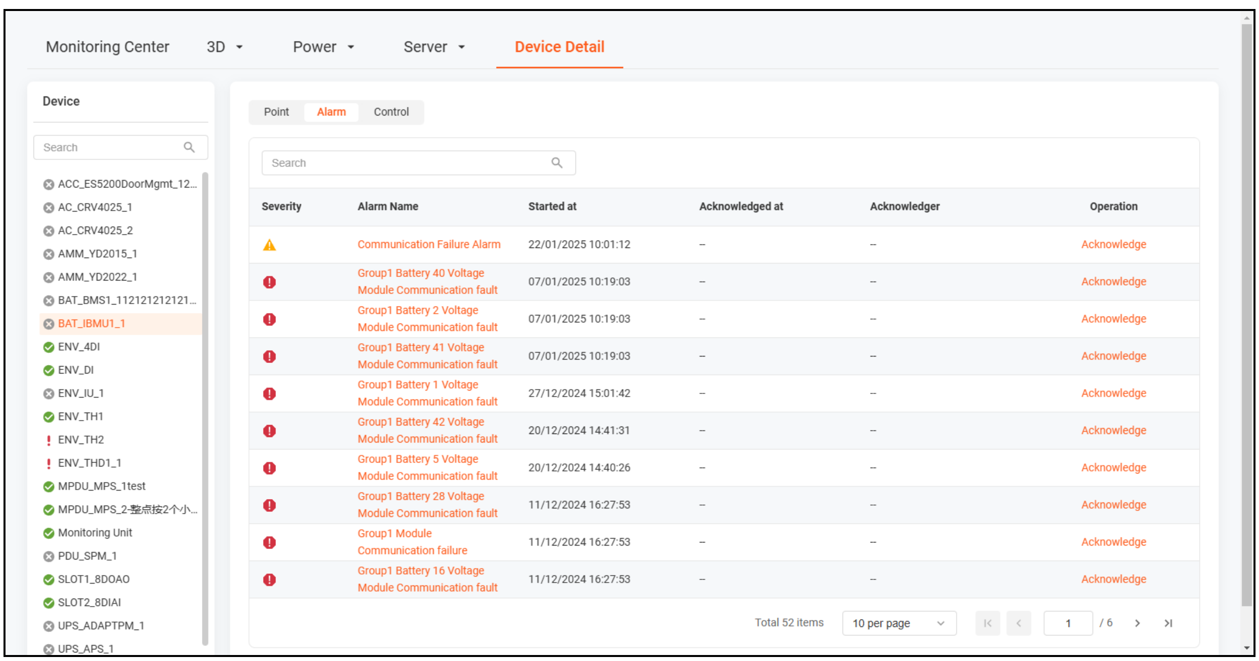
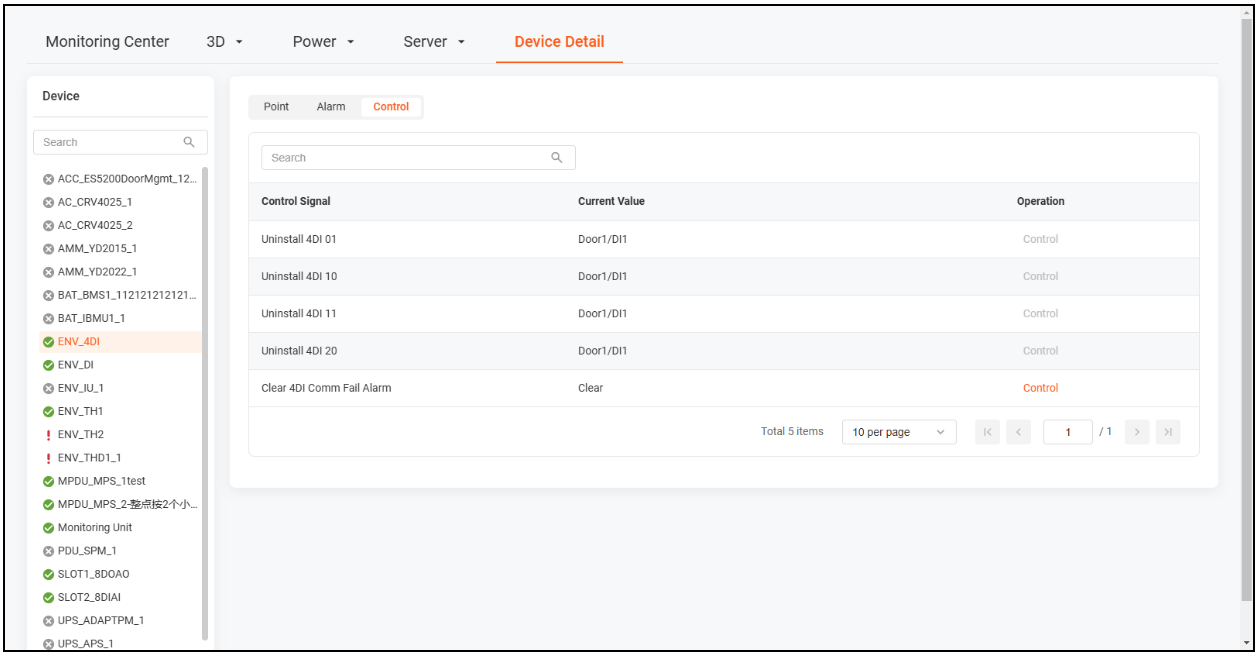
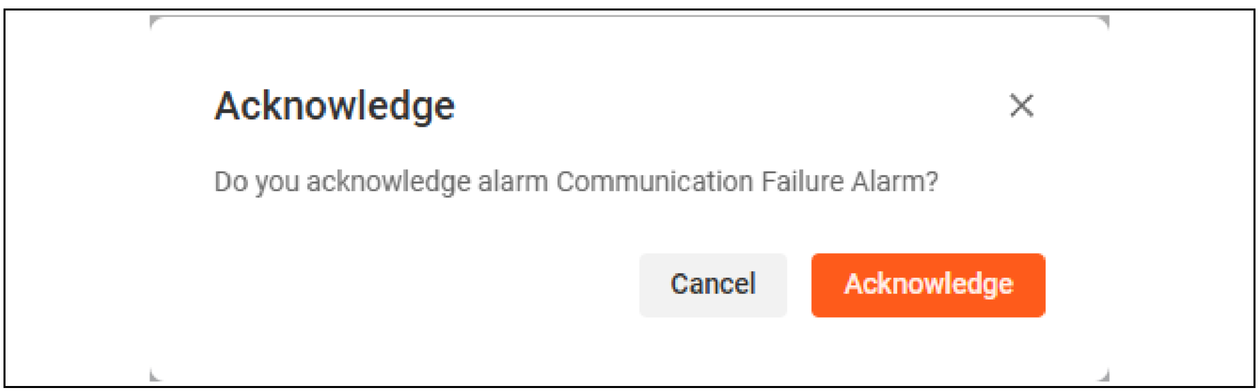


Figure 3.41 Device Control Details



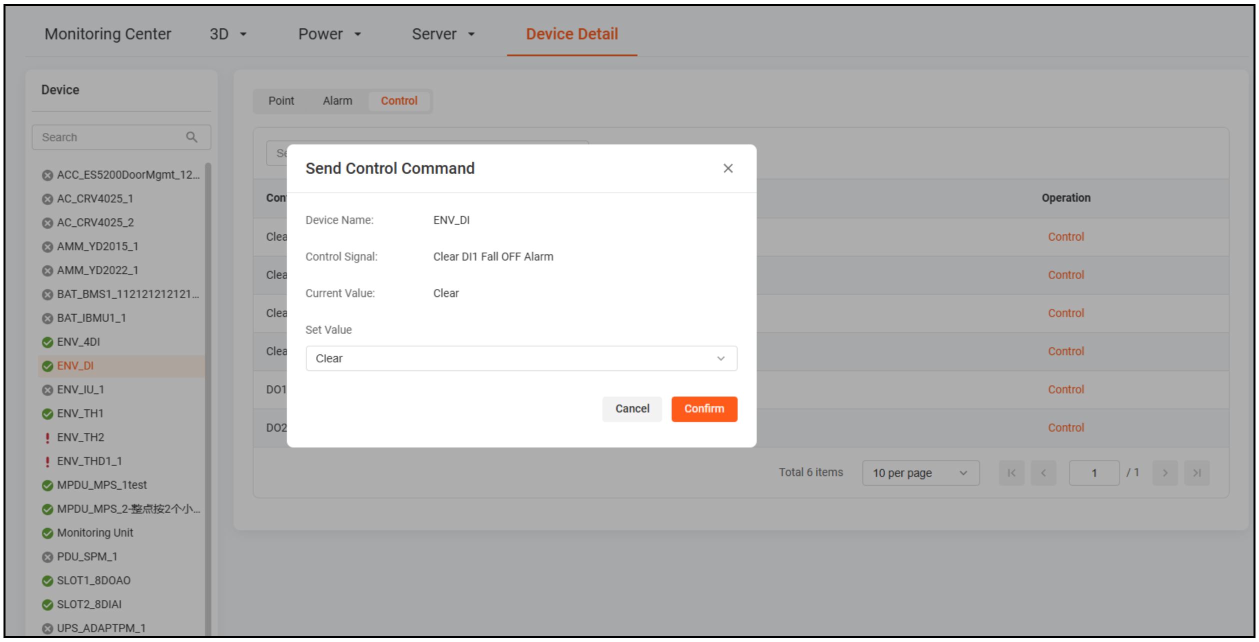
Click the Alarm tab to view all the alarms of the current device. You can acknowledge any active alarms on this page. As shown in Figure 3.42 below .

Figure 3.42 Alarm Acknowledging



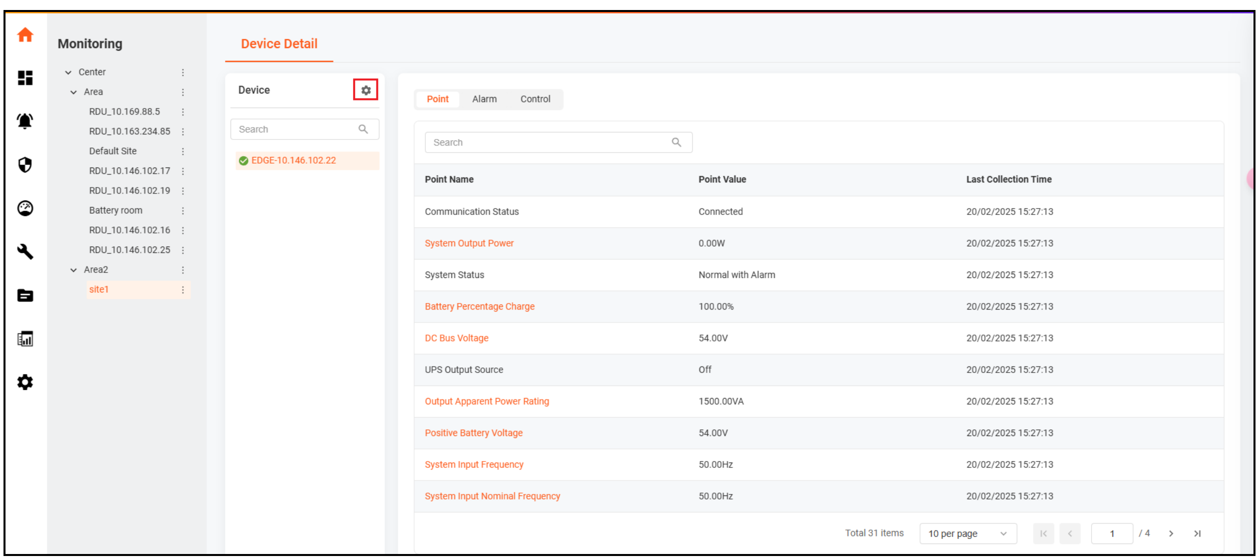
Click the *Control* button to send control command to the device. As shown in Figure 3.43 on the next page .

Figure 3.43 Device Control sends Control Commands



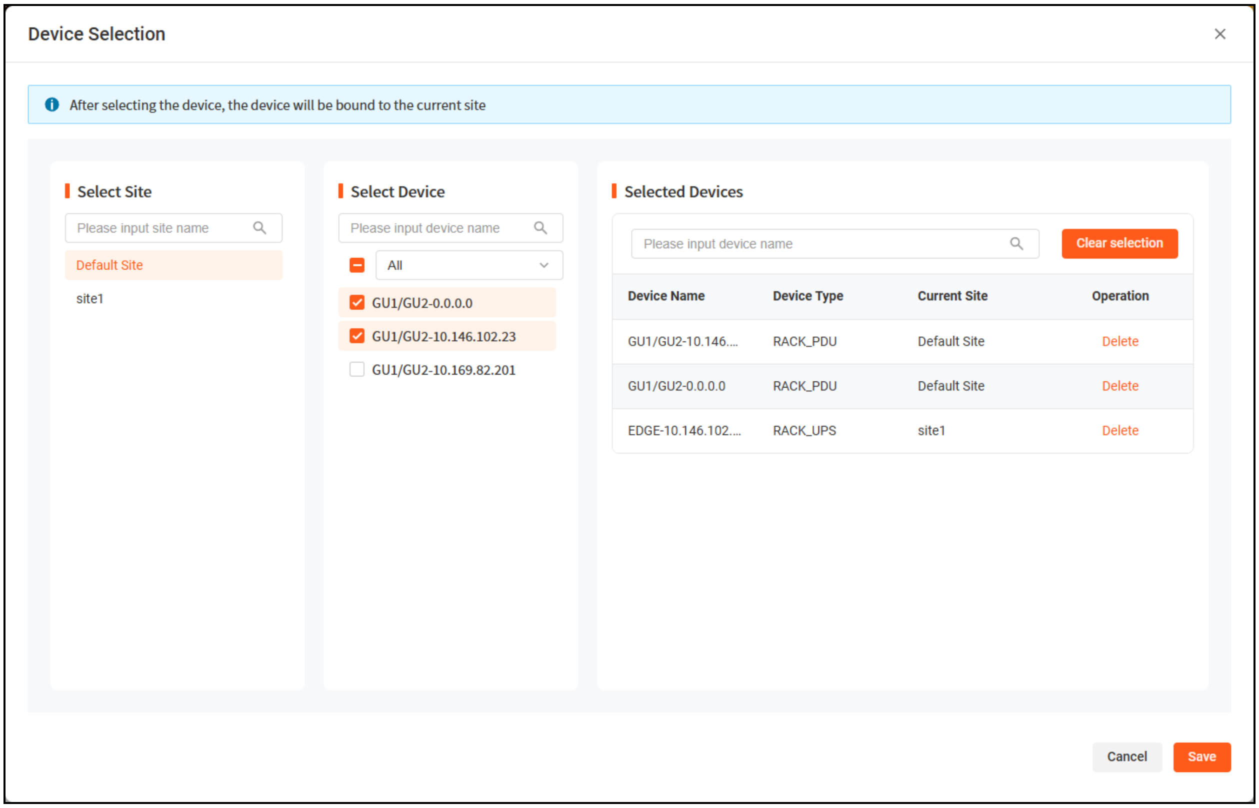
For General Site or Default Site that managing SNMP devices, you can manage SNMP devices under the current site by clicking the configuration button on the right-upper of the device list, as shown in **Figure 3.44** below .

Figure 3.44 Managing Devices Button



After clicking the button, you can add or remove SNMP devices from the current site. Removed devices will automatically be reassigned to the Default Site, as shown in **Figure 3.45** on the facing page .

Figure 3.45 Site Selection Device Popup Window

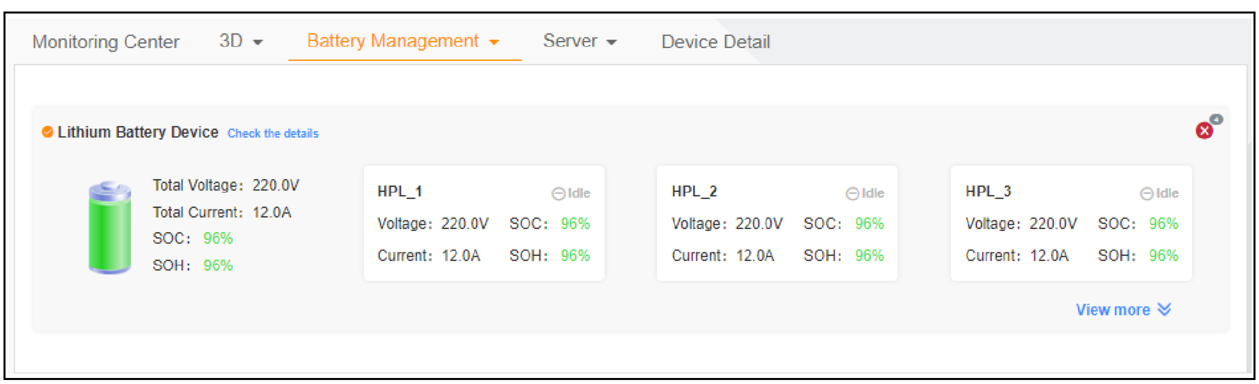


3.3.7 Site: Monitoring Battery Devices

In RDU site, if there are lithium batteries or lead-acid batteries being monitored, the third tab in monitoring home page will display the Battery Management entrance.

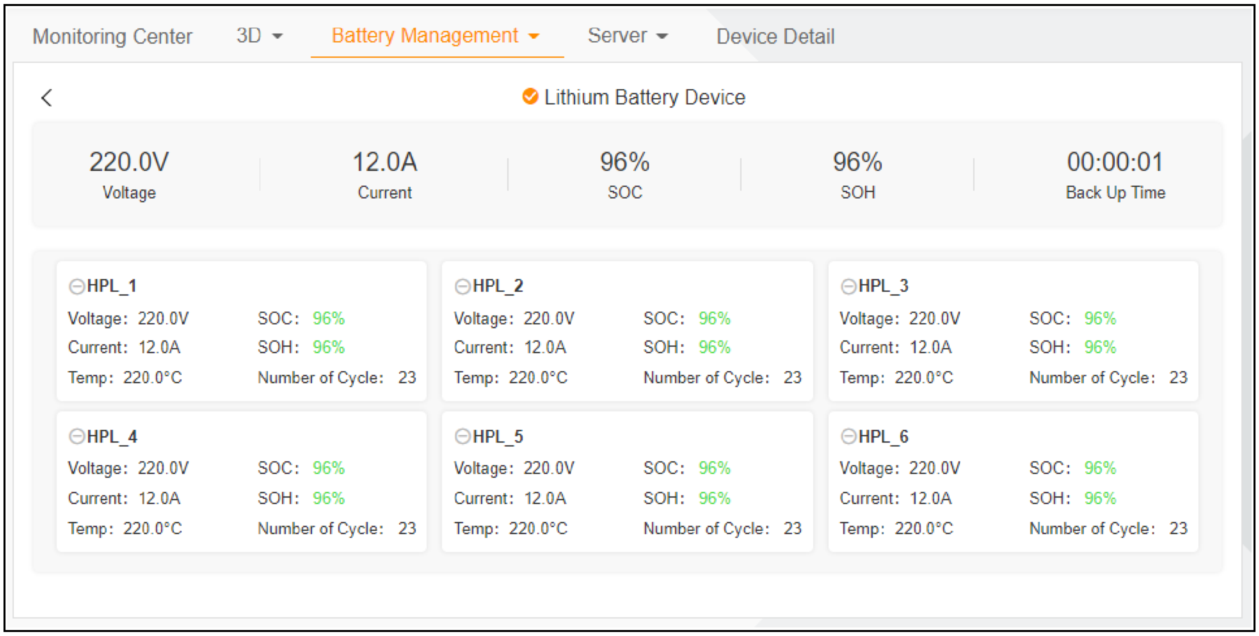
NOTE: Supported lithium battery device model: Vertiv™ HPL.

Figure 3.46 Battery Device Overview



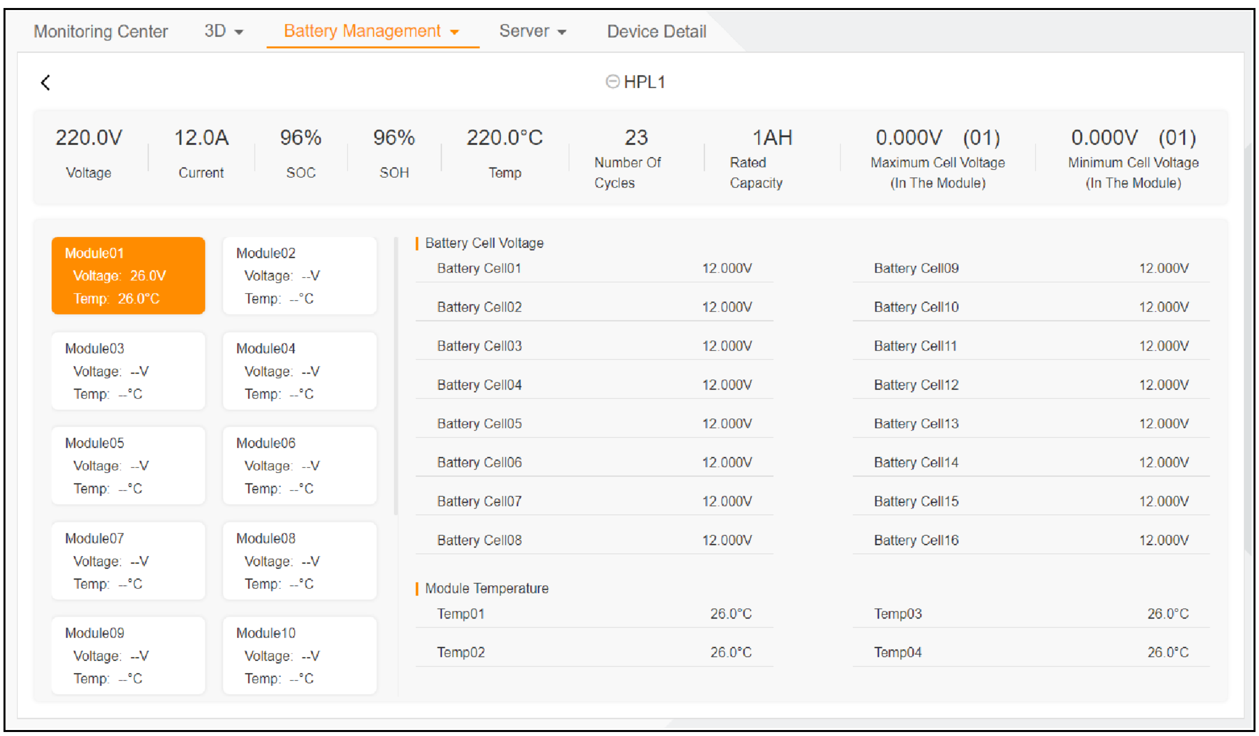
The overview page displays information about the lithium battery systems connected to the current site as shown in **Figure 3.47** on the next page , This includes total voltage, current, state of charge (SOC), state of health (SOH), and alarm counts for each severity level. The page also provides a summary of each battery cabinet's status. For more detailed information, click **check the details** to access the lithium battery device details page.

Figure 3.47 Lithium Battery Device Details



Click on of the lithium battery cabinets to view lithium battery cabinet details page, as shown in **Figure 3.48** below .

Figure 3.48 Lithium Battery Cabinets Details



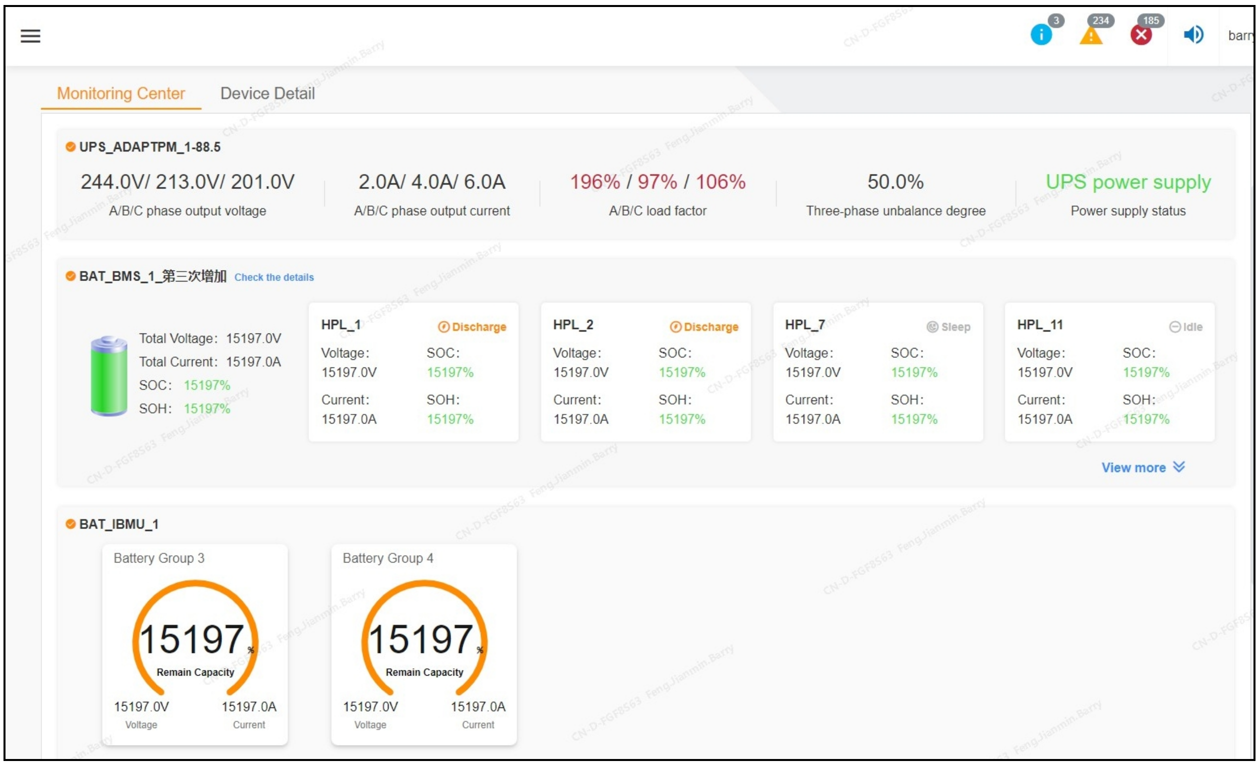
On the details page of the lithium battery cabinet, the summary information of the current lithium battery cabinet is displayed at the top, and the different battery modules in the battery cabinet are displayed on the left.

Battery Room Site Monitoring Homepage

If a lithium battery device or lead-acid battery device is placed in an independent battery room site, you can add a battery room site to the site tree.

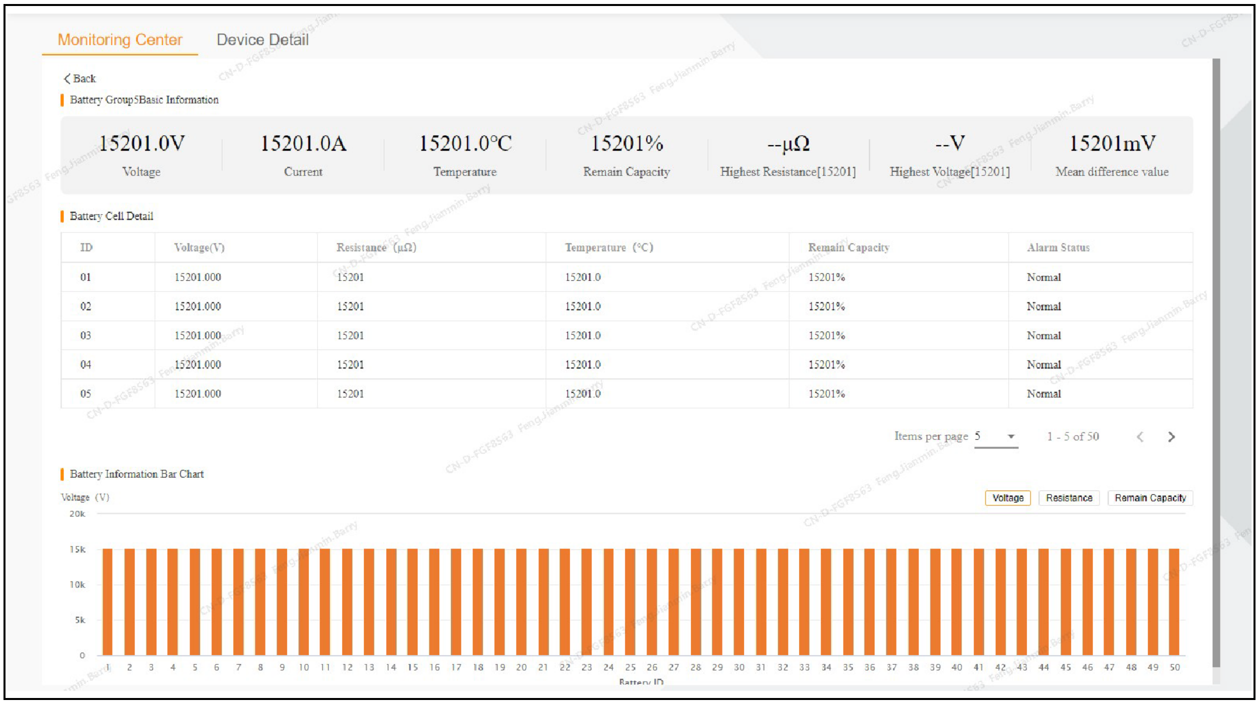
In the site monitoring tree, click the battery room site to open the battery room monitoring page, as shown in **Figure 3.49** below .

Figure 3.49 Battery Room Monitoring Home Page



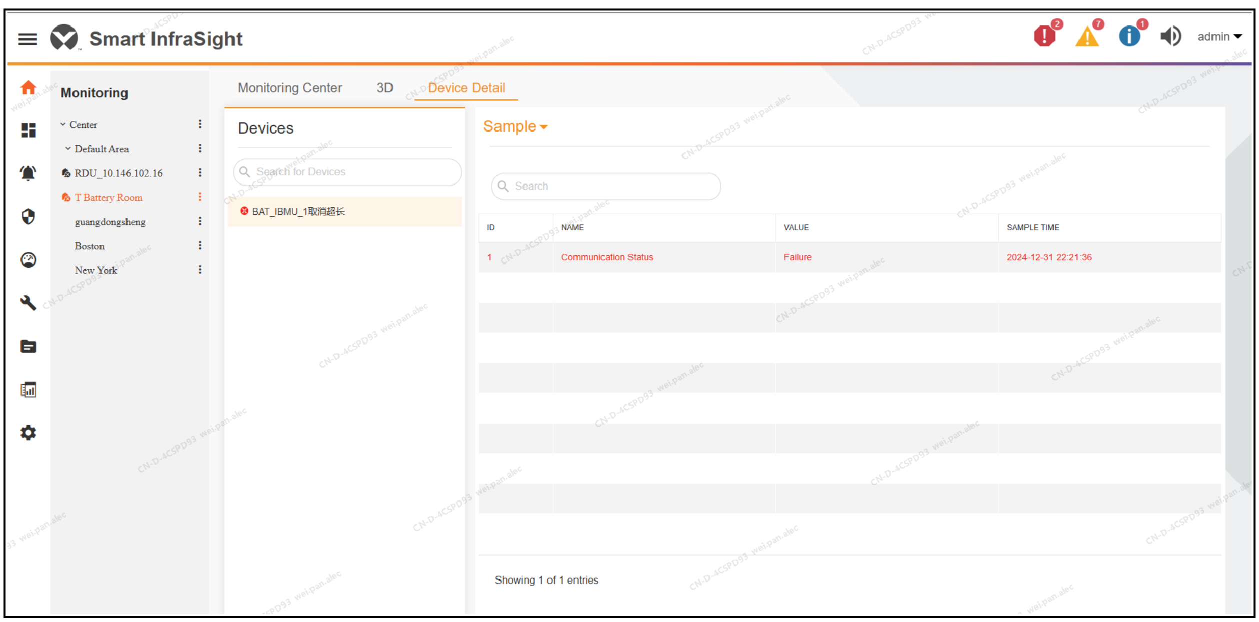
In the **Monitoring Homepage** of the battery room, you can view the operation status information of the added UPS equipment, lithium battery equipment, and lead-acid battery equipment (IBMU), The detail page of lithium battery equipment is the same as previous, but we can click on the IBMU card to view the IBMU details, as shown in **Figure 3.50** on the next page .

Figure 3.50 IBMU Device Details



In the **Device Details**, you can query the detailed signal values of the devices under the battery room site, as shown in **Figure 3.51** below .

Figure 3.51 Battery Room Device Details



4 3D Configuration

4.1 Overview

This chapter describes how to configure the 3D module for a site or location, such as adding devices, modifying, deleting, previewing, saving, and other functions.

4.2 Quick Start

4.2.1 Rapid Deployment Steps

To quickly configure a 3D SmartAisle 3.0 site:

1. Go to Monitoring. In the monitoring tree, click the ellipses next to the site and select User Authentication. Refer to the User Authentication Configuration on page 165.
2. Click on the *ellipses* next to the site again and select 3D Configuration. 3D modeling will be completed automatically.
3. Go to 3D Configuration of the site, double-click one of the cabinets to enter the Cabinet Configuration page, and bind the required devices.
4. Click *Preview* to view the 3D appearance of the SmartAisle 3.0 site.

To quickly configure a 3D SmartAisle 2.0 site:

1. Go to Monitoring. In the monitoring tree, click the ellipses next to the site and select **3D configuration**.
2. On the left side of the page, you'll see a list containing cabinets, UPS, CRAC and other devices.
3. Drag and drop the desired devices from the list into the canvas on the right to add them to the site.
4. In the upper-right corner, adjust the length of the SmartAisle 2.0 station as needed.
5. Click Preview to view the 3D appearance of the SmartAisle 2.0 site.
6. Click *Save* to save the 3D configuration.

To quickly configure a General 3D Site:

1. Go to Monitoring. In the monitoring tree, click the ellipses next to the site and select 3D Configuration.
2. On the left side of the page, a list displays UPS, CRAC, and other devices.
3. Drag and drop the desired devices into the canvas on the right to add them to the site.
4. Adjust the length and width of the general site according to the actual site layout.
5. Click *Preview* to view the 3D appearance of the site.
6. Click *Save* to save the 3D configuration.

To quickly configure a 3D SmartRow2 site:

1. Go to Monitoring. In the monitoring tree, click the ellipses next to the site and select 3D Configuration.
2. On the left side of the page, a list displays UPS, CRAC, and other devices.
3. Drag and drop the desired devices into the canvas on the right to add them to the site.
4. Double click the PMC cabinet and you can configure the devices inside the cabinet.
5. Adjust the length of the Smart Row2 site according to the actual site layout.
6. Click Preview to view the 3D appearance of the site.

7. Click Save to save the 3D configuration.

To quickly configure a location:

1. Go to Monitoring. In the monitoring tree, click the ellipses next to the site and select 3D Configuration.
2. In the left part of the page, you'll find a list containing sites and graphical tools.
3. Drag the site from the list to the canvas on the right and position it as needed.
4. Drag and drop horizontal and vertical walls from the graphical tools into the canvas as required.
5. Left click on the edge of a wall to adjust its length.
6. Adjust the overall length and width of the region based on actual site dimensions.
7. Click Preview to view the 3D appearance of the configured area.
8. Click Save to save the configuration.

To quickly configure a rack:

1. Go to Monitoring. In the monitoring tree, click the *ellipses* next to a site, and select 3D Configuration from the menu.
2. If no racks are listed under the site in the left panel, click the *Add* icon and select a rack to add.
3. Set the rack's parameters, including asset name, asset number, asset template, width, etc., then click *Save* to complete the addition.
4. Drag the rack to the canvas on the right. Double-click the *cabinet* to open the rack configuration page.
5. In the rack configuration page, drag and drop devices such as servers, PDUs, temperature and humidity sensors, and switches from the left list into the appropriate positions in the cabinet.
6. If the required equipment is not in the list, click *Add* to create it. Similar to rack creation, you'll need to set the asset name, asset number, and other parameters. Once added, the device will appear in the list.
7. After completing the configuration, click *Save* to save the rack configuration.

To quickly configure a power distribution cabinet:

1. Go to Monitoring. In the monitoring tree, click the *ellipses* next to the SmartAisle 2.0 room or a general site, and select 3D Configuration from the menu
2. Drag a power distribution cabinet onto the site canvas.
3. If the cabinet is not available in the list, click *Add* to manually create one.
4. For manually added cabinets, configure the required parameters, such as: Asset name, Asset number, Asset template, Associated metering device.
5. For automatically discovered cabinets, double-click the *cabinet* to open the Power Distribution Cabinet Configuration page.

a) To add PDUs, drag and drop them from the list on the left to their corresponding positions in the cabinet.

> a) The user can add PDUs by dragging and dropping the PDU from the graphic list on the left to the corresponding position of the distribution cabinet (if the distribution cabinet is available).
>
> b) If there is no available PDUs on the left, click *Add*, fill in the configuration information and add a new PDU.
>
> C) After the configuration is complete, click on the *Save* button.

To quickly configure a battery room 3D configuration:

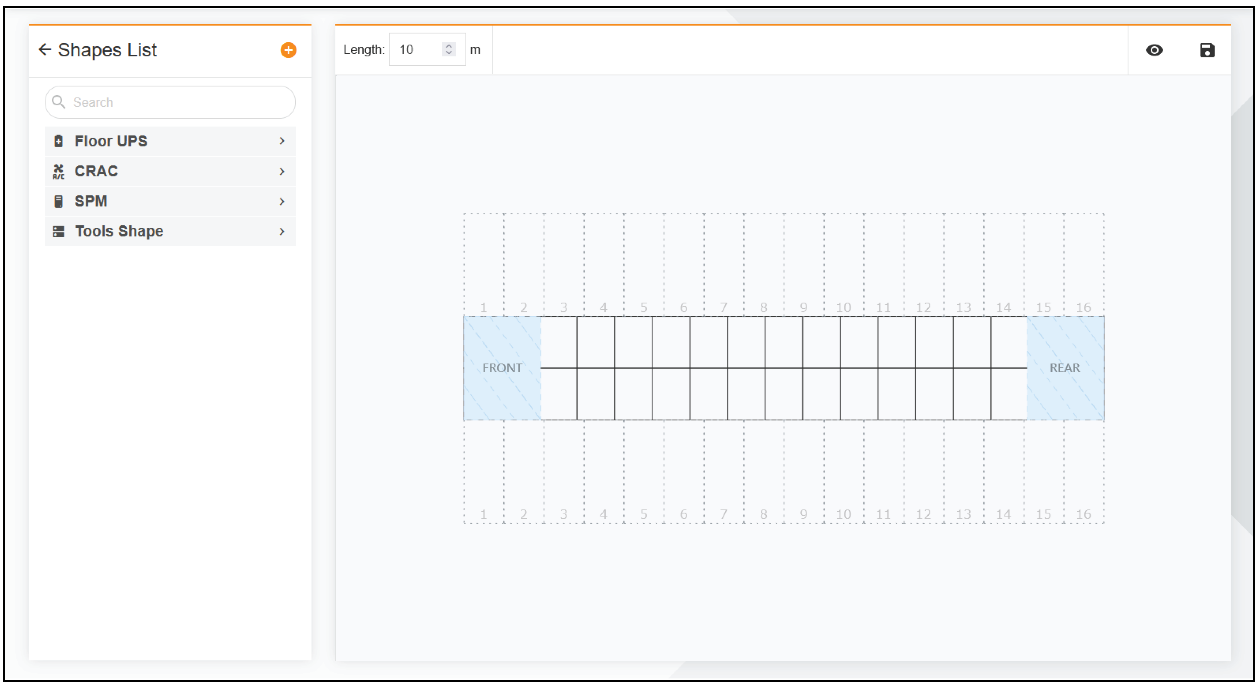
1. Go to Monitoring. In the monitoring tree, click the eclipses next to the battery room site and select 3D Configuration from the menu.
2. Drag the desired devices from the list to the canvas. If the required device is not in the list, click Add to create it. User can add battery devices or power distribution cabinets manually and bind real devices with them.
3. After completing the configuration, click *Save* to save the configuration.

4.2.2 Examples

SmartAisle2 Single-Site 3D Configuration

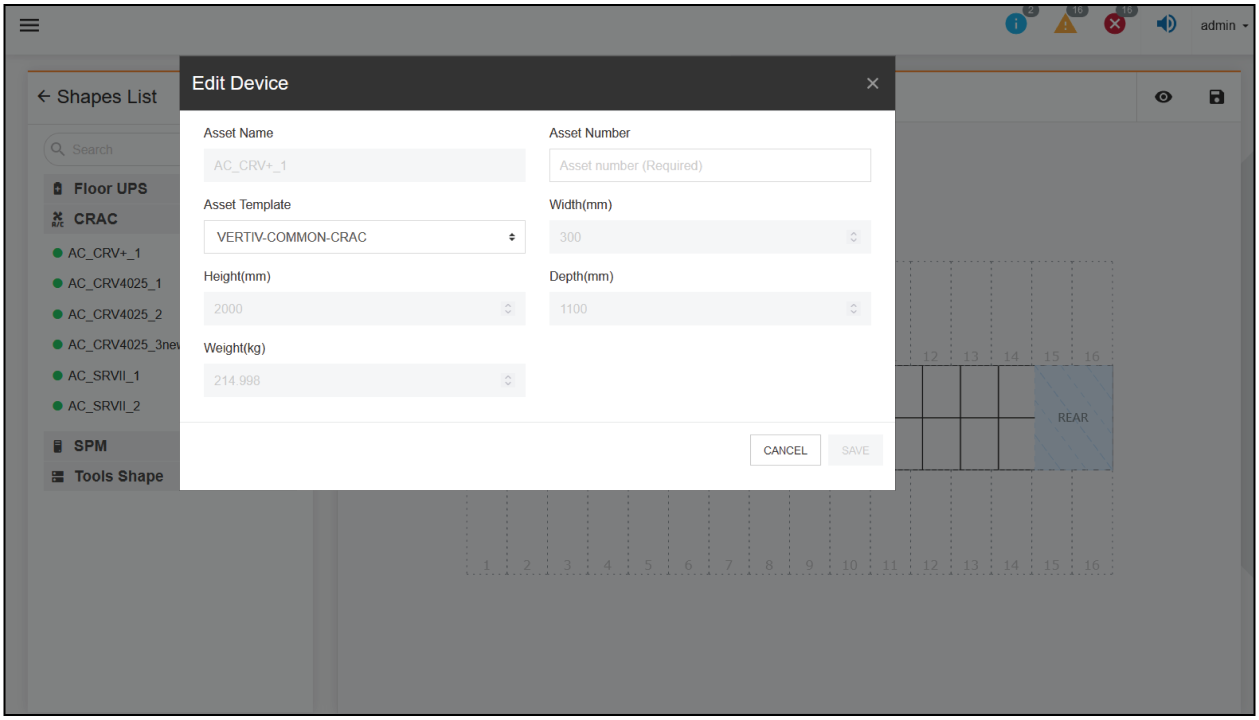
Go to Monitoring. In the monitoring tree, click the *eclipses* next to the Smart Aisle2 site and select 3D Configuration from the menu to enter the 3D room configuration page, as shown in Figure 4.1 below .

Figure 4.1 SmartAisle2 3D Configuration Page



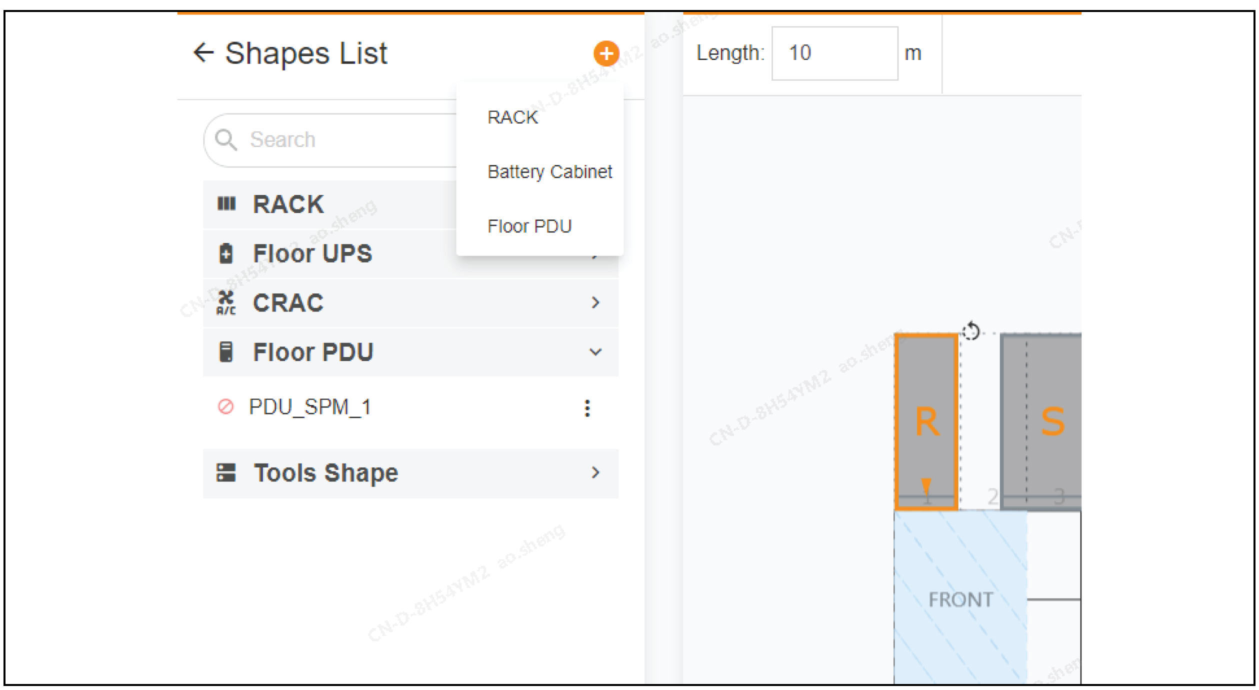
If you need to modify the size of the 3D model of the device, find the device in the list of devices on the left, click on eclipses to open the menu, click *Edit*, modify the relevant information of the device in the pop-up window, and click *save*. As shown in Figure 4.2 on the next page .

Figure 4.2 Editing the Device Information



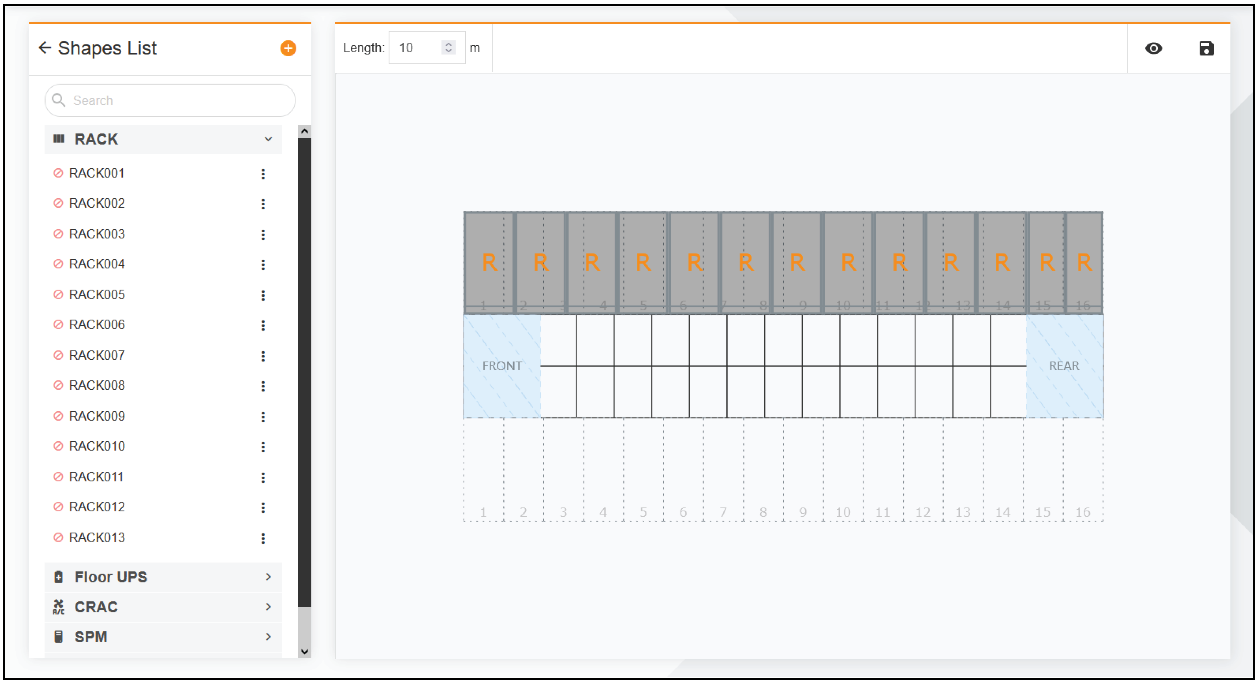
If the necessary device is missing, click the *Add* at the top of the shapes list to add it. As shown in **Figure 4.3** below .

Figure 4.3 Adding the Device



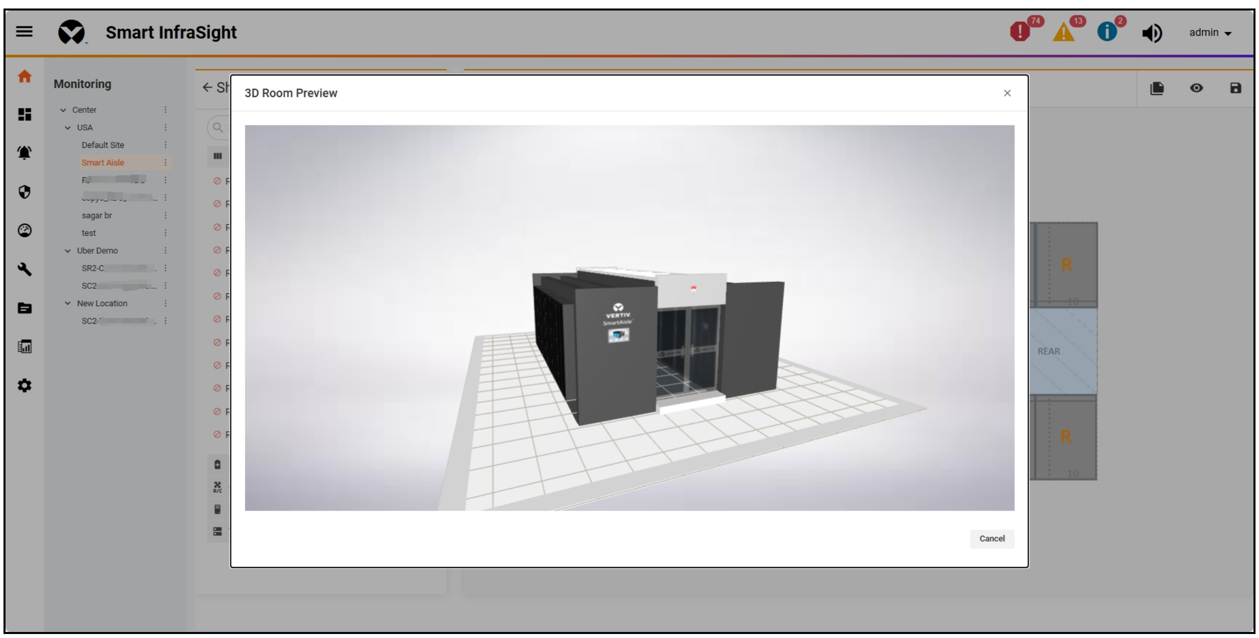
Drag the device on the left to the canvas on the right, and adjust the length of the SmartAisle2 site according to the actual situation as shown in **Figure 4.4** on the facing page .

Figure 4.4 Dragging and Dropping the Device to the Canvas



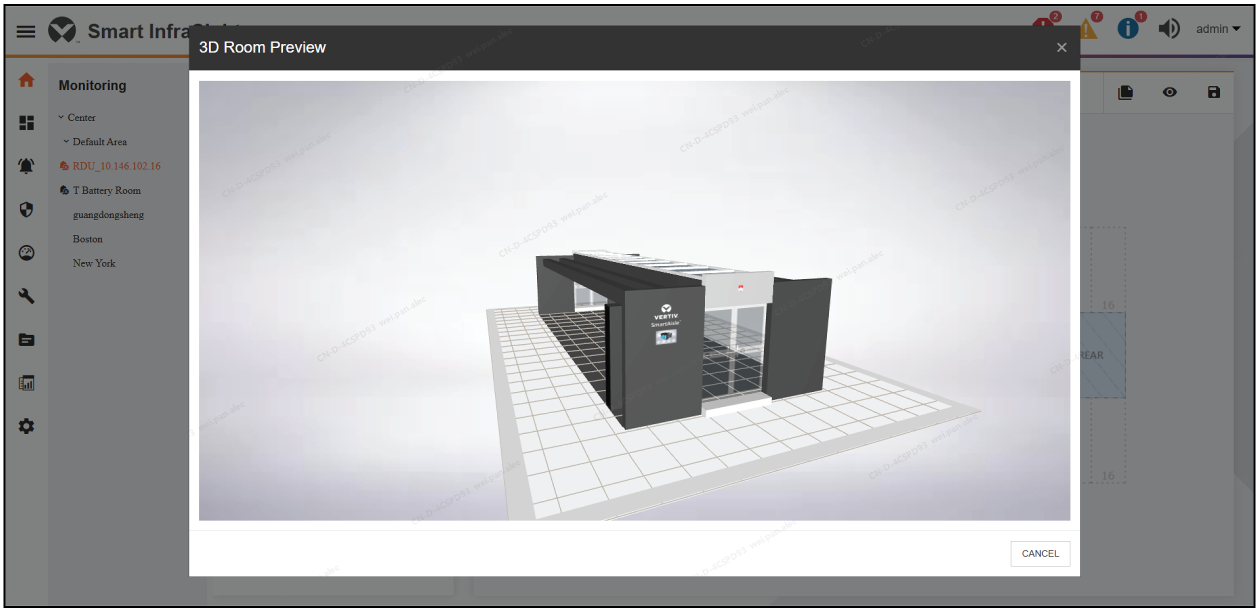
Click the *preview* to make a 3D preview as shown in **Figure 4.5** below . Drag the left mouse button to rotate the viewpoint and scroll the wheel to zoom in and out.

Figure 4.5 Previewing the 3D SmartAisle2 site



You can zoom in and zoom out on the 3D preview of the site. As shown in **Figure 4.6** on the next page .

Figure 4.6 Scrolling the Wheel to Zoom in the Preview of 3D SmartAisle2 Site

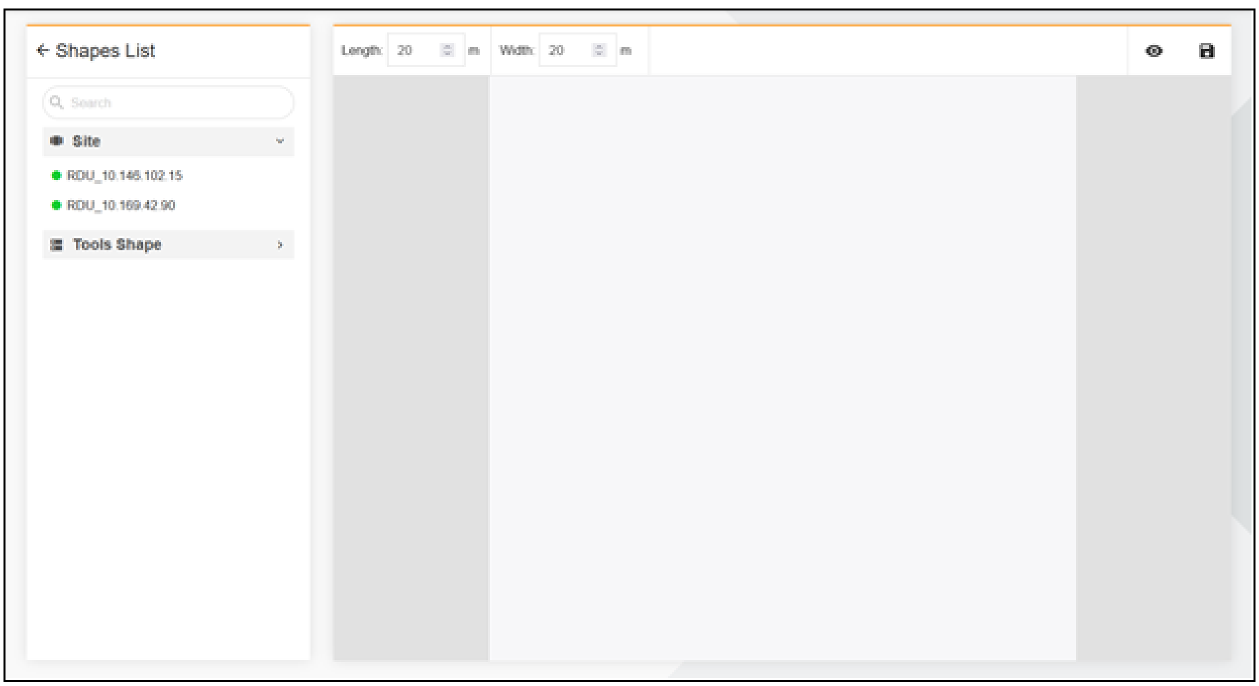


At this point, the 3D configuration of the SmartAisle2 site has been completed.

Location 3D Configuration

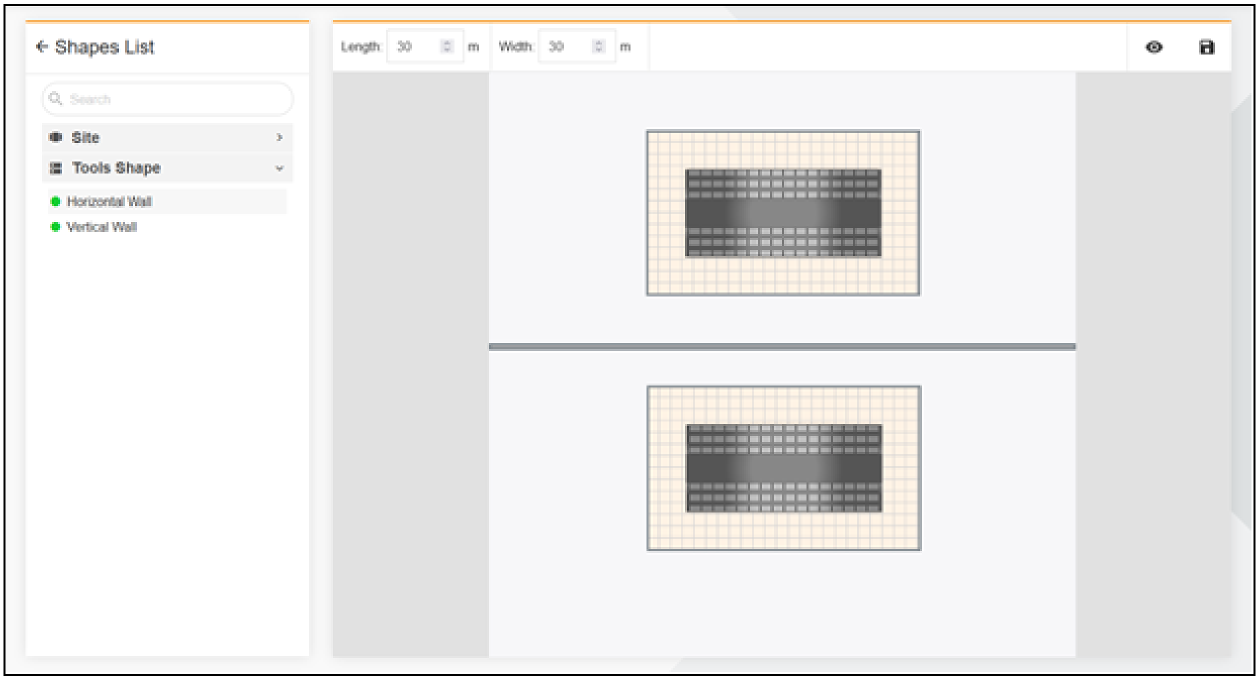
Go to Monitoring. In the monitoring tree, click the eclipses next to the location, select **3D Configuration** from the menu and enter the location 3D configuration page, as shown in **Figure 4.7** below .

Figure 4.7 Location 3D Configuration Page



Begin by dragging the site onto the canvas. Next, add the wall by dragging it onto the canvas as well. Adjust the wall length to fit your needs, and then modify the length and width of the area to match your desired specifications, as shown in **Figure 4.8** below .

Figure 4.8 Dragging the Site and Wall into the Canvas



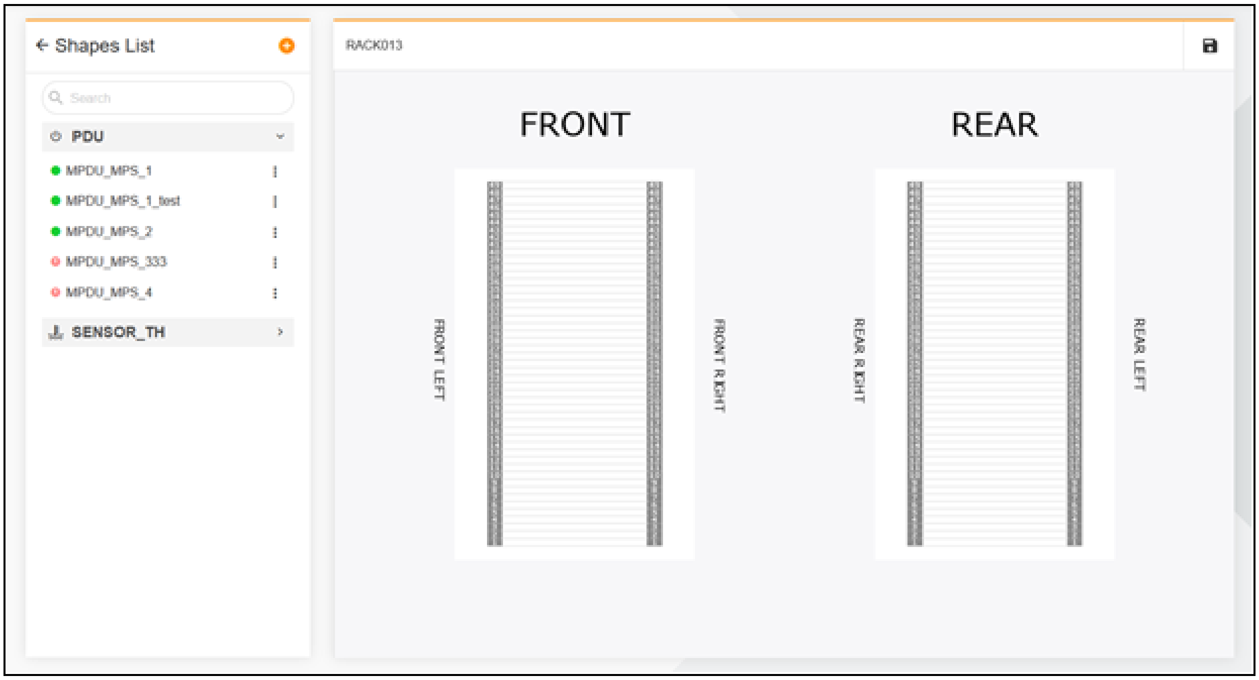
This completes the 3D configuration of the area.

Figure 4.9 Preview the 3D of the Location

Rack Configuration

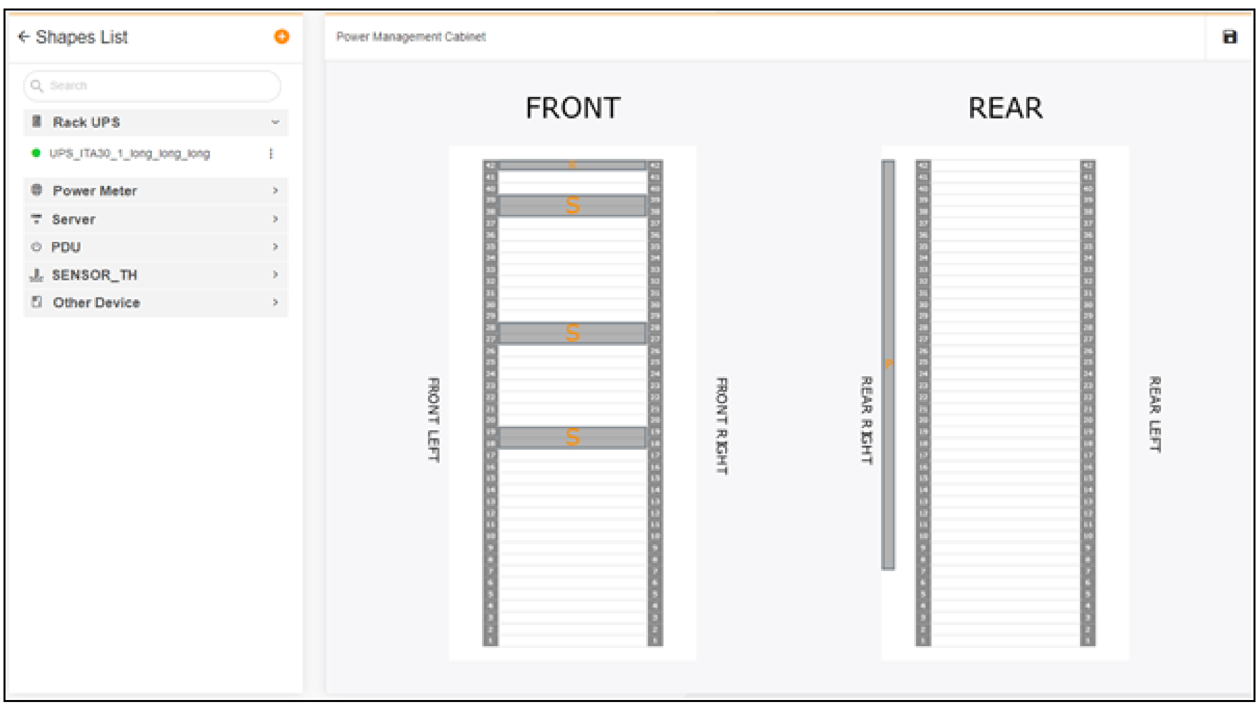
In the 3D configuration of site, you can double-click the rack to dive into the 3D configuration of the rack

Figure 4.10 Rack Configuration Page



Drag the server, switch, PDU, and temperature sensor to the corresponding location. As shown in **Figure 4.11** below .

Figure 4.11 Dragging the Device into the Rack

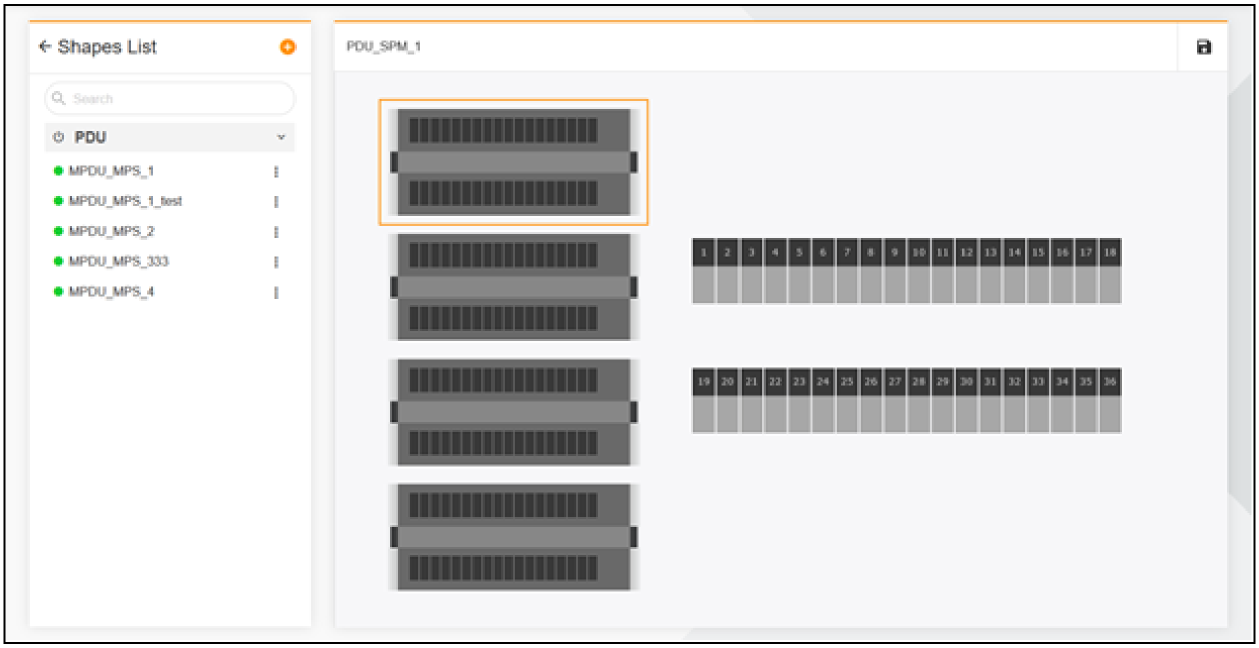


Click *Save* and finish editing.

SPM Power Distribution Cabinet Configuration

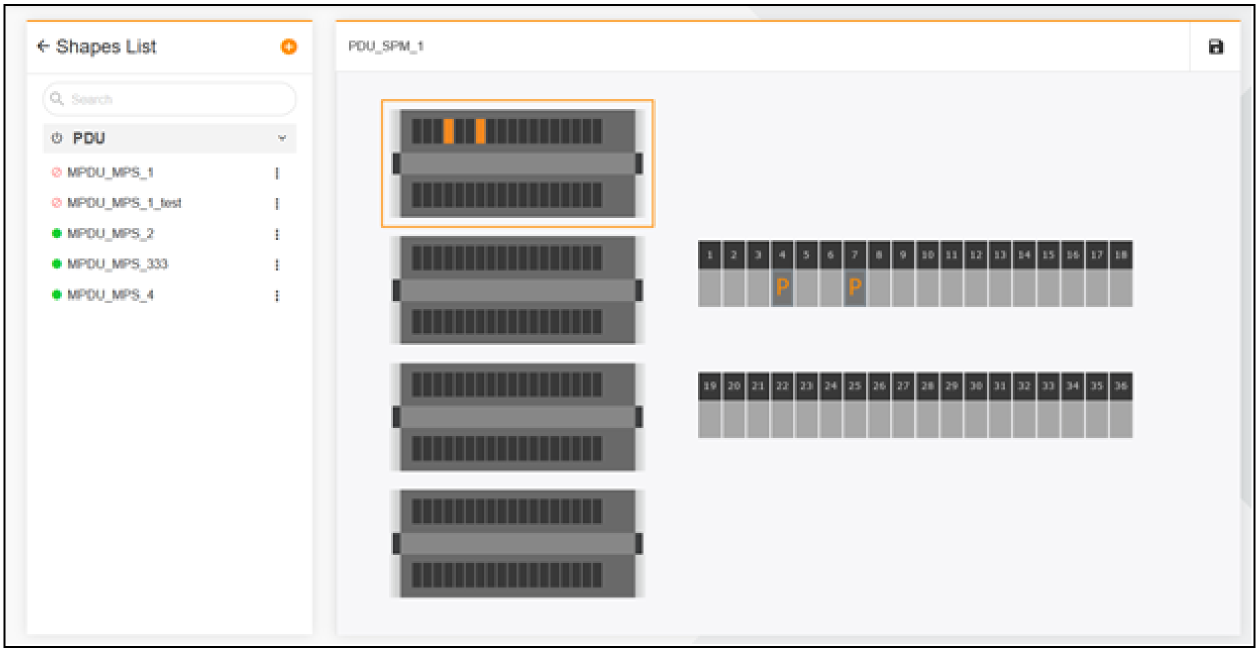
In the 3D configuration of site, you can double-click the SPM power distribution cabinet to enter the SPM power distribution cabinet configuration page.

Figure 4.12 SPM Power Distribution Cabinet Configuration Page



You can drag the PDUs (generally non-monitorable PDU devices) from the device list to a specific branch of the SPM distribution cabinet on the right side. Later, in a 3D display of the rack, these non-monitorable PDUs will be able to show the power signals from that particular branch circuit of SPM, as shown in **Figure 4.13** on the facing page .

Figure 4.13 Placing the PDU in the SPM Power Distribution Cabinet

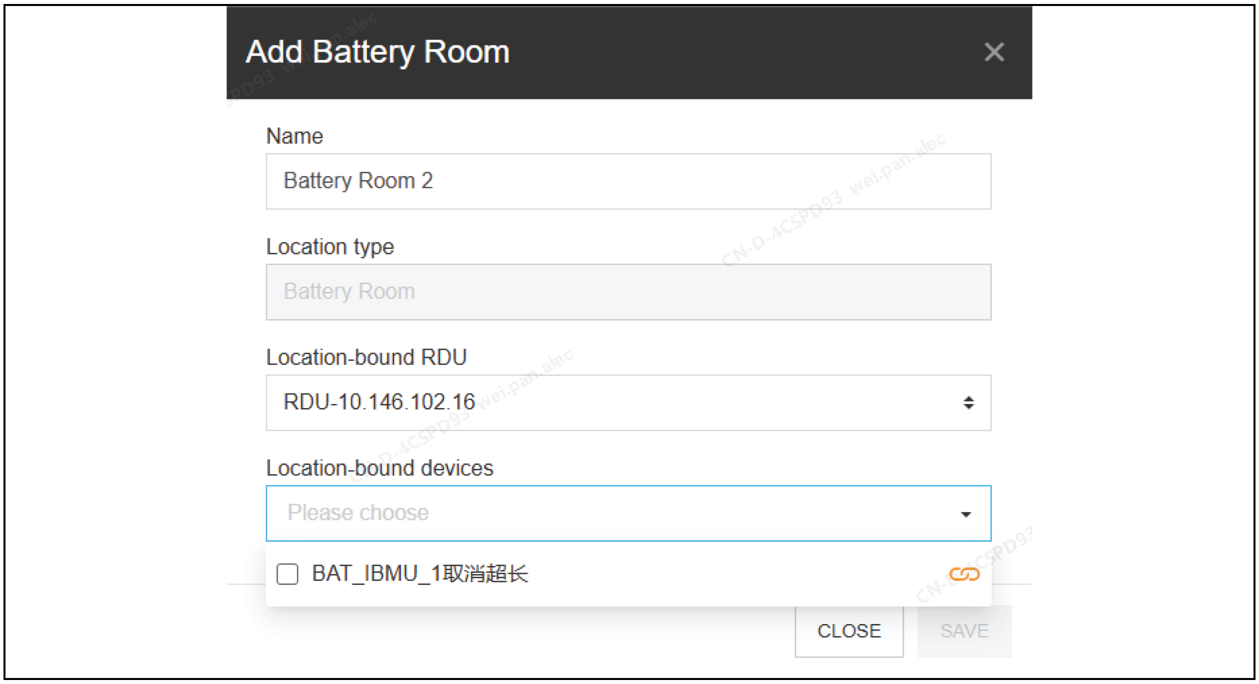


Click *Save* to complete the configuration of the power distribution cabinet.

3D Configuration of the Battery Room

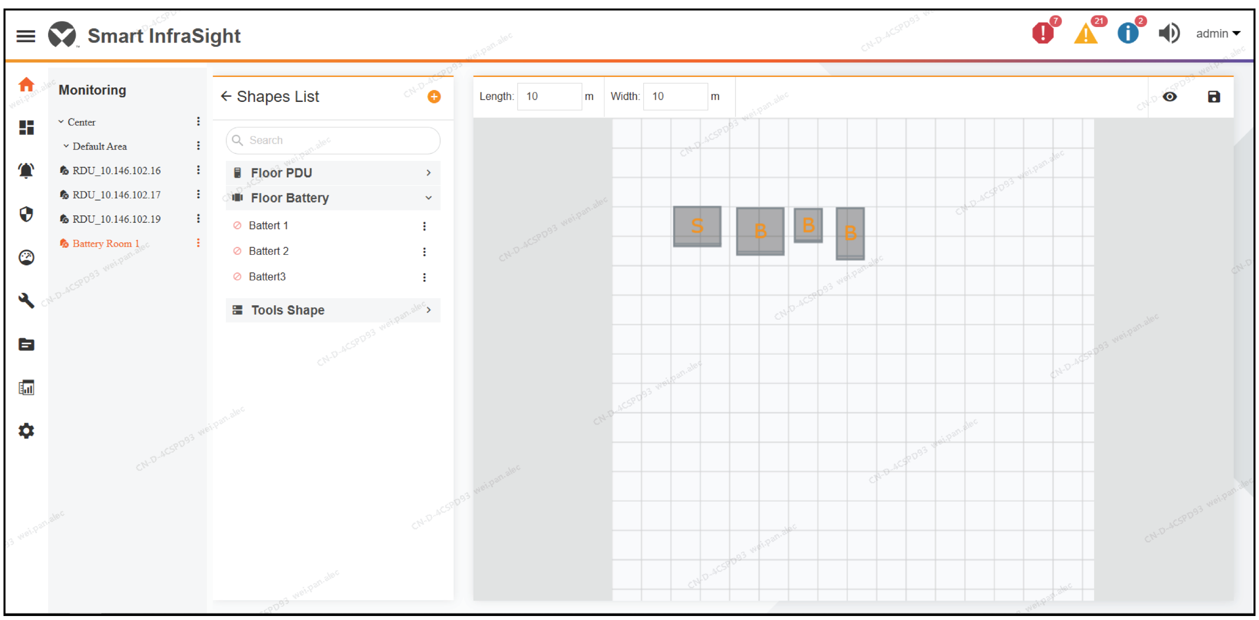
In the monitoring tree, click on the *ellipses* next to the location level and select *Add* Site. In the pop-up window, select Type as Battery Room, select the RDU where the devices come from and select UPS, Lead-acid Battery, Lithium Battery, Power Meter devices that you want to place into the battery room. Click *Save* to create this new battery room site, as shown in **Figure 4.14** on the next page .

Figure 4.14 Adding a 3D Battery Room Site



Click on the *ellipses* on the right side of the added battery room site, select the **3D configuration**, enter the configuration interface, and drag the UPS and battery into the canvas, as shown in **Figure 4.15** below .

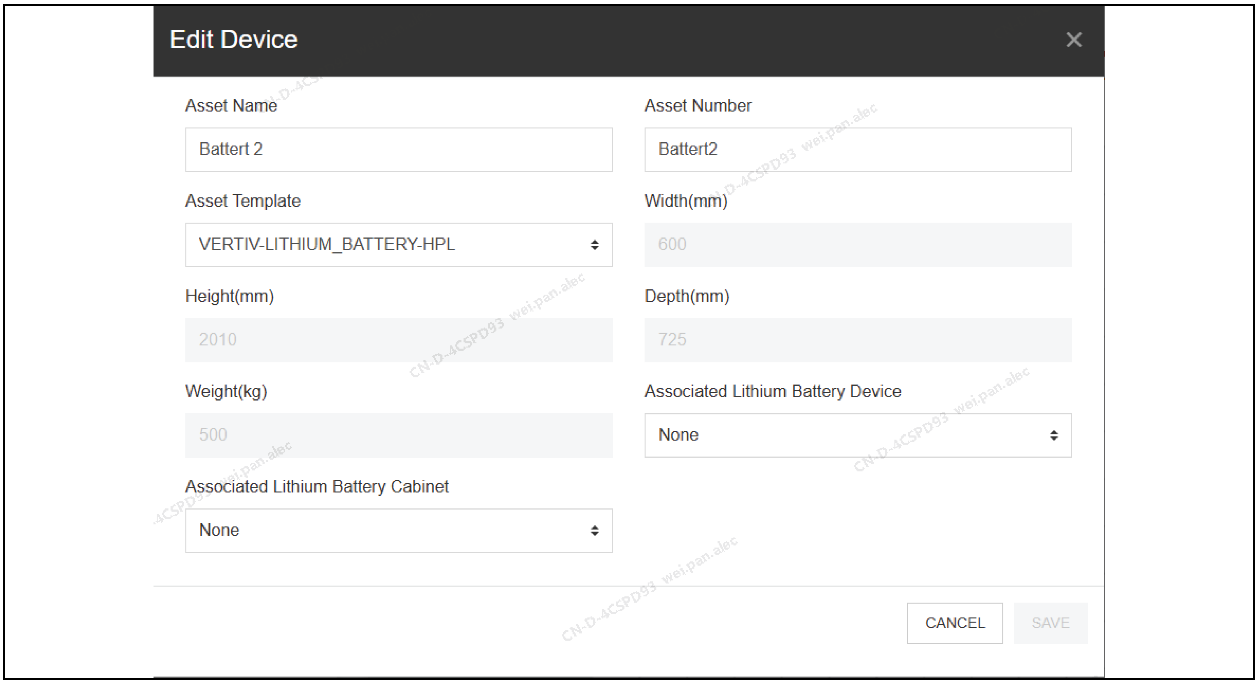
Figure 4.15 Adding a 3D Battery Room Site



Lithium Battery 3D Configuration

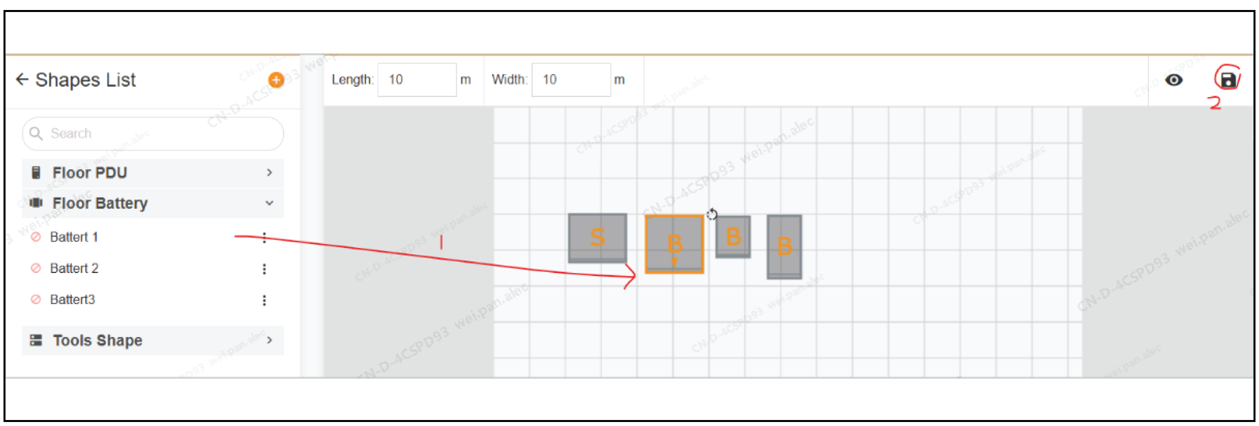
In the 3D configuration page of sites, you can manually add a device of type Floor Battery, and in the Edit pop-up window of the device, the asset template selects VERTIV-LITHIUM_BATTERY-HPL, at this time, you can associate a battery device with a HPL lithium battery cabinet that has monitorable signals (if there are multiple lithium battery cabinets, you need to add multiple Floor Battery devices). After that, you can show the real-time power signal of the lithium battery cabinet in 3D. As shown in **Figure 4.16** below .

Figure 4.16 Editing the Device



After saving, drag the Floor Battery asset you just added from the shapes list to the canvas on the right, and then click *Save*, as shown in **Figure 4.17** below .

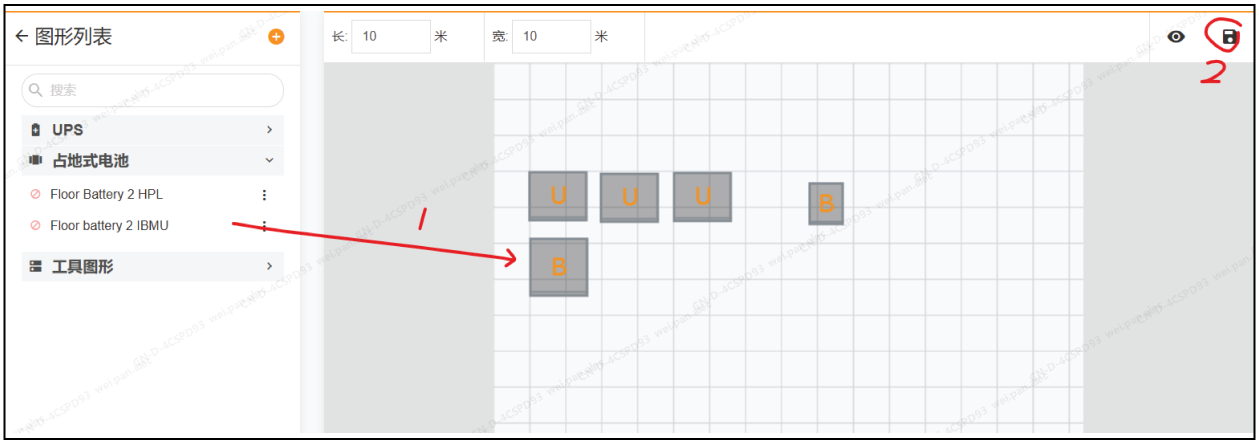
Figure 4.17 Lead-acid Battery 3D Configuration



Lead-acid Battery 3D Configuration

To display lead-acid batteries in 3D, In the 3D configuration page of sites, you can manually add a device of type Floor Battery, and in the Edit pop-up window of the device, the asset template selects LEAD-ACID_BATTERY-RACK, at this time, you can associate a floor battery device with a lead-acid device that has monitorable signals. You can change the size and tiers of the 3D model of the lead-acid device After that, you can show the real-time power signal of the lead-acid battery in 3D , as shown in **Figure 4.18** below .

Figure 4.18 Lead-acid Battery 3D Configuration



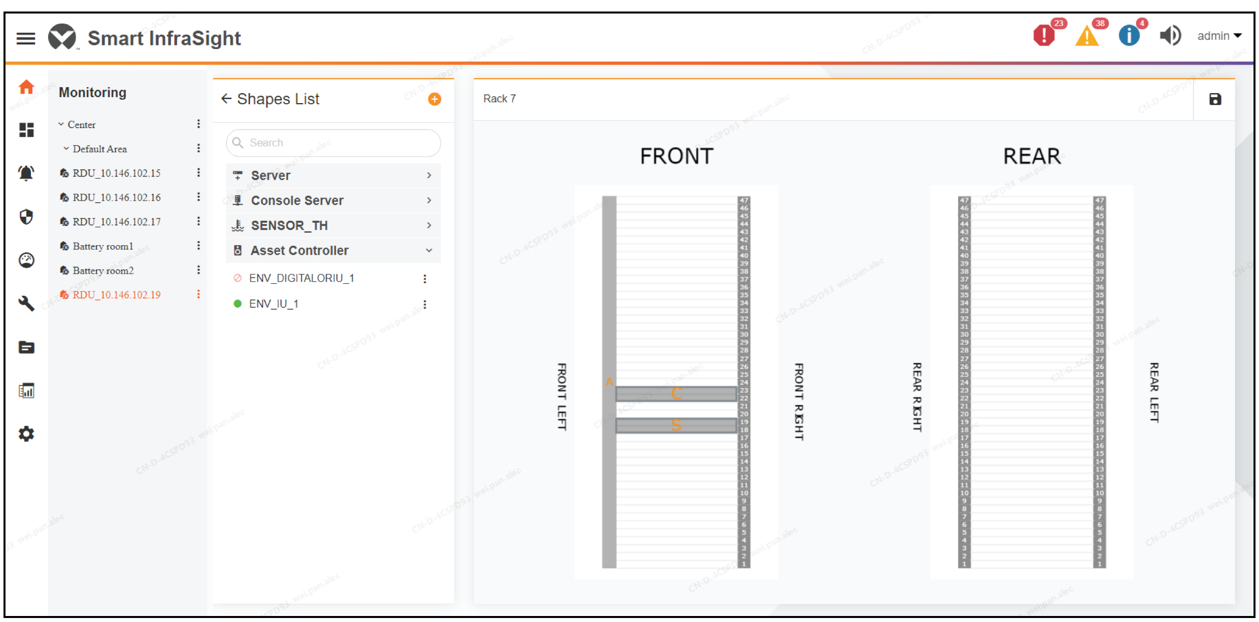
U-position Asset Manager Configuration

The U-position Asset Manager must be associated with the rack. To do this, access the 3D configuration of the site and then the rack 3D configuration. The list of available U-position Asset Managers will then appear in the shapes list on the left.

When you drag the U-position Asset Manager into the rack, any existing devices occupying U positions will be automatically removed. The system will then query the current site for devices corresponding to the U-position Asset tags assigned by the Asset Manager. These devices will be automatically placed in the appropriate U positions within the rack.

Please refer to the U-position Asset Manager Configuration below for visual representation of this process.

Figure 4.19 U-position Asset Manager Configuration



4.3 Detailed Functions

4.3.1 Enter the Site/Location 3D Configuration

In Monitoring, click the *ellipses* on the location/site of the monitoring tree to open the menu, and select **3D configuration** to enter the 3D configuration page as shown in **Figure 4.20** below and **Figure 4.21** below .

Figure 4.20 Site 3D Configuration Entrance

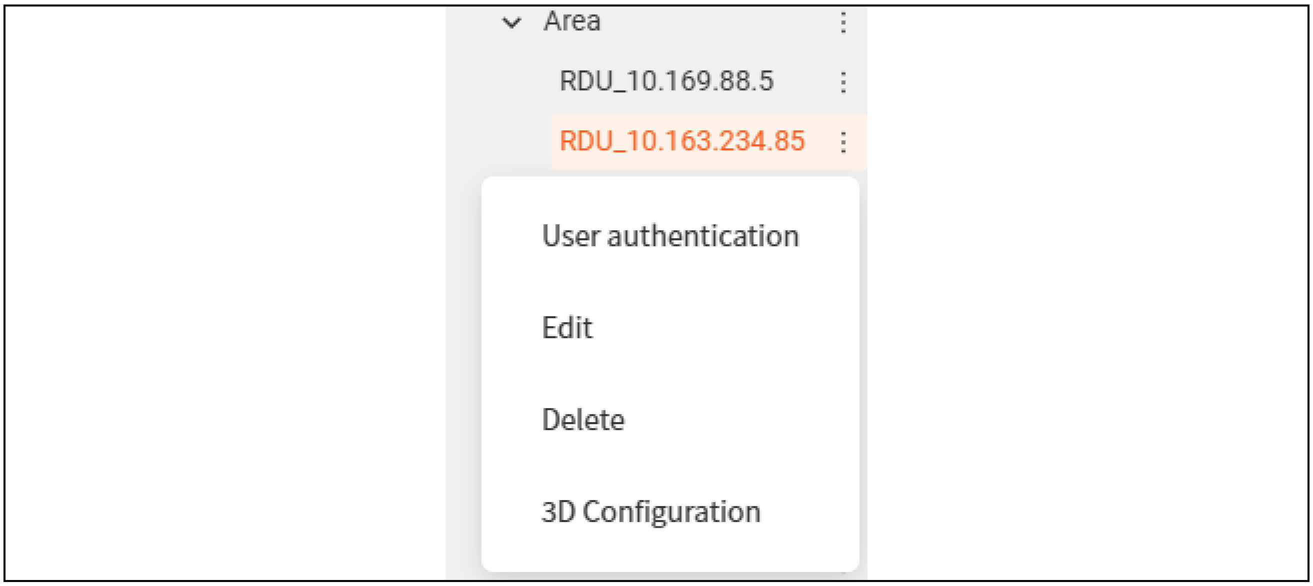
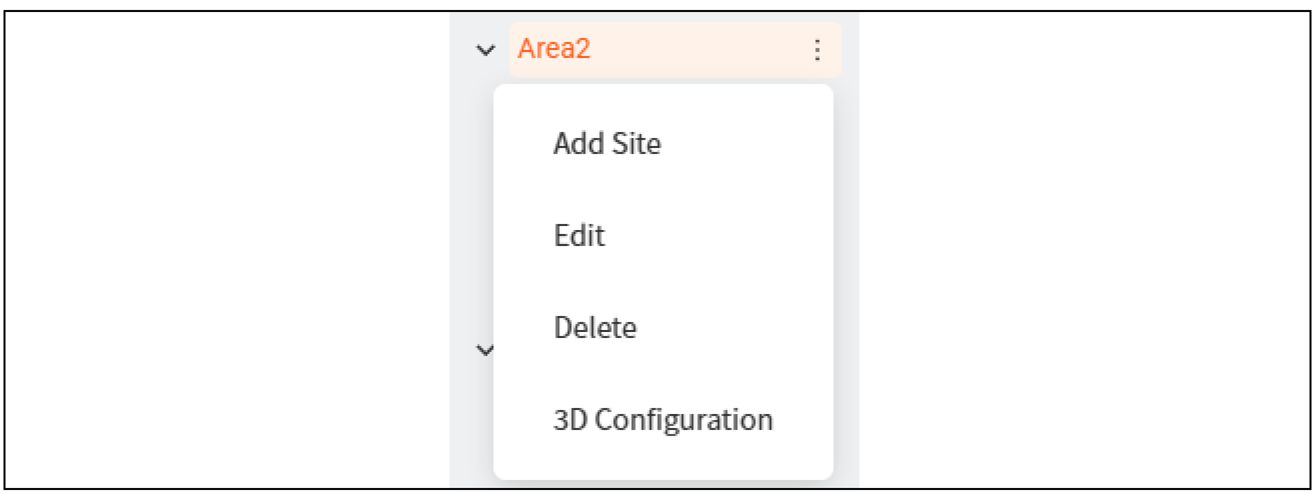


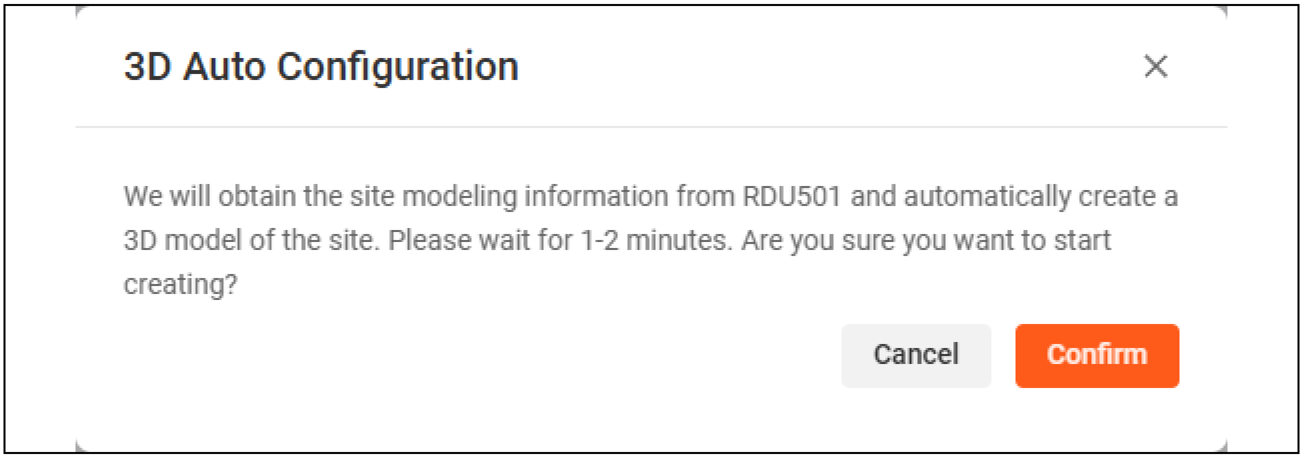
Figure 4.21 Location 3D Configuration Entrance



SmartAisle3 site

For Smart Aisle 3.0 sites, before entering the 3D configuration page, it will check whether the Restful protocol user authentication has been configured, if not, the pop-up window will let the user enter the Username and password of the RDU, and click *Save*, please refer to User Authentication Configuration on page 165. If the RESTful protocol user authentication configuration has been performed, the site will be checked to see if the 3D automatic configuration has been performed. The site will perform the 3D initialization automatically. (Or enters the 3D configuration page once the 3D has been configured).

Figure 4.22 3D Auto-Configuration Popup Window (Smart Aisle 3 Only)



Click *Confirm*, the system will automatically complete the 3D configuration modeling of the Smart Aisle 3.0 site, then enter the 3D configuration page. Generally, you don't need to drag and drop any devices manually anymore. You can directly adjust the rack configuration of your Smart Aisle 3.0 site according to Section Configuring the Rack on page 68.

The 3D automatic configuration feature uses the modeling information from the RDU501 collector for Smart Aisle 3.0 to automatically arrange the spatial relationships between the site and floor equipment (air conditioners, UPS units, and cabinets). Once the automatic configuration is complete:

1. No new cabinets or battery cabinets can be added to the site.
2. Existing cabinet devices cannot have their Width, Height, Depth, Total U-Position, Rated Power, or Asset Template fields modified.
3. The Width, Height, Depth, and Asset Template fields of air conditioners and UPS units cannot be edited.
4. Dragging or rotating any devices (air conditioners, UPS units, and cabinets) within the site is not permitted.
5. The shapes list on the left will only display cabinet, air conditioner, and UPS equipment drop-down menus.
6. By default, only devices that are automatically bound to the cabinet, like air conditioner, and UPS device lists are shown.
7. The site length cannot be modified.

These restrictions ensure the integrity of the automatically configured layout.

NOTE: To perform the 3D automatic configuration, you must first set up user authentication.

The 3D configuration page of the Smart Aisle 3 site is only accessible after completing the 3D automatic configuration process.

In the following situations, you need to manually delete the Smart Aisle 3 site and reconfigure the 3D automatic configuration:

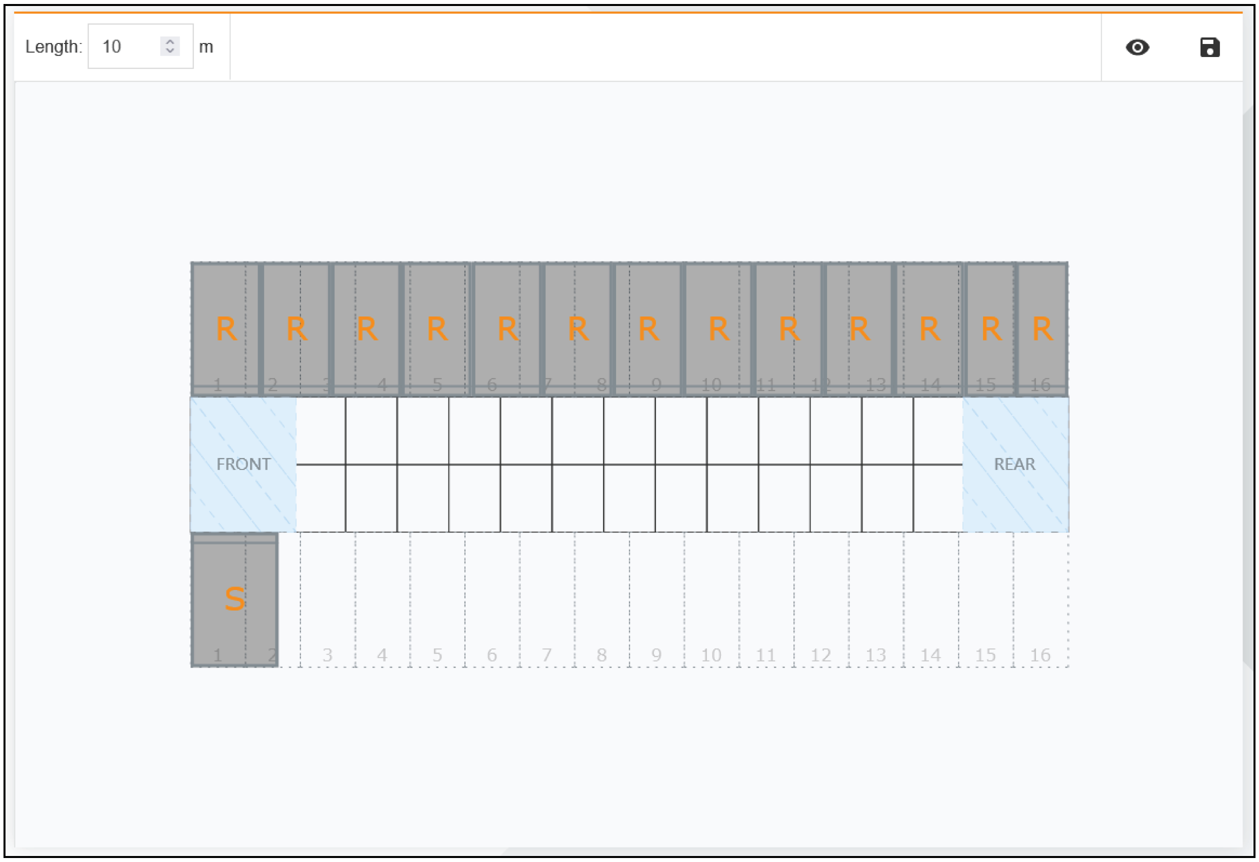
1. After the RDU501 adjusted the Smart Aisle 3 layout

2. After the RDU501 added or modified devices in the Smart Aisle 3.

4.3.2 Dragging and Dropping the Device to Edit the Canvas Size

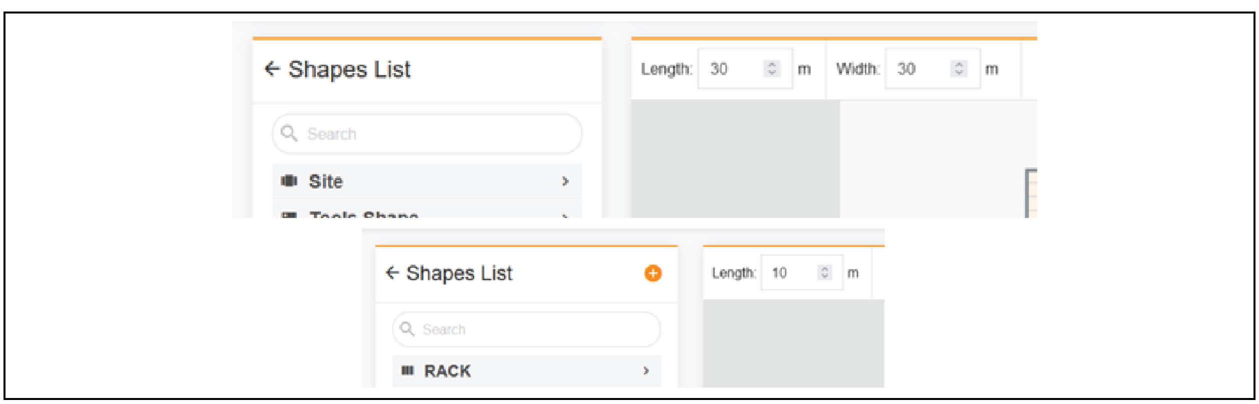
In the 3D configuration page, you can drag and drop devices from the shapes list to the canvas on the right side. You can place the devices in any position you want. As shown in the Figure 4.23 below .

Figure 4.23 Drag and Drop the Device to the Canvas



If you find that the size of the canvas is not suitable, you can modify the size of the canvas through the size input box at the top of the site/location, as shown in Figure 4.23 above .

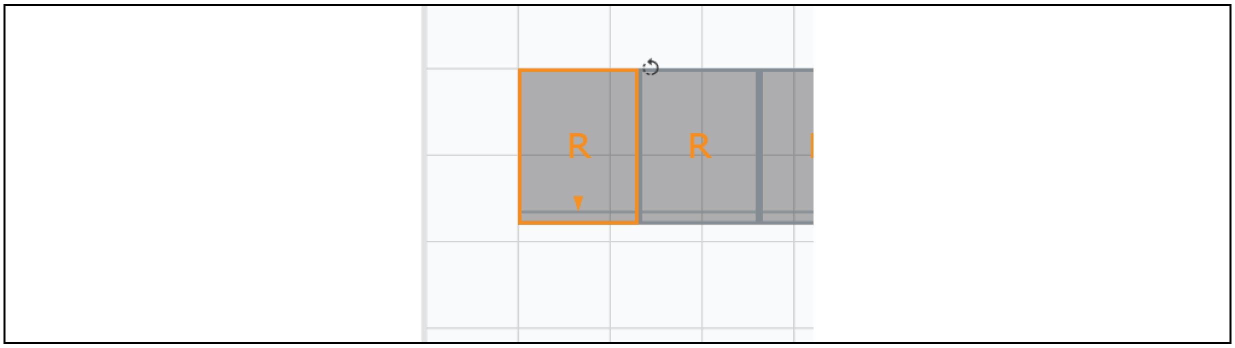
Figure 4.24 Modify the Size of the Canvas for a Location/Site



In the canvas of SmartAisle2/SmartRow2/Battery Room site, you can rotate device. Select a device, click the rotation button to rotate the device by 180 degrees.

The device in the Battery Room site can be rotated between 0 degrees, 180 degrees, 270 degrees. As shown in **Figure 4.25** below .

Figure 4.25 Rotating the Device on the Canvas



In the SmartAisle2 or SmartRow2 site, the device can be rotated between 0 degrees and 180 degrees. As shown in **Figure 4.26** below .

Figure 4.26 Rotation Device in SmartAisle2

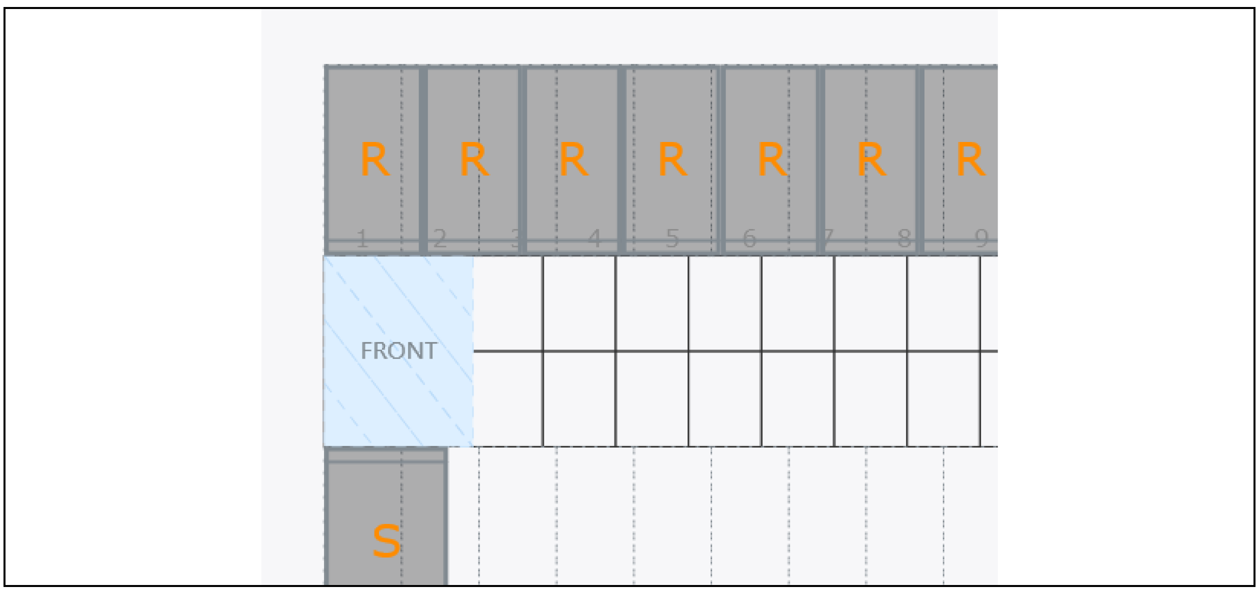
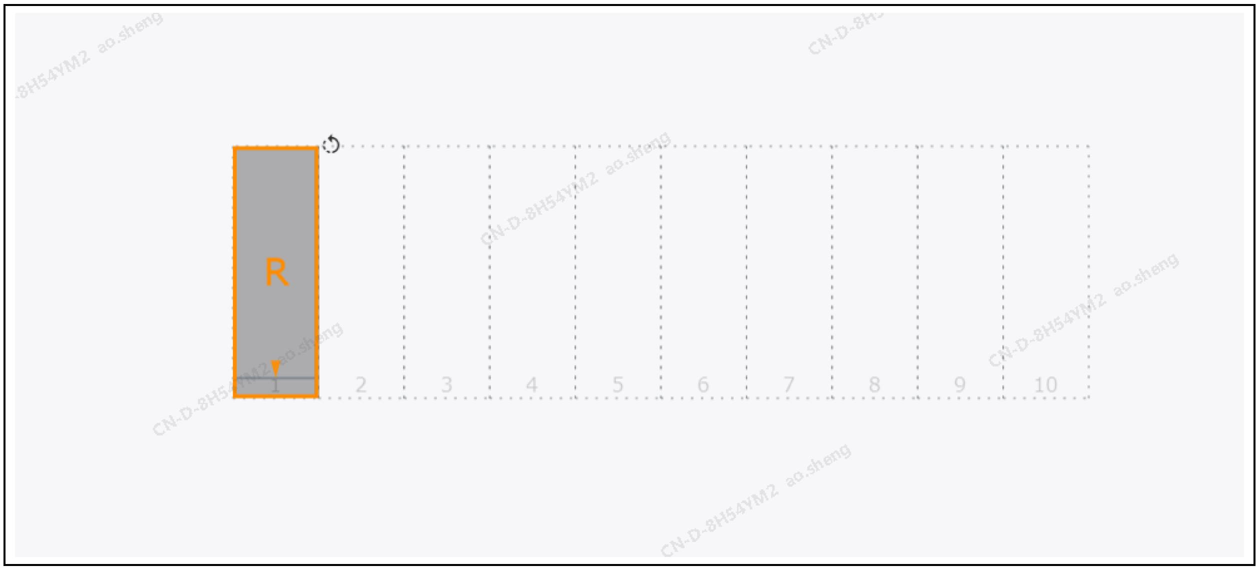


Figure 4.27 Rotation Device in the SmartRow 2 site

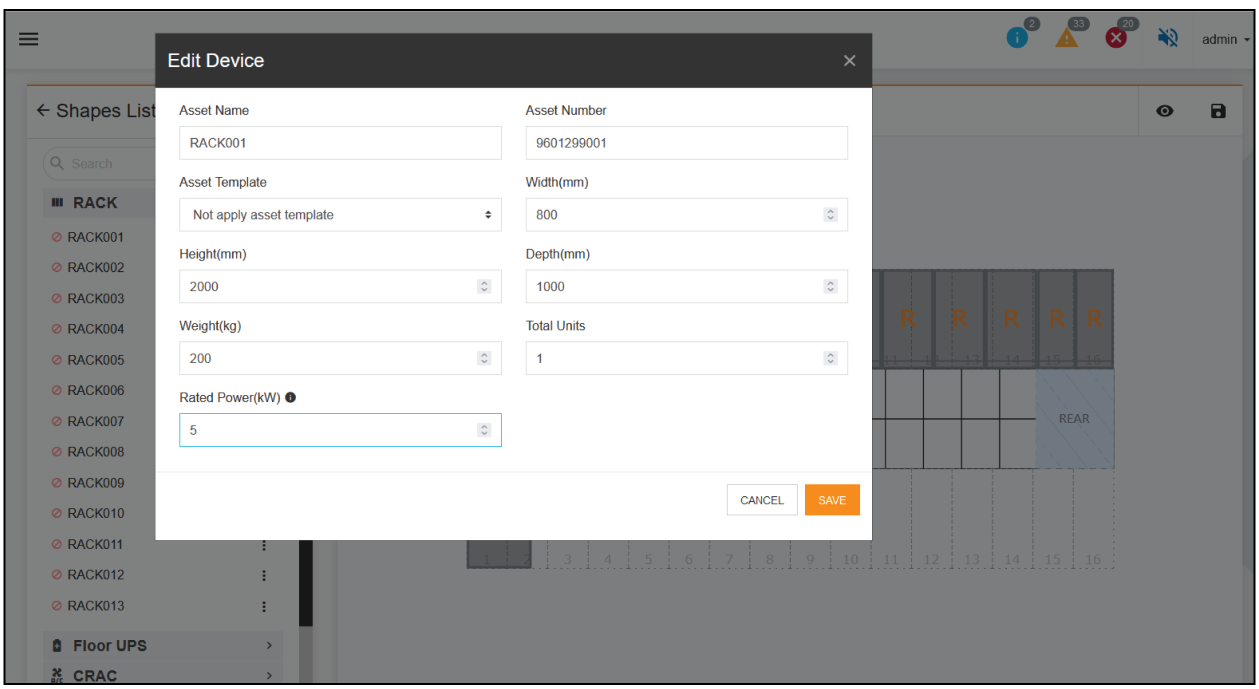


4.3.3 Editing or Adding the Devices

Editing the Device

After entering the 3D configuration page of the site, users can click on the *ellipses* in the shapes list on the left, open the function menu, and select *Edit*, you can edit the asset name, asset number, width, depth, height, etc. of the device. When you have completed, click *Save* to save your edits. This is shown in Figure 4.28 below .

Figure 4.28 Edit Device

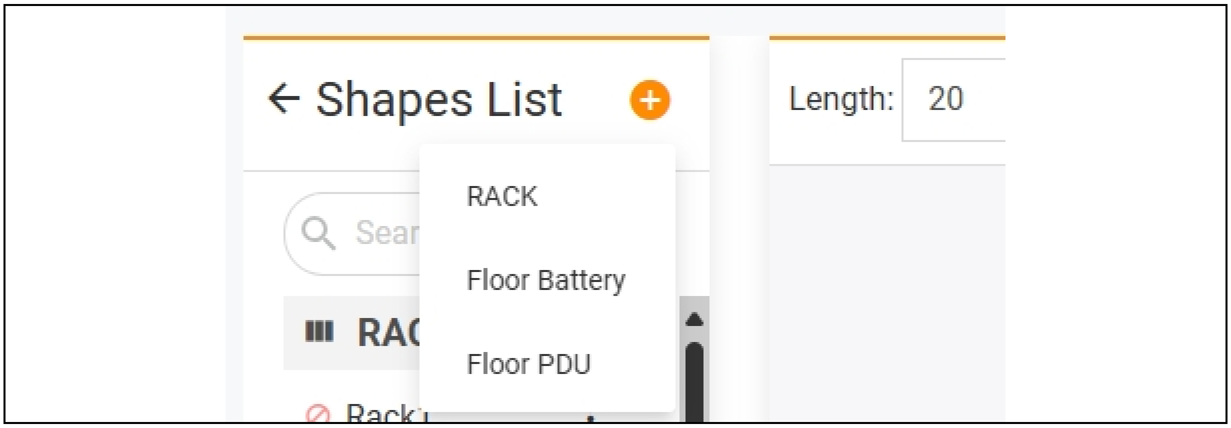


Adding a New Device

If the necessary equipment is missing from the shapes list, you can *add* one by clicking the Add button on the top-right of the shapes list.

Currently supported device types: Rack, Floor Battery, Floor PDU.

Figure 4.29 Add Device in 3D Configuration

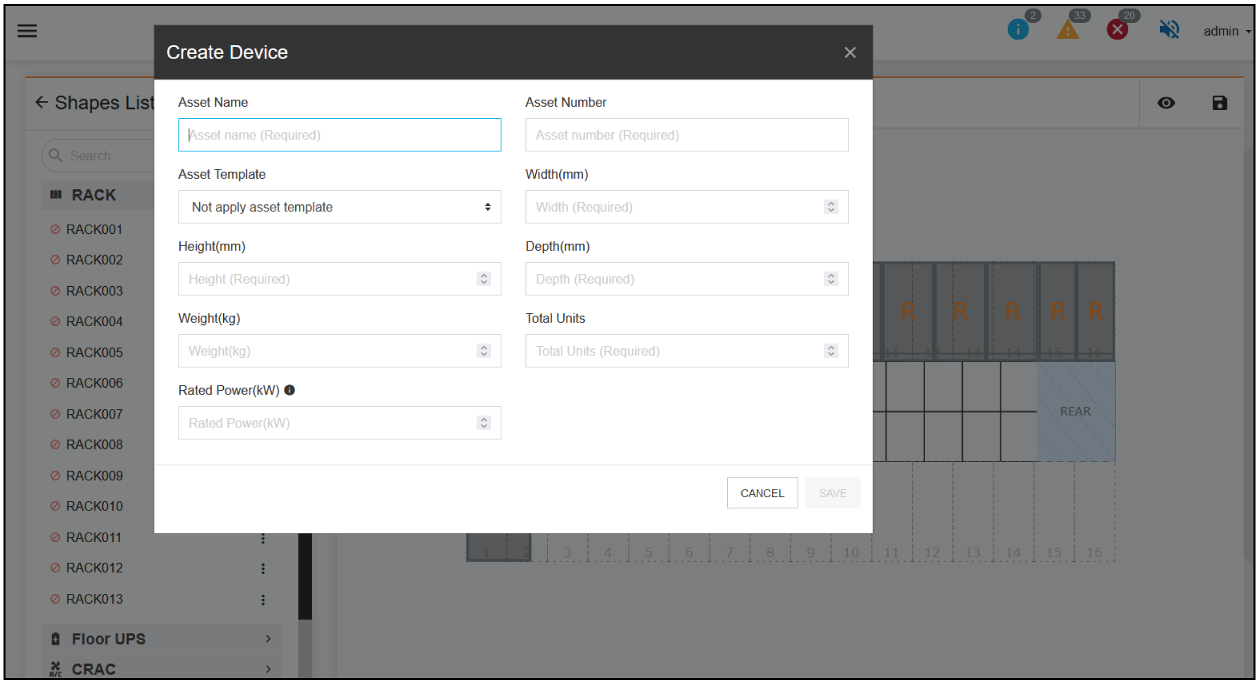


1. Adding Rack and Floor Battery

When adding a rack, you'll need to provide the asset name and asset number. You can either select an asset template or manually input the device parameters, such as width, height, and depth. Input the Rated Power of the rack so that you can evaluate the power capacity in 3D. Once you've entered the necessary information, click *Save* to add the device to the shapes list.

Adding a floor battery is the same as adding a rack, unless you need to combine the real time signals of lithium battery or lead-acid battery to the battery device. Please refer to Lithium Battery 3D Configuration on page 83 and Lead-Acid Battery 3D Configuration on page 84.

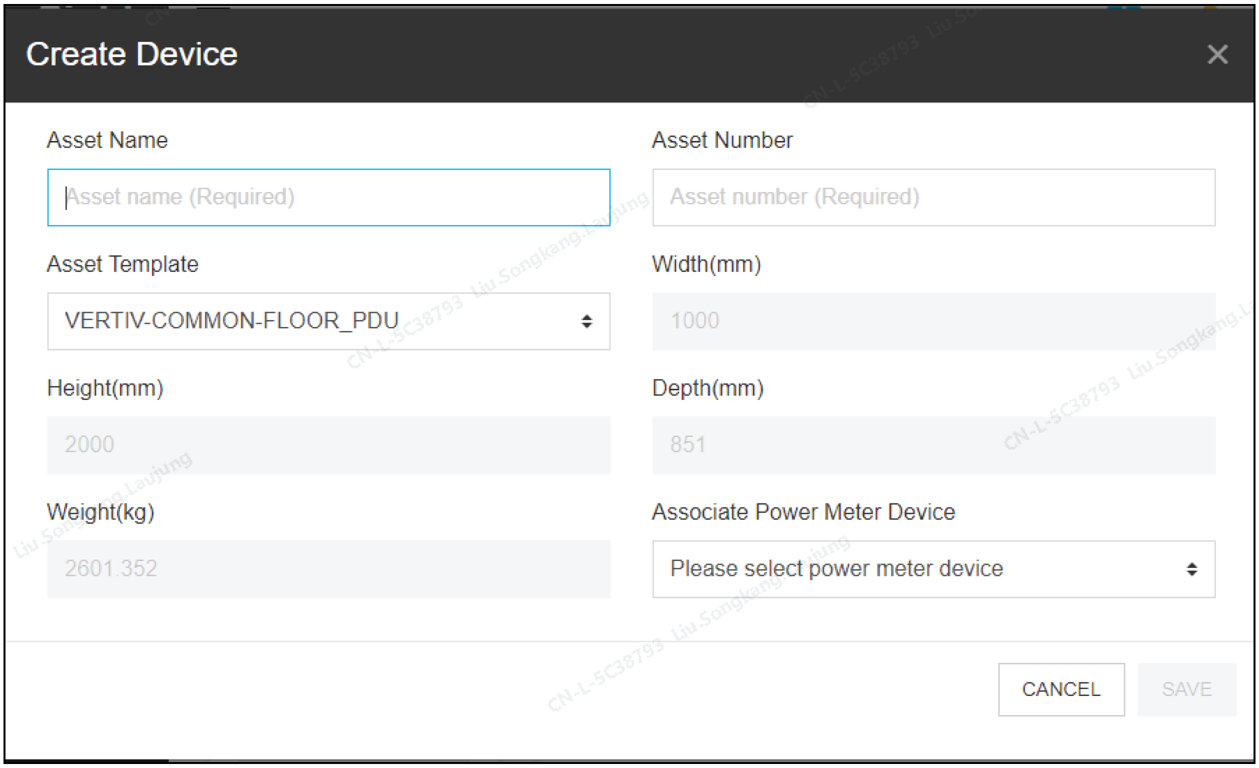
Figure 4.30 Add Device Popup Window



2. Adding a Floor PDU

When manually adding a Floor PDU (power distribution cabinet), you can associate it with a specific meter device. Once linked, the 3D visualization display will show the signal data and alarm from the connected power meter.

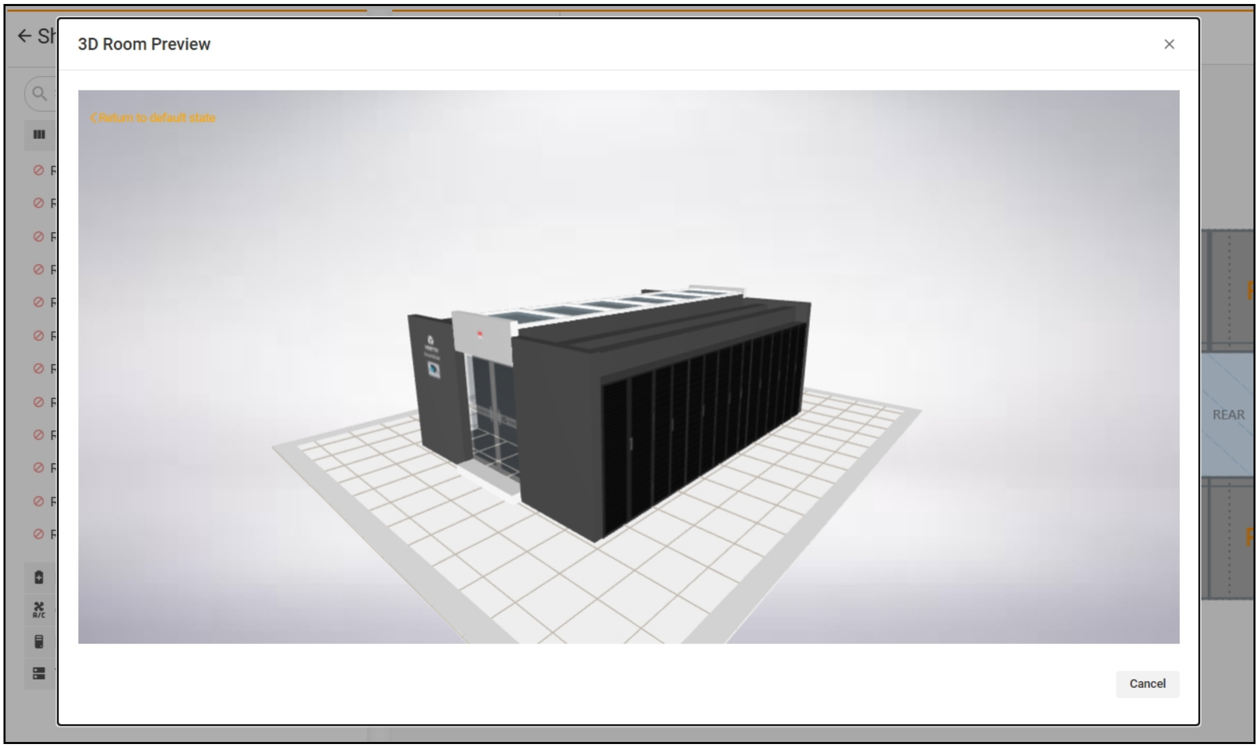
Figure 4.31 Adding a Floor PDU



4.3.4 Preview or Save 3D Configuration

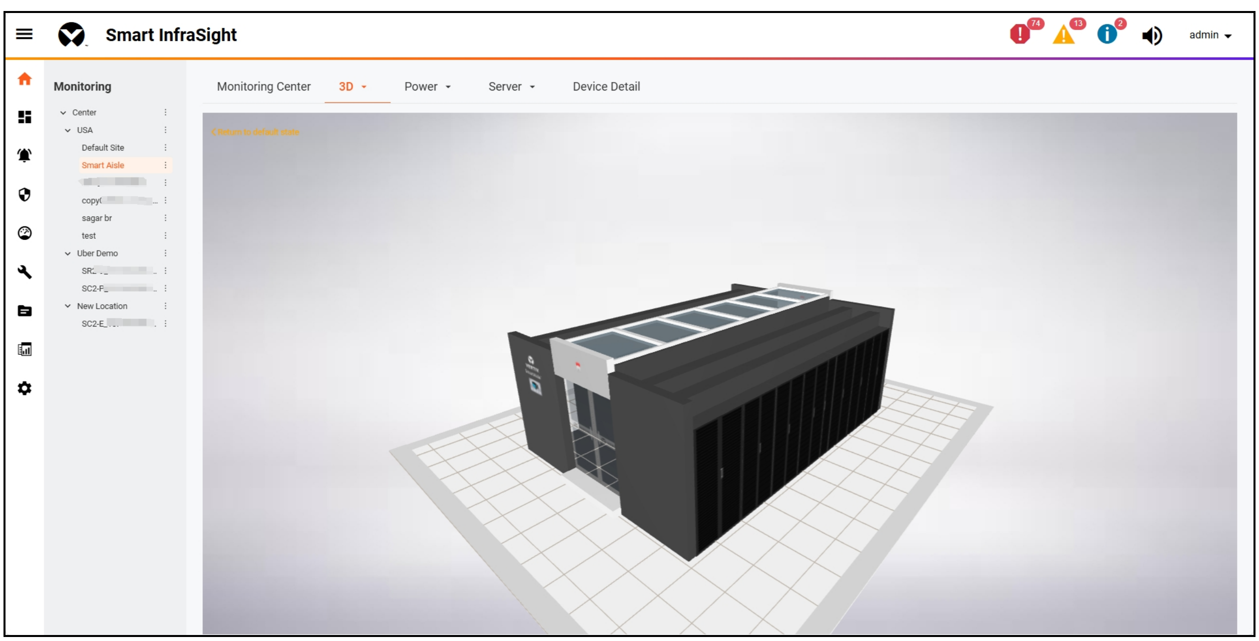
After all the configurations are completed, click the *preview* button at the top to view the 3D appearance of the corresponding site/location in the pop-up preview pop-up window. As shown in Figure 4.32 on the facing page .

Figure 4.32 Preview of 3D View



Once you have verified that all the information is correct, click *Save* button at the top of the page. Then, click the *Back* button on the top-left of the page to return to the monitoring center of the site. From there, click the *3D* tab to view the 3D models of the site, as shown in Figure 4.33 below .

Figure 4.33 3D Room Monitoring



4.3.5 Configuring the Rack

After entering the 3D configuration page of the site, you can double-click any rack on the graph to enter the 3D configuration of the current rack. As shown in Figure 4.34 below .

Figure 4.34 3D Configuration of the Smart Aisle 3 Site

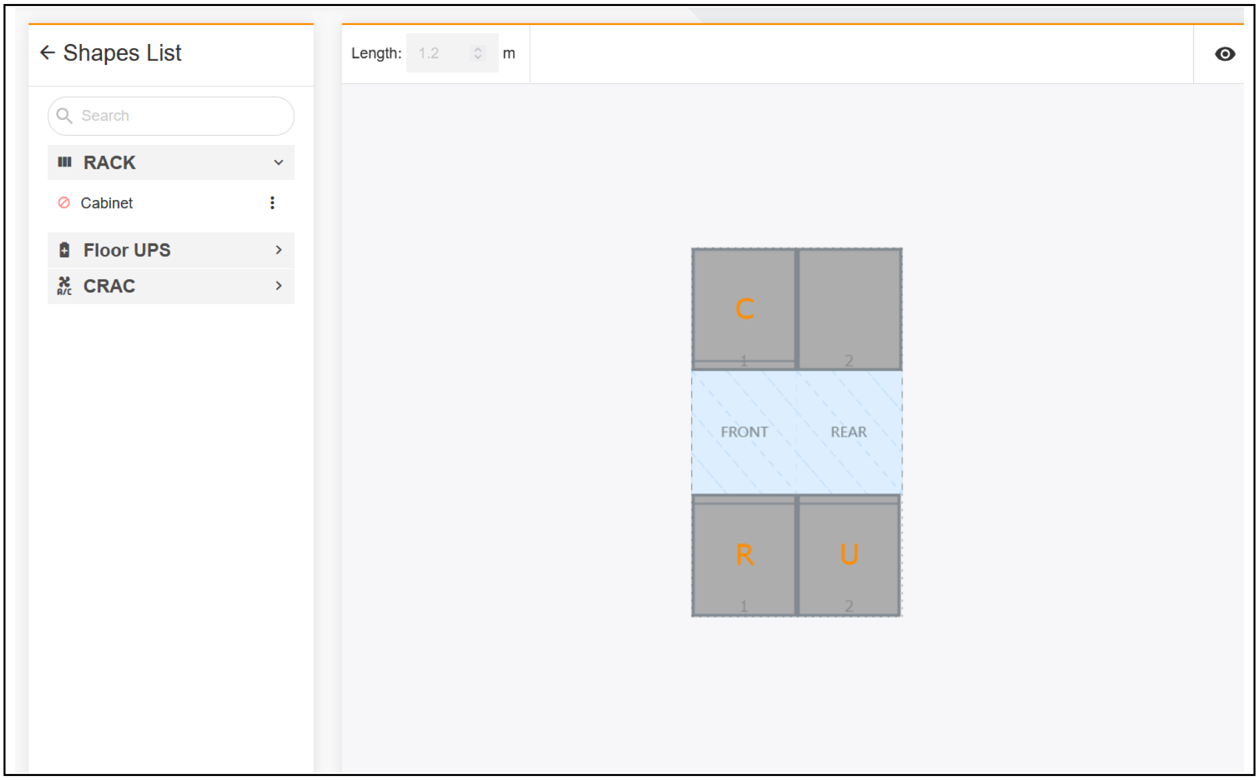
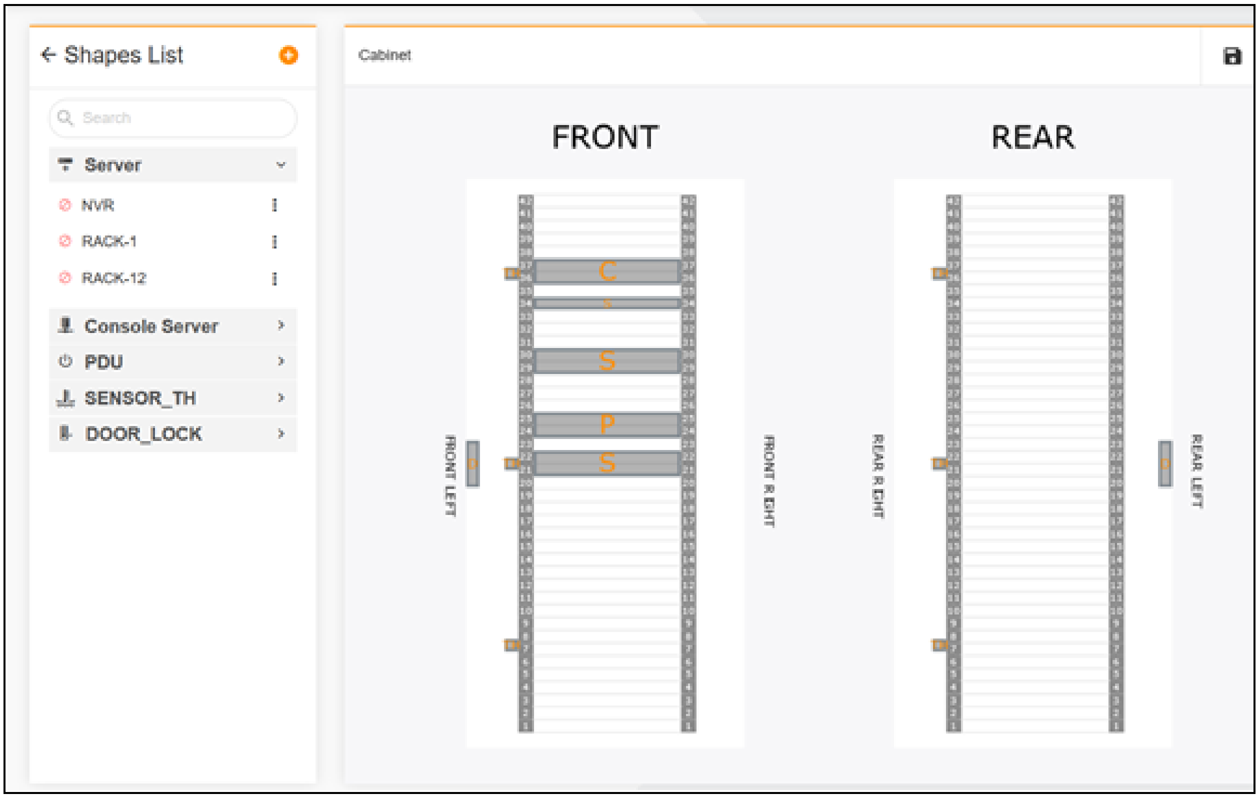
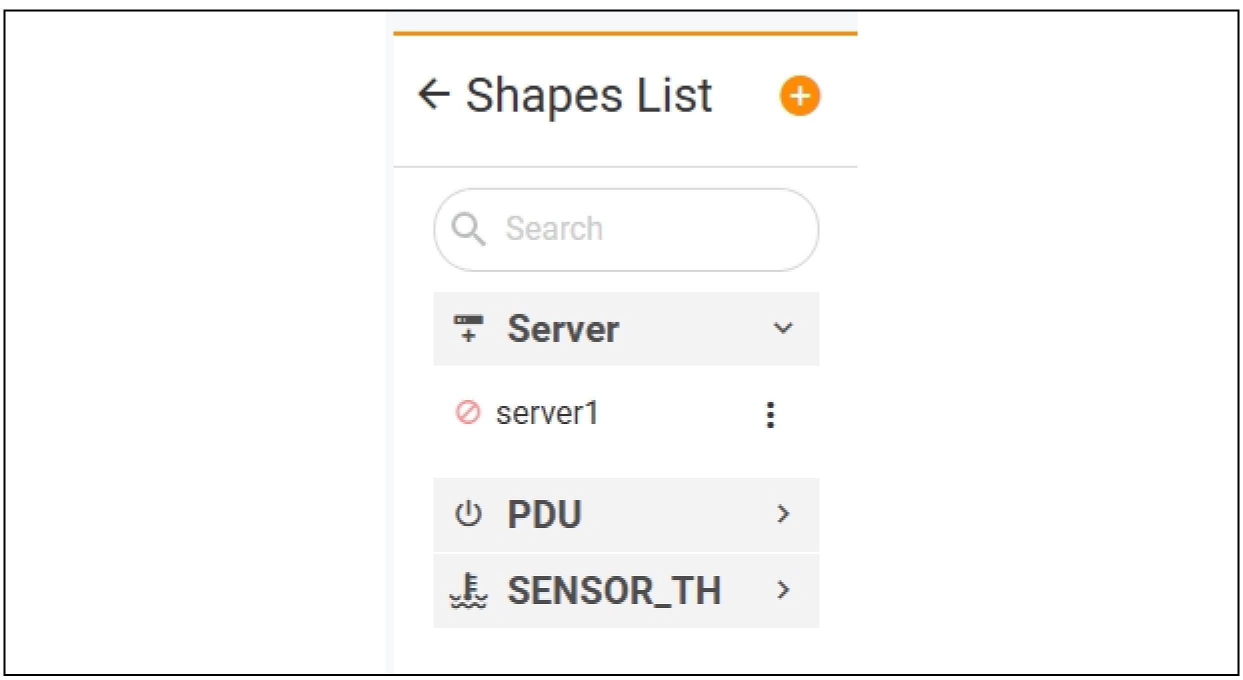


Figure 4.35 3D Configuration of Rack



After entering the 3D configuration page of rack, the shapes list contains all devices that can be place inside the rack. As shown in Figure 4.36 below .

Figure 4.36 Shapes List of Rack



The shapes list contains servers, switches, temperature and humidity sensors, and door locks, and their relationships with racks are as follows:

- In SmartAisle2, medium temperature and humidity sensor need to be manually configured, while in SmartAisle3, temperature and humidity sensor and door lock are automatically configured and cannot be edited and modified.
- Switches, PDUs, and servers need to be manually added and configured.

In the SmartRow2 site, double-click the power management cabinet (PMC cabinet for short) to enter the 3D configuration of the PMC cabinet, as shown in **Figure 4.37** below .

Figure 4.37 3D Configuration of the SmartRow2 Site

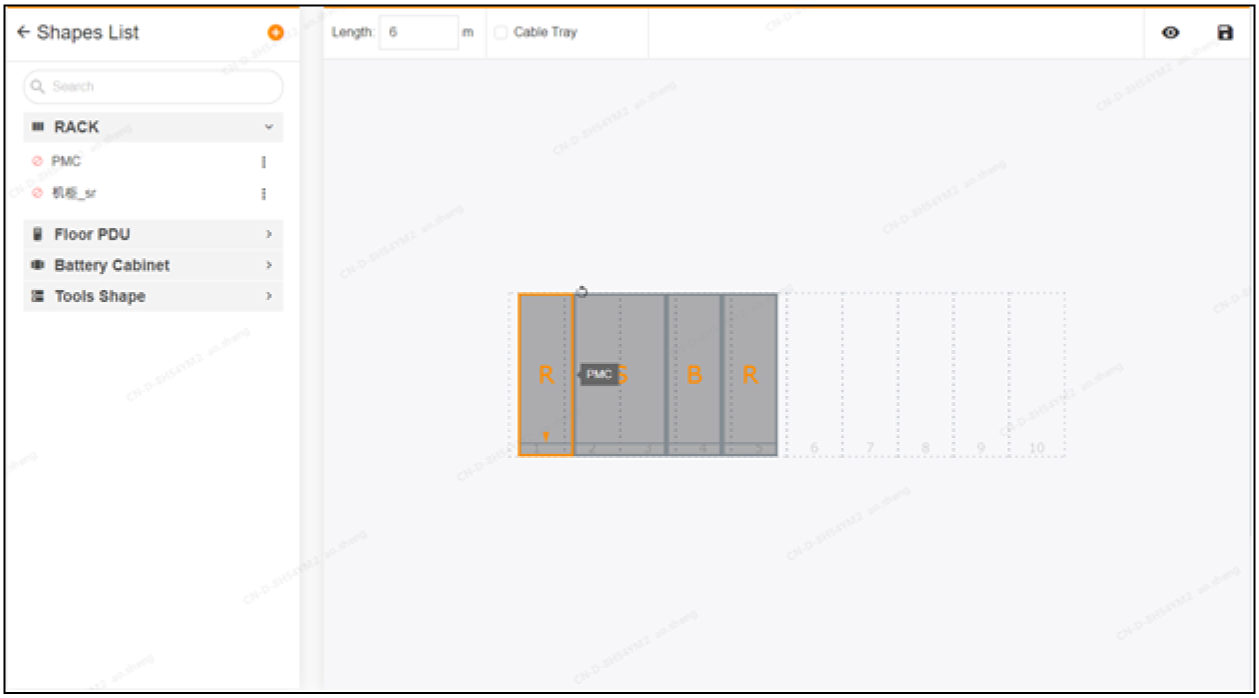


Figure 4.38 PMC Cabinet 3D Configuration

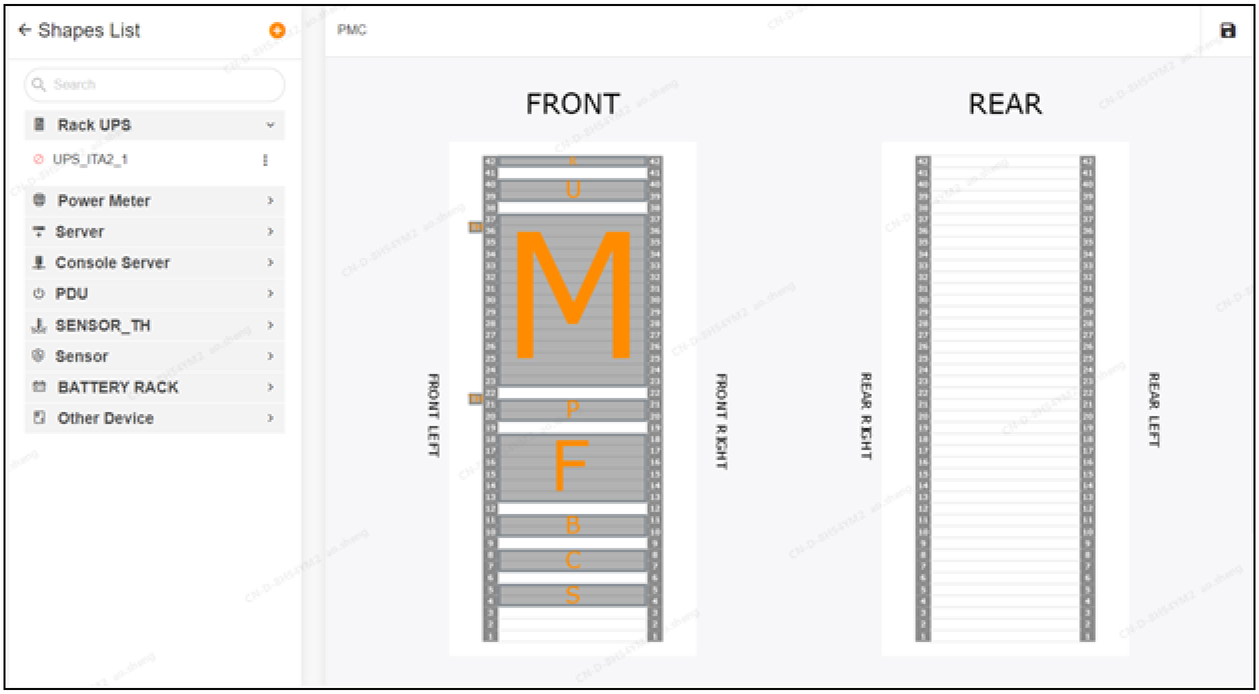
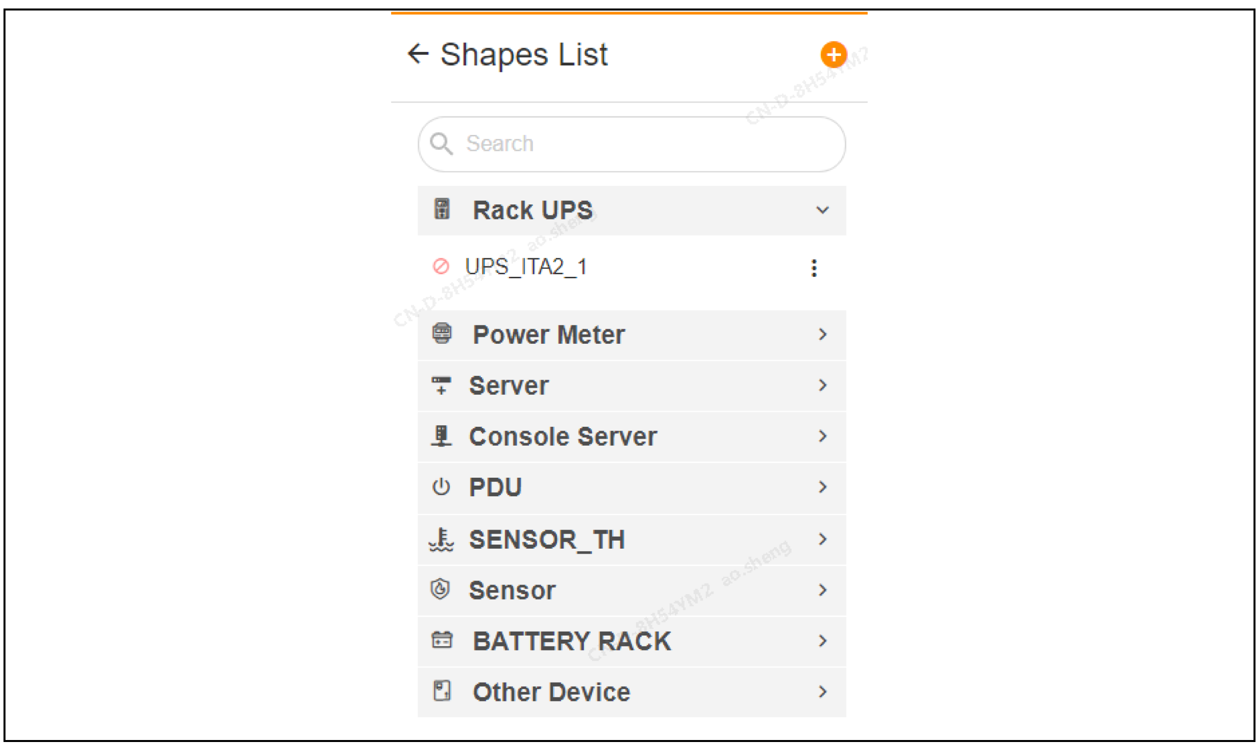


Figure 4.39 Shapes List of PMC Cabinets



The shapes list in PMC cabinet includes rack-mounted UPS, power meters, servers, switches, PDUs, temperature and humidity sensors, sensors, rack-mounted batteries, and others, and their relationship with the PMC cabinet is as follows:

- **Rack UPS** All rack-mounted UPS devices under the current site are listed under the Rack UPS category, and the rack UPS can be modified for asset templates and U-position number, and configured to position in the PMC cabinet.
- **Meter** All power meter devices for the current site is listed under the Power Meter category, the meter equipment in the PMC cabinet represents the distribution switch of the PMC cabinet, you can modify their U position and configure them in the PMC cabinet.
- The **temperature and humidity sensor** needs to be manually configured in the position of the PMC cabinet.
- **Switches**, **PDUs**, **Servers**, **Rack Batteries** need to be manually added and configured in the location of the PMC cabinet.
- The **Fire Extinguisher** under the **Sensor** categories need to be added manually, and can be associated with the actual fire extinguisher device (in the name of ENV_DI for most cases), and the alarm information of the fire extinguisher can be displayed in the 3D visualization after the association is completed. The position of the fire-fighting equipment in the PMC cabinet can be manually configured.
- The **RDU intelligent monitoring unit device** under **Other** categories is an automatically created equipment asset, which is placed at the top of the PMC cabinet and cannot be deleted.

Device Status

The device list displays four possible statuses:

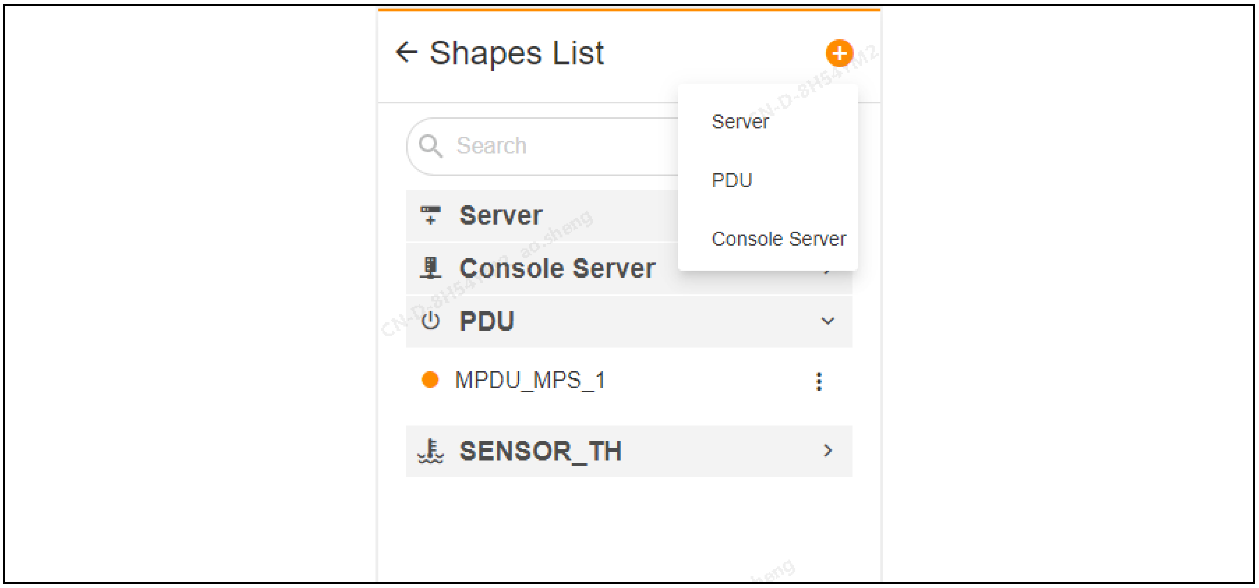
- Incomplete information: The device cannot be dragged. Users must edit the device's basic information.
- Ready to place: The device can be dragged into the current cabinet without additional information.
- Exists in another cabinet: The device can be dragged, but users will be prompted to unbind it from its current cabinet.
- Already in current cabinet: The device cannot be dragged.

To remove a device from the canvas of 3D configuration, select it and press the Delete key on keyboard.

General Rack Configuration

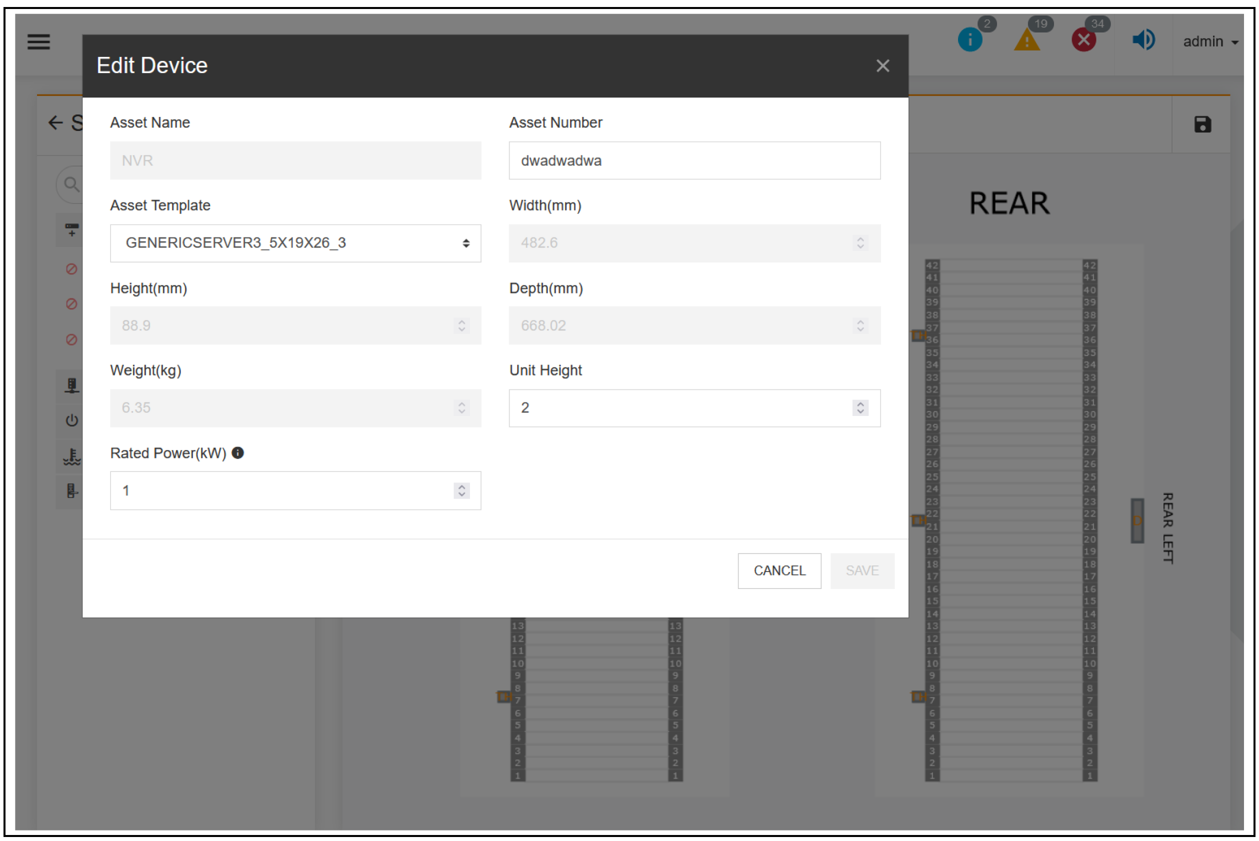
You can add servers, PDUs, and switches by clicking next to the *Add* graphical list of common cabinets, as shown in the **Figure 4.40** on the facing page .

Figure 4.40 3D Configuration of a Common Cabinet—Adding Devices



After adding the server device, the user can edit the device information. As shown in **Figure 4.41** below .

Figure 4.41 The Server Configuration window

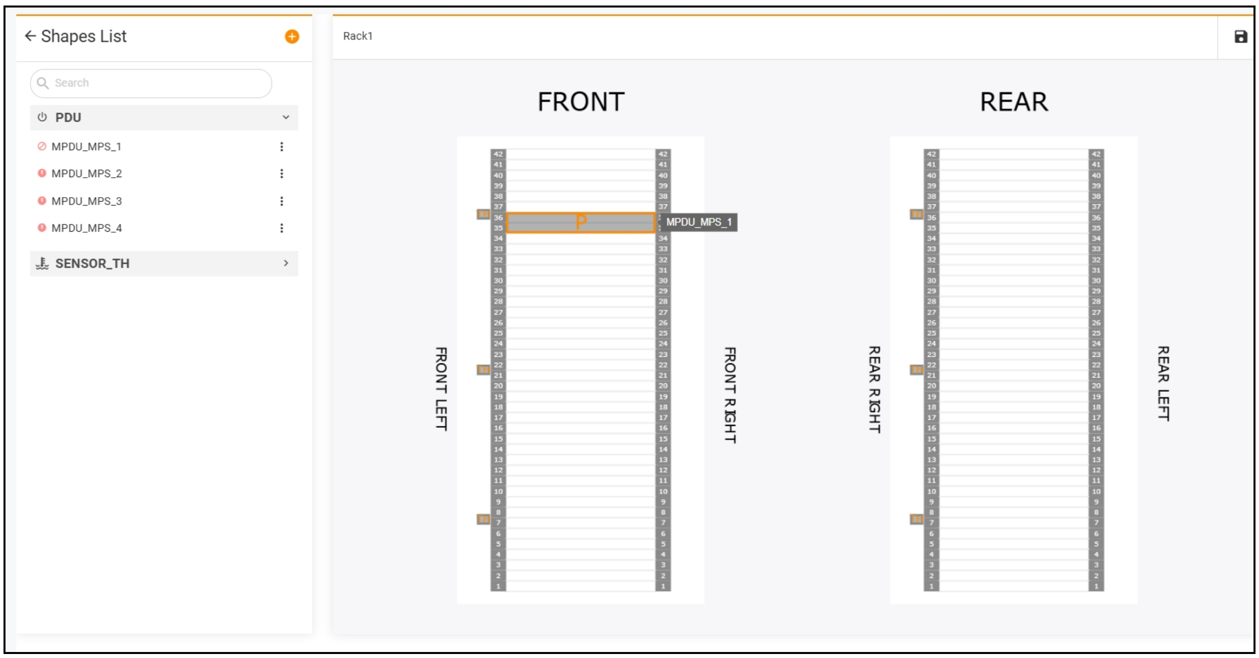


The information that can be changed for the server device includes:

1. **Asset Number**
2. **Asset Template:** The width, depth, height, and weight change with the asset template, or you can choose not to apply the asset template to change the depth, height, and weight by yourself.
3. **U Height**: It affects the U position occupied by server equipment in the cabinet.
4. **Rated Power**: After setting, it will participate in the calculation of the power distribution capacity of the cabinet.
5. **Outlet Air Temperature Signal**: If the server device is an IPMI device (see Server Management Detailed Functions on page 166 details for the addition and management of IPMI equipment, you can configure the **air outlet temperature signal**, and select the corresponding temperature signal in the server device in the drop-down box. The **Outlet Temperature Signal** will be used in the Heatmap 3D Module, which will display the temperature heat map of the server device.

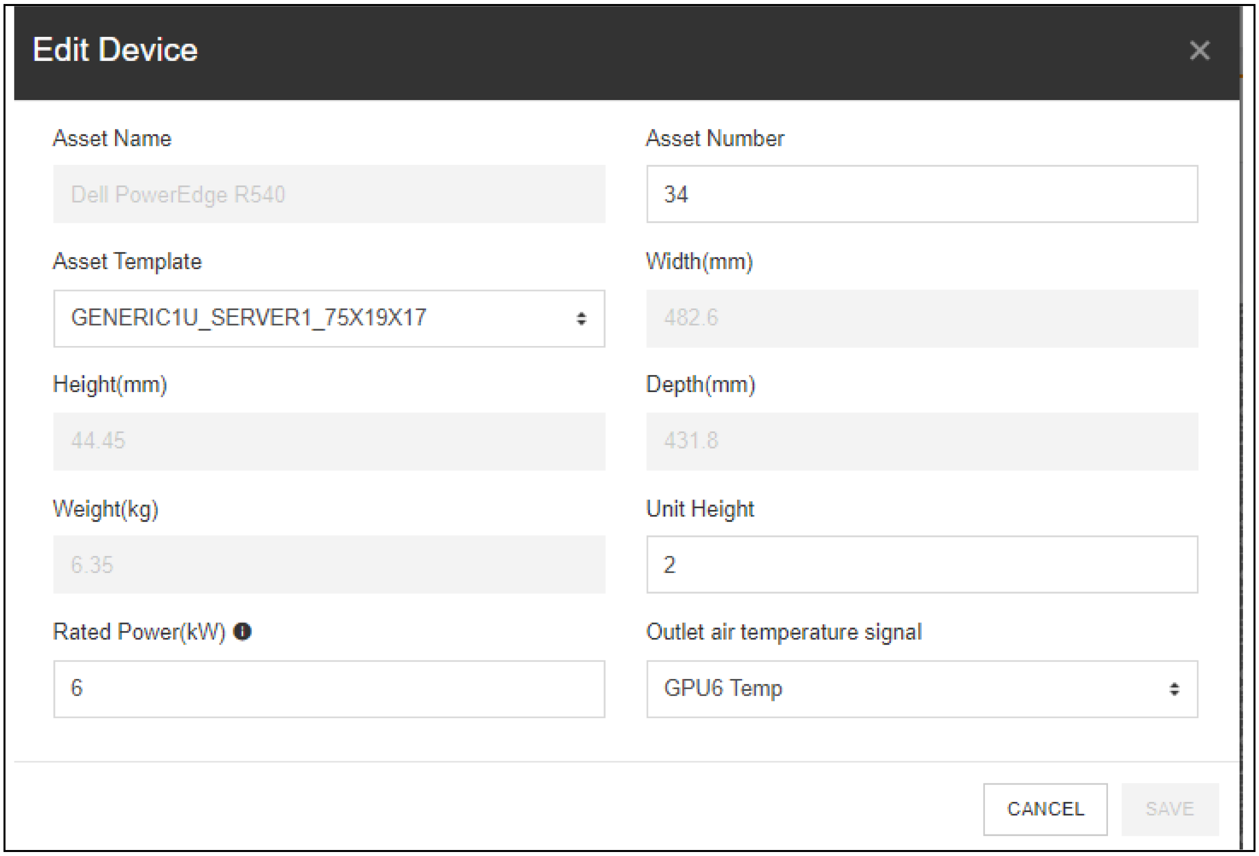
After the server or switch device is added, you can drag the server from the shapes list on the left. As shown in **Figure 4.42** below .

Figure 4.42 3D Configuration—Dragging the Device



After adding a PDU device, you can edit the PDU device information. As shown in **Figure 4.43** on the facing page .

Figure 4.43 PDU Configuration Window

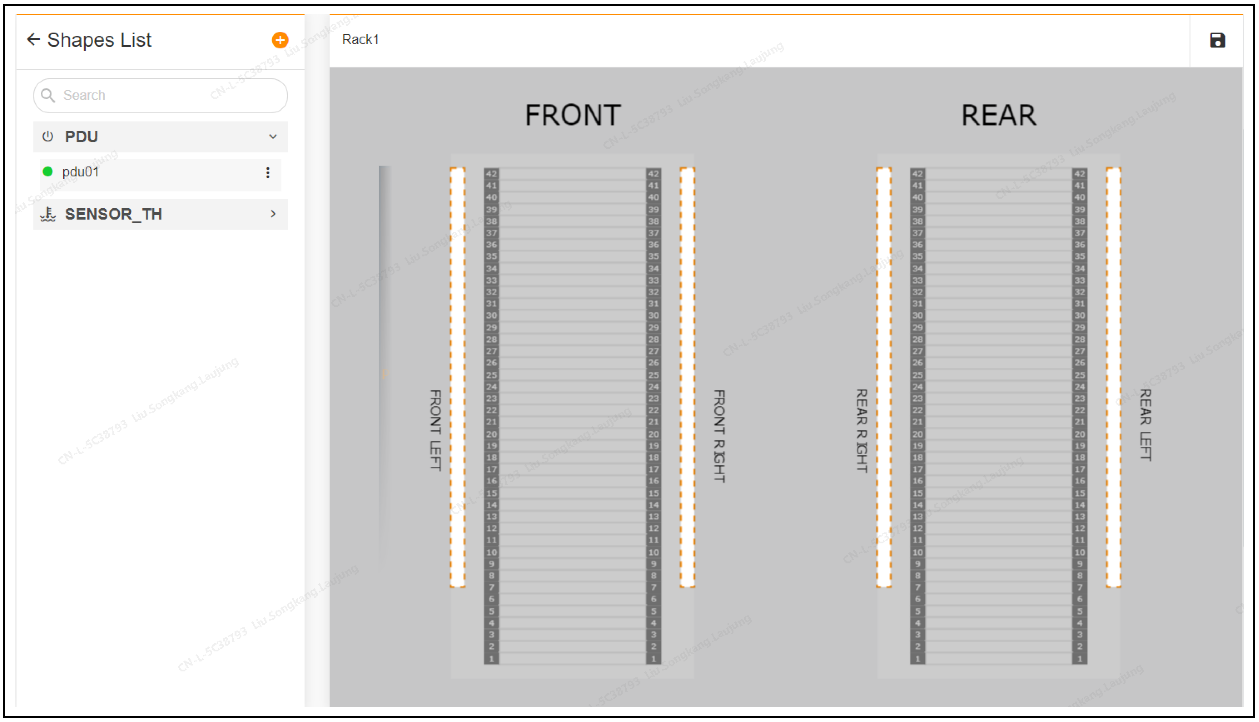


The PDU device information that can be changed includes:

1. Asset Number

2. Asset Template: The width, height, depth, weight, and number of phases follow the change of the asset template, or you can choose not to apply the asset template to modify it yourself.

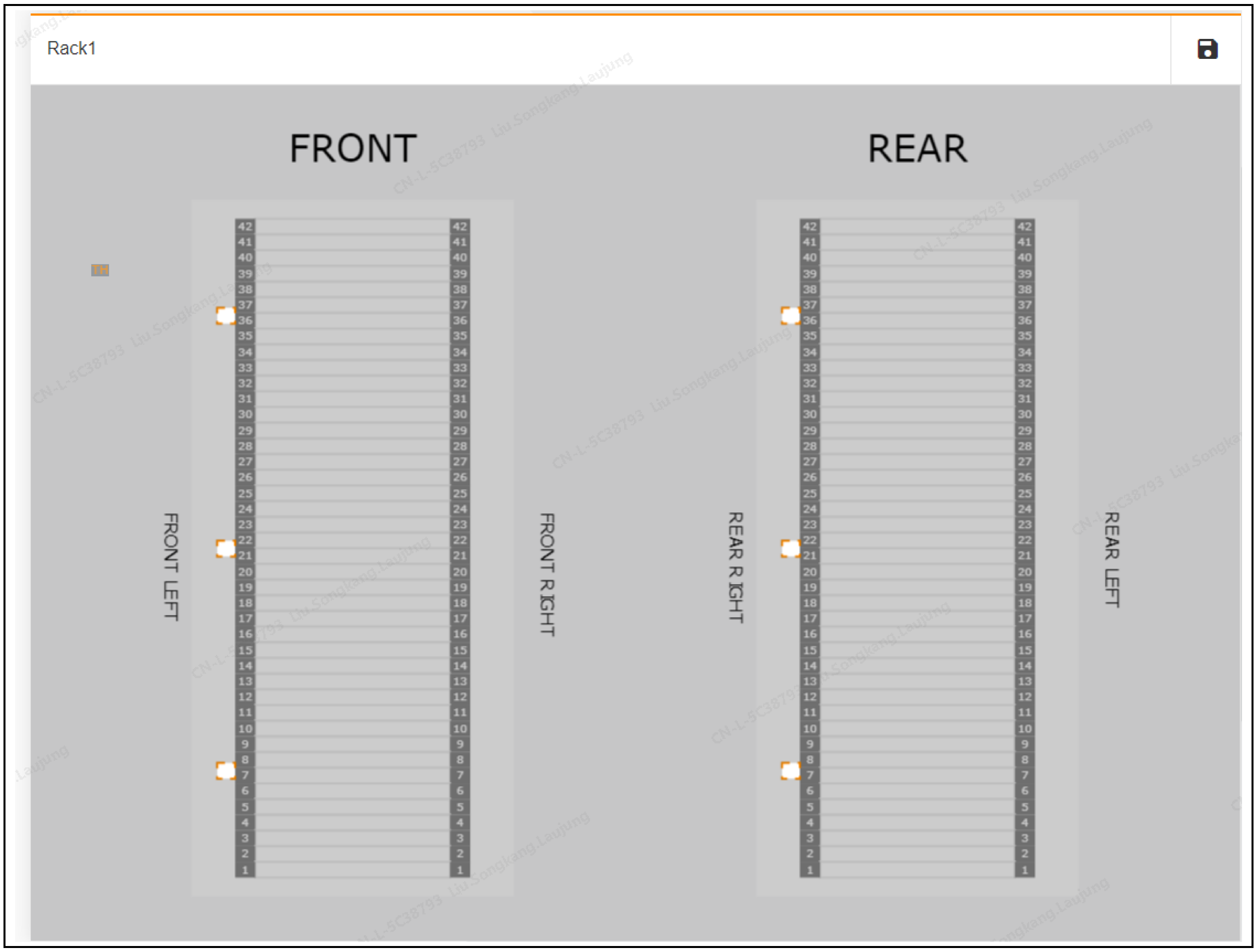
Figure 4.44 A ZERO U PDU can be Configured in Four Positions at the Front and Rear Doors



3. U Height: When it is 0, it does not occupy the U position of the cabinet, when it is not 0, dragging the PDU into the cabinet will occupy the U position of the cabinet.

4. Rated Power: Affects the distribution capacity display of the cabinet in 3D visualization.

Figure 4.45 Cabinet Power Distribution



The temperature and humidity sensor list displays all available sensors for the site. These can be dragged and dropped to six positions on the cabinet's front and rear doors.

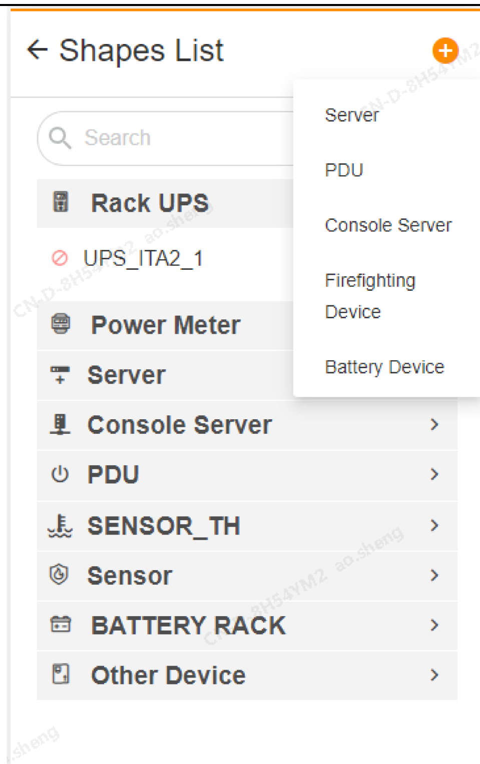
After configuring all devices in the cabinet, click Save in the upper-right corner to store the cabinet's 3D configuration.

NOTE: Under the SmartAsile3 site, the temperature and humidity sensors, door locks, and other devices in the cabinet cannot be edited, configured, or deleted. Door locks, POD BUST, POD DIDO, POD POWER devices are also not displayed in the shapes list.

PMC Cabinet Configuration

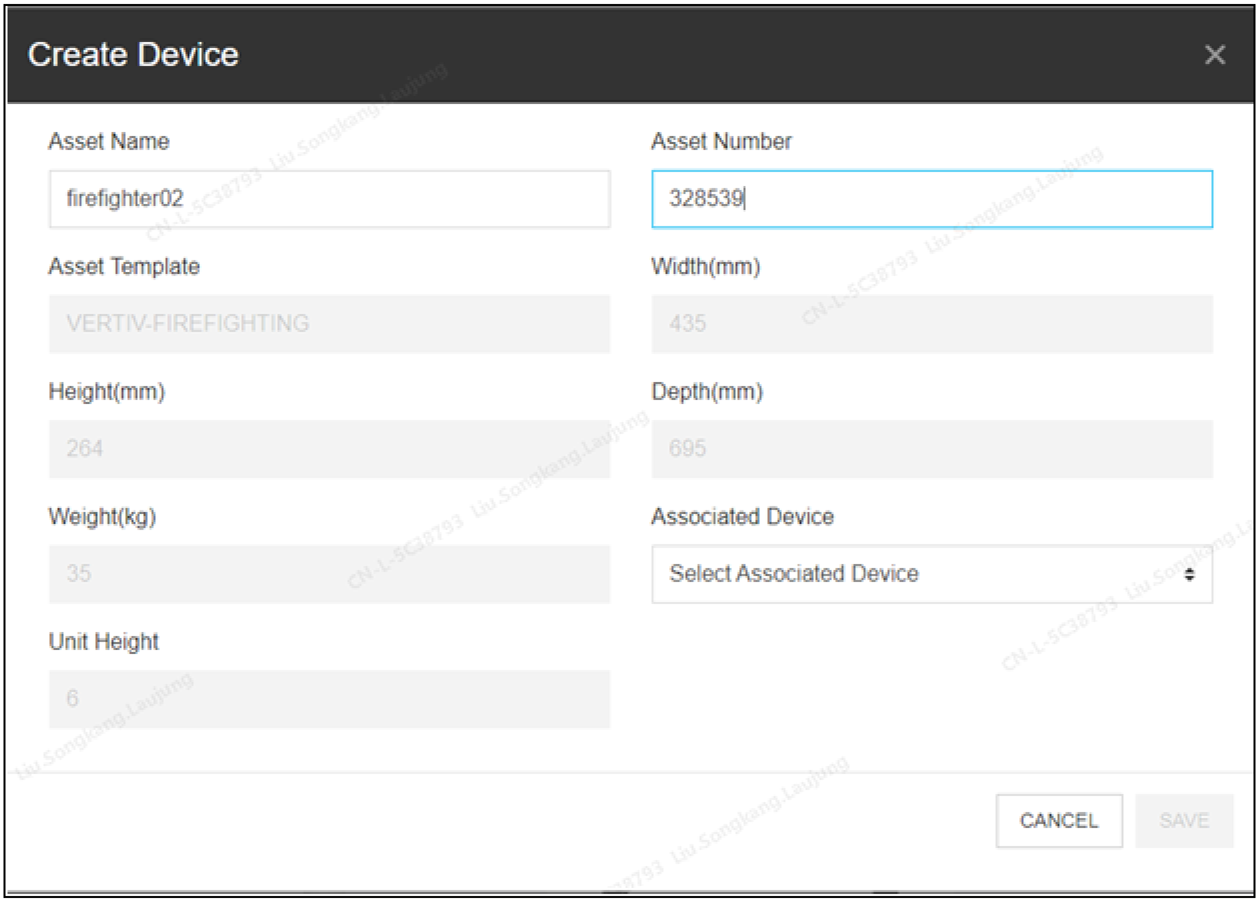
Click *Add* to the shapes list to add servers, PDUs, switches, firefighting equipment, and battery equipment, as shown in Figure 4.46 on the next page.

Figure 4.46 PMC Cabinet 3D Configuration—Add Equipment



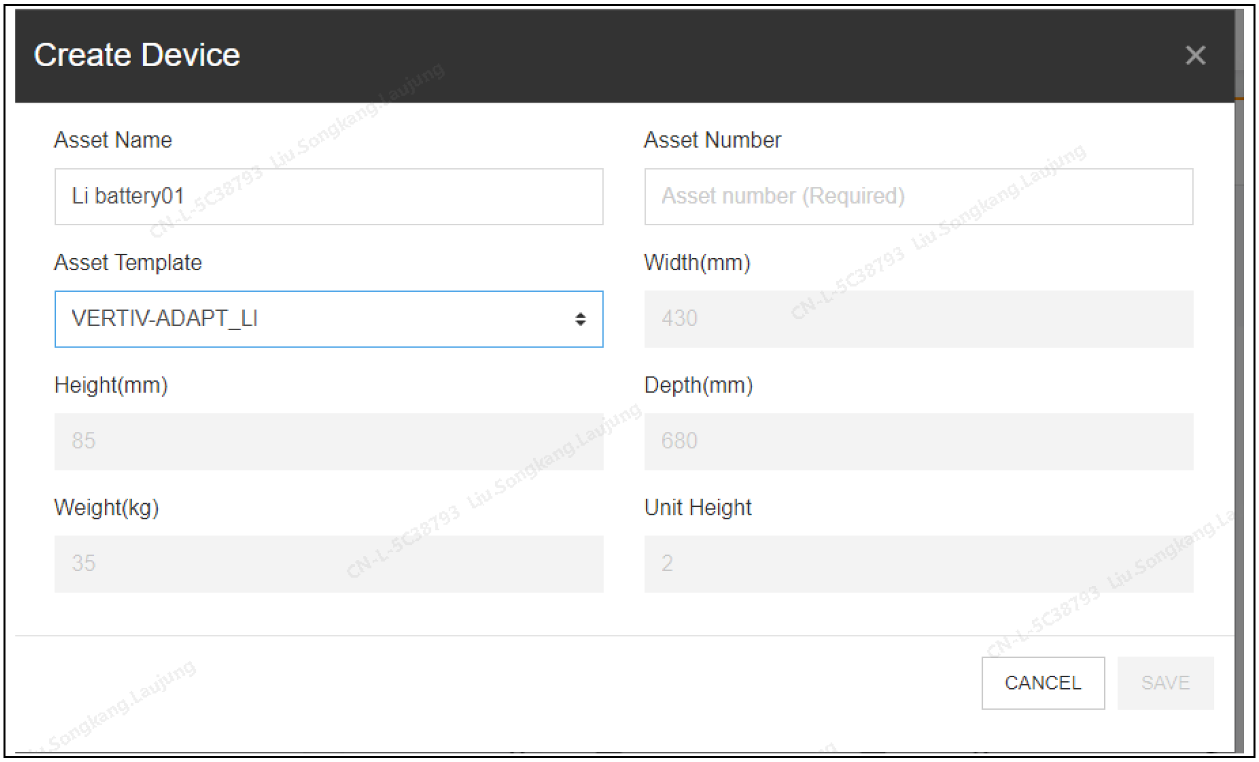
When adding fire-fighting equipment, you can associate it with the monitorable fire-fighting device as shown in **Figure 4.47** on the facing page , and the alarm information of the device can be displayed in the 3D visualization after association.

Figure 4.47 Firefighting Equipment Configuration Popup Window



To add a rack-mounted battery device, you can configure the asset number, select the asset template, and change the width, height, depth, weight, and floor height with the asset template. As shown in **Figure 4.48** on the next page .

Figure 4.48 Adding a Rack-Mounted Battery Device



4.3.6 Configure the Power Distribution Cabinet

The power distribution cabinet is configured based on the relationship between the PDU and the power distribution cabinet.

General Configuration

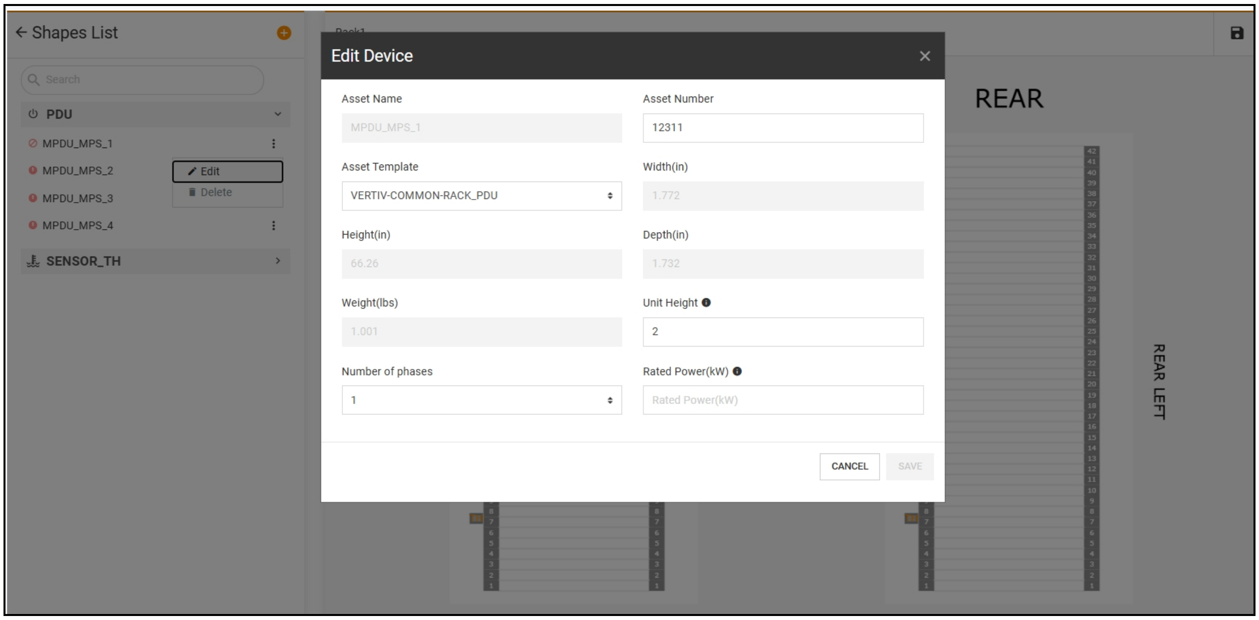
The device list displays four possible status for each item:

- Incomplete information: Devices with incomplete information cannot be dragged. Users must edit the device's basic information first
- Available for placement: Devices available for placement can be dragged into the current cabinet without additional information.
- Already placed in another cabinet: Cannot be dragged
- Already placed in the current cabinet: Cannot be dragged

Distribution Cabinet Configuration

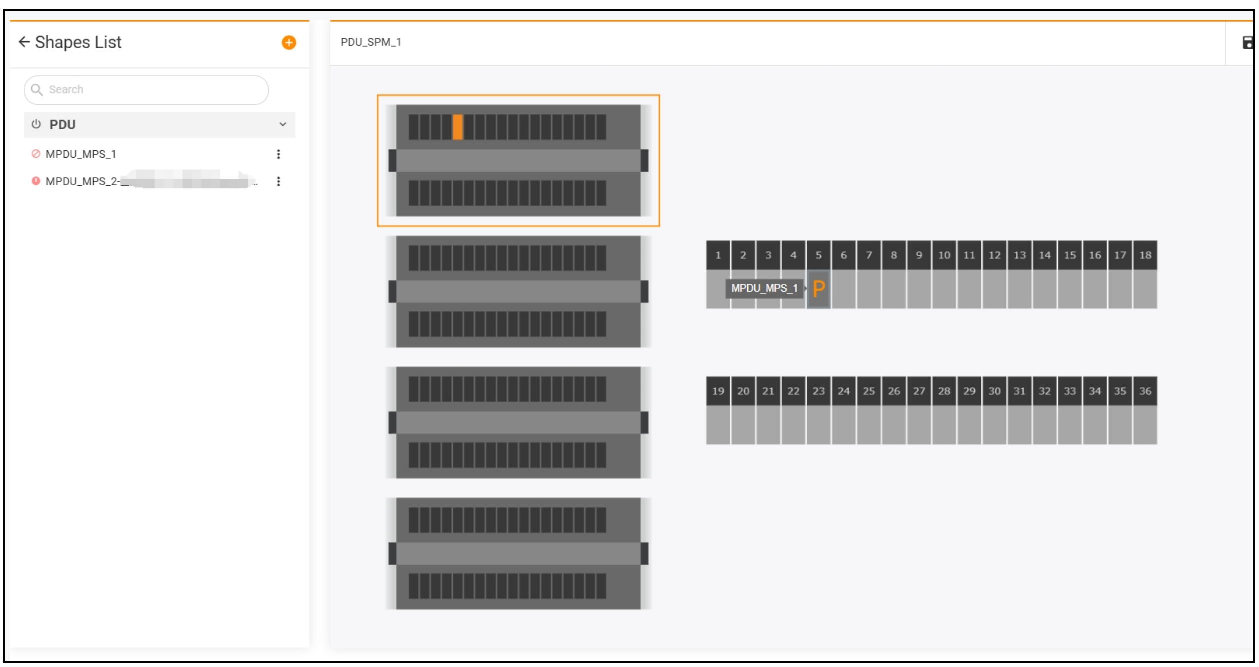
Users can add and edit PDU device information. As shown in **Figure 4.49** on the facing page .

Figure 4.49 Adding/Editing PDUs



If you drag a PDU to a branch of the SPM distribution cabinet, the PDU can be associated with the data of the corresponding branch of the SPM distribution cabinet. As shown in **Figure 4.50** below .

Figure 4.50 Dragging and Adjusting the Position of the Device in the PDU

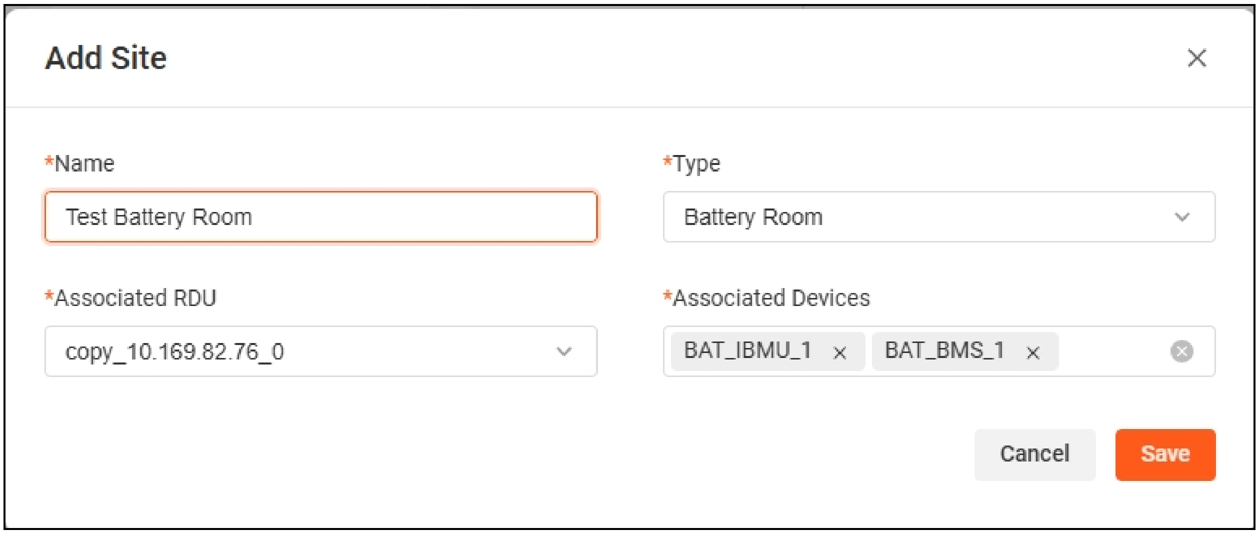


After the configuration is complete, click *save* icon to completed Configuration.

4.3.7 3D Configuration of the Battery Room

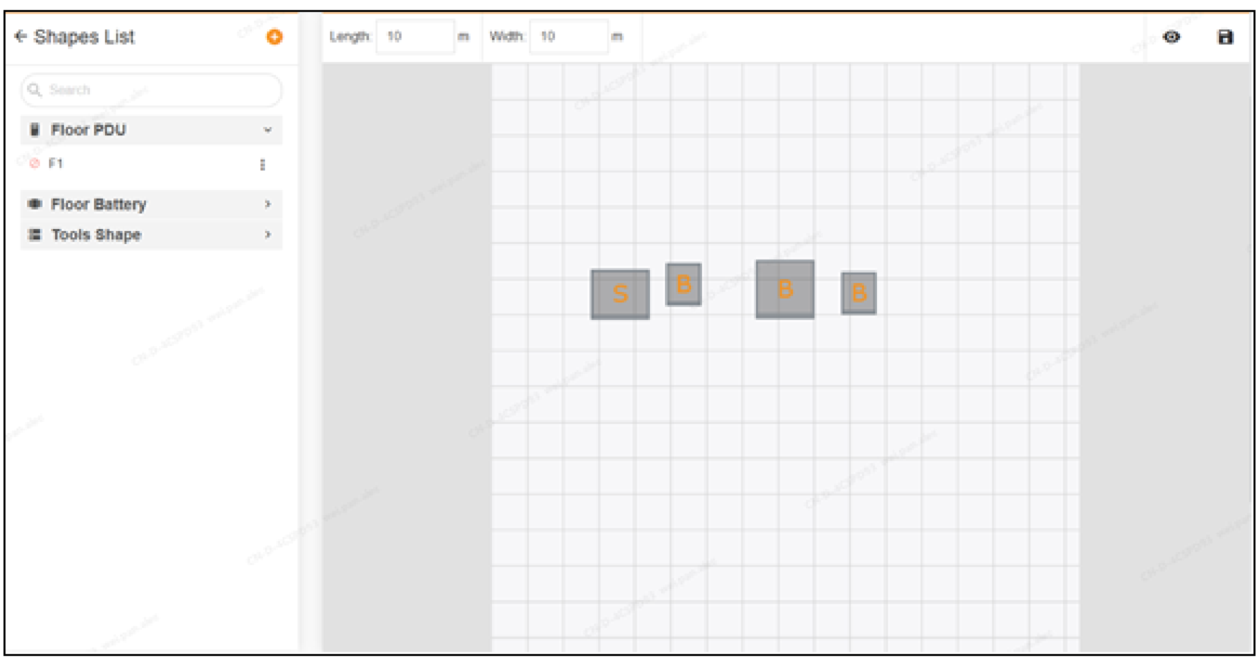
In the monitoring tree, click on the ellipses next to the location level and select Add Site. In the pop-up window, select Type as Battery Room, select the RDU where the devices come from and select UPS, Lead-acid Battery, Lithium Battery, Power Meter devices that you want to place into the battery room. Click Save to create this new battery room site. As shown in Figure 4.51 below .

Figure 4.51 Adding a 3D Battery Room Site



Click on the *ellipses* on the right side of the added battery room site, select the 3D configuration, enter the configuration interface, and drag the UPS and battery into the canvas. As shown in Figure 4.52 below .

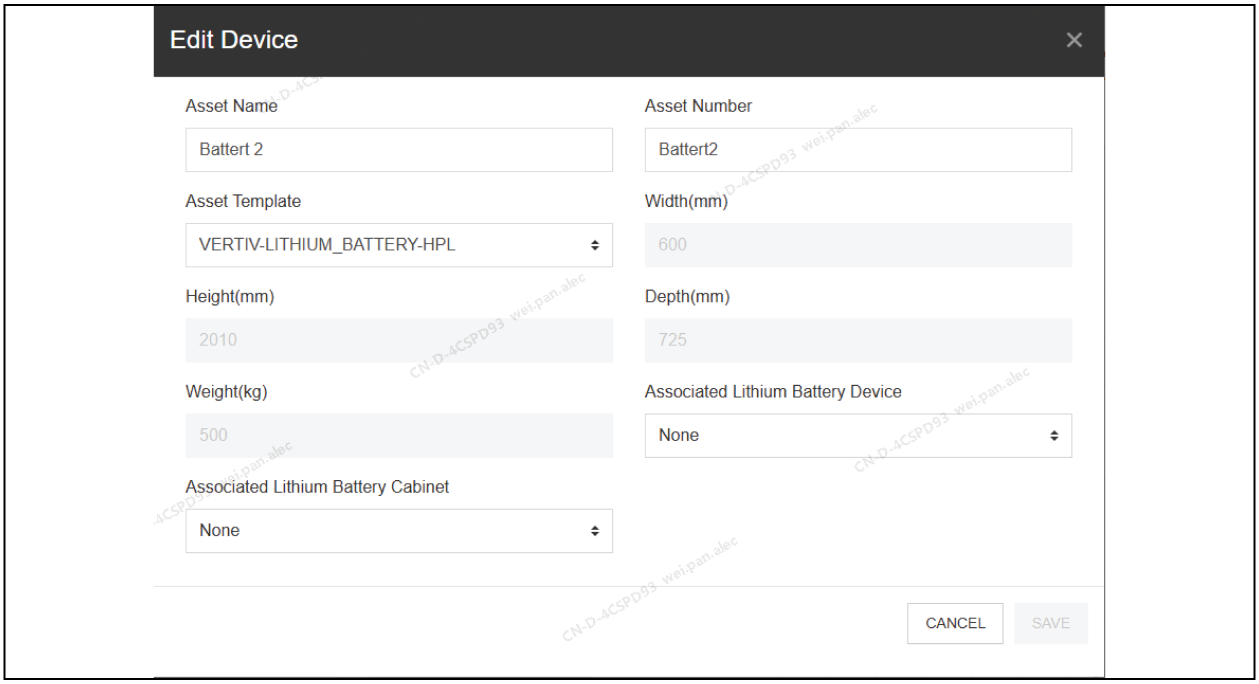
Figure 4.52 Placing Devices in Battery Room 3D Configuration



4.3.8 Lithium Battery 3D Configuration

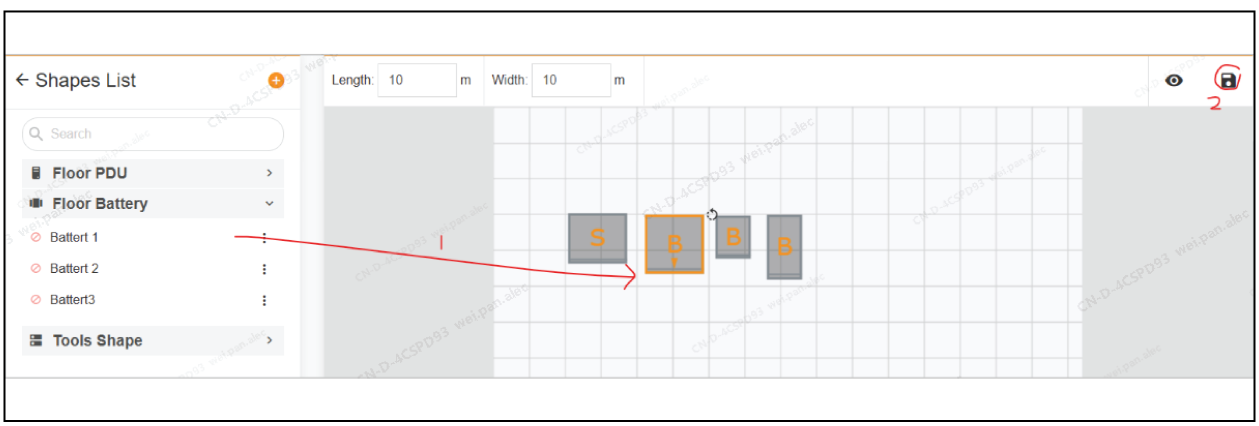
In the 3D configuration page of sites, you can manually add a device of type Floor Battery, and in the Edit pop-up window of the device, the asset template selects VERTIV-LITHIUM_BATTERY-HPL, at this time, you can associate a battery device with a HPL lithium battery cabinet that has monitorable signals (if there are multiple lithium battery cabinets, you need to add multiple Floor Battery devices). After that, you can show the real-time power signal of the lithium battery cabinet in 3D.

Figure 4.53 Editing the Battery Device



After saving, drag the Floor Battery asset you just added from the shapes list to the canvas on the right, and then click the Save button as shown in Figure 4.54 below .

Figure 4.54 Battery Configuration



4.3.9 Lead-Acid Battery 3D Configuration

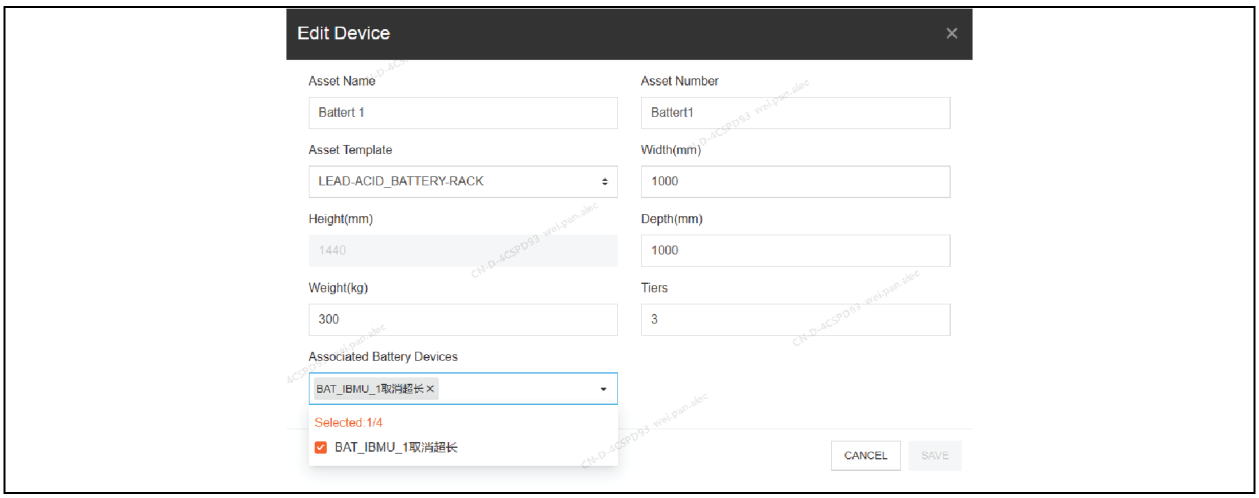
To display lead-acid batteries in 3D, you need to create a 3D model of the lead-acid battery first, the size of the model can be adjusted according to the size of the real device, and then you need to correlate the model with the real lead-acid battery device, so that you can display the signals and alarms of the lead-acid battery in 3D.

Click on the *ellipses* on the right side of the added battery room site, select 3D configuration, enter the configuration interface, and click *Add* button, select Floor Battery, and the Add Device pop-up box will appear.

Enter the asset name and asset number.

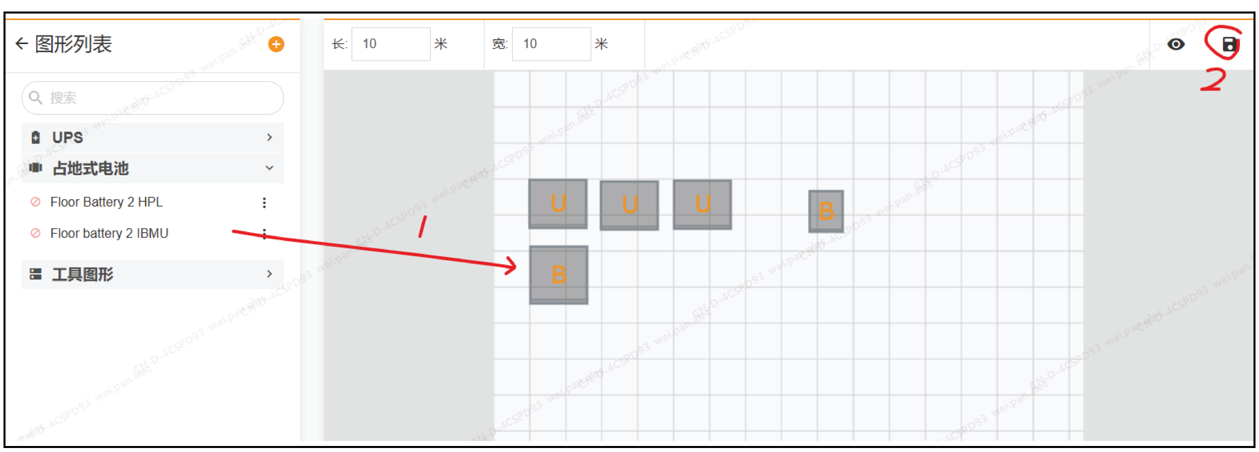
Select the template **lead-acid battery rack**, fill in the relevant information, and save it. In the configurable fields, the Height of the lead-acid battery model is determined by tiers, the more tiers the higher the battery model. And you can associate battery devices with the battery model so that when displaying the 3D of lead-acid battery, the signals and alarms of the selected battery devices can be shown in the **Figure 4.55** below .

Figure 4.55 Editing the Device



After saving, drag the Floor Battery asset you just added from the shapes list to the canvas on the right, and then click *Save*, as shown in **Figure 4.56** below .

Figure 4.56 Battery Configuration

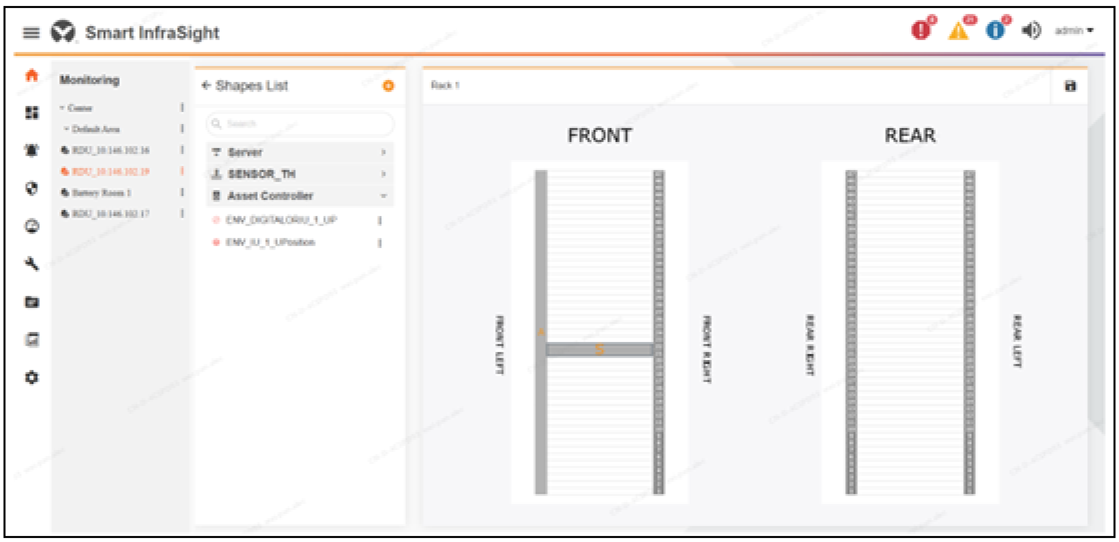


4.3.10 Configure the U-level Asset Manager

U-position Asset Manager is used to synchronize asset location information from the field and keep the asset location in the cabinet consistent with the field. To use U-position Asset Manager, follow these steps:

1. Associate the U-position Asset Manager with the corresponding cabinet. You first need to establish the relationship between the U-position Asset Manager and the cabinet: go to the 3D configuration of the site, and then double-click on a cabinet to go to the 3D configuration of the cabinet. If the U-position asset manager has already been monitored by Smart Infrasight through RDU501, then we can find the corresponding U-position asset manager of the current cabinet from the device list on the left. (In the field, the U-Position Asset Manager should have already been placed inside the current cabinet). Drag the U-Position Asset Manager out of the device list on the left and place it in the specified location in the cabinet. As shown in Figure 4.57 below .

Figure 4.57 Dragging the U-Position Asset Manager

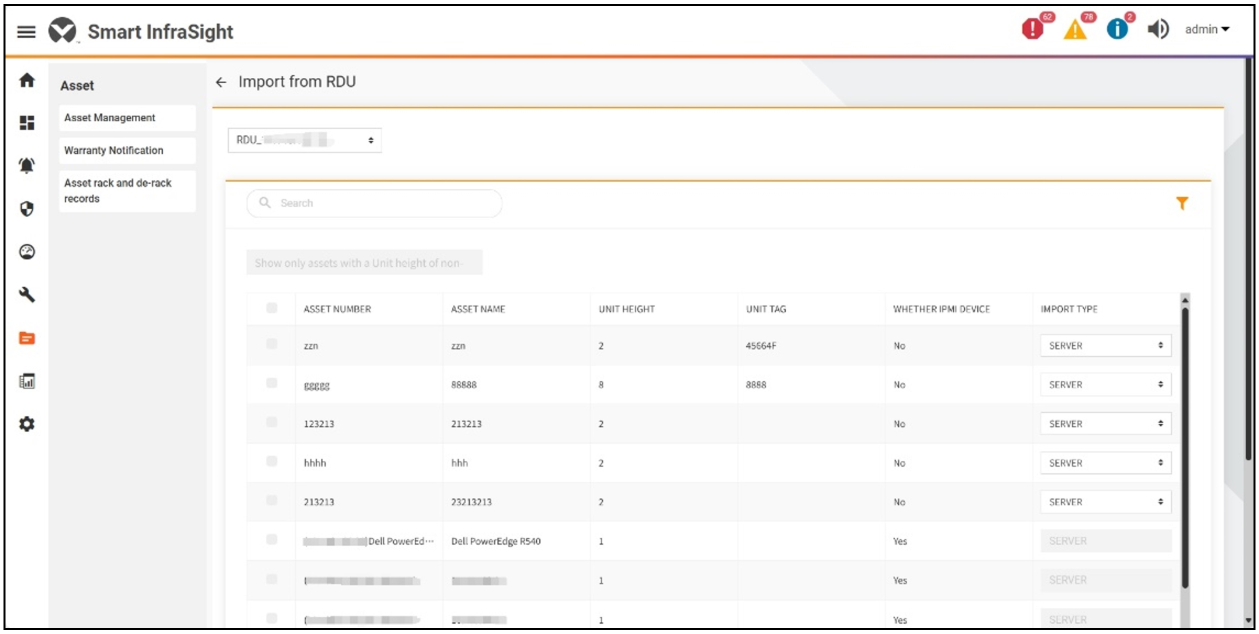


NOTE: After the cabinet is bound to the U-position Asset Manager, no new assets can be moved into the cabinet, and the position of the assets in the cabinet cannot be modified, the mounting or demounting of the assets, and the movement of the assets are all controlled by the U-position Asset Manager.

2. Ensure that the managed assets (servers, switches, etc.) have their U-position labels. There are two main ways to do this:

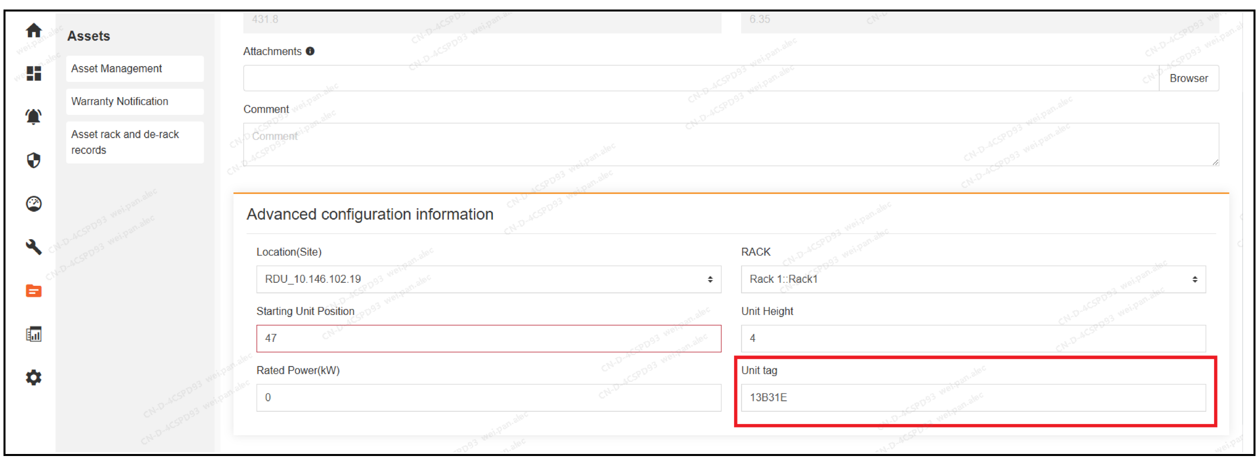
a) Use the Asset Import function in Smart Infrasight to import the managed assets from RDU501. Using RDU501 APP, you can easily scan and enter U-position tags (Unit tag in Smart Infrasight) into RDU501, and then you can import the managed assets in RDU501 together with their U-position tags into Smart Infrasight through Smart Infrasight's Asset Import function, as shown in Figure 4.58 on the next page , which can be used to import assets from RDU501 to Smart Infrasight.

Figure 4.58 Importing from RDU



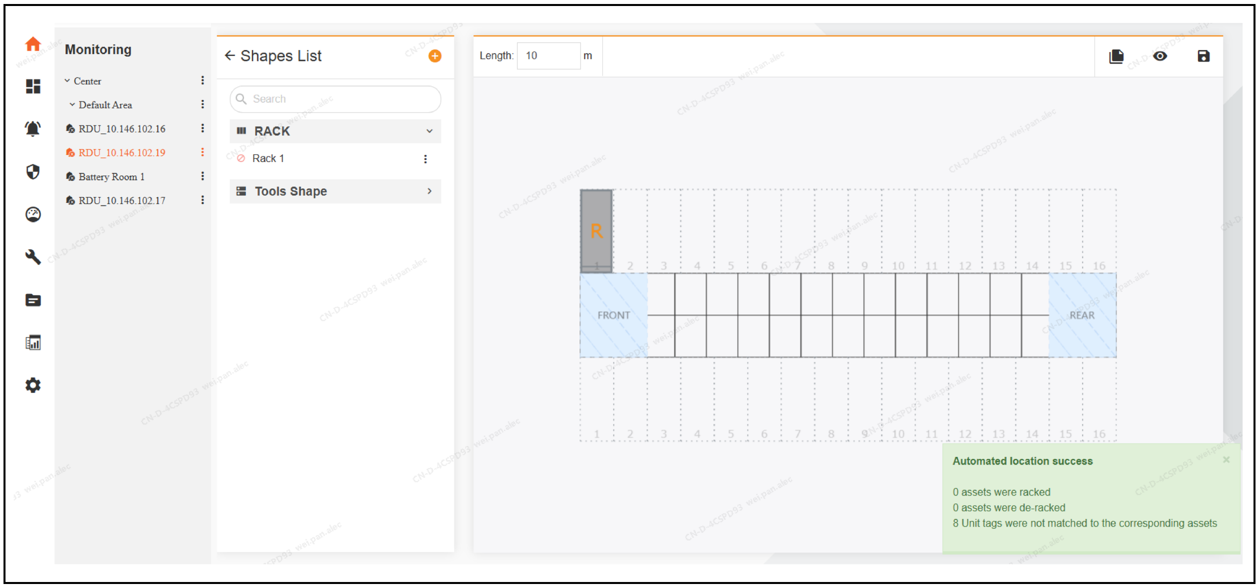
b) Enter the asset management function and manually enter the 6-digit hexadecimal U-position asset tag code in the edit page of each asset. As shown in below .

Entring the U-Position Asset Tag Code



After completing the configuration of U-position Asset Manager, Smart Infrasight can automatically synchronize the asset location information and move the asset from the original cabinet to the new cabinet when the asset location is moved at the data center field.

Asset Inventory: After manually entering the U-position asset tag code of an asset, you can enter the 3D configuration of the site and click on the **Asset Inventory** function to manually trigger a synchronization of the asset location.


Monitoring
Center
Default Area
RDU_10.146.102.16
RDU_10.146.102.19
Battery Room 1
RDU_10.146.102.17
Shapes List
Search
RACK
Rack 1
Tools Shape
Length: 10 m
FRONT
REAR
Automated location success
0 assets were racked
0 assets were de-racked
8 Unit tags were not matched to the corresponding assets

This page intentionally left blank

5 Power Train

5.1 Overview

The Power Train function allows users to configure a data center's power distribution diagram using a drag-and-drop interface for 3D models and automatic connection lines. Users can easily map the power flow from generators and mains through medium voltage distribution cabinets, UPS systems, and low-voltage distribution cabinets to smart solution cabinets, reflecting the actual power distribution in the computer room. Once configured, the diagram can display real-time operational status and signals for each power equipment connection. It also provides timely alerts for any issues detected in equipment or power lines.

5.2 Quick Start

5.2.1 Quick Start Steps

To quickly configure a power train diagram, perform the following steps:

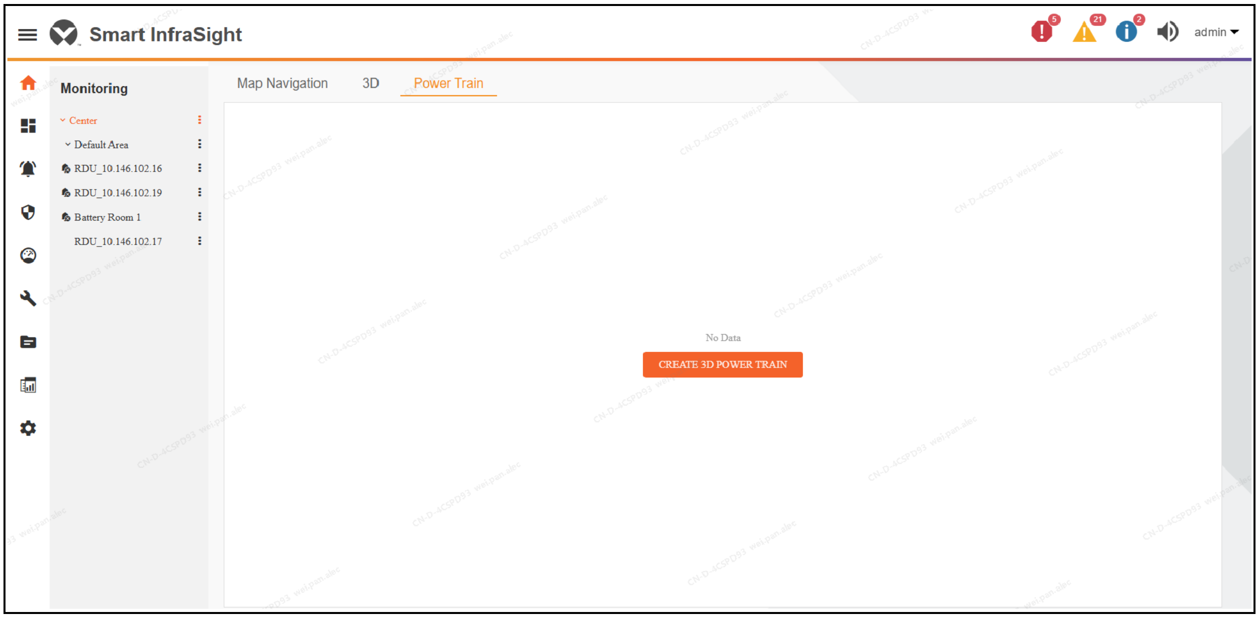
1. Go to Monitoring and navigate to the monitoring tree on center or location level item. Then select the **Power Train tab**.
2. Create a new Power Train.
3. Drag assets from the list on the left onto the canvas on the right. The corresponding asset models will appear on the canvas.
4. Adjust the camera angle using your mouse. Click and drag assets on the canvas to position them as desired.
5. Click the *Draw icon* to connect assets with lines, establishing their power relationships.
6. Click *Save* to finalize the Power Train configuration.

5.2.2 Example

Power Train Location:

Log in to the SI system, enter the location or center level item on the monitoring home page, and click the *Power Train* option in the tab column above the canvas area on the right to enter the creation process of the power train diagram as shown in **Figure 5.1** on the next page .

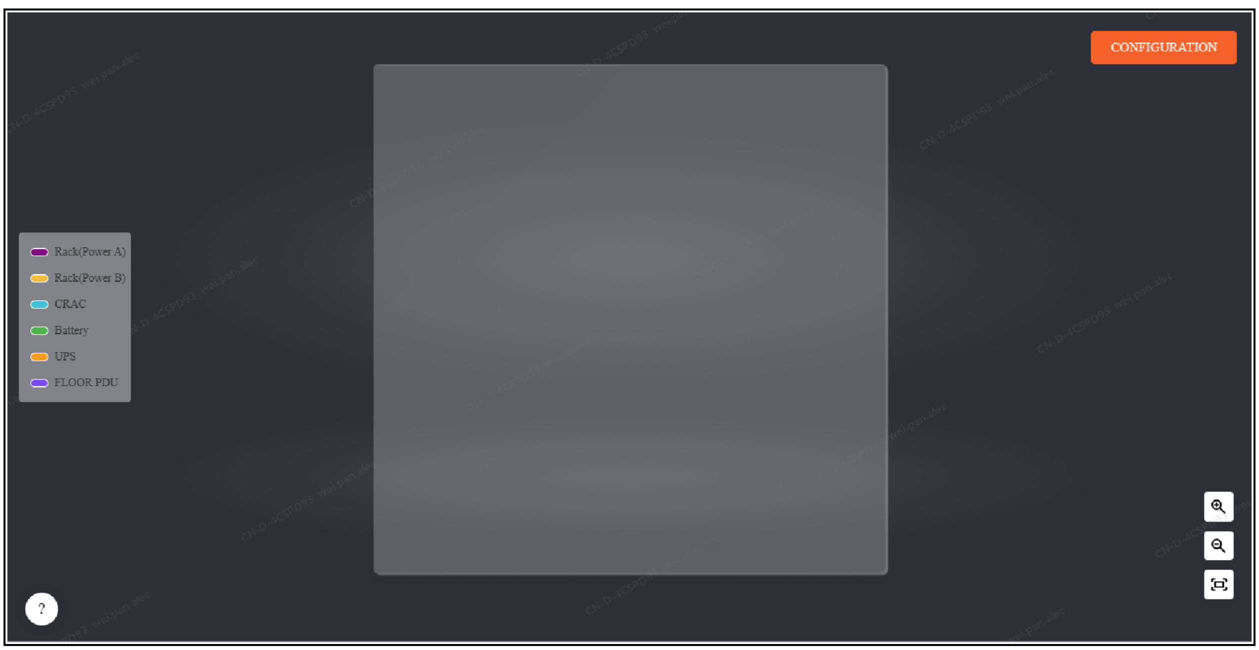
Figure 5.1 Power Train Diagram



Creating a Power Train Diagram:

Click *Create 3D Power Train* to enter the default scene area, as shown in **Figure 5.2** below .

Figure 5.2 Creating a Power Train Diagram



Configuring the Power Train Diagram:

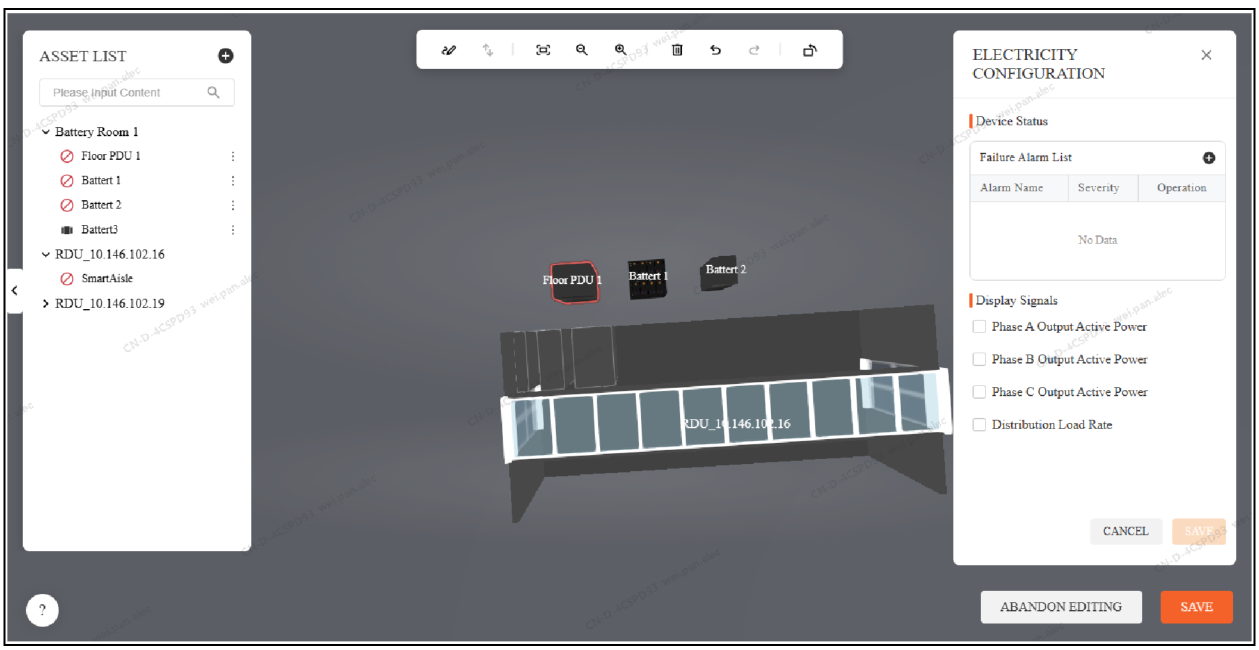
Figure 5.3 on the facing page the left asset list displays a list of assets that can be dragged to the right canvas, above the canvas is the toolbar, the question mark in the lower left corner is the operation guide, and in the lower right corner is the Save and Abandon Edit button.

Figure 5.3 Configuring the Power Train Diagram

Completing the Asset Layout for the Power Train Diagram:

Drag the asset on the left to the canvas on the right to complete the device layout, as shown in **Figure 5.4** below .

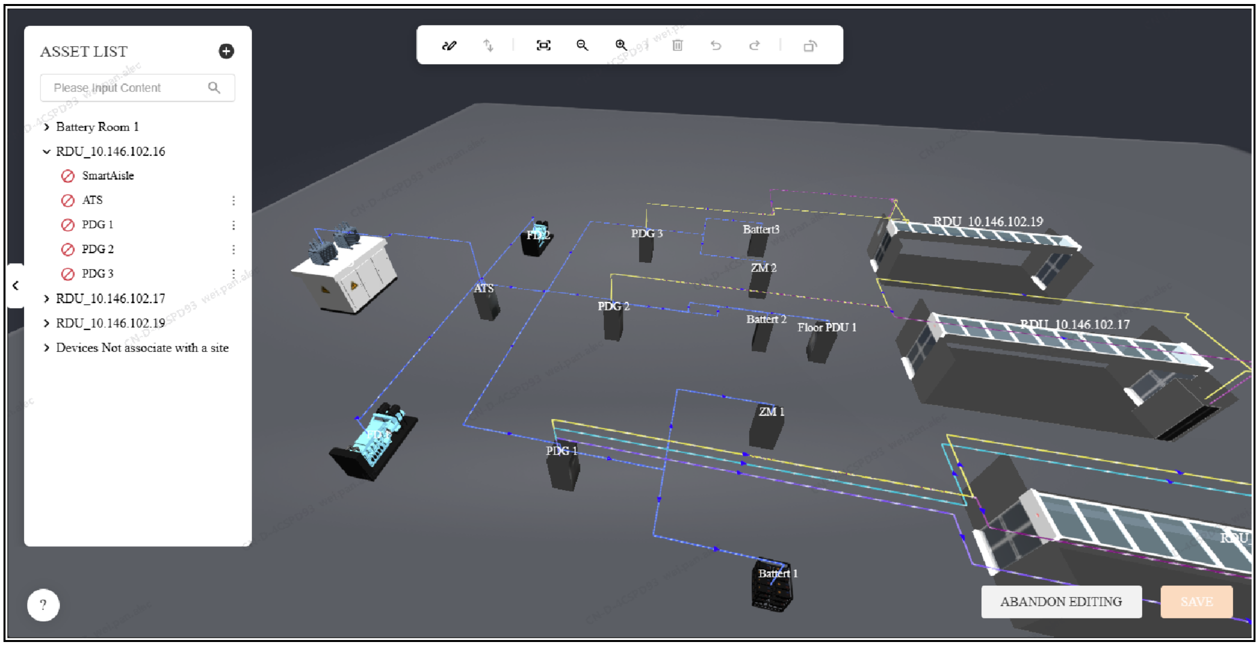
Figure 5.4 Completing the Asset Layout for the Power Train Diagram



Adding Line Relationships to the Power Train Diagram:

To draw a power line in the diagram, firstly you need to click the *Draw* button on the toolbar to enter the connection mode, after that clicking on the circuit upstream device and downstream device in sequence will automatically complete the connectivity, and finally click the *finish* button on the toolbar icon to complete the connection, as shown in **Figure 5.5** below .

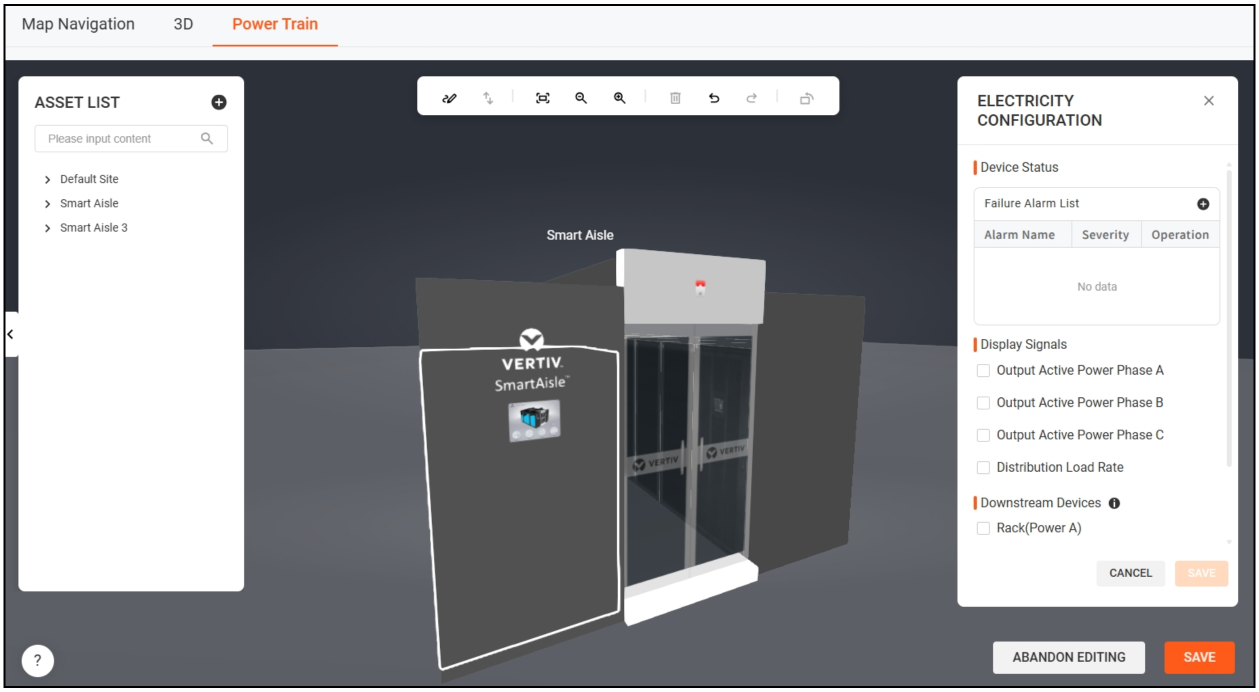
Figure 5.5 Adding Line Relationships to the Power Train Diagram:



Click *Save*, to finish configuring the power train diagram, then the diagram will enter the display mode.

Configure asset power configuration: After clicking on the asset, the power configuration card will pop up, and you can configure the alarms, power properties and downstream power devices, as shown in **Figure 5.6** on the facing page .

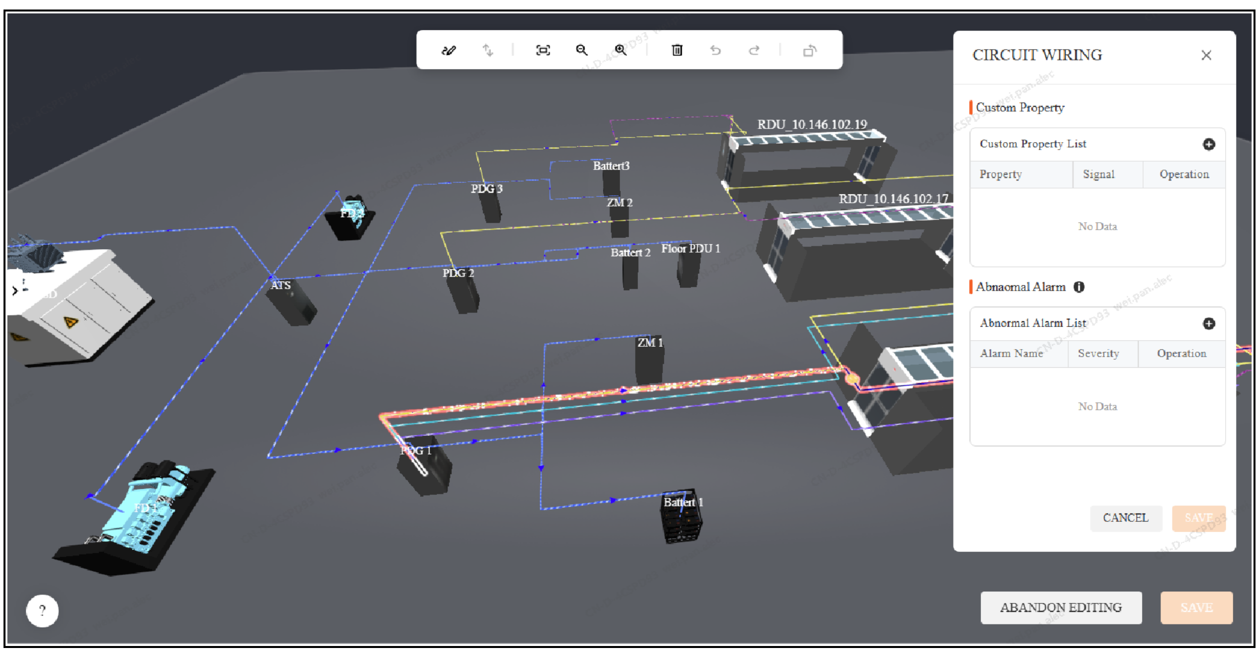
Figure 5.6 Configuring Asset Power Configuration



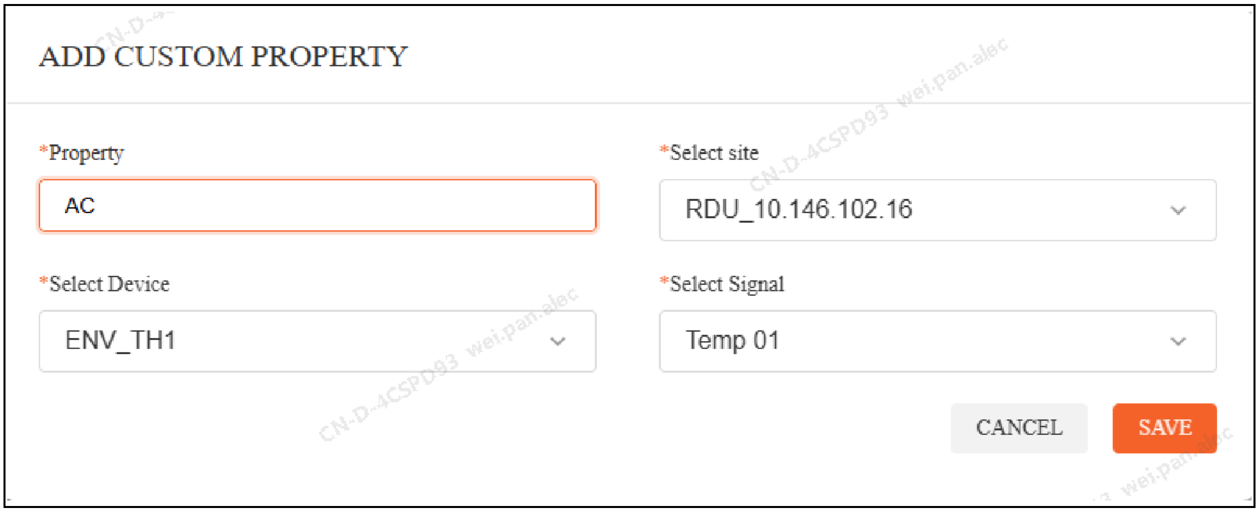
Configure Circuit Wiring Properties:

After clicking on the circuit connection, the circuit connection will get highlighted , and the circuit connection card will popup. As shown in **Figure 5.7** below .

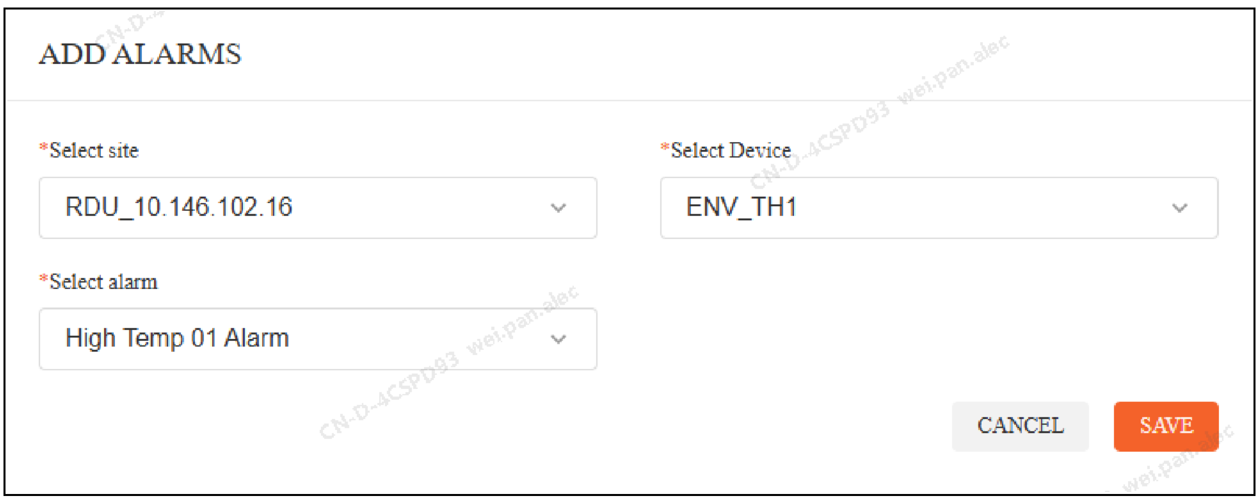
Figure 5.7 Configure Circuit Wiring Properties



Click *Add* in the list of custom attributes to bind power properties from devices with the circuit.



Click *Add* in the **Abnormal Alarm List** to bind alarms from power devices with the circuit so that the circuit will enter alarm status once the selected alarms are activating.



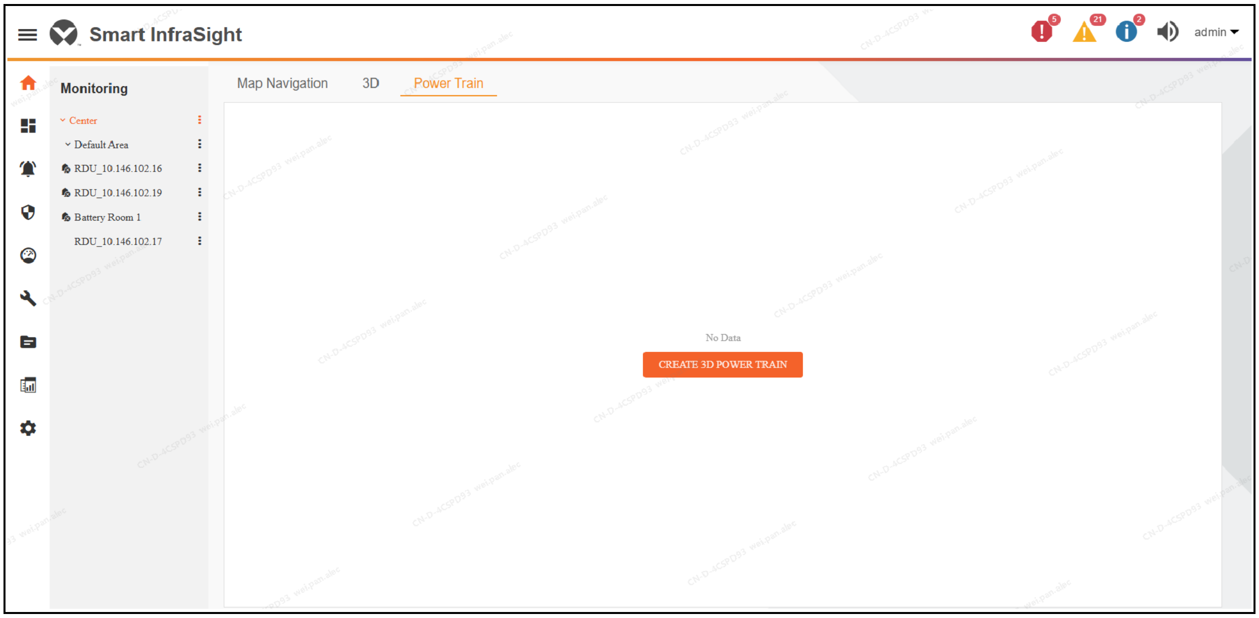
5.3 Detailed Functions

5.3.1 Creating a Power Train Diagram

After the user logs in to the SI system, he can click on the center or location level items in the monitoring tree list, the right side will display the tab list and canvas, at this time, click the Power Train in the tab, user can enter the Power Train Diagram creation interface.

Click Create 3D Power Train to enter the power train diagram configuration process, as shown in **Figure 5.8** on the facing page .

Figure 5.8 Creating a Power Distribution Link Diagram



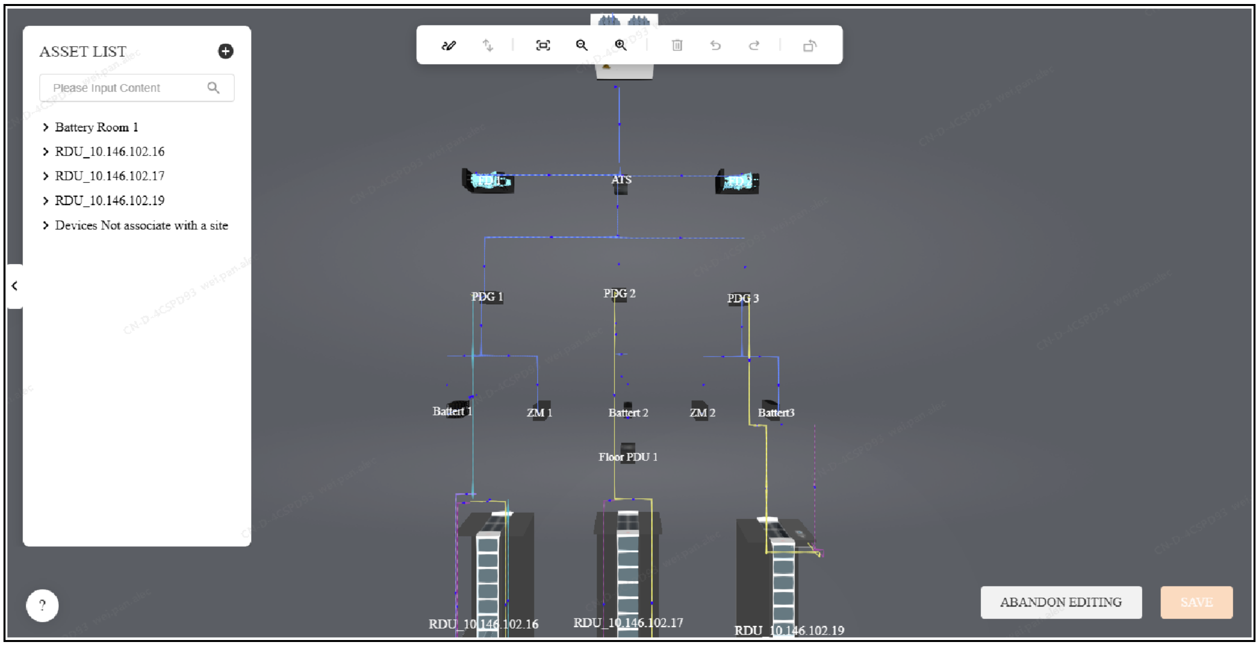
5.3.2 Asset List and Operations

Asset List

Sites are sorted alphabetically and collapsed by default. Within each site, assets are grouped by type and then listed alphabetically. A special category, "Devices not associated with a site," includes all unassigned assets. Expanding a site reveals all assets stand outside the Smart Solution infrastructure, including generators, lighting equipment, utility equipment, ATS, power distribution cabinets, floor UPS, floor batteries, air conditioners, and cabinets.

For Smart Solution infrastructure, the first asset entry under the site shows **Smart Aisle2** or **Smart Aisle3** or **SmartRow 2** (not editable and cannot be deleted) , if you drag them in the canvas, the 3D models of these sites will be displayed, as shown in **Figure 5.9** on the next page .

Figure 5.9 3D Configuration

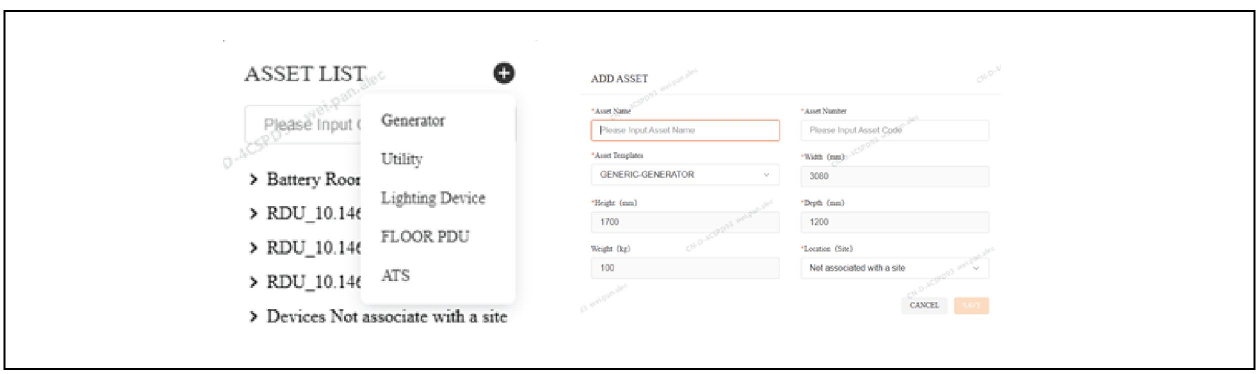


NOTE: If the asset collides with other assets on the canvas when dragged into the canvas, the dragging action fails.

1. Adding Asset

Click *add* in the list of assets. There are 5 types of assets that can be added, namely generators, Utility, lighting device, Floor PDU and ATS. Among them, Floor PDU assets can be bound to the associated power meter device. After saving the asset item you just added will appear in the asset list on the left, as shown in Figure 5.10 below .

Figure 5.10 Asset List



2. Editing the Asset

Click to the right of the asset name, the dotted button shows the action column and click *Edit* to edit the asset.

3. Deleting the Asset

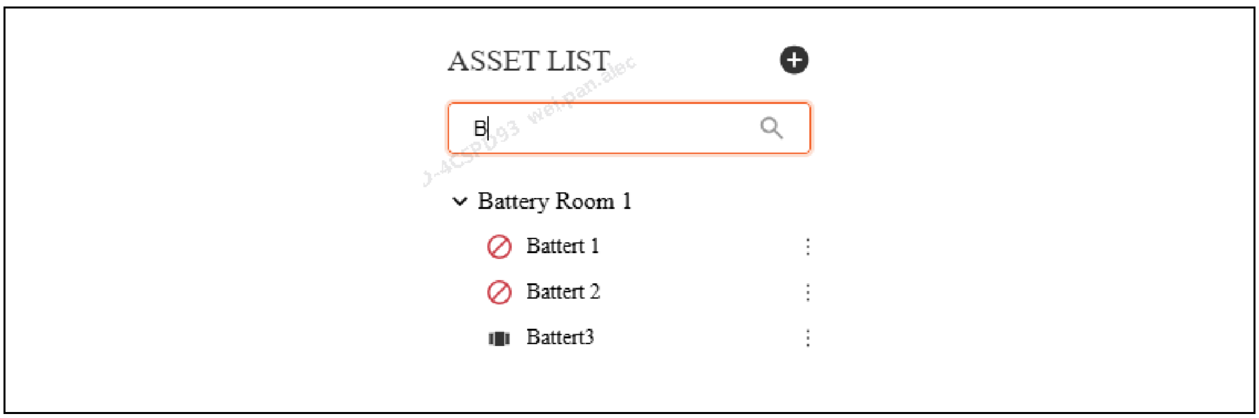
Click the *delete* button on the right side of the asset to delete the asset, as shown in Figure 5.11 on the facing page .

Figure 5.11 Deleting the Asset

4. Searching the Asset

Enter your search term in the asset list to see instant fuzzy search results based on asset names. The results will be displayed in the asset list, as shown in Figure 5.12 below .

Figure 5.12 Searching the Asset



NOTE: If an asset placed in the power train diagram is deleted, both the assets in the power train diagram and the asset connections (outgoing and incoming) will be deleted.

5.3.3 Canvas and Operations

1. Canvas

The canvas serves as the main workspace for placing power assets and creating circuit connections. By default, it displays a top-down view with the center of the canvas in focus. The default dimensions are 100m × 100m.

2. Navigation Controls

Zoom-In: Scroll the mouse wheel up; the view zooms in centered on the cursor.

Zoom-Out: Scroll the mouse wheel down; the view zooms out centered on the cursor.

Pan: Hold and drag the right mouse button to move the canvas.

Rotate View: Hold the left mouse button and drag to adjust the 3D perspective.

Select Asset or Line: Click the left mouse button. Use CTRL + click to multi-select objects.

3. Toolbar

Drawing lines

Steps to Draw a Circuit Line:

1. Click *Draw* button on the toolbar to enter drawing mode.
2. Click on an asset to set it as the starting point.
3. Move the mouse to the second asset and click to connect them automatically.
4. Once the connection is complete, click the Finish button on the toolbar to confirm and exit drawing mode.

Reverses the Direction of the Line

If you need to reverse the flow direction of the circuit line, click on the circuit line and then click on the Turn direction of the line button on the toolbar to change the direction.

Central Viewpoint

After multiple operations, the viewing angle may shift, making navigation difficult. Clicking Central Viewpoint button resets the bird's-eye view, displaying the entire canvas with all assets and circuit lines at an optimal scale.

Zoom-Out

Narrowing the angle of view.

Zoom-In

Expanding the angle of view.

Delete

When an unwanted asset exists on the canvas, click on the asset and then click on the Delete button to delete the asset from the canvas or press delete on the keyboard to delete it.

Undo

When you perform additional operations, you can use this function to roll back to the previous state step by step.

Redo

You can use this button to re-perform the previous undo steps.

Rotate

By default, this button is grayed out. It becomes highlighted when you select an asset and, when clicked, rotates the asset model 90 degrees counterclockwise.

5.3.4 Power Configuration

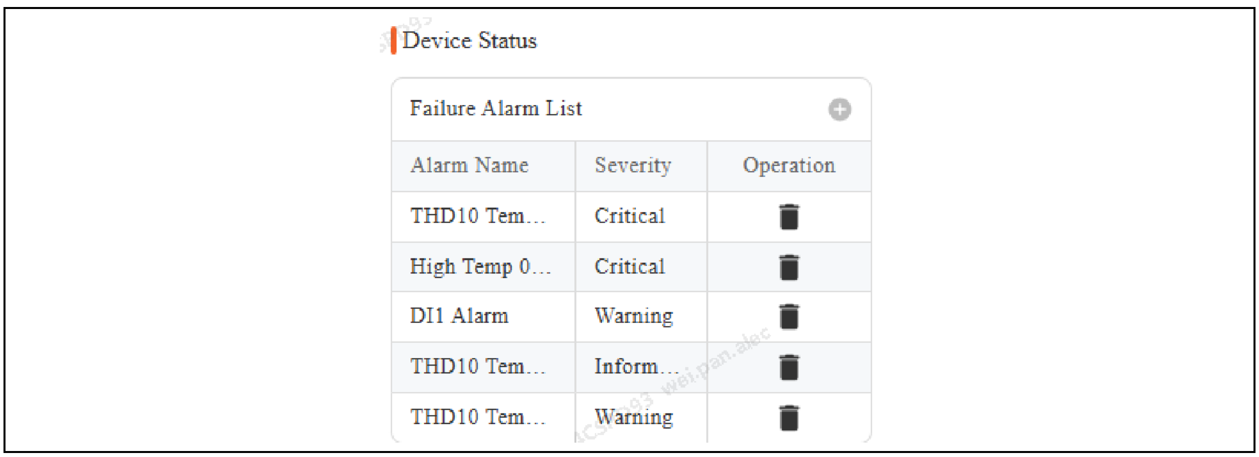
In Editing mode, by clicking the assets, you can open the power configuration of the asset. There are three main parts that need to be configured, namely device failure alarms, display signal, and downstream equipment. In the display mode, clicking the device and the status card of the device will show up, displaying content configured in the power configuration:

Device Failure Alarms

Click *Add* on the Fault Alarms list to select and add alarms that can indicate that the device is malfunctioning. You can select alarms from any monitored devices.

Click the drop-down box to select the alarms you want to view, click the save button to complete the operation, the fault alarm list allows you to add up to 5 alarms, as shown in **Figure 5.13** below .

Figure 5.13 Failure Alarm List

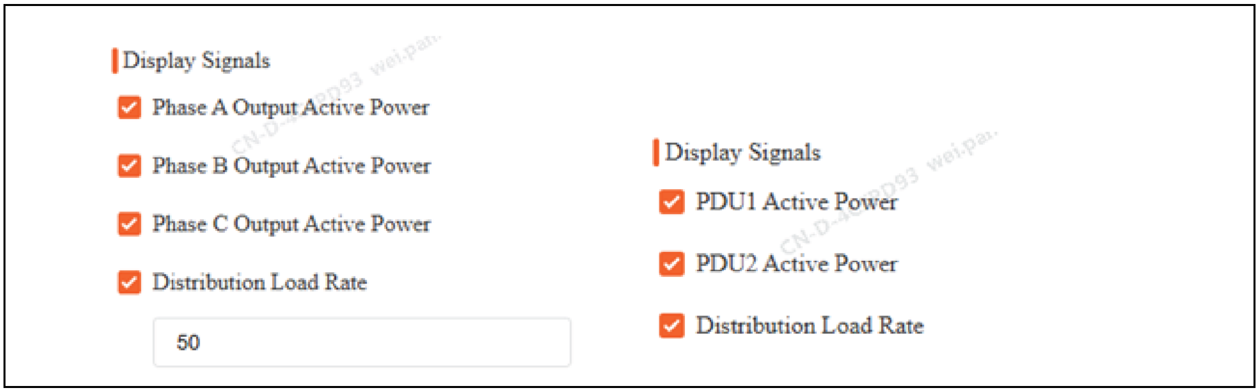


If you need to change the monitored alarm, you need to delete the alarm first and then add the alarm, click the *Delete* button on the right side of a single alarm to delete the alarm.

Display Signals

In the configuration of display signals, the distribution load rate is divided into two cases. The first case involves the Smart Aisle3 site cabinet, where the POD distribution load rate corresponding to the cabinet is used for calculation after checking the distribution load rate. The second case concerns normal rack cabinets, where the output power of up to two rack PDUs in the rack is used for signal display and calculation of the distribution load rate after checking the distribution load rate option. These two scenarios are illustrated in the **Figure 5.14** on the next page .

Figure 5.14 Display Signals Configuration



When the display signal is configured, enter the display mode, and you will find that the card of the device will display the percentage indicator of the load factor, as follows:

The load factor is calculated as follows:

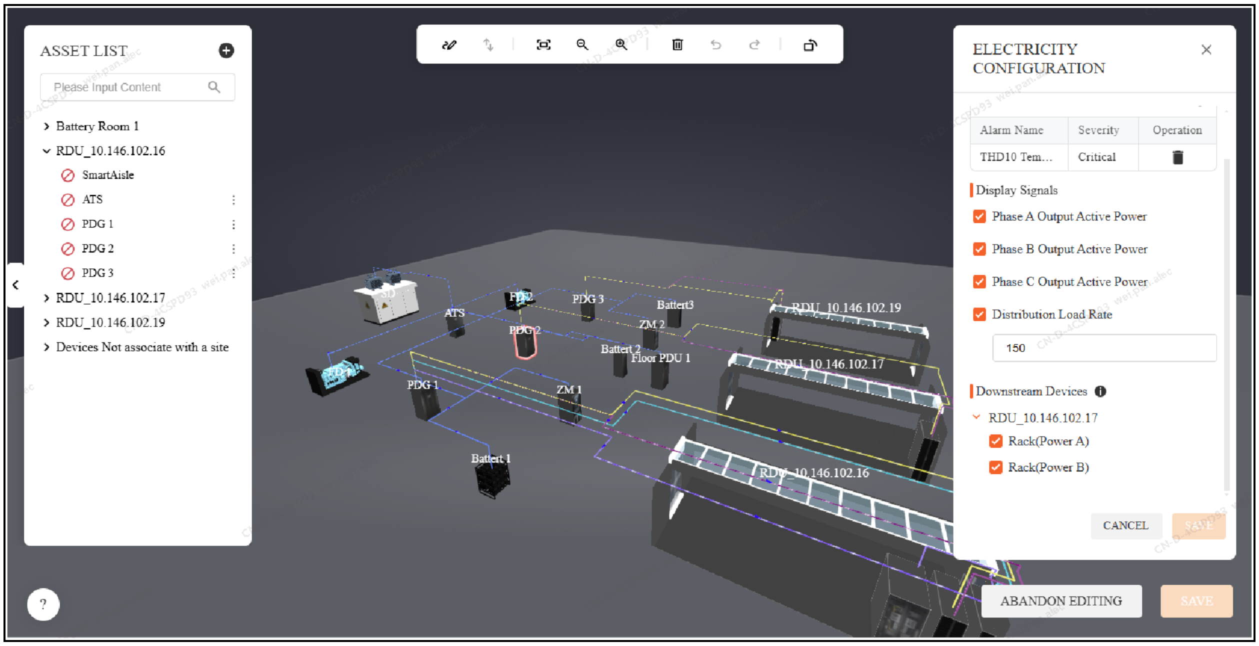
1. Distribution Utilization or Remaining Capacity Percentage Indicator: If Distribution Load Factor or Remaining Capacity is selected, a percentage indicator (0-100%) is displayed. Percentages for different assets are calculated as follows:
2. Cabinet at Smart Aisle3 site: (Active power of POD_Power device Source A + Source B) / Cabinet's rated power
3. Cabinets at other sites: (Active power of PDU1 + PDU2) / Cabinet's rated power
4. UPS: (Output active power of phase A + B + C) / UPS rated power
5. Intelligent power distribution cabinet (SPM): Total active power / Rated power
6. Non-intelligent distribution cabinet (with associated power meter): (Active power of phase A + B + C from associated power meter) / Cabinet's rated power

NOTE: 1. Only checked signals in the power configuration are included in calculations.

NOTE: 2. If the signal cannot be obtained or the calculation is incorrect, a dash (--) is displayed when calculating the load rate.

Downstream Equipment

The downstream equipment feature primarily helps quickly identify affected devices when intermediate power equipment fails. It provides a clear, intuitive understanding of power dependencies between data center components. You can modify the downstream devices of the current device and the circuit line between the upstream device and the downstream device will be established or cancel accordingly.

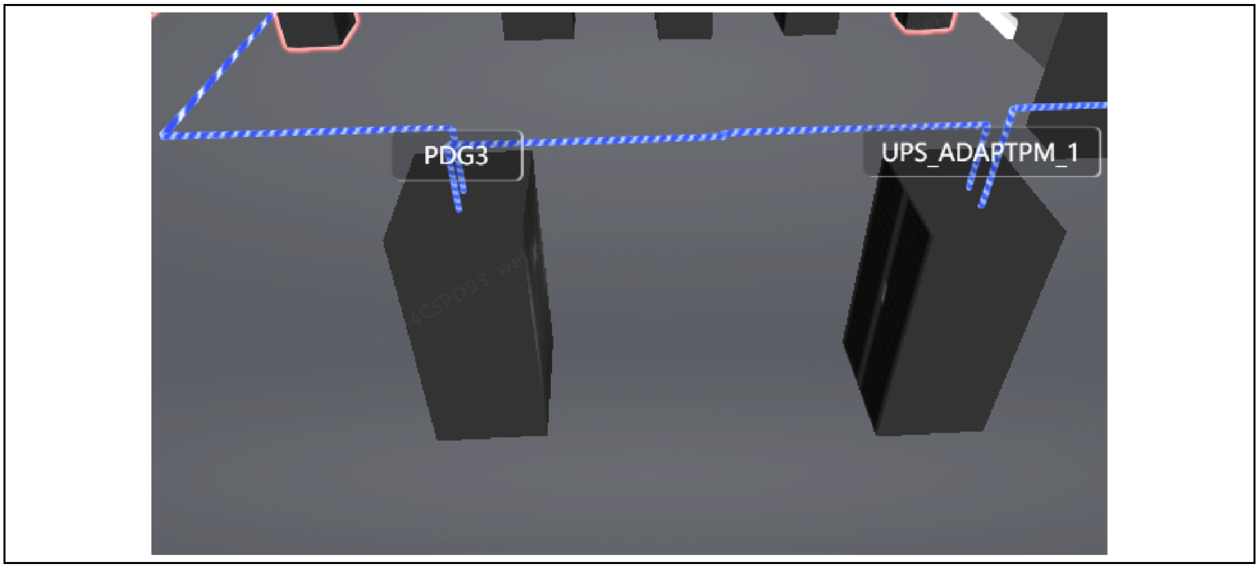


5.3.5 Circuit Configuration

The circuit lines in the power train diagram indicate the power flow from the upstream devices to the downstream devices. The circuit configuration makes sure the circuit line dynamically displays the flow direction and the alarm status of the circuit.

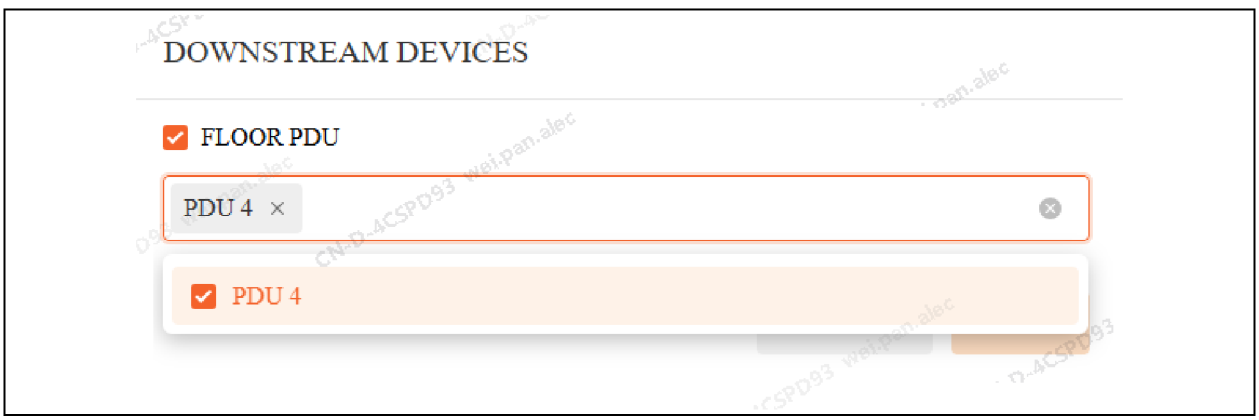
Creating a Circuit Connection

To create a circuit connection between assets outside the Smart Solutions, click the Draw button on the toolbar to enter the drawing mode. Click the upstream device, the downstream device, and finally the Finish button on the toolbar, then the circuit connection is automatically completed.

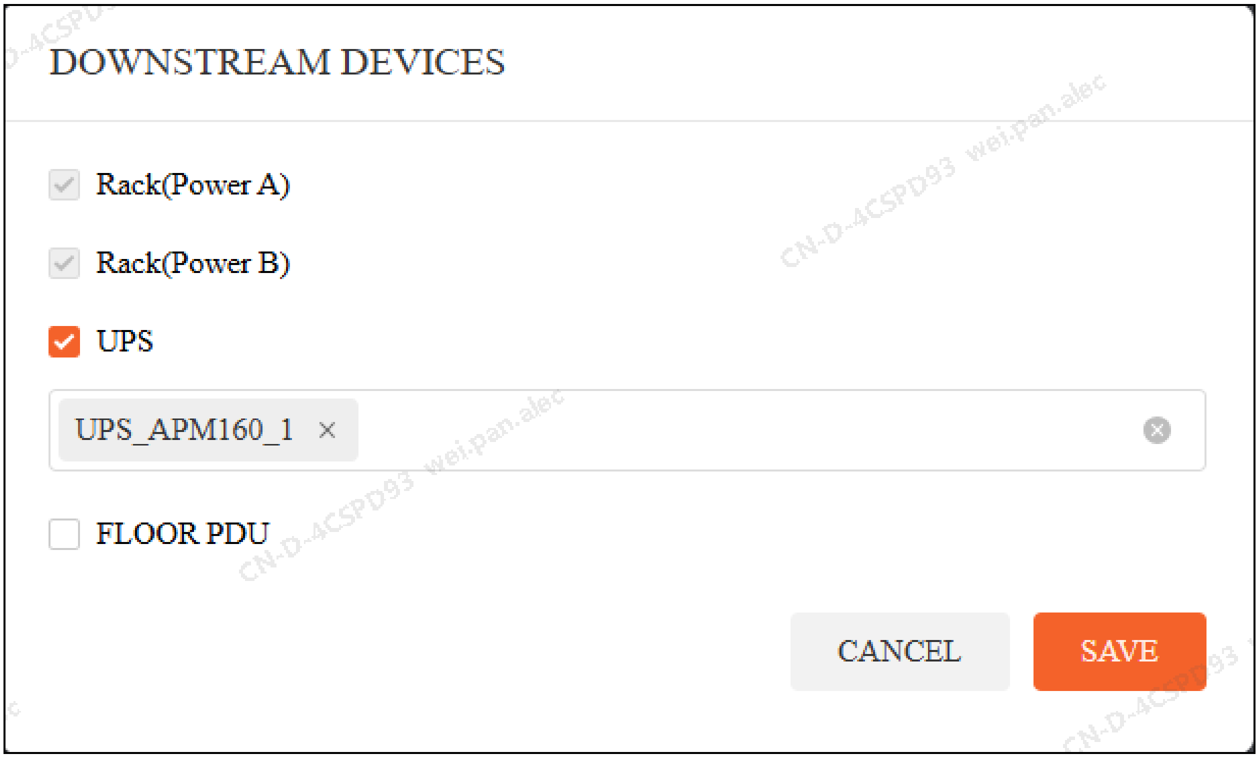


To create a circuit connection between assets with the Smart Solution infrastructure like Smart Aisle or Smart Row, you still use the Draw button on the toolbar. But this time, when you connect the Smart Solution as a downstream device, a Downstream Devices window will appear. You can select the appropriate downstream device type from the list. After saving, the system will automatically create a circuit connection between the asset and the Smart Solution.

1. If the upstream asset of the circuit connection is a floor UPS, the **Downstream Devices** pop-up window displays a multi-check box of the Floor PDU device), and you can select the distribution cabinet in the Smart Solution and the PMC cabinet in Smart Row as the downstream equipment of the floor UPS.



2. If the upstream asset of the circuit connection is a floor battery, a device multi-check box will be displayed, and you can select the UPS device in the Smart Solution as the downstream equipment of the floor battery.



3. If the upstream asset of the circuit connection is a power distribution cabinet, the following is displayed in the **Downstream Devices** pop-up window:

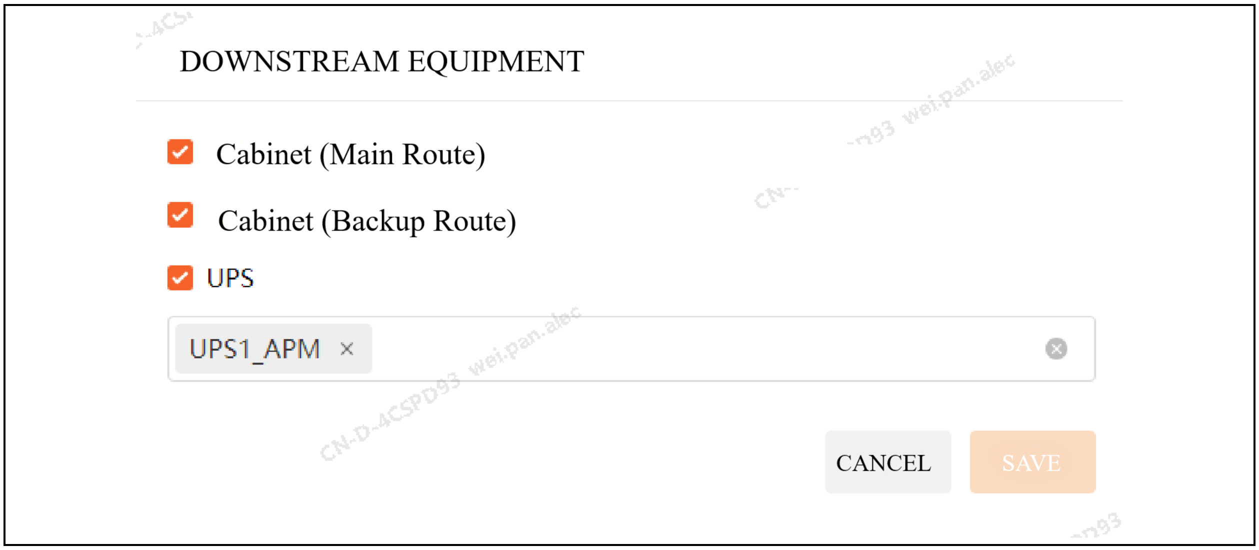
Rack Power A: Once checked and saved, circuit connections from the power distribution cabinet to each rack in the Smart Solution will be established. The power distribution cabinet will be seen as power source A of all racks in the Smart Solution.

Rack Power B: Similarly, circuit connections from the power distribution cabinet to each rack in the Smart Solution will be established and the power distribution cabinet will be seen as power source B of all racks in the Smart Solution.

CRAC: Once checked and saved, circuit connections from the power distribution cabinet to each CRAC unit in the Smart Solution will be established . The power distribution cabinet will be seen as the power supplier of all CRAC in the Smart Solution.

UPS: Once checked, you need to select the specific UPS devices in the Smart Solution that are downstream from the power distribution cabinet.

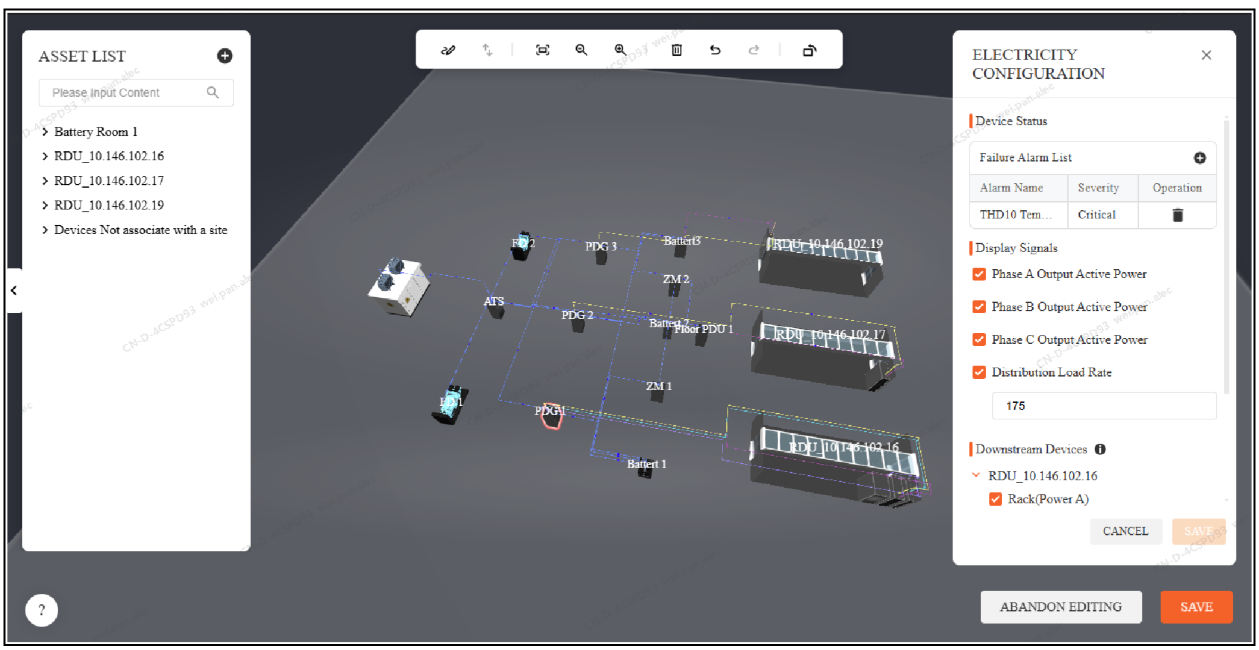
Power Distribution Unit (PDU): Once checked, you need to select the specific PDU devices within the Smart Solution that are downstream from the external power distribution cabinet.



Editing the Circuit Connections between Assets and Smart Solution

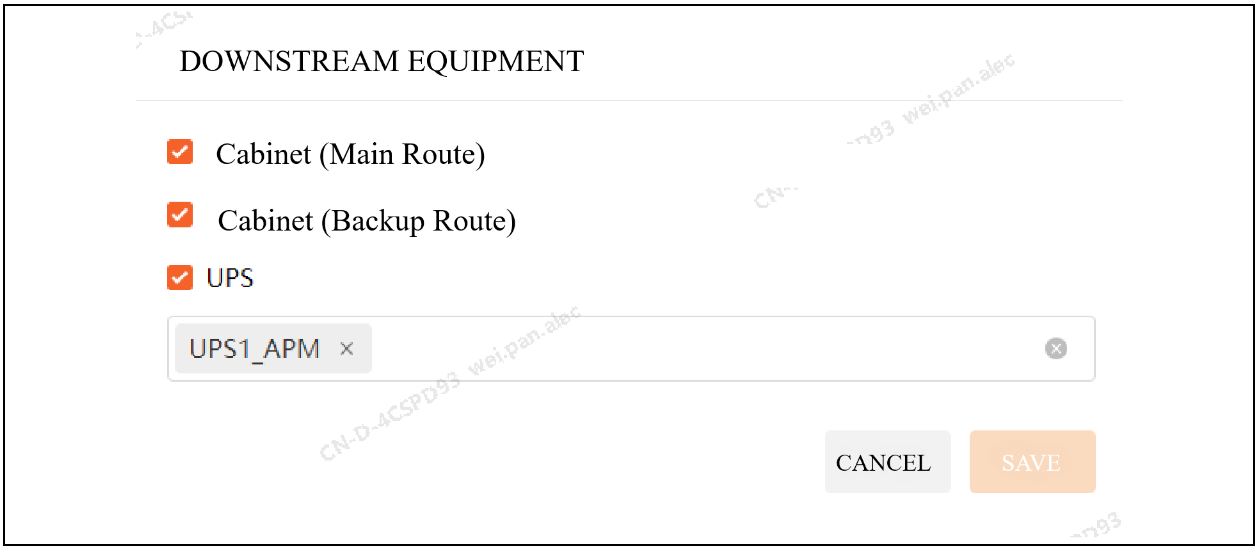
When editing the power train diagram for Smart Solution with assets independent from the Smart Solution, click on the independent assets to show its power configuration panel. The panel will display the configuration of downstream devices.

To remove a circuit line to a downstream device in Smart Solution, you can either uncheck the device in the panel or select the circuit line and press the Delete key on your keyboard.

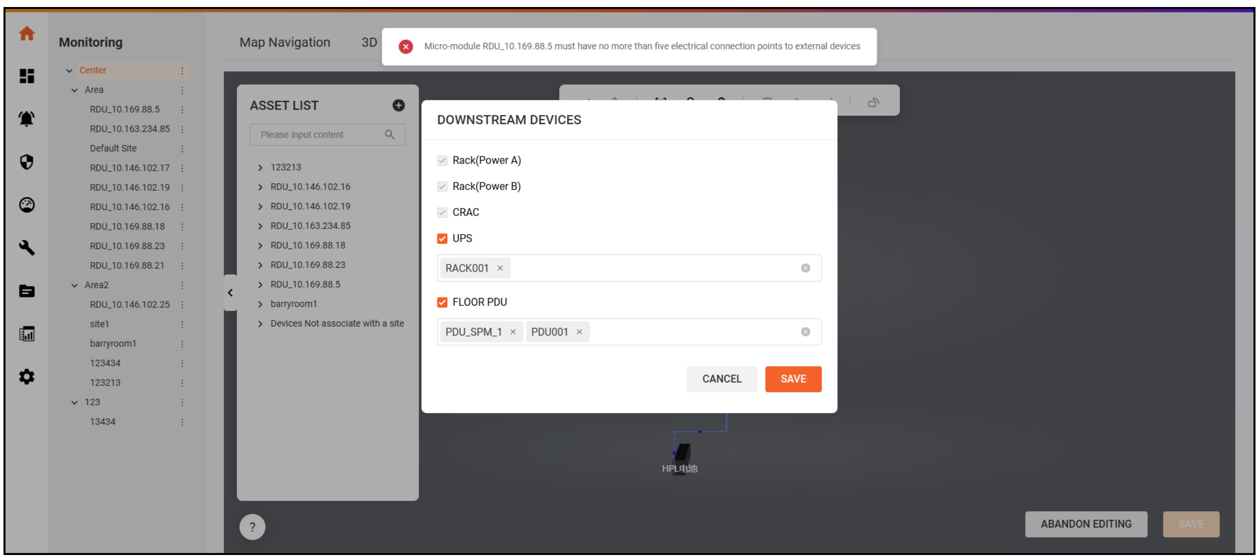


Connection Restriction

In this specific Smart Solution, only one device can serve as the upstream device for cabinets (Source A or B) or air conditioning.



At most 5 external devices can establish circuit connections to a Smart Solution.



Deleting the Connection

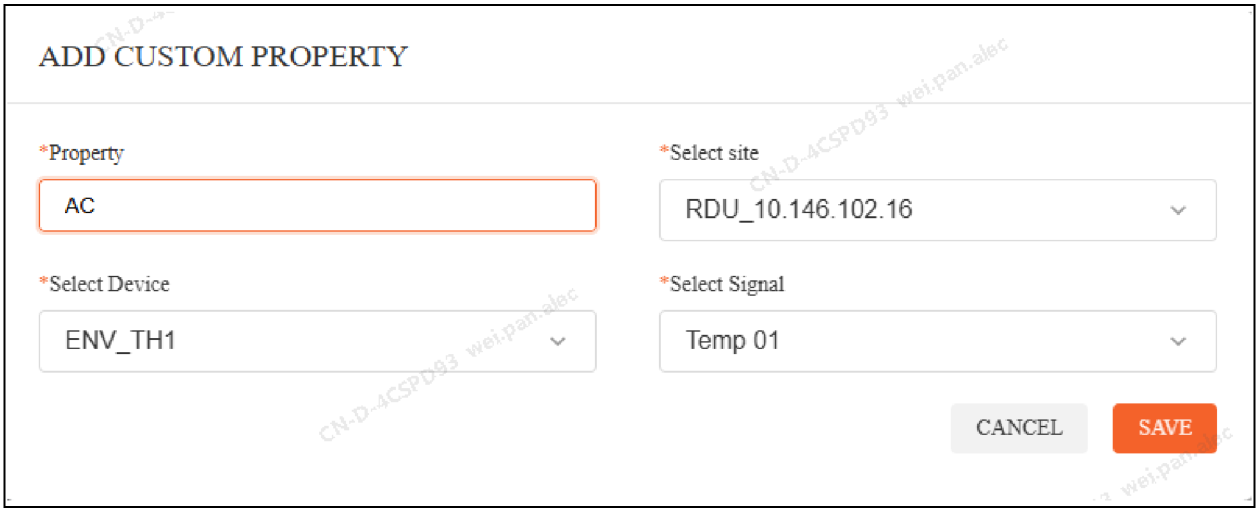
The circuit connection in the Smart Solution cannot be deleted directly. You need to open the power configuration panel of the upstream device and uncheck the downstream devices to remove the circuit connection. The connection between the assets and the Smart Solution can be deleted after selection.

Circuit Line Configuration

In editing mode, double-click the line in the canvas to start configuring the content of the line, and the list of custom attributes is empty by default, and you can add up to 5 custom attributes.

Click *Add* on the list of custom attributes, you can add the custom attributes of the circuit, fill in the required information and click *Save* to complete this operation as shown in **Figure 5.15** on the next page .

Figure 5.15 Adding the Custom Properties



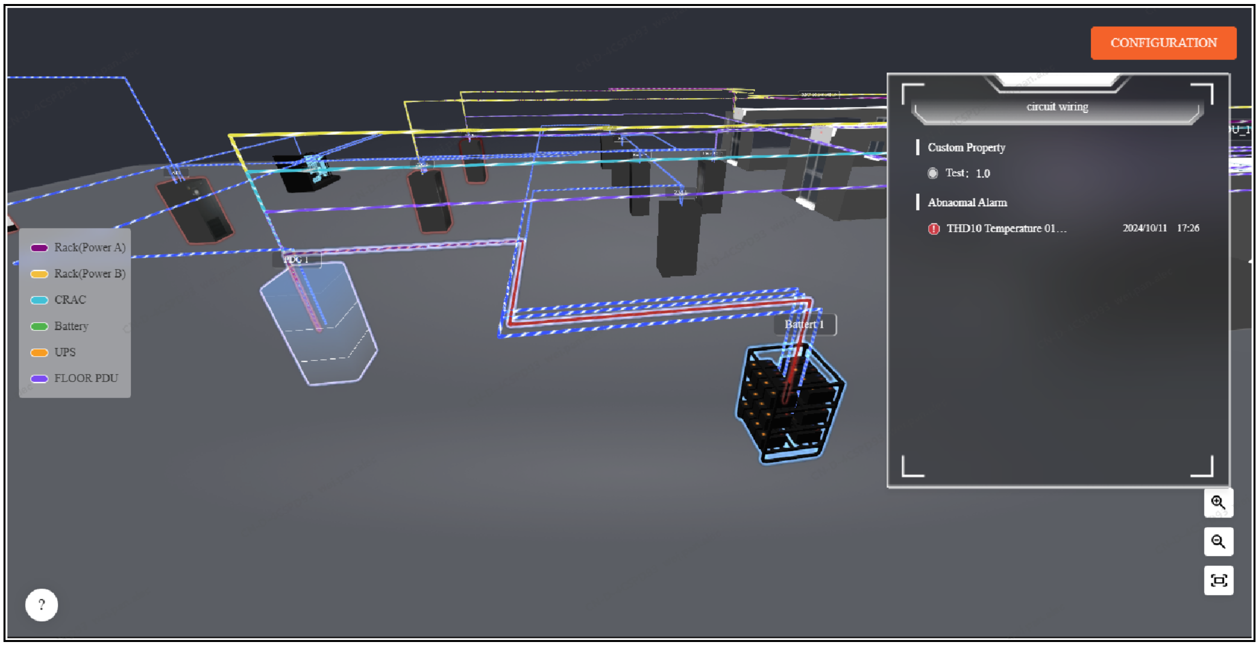
Abnormal Alarm List: The default alarm list is empty, and you can add up to 5 alarms. When no abnormal alarm is generated, the color of the line will not change, and when an abnormal alarm is generated, the color of the line will continue to flash the prompt, click **Add** button to add abnormal alarm that can imply the connection is abnormal, click *Save* to add abnormal alarm to be monitored in Exception.

In the alarm list, the following **Figure 5.16** below shows the alarms.

Figure 5.16 Adding Alarms

After the configuration is completed and exits the editing mode, we can see the configuration information by clicking on the circuit connection just configured, as shown in **Figure 5.17** on the facing page .

Figure 5.17 Viewing the Completed Configuration



This page intentionally left blank

6 3D Visualization

6.1 Overview

This chapter will guide you through the 3D visualization capabilities of Smart Infrasight. The system supports 3D views of Smart Aisle2, Smart Aisle3, Smart Row2, Battery Room, and CREMS Site. Additionally, it can display key performance properties of infrastructure devices such as UPS, CRAC, PDU, and racks, as well as IT devices using the IPMI protocol.

6.1.1 Functional Modules

3D visualization has the following functional modules.

NOTE: If the client's hardware falls below the recommended specifications for using the power train diagram function, loading more than 20 Smart Solution in 3D simultaneously may be slow (taking 15 seconds or longer). For optimal performance, ensure the client computer has sufficient memory before opening the 3D page.

- Smart Aisle2 Site 3D Visualization
- Smart Aisle3 Site 3D Visualization
- Smart Row2 Site 3D Visualization
- CREMS Site 3D Visualization
- Location 3D Visualization
- Battery Room Site 3D Visualization
- Power Train Diagram 3D Visualization

6.2 Detailed Features

6.2.1 Smart Aisle2 Site 3D Visualization

View 3D scenes of Smart Aisle2 sites, including space capacity, power capacity, temperature labels, and heat maps. To access the 3D model, click on a Smart Aisle2 site in the Monitoring Tree, then select the desired view (3D, space capacity, power capacity, temperature label, or heat map) from the 3D tab on the right.

3D Model

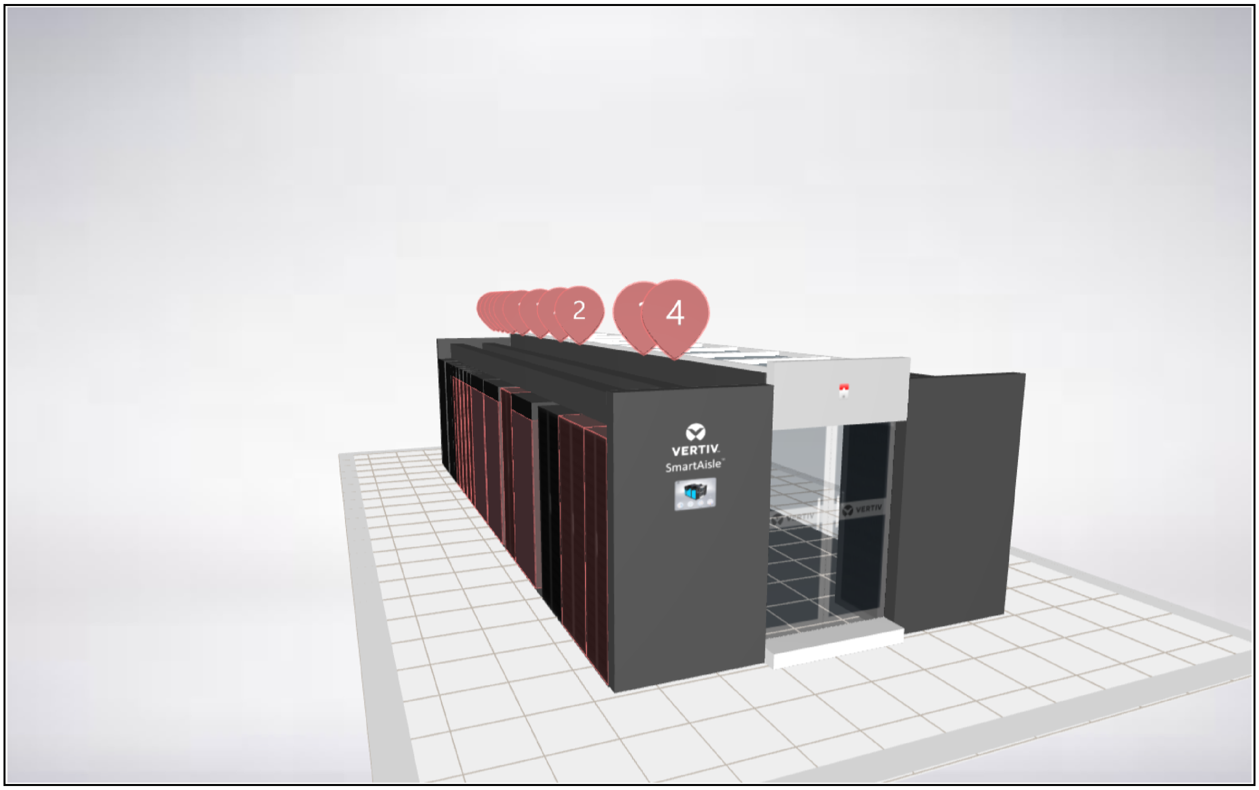
The Smart Aisle2 3D model shows devices inside the Smart Aisle and activating alarms from different devices.

Users can interact with the 3D view as follows:

- Left mouse button: Rotate the view
- Right mouse button: Pan the view
- Scroll wheel: Zoom in and out
- Hold scroll wheel: Reset to default view

The default view is illustrated in Figure 6.1 on the next page.

Figure 6.1 The Default 3D View of Smart Aisle2



You can rotate the 3D view to see different perspective of the Smart Aisle 3D model. As shown in the Figure 6.2 on the facing page .

Figure 6.2 Rotated 3D View of the Smart Aisle2 Site

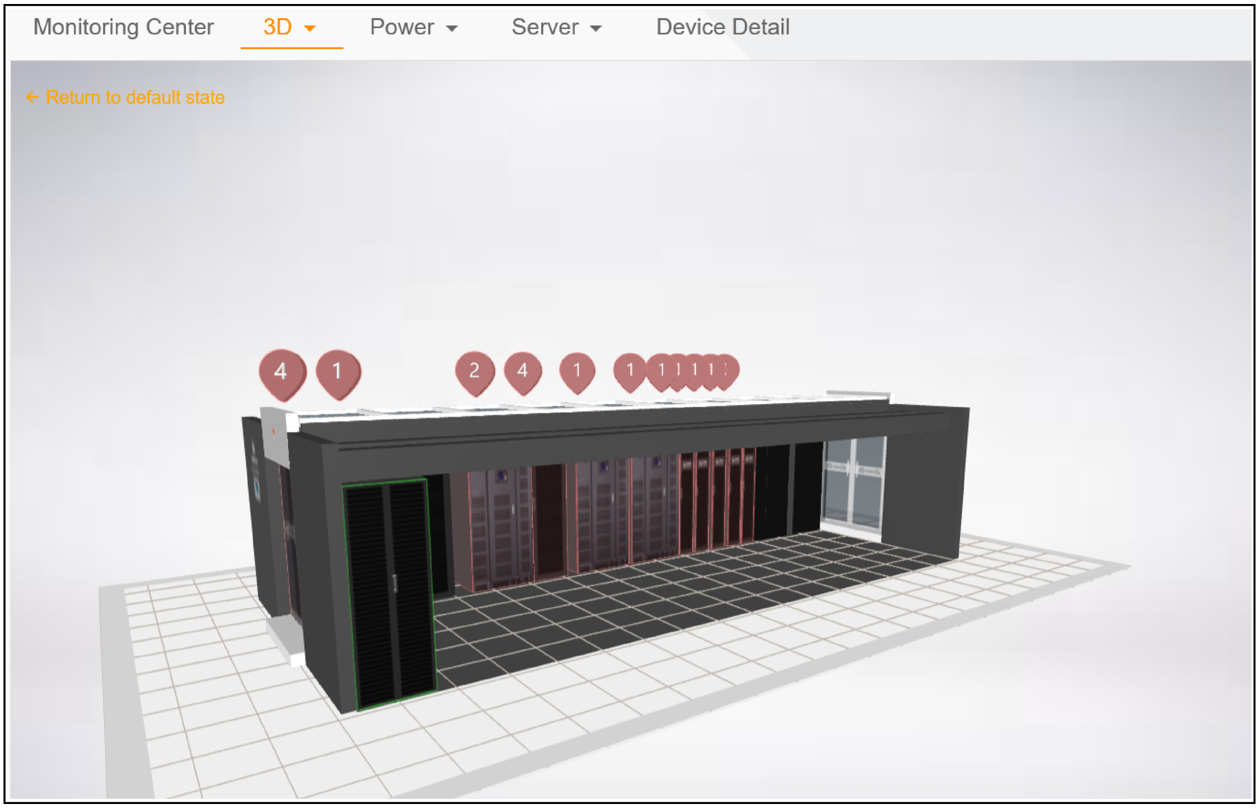


Figure 6.3 Top View of Smart Aisle2

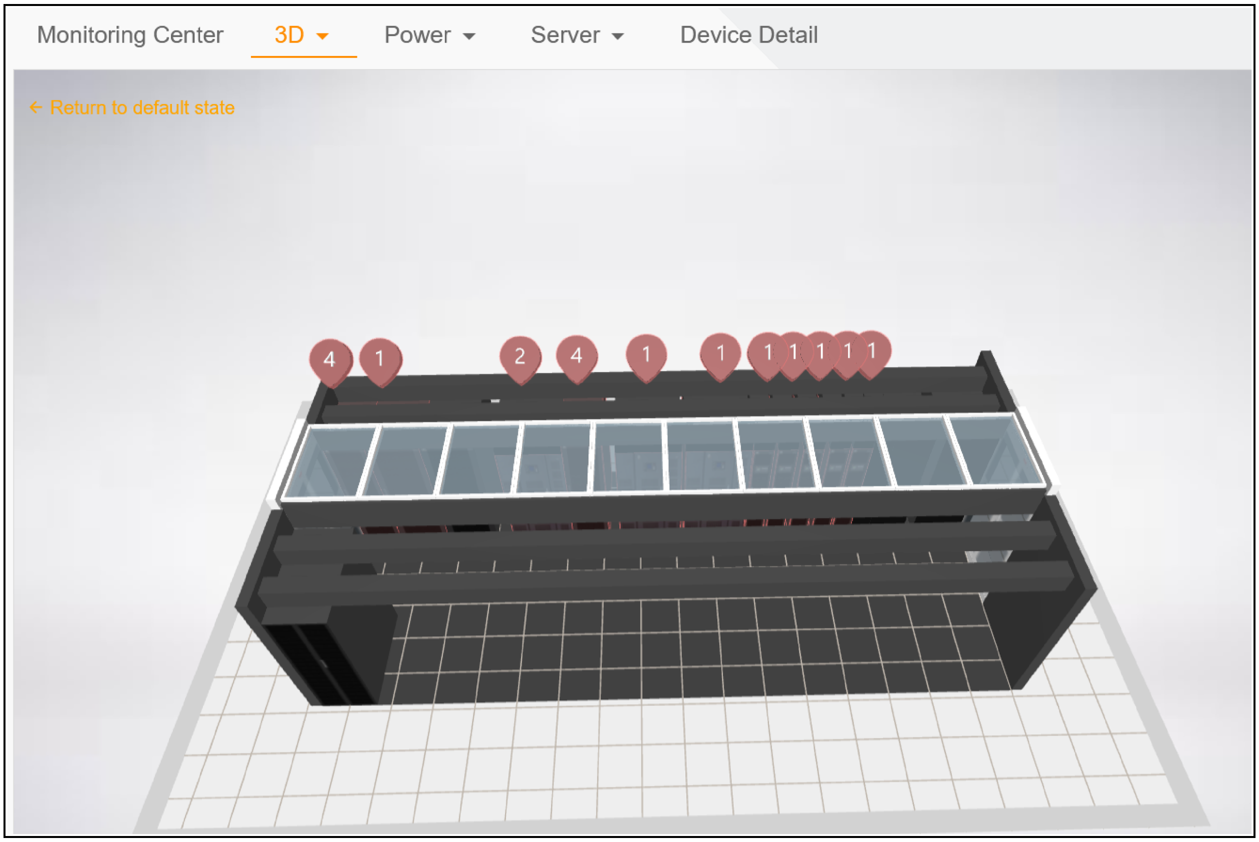


Figure 6.4 Zoom-in View of Smart Aisle2

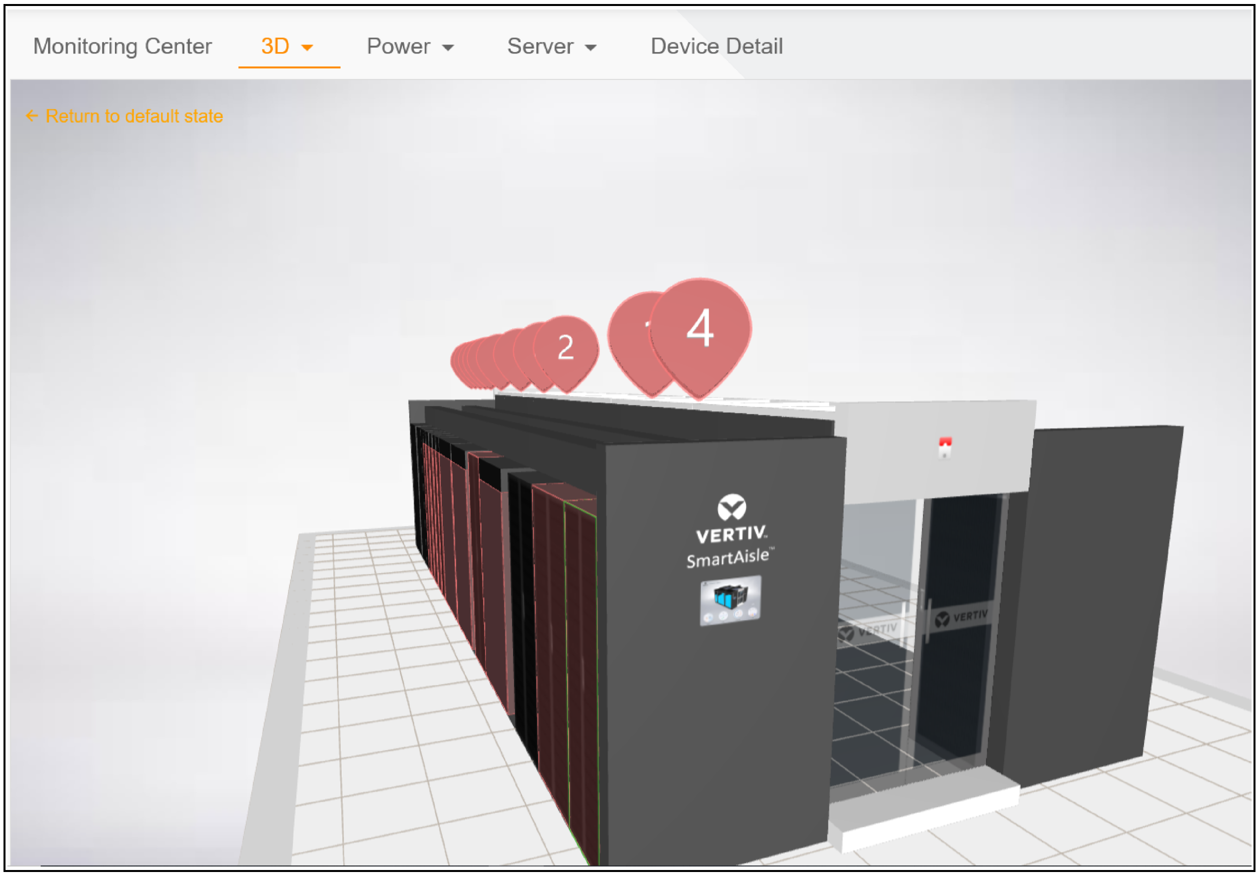
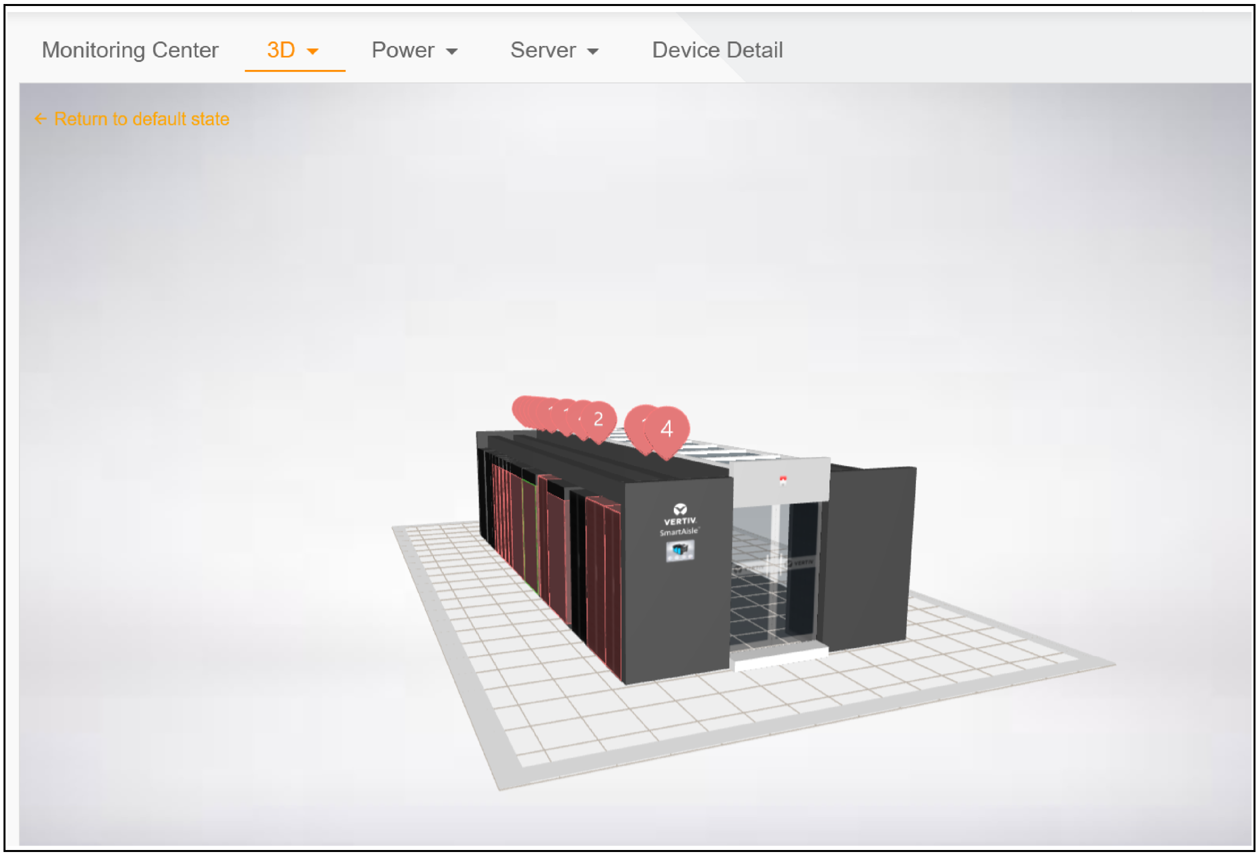


Figure 6.5 Zoom-out View of Smart Aisle2



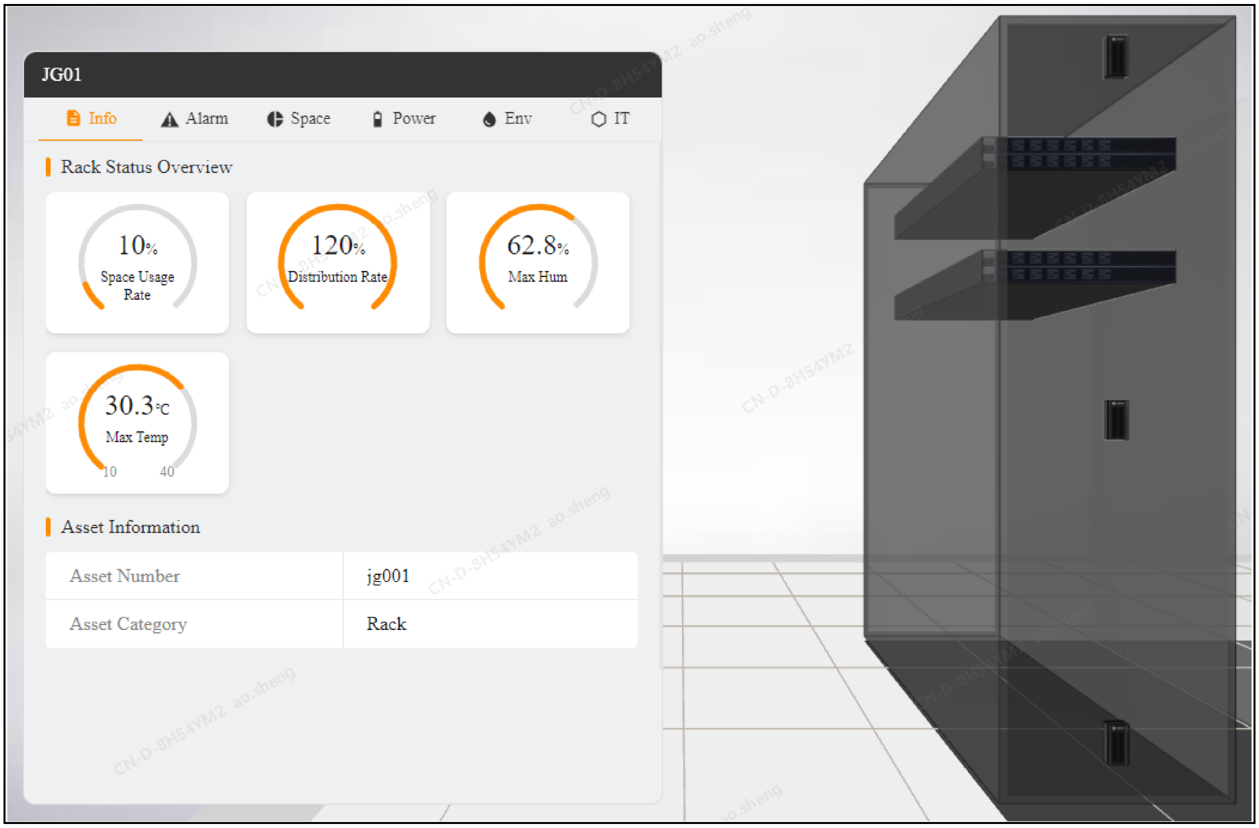
At this time, you can click on a device (for example a cabinet) to enter the view of row angle.

The Smart Aisle2 row angle viewing is shown in the **Figure 6.6** below .

Figure 6.6 3D Row Angle Viewing of Smart Aisle2

In the row angle viewing, click on any cabinet to enter the single-cabinet view. This is shown in the Figure 6.7 below . On the left side, you'll find essential information about the cabinet, including its status, alarms, space utilization, power distribution, environmental conditions, and IT inventory. The overview displays basic cabinet details and asset information, along with a 3D model showing all installed equipment. Switching to the alarm view highlights devices with active alerts in the 3D model. Selecting the IT category displays servers, switches, and other IT equipment.

Figure 6.7 3D Single Cabinet View of Smart Aisle2 Site



Click Alarm, Space, Power, Environment, and IT to switch to the corresponding card and display the corresponding content, as shown from Figure 6.8 below to Figure 6.13 on page 117 .

Figure 6.8 Alarm Window

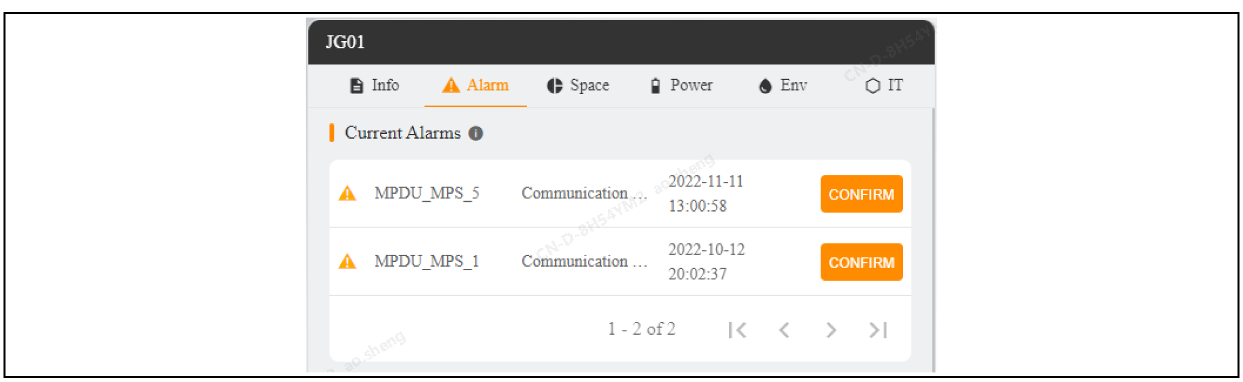


Figure 6.9 Alarm Trends

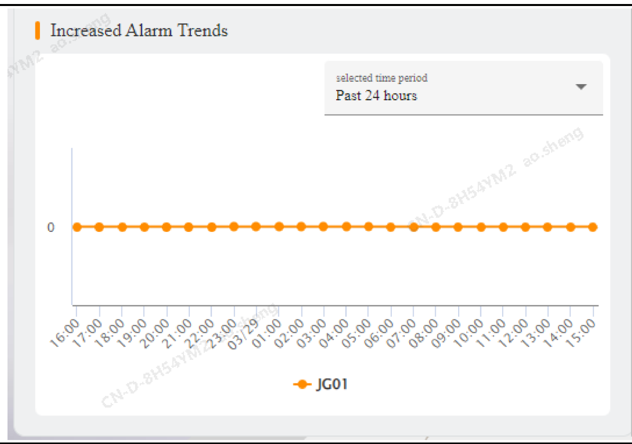


Figure 6.10 Space Card

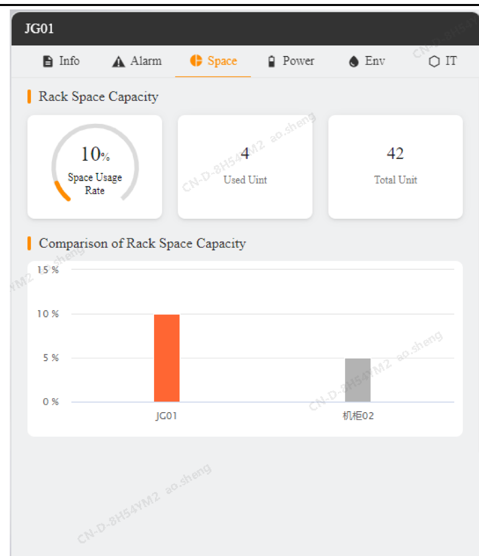


Figure 6.11 Power Distribution Card

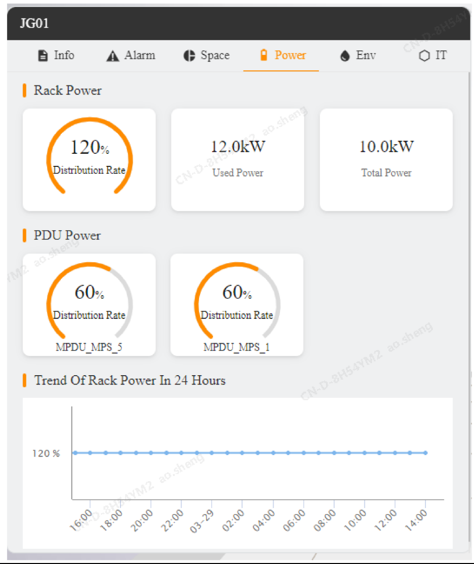


Figure 6.12 Environment Card

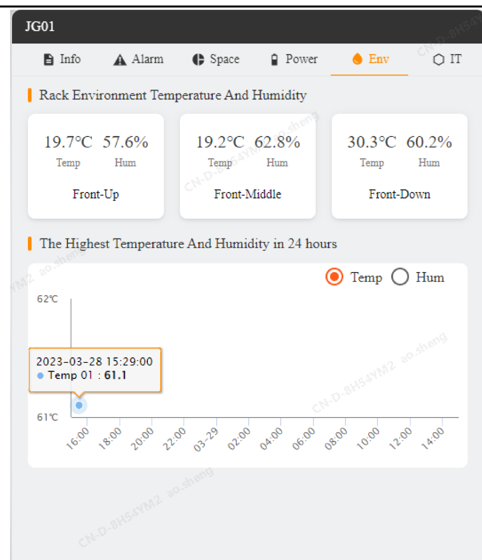
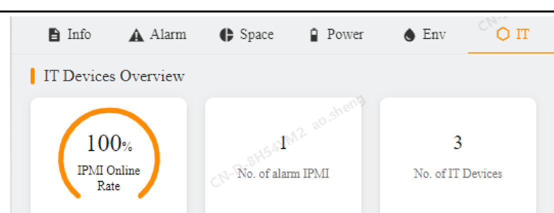


Figure 6.13 IT Card

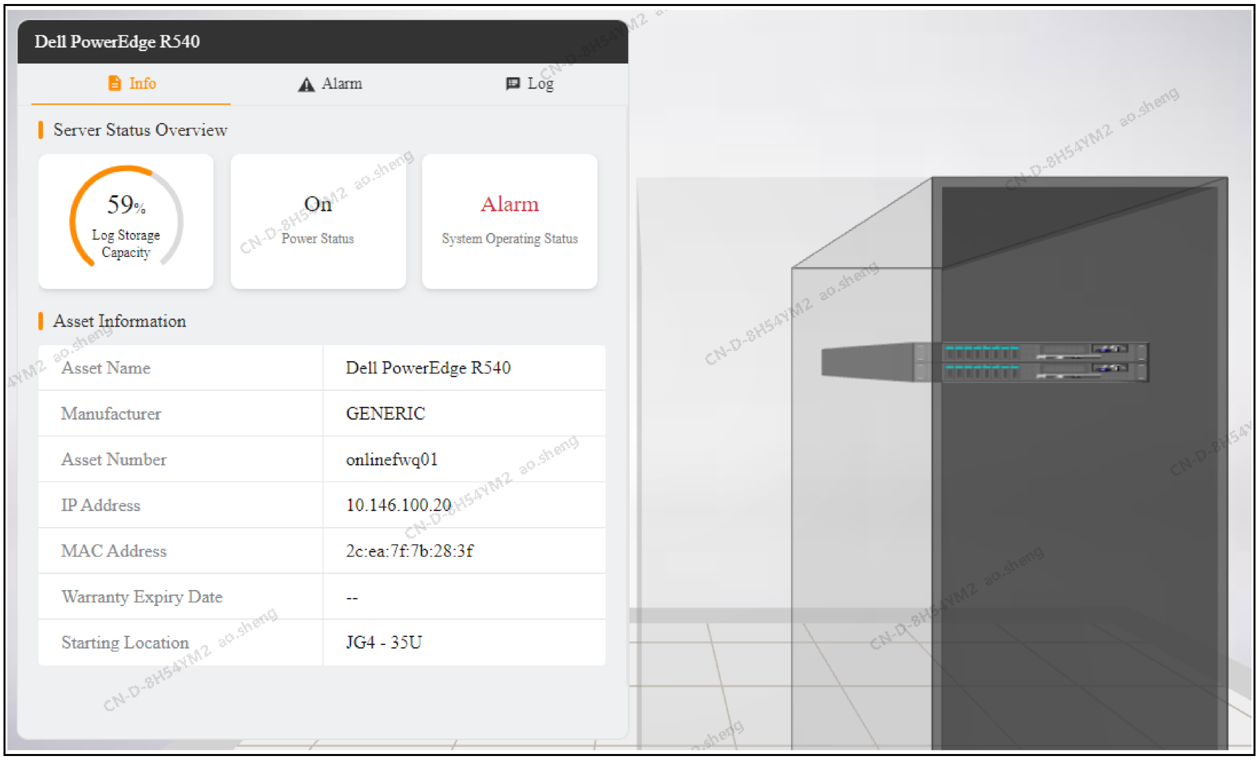


When switching to the IT class, click on the server model on the right to enter the server view as shown in **Figure 6.14** on the next page (if there is no IT device model, you need to manually add it in the 3D configuration).

Figure 6.14 3D single-cabinet view of Smart Aisle2 site - IT

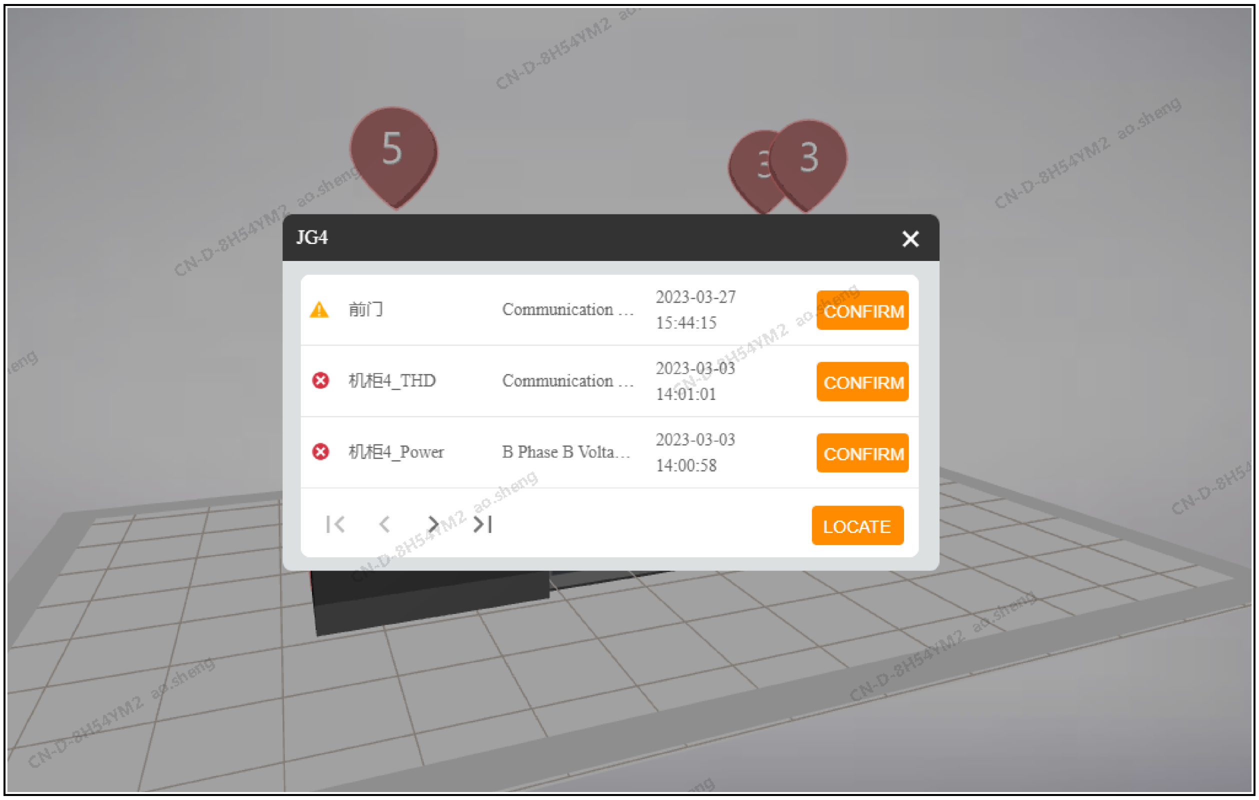
The IT card has basic information, alarms, and logs. As shown in the Figure 6.15 on the facing page .

Figure 6.15 Smart Aisle2 Site Server View



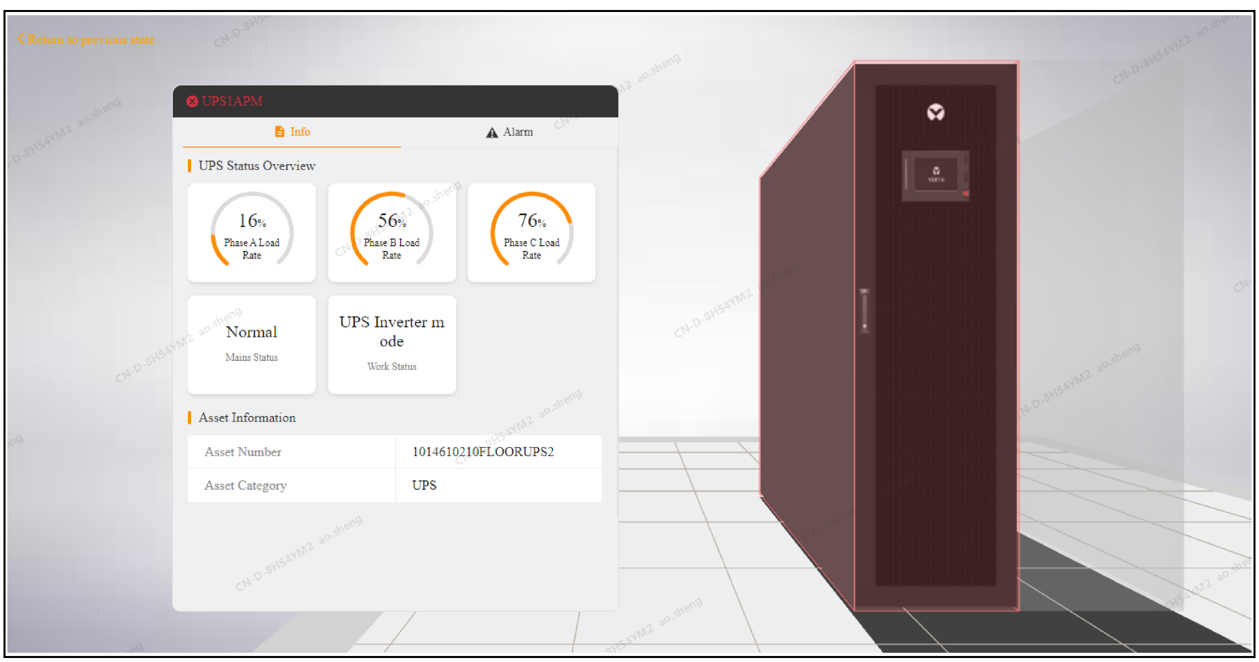
When a device has an active alarm, it displays a flashing red light and a floating alarm bubble at the top, as shown in **Figure 6.16** on the next page , Clicking the bubble reveals the alarm details and additional device information.

Figure 6.16 Smart Aisle2 Site - Alarm Popup Window



The UPS single cabinet view primarily displays essential UPS information, including a status overview and asset details, as illustrated in Figure 6.17 below . The alarm card shows current UPS alarms and visualizes new alarm trends using line charts for the past 24 hours and 7 days, similar to the cabinet alarm card.

Figure 6.17 Basic Information Card of the UPS



As shown in **Figure 6.18** below , the air conditioner's single cabinet houses three cards: basic status, alarm, and environment. The basic status card provides an overview of the air conditioner's status and asset information. The alarm card, similar to those for UPS and cabinet systems, displays current alarms and trends. Finally, the environment card shows temperature and humidity records along with temperature trend curves.

Figure 6.18 Air-conditioner Information

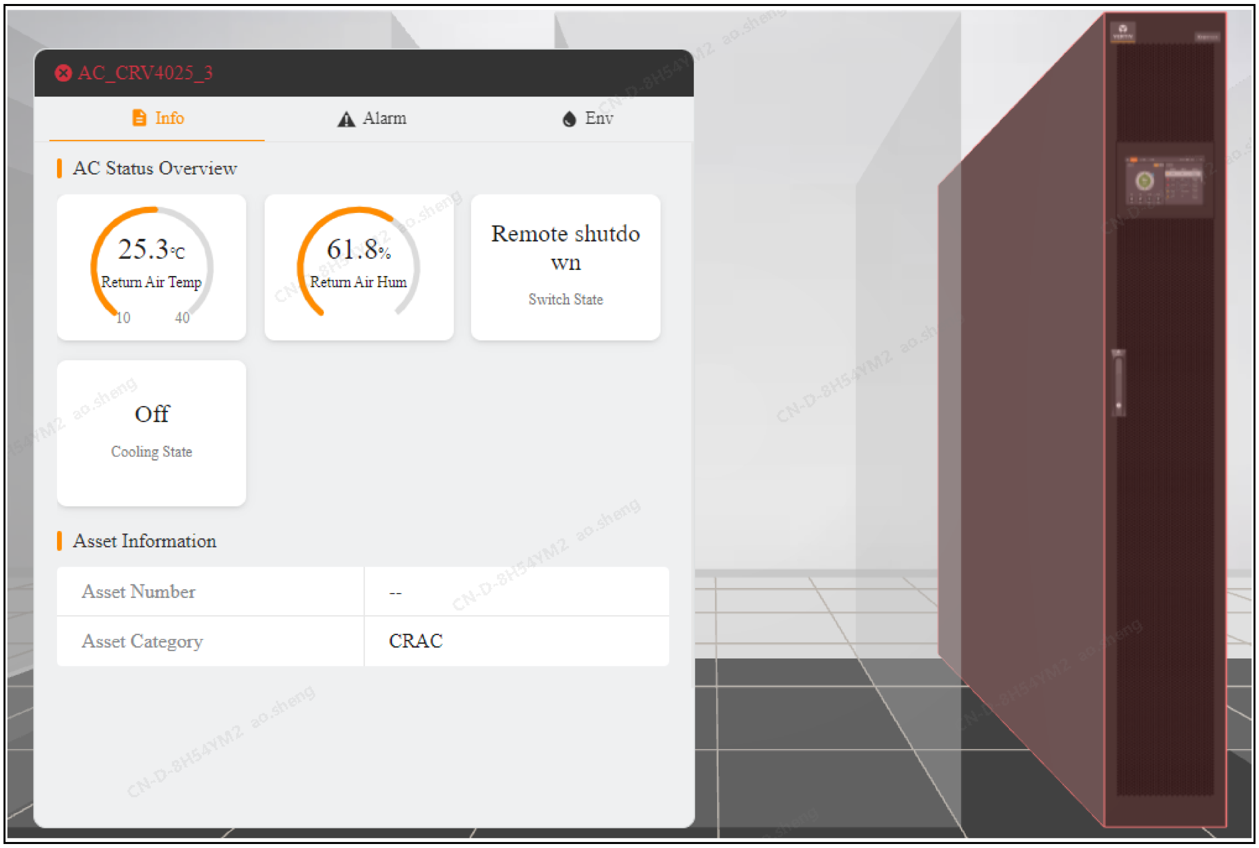
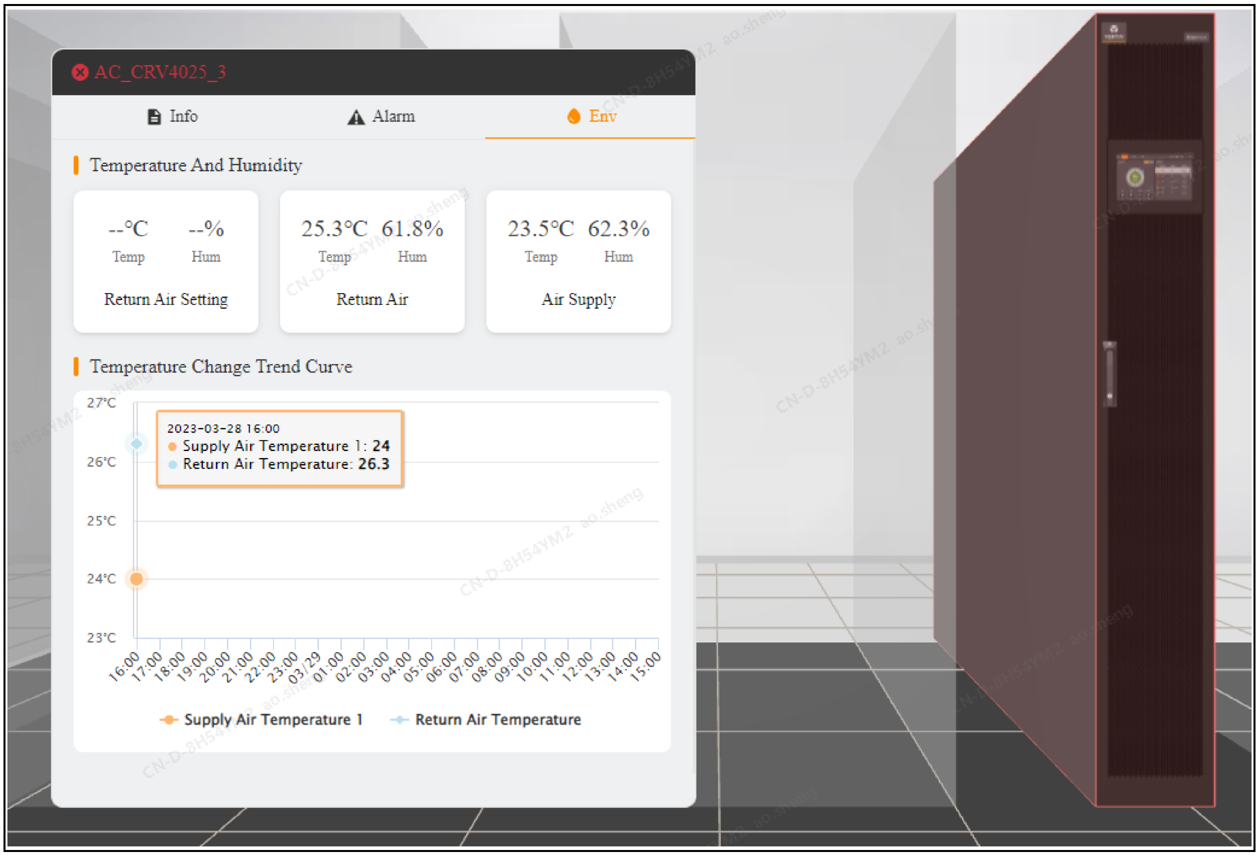


Figure 6.19 Air-condition Environment Card



The power distribution cabinet mainly contains three cards: basic information, alarm, and status, as shown in **Figure 6.20** on the facing page . The basic information card mainly includes an overview of the status of the SPM and the asset information of the added SPM. Alarm cards are similar to cabinets and UPS. The status card is a real-time power state diagram as shown in **Figure 6.21** on the facing page that depicts the status of the branch and the TOP20.

Figure 6.20 Basic Information Card of the SPM Cabinet

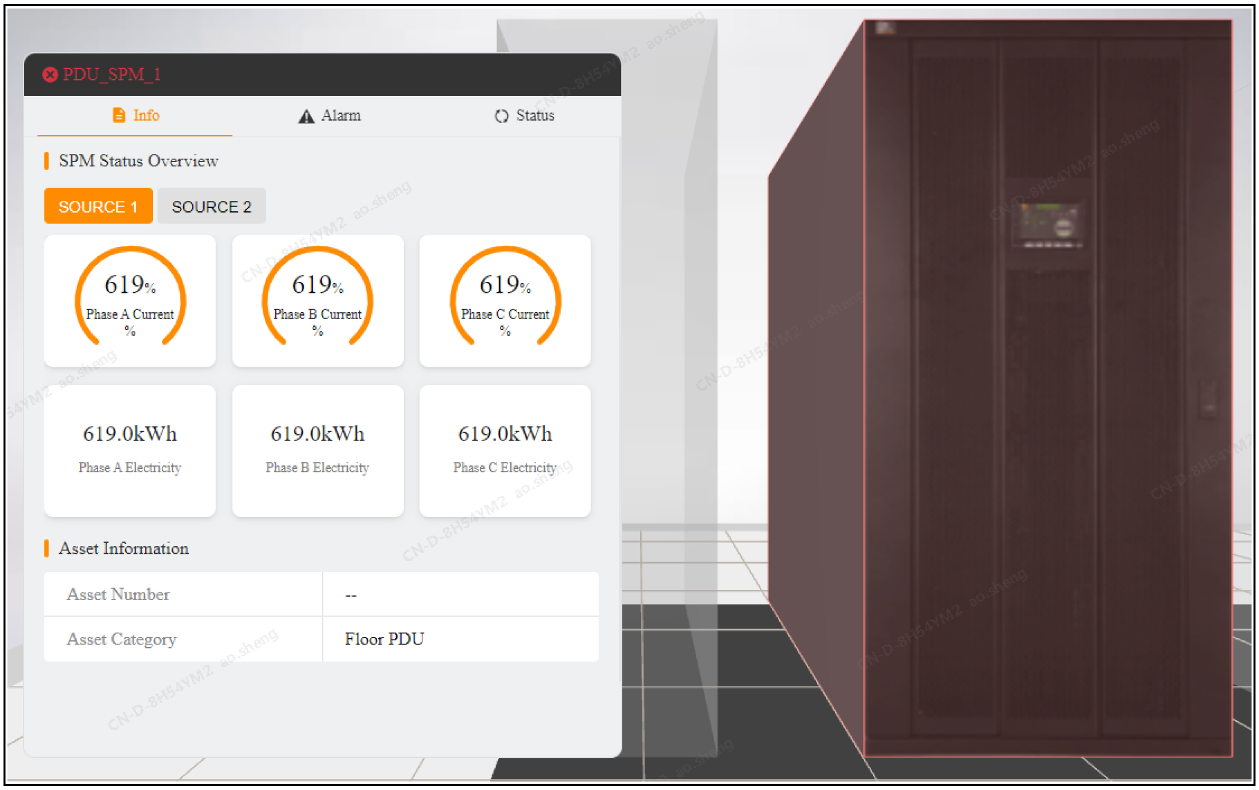


Figure 6.21 SPM Cabinet Status Card

Space Capacity 3D Visualization

Navigate to the Space Capacity tab to access the 3D view. This feature uses color-coded blocks to represent space utilization in each cabinet at the current site, as illustrated in in Figure 6.22 below . You can rotate, zoom, and pan the 3D model for a better view. Click on a specific cabinet to focus on it (similar to Smart Aisle2's single-cabinet view). From there, you can view detailed space capacity information.

Figure 6.22 Smart Aisle2 Space Capacity 3D View

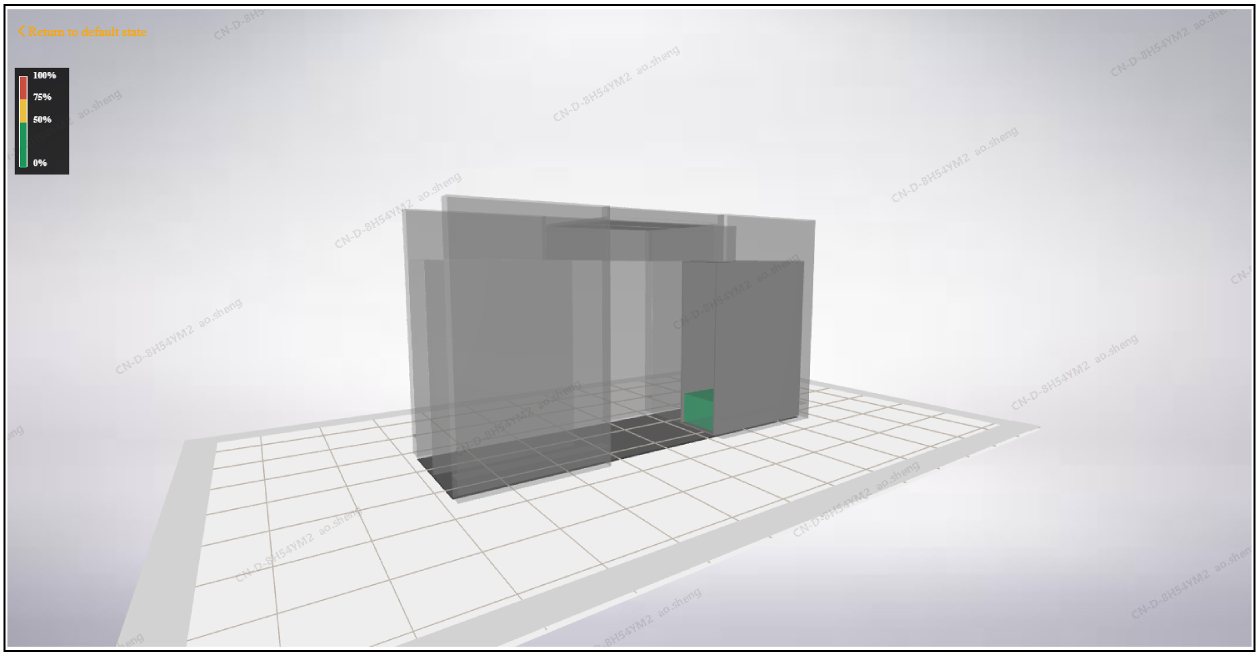
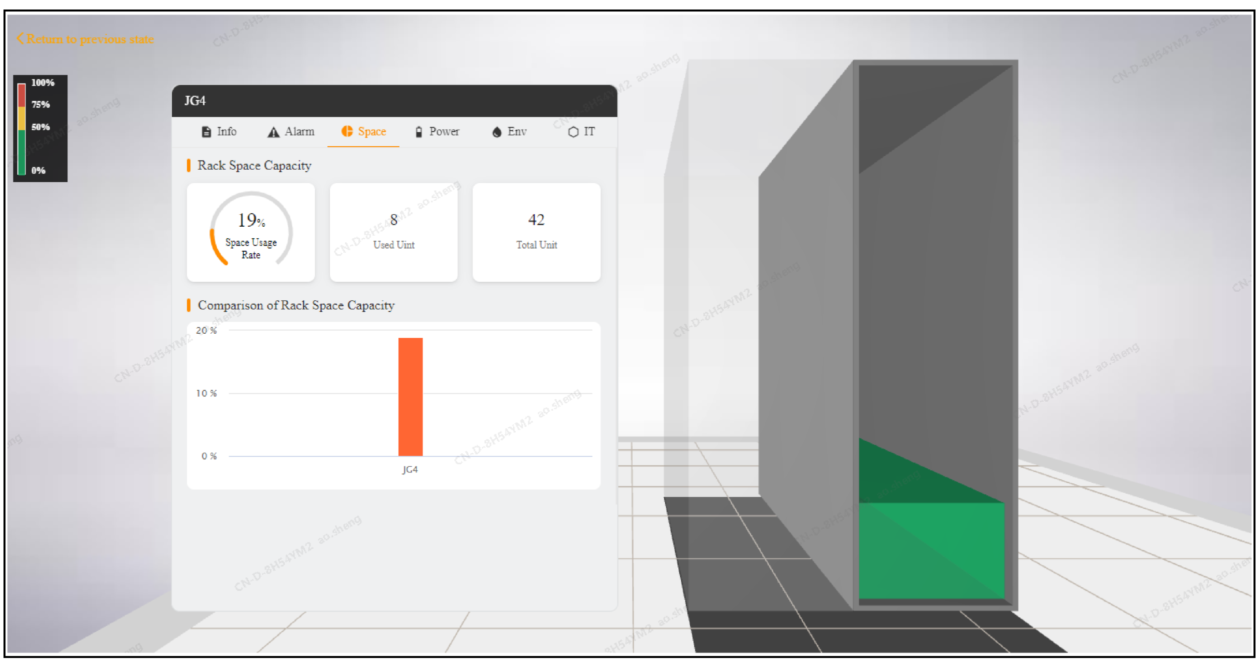


Figure 6.23 Cabinet Space Capacity

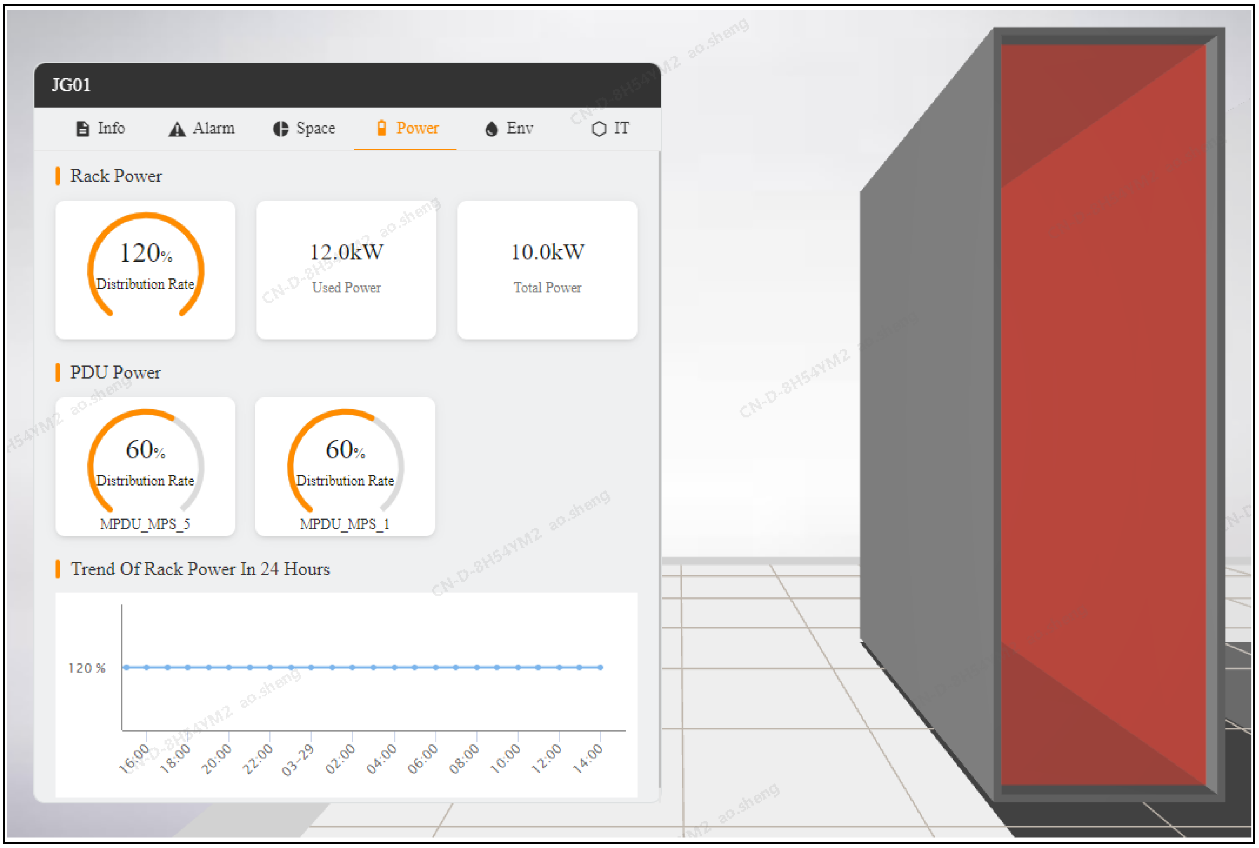


Power Capacity 3D Visualization

Navigate to the Power Capacity tab to access the 3D view, as shown in **Figure 6.24** below ,This view displays power distribution usage for each cabinet at the current site using color-coded 3D blocks. You can rotate, zoom, and pan the view. Click on a cabinet to focus on it (similar to Smart Aisle2.0's single-cabinet view) and view its total distribution capacity and power usage.

Figure 6.24 Smart Aisle2 Power Capacity View

Figure 6.25 Power Capacity of the Cabinet



Temperature Label 3D Visualization

Select the Thermal View tab to access the 3D view. This displays temperature labels for the rack: upper, middle, and lower, as illustrated in Figure 6.26 on the facing page . You can manipulate the 3D view by rotating, zooming, moving, and focusing. To adjust the temperature monitoring range, click Settings on the left-side temperature bar and set the maximum and minimum values. The system will update the label colors based on the rack's temperature.

Figure 6.26 Temperature Labels of Smart Aisle2

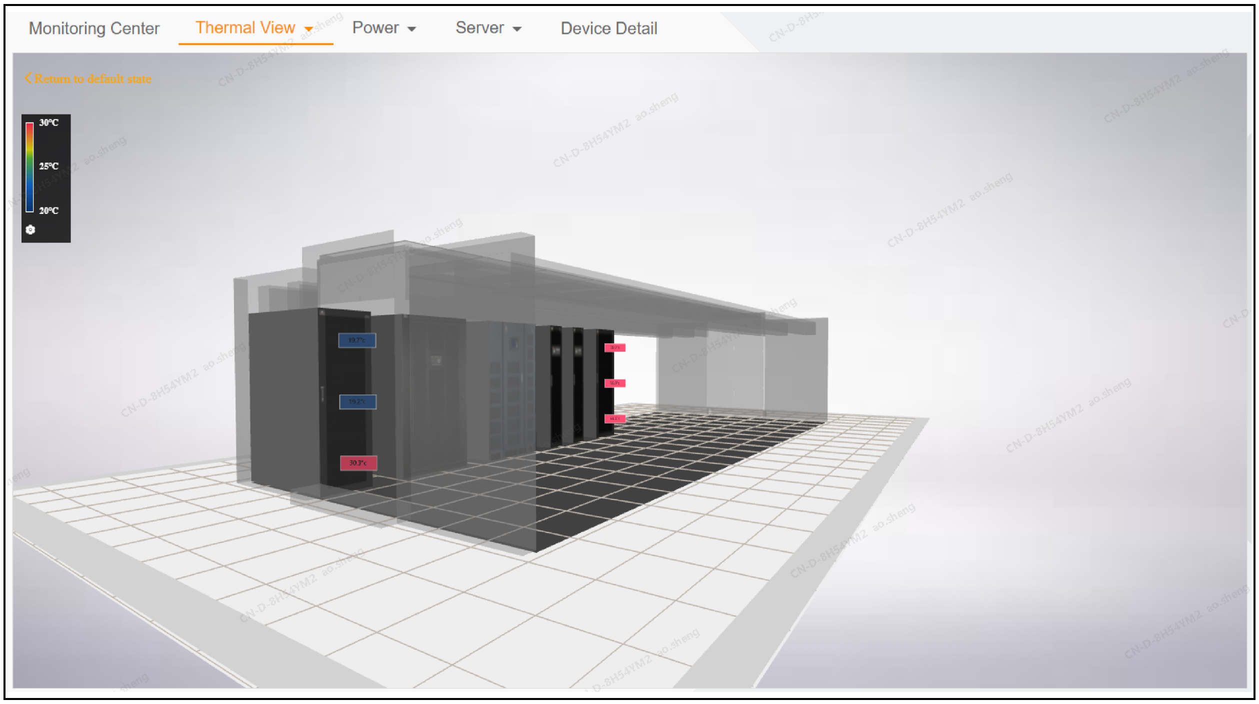
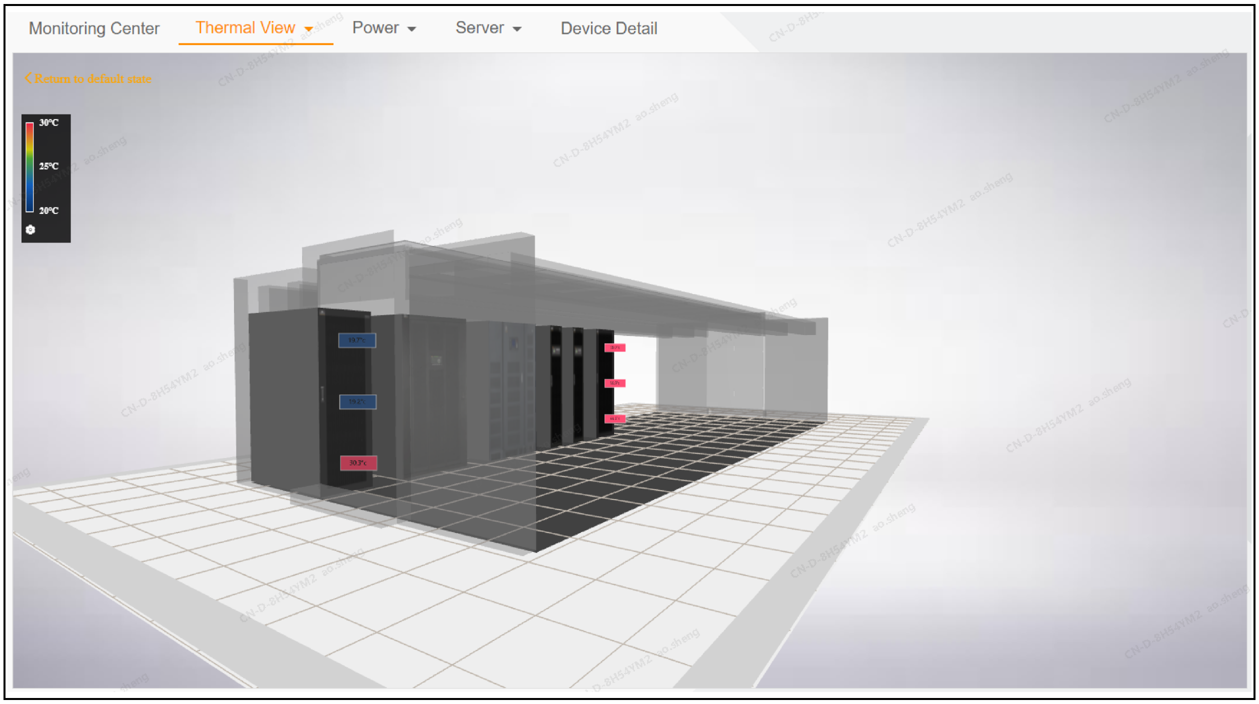


Figure 6.27 Temperature Label Detail

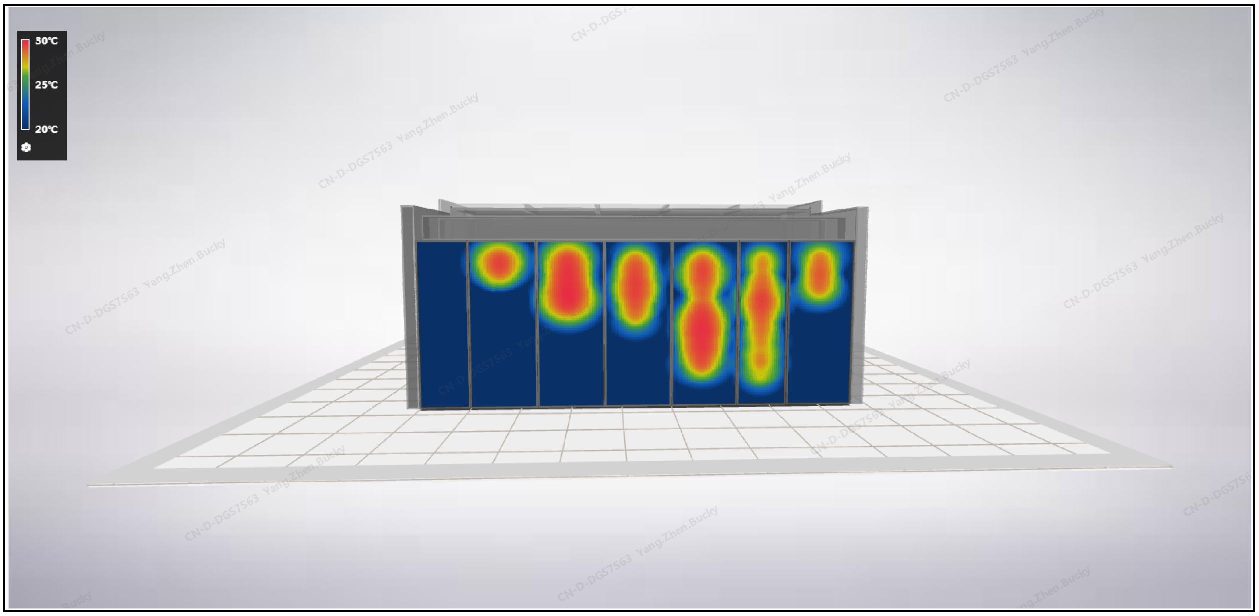
Figure 6.28 The Color of the Label Changes after Adjusting the Temperature Range



Heat Map

Click the Heat Map tab to access the Heat Map 3D view, as shown in the **Figure 6.29** below . This module displays the temperature status of IT equipment at the site through color-coded cabinets. Adjust the temperature range using the settings bar on the left; cabinet colors will update accordingly. To change your view, simply tap on a device.

Figure 6.29 Smart Aisle2 Site Heat Map



6.2.2 Smart Aisle3 Site 3D Visualization

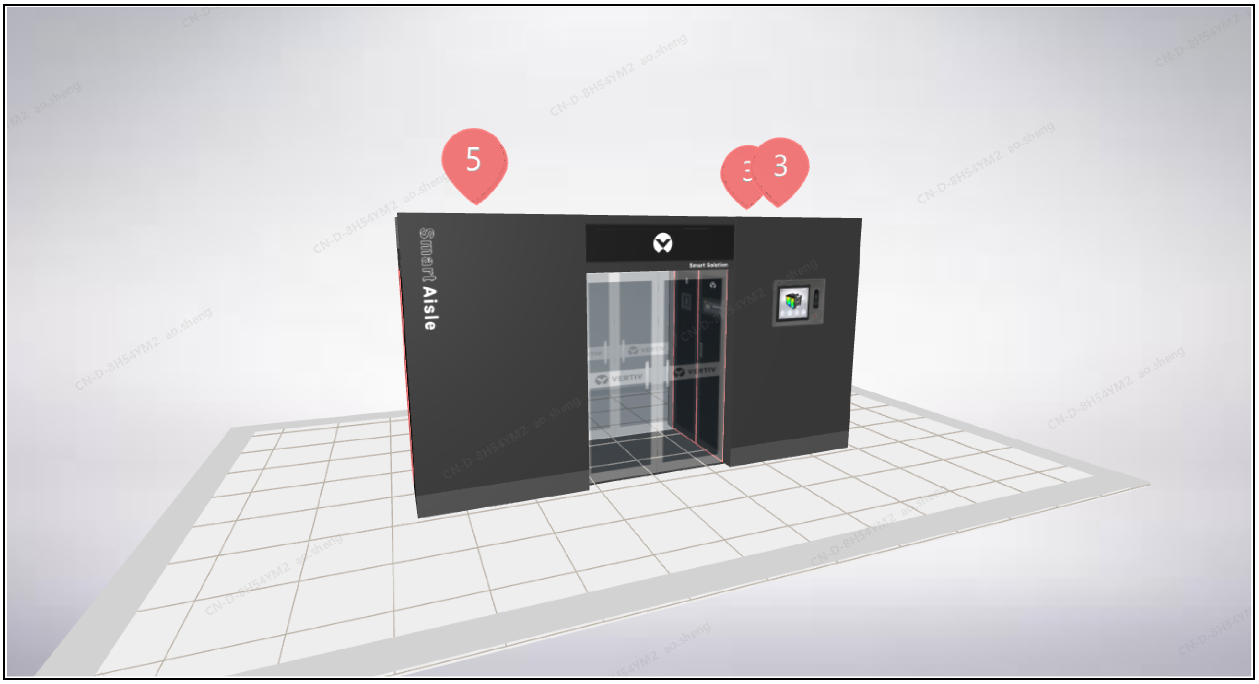
Building on Smart Aisle2, Smart Aisle3's 3D view provides even more intelligence with real-time displays including door lock status, zenith status and more.

3D View

As shown in **Figure 6.30** on the next page , the 3D view of the Smart Aisle3 site, showing assets inside Smart Aisle3 and alarms. Users can navigate the 3D environment as follows:

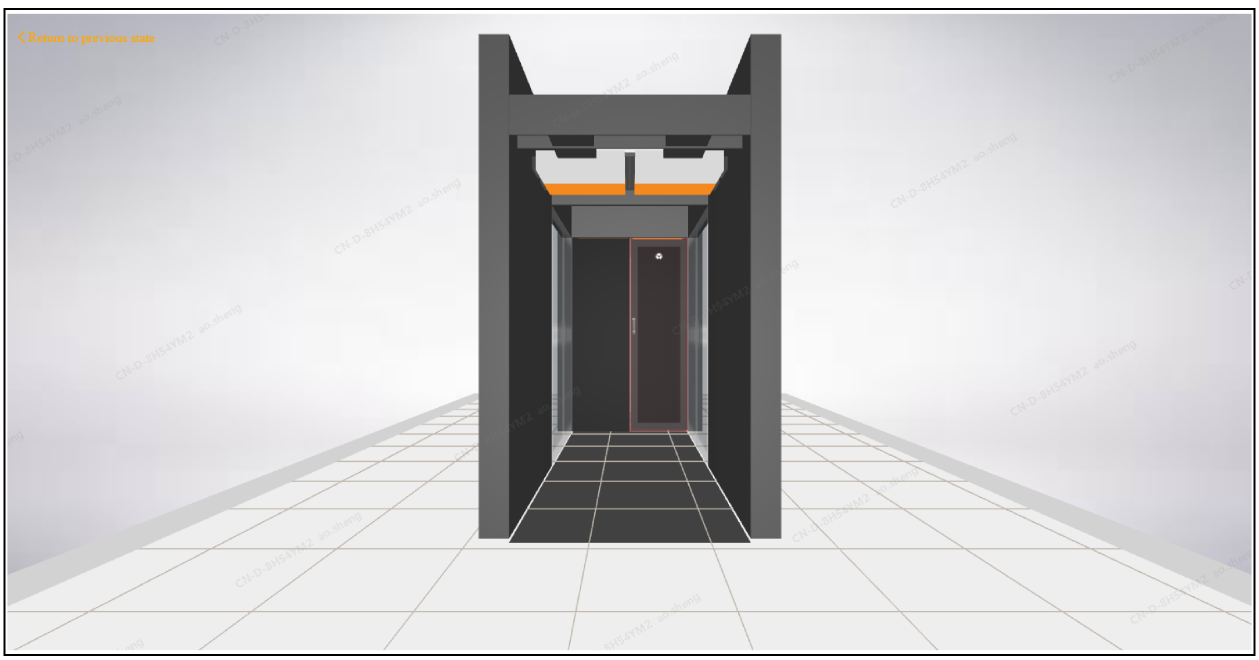
- Left mouse button: Rotate the view
- Right mouse button: Pan the view
- Scroll wheel: Zoom in and out
- Hold scroll wheel: Reset to default view

Figure 6.30 The Default 3D View of the Smart Aisle3 Site



Click the Smart Aisle3 and it will display the row angle view, as shown in Figure 6.31 below . You can now click on a device, like a cabinet or battery unit, to view its individual details, or use the back button on the left to return to the previous view.

Figure 6.31 3D Single-Row View of Smart Aisle3 Site



In the single-row view, click on any cabinet to access the single-cabinet view, as shown in the **Figure 6.32** below . The left panel displays different perspectives about the cabinet, including basic details, alarms, space, power, environment, and IT categories. The basic information provides an overview of the cabinet's status. The 3D model shows all equipment in the cabinet. Switching to the alarm card highlights devices with active alarms in the 3D view. Selecting the IT category displays IT equipment such as servers and switches.

Figure 6.32 3D Single-Cabinet View of Smart Aisle3 Site

Click Alarm, Space, Power Distribution, Environment, IT, etc. to switch to the corresponding card and display the corresponding content. As shown in from **Figure 6.33** below to **Figure 6.38** on page 134 .

Figure 6.33 Alarm Card Content

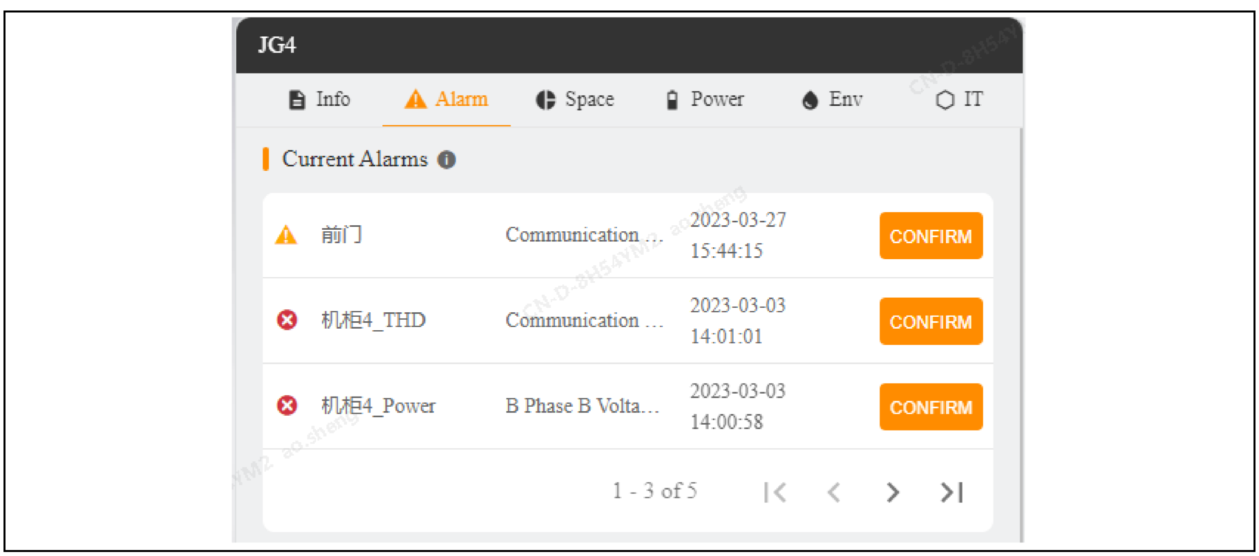


Figure 6.34 Alarm Trend

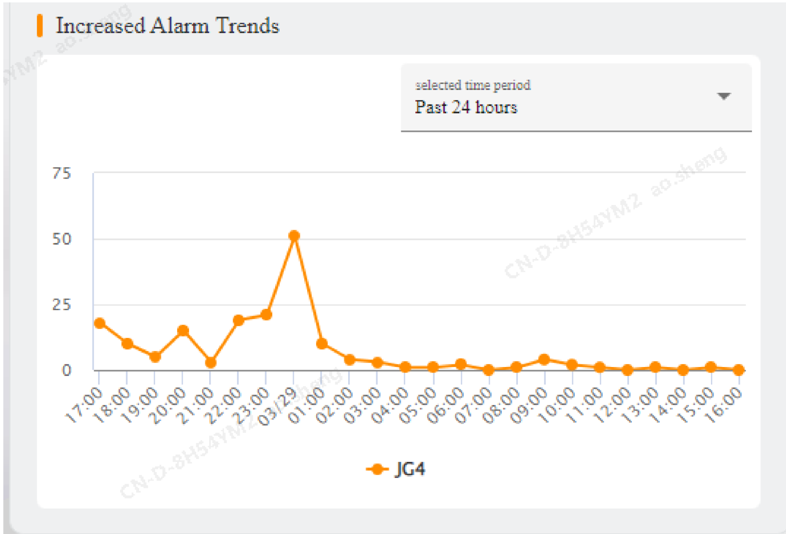


Figure 6.35 Space Usage

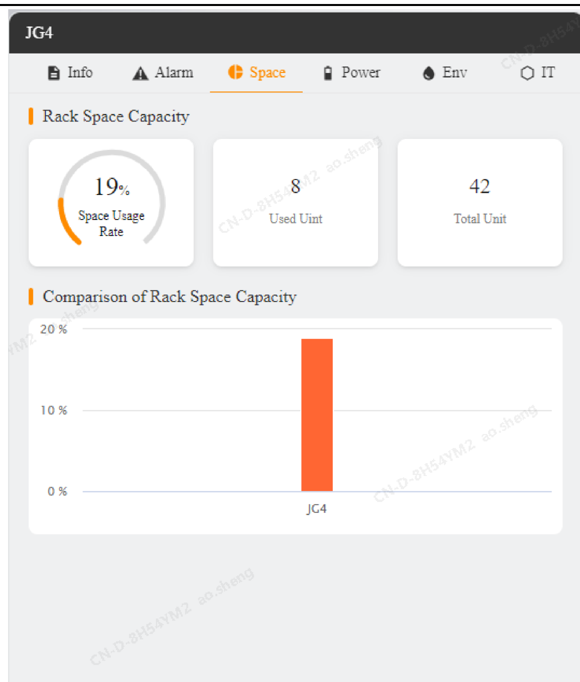


Figure 6.36 Power Usage

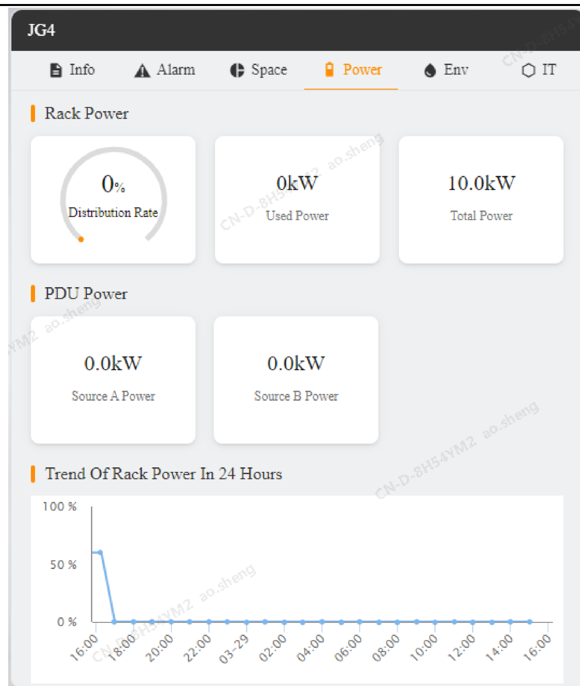


Figure 6.37 Environment Information

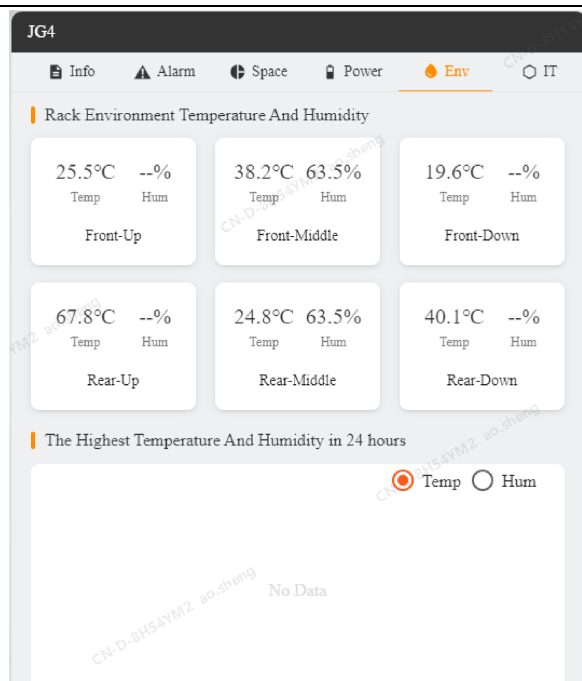
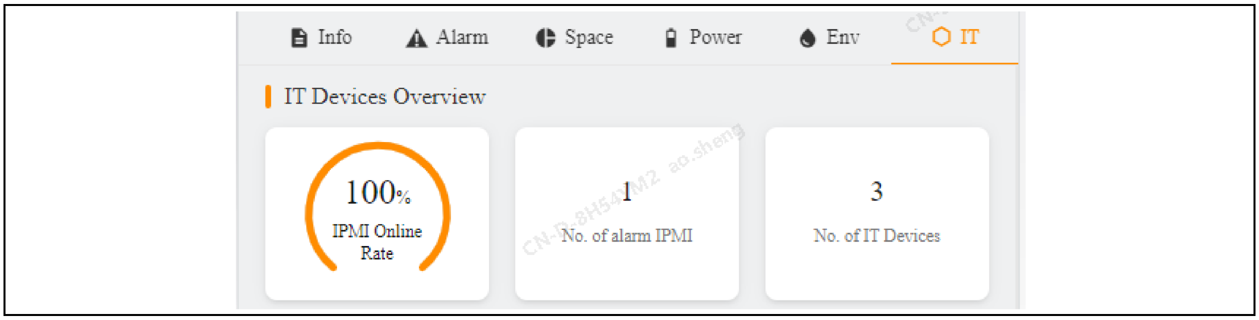


Figure 6.38 IT Devices Overview



When an alarm exists on a device, it flashes red and there is an alarm bubble floating on the top, and you can click the bubble to know the alarm content and other information of the device. As shown in Figure 6.39 below .

Figure 6.39 Smart Aisle3 Site— Alarm Popup Window

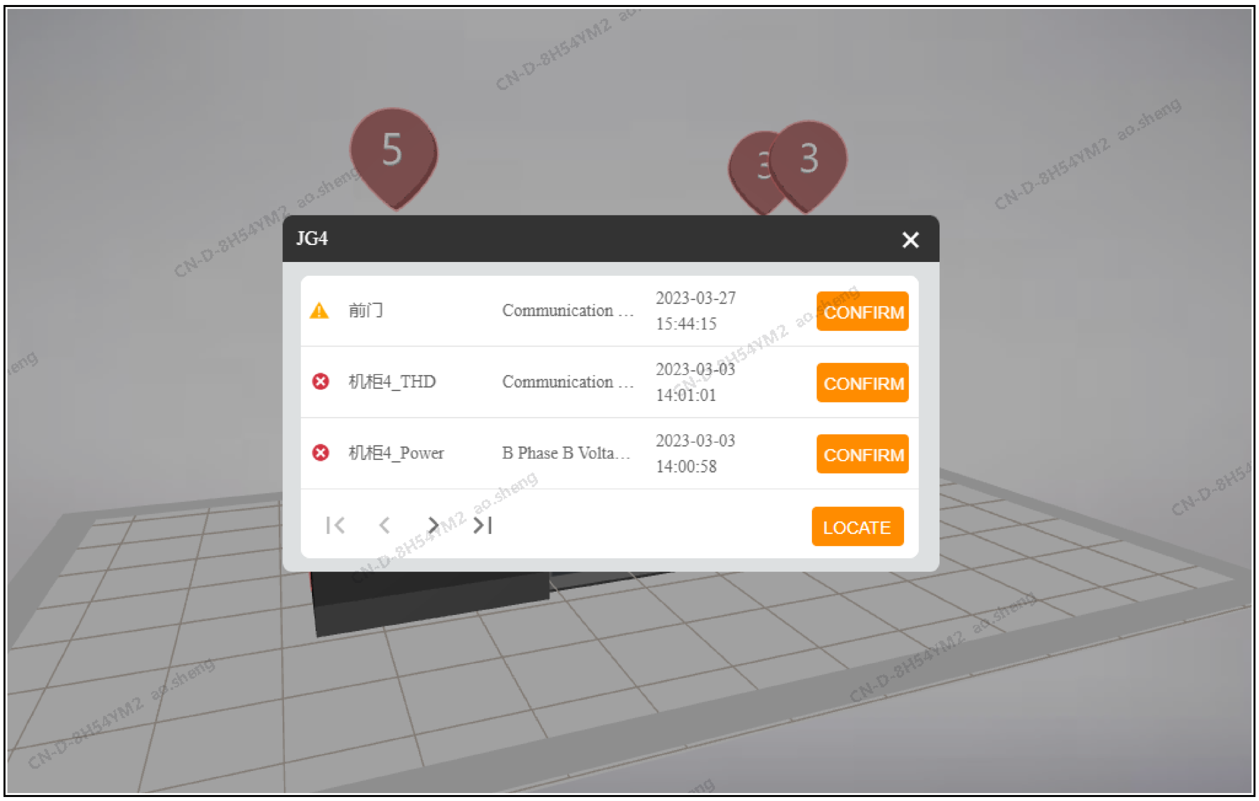
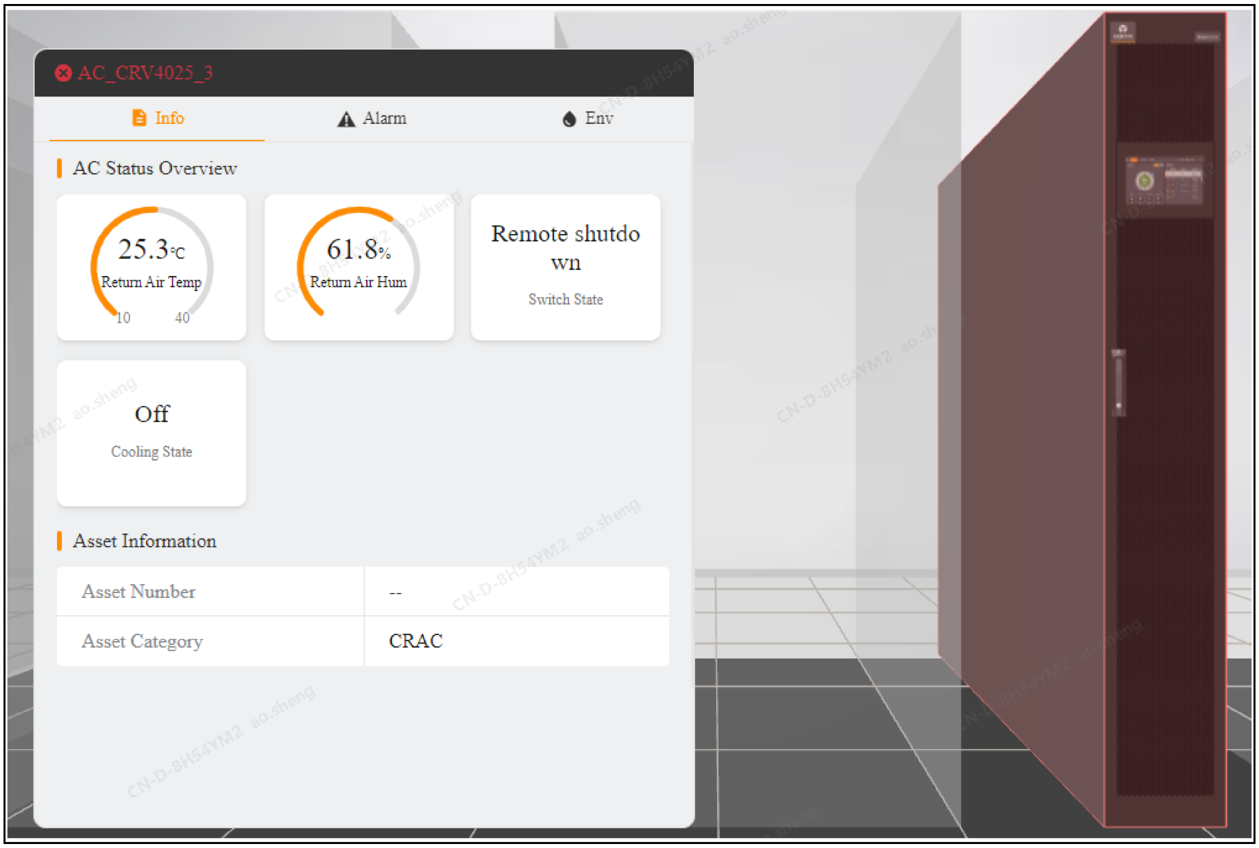


Figure 6.40 Basic content of an Air Conditioner



6.2.3 Smart Row2 Site 3D Visualization

In the 3D visualization of Smart Row, the 3D view will display 3D model base on 3D configuration of the site.

3D View

As shown in **Figure 6.41** on the next page .The 3D appearance of the Smart Row site, assets and alarms from devices of the site are displayed.

Figure 6.41 The Default 3D View of Smart Row Site

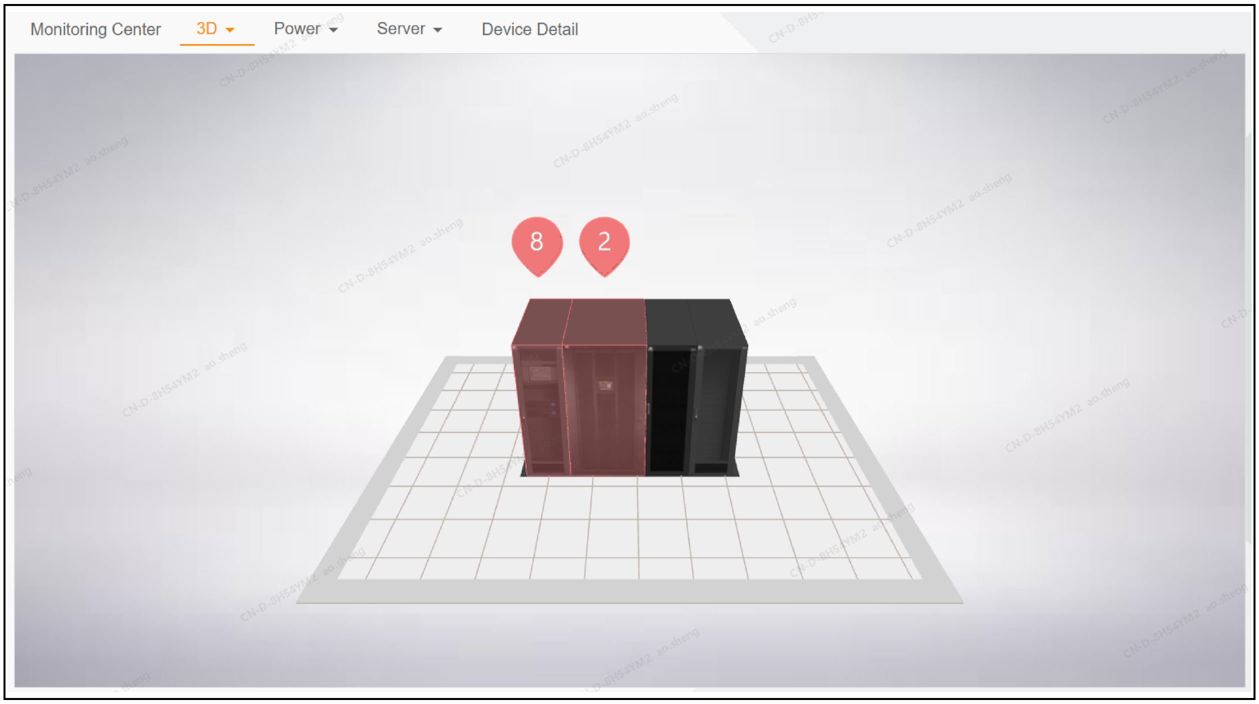
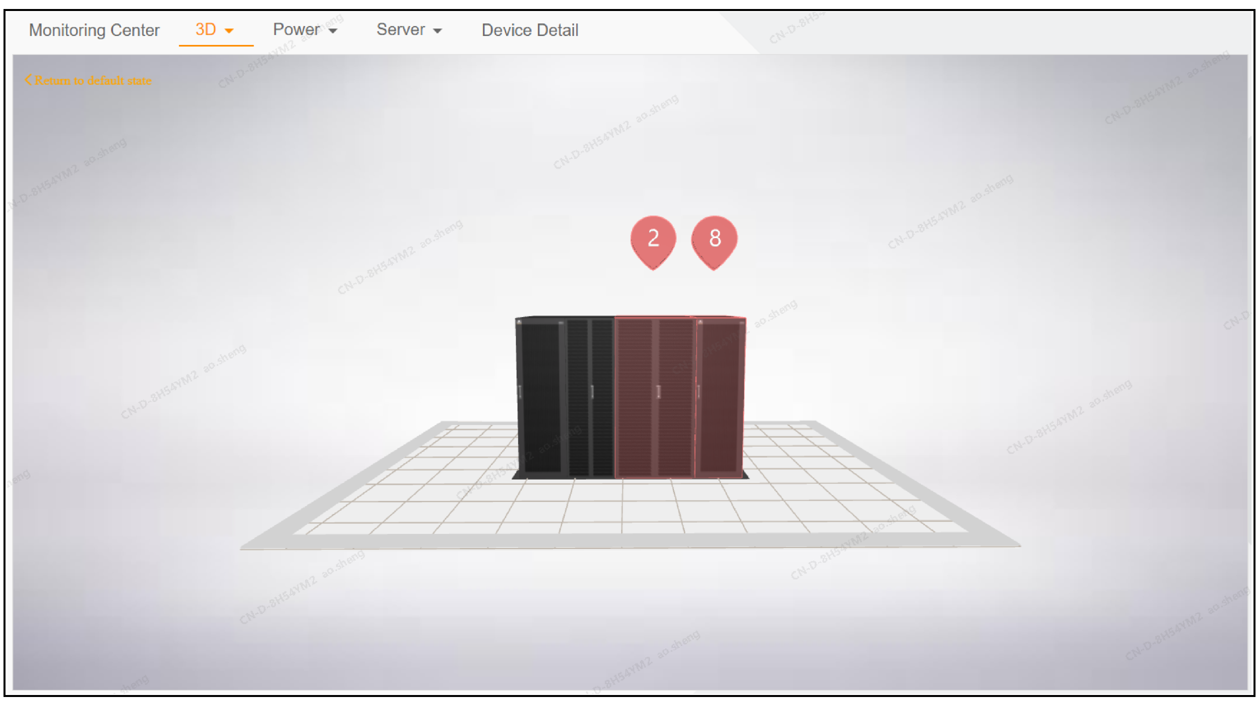
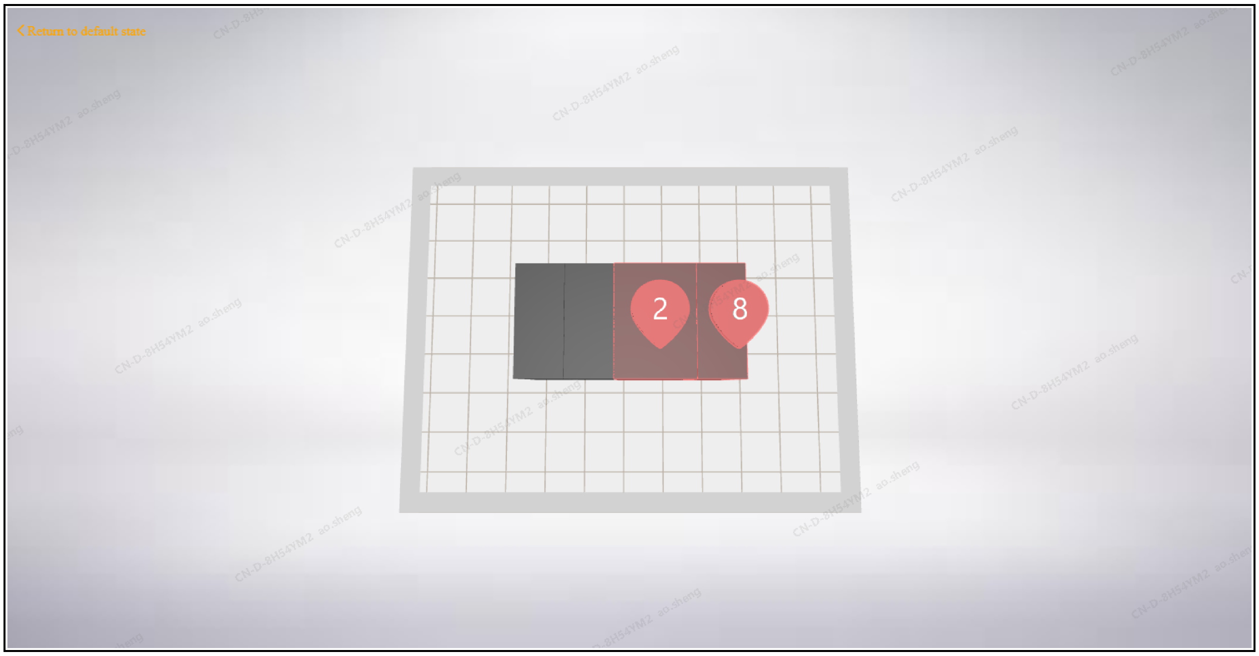


Figure 6.42 3D Back View of the Smart Row Site



The 3D appearance of the SR site can also be zoomed in or out with a mouse wheel.

Figure 6.43 Top View of the SR Site



Users can click on a device, such as a cabinet or power distribution cabinet, to view details of a single cabinet. In the single-cabinet view, clicking any cabinet opens the PMC cabinet view, as shown in **Figure 6.44** on the next page .

The left panel displays the cabinet's basic information, alarm, power supply, power, environment, and IT categories. The basic information provides an overview of the cabinet status and asset details, while the 3D model shows all equipment in the cabinet.

Switching between different cards in the left panel updates the 3D model accordingly:

- Alarm card: Highlights devices with active alarms
- Power Supply card: Displays meters and UPS devices
- Power Distribution card: Shows PDU devices
- IT card: Presents IT equipment like servers and switches

In **Figure 6.44** on the next page , offers an overview of the PMC cabinet's basic information and a 3D representation of its contents.

Figure 6.44 Single-Cabinet View of the PMC Cabinet at the Smart Row Site

Click Alarm, Power Supply, Power Distribution, Environment, IT, etc. to switch to the corresponding card and display the corresponding content, as shown in from **Figure 6.45** on the facing page to **Figure 6.49** on page 143 .

Figure 6.45 Alarm Card of the PMC Cabinet

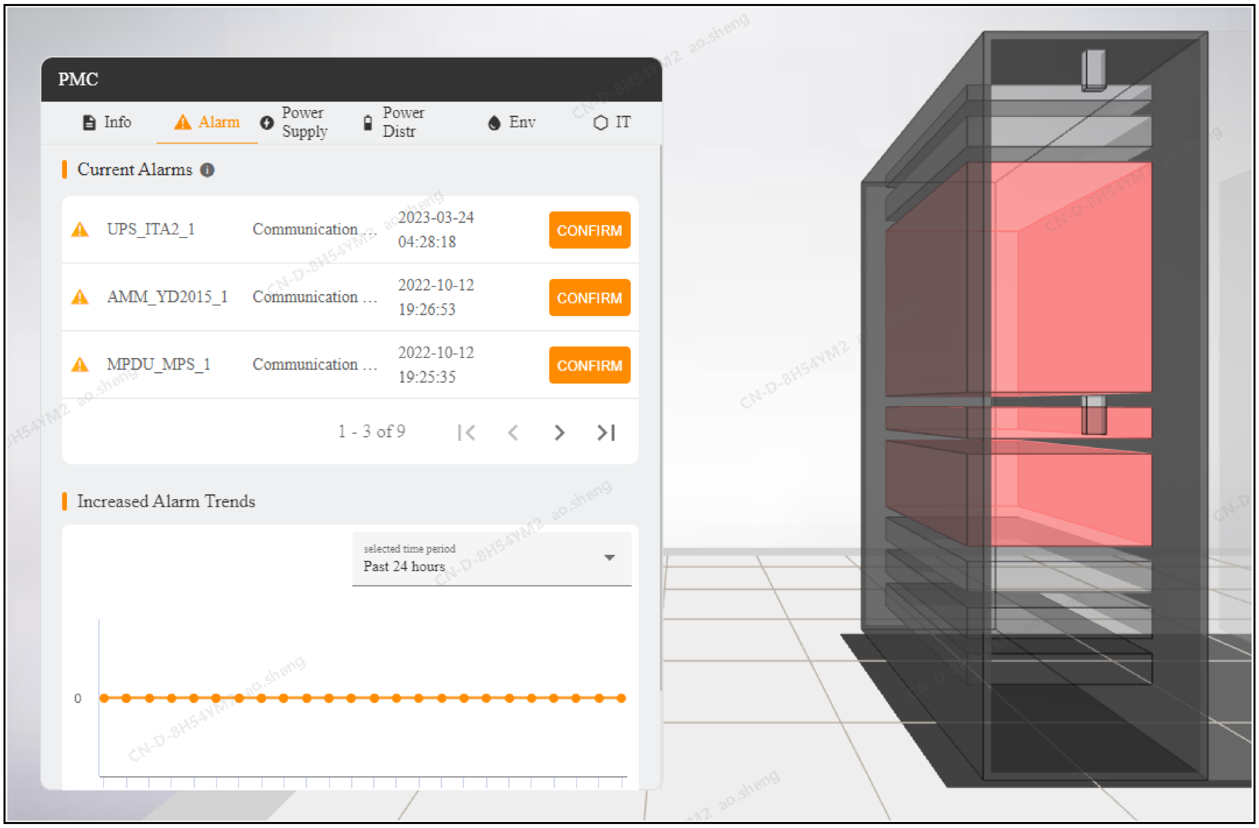


Figure 6.46 Power Supply Card of the PMC Cabinet is Displayed

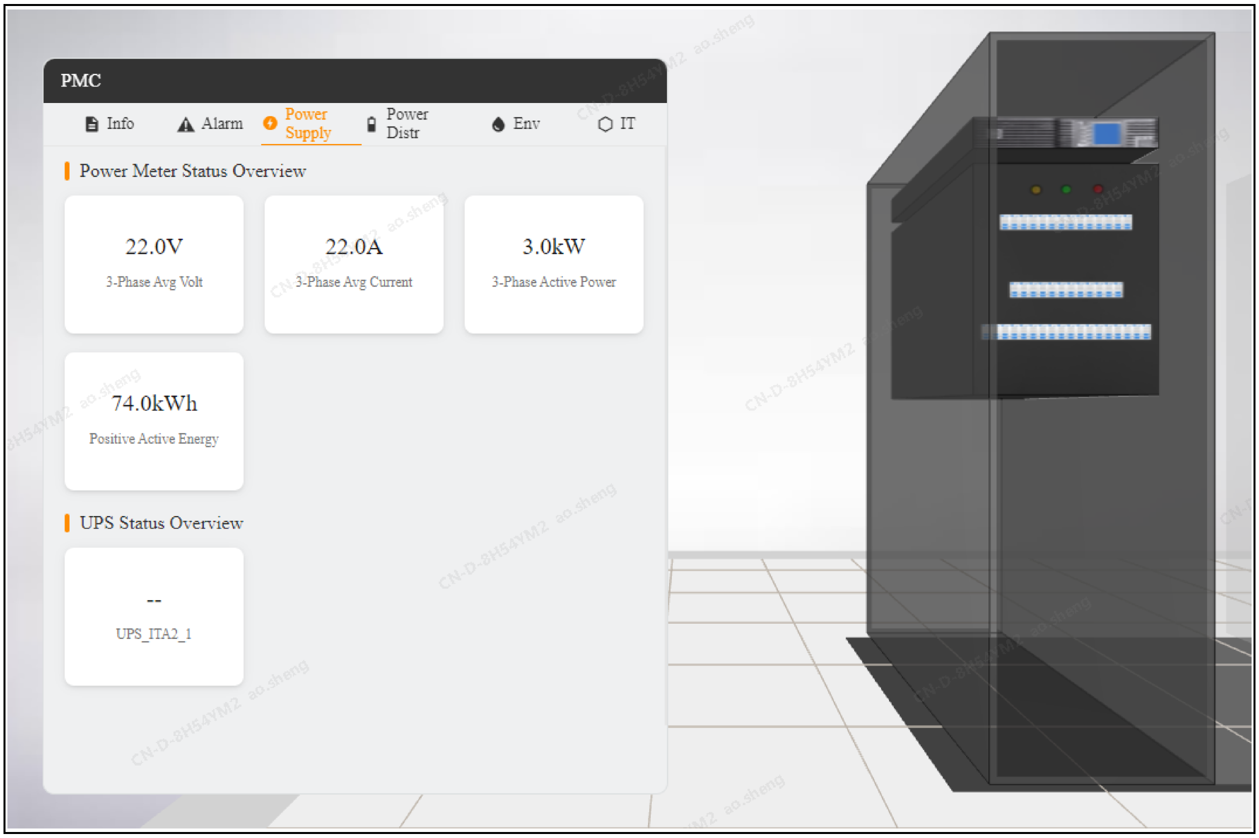


Figure 6.47 Power Distribution Card of the PMC Cabinet

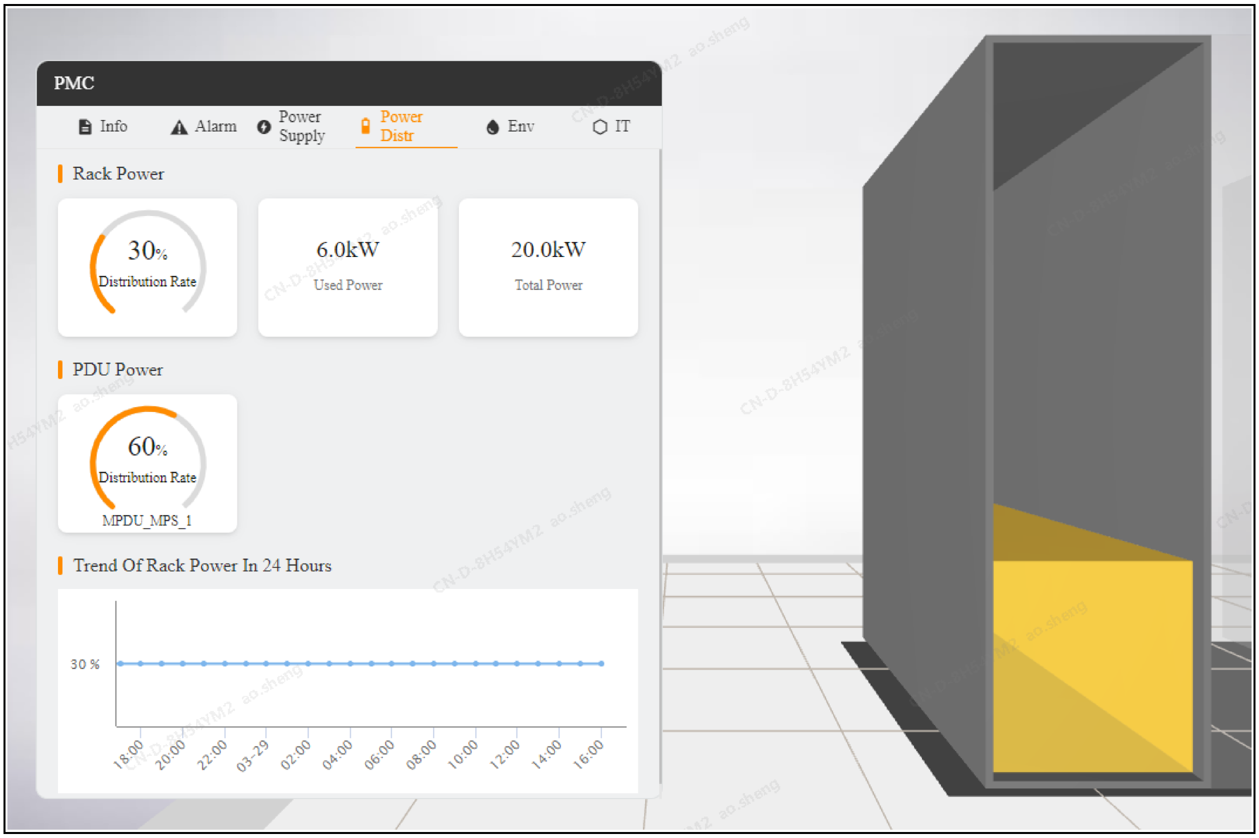


Figure 6.48 PMC Cabinet Environment Card

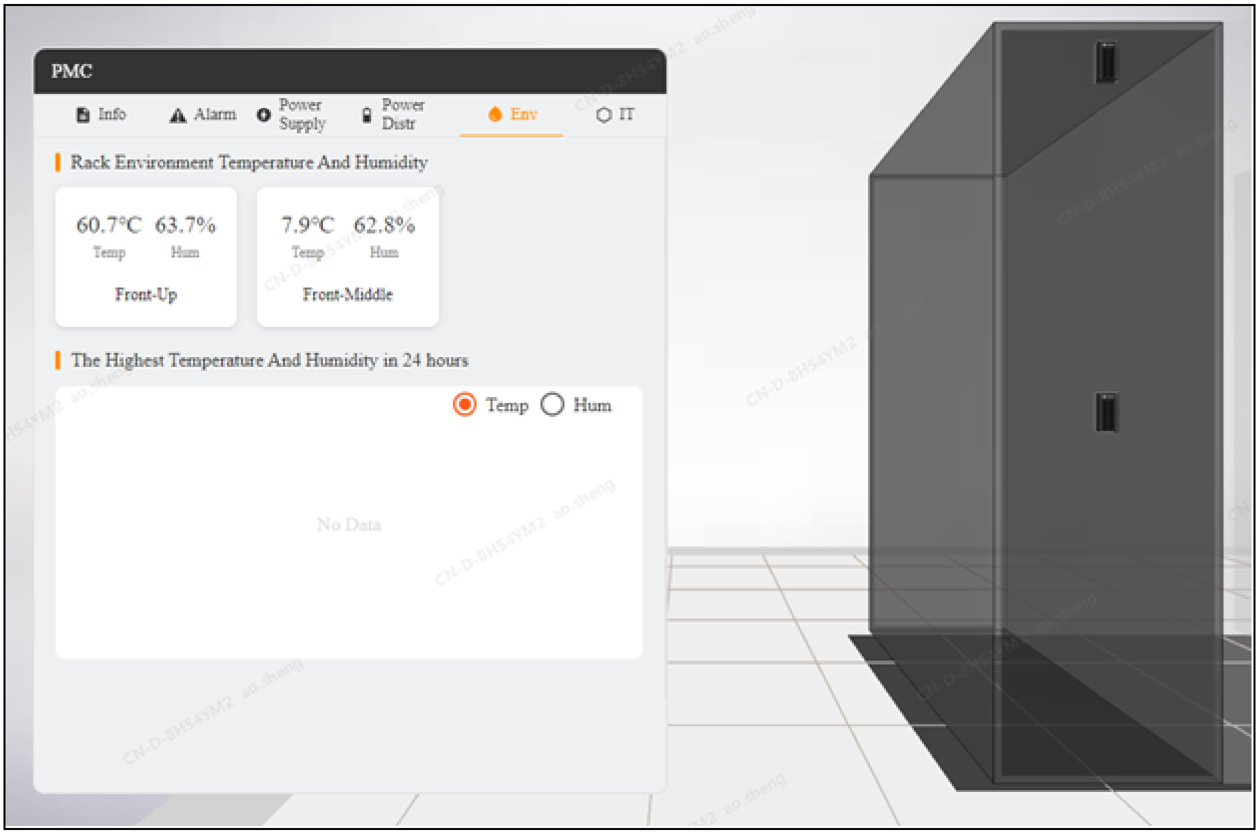
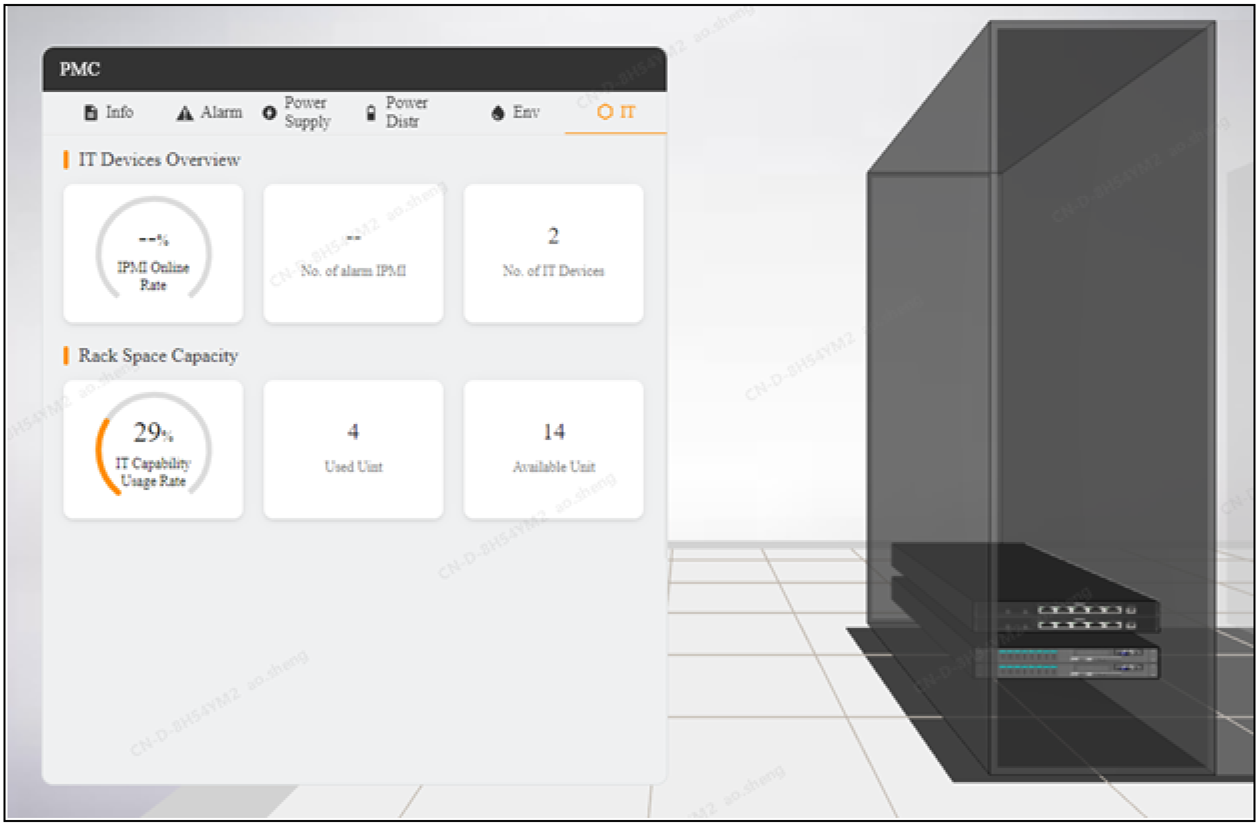
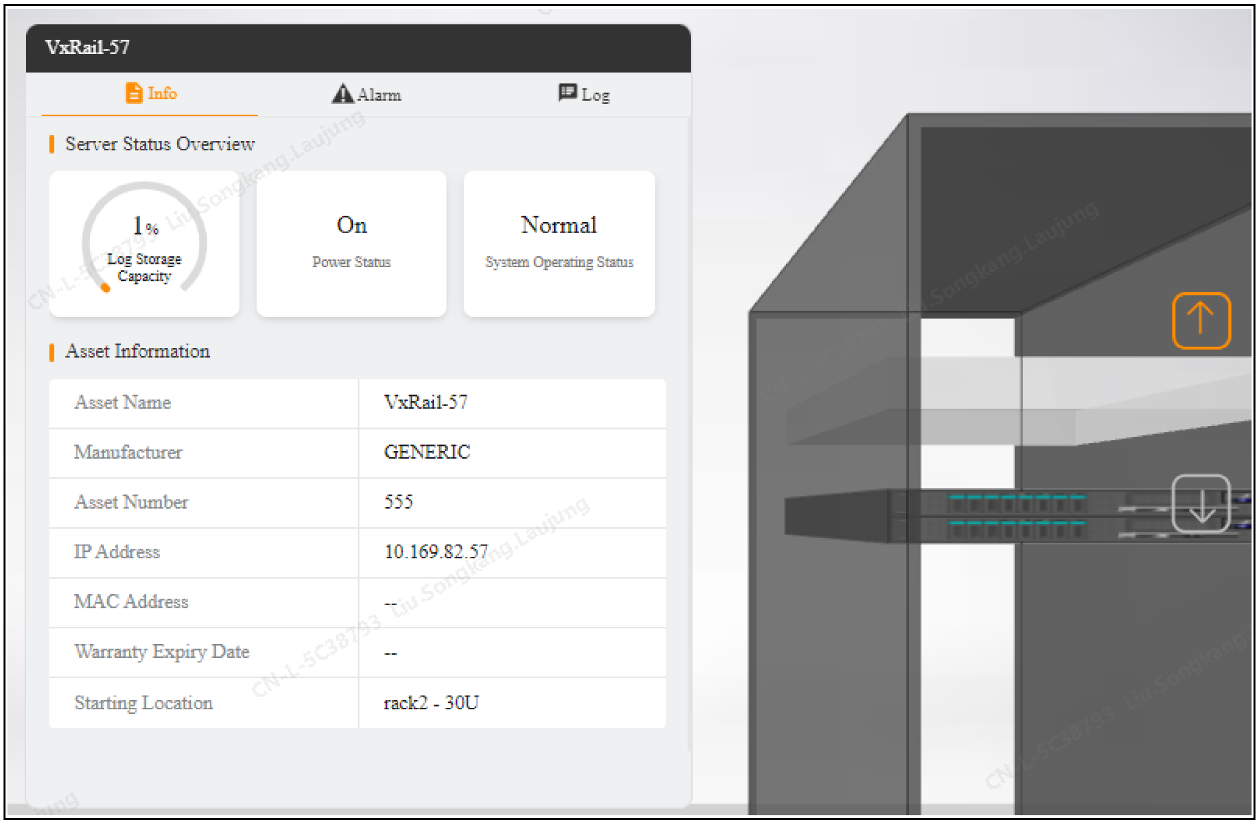


Figure 6.49 IT Card of the PMC Cabinet



When switching to the IT card, click on the server model on the right to enter the server view.

Figure 6.50 View of the Smart Row Site Server



The single-cabinet view of the power distribution cabinet (SPM) mainly contains three cards: basic information, alarm, and status. The basic information card mainly includes the status overview asset information. Alarm cards are similar to cabinets. The status card displays the current rate and energy consumption of different branches from the SPM.

Figure 6.51 Basic Information and Cards of the SPM Cabinet

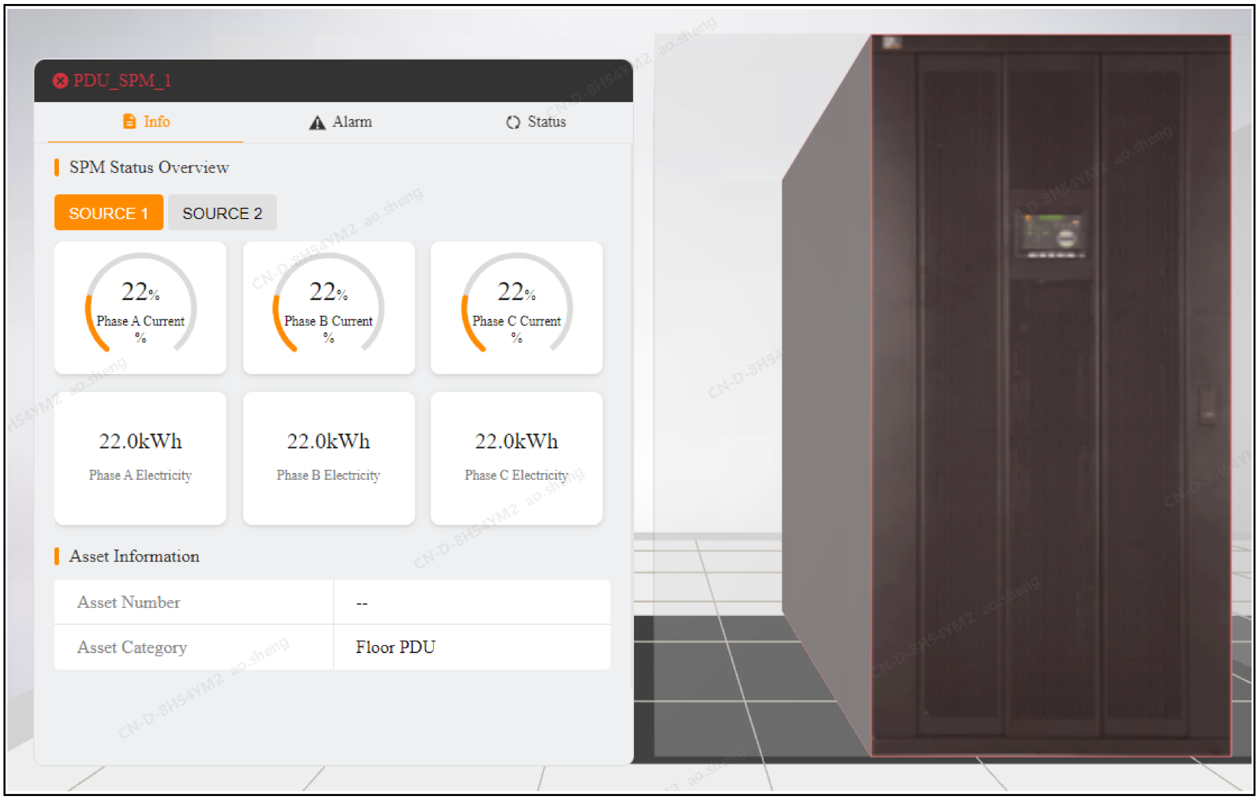
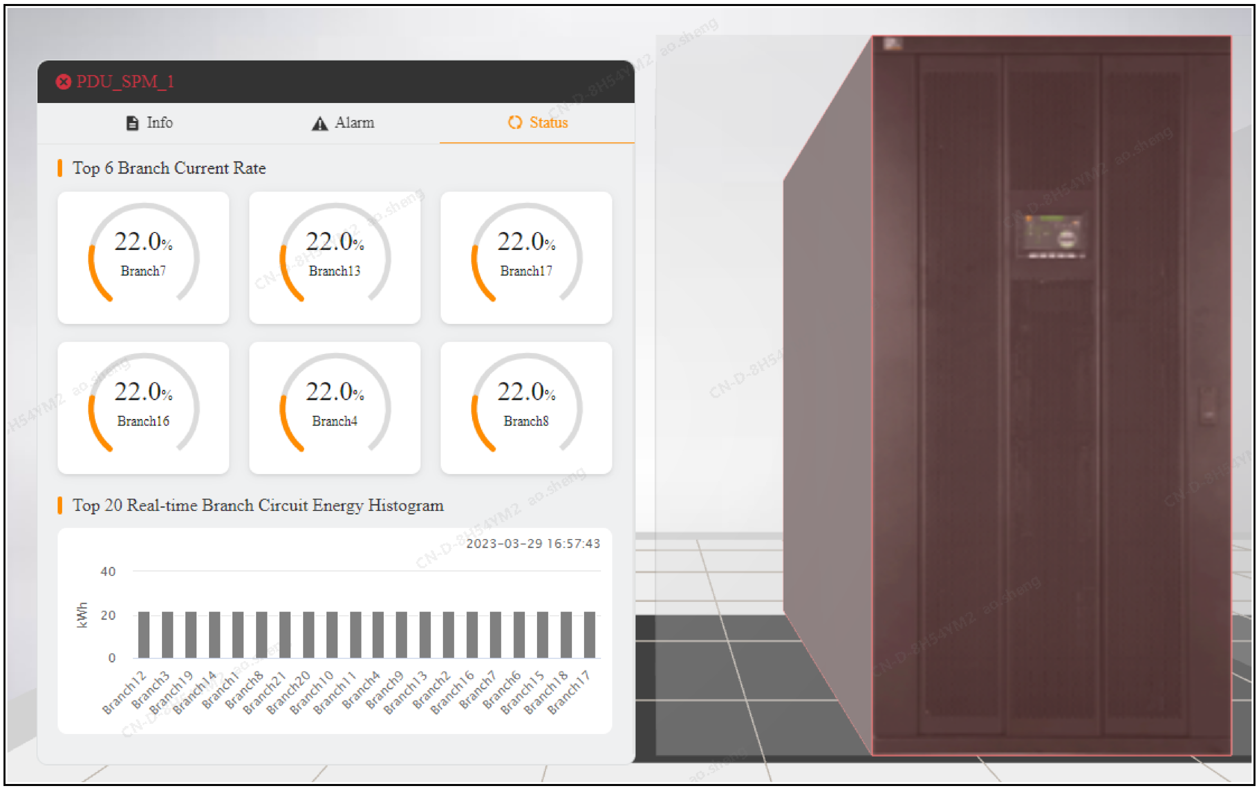


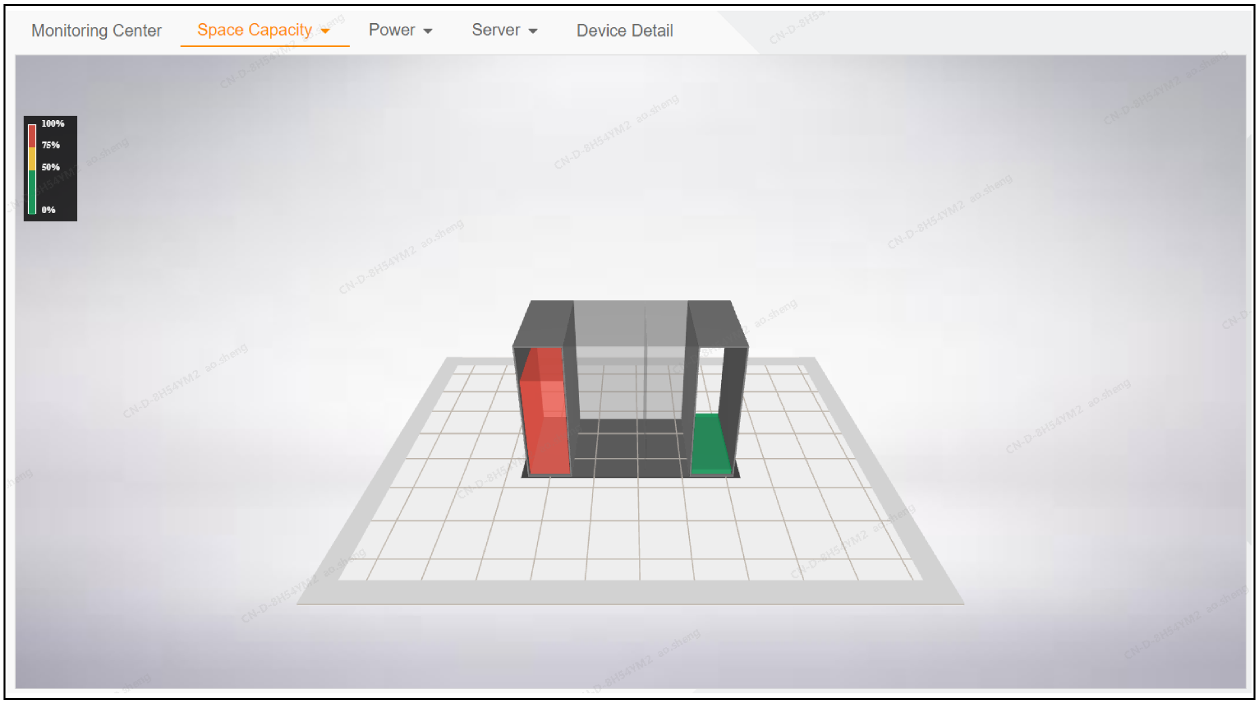
Figure 6.52 SPM Cabinet Status Card



Space 3D View

Navigate to the Space Capacity tab , as illustrated in **Figure 6.53** on the facing page . This module displays each cabinet's space usage at the current site using color-coded 3D blocks. You can rotate, zoom, and pan the view for better visibility.

Figure 6.53 Smart Row Site Space Capacity 3D View



Power Capacity 3D View

Navigate to the Power Capacity tab, as illustrated in **Figure 6.54** on the next page . This view displays each cabinet's power distribution usage at the current site using color-coded 3D blocks. You can rotate, zoom, and pan the view. Click on a cabinet to focus on it and view its total distribution capacity and current power usage.

Figure 6.54 Power Capacity 3D View of Smart Row Site

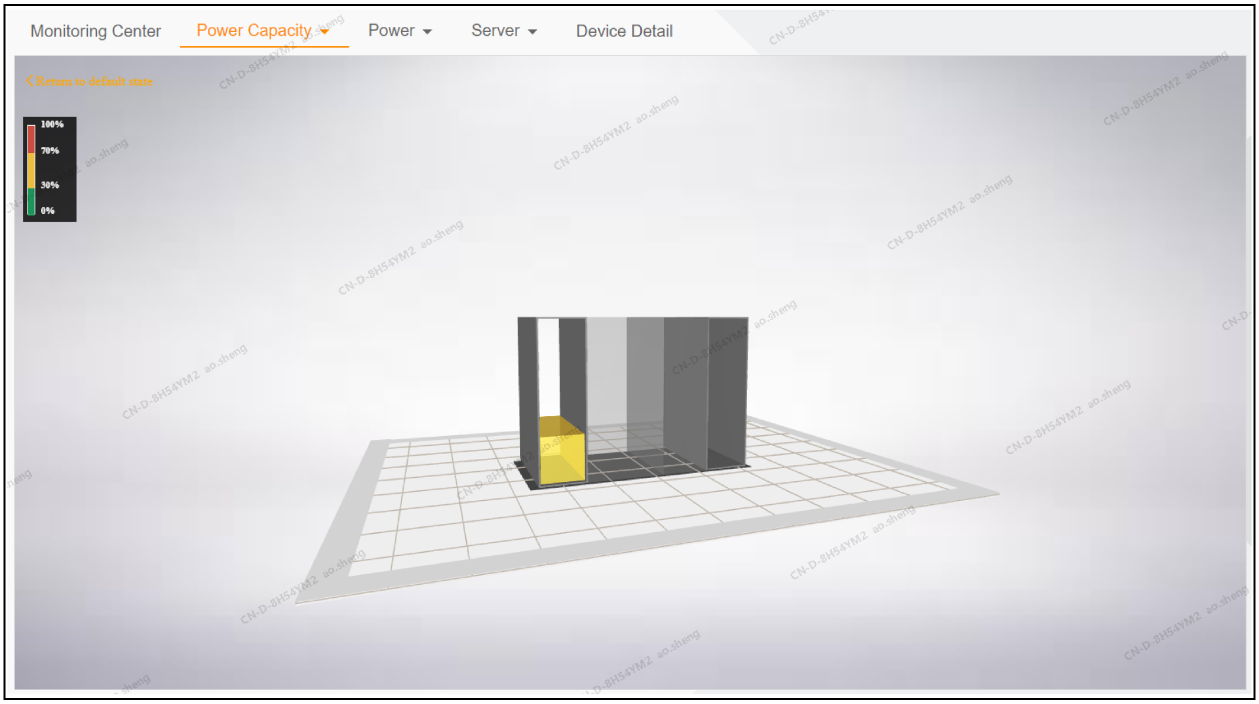
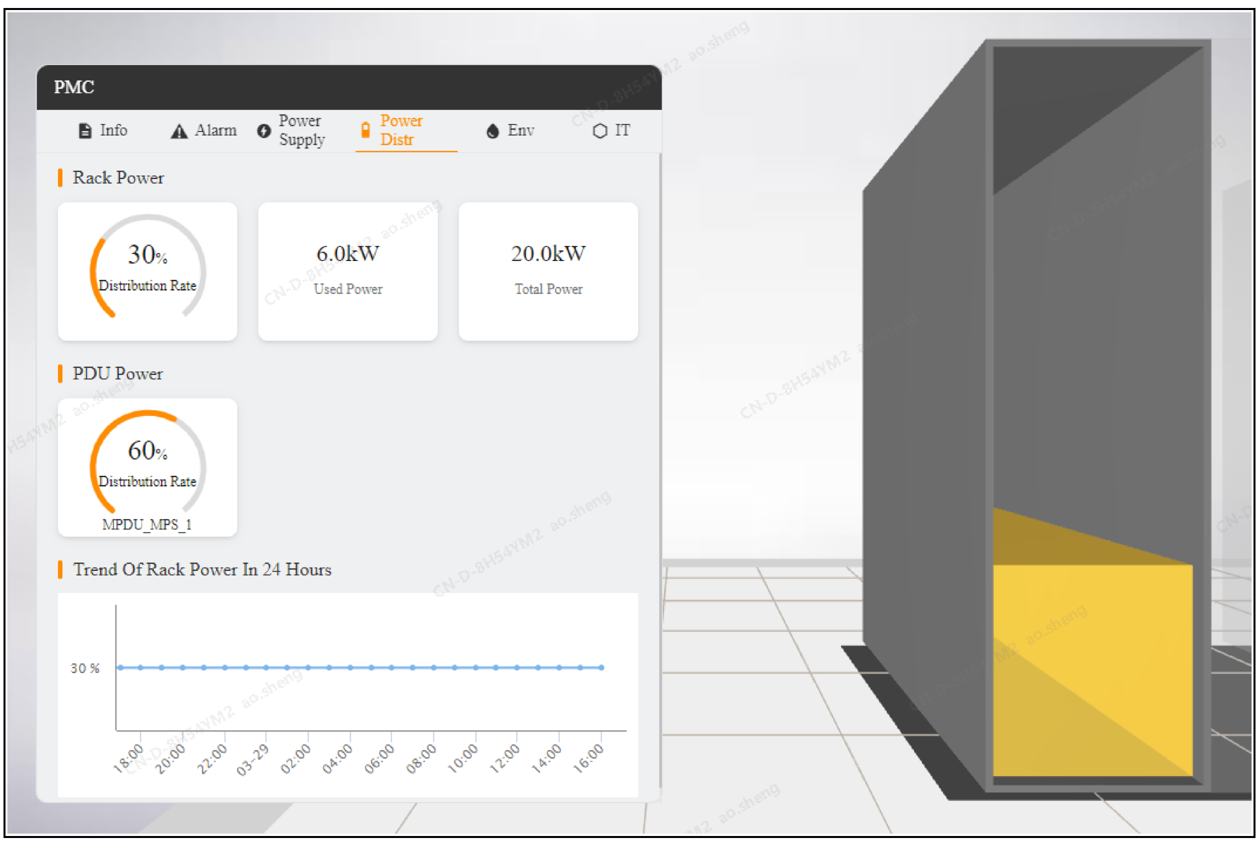


Figure 6.55 Power Capacity of a PMC Cabinet



Temperature Label 3D View

Click on the Thermal View tab to access the Temperature Label 3D view, as illustrated in **Figure 6.56** below . The cabinets display upper, middle, and lower temperature labels. The temperature labels are configured in the 3D Configuration of the cabinet. You can modify maximum and minimum temperatures by adjusting the settings in the temperature bar on the left. The label colors in the cabinet will change according to these settings.

Figure 6.56 Temperature Label 3D View of Smart Row Site

Figure 6.57 Temperature Label and Environmental Information of a PMC Cabinet

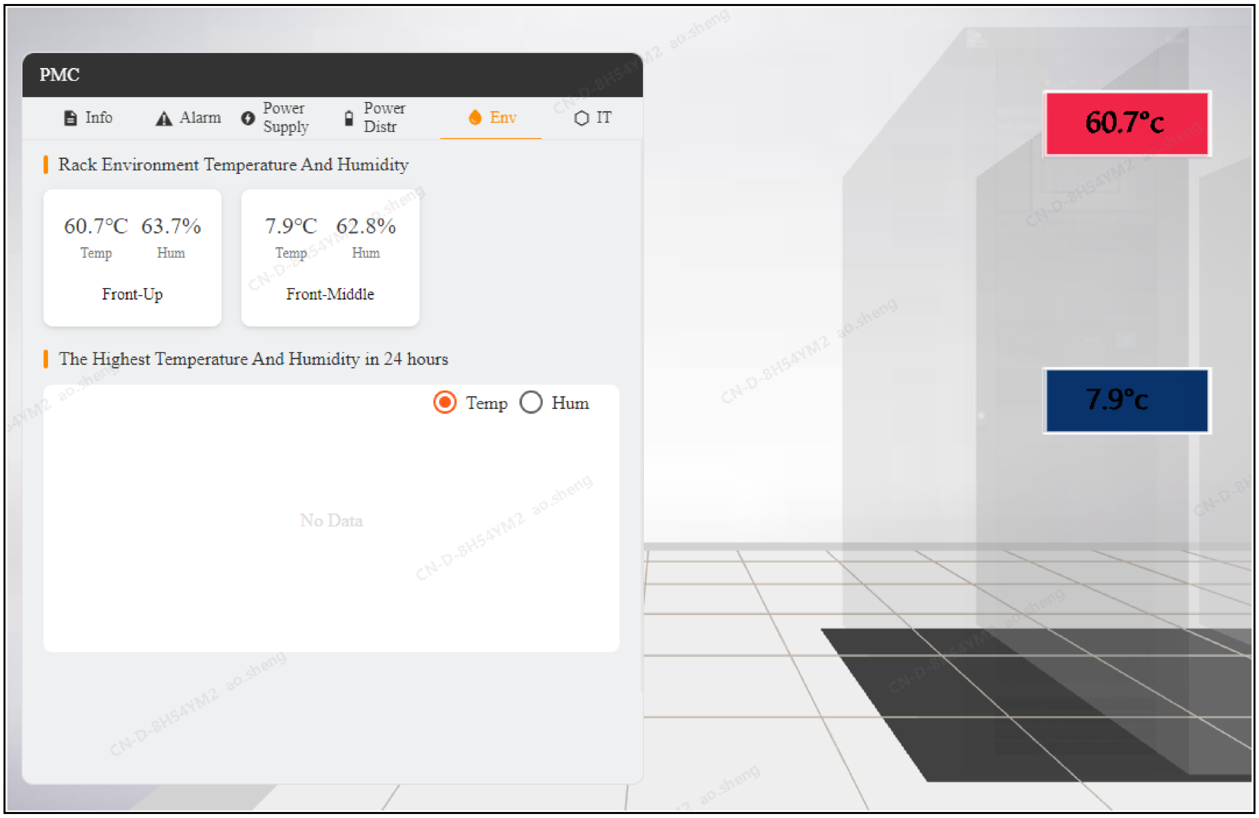
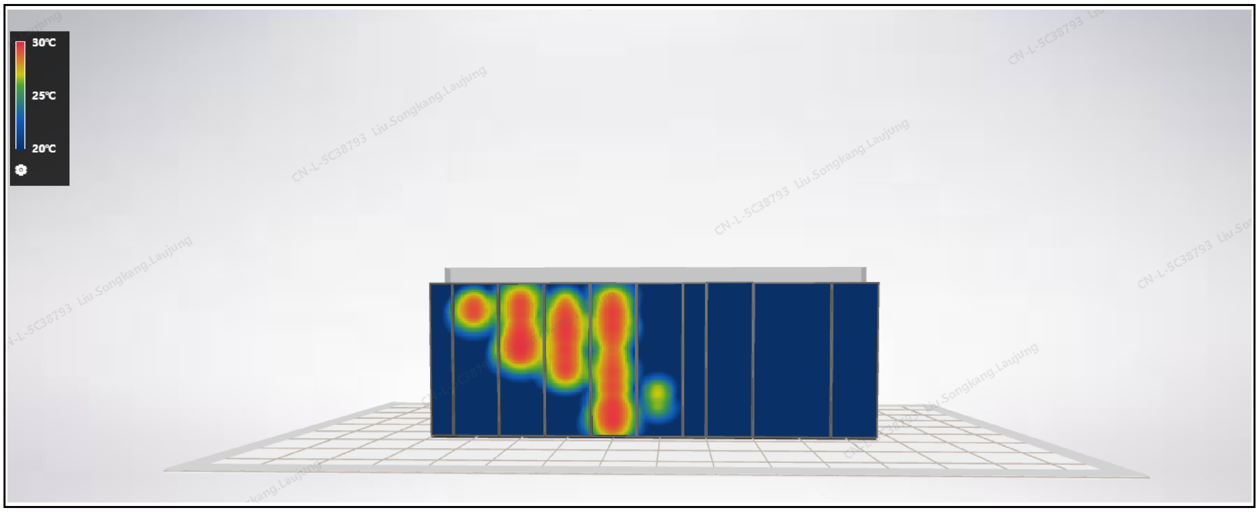


Figure 6.58 The color of the Label Changes after Adjusting the Temperature Range

Heatmap

Navigate to the Heat map tab to access the Heat map 3D view, as shown in Figure 6.59 below . This module displays temperature monitoring for IT equipment at the Smart Row site. You can adjust the temperature range by clicking the Settings icon on the temperature bar to the left. The cabinet temperature display will update accordingly.

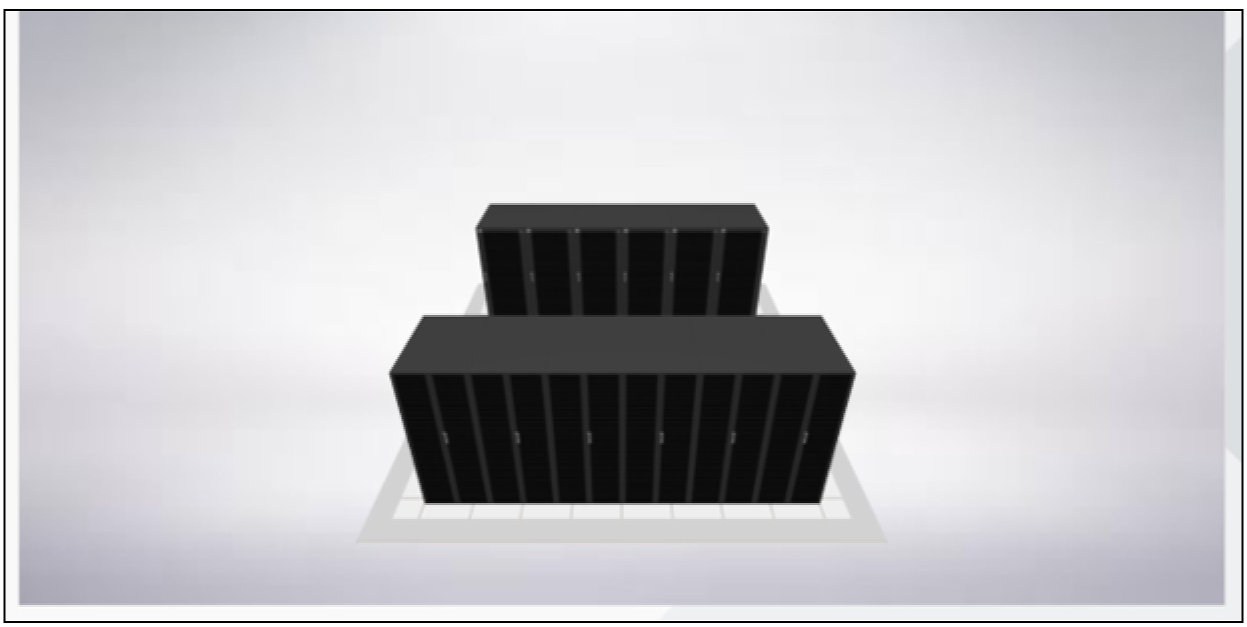
Figure 6.59 Heat Map 3D View of Smart Row Site



6.2.4 CREMS Site 3D Visualization

The 3D module of the CREMS site is the same as the 3D module of the SmartAisle (SA2.0, SA3.0) site. As shown in Figure 6.60 below .

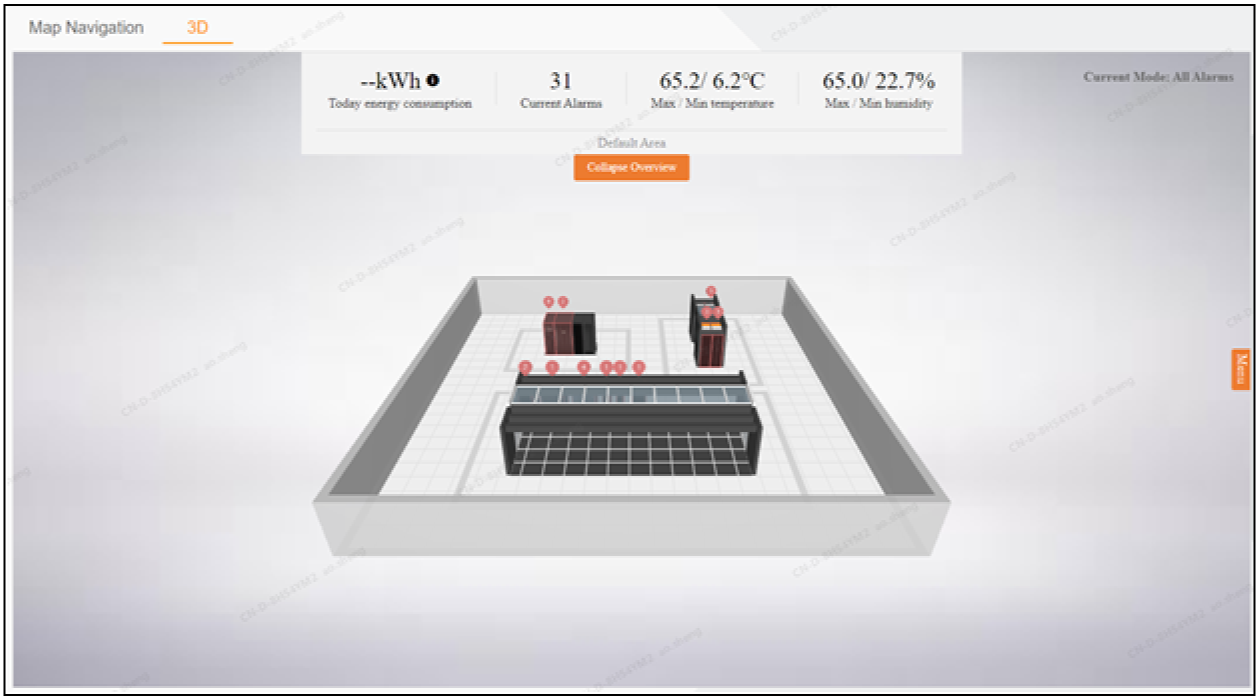
Figure 6.60 3D View of CREMS Site



6.2.5 Location 3D Visualization

Click a location node on the monitoring tree, and then select the 3D tab on the right side of the tab page to enter the location-level 3D view. The 3D view of the location displays all the 3D Location models of sites. The details are shown in **Figure 6.61** below .

Figure 6.61 Location-Level 3D Module

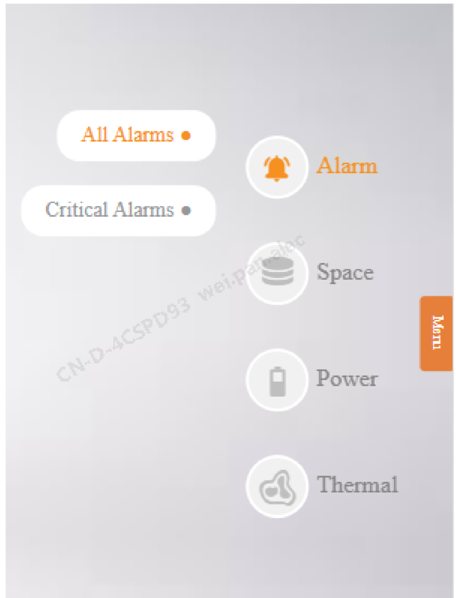


The Overview panel displays the total energy consumption for all sites in the 3D view. It also shows the number of active alarms across all sites, as well as the maximum and minimum temperature and humidity readings from all sites.

Change Display Mode

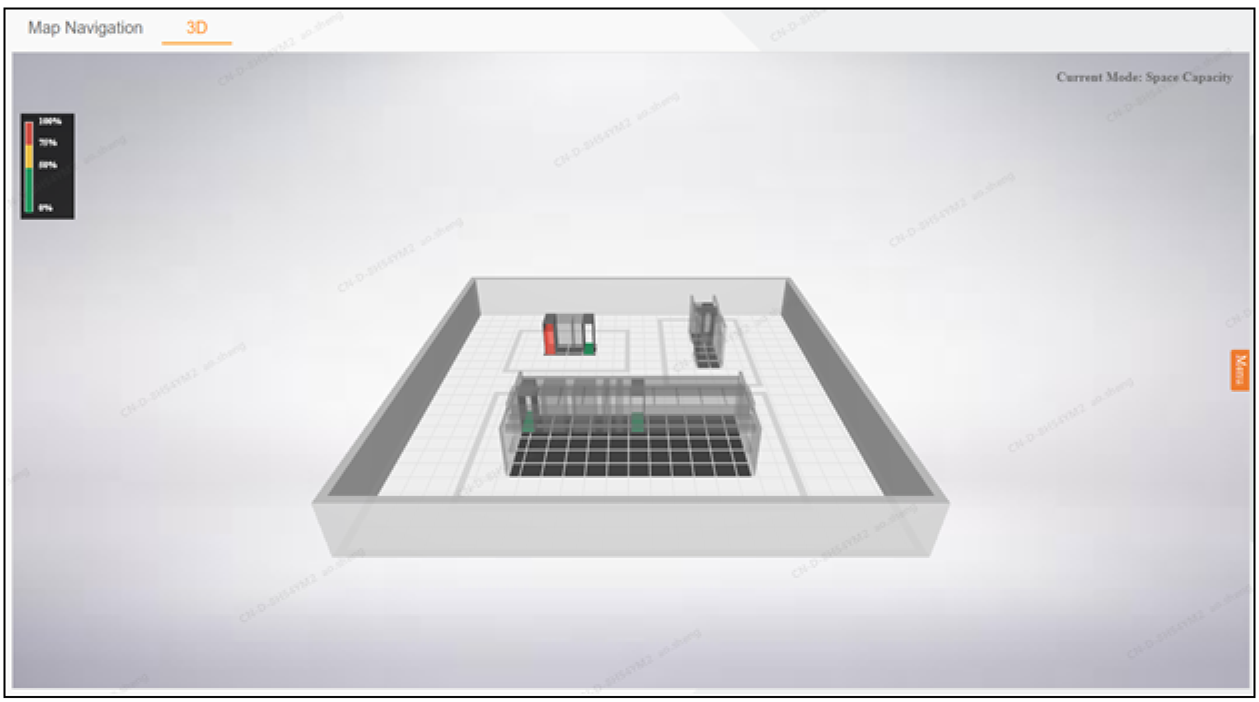
Click the function menu on the right side to change the location 3D view to other modes.

Figure 6.62 Changing Mode



For example, when you change to the space mode, the space capacity of different sites in the location is displayed. The details are shown in Figure 6.63 below .

Figure 6.63 Location-Level 3D Module—Space Capacity



Similarly, you can change to other modes to check with the power capacity, temperature labels and heat map of all sites under the location.

6.2.6 Battery Room Site 3D Visualization

Entrance to the 3D module of the battery room

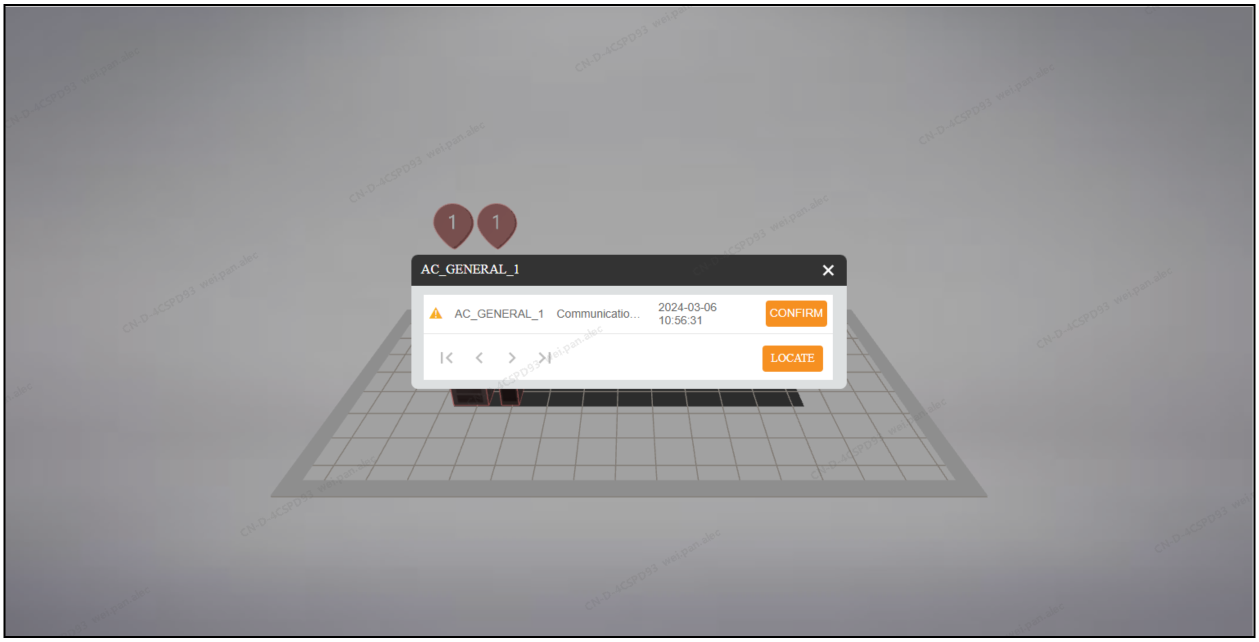
Click on a *battery room site* on the monitoring tree, and click on the 3D tab page on the right side of the tab page to enter the 3D module. As shown in **Figure 6.64** below .

Figure 6.64 3D View of Battery Room Site

In the 3D view of the battery room site, all assets include the floor UPS, lead-acid battery racks, lithium battery cabinets, etc will be displayed. You can click on each device to open the device detail panel. The running status points and alarms status can be seen from the panel.

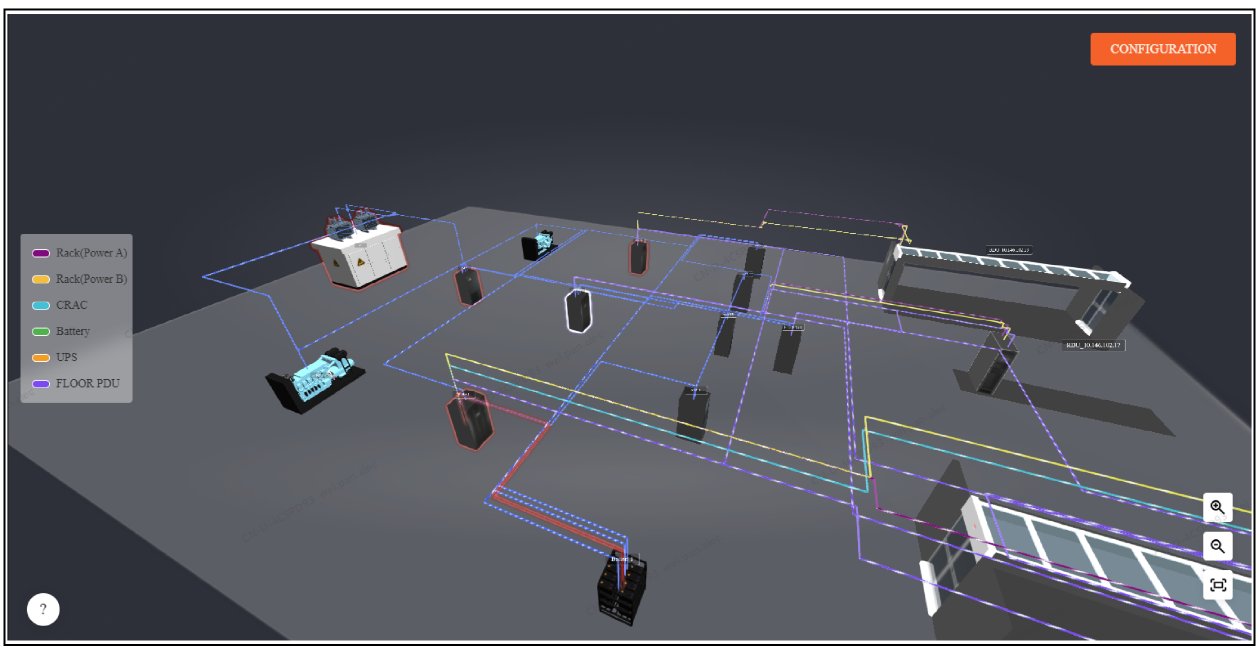
Click the alarm popup at the top of a device to pop up the relevant alarm content, as shown in **Figure 6.65** on the facing page . Click Locate to quickly locate the cabinet or UPS cabinet where the problem has occurred.

Figure 6.65 Region-Level 3D Module—Alarm Popup



6.2.7 Power Train Diagram 3D Visualization

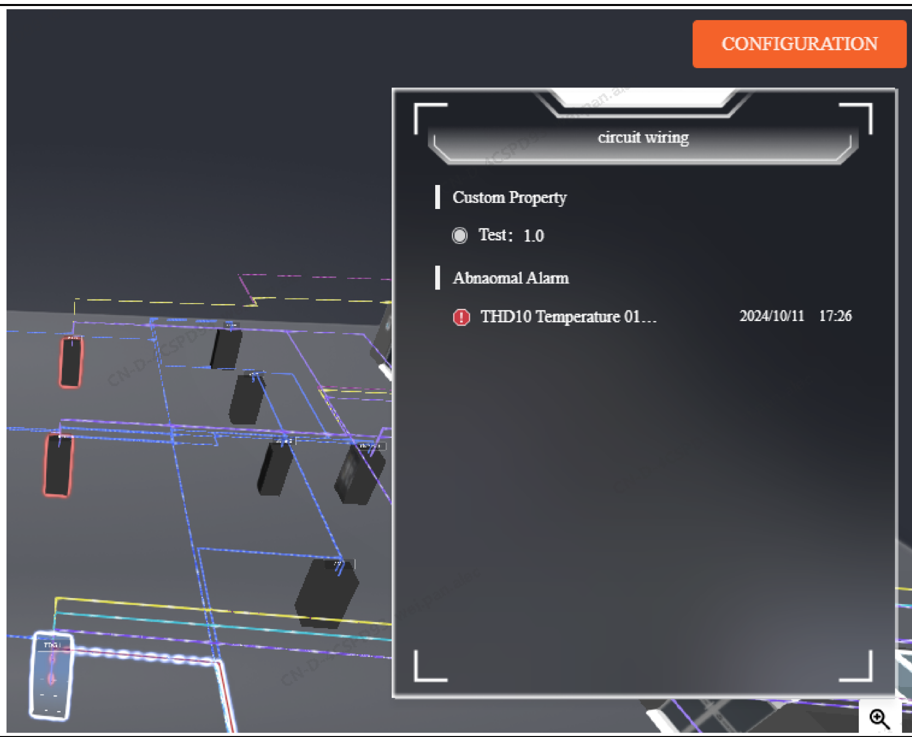
In display mode of Power Train, you can view the detail of the configured power train.



You can also view the power configuration panel of a specific device, and after clicking on the device, the currently selected panel will pop up, displaying the signal and alarms and other information.

Click on the circuit connection to see the alarms and attributes of the circuit connections between devices, as shown in Figure 6.66 below .

Figure 6.66 Alarm Attributes



7 Single-Site Power Distribution and Thermal

7.1 General

7.1.1 Overview

In the Power Distribution/Cooling tab page of the monitoring home page, users can view the power distribution and Cooling related professional information under the current site.

7.1.2 Functional Modules

The power distribution/refrigeration tab page contains the following functional modules, please refer to the Detailed Features about each functional module.

- Three-phase unbalance
- Hourly maximum power trend
- Bar Chart of energy consumption
- UPS topology diagram
- Air conditioning status
- Alarms related to air conditioning
- Comparison between the supply air temperature and the return air temperature of multiple air conditioners
- Comparison of cold and hot aisle temperatures of multiple air conditioners

7.2 Quick Start

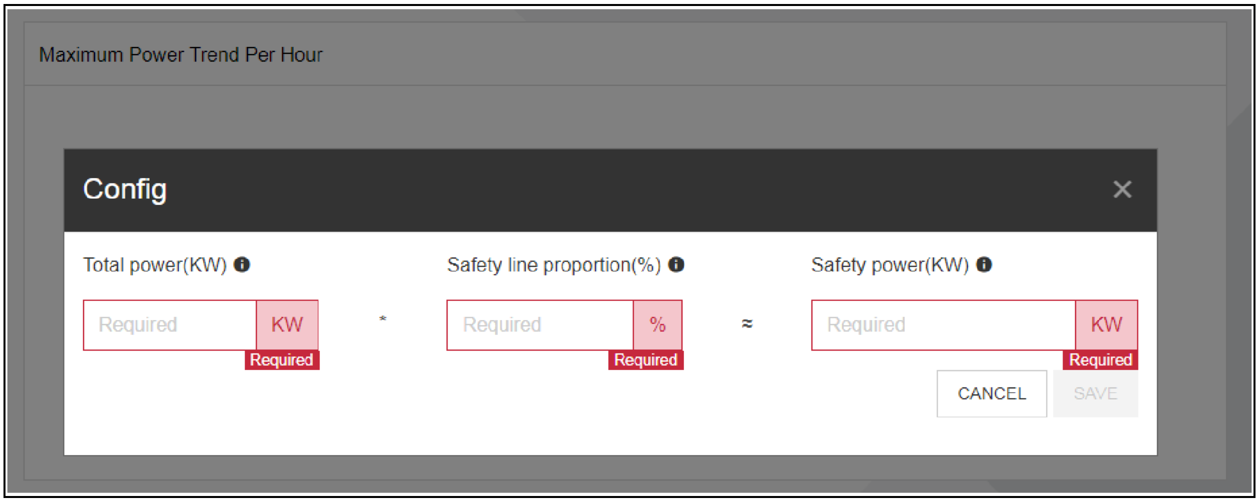
7.2.1 Rapid Deployment Steps

1. Open Smart InfraSight™ and click on the region; For a site in the site tree, click the tab page on the right to enter the power distribution professional interface.
2. To configure the Hourly Maximum Power Trend widget module, click the function menu in the upper right corner of the widget, and configure the relevant information in the configuration pop-up window.
3. To configure the widget module of the energy consumption Bar Chart, you need to add the energy consumption configuration scheme to the energy consumption module first.
4. Click on the air conditioning tab at the top to enter the professional interface.
5. Configure the multi-air conditioner supply air temperature and return air temperature comparison widget module, click the function menu in the upper right corner of the change widget, and configure the relevant information in the configuration pop-up window.

7.2.2 Example

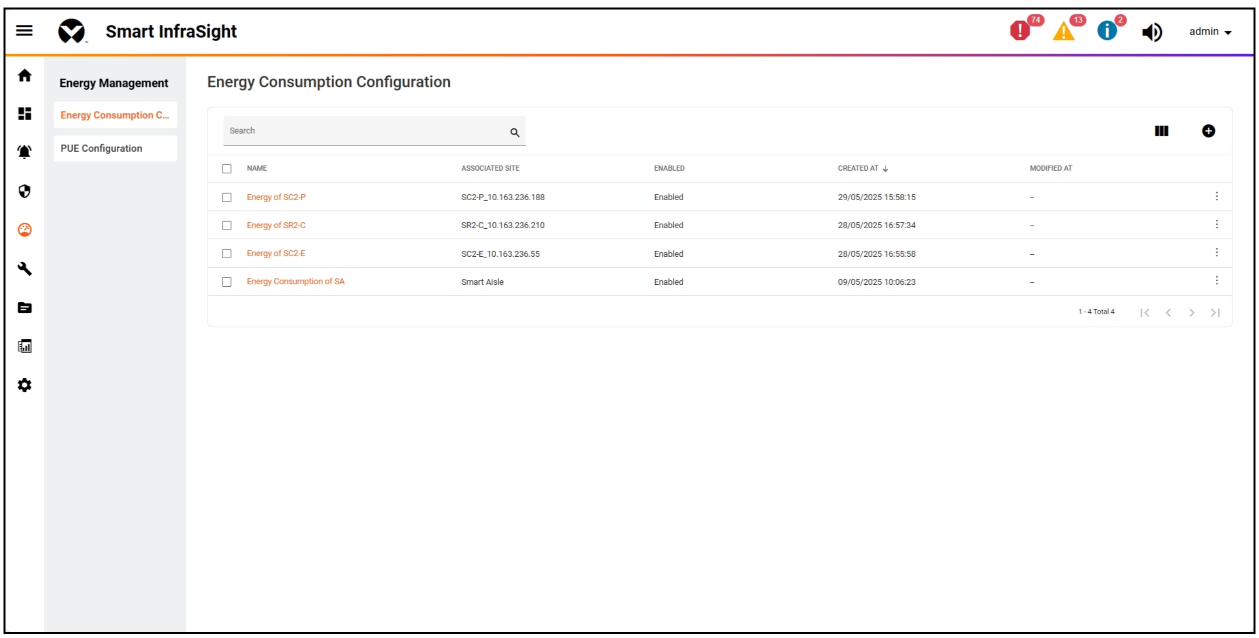
Configuration Steps in the Power Distribution Professional Interface

Figure 7.1 Hourly Maximum Power Trend Configuration



Click the function menu in the upper right corner of the Hourly Maximum Power Trend widget module as shown in **Figure 7.1** above , configure the safety line ratio and other related information of the power in the configuration pop-up window, and then *save*.

Figure 7.2 Energy Consumption Configuration in the Energy Consumption module



For the configuration of the energy consumption Bar Chart widget module, it is described in detail in the energy consumption configuration menu, and the specific steps refer to the Detailed Features .

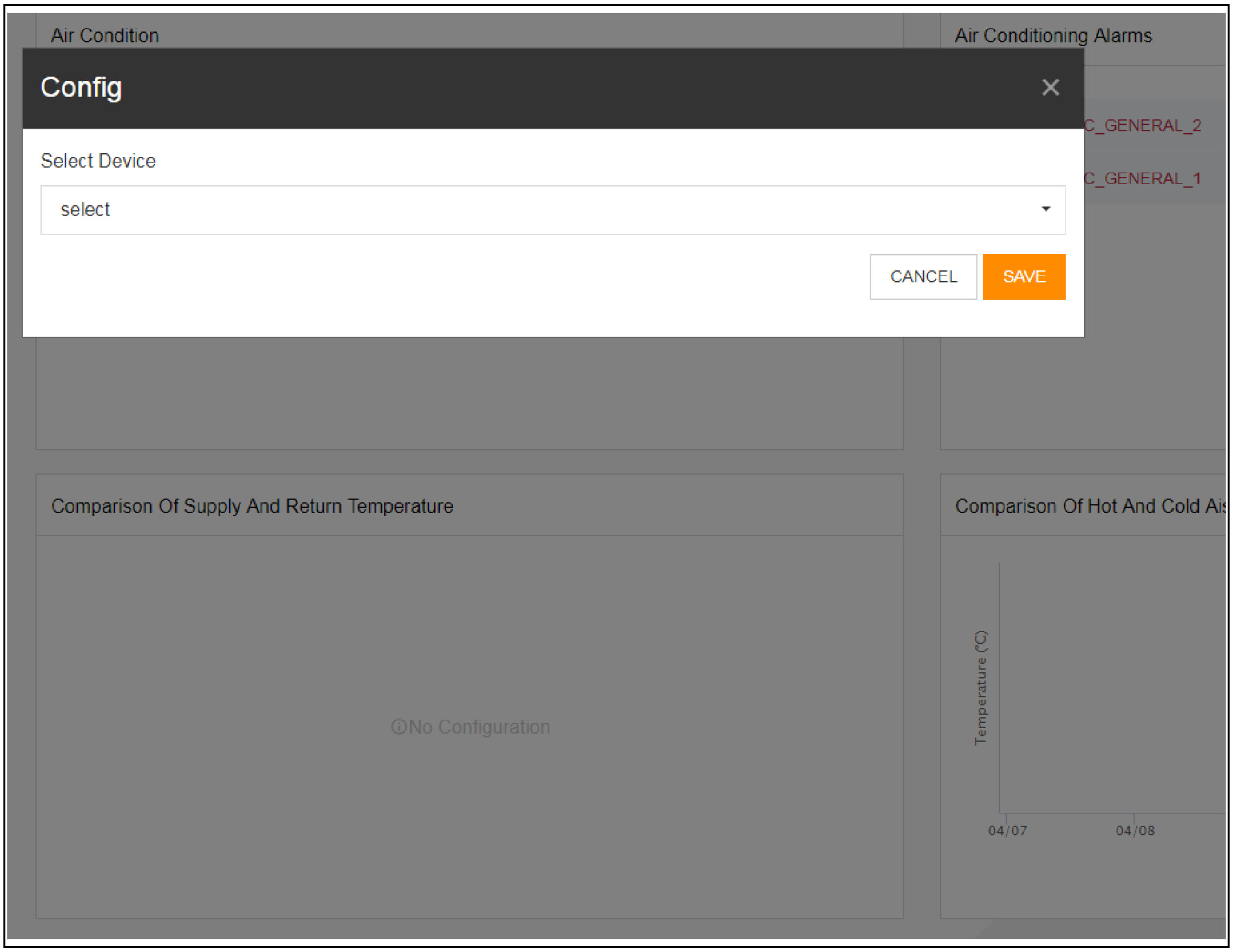
Then you can see all the information in the power distribution professional interface.

Figure 7.3 Configuration Steps in the Professional Interface

Click the function menu in the upper right corner of the multi-air conditioner supply air temperature and return air temperature comparison widget module, and select the name of the target air conditioner and other relevant information in the configuration pop-up window.

Click *save*. Then the information in the refrigeration professional interface is available.

Figure 7.4 Multiple Air Conditioner Configuration

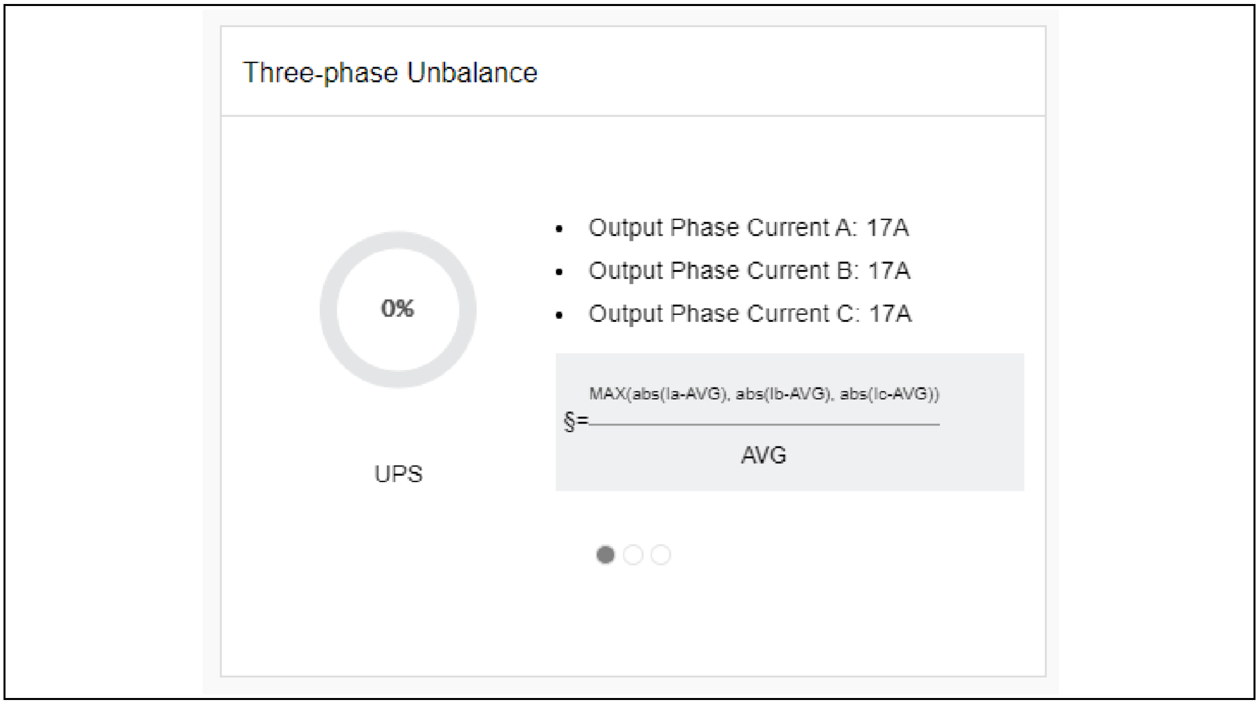


7.3 Detailed Features

7.3.1 Browse the Power Distribution Professional Interface

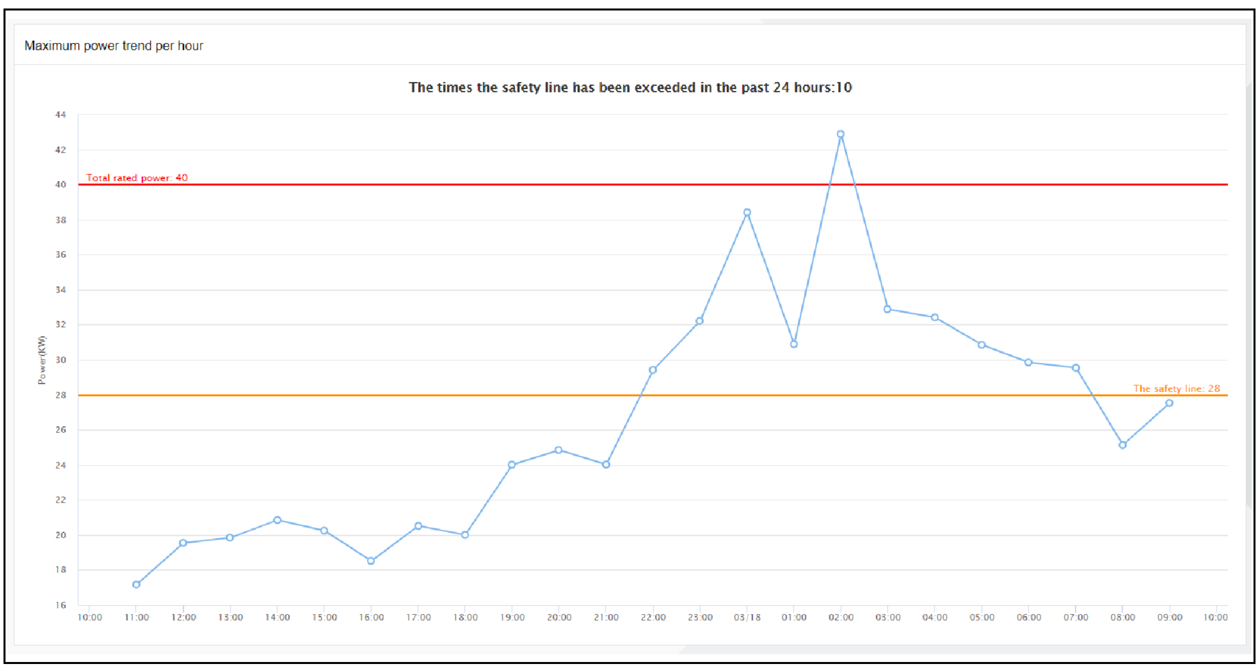
In the professional interface of power distribution, there are widget modules such as three-phase unbalance, hourly maximum power trend, energy consumption Bar Chart, UPS topology diagram, etc. In the three-phase unbalance widget module as shown in Figure 7.5 on the next page , the three-phase unbalance degree of each UPS device under the current site is displayed.

Figure 7.5 Three-Phase Unbalance



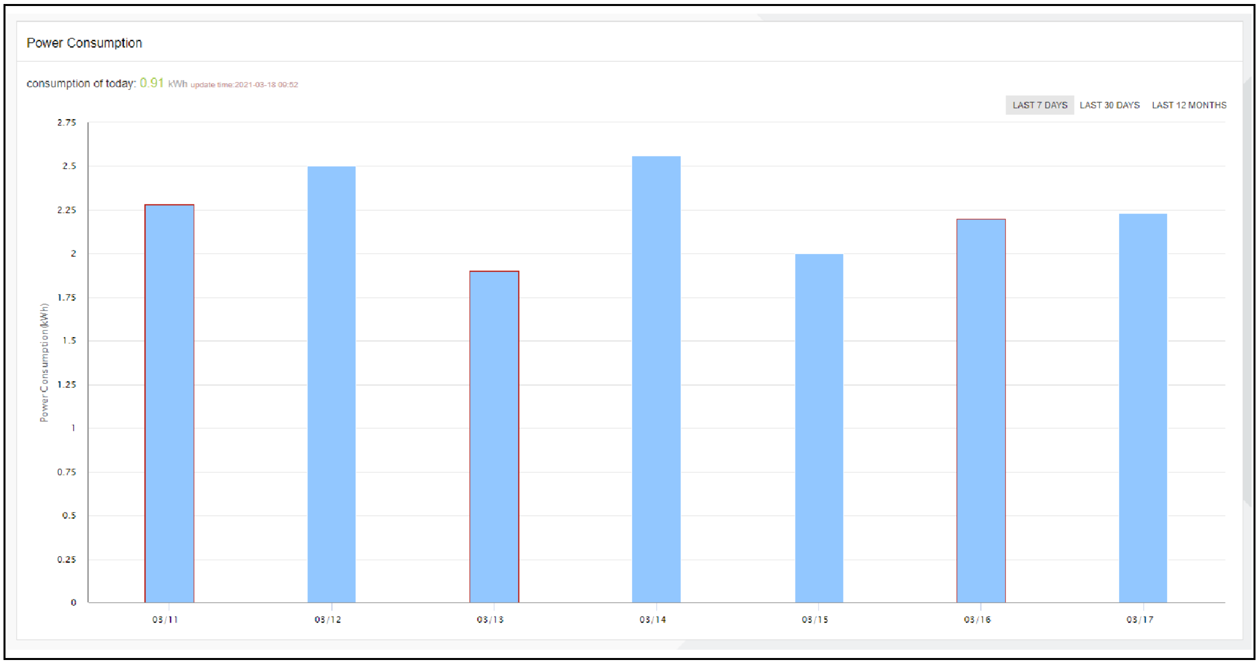
In the Hourly Maximum Power Trend widget as shown in Figure 7.6 below , the maximum power trend of all UPS devices in the current site in the past 24 hours is displayed.

Figure 7.6 Hourly Maximum Power Trend



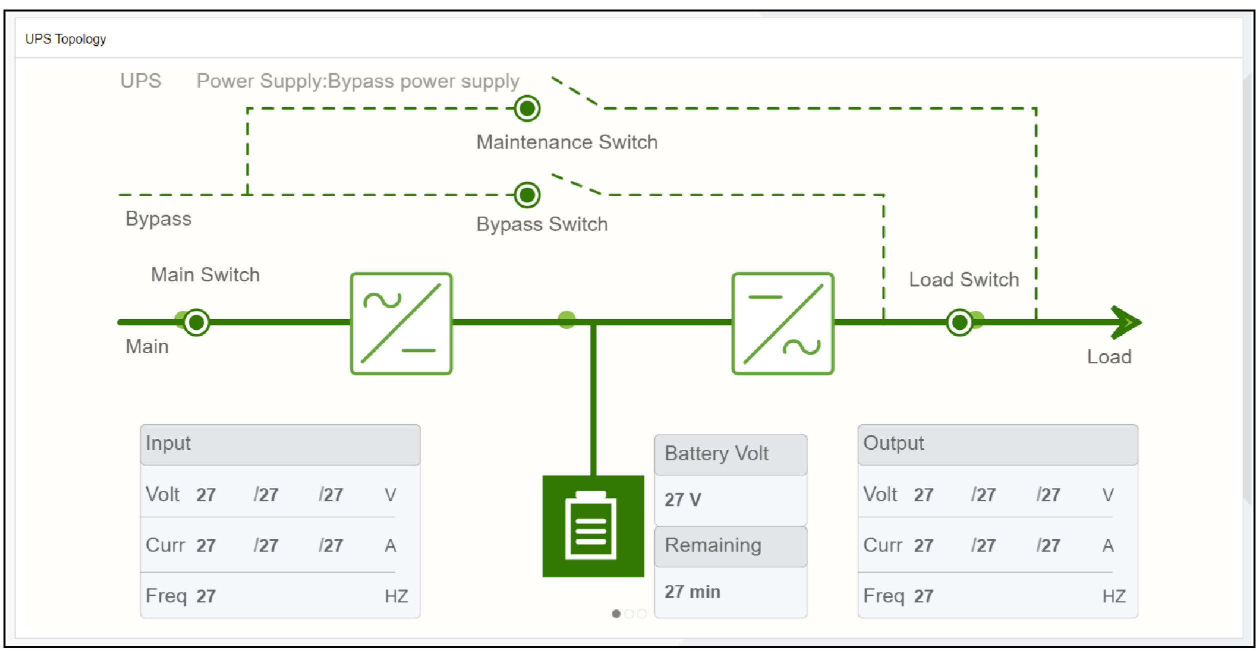
In the energy consumption Bar Chart widget module as shown in **Figure 7.7** below , the energy consumption information such as the total energy consumption of the current site in the past and today is displayed. The content of the Bar Chart can be switched between the last 7 days, the last 30 days, and the last 12 months.

Figure 7.7 Bar Chart of Energy Consumption



In the UPS topology widget module, the flow chart information of each UPS device under the current site is displayed.

Figure 7.8 UPS Topology



7.3.2 Browse the Refrigeration Professional Interface

In the professional interface, there are widget versions such as air conditioning status, air conditioning related alarms, comparison of air supply temperature and return air temperature of multiple air conditioners, and temperature comparison of hot aisles of multiple air conditioners.

In the air conditioning status widget module, the status information of each air conditioning device under the current site is displayed.

Figure 7.9 Air Conditioning Status

Air Condition

TeamWork Entrance

Name	Switch State	Cooling State	Supply/Return Temperature	Return Humidity
AC_CRV+_3	Run	Yes	11.0/11.0°C	11.0%
AC_CRV+_2	Standby	Yes	11.0/11.0°C	11.0%
AC_CRV+_1	Standby	Yes	11.0/11.0°C	11.0%
AC_SRVII_1	lockdown	NotIn	11.0/11.0°C	11.0%
AC_SRVII_2	Running	NotIn	11.0/11.0°C	11.0%
AC_CRV4025_1	Panel shutdown	On	11.0/11.0°C	11.0%
AC_SRVII_3	backup	NotIn	11.0/11.0°C	11.0%
AC_CRV4025_2	Monitor shutdown	On	11.0/11.0°C	11.0%
AC_CRV4025_3	Remote shutdown	On	11.0/11.0°C	11.0%
AC_GENERAL_1	Standby	On	11.0/11.0°C	11.0%
AC_GENERAL_2	Off	Off	11.0/11.0°C	11.0%
AC_GENERAL_3	Run	On	11.0/11.0°C	11.0%

In the air conditioner-related alarm widget module, the alarm information of each air conditioner device under the current site is displayed.

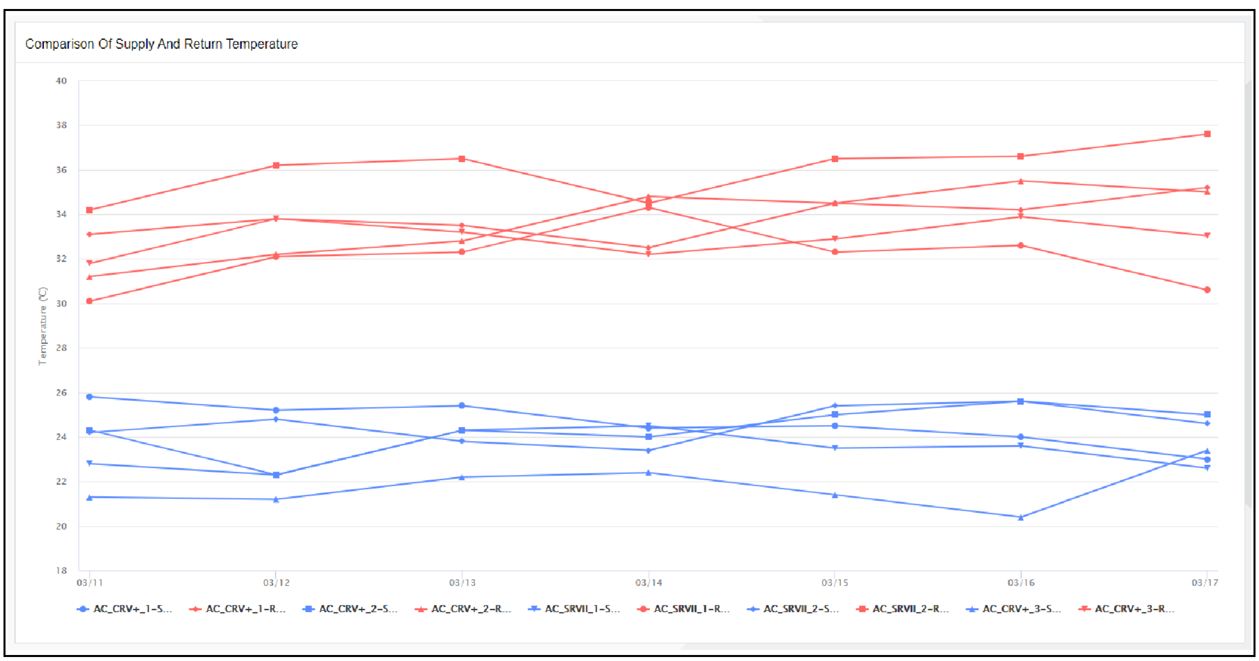
Figure 7.10 Air Conditioner Alarms

Air Conditioning Alarms

1	AC_CRV4025_1	CommunicationFailure	2021-03-16 15:30:56
2	AC_CRV+_1	CommunicationFailure	2021-02-26 11:07:01
3	AC_CRV+_1	Exhaust temperature alarm	2021-02-25 18:58:01
4	AC_CRV+_1	Airflow loss alarm	2021-02-13 23:23:01
5	AC_CRV+_1	Filter clogged alarm	2021-02-11 23:58:01
6	AC_CRV+_1	Power lose phase alarm	2021-02-05 18:02:01
7	AC_CRV4025_1	Loss Of Power Alarm	2021-02-01 18:15:01
8	AC_CRV4025_1	Loss Of Airflow Alarm	2021-01-25 19:42:52
9	AC_CRV+_1	Low Pressure Lock alarm	2021-01-25 18:58:01
10	AC_CRV4025_1	Supply Air High Temperature Alarm	2021-01-24 22:44:34
11	AC_CRV4025_1	Lighting Protection Alarm	2021-01-22 19:22:23
12	AC_CRV4025_1	Smoke Detector Alarm	2021-01-20 03:12:12
13	AC_CRV4025_1	Remote Shutdown Alarm	2021-01-10 03:06:01
14	AC_CRV4025_1	Power Frequency Offset Alarm	2021-01-01 18:20:01

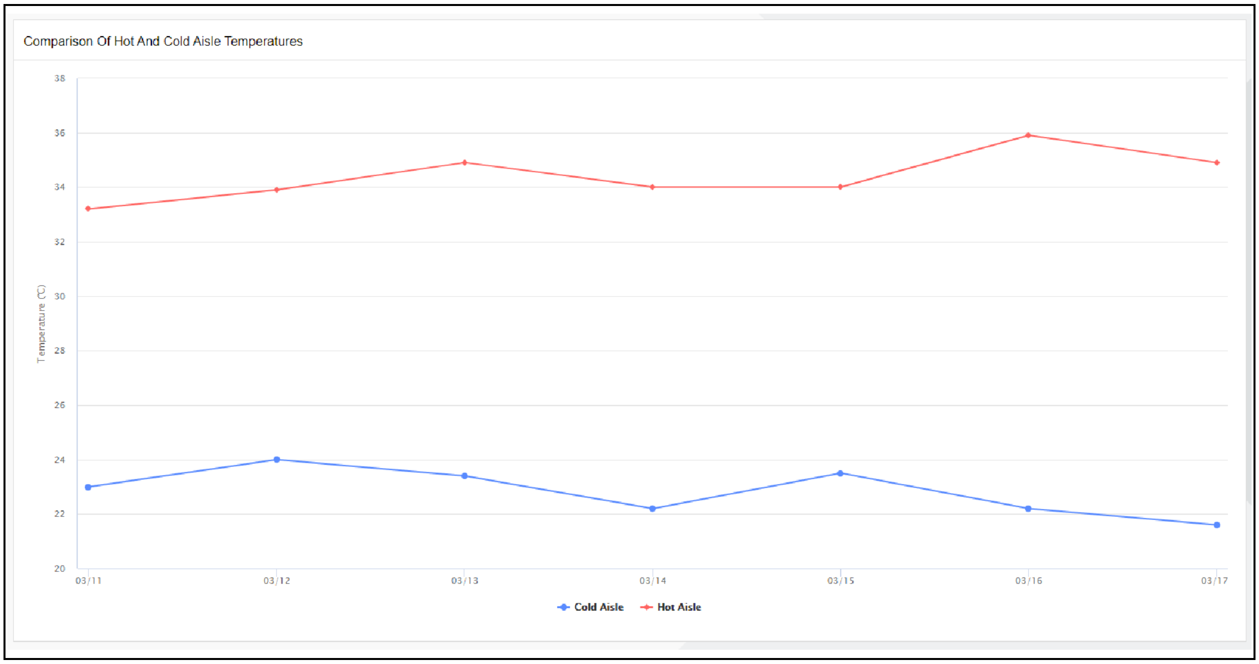
In the Multi-Air Conditioner Supply Air Temperature and Return Air Temperature Comparison widget module, the line information of the supply air temperature and return air temperature of the selected air conditioner at the current site is displayed

Figure 7.11 Comparison of Hot and Cold Aisle Temperatures of Multiple Air Conditioners



In the Multi-Air Conditioner Hot Aisle Temperature Comparison widget, the maximum return air temperature and minimum supply air temperature of all air conditioners in the current site in the past 7 days are displayed.

Figure 7.12 Comparison of Hot and Cold Aisle Temperatures of Single Air Conditioner



8 IT Management

8.1 General

8.1.1 Overview

The IT management function monitors and manages IT devices connected via the RDU501 collector through server management and console device management functions.

8.1.2 Functional Modules

The IT management function includes the following functional modules, refer to Detailed Configuration below for detailed information about each functional module.

- User Authentication Configuration
- Server Management
- Console Device Management

8.2 Quick Start

8.2.1 Rapid Deployment Steps

To use the IT management function to manage server and console devices, you need to configure the following configurations:

1. Open a browser, open the RDU501 webpage and login, create a new administrator user in the user management of the RDU collector, and remember the Username and password.
2. Open Smart InfraSight™ with a new browser, navigate to Monitoring, in Monitoring Tree, find the site that is related to the RDU501, click the ellipses(...) on the right side of the site and select User Authentication. (If the RDU501 has not been monitored, please refer to Chapter15 Configuration Tool and monitor the RDU501).
3. Enter the Username and password. After the User Authentication complete, click the site's name and click the Server tab on the right side of the page, all the IPMI devices including servers and console devices will be synchronized from the RDU501 automatically.

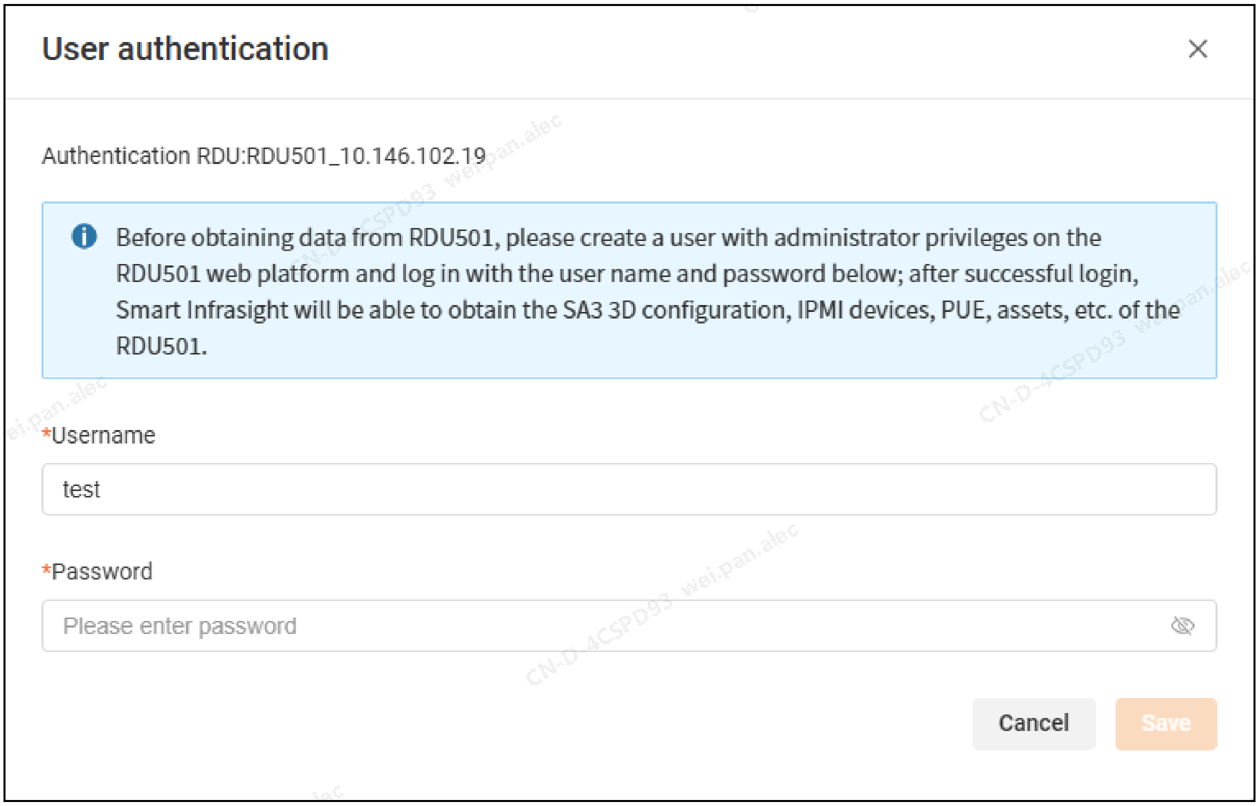
8.3 Detailed Configuration

8.3.1 User Authentication Configuration

The Smart Infrasight system retrieves IPMI device data from the RDU501 using an administrator account. Before managing IT devices, you need to complete user authentication. Follow these steps:

1. Open a new browser and navigate to the RDU501 webpage. Create a new administrator account, noting the username and password. It's recommended to create a dedicated account for Smart Infrasight, as this account cannot be used to access RDU501 web pages while Smart Infrasight is retrieving data.
2. In the Smart Infrasight system, go to Monitoring and locate the corresponding RDU501 site in the monitoring tree. Click the ellipsis (...) next to the site and select User Authentication.
3. Enter the username and password of the newly created RDU501 account and click Save.

Figure 8.1 User Authentication



NOTE: 1 . The RDU collector cannot enable two-factor authentication login.

2. The username and password in the user authentication configuration are the users on the RDU collector and the user must be administrators.

3. The user is used to communicate between the Smart InfraSight™ system and the RDU collector, and must not be occupied, and cannot be used to log in to the RDU collector page.

4. If the user name or password is entered incorrectly, the security policy of the RDU collector will be triggered, resulting in the inability to repeat the authentication, and you need to wait for a certain period of time until the RDU collector lifts the security policy restrictions before you can repeat the authentication.

8.3.2 Server Management Detailed Functions

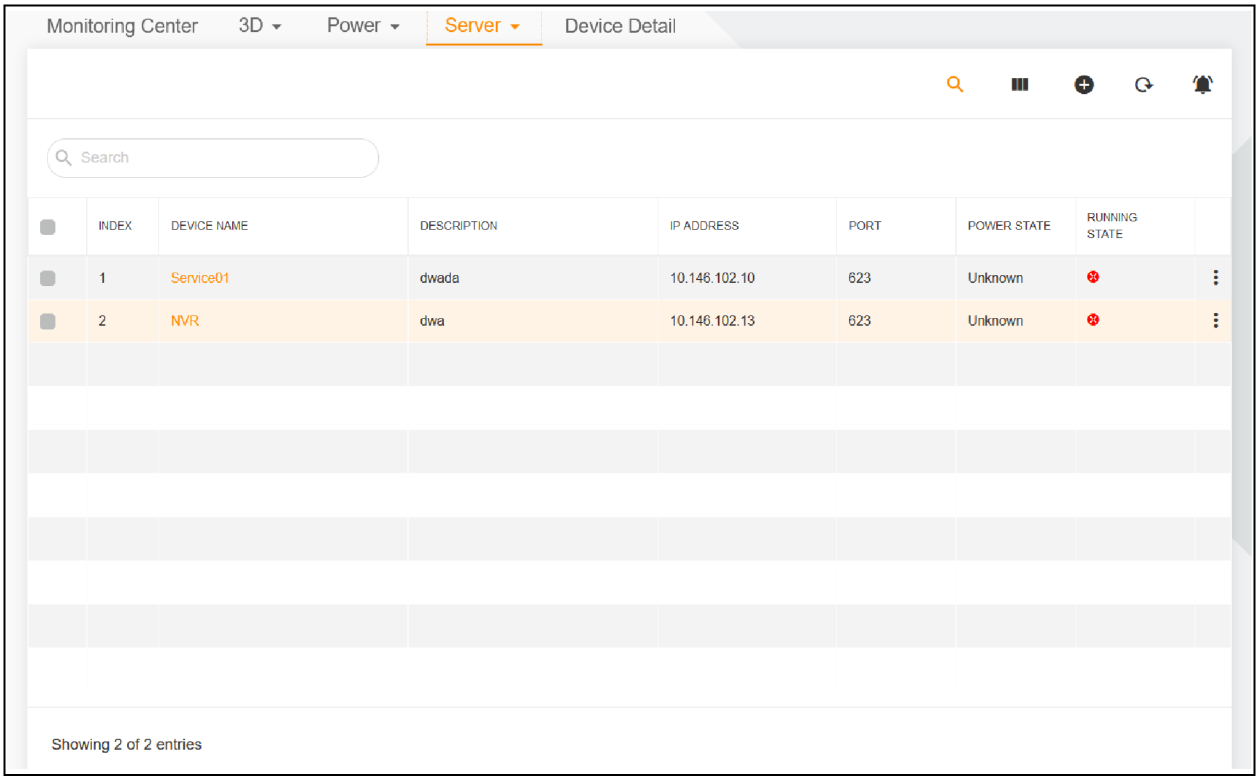
Server management is to manage the IPMI equipment accessed by the RDU501, and the IPMI device specifically refers to the IT equipment accessed through the IPMI2.0 protocol, and its accessibility and communication stability are related to the support ability of the IT equipment itself.

IPMI Device Management

Click on a site in the monitoring tree, if the site supports server management, the **Server** tab will appear in the tab at the top of the right page. Click the **Server** tab to enter the IPMI device management page, as shown in **Figure 8.2** on the facing page . This page lists the IPMI devices connected to the RDU collector, including the serial number, device name, device description, IP address, port, power status, and running status.

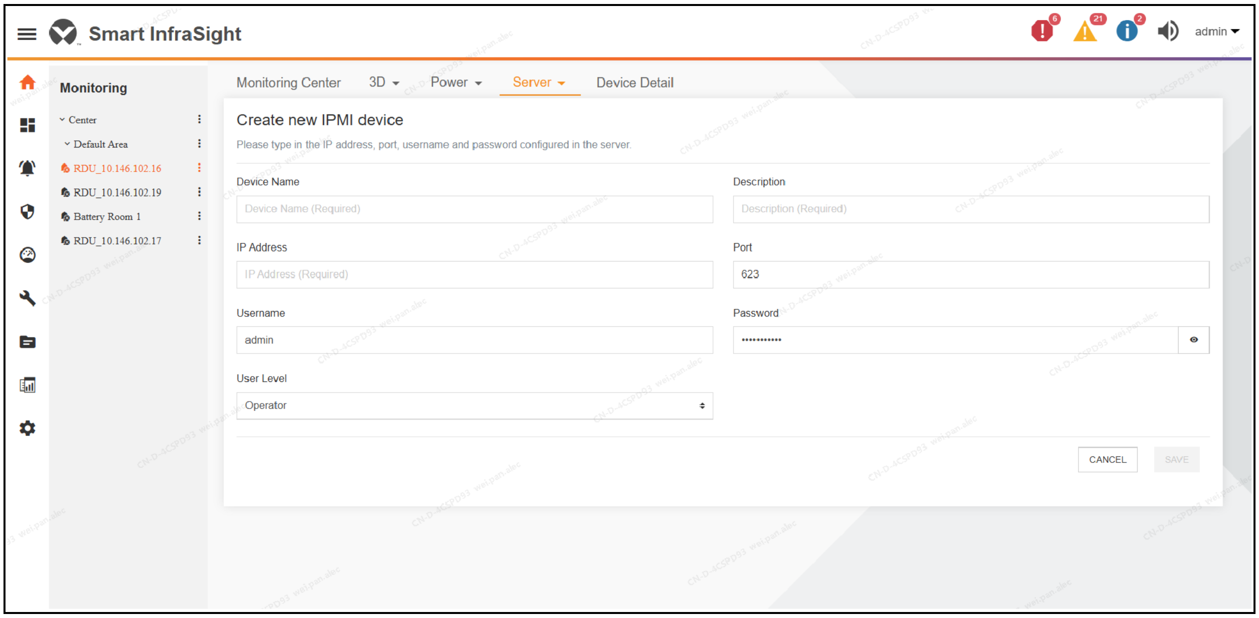
- You can open the **search** box through the button in the upper right corner, and enter content to search for the specific devices.
- You can use the **Add** button in the upper right corner to open the Add IPMI Device page to add a new IPMI device to the system.
- You can use the **Refresh** button in the upper right corner to re-request the IPMI device information on the RDU collector and refresh the IPMI device information in the list.
- You can use the **Alarm** button in the upper right corner to open the alarm management page of the IPMI device.

Figure 8.2 IPMI Device List



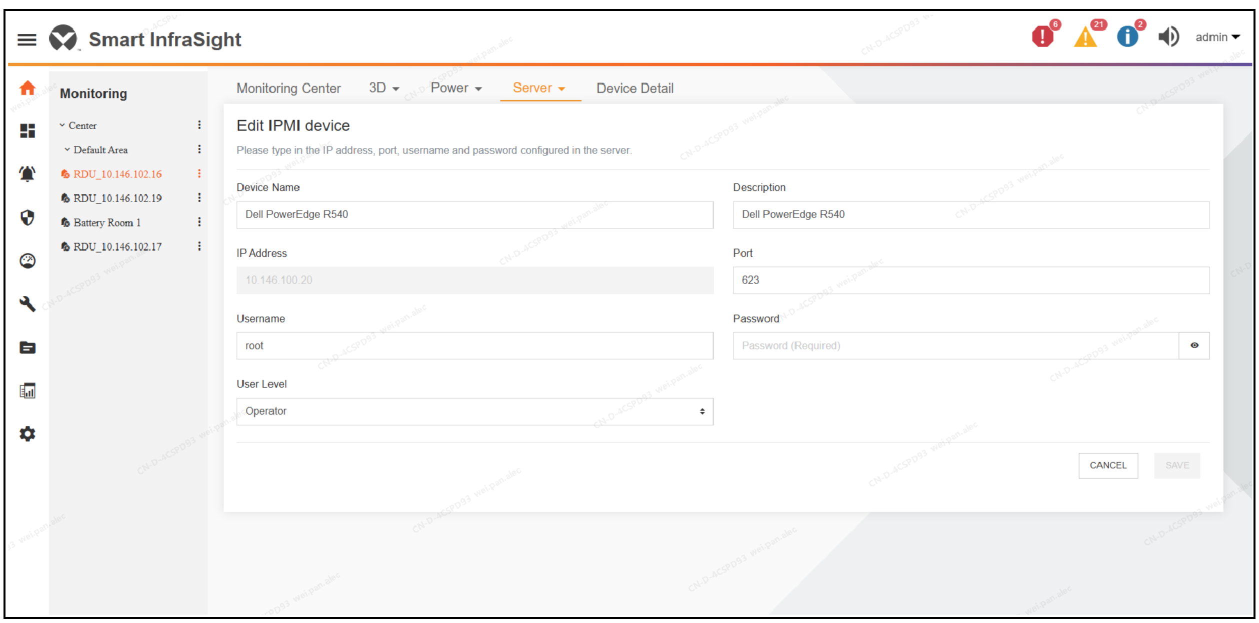
Open the Add IPMI Device page through the Add button on the upper right, enter the IPMI device information (IP address, port, Username, password, and user permissions must be entered correctly according to the configuration of the IPMI device), and then click the Save button, as shown in **Figure 8.3** on the next page . The newly added IPMI device will be added to the RDU collector side synchronously.

Figure 8.3 Adding an IPMI Device



Click the ellipses (...) behind an IPMI device in the IPMI device list and select the *Edit* to open the Edit IPMI Device page, as shown **Figure 8.4** below . Enter the new information of the IPMI device (the IP address is not allowed to be modified, the port, Username, password, and user rights must be entered correctly according to the configuration of the IPMI device), and then click the Save button. The modified information of the IPMI device is synchronized to the RDU collector.

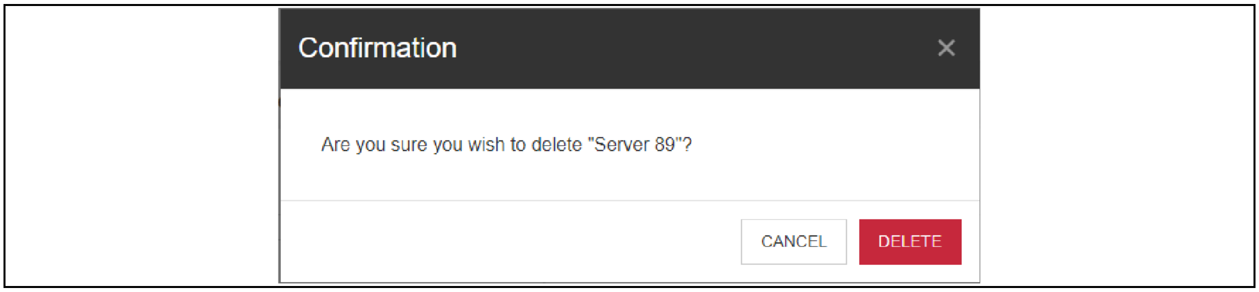
Figure 8.4 Editing the IPMI Device



Click the ellipses (...) behind an IPMI device in the IPMI device list, select the *Delete* button, and a confirmation and deletion window will pop up to delete the IPMI device. As shown in **Figure 8.5** on the facing page .

After you click *Delete*, the IPMI device will be deleted from the system, and the RDU collector will also delete the IPMI device simultaneously.

Figure 8.5 Removing the IPMI Device



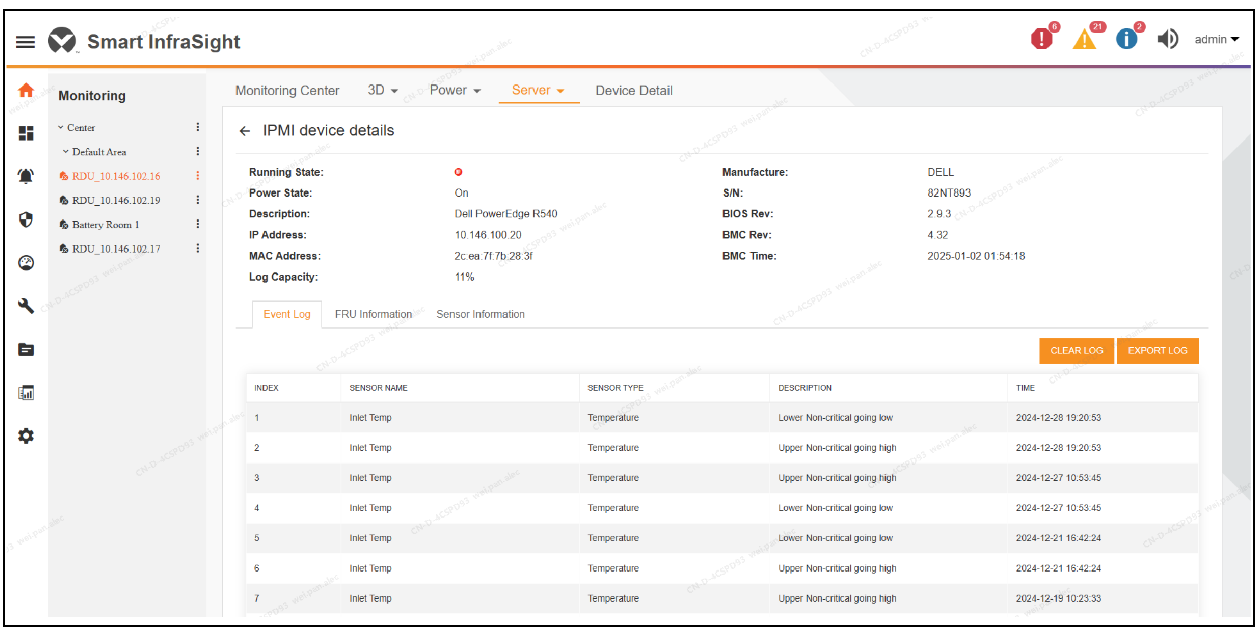
View IPMI Device Details

Click the ellipses (...) behind an IPMI device in the IPMI device list and select View Details to open the IPMI device details page, as shown in **Figure 8.6** below . This page displays the operating status of the IPMI device (green when communication is normal, gray when communication fails, and red when there is an alarm on the device), power status, device description, IP address, MAC address, log storage capacity, manufacturer, serial number, BIOS version, BMC version, BMC time.

Click the Event Logs tab on the IPMI device details page to display the event logs of the IPMI device in separate pages. All event logs can be downloaded by clicking on the **Export Logs** button. Click the **Clear Log** button to clear all event logs for that device.

Click the FRU Information tab on the IPMI device details page to display the attributes and values of the FRU System Board in several pages.

Figure 8.6 IPMI Device Details Page

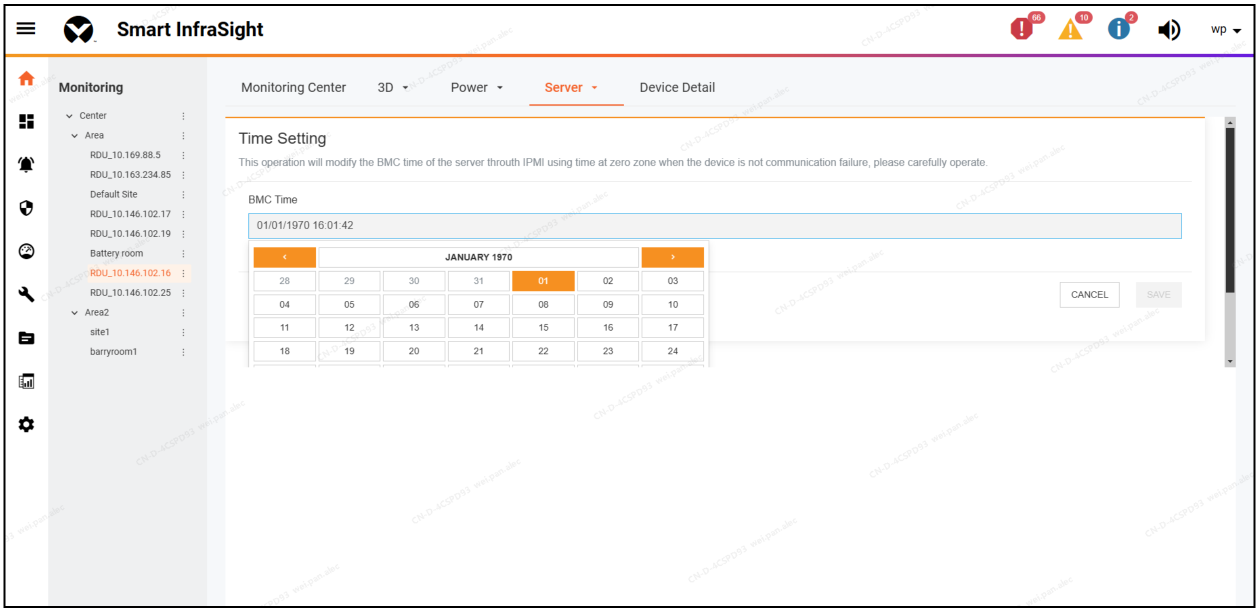


Click the Sensor Information tab on the IPMI device details page to display the sensor information of the IPMI device in pages. The sensor status is divided into normal, alarm and unknown, the green icon is displayed when the normal state is normal, the red icon is displayed when the alarm status is displayed, and the gray icon is displayed when the unknown state is displayed. The sensor information of the IPMI device is refreshed every 10 seconds.

IPMI Device Time Setting

Click on the ellipses (...) behind an IPMI device in the IPMI device list and select the **Time Setting** button to open the IPMI device time setting page, as shown **Figure 8.7** below . BMC time here is indicating time in GMT+00 time zone. After selecting the time you want to set, click the *Save* button to complete the modification of the BMC time of the device.

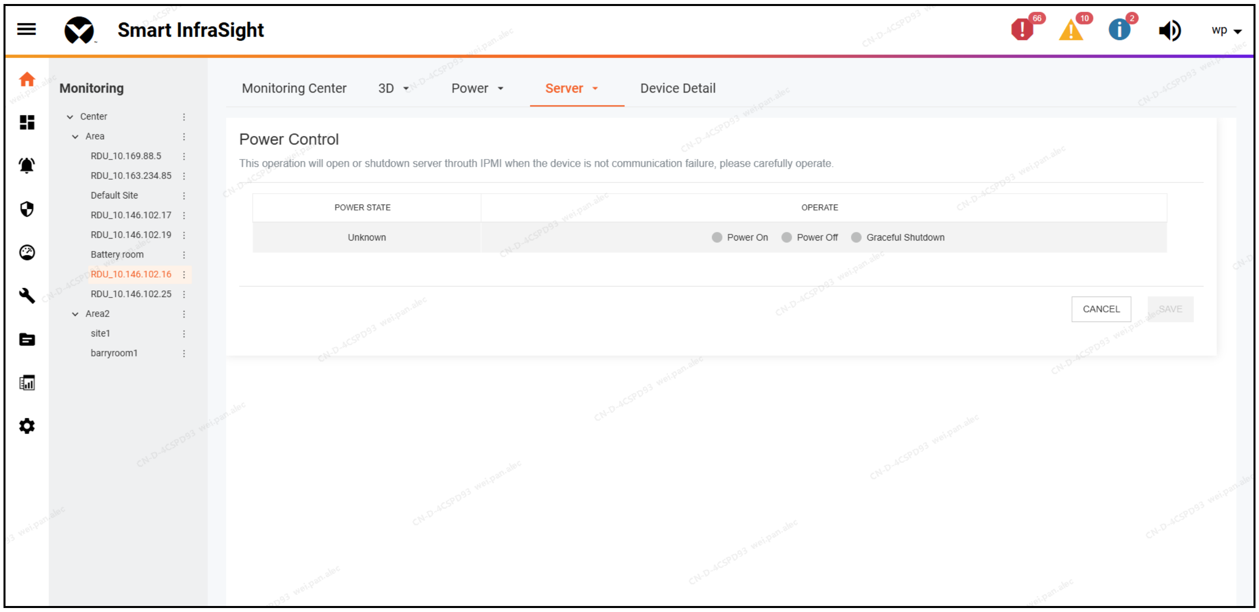
Figure 8.7 IPMI Device Time Setting



IPMI Device ON/OFF Control

Click the ellipses (...) behind an IPMI device in the IPMI device list and select the **Power Control** button to open the IPMI device power on and off control page, as shown in **Figure 8.8** on the facing page . After selecting the control option (power on, power off, or graceful shutdown), click the *save* button to complete the power on and off control of the device.

Figure 8.8 IPMI Device Power ON/OFF Control

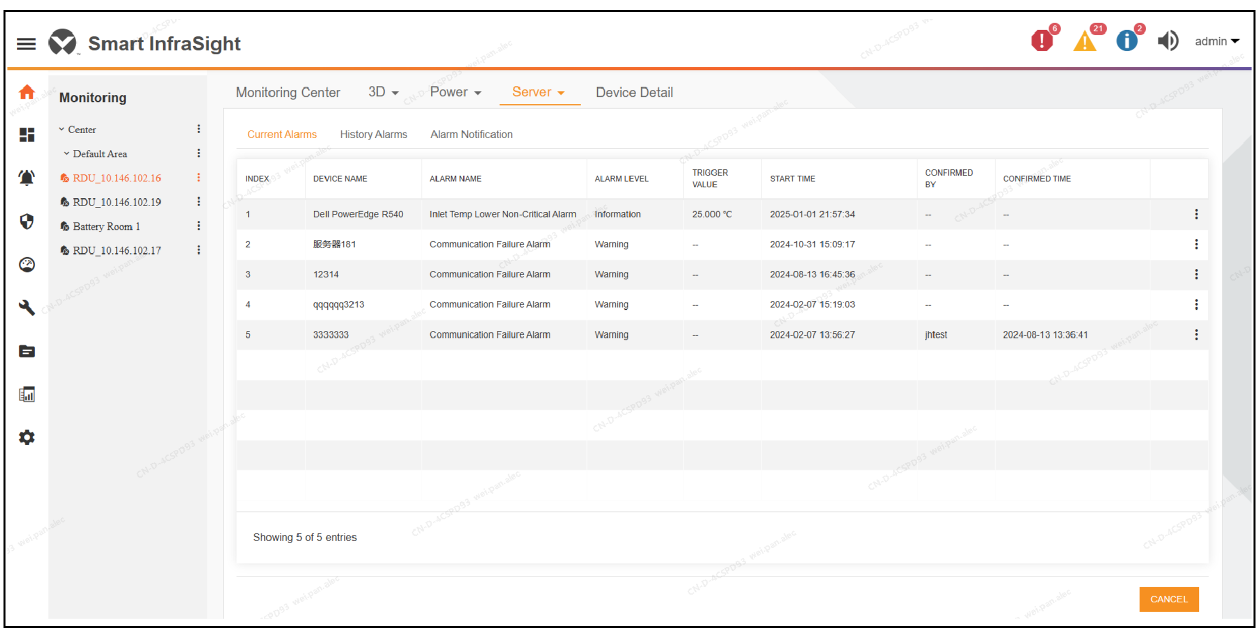


IPMI Device Alarm Management

Click the **Alarm** button in the upper right corner of the IPMI device list page to open the alarm management page of the IPMI device. The IPMI Device Alarms page contains the current alarms and history, as shown in **Figure 8.9** below .

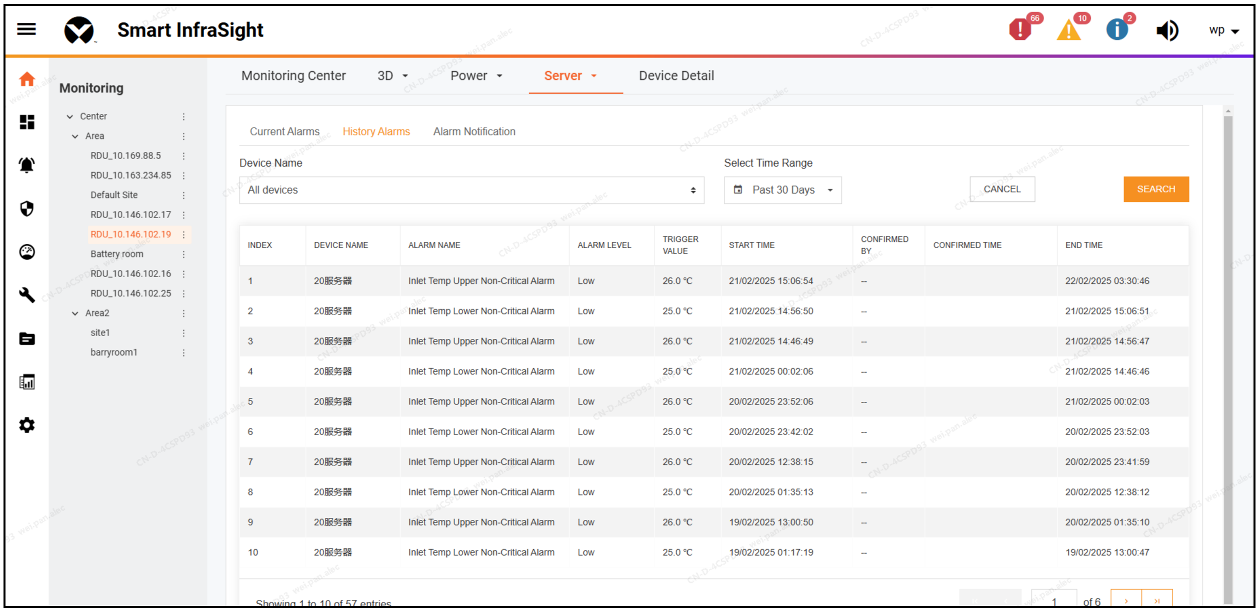
There are three tabs for Alarms and Notifications, and the current Alarms tab is displayed by default, as shown in the following figure. Click on the *Confirm* button in the ellipses (...) behind the current alarm record. After the alarm is confirmed, no alarm notifications will be sent.

Figure 8.9 IPMI Device Alarm Notification Configuration



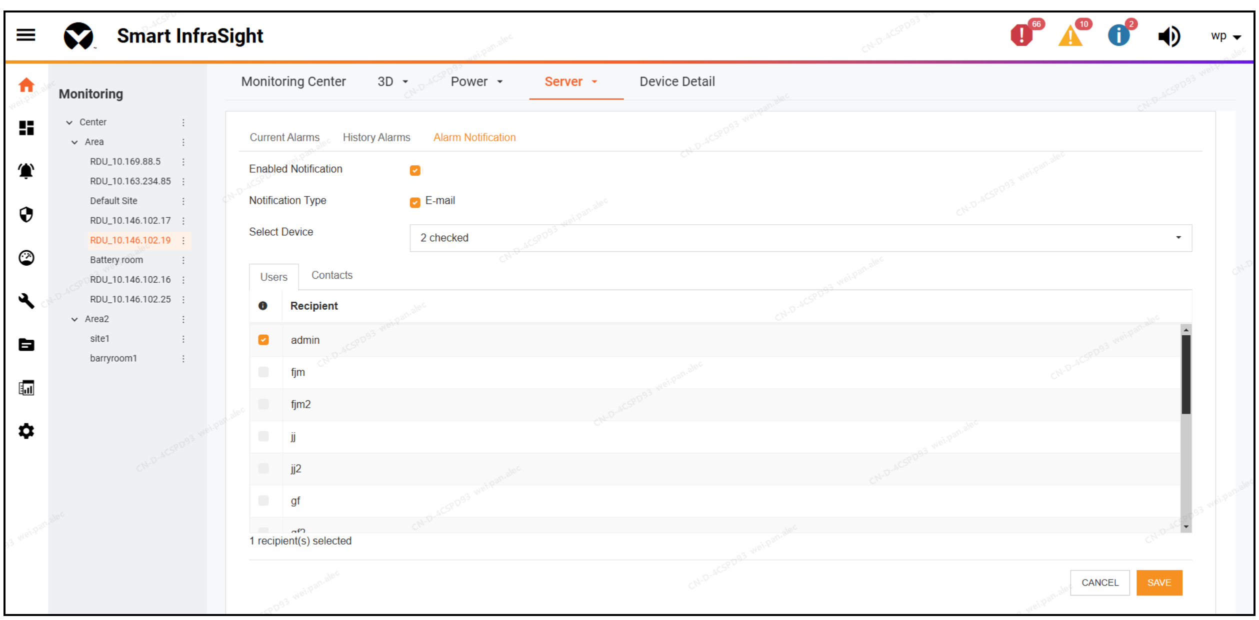
Click the History Alarms tab to display the page as shown in **Figure 8.10** below . Select the device name and search time, and click the search button to search the history alarms of the selected device.

Figure 8.10 IPMI Device Alarm History



In Alarm Notification, after you select Enable notifications as shown in **Figure 8.11** below , select your preferred notification method (currently limited to email) and choose which IPMI devices will trigger alarms. Then, specify the recipient of these notifications and click 'Save.' If an alarm persists on a selected IPMI device, the system will send notifications every 4 hours, up to a maximum of 3 times.

Figure 8.11 IPMI Device Alarm Notification Configuration



8.3.3 Console Management Detailed Function

Console Device Management

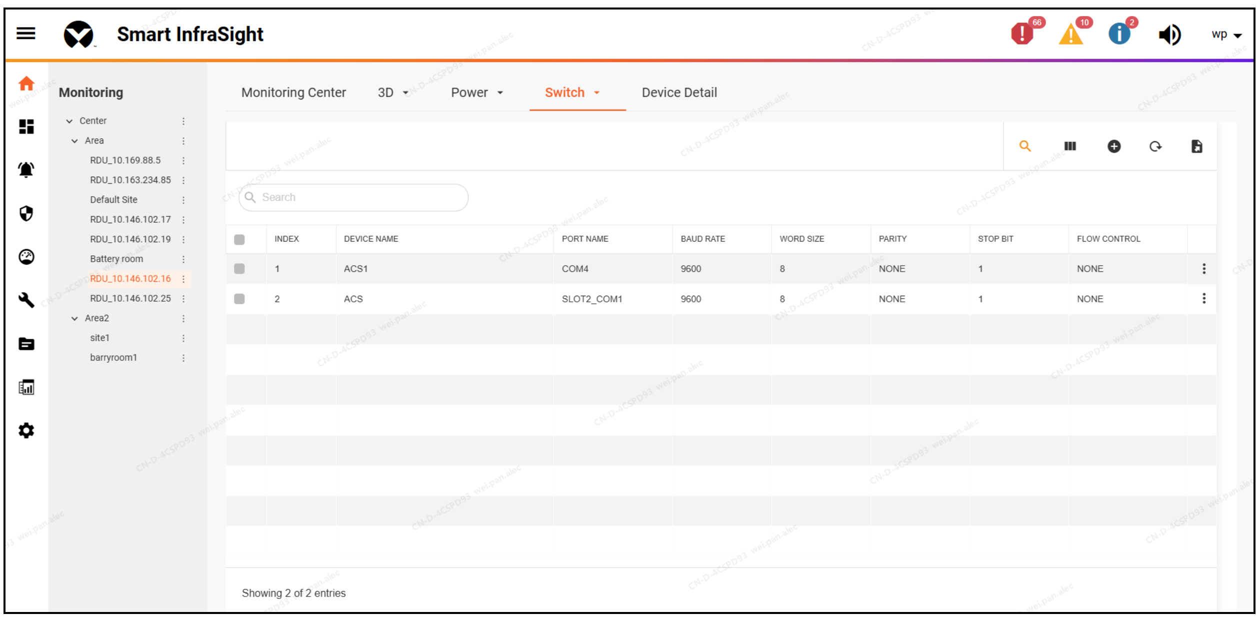
Click a site in the monitoring tree, if the site supports console device management Switch will appear in the tab at the top of the right page.

Click the Switch tab to enter the console device management page, as shown in **Figure 8.12** below .

The console device list display information, including sequence number, device name, port name, baud rate, data bits, check bits, stop bits, and flow control.

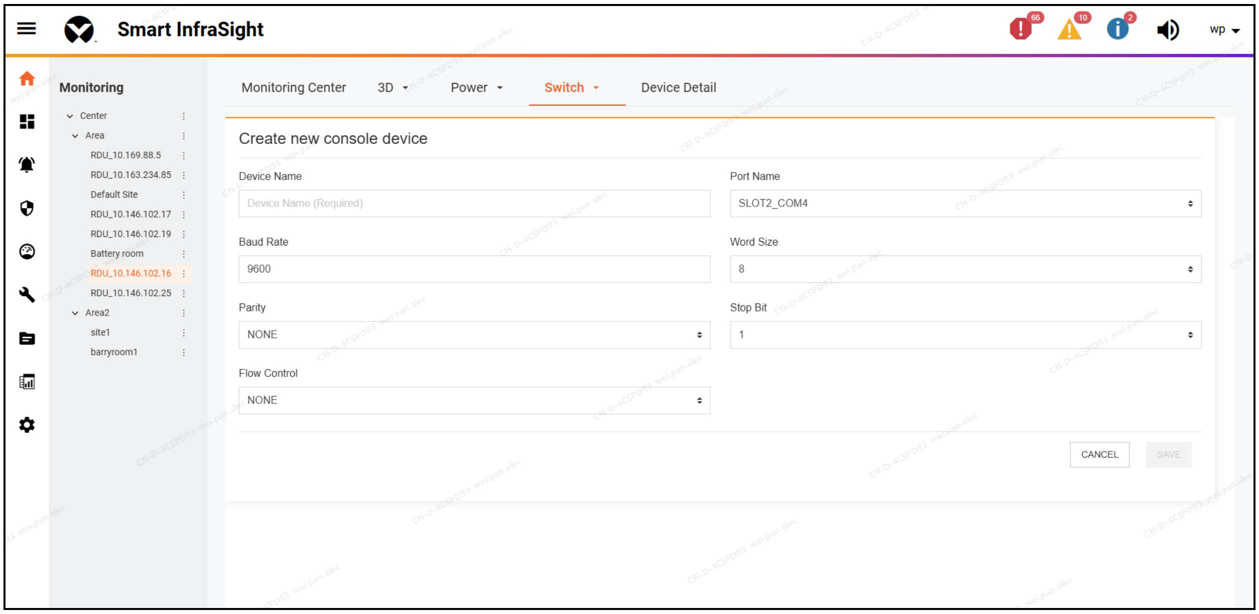
- Use the **Search** button in the upper right corner to open the search box and search for the specific console devices.
- Use the **Add** button in the upper right corner to open the Add Console Device page to add a new console device to the system.
- Use the **Refresh** button in the upper right corner to re-request the console device information on the RDU collector and refresh the console device information in the list.
- Use the **Console History Log** button in the upper right corner to open the log management page of the console device.

Figure 8.12 Console Device List



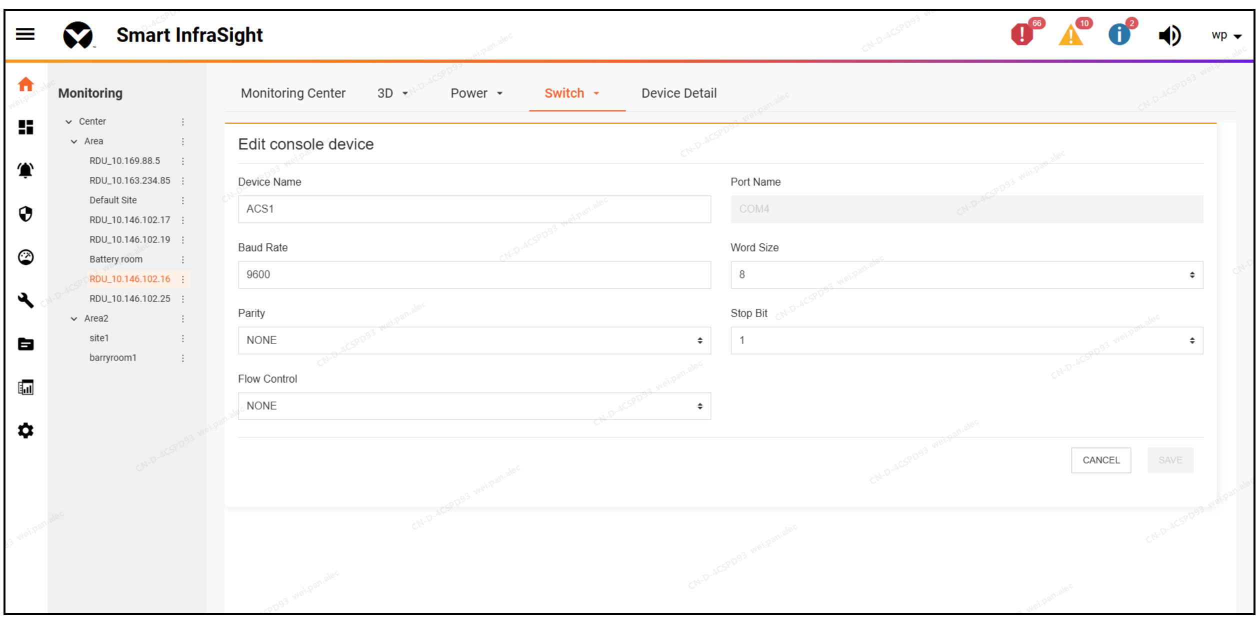
Use the **Add** button in the upper right corner to open the Add Console Device page, and enter the console device information (port, baud rate, data bits, check bits, stop bits, and traffic rates). The control must be entered correctly according to the configuration on the console device), click the *Save* button, as shown in **Figure 8.13** on the next page . Newly added console devices are added in RDU501 synchronously.

Figure 8.13 Adding a Console Device



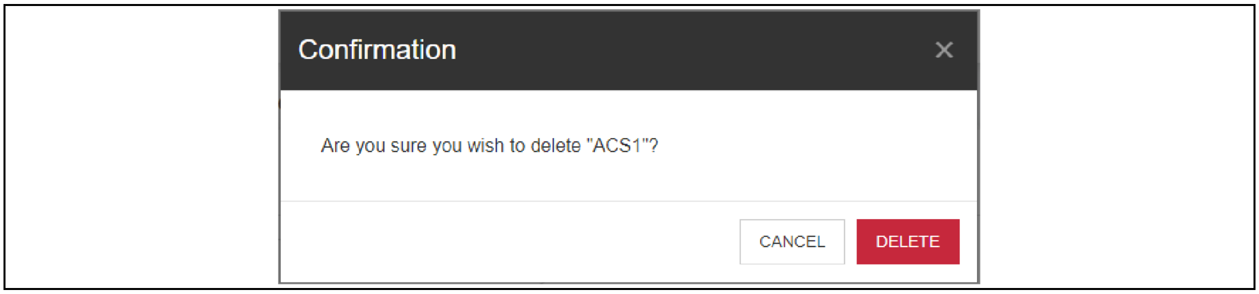
Click the ellipses (...) menu behind a console device in the console device list and select Edit to open the Edit Console Device page, as shown in **Figure 8.14** below . Enter the new information of the console device (the port information is not allowed to be modified, the baud rate, data bits, check bits, stop bits, and flow control must be entered correctly according to the configuration of the console device), and then click the save button. The modified information of the console device is synchronized to the RDU collector.

Figure 8.14 Editing a Console Device



Click the ellipses (...) menu behind a console device in the console device list, and select the *Delete* button, and a confirmation window will pop up to delete the console device, as shown in **Figure 8.15** on the facing page . After you click *Delete*, the console device will be deleted from the system, and the RDU collector will also delete the console device synchronously.

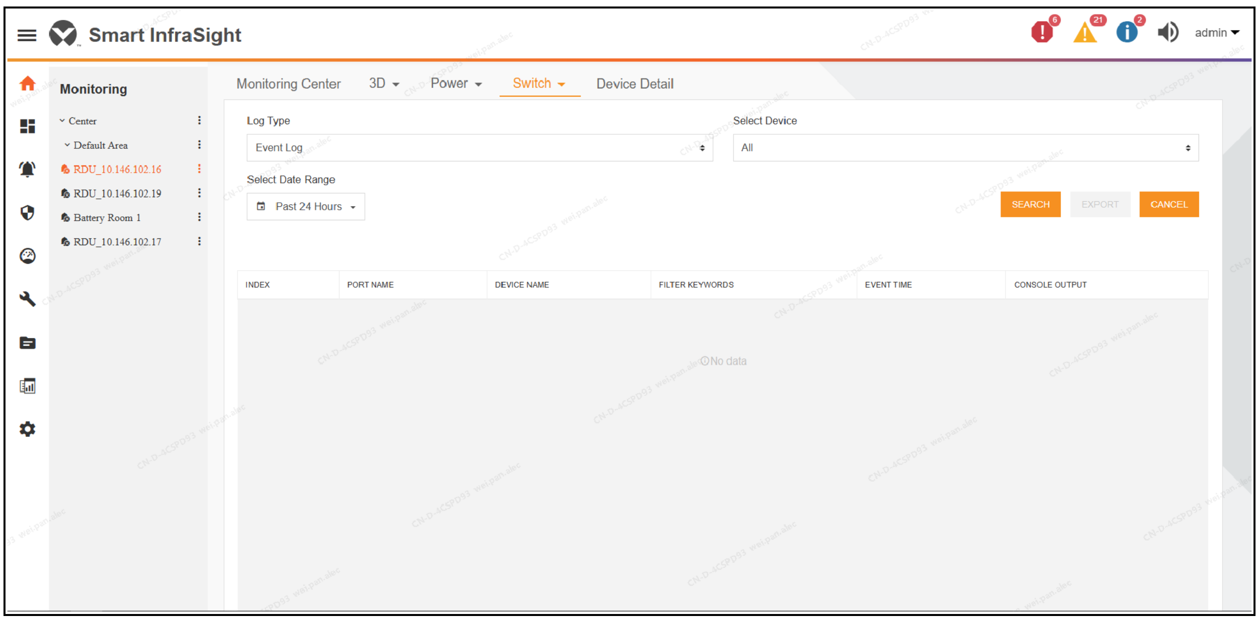
Figure 8.15 Deleting the Console Device



Console Logs

Use the Console History Log button at the top right of the IPMI device list page to open the Console Device Logs page. Console Device Log, The console log data contains event logs and history logs, and the event logs are displayed by default, as shown in **Figure 8.16** below . If you set Log Type to Event Log, select the specified console device, click the *Query* button to query the event logs of the selected device within the selected time period. Click the **Export Logs** button to download the logs that match the filter conditions.

Figure 8.16 Console Device Event Log



History logs can only be downloaded and viewed, and cannot be queried directly.

This page intentionally left blank

9 Dashboard

9.1 Overview

Users can add, remove, and edit dashboard pages. To add a dashboard, click the Add button to open the Add Dashboard page. After setting the dashboard title, click Save to create it. When deleting, users can delete it directly from the delete button. When editing, the user can click the edit button to enter the editing mode, and then the user can edit the dashboard content. All dashboards are visible and editable to users with dashboard permissions.

9.1.1 Functional Modules

The Smart InfraSight™ dashboard includes the following functional modules:

- Add a dashboard
- Edit the widget
- Add widgets
- Configure, and delete widgets
- The dashboard pops up
- Delete the dashboard

9.2 Quick start

9.2.1 Rapid deployment steps

1. Open Smart InfraSight™, enter the dashboard module, and display the dashboard interface.
2. Click the *Add* icon, enter the name of the dashboard in the Add pop-up box, and click *Save* to enter the dashboard interface.
3. After clicking Save, the interface shows No Configuration. Then, clicking the Edit icon in the upper-right corner enters the editing mode. The left dashboard list is hidden, and the Widget list is displayed instead.
4. The user can select a widget from the list and drag it into the dashboard area by holding down the mouse button. During the drag, a shaded area indicates the widget's target position. Once released, a blank widget appears in that location. The user can drag the same widget or other widgets repeatedly.
5. The blank widget is initially unconfigured. When the mouse hovers over it, a close icon appears in the upper left corner, click to delete the widget. The Edit icon is displayed in the upper-right corner. When clicked, a Configuration pop-up box appears. The Drag icon is shown in the lower-right corner of the widget. You can press and hold the mouse to resize the entire widget, or resize it by dragging its edges. To move the widget, press and hold the mouse on the widget and drag it to the desired position.
6. After all widgets are configured, click the save button in the upper right corner of the dashboard, save and exit the editing mode, enter the display mode, hide the widgets list, and redisplay the dashboard list, at this time, the widgets cannot do any operation.
7. In display mode, users can click the edit icon in the upper left corner to modify the dashboard name in the edit pop-up box.

8. After the dashboard configuration is completed, the user can click the pop-up icon in the upper right corner to open a separate web page, hide the first and second menus and headers, and only display the content of the current dashboard.
9. If the user is not satisfied with the dashboard, move the mouse to the current dashboard in the dashboard list on the left, the delete icon will be displayed in the list content, Click the icon, and a pop-up box will ask for confirmation, and click the confirm button to delete the dashboard.

NOTE: The maximum size of the dashboard canvas is 6×18 standard tiles.

NOTE: Widget Movement Instructions: If the dragged widget has covered half or more of the area on a standard grid, the standard grid becomes the target position of the widget.

NOTE: Widgets collision description: During the move/zoom process of the widget, if the target position has been occupied by another widget, the other widget will automatically move to other spaces, if there is no space, the other widget will push the other widgets to move down; If the two widgets are of equal height, the position is swapped first.

9.2.2 Examples

Enter the dashboard name as shown in Figure 8.13 on page 174, and click the *Save* to jump to the dashboard interface.

Figure 9.1 Adding a Dashboard

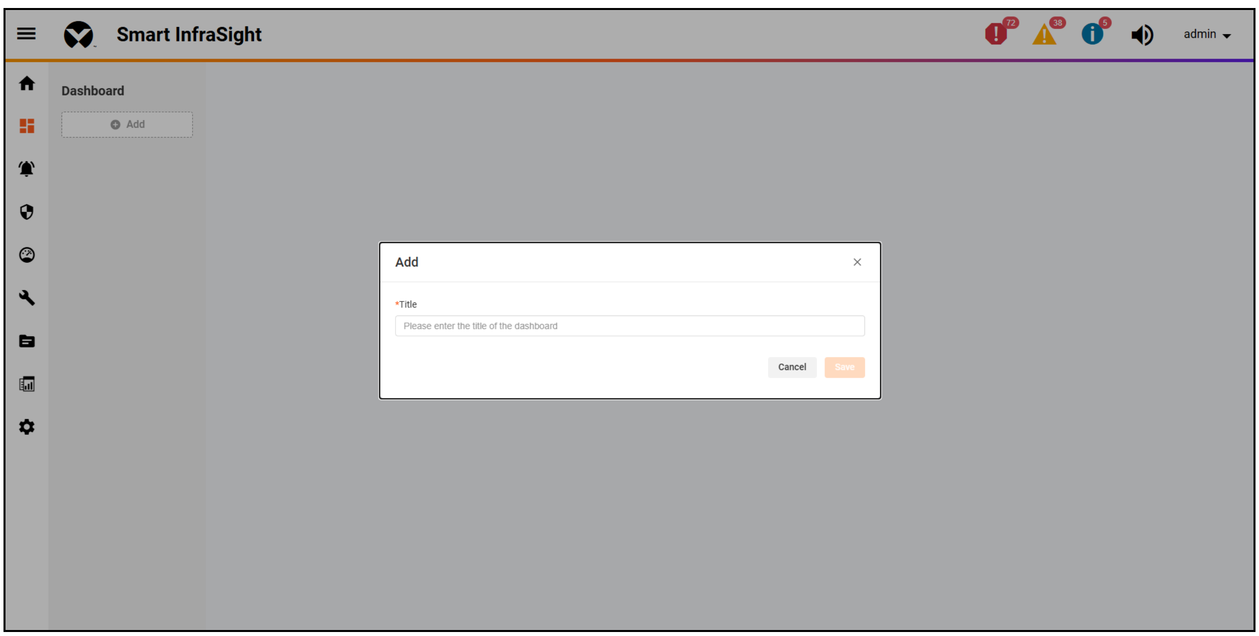
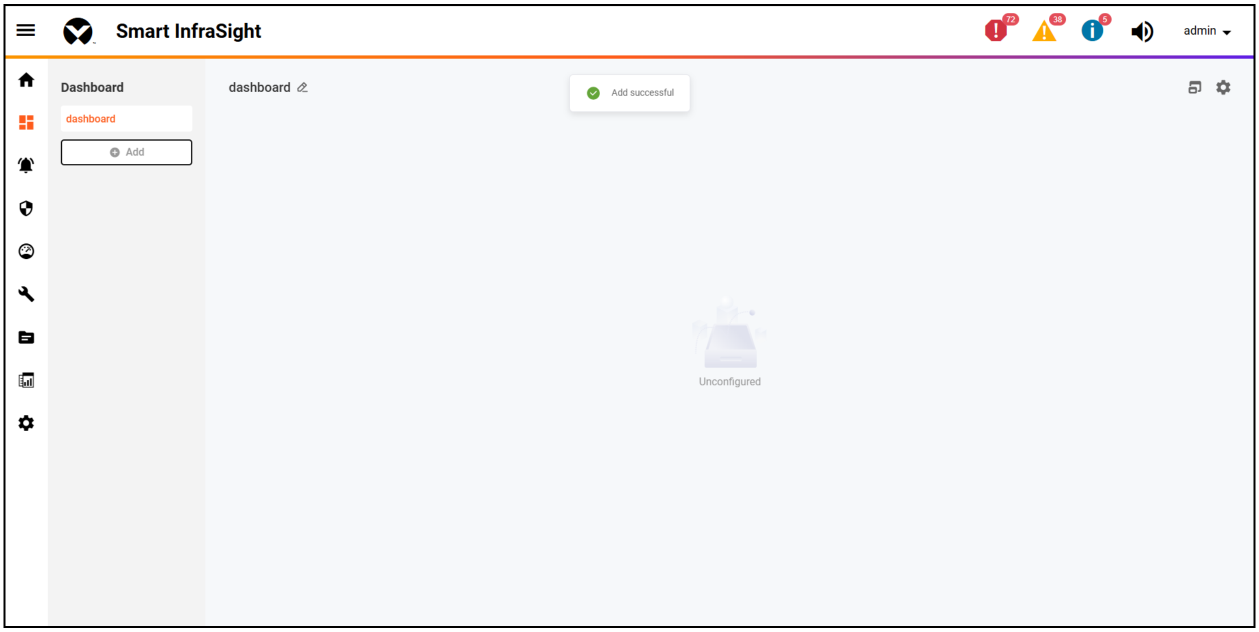


Figure 9.2 Dashboard Added



Click *Edit* to enter edit mode. From the widget list on the left, drag and drop the desired widget onto the canvas, then adjust its position as needed.

Add the appropriate widgets, adjust their positions, complete the configuration, and then click Save to display the dashboard content.

Figure 9.3 Adding the Widgets

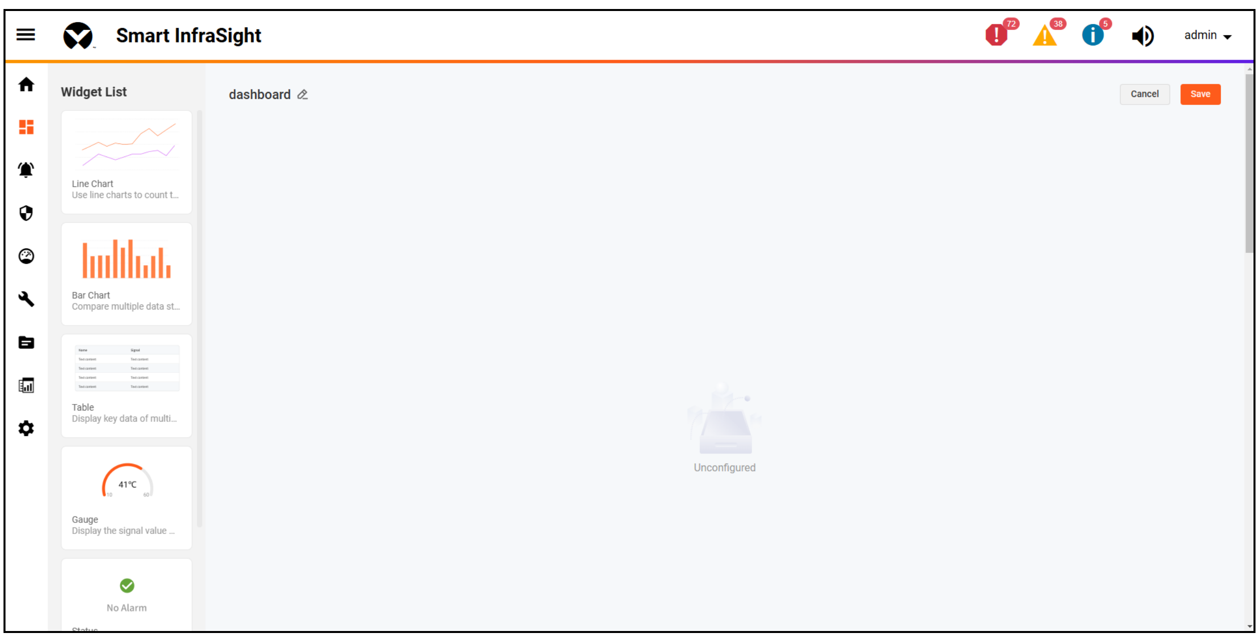
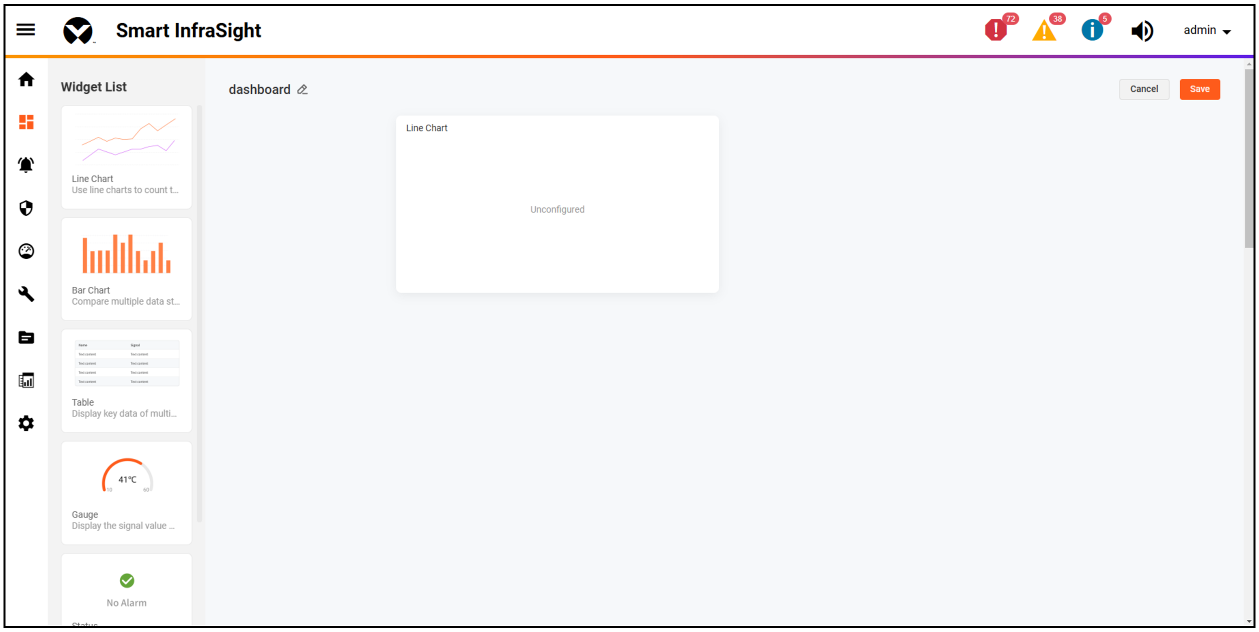
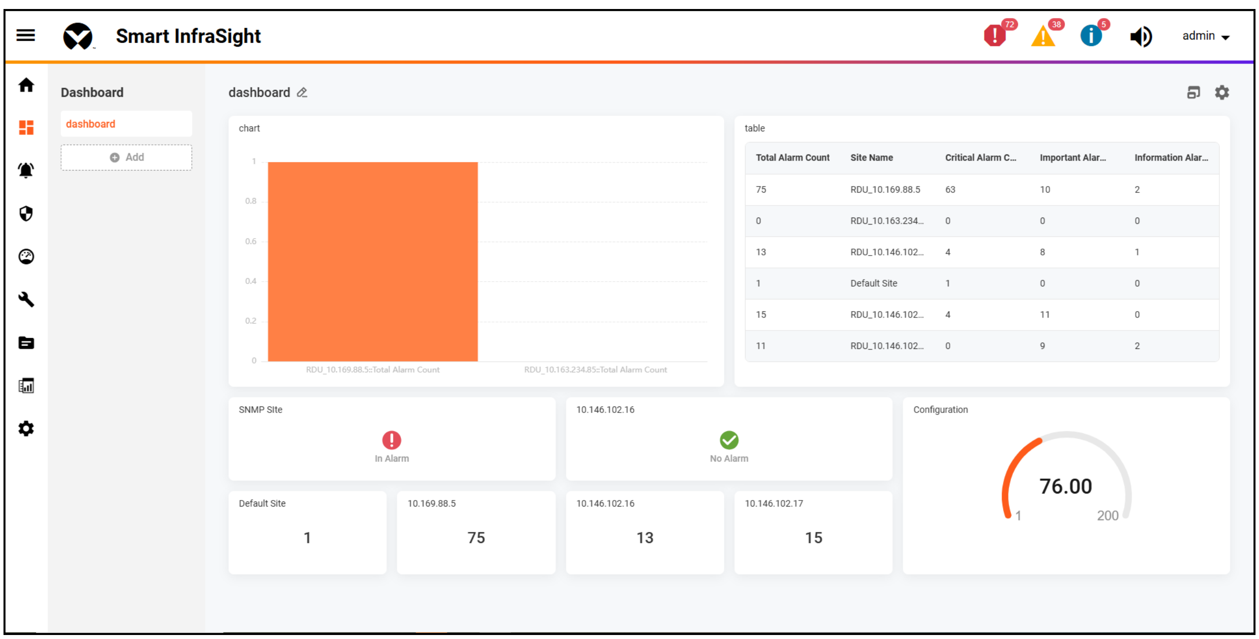


Figure 9.4 The Added Widget



After adding the appropriate widget, the display content of the dashboard is shown in Figure 9.5 below .

Figure 9.5 The Dashboard Content



9.3 Detailed Features

In the dashboard list, click the Add button and enter a dashboard name in the Add pop-up box, and click *Save* to enter the dashboard interface.

Figure 9.6 Adding a Dashboard

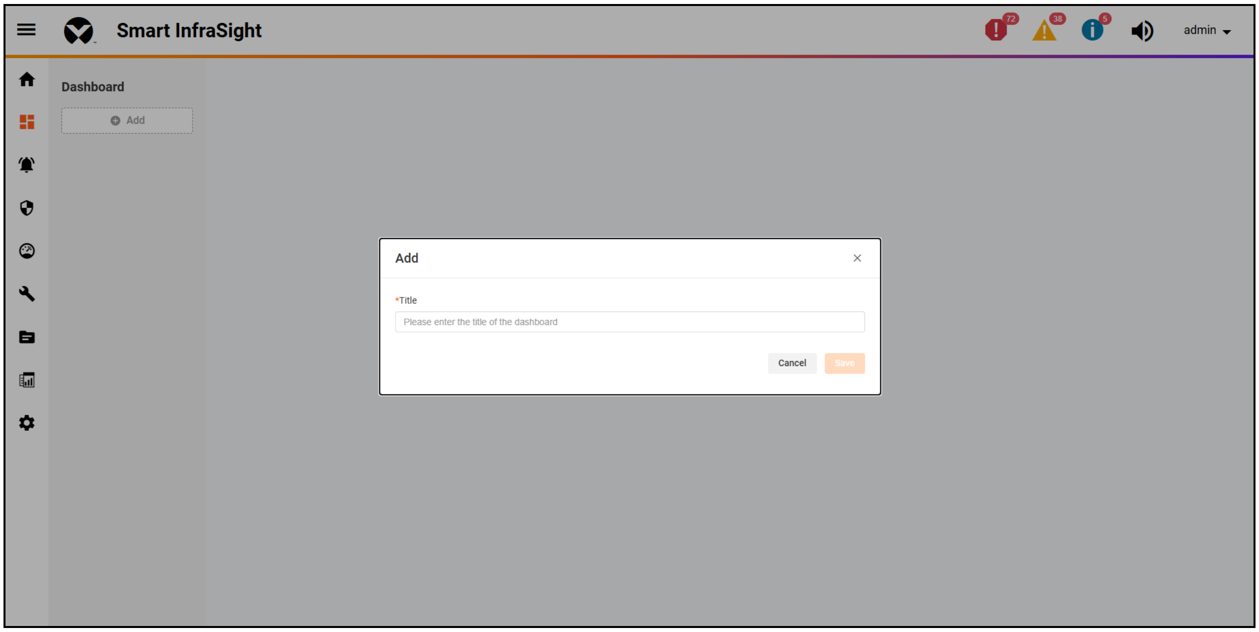
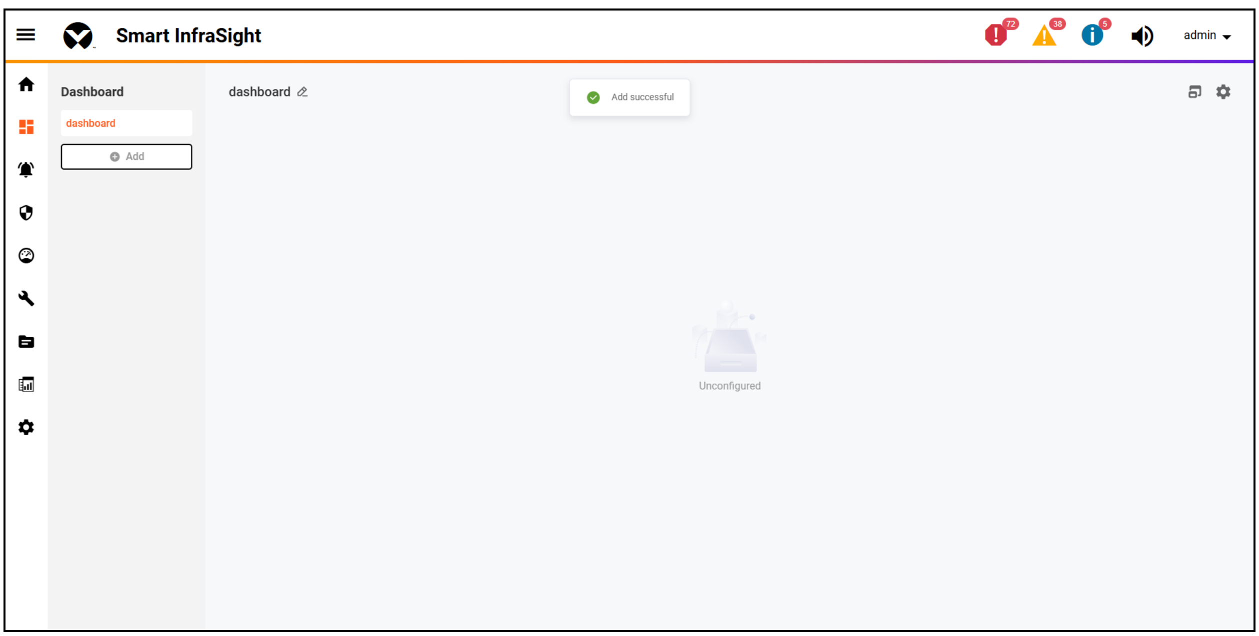


Figure 9.7 The Added Dashboard



9.3.1 Adding Widgets

Click the *Edit* button to enter editing mode. At this time, the dashboard list is hidden, and the widgets list is displayed, as shown in Figure 9.8 on the next page , the user can press and drag the mouse to add widgets, and can also move the widgets position by dragging and dropping. The system provides the following widgets: line chart, bar chart, table, gauge chart, status, Signal point. The basic introduction of each widget is as follows.

Line Chart: Use a line chart to track changes in multiple data sets over a specific time range.

Bar Chart: Compare statistics of multiple data items through bar charts.

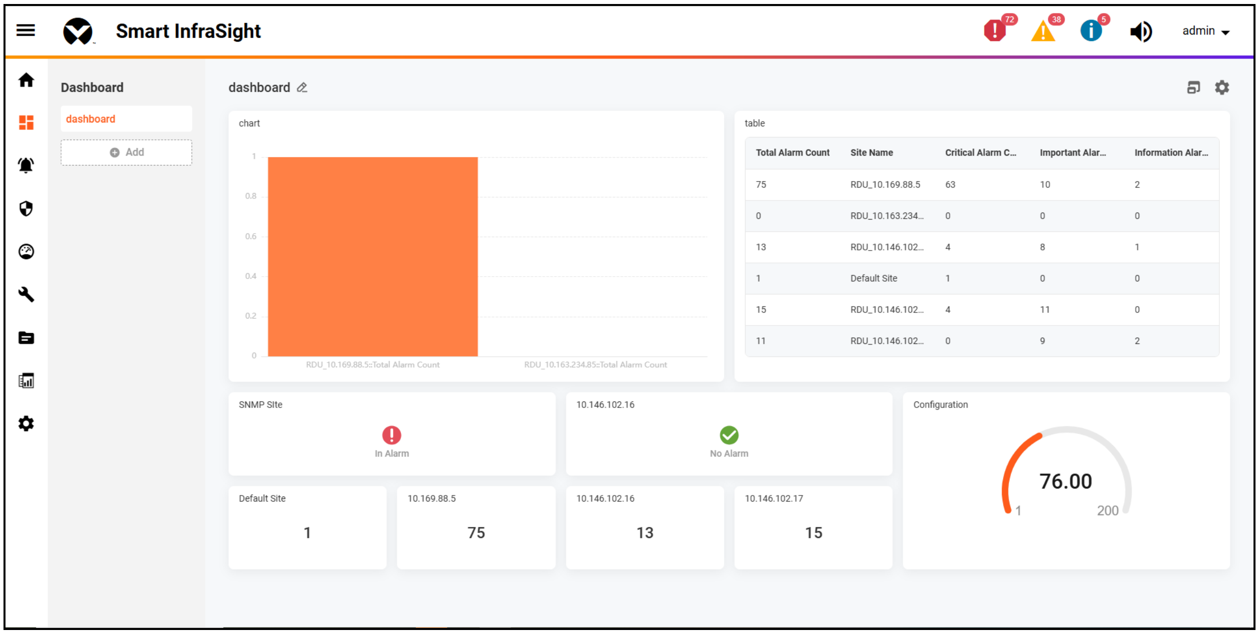
Table: Displays key data from multiple devices in a tabular format.

Gauge Chart: Displays the size of the signal value within a specific range.

Status: Displays whether the site or device has alarms.

Signal: Displays the single-point signal value of a device or site.

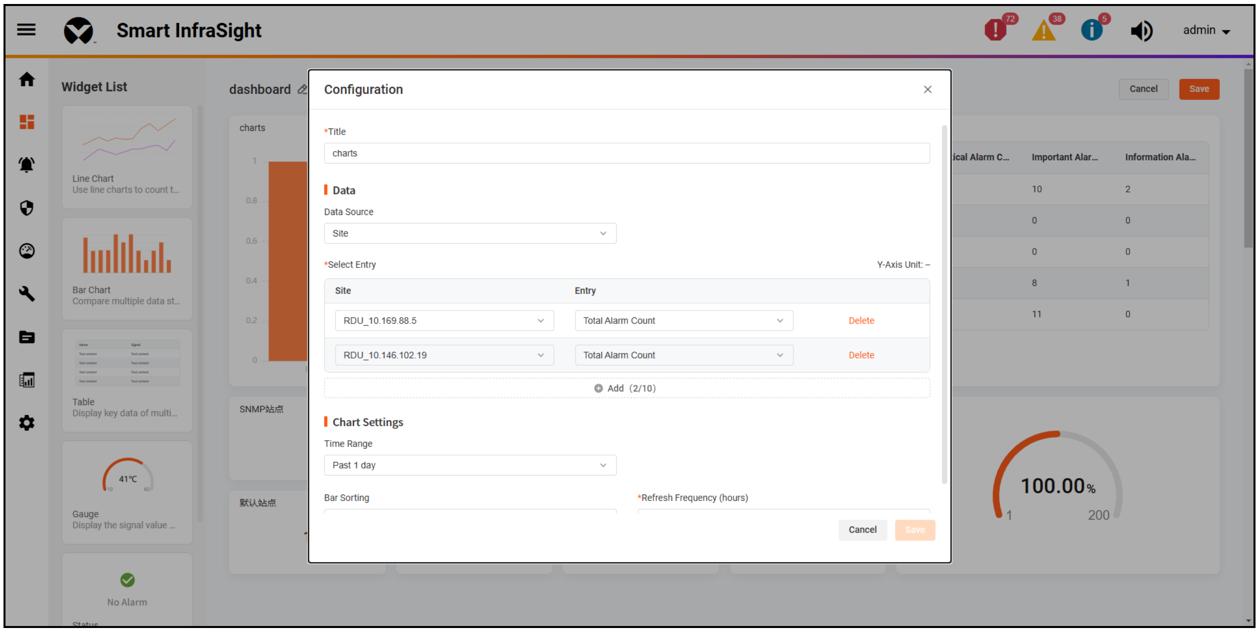
Figure 9.8 Adding the Widgets



9.3.2 Configuring, Moving, Resizing, and Deleting the Widgets

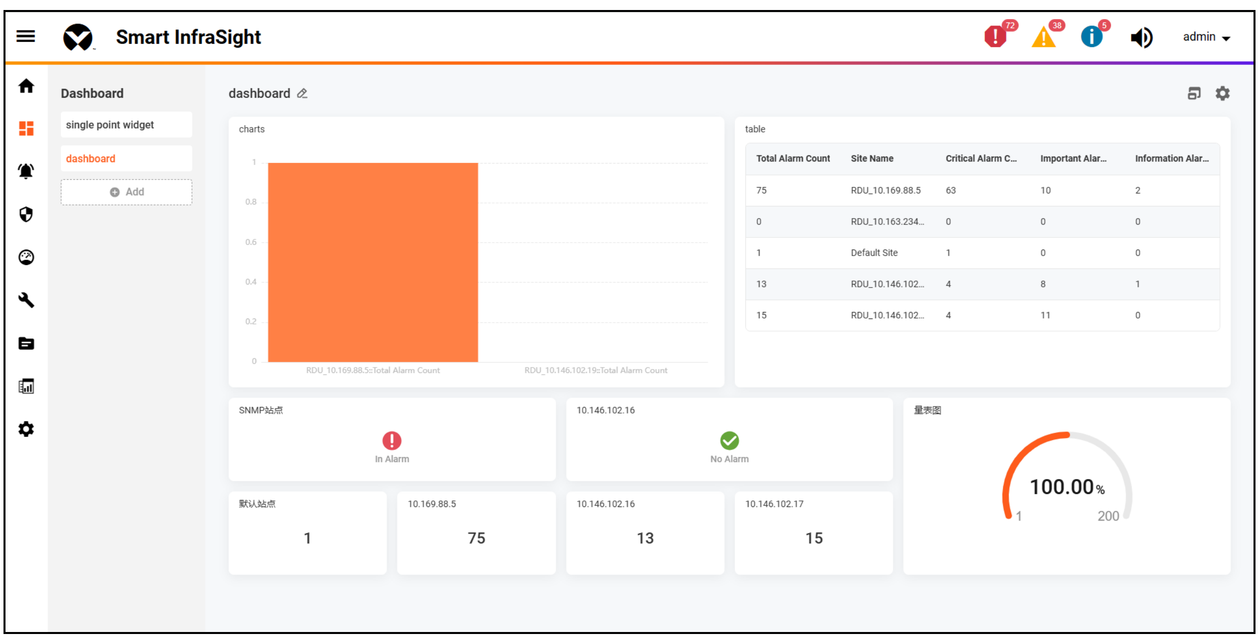
Click the *Edit* button to enter editing mode, as shown in **Figure 9.9** on the facing page . Hover over a widget to begin editing.

Figure 9.9 Setting up the Widget



Select the widget, click and hold to drag the widget as shown in **Figure 9.10** below , you can adjust the position of the current widget, the shaded part indicates the final position of the current widget, after releasing the mouse, complete the widget movement.

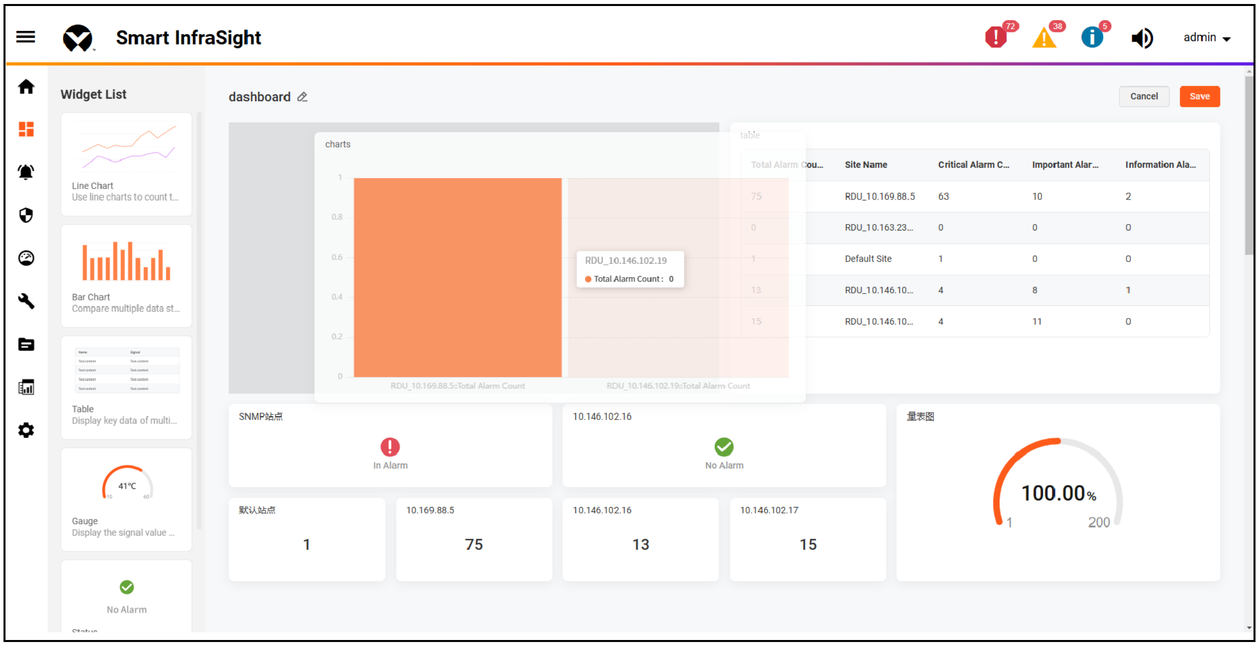
Figure 9.10 Dragging and Dropping the Widgets



9.3.3 Editing the Dashboard

As shown in **Figure 9.11** on the next page , In the edit mode, slide the mouse over the widget to display the three icons of delete, configuration, and zoom.

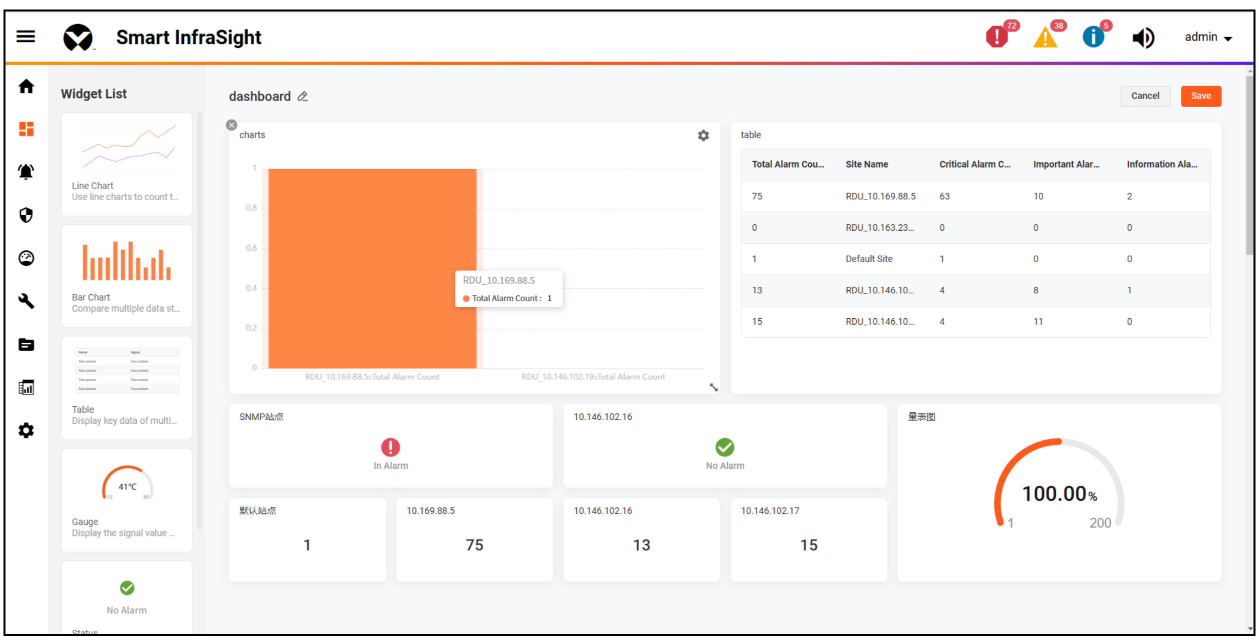
Figure 9.11 Editing the Dashboard



Zoom Widget

Click the zoom icon in the lower right corner, as shown in below .Press and hold to resize the entire widget, or drag the widget edges individually to adjust its size.

Zooming the Widget



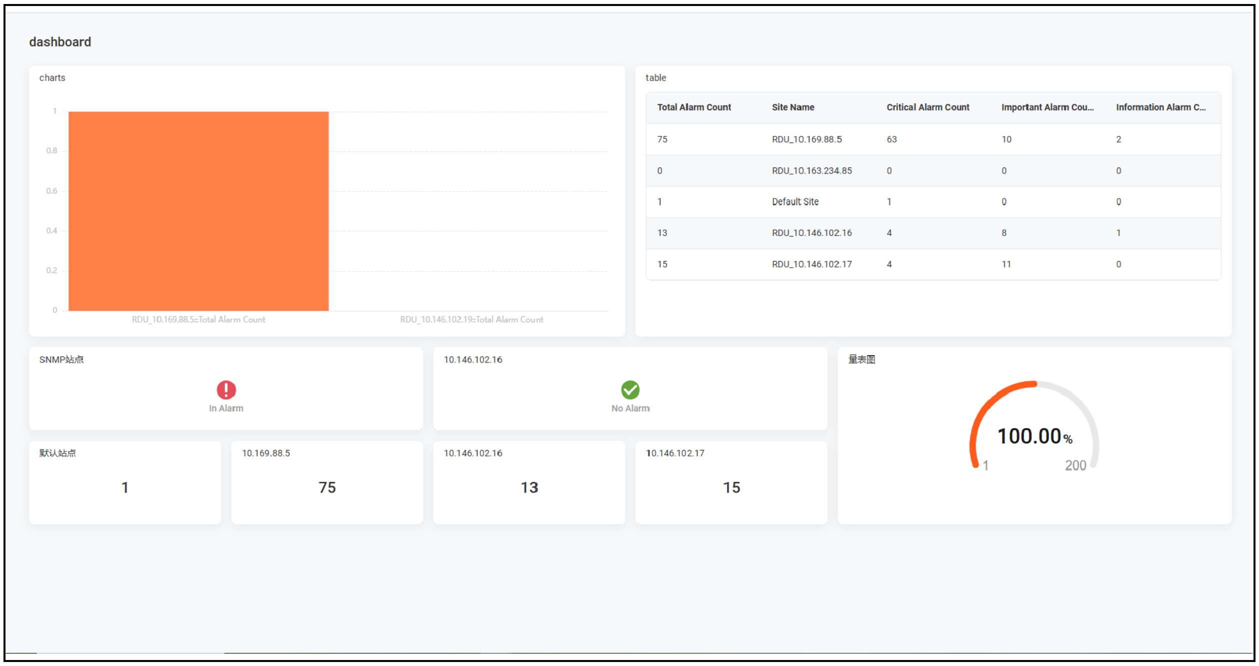
Deleting the Widget

All of the above operations must be implemented in edit mode, and after editing, click *Save* in the upper right corner to retain all the configurations of the widgets.

9.3.4 The Dashboard Pops up

After the above adjustments are configured, after all the widgets are configured, after saving the dashboard, click the icon in the upper right corner of the dashboard, and you can view the dashboard information separately in a new page.

Figure 9.12 The Popup Dashboard



9.3.5 Deleting the Dashboard

After configuring a dashboard, the user can view all dashboards in the dashboard list, the dashboard displays a delete button. After clicking Confirm, the dashboard list will be automatically refreshed, automatically jump to the first dashboard, and prompt that the deletion is successful.

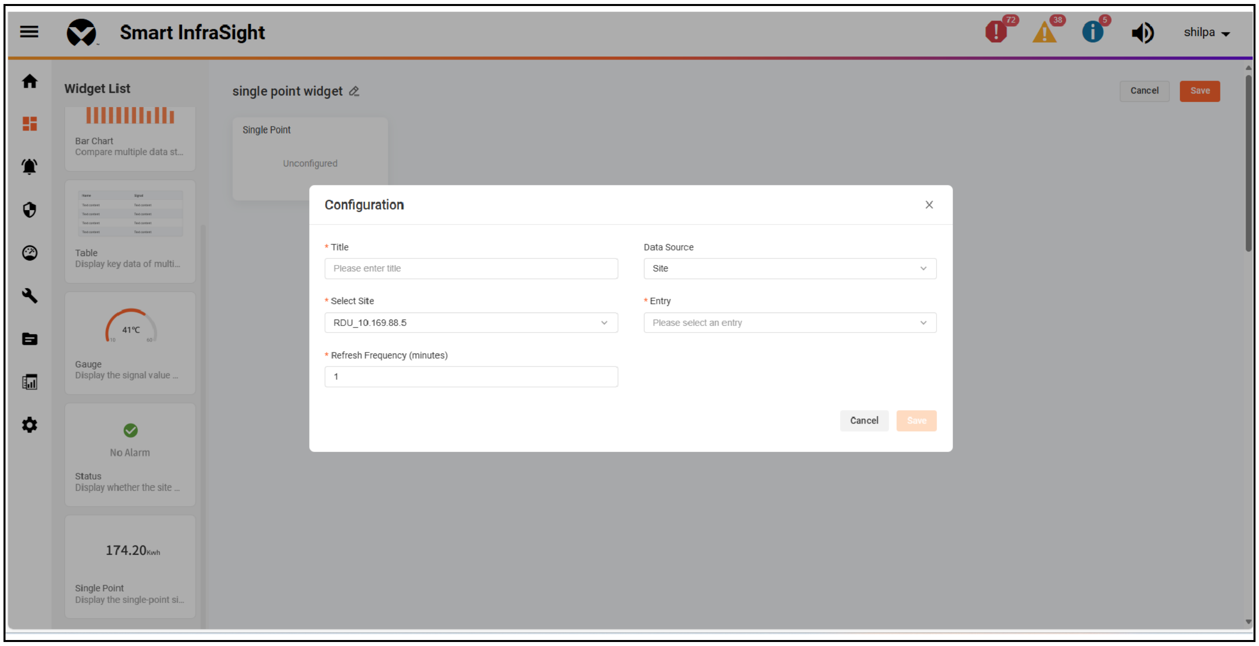
NOTE: All dashboards are visible and editable to users with Dashboard permissions, so be careful when deleting them.

9.4 Widgets in Detail

9.4.1 Signal Widget

The signal widget is used to display the single-point signal value of the device or site; After the configuration is completed, the widget will display the data of the signal and refresh the data in real time, so that the user can view the data values of important signal points in the dashboard at any time. The pop-up box is as shown in Figure 9.13 on the next page.

Figure 9.13 Signal Widget Configuration Item

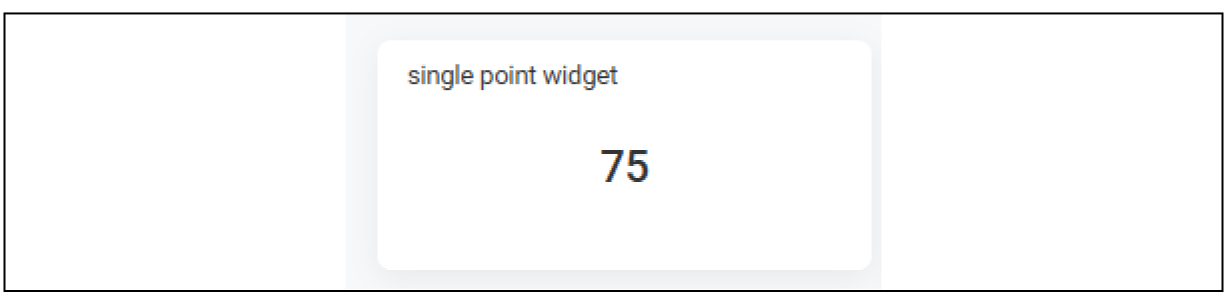


The configuration items are as follows:

- Title: Define the widget title, which will be displayed in the widget header after configuration.
- Data source: Users can select a site or device as the data acquisition source.
- Select Site/Select Device: When you select a site for the user data source, select the site to be displayed in the corresponding drop-down list. When you select a device for the user data source, select the device under the site in the drop-down list.
- Entry: After selecting the rear device or site, the user can select the signal information in the drop-down box;
- Refresh frequency: The widget will refresh the displayed data in real time based on the configuration settings. Users can set the refresh frequency from 1 to 10, with the default frequency set to 1.

After all the configuration information is completed, click the save button, and you can see the signal value display in the widget. The final widgets look like this:

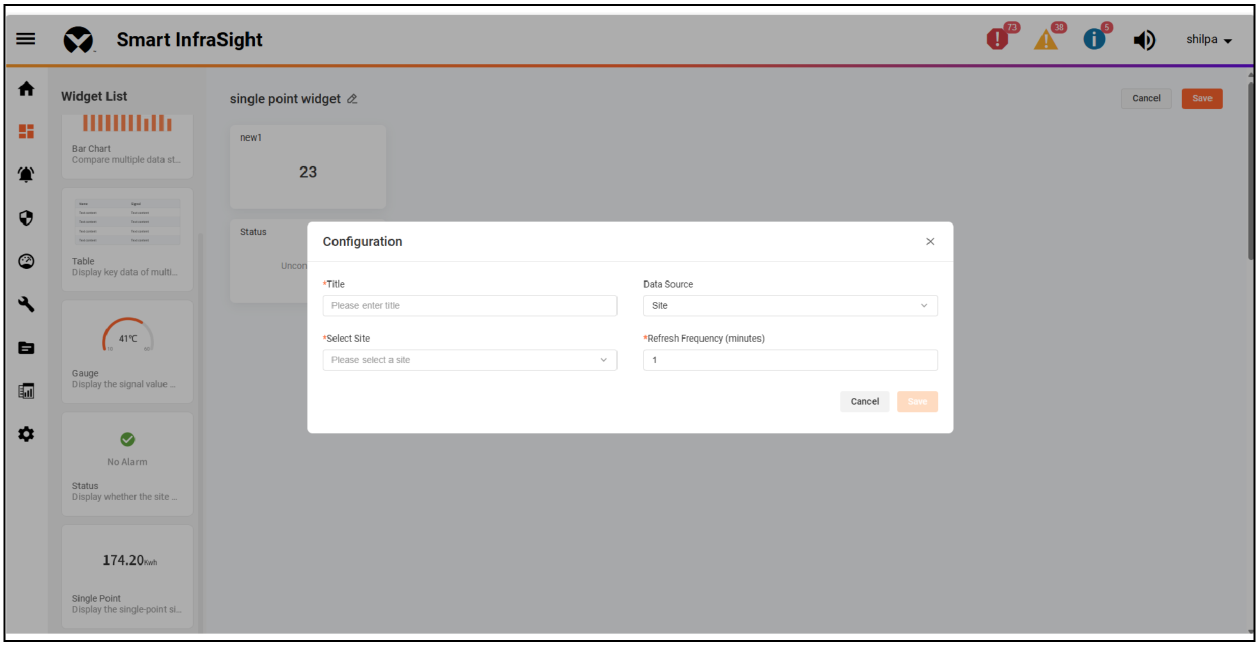
Figure 9.14 Signal Widget Renderings



9.4.2 Status Widget

The Status widget is used to indicate whether the current site or device has any alarms. In the configuration settings, users can select the site or device to monitor. The widget will then display the alarm status of the selected site or device and refresh in real time. The pop-up box is as shown in Figure 9.15 below .

Figure 9.15 Status Widget Configuration Item

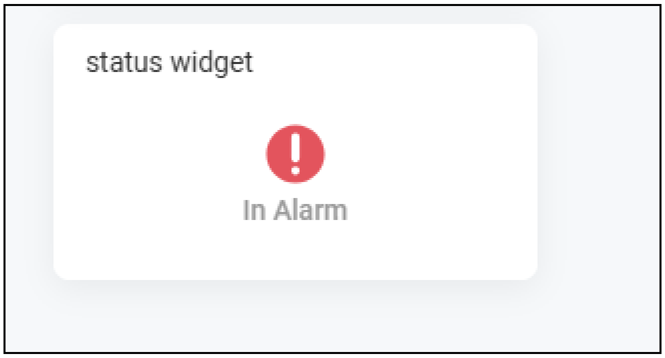


The configuration items are as follows:

- Title: Defines the widget title and displays it in the widget header after it is configured.
- Data source: The user can select a site or device as the source of data collection.
- Select Site/Select Device: When the user selects a site as the data source, all the current sites are displayed in the corresponding drop-down list. When you select a device as the data source, the drop-down list displays all the devices that can be monitored.
- Refresh Frequency: The widget will refresh the displayed data in real time based on the configuration settings. Users can set the refresh frequency from 1 to 10, with the default frequency set to 1.

After all the configurations are completed, click the save button to see the status value display in the widget. The final widget renders as shown in Figure 9.16 on the next page .

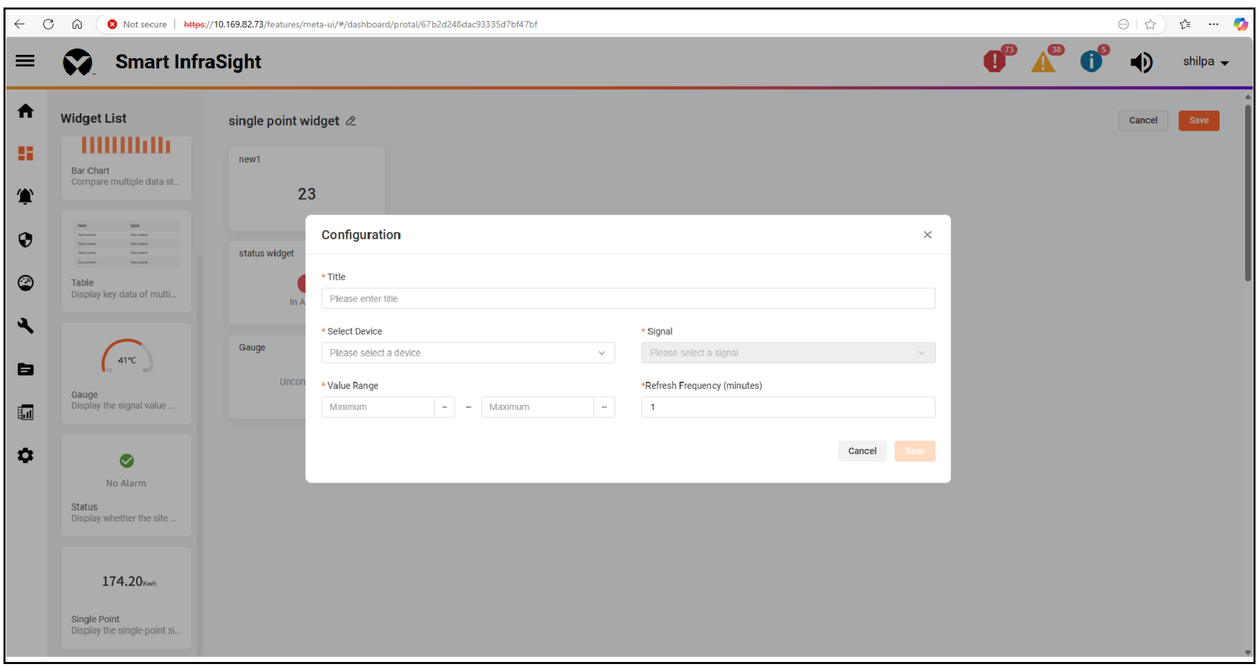
Figure 9.16 Status Widget



9.4.3 Gauge Widget

For certain device signal values, users can use the Gauge Graph widget to display the current value along with the normal value range. After configuration is completed, users can quickly determine whether the signal point is within the normal range based on the widget display and make timely adjustments to ensure device safety.

Figure 9.17 Gauge Diagram Widget Configuration Item



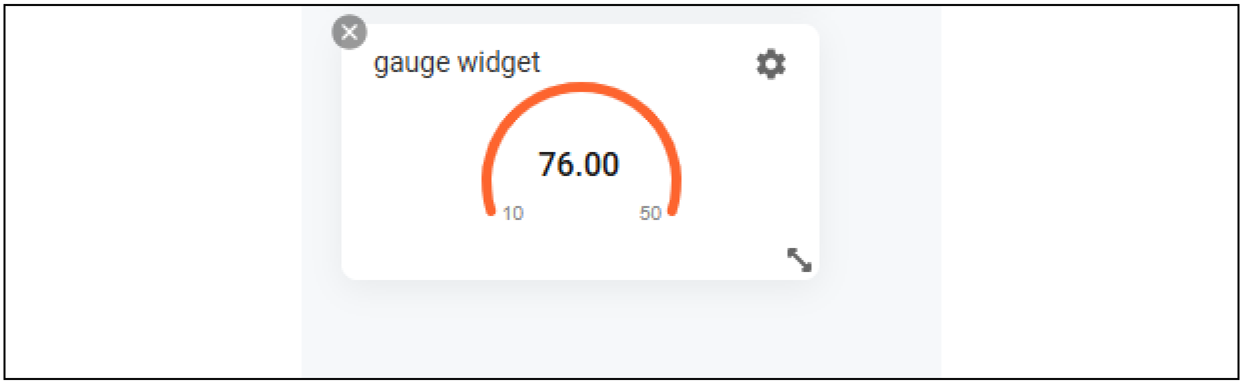
The configuration items are as follows:

- Title: Defines the widget title and displays it in the widget header after the configuration is complete.
- Select Device: Users can select the device they need to focus on in the drop-down box.
- Signal: Once the user selects a device, they can choose a more specific signal from the drop-down menu.

- Value range: Define the minimum and maximum values of the widget, which will be displayed at the bottom of the meter diagram after configuration.
- Refresh Frequency: The widget will refresh the displayed data in real time based on the configuration settings. Users can set the refresh frequency from 1 to 10, with the default frequency set to 1.

After all the information is configured, click the save button to see the value display of the widget in the dashboard. The final widget renders as follows:

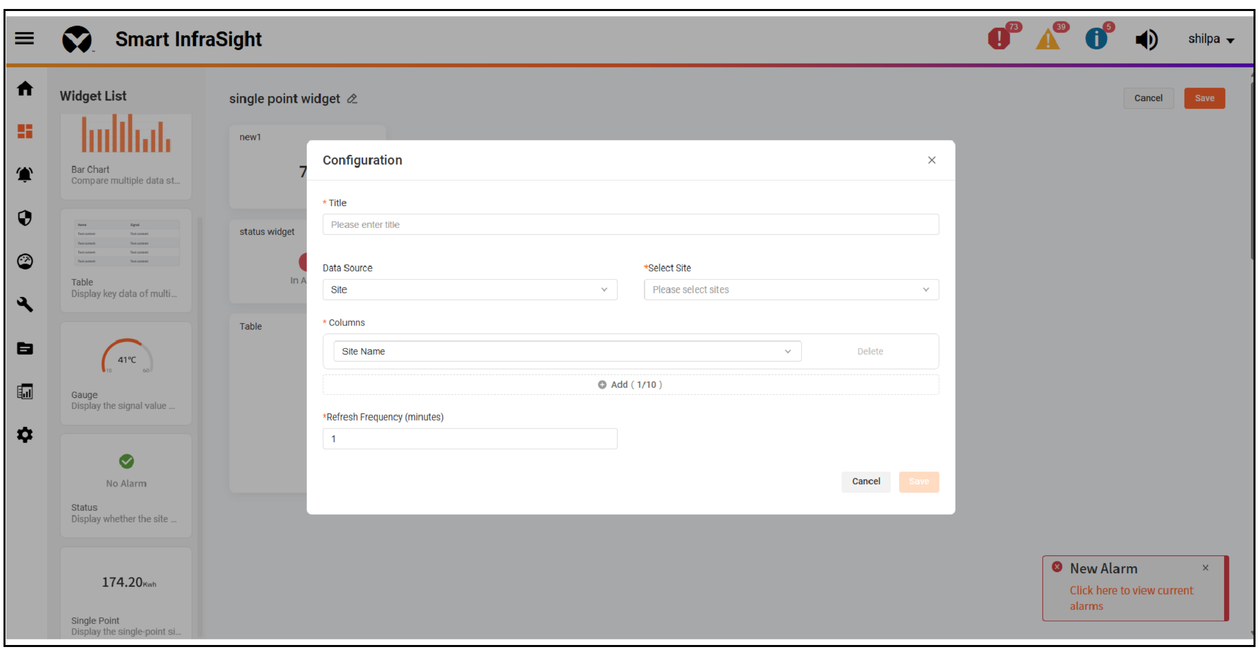
Figure 9.18 Gauge Widget



9.4.4 Table Widget

The Table widget displays key data from multiple devices in a tabular format. Users can freely select the text and data to be shown in each row. After configuration is complete, the widget will display the selected data and refresh it in real time. The configuration pop-up box is shown in Figure 9.19 below .

Figure 9.19 Table Widget Configuration Item



The configuration items are as follows:

- **Title**: Defines the title of the widget and displays it in the widget header after the configuration is complete.
- **Data source**: The user can select a site or device as the source of data collection.
- **Select Site/Select Device**: When a user selects a site from a data source, the user can add multiple selected sites; If the user selects a device, the user can add up to 20 devices, and each time they are added, an additional row will be added to the table display.
- **Column**:
    - When selecting a site as the data source, users can choose to display the site name, total number of alarms, number of emergency alarms, number of important alarms, and number of general alarms.
    - When selecting a device as the data source, users can choose to display the device name, signal, alarm, total alarms, emergency alarms, important alarms, and general alarms. If signal or alarm is selected, users must further specify the corresponding signal name or alarm name.
    - Users can add up to 10 columns in the column settings, and the selected data will be displayed in the table.
- **Refresh Frequency**: The Table widget displays key data from multiple devices in a tabular format. Users can freely select the text and data to be shown in each row. After configuration is complete, the widget will display the selected data and refresh it in real time.

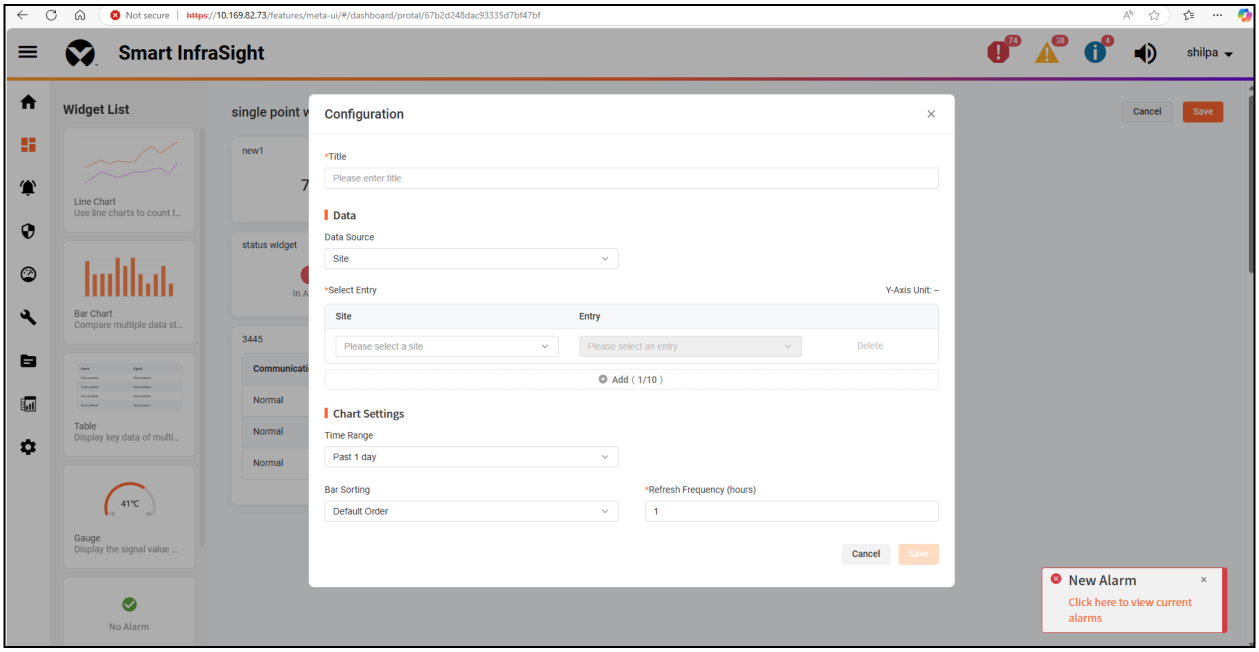
After completing all the configuration items, click the save button, and you can see the display of the table widget in the widget; The final widget will be rendered as follows:

Figure 9.20 Table Widgets

9.4.5 Bar Chart Widget

The Bar Chart is used to compare the statistics of specific signals, users can select the sites or devices they are interested in, and the Bar Chart widget can quickly compare and find out the differences, and the Bar Chart widget supports real-time data refresh. **Figure 9.21** on the facing page shows the pop-up box.

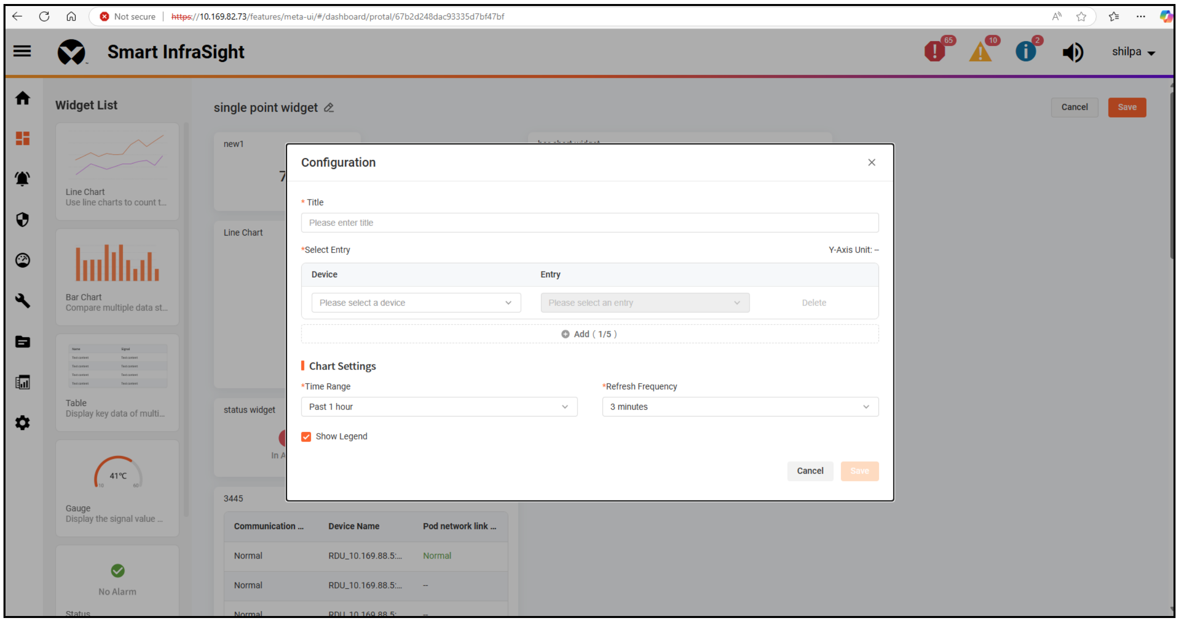
Figure 9.21 Bar Chart Widget Configuration Item



The configuration items are as follows:

- Title: Defines the widget title and displays it in the widget header after it is configured.
- Data Source: Users can select a site or device as the data collection source.
- Options:
  - When a user data source selects a site, a drop-down list of sites and entry is displayed in the selection. After selecting any site, the user can select the total number of alarms, the number of emergency alarms, the number of important alarms, and the number of general alarms.
  - When the user selects a device as a data source, a drop-down box of the device and the entry will be displayed in the selection, and the user can select the total number of alarms, the number of emergency alarms, the number of important alarms, the number of general alarms, and the alarm signal point in the item.
  - Users can click the Add button to add multiple data for comparison (up to 10 items), and the added entries must have the same unit; The signal unit selected in the first row is displayed on the Y axis as a uniform Y-axis unit; Users can also click the delete button in each row to delete the operation.
- Time range: Select the time range from the Time Range drop-down menu. The options must include Past 1 Day and Past 7 Days, with Past 1 Day set as the default.
- Signal aggregation method: When the user data source selects the device, the signal summary configuration item is displayed, and the user can select the signal aggregation method from the drop-down box, the signal aggregation method will affect the final statistical value of the device signal, please carefully select the appropriate aggregation method;

Figure 9.22 Bar Chart Widget



- Bar sorting: The user can select different bar sorting options, which will affect the sorting of the column. The default sorting is set to Default Order.
- Refresh frequency: Users can refresh the widget based on this configuration item to refresh the display of the Bar Chart in real time. default refresh frequency is 1 hour.

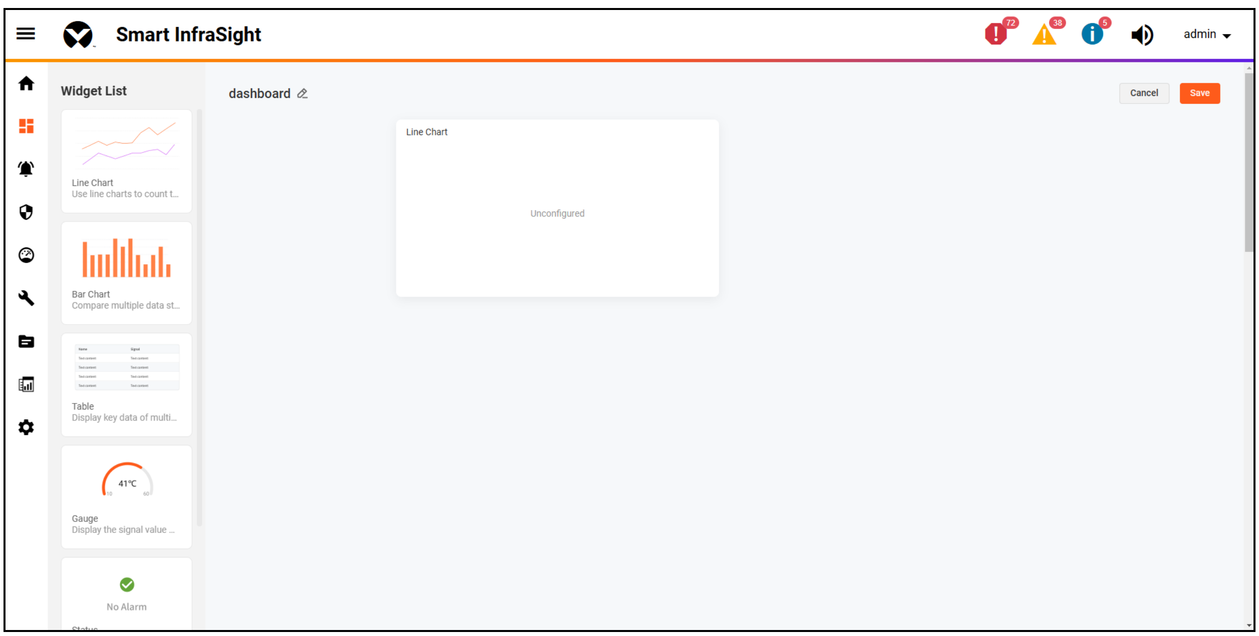
Once all the configurations are done, click on the Save button and the title will show the widget name. The user can scroll the mouse wheel to zoom in and out of the Bar Chart, and the mouse will display the details of the current bar when the mouse slides over the corresponding bar; The final widget renders as follows:

Figure 9.23 Bar Chart widget

9.4.6 Line Chart Widget

The line chart widget is used to count the changes of multiple data in a specific time range, and users can select important signals, view the change trend of the signal point within a certain range, and judge whether there is a risk in time. The configuration pop-up box is shown in Figure 9.24 below .

Figure 9.24 Line Chart Widget Configuration Item

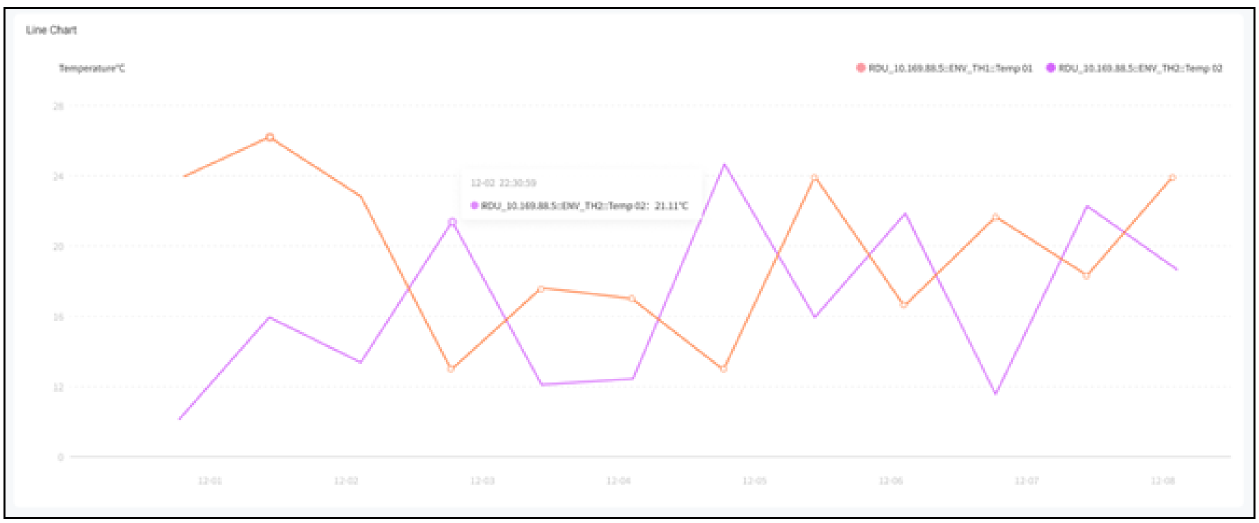


The configuration items are as follows:

- Title: Defines the widget title and displays it in the widget header after it is configured.
- Select Entry:
  - The user can select a device and then choose an entry (signal) value under that device as the data source for the line chart. Up to 5-line charts can be added;
  - The user can view the Y-axis units of the current line chart outside the list; The units of all selections must be consistent;
- Time range: User can select the time range for displaying the changes of signal points within this time range. default time range is set to be past 1 hour (The custom time range must not exceed two weeks).
- Refresh rate: Users can select an appropriate refresh rate to update data in a timely manner.
- Show Legend: the user can choose whether to display the legend, when the legend is displayed, after clicking the legend, the line will be dynamically hidden, which is more convenient to view the data.

After all configurations are completed, based on the display legend toggle, the user can view the legend in the format of station, device, and signal. All lines will be displayed, allowing the user to observe data trends over the selected time range. The line chart is minimized to a 1×1 size, with the units, legend, and horizontal axis hidden, showing the final compact view, as shown in **Figure 9.25** below .

Figure 9.25 Line Chart



10 Alarm

10.1 General

10.1.1 Overview

Alarm is the main function module of the entire Smart InfraSight™ platform to monitor alarms and obtain alarm information, users can obtain the Active alarm and Alarm history list in the alarm module, and can export the alarm list to the local computer in excel format.

10.1.2 Functional Modules

Smart InfraSight™ alarms include the following functional modules, and for details about each feature refer Detailed Functions .

- Active Alarm
- Alarm history

10.2 Quick Start

10.2.1 Rapid Deployment Steps

To ensure that you can view the alarm information, perform the following operations:

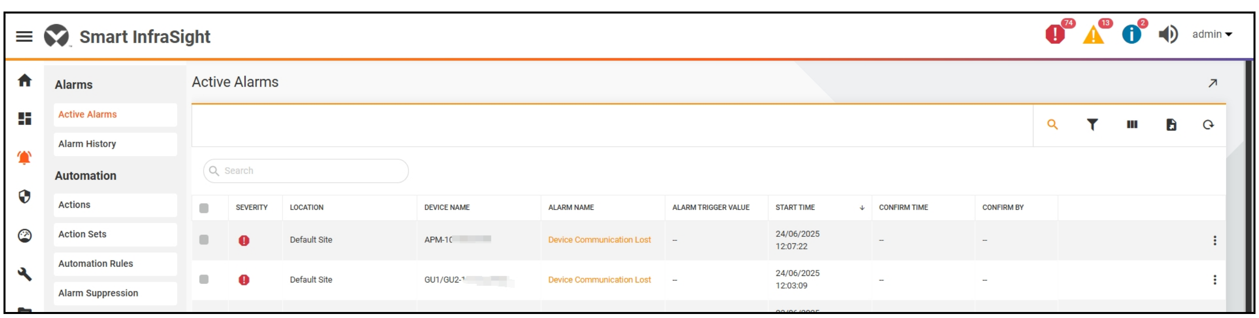
1. View the list of Active Alarms.
2. View the list of Alarm history.

10.2.2 Example

Active Alarm

When you select the Alarm tab in Smart Infrasight, the first menu that opens is Active Alarms, where you can view a list of active alarms. The list includes columns for Severity, Location, Device Name, Alarm Name, Alarm Trigger Value, Start Time, Confirm Time, and Confirmed By. You also have the operation to View Details and perform the Confirm action. As shown in Figure 10.1 below .

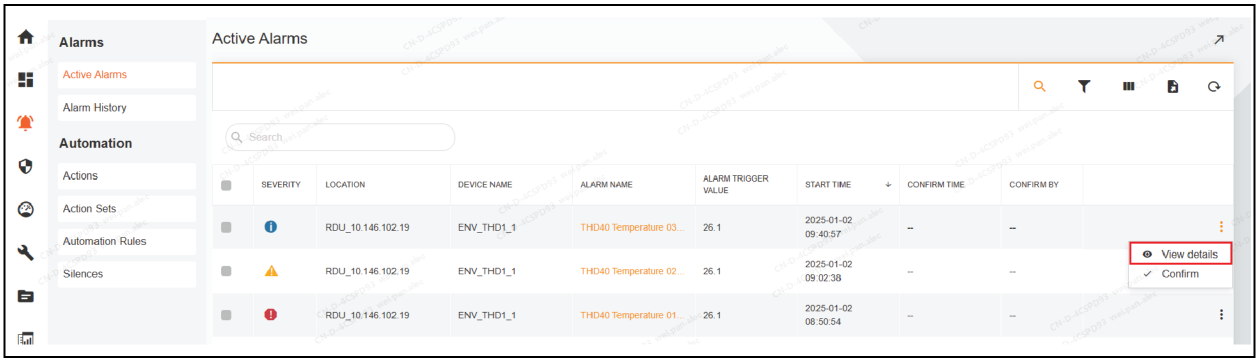
Figure 10.1 Current Alarms



Viewing the Alarm Details

On the Current Alarm or Stored Alarms page, click on the *ellipses* icon on the right side of an alarm row and click on the *View Details* icon. As shown in **Figure 10.2** below .

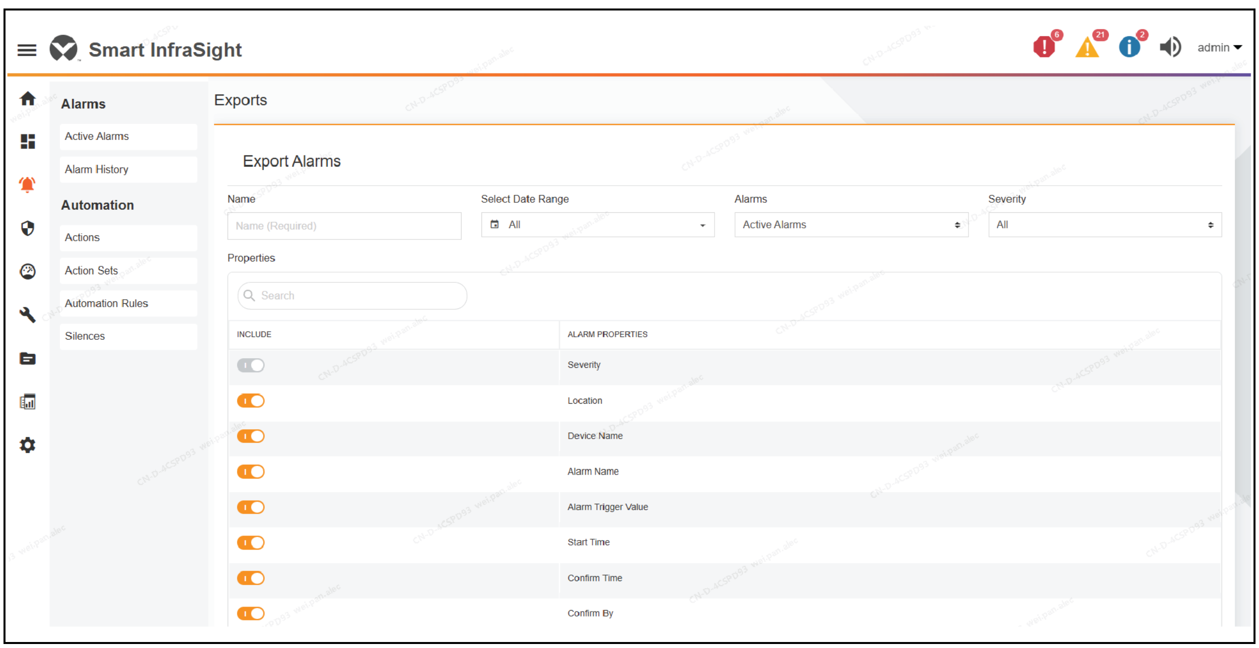
Figure 10.2 Viewing the Alarm Details



Export Alarms

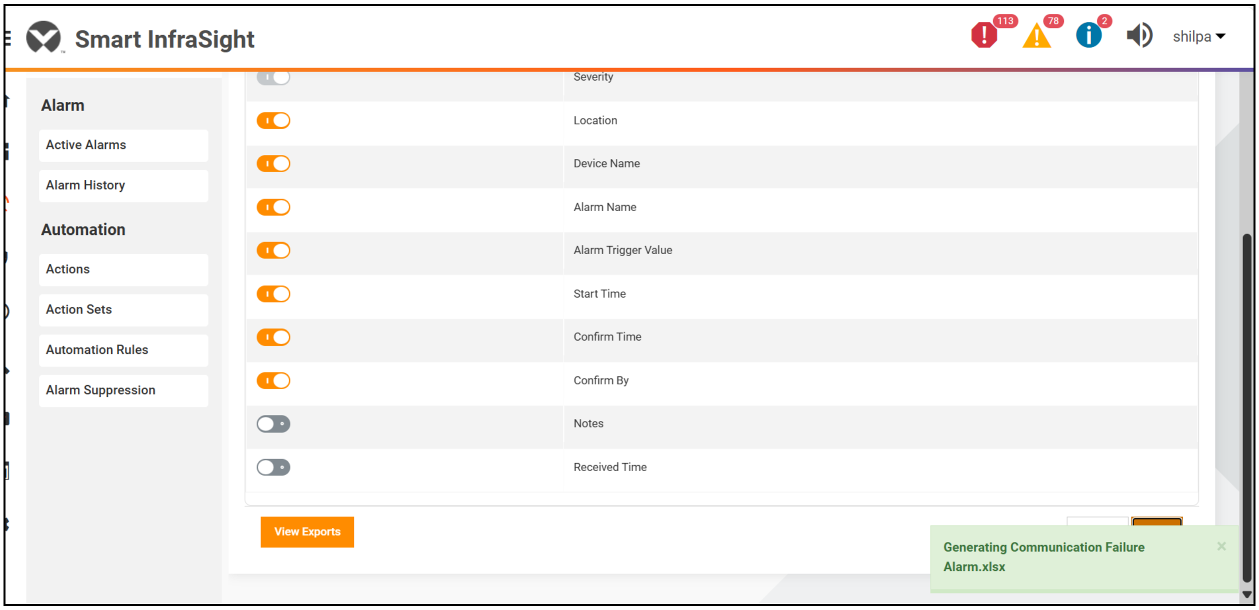
As show in **Figure 10.3** below In the alarm list, click the Export Alarm button in the upper-right corner. This will redirect you to the Export Alarm page, where you need to enter the file name, select the date range, alarm type, alarm severity, and other relevant properties. Finally, click the Save button to export the alarm data.

Figure 10.3 Export Alarm List



After clicking Save, a **Generating alarm.xlsx successful** message will appear in the lower-right corner, as shown in **Figure 10.4** on the facing page .

Figure 10.4 Export Successful Popup

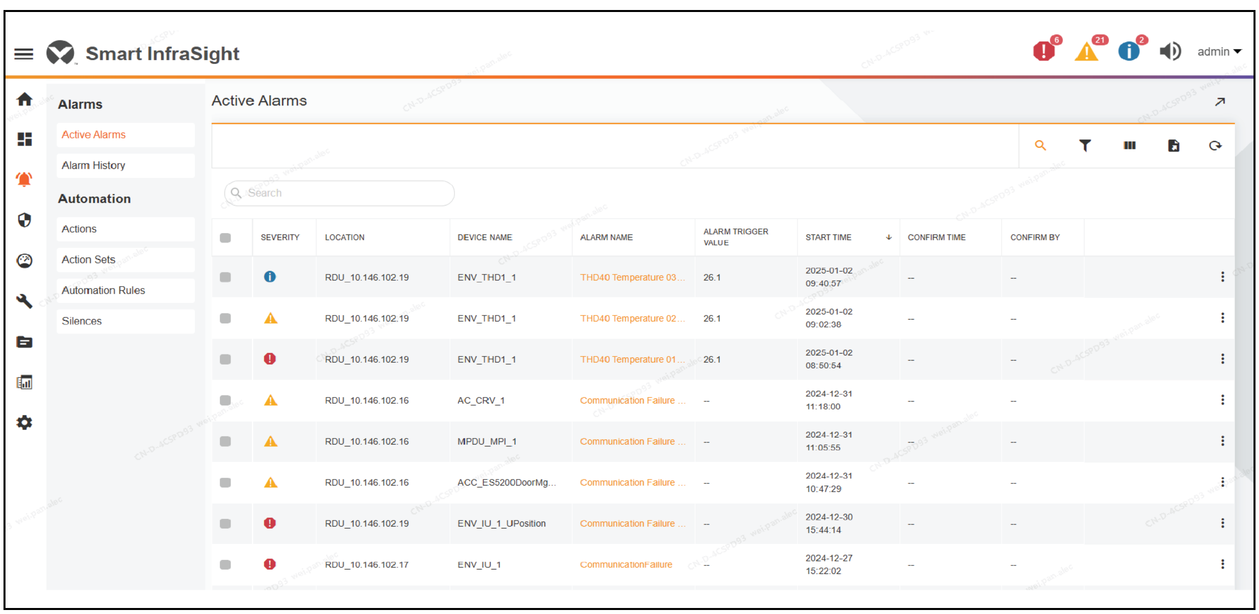


10.3 Detailed Functions

10.3.1 Active Alarms

If you select **Active Alarm** in the first-level menu, the Active alarm page will be opened by default, and the column menu will display the following fields: Select Icon, Severity, Location, Device Name, Alarm Name, Alarm Trigger Value, Start Time, Confirm Time, and Confirmed By, along with the operations View Details and Confirm, as shown in **Figure 10.5** below .

Figure 10.5 Active Alarm



NOTE: 1. If no alarm is found, no alarm is displayed in the list.

2 The search button in the table is orange by default, the search box is displayed by default, when the search button is clicked, the button turns black and the search box is hidden. The system saves the last state of the search button.

3. When the Filter button is clicked, fields for Date Range, Group By, and Alarm Severity should be displayed. The Filter button should appear in orange when the filter fields are visible, and in black when the filter fields are hidden.

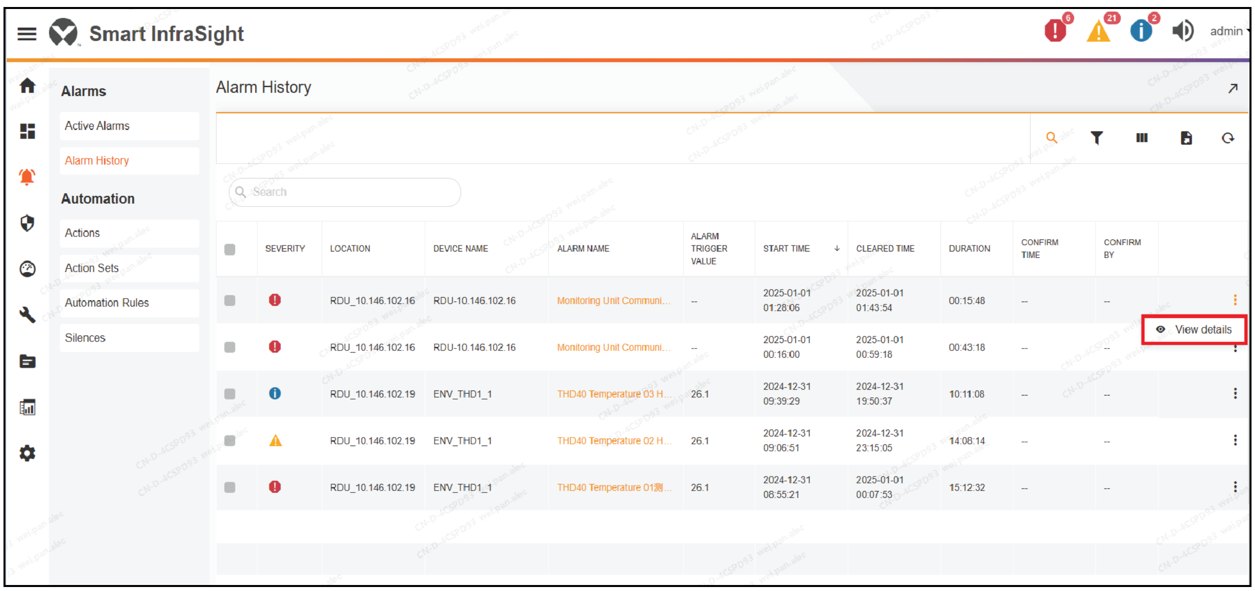
4. When the Column icon is clicked, a list of all column names is displayed. By clicking on a column name, you can toggle the visibility of that specific column in the list.

5. on click the reload icon we can reload the page.

10.3.2 Alarm History

When the Alarm History tab is selected from the menu, as shown in Figure 10.6 below , it displays the existing list of alarms in the current system. The table includes the following columns: Severity, Location, Device Name, Alarm Name, Alarm Trigger Value, Start Time, Cleared Time, Duration, Confirm Time, and Confirmed By, along with a View Details operation.

Figure 10.6 Viewing Alarm history



NOTE: 1. If no alarm is found, No Alarm is displayed in the list.

2. The search button in the table is orange by default, the search box is displayed by default, when the search button is clicked, the button turns black, and the search box is hidden. The system saves the last state of the search button.

3. When the Filter button is clicked, fields for Date Range, Group By, and Alarm Severity should be displayed. The Filter button should appear in orange when the filter fields are visible, and in black when the filter fields are hidden.

4. When the Column icon is clicked, a list of all column names is displayed. By clicking on a column name, you can toggle the visibility of that specific column in the list.

5. Click on the reload icon we can reload the page.

10.3.3 View Details

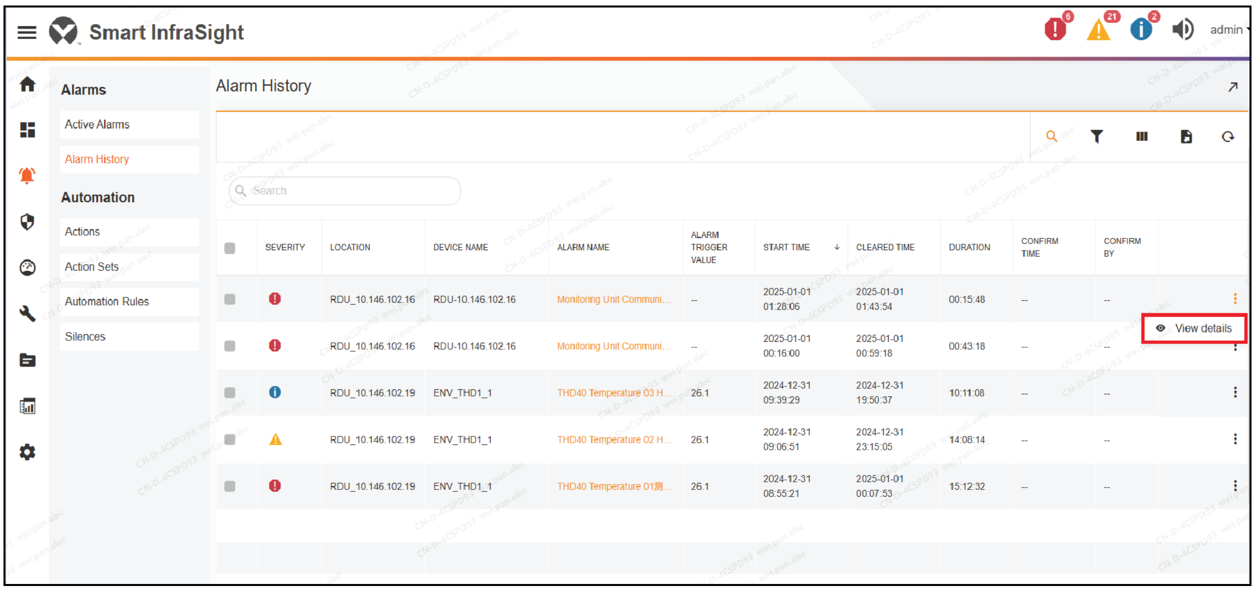
You can view alarm details in either of the following ways:

1. On the Active alarm or alarm history page, click the *ellipses* on the right side of an alarm line, and then click View Details, as shown in **Figure 10.7** below .

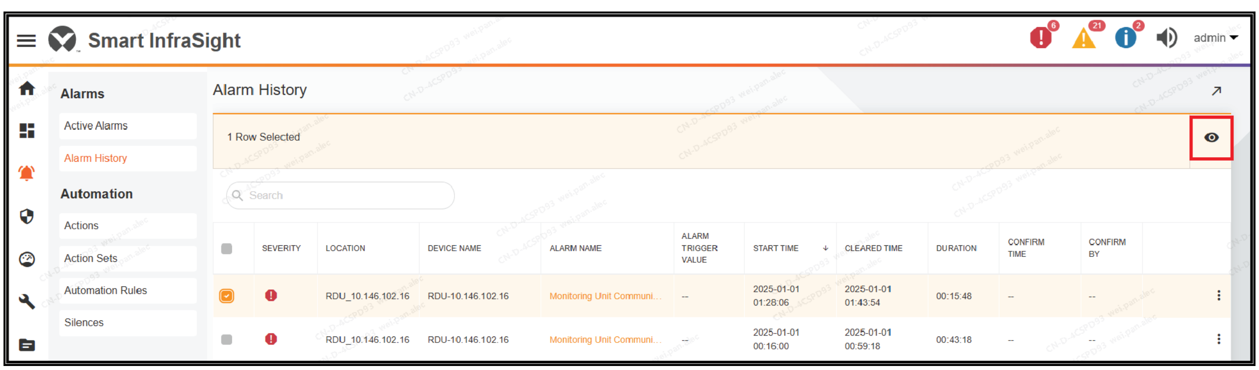
2. Or select an alarm in the multi check box on the left, and one row will be display on the top of the search box then click on eye icon for view details, as shown in below .

After clicking View Details, detailed information about the alarm is displayed, including additional attributes such as Add Notes, Action History, and Status Record.

Figure 10.7 Viewing Alarm Details—Method 1



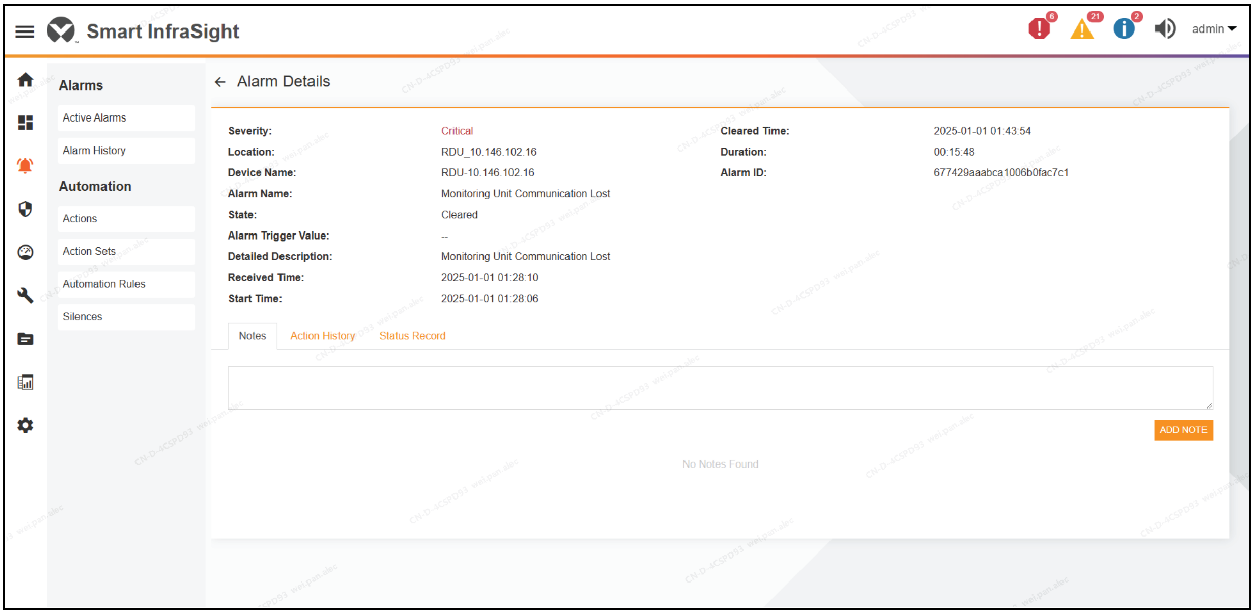
Viewing Alarm Details—Method 2



10.3.4 Alarm Notes

On the alarm details page, click the *Notes* tab at the bottom, enter a comment in the input box, and click the *Add Note* button. The successfully added note will be displayed in the list of notes below, as shown in **Figure 10.8** on the next page , after adding the notes on page you can edit or delete the notes.

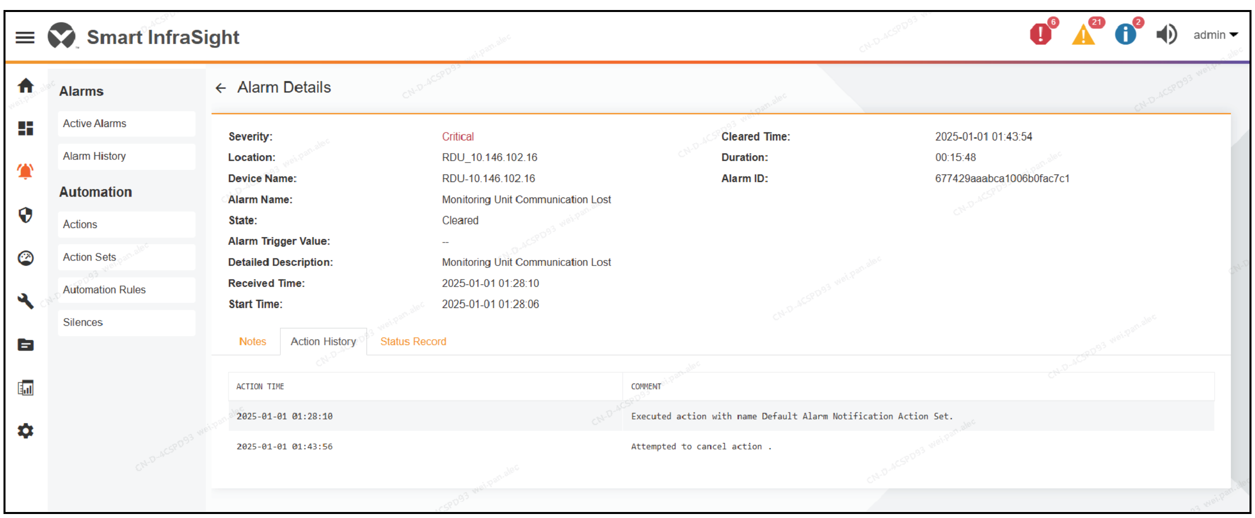
Figure 10.8 Adding an Alarm Note



10.3.5 Action History

Click on the *Alarm Details* page as shown in **Figure 10.9** below , click the **Action History** tab at the bottom of the page to display the Action time and comment of records.

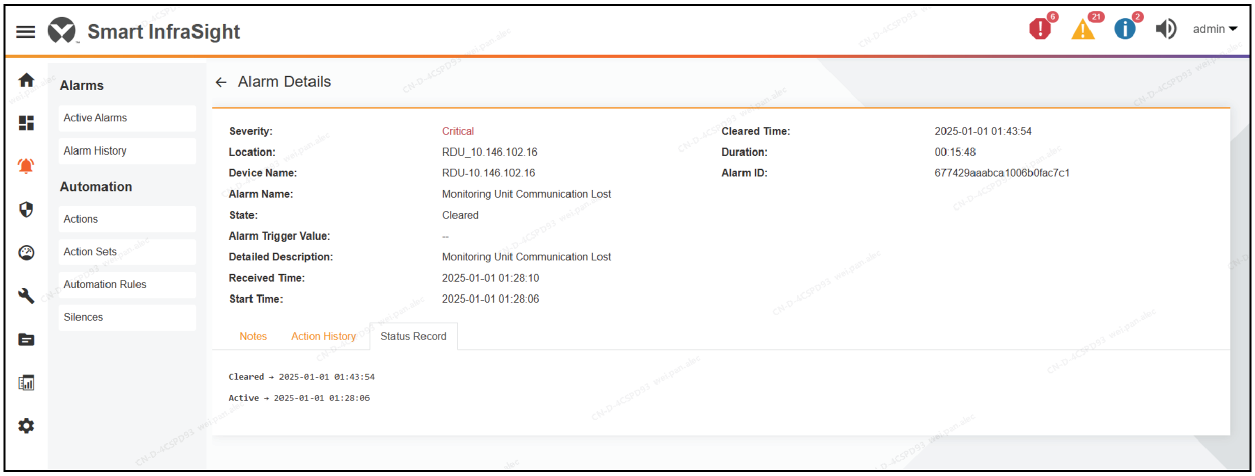
Figure 10.9 Viewing the Alarm Notification Records



10.3.6 Alarm Status Records

On the *Alarm Details* page, click the Status Records tab at the bottom to display the status record of the alarm as shown in **Figure 10.10** on the facing page , such as the time when the alarm was generated and the time when the alarm ended.

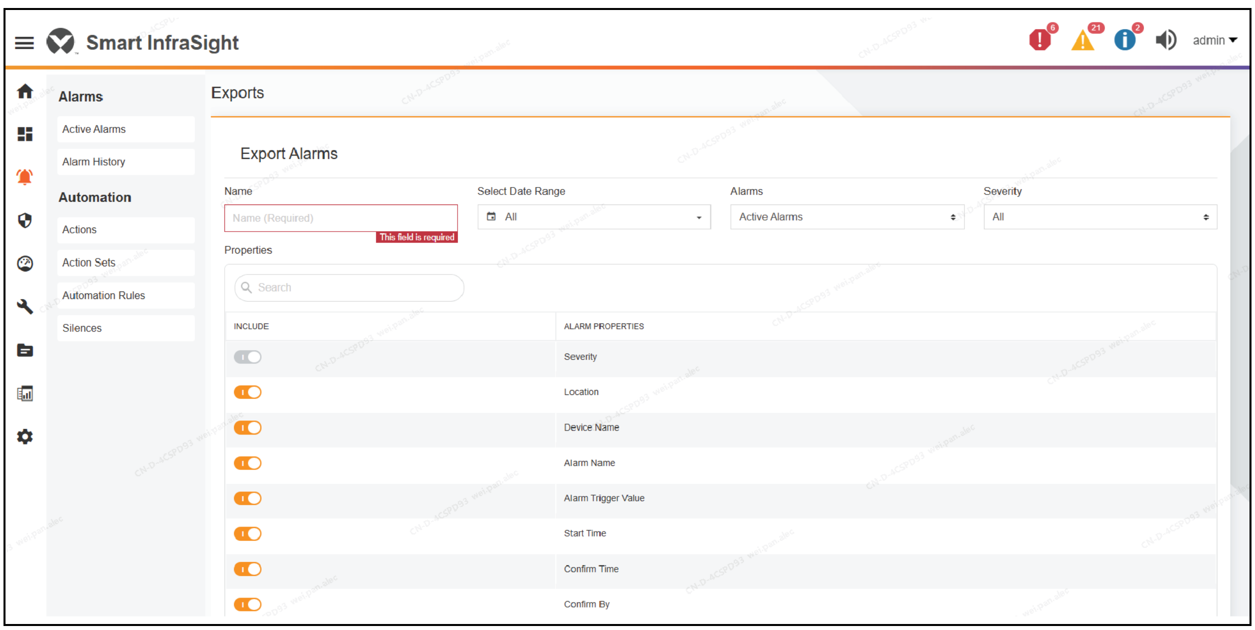
Figure 10.10 Viewing the Alarm Status Record



10.3.7 Export Alarms

On the alarm list page, click *Export* in the upper right corner, as shown in Figure 10.11 below ,Enter the file name, select the date range, alarm type, and severity, then click the Save button to export the alarm.

Figure 10.11 Export Alarm



After clicking save, you will see a message as shown in Figure 10.12 on the next page in the lower right corner indicating that it is generating. After the export is successful, you can display a message in the lower right corner.

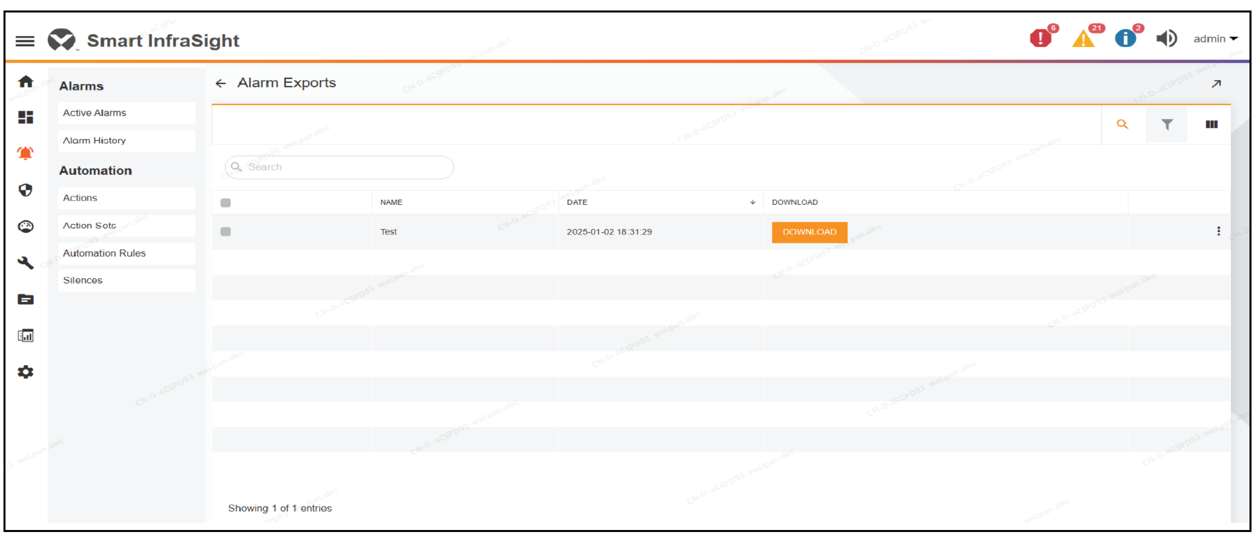
Figure 10.12 Export Alarm Popup

After the export is successful as shown in **Figure 10.13** below , you can click the *View Export Record* button to enter the export record, on the Alarm Export Records page, you can download alarm record in Excel as shown in **Figure 10.14** below .

Figure 10.13 Export Completion Popup

NOTE: Users can only search and download the alarm records exported from this account.

Figure 10.14 Downloading and Exporting the Report to Excel



11 Automation Notification

11.1 General

The alarms generated by the computer room monitoring system can be notified to users by email, SMS, and voice, and the devices under the site can also be controlled through alarm linkage.

11.1.1 Functional Modules

The following function modules are set for notification, and refer the Detailed Features on page 210 for detailed information about each function module.

- Action settings, including notification selection and notification rule settings for email, SMS, voice, and linkage
- Action combination settings
- Alarm binding settings
- Alarm silence rules

11.2 Quick Start

11.2.1 Rapid Deployment Steps

The main deployment steps of linkage settings are as follows:

1. Set the e-mail server connection configuration, SMS modem configuration, and test voice notification configuration separately.
2. Set the action.
3. Set the action combination.
4. Set alarm binding.

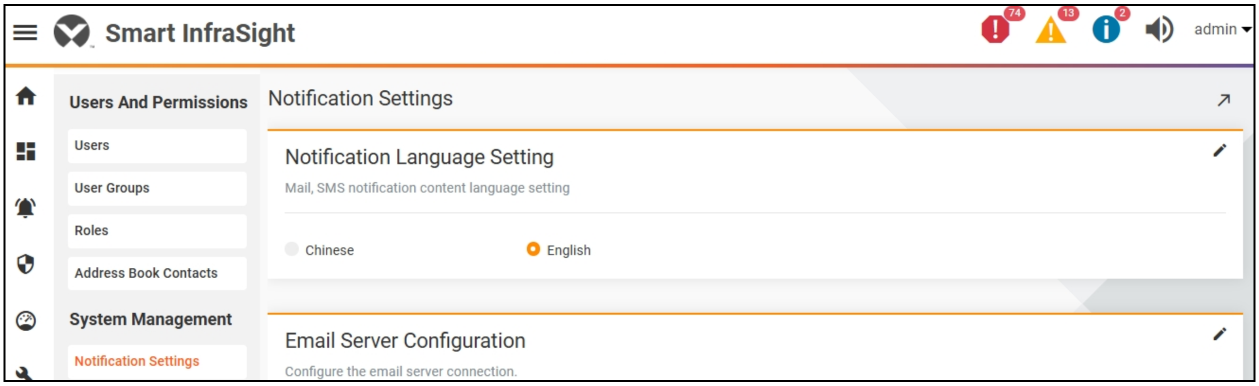
11.2.2 Example

Suppose that the ambient temperature of the front door temperature sensor device of Cabinet 1 is too high and the alarm needs to be notified to the user by email, SMS, and voice, and the related devices can be controlled.

Set the Notification Content Language Type

In the Smart InfraSight™ web page, click on the *Settings* and open the menu to enter the notification settings page as shown in Figure 11.1 on the next page , and set the language in which the notification content will be sent, which is the server by default Language, select the language of the notification content, and click the *Save*.

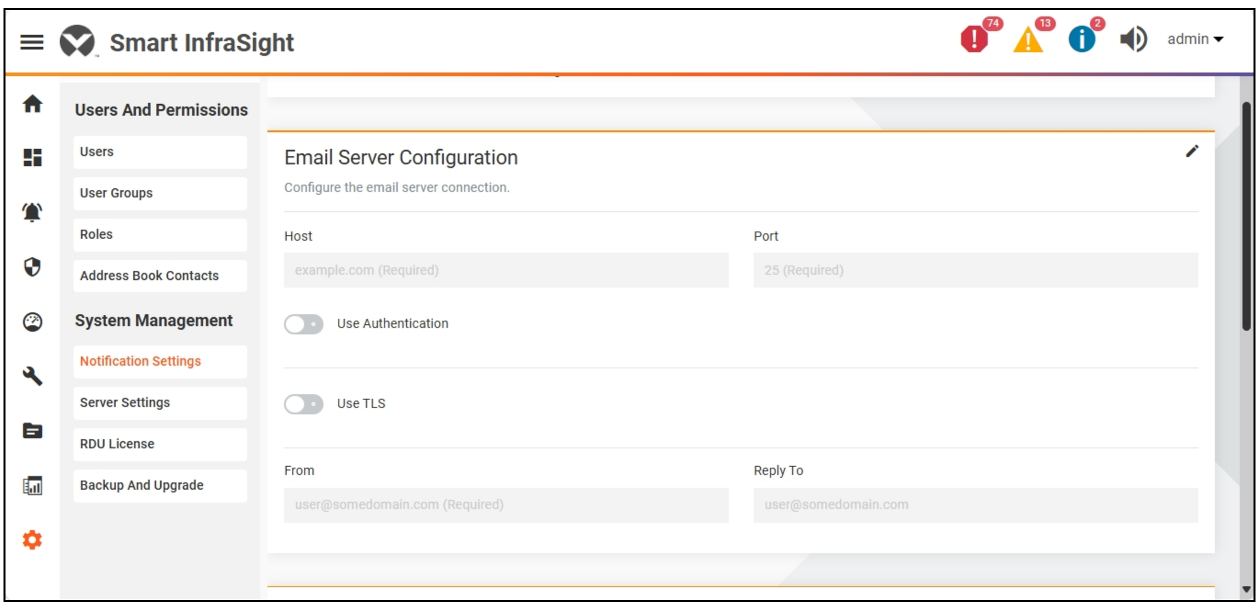
Figure 11.1 Notification Settings— Notification Content Language Settings



Set up the e-mail Server Connection Configuration

On the Notification Settings page, set the email server connection configuration. As shown in **Figure 11.2** below .

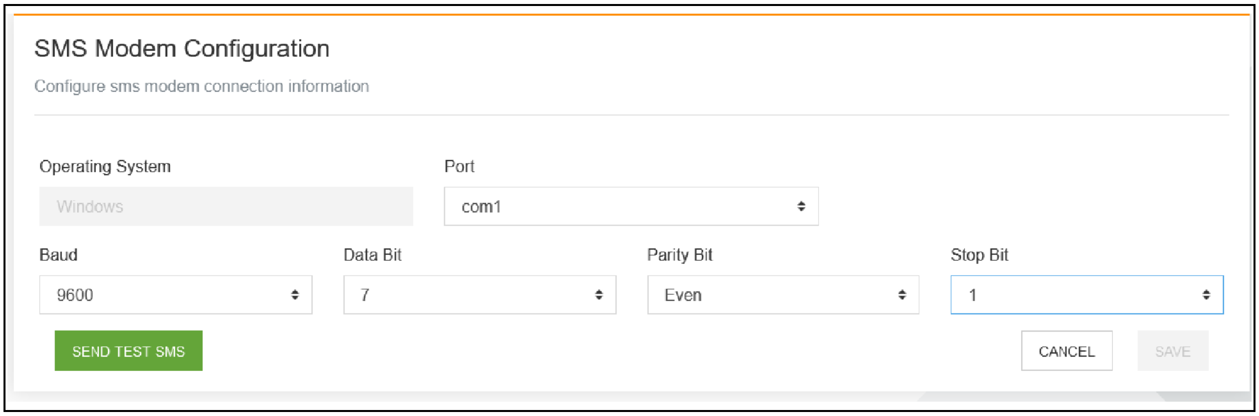
Figure 11.2 Notification Settings— Mail Server Configuration Settings



Set up the SMS Modem Configuration

Smart Insight only supports certain models of SMS modems, if necessary, contact customer service to purchase. Set up the SMS modem configuration, as shown in **Figure 11.3** on the facing page , when plugged into the SMS modem, select **USB** for **Port**.

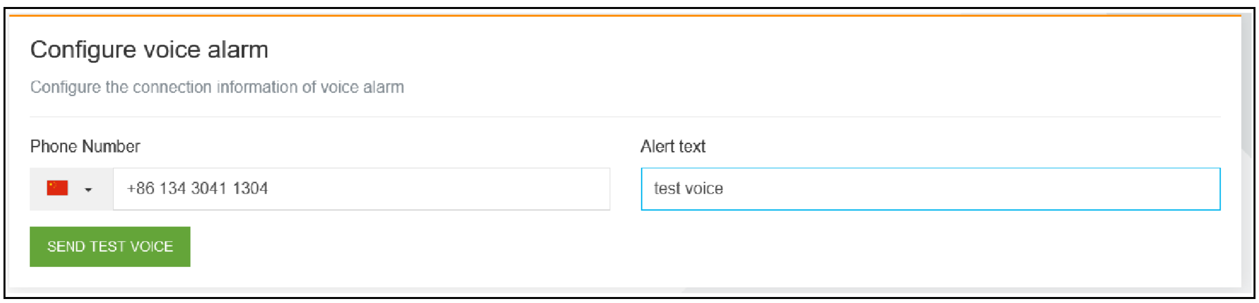
Figure 11.3 Notification Settings - SMS Modem Configuration Interface



Configuring the Voice Alarms

Smart Insight only supports specific models of voice modems, if necessary, please contact customers to purchase (only for use in Chinese mainland). Set the voice alarm configuration, **Figure 11.4** below , and select **USB** for **Port** after the voice modem is plugged in.

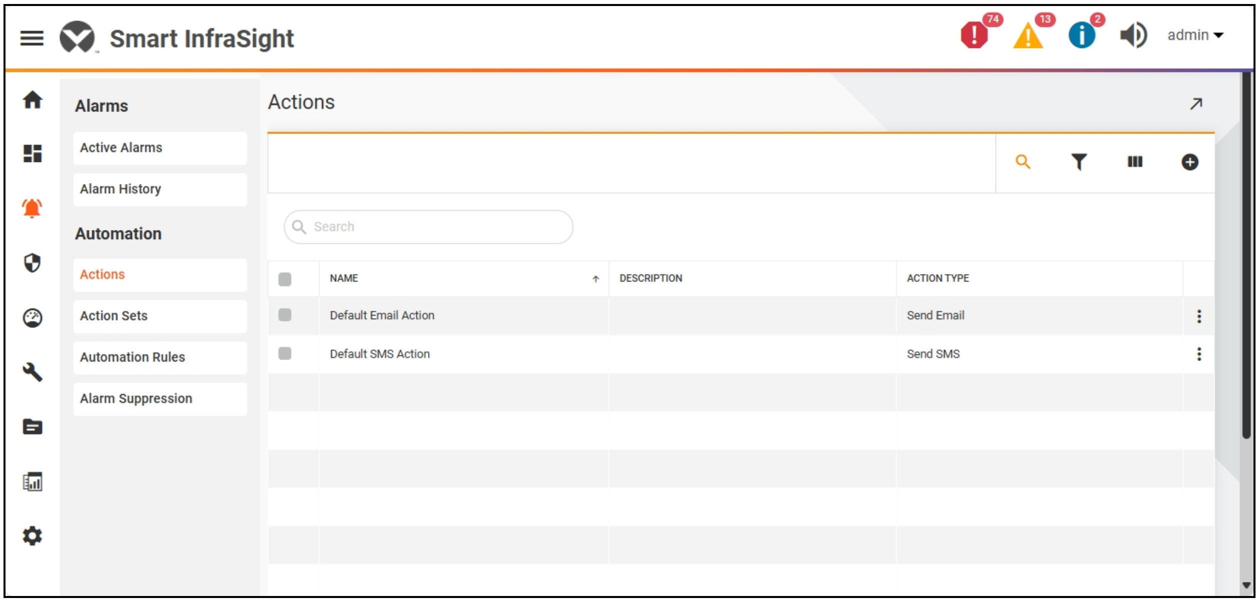
Figure 11.4 Configuring the Voice Alarms



Set up the Action

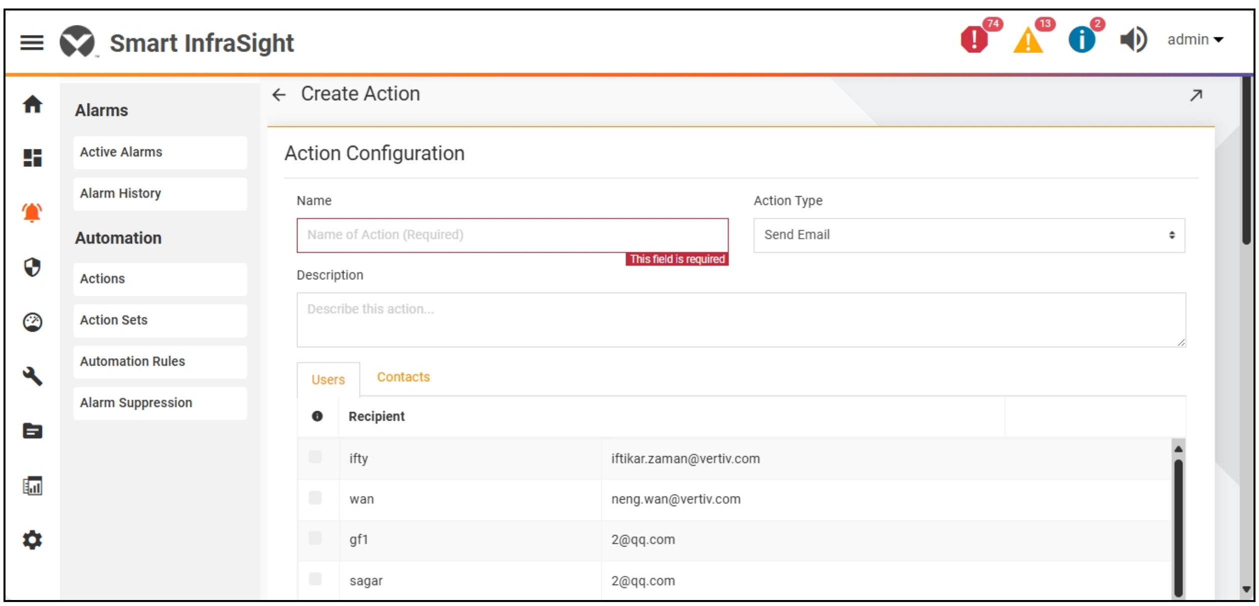
1. On the smart InfraSight click on the Action tab from the automation to enter the Action page. As shown in **Figure 11.5** on the next page .

Figure 11.5 Action Interface



2. On the Action page, click the Add icon to add the action configuration. As shown in **11.1** on page 203 .

Figure 11.6 Adding an Action Page



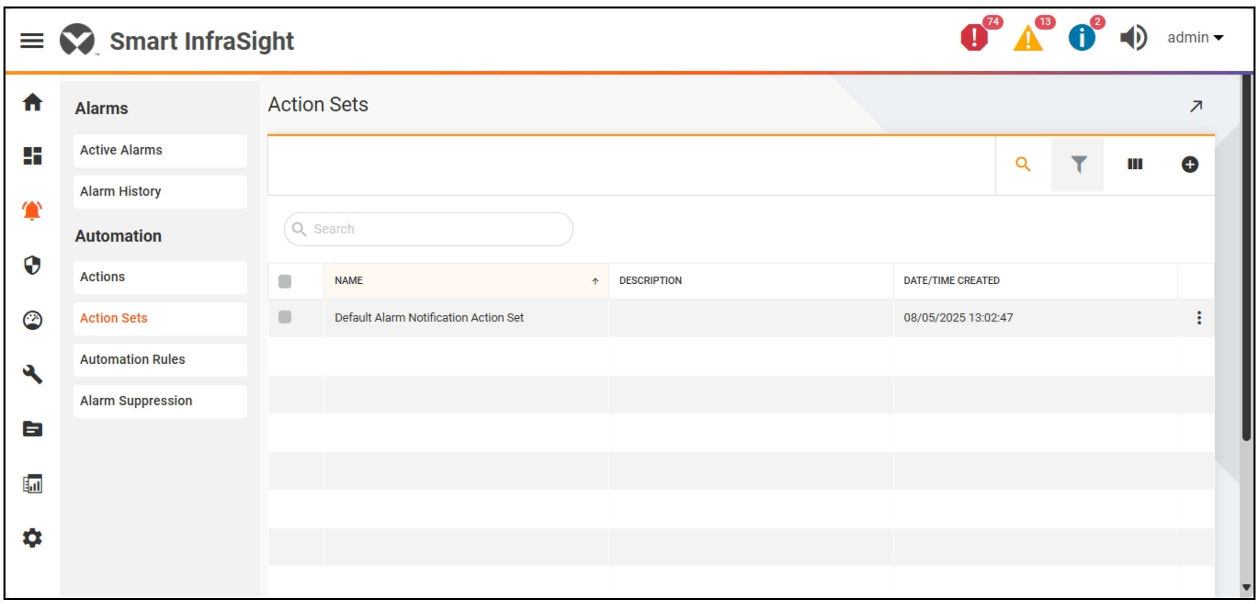
3. Enter the name and select the action type as 'Send Email'. Add a description in the description box. Then, select the recipient from the user list or contact list. Set the action delay (in seconds), retry count (for unrecognized alarm repeat notifications), retry interval and unit, and add a comment if needed. Finally, set the schedule notification and click *save*.
4. Enter the name and select the action type as 'Send SMS'. Add a description in the description box. Then, select the recipient from the user list or contact list. Set the action delay (in seconds), retry count (for unrecognized alarm repeat notifications), retry interval and unit, and add the comment if needed. enable clear Alarm notification and Enable alarm escalation if needed. Finally set the schedule notification and click *save*.

5. Enter a name and select *Send Control* as the action type. Provide a description in the description field. If required, enable the *Alarm End Control* checkbox. Next, in the Command List section, click the Add icon to open the *Select Command* pop-up window. Within the pop-up, choose the desired location and device, then select the appropriate command name and parameters by checking the corresponding boxes. Click *OK* to confirm. Finally, configure the action delay and click *Save*.
6. Enter the name and select the action type as *Send Voice*. Add a description in the description box. Then, select the recipient from the user list or contact list. Set the action delay (in seconds), retry count (for unrecognized alarm repeat notifications), retry interval and unit, and add the comment if needed. enable clear Alarm notification and Enable alarm escalation if needed. Finally set the schedule notification and click *Save*. Retry interval and unit and add the comment if needed. enable clear Alarm notification and Enable alarm escalation if needed. Finally set the schedule notification and click Save.

Setup Action Sets

1. On the Smart InfraSight™ page, click the *Alarm menu* to enter the Action Set Settings on page 215 page. As shown in **Figure 11.7** below .

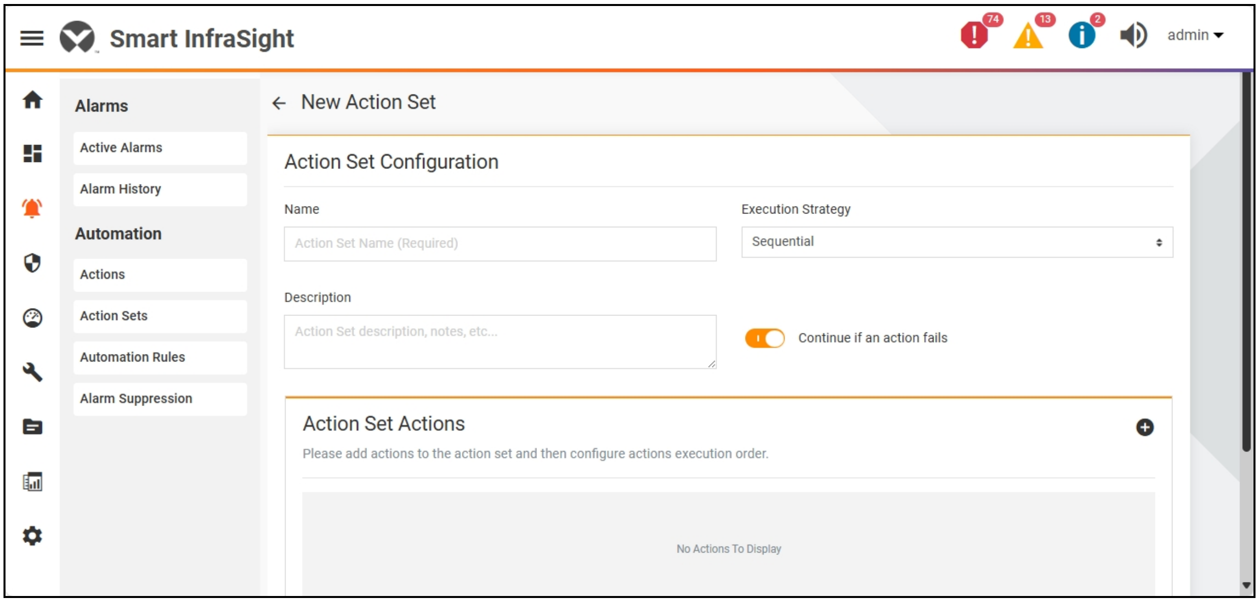
Figure 11.7 Action Set Interface



Add Action Sets

2. On the Action Sets, click *Add* button to enter the New Action Set. As shown in **Figure 11.8** on the next page .
3. Enter a name, execution strategy, description, and **add actions in the action set and arrange them in sequence.** Click *Save*.

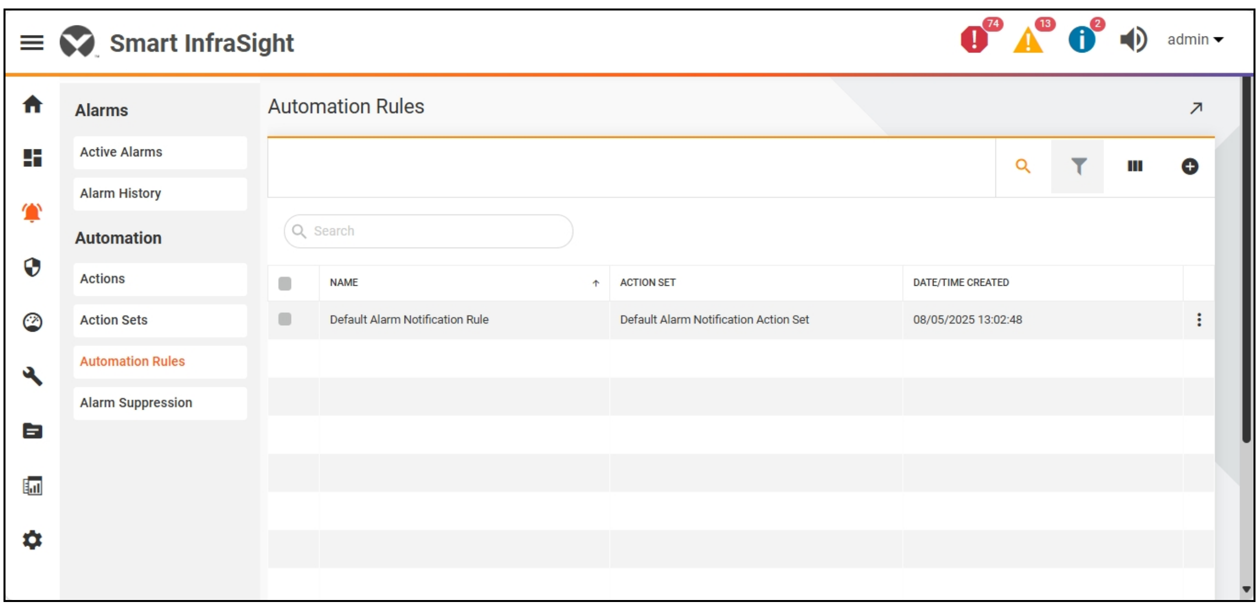
Figure 11.8 Creating a New Action Set



Configure Automation Rule

1. On the Smart InfraSight™ page, click the *Alarm* menu to enter the alarm binding settings page. As shown in Figure 11.9 below .

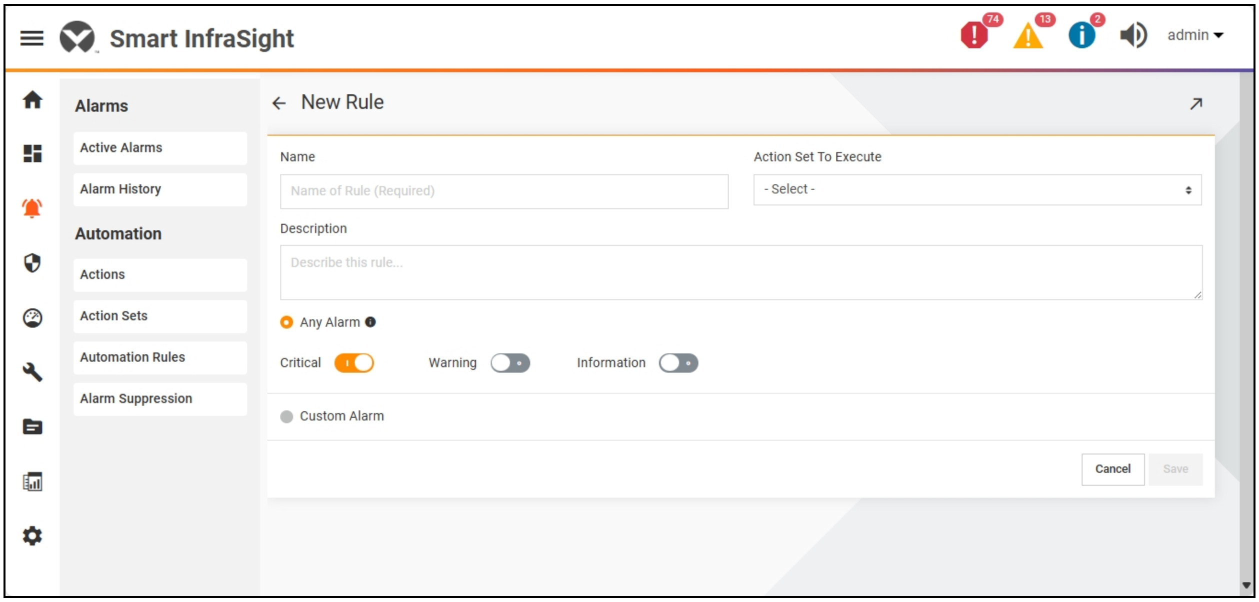
Figure 11.9 Alarm Automation Rule



Add Alarm Automation Rule

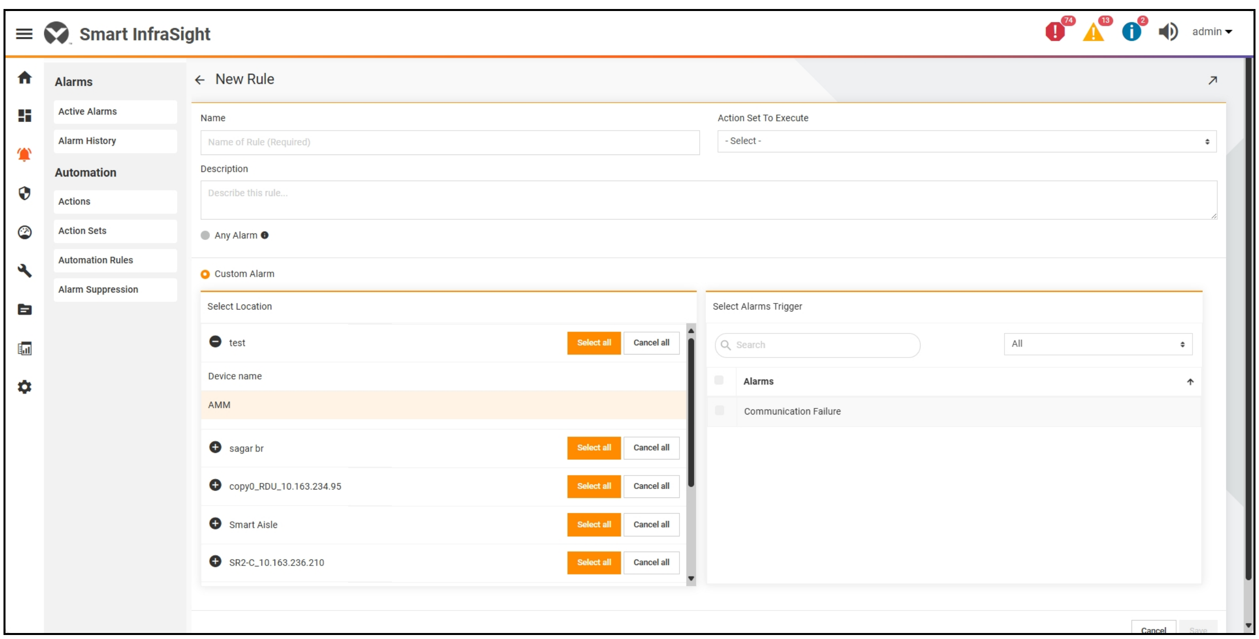
2. On the Alarm Automation Rule page, click the *Add* button to enter the Add Alarm Automation Rule page for creating new rule as shown in Figure 11.10 on the facing page .

Figure 11.10 Creating New Rule



3. Select or enter a name, select the Action Set that will be executed, a description, select the alarm severities (or some custom alarms that can trigger the action set) and click *Save*.

Figure 11.11 Adding Custom Alarms



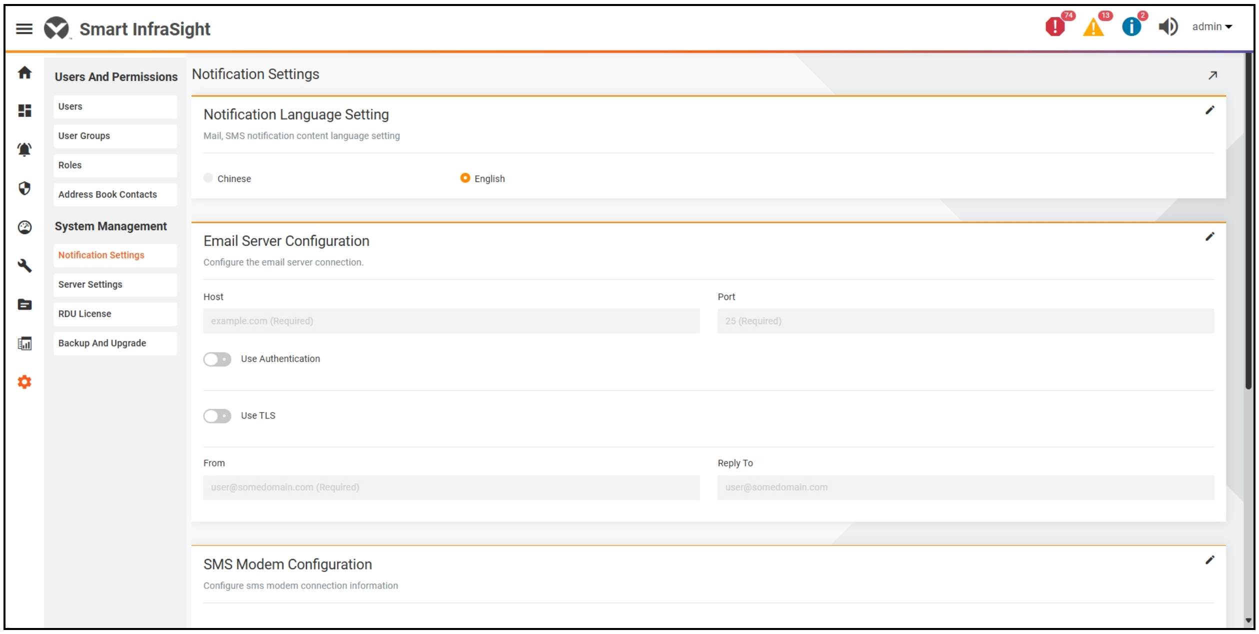
Once these steps are completed, the system will respond to selected alarms by notifying the specified email address and mobile phone number through email, SMS, and voice alerts. If alarm control is enabled, the system will also send the preset device commands accordingly.

11.3 Detailed Features

11.3.1 Email and SMS Notification Settings

On the Smart InfraSight™ web page, click on the *Administration* and open the notification settings page. As shown in **Figure 11.12** below .

Figure 11.12 Notification Setting Page



Notification Language Settings

On the notification settings page, click the *edit* icon in the upper right corner of the notification language setting screen to switch to the edit status. The Notification Language Setting affects the text in notification email, SMS, Voice.

E-mail Notification Settings

1. On the notification settings page, click the *edit* icon of the email server connection configuration, and the notification settings page switches to the edit state.
2. Enter the host, port (range: 1~65535), mail server login username, mail server login password, sender email address and reply email address (optional).

If you do not set a reply mailbox, the message will be replied to the sender's mailbox, and select whether to use TLS.

3. Click the **Send Test Email** to verify if Smart Infrasight can send emails through the email server.
4. Click *Save* to save the settings.

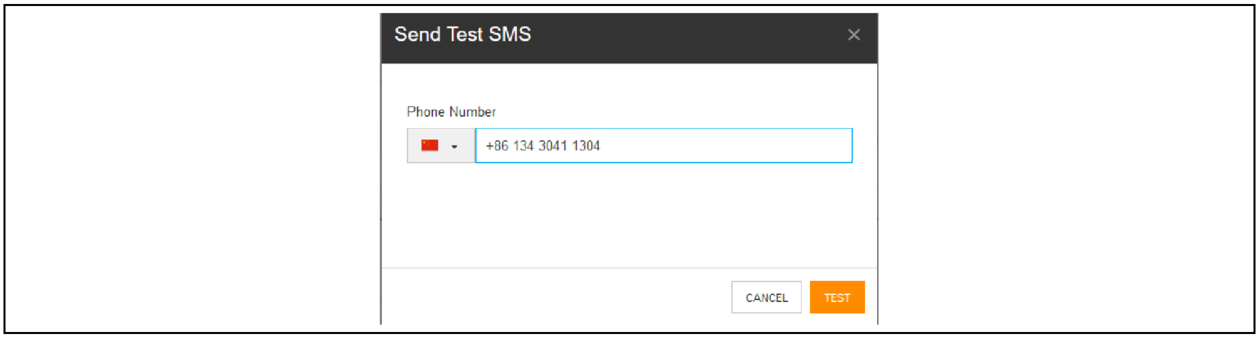
NOTE: The sender's mailbox and reply-to mailbox must actually exist in the mail server.

SMS Notification Settings

1. In the notification settings page, click the edit icon button of the SMS modem configuration, and the notification settings page switches to the edit state.

2. The recommended values for configuration are as follows: port selection **USB** (can only be selected after inserting the SMS modem), baud rate selection **9600**, data bit selection **8**, parity bit selection **No check**, stop bit selection **1**.
3. Click the Send Test SMS button, select the international number and set the recipient's mobile phone number in the pop-up window, as shown in the **Figure 11.13** below , click the Test button to check the SMS test result.

Figure 11.13 Sending the Test SMS



4. Click *Save* to save the settings.

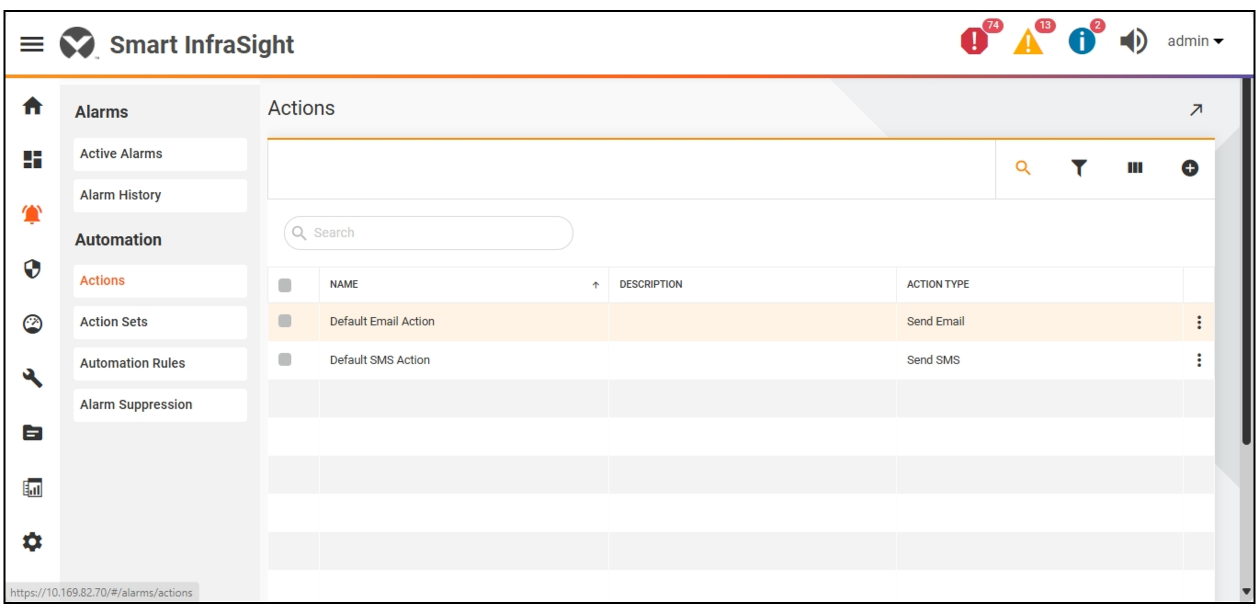
NOTE: 1. Sending SMS too often will cause the SMS to be intercepted by the telecom operator, and the intercepted SMS will not be sent to the target mobile number. If the sending number is intercepted, please call the telecom operator customer service number to cancel the interception. We recommend that you configure the SMS sending feature only for important events.

2. Supported modem model: TD-8411.

11.3.2 Action Settings

The action setting function is used to configure the alarm notification email, SMS, voice sending content and the action triggered by the alarm, click the *Alarm—Action* menu to enter the action setting page, as shown in **Figure 11.14** below .

Figure 11.14 Alarm Actions



New Actions

1. In the action settings page, click on Add button to enter the Add Action page, as shown in **Figure 11.15** below .

Figure 11.15 Adding an Action Page

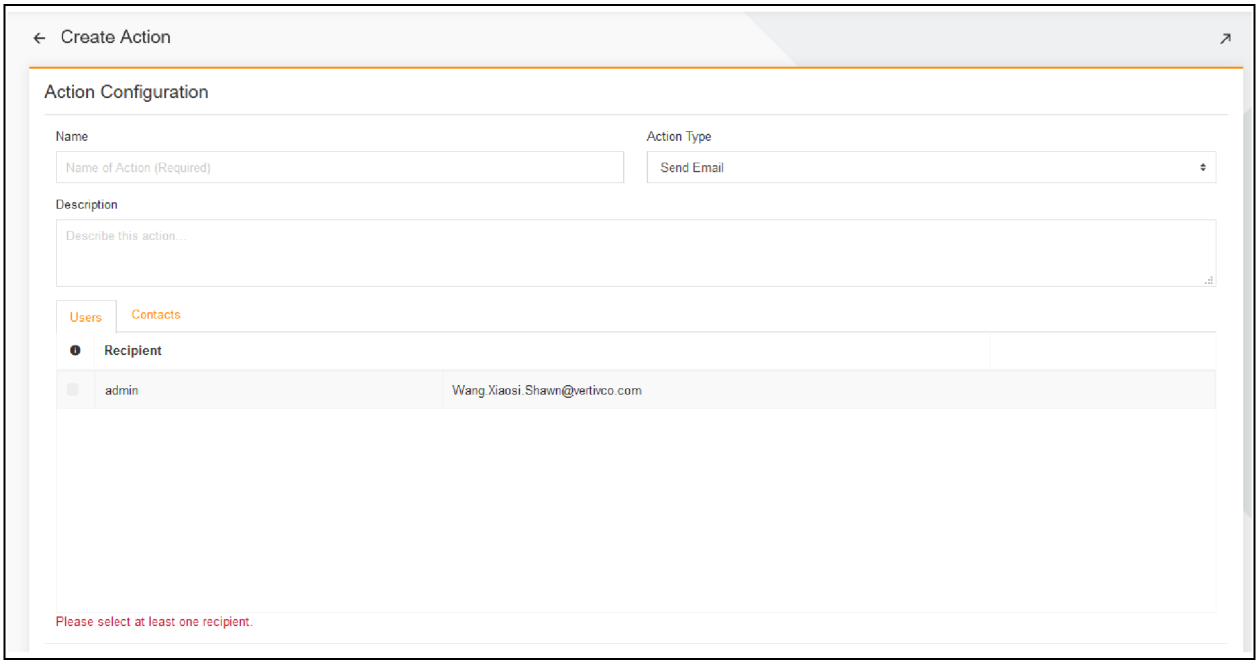
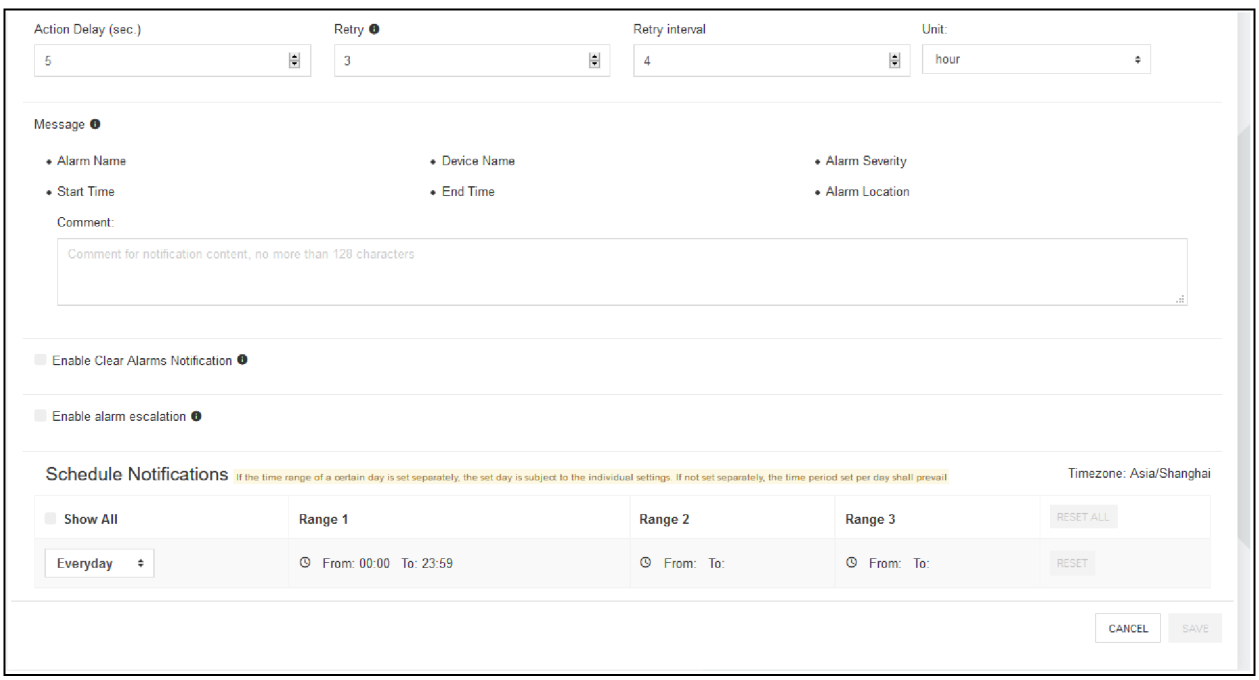
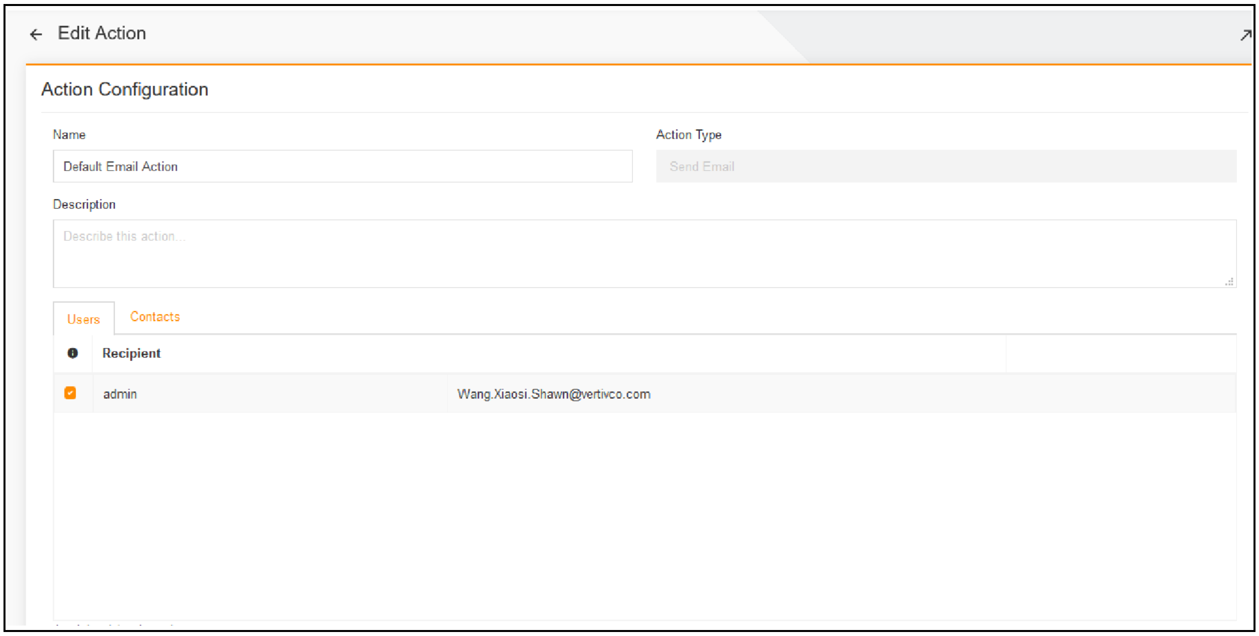


Figure 11.16 Action Page



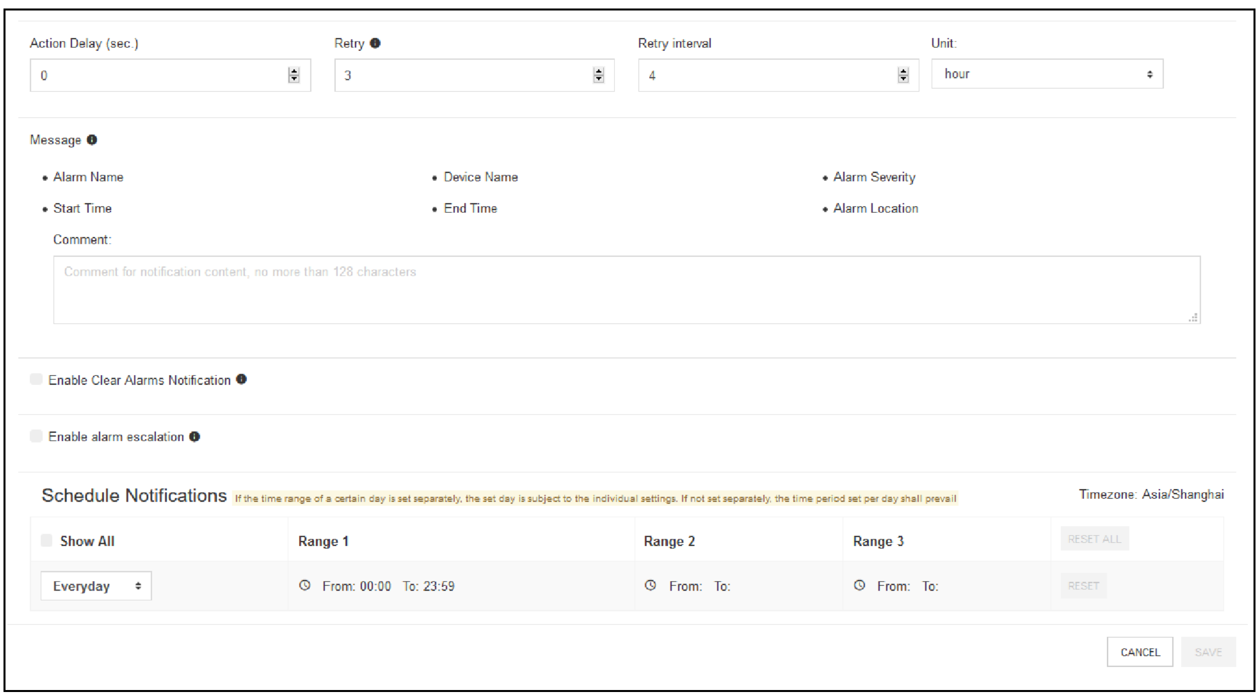
2. Enter the name, select the action type, description, recipient, operation delay, number of repetitions configuration, alarm notification content, and check whether to enable alarm end notification. Select whether to enable alarm escalation and schedule notifications, and click *Save*.



Editing the Action

In the Action list, click ellipses (...) on the right side of the action and select Edit to enter the Edit Action page. As shown in the **Figure 11.17** below .

Figure 11.17 Editing Action



Modify the Name, Description, Recipient, Operation Delay, Repeat Configuration, Alarm Notification Content, Enable Alarm End Notification, Enable Alarm End Escalation, Time Period Setting, and click *Save*.

Configuring Alarm Escalation

1. Check the **Enable alarm escalation**.

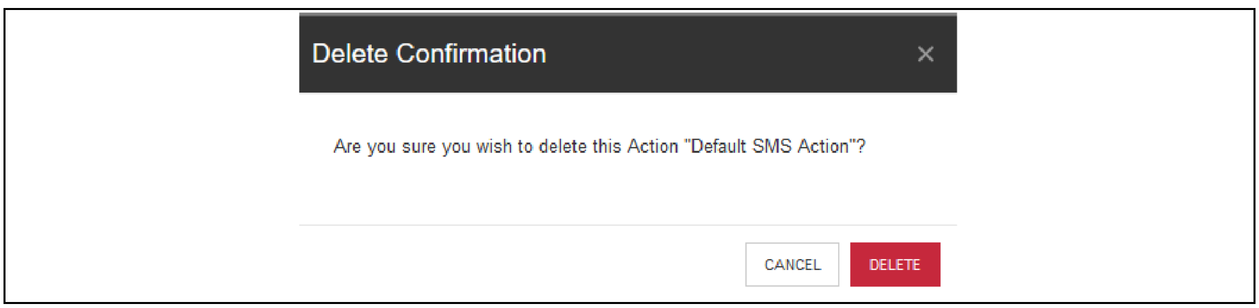
Figure 11.18 Alarm Escalation Configuration

2. Select receivers to which the alarm escalation notification are sent.

Deleting an Action

1. In the action list page, click the ellipses (...) on the right side of the action and, click the *Delete* button, and the page as shown **Figure 11.19** below will popup.

Figure 11.19 Deletion Confirmation Popup



2. Click *Delete*, and the action in action will be deleted.

Copy a Single Action

1. In the action list page, click ellipses (...) on the right side of the action.
2. Select Copy to copy the target action.

Batch Copying

1. In the action list page, select multiple actions to be copied. Click the *Copy* button to copy it.

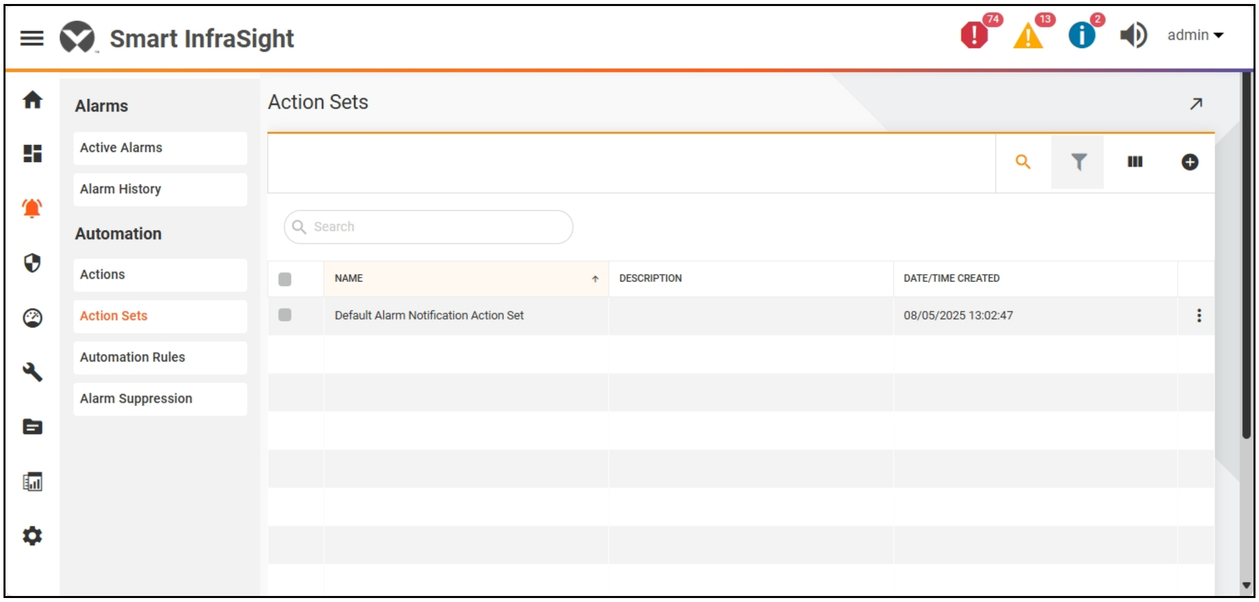
Batch Deletion

1. In the action list page, select multiple actions to be deleted. Click the *Delete* button to delete.

11.3.3 Action Set Settings

You can combine multiple alarm actions and set the order of action execution, and click the *Alarm—Action Combination* as shown in Figure 11.20 below menu to enter the action Set page.

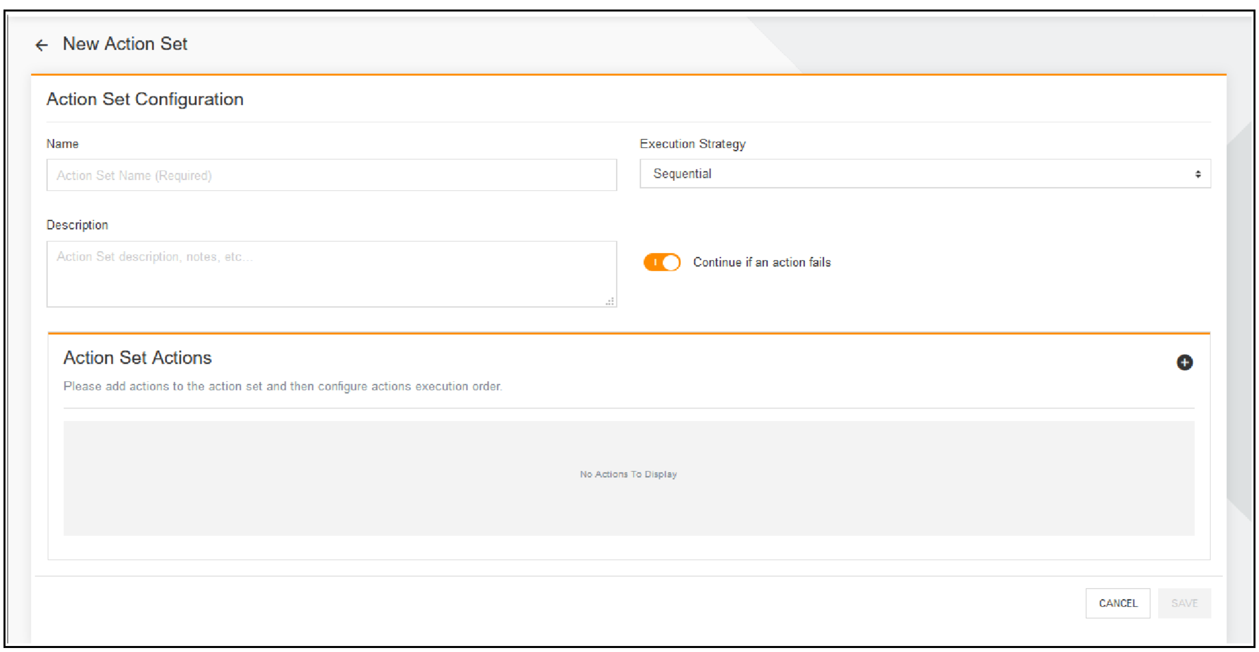
Figure 11.20 Action Sets List



Adding the New Action Set

1. In the action sets list page, click *Add* enter the New Action Set page. As shown in Figure 11.21 below .

Figure 11.21 Adding New Action Set



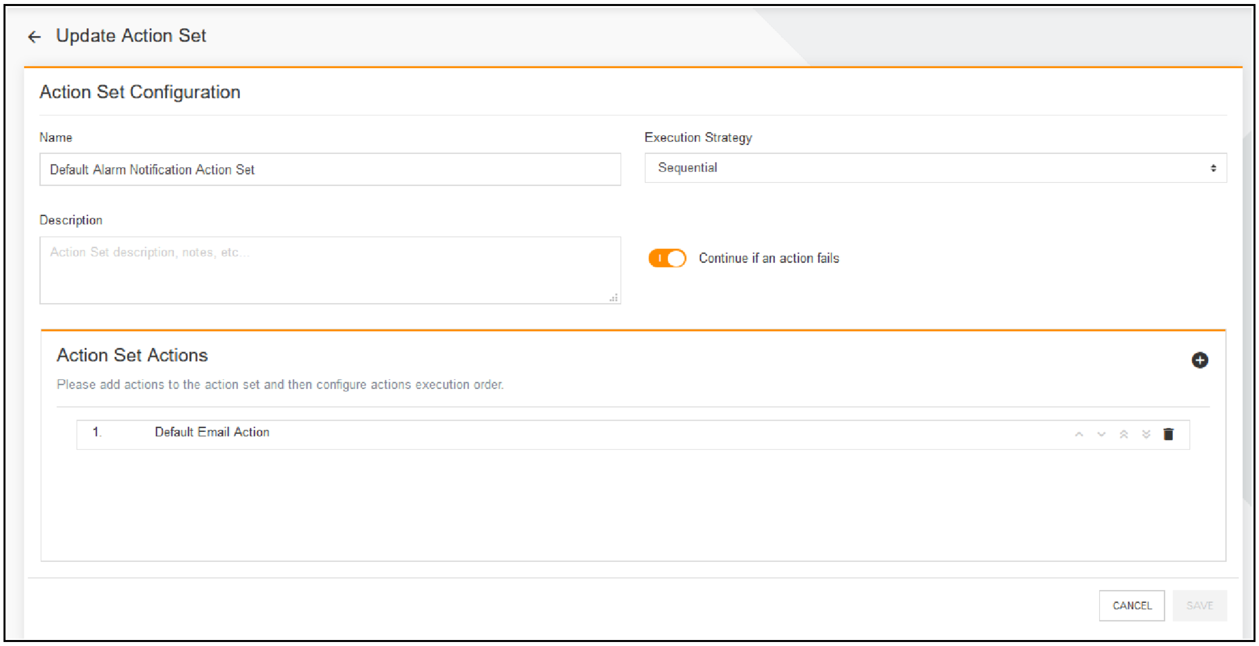
2. Enter the name and description.

3. Choose whether actions should be executed sequentially or in parallel.
4. Decide whether to continue with subsequent actions if one action fails.
5. Select actions and specify their execution order.

Editing the Action Combinations

1. Click ellipses (...) on the right side of the action set and select Edit to enter Update Action Set page. As shown in **Figure 11.22** below .

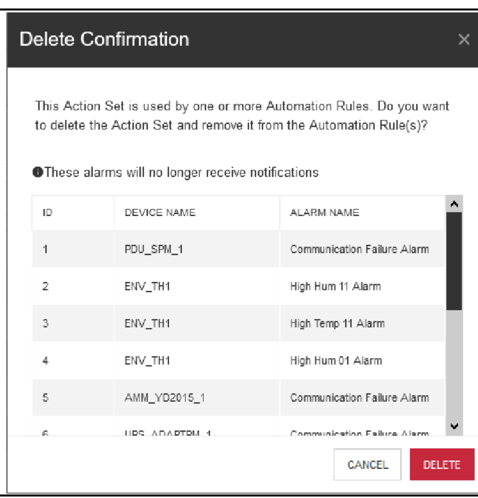
Figure 11.22 Editing the Action Page



Deleting a Single Action Combination

1. Click ellipses (...) on the right side of the action set and select Delete, and the page shown in **Figure 11.23** below will popup.

Figure 11.23 Deletion Popup Window



Click on *delete*, to delete the selected action set.

Copying a Single Action Set

1. Click ellipses (...) on the right side of the action set and select Copy to copy the selected action set.

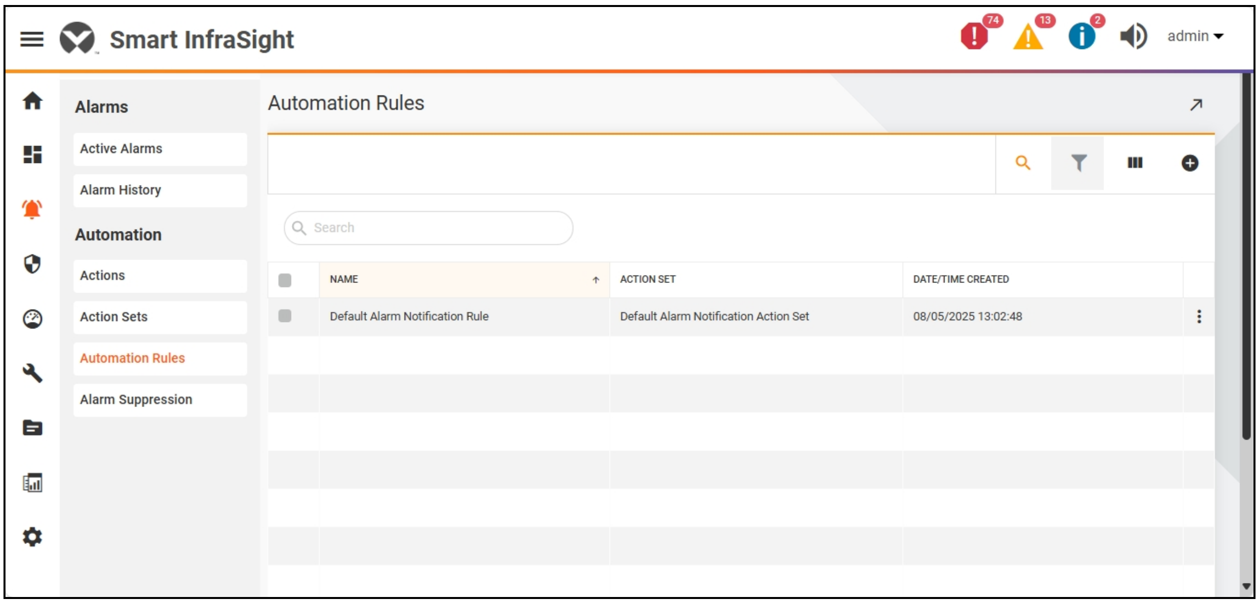
Batch Copy Action Set

1. Select multiple action sets and click the Copy button to copy them.

11.3.4 Alarm Automation Rules

On the Automation Rules page as shown in Figure 11.24 below , you can create and manage alarm automation rules that bind alarms with action sets so that when the alarms occur, actions in action sets will be executed.

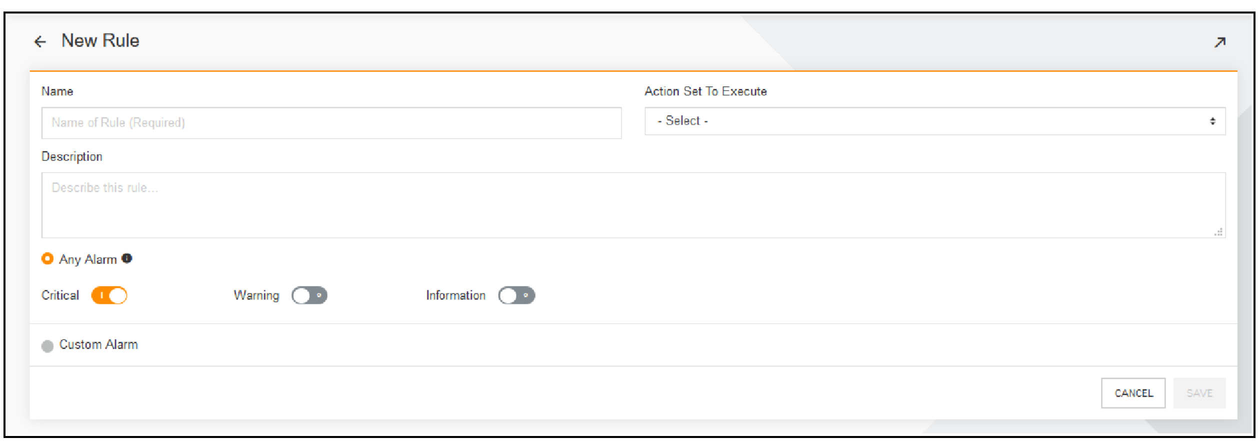
Figure 11.24 Alarm Automation Rules Settings

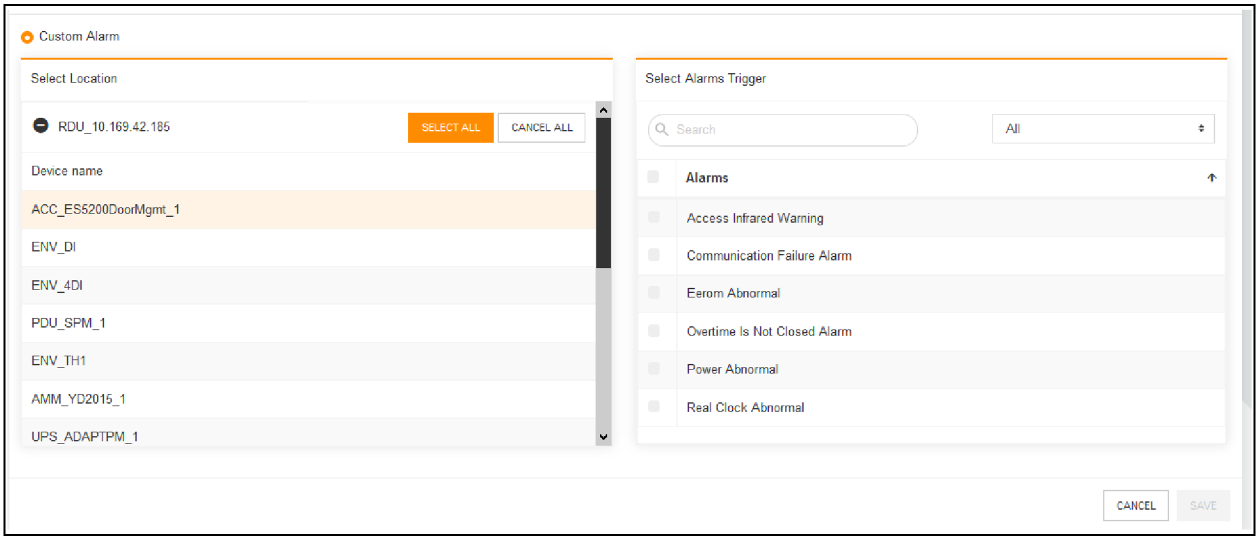


Adding an Alarm Automation Rule

1. On the Automation Rules List page, click *Add* to enter the New Rule page, as shown in Figure 11.25 below .

Figure 11.25 Adding an Alarm Automation Rule



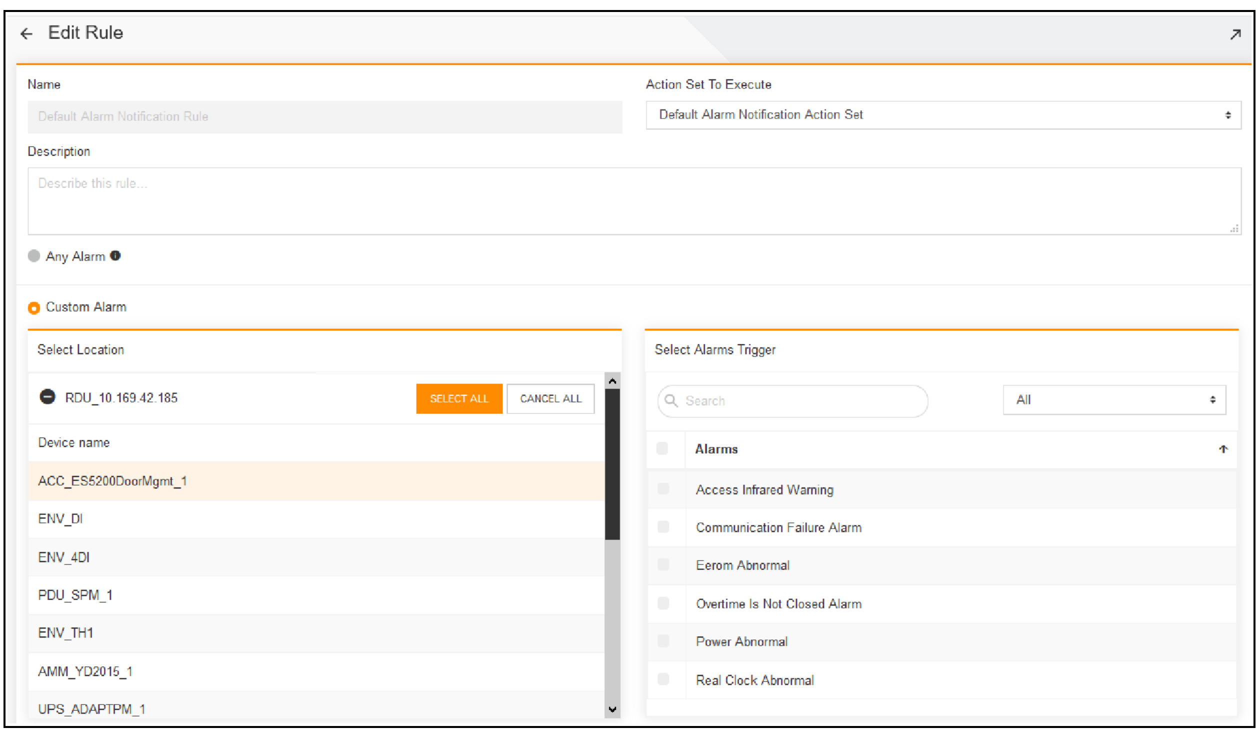


2. Enter the name and description.
3. Select the action set that will be executed.
4. Select alarms that will trigger the action set. You can select by alarm severities or select custom alarms from devices.

Editing an Alarm Automation Rule

1. In the alarm automation rule page, click the ellipses (...) on the right side of the automation rule, select Edit to enter the Edit Rule page, as shown in **Figure 11.26** below .

Figure 11.26 Editing the Automation Rule

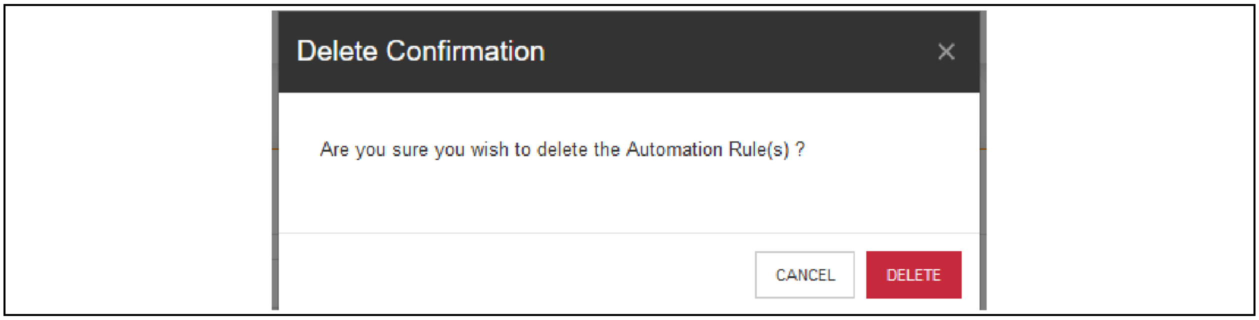


2. Modify the name, binding action combination, description, select device and alarm, click *Save*.

Deleting an Alarm Automation Rule

1. On the alarm Automation rule page, click the ellipses(...) on the right side of the automation rule, select Delete, the confirmation popup will show up as shown in **Figure 11.27** below .

Figure 11.27 Deletion Confirmation Popup

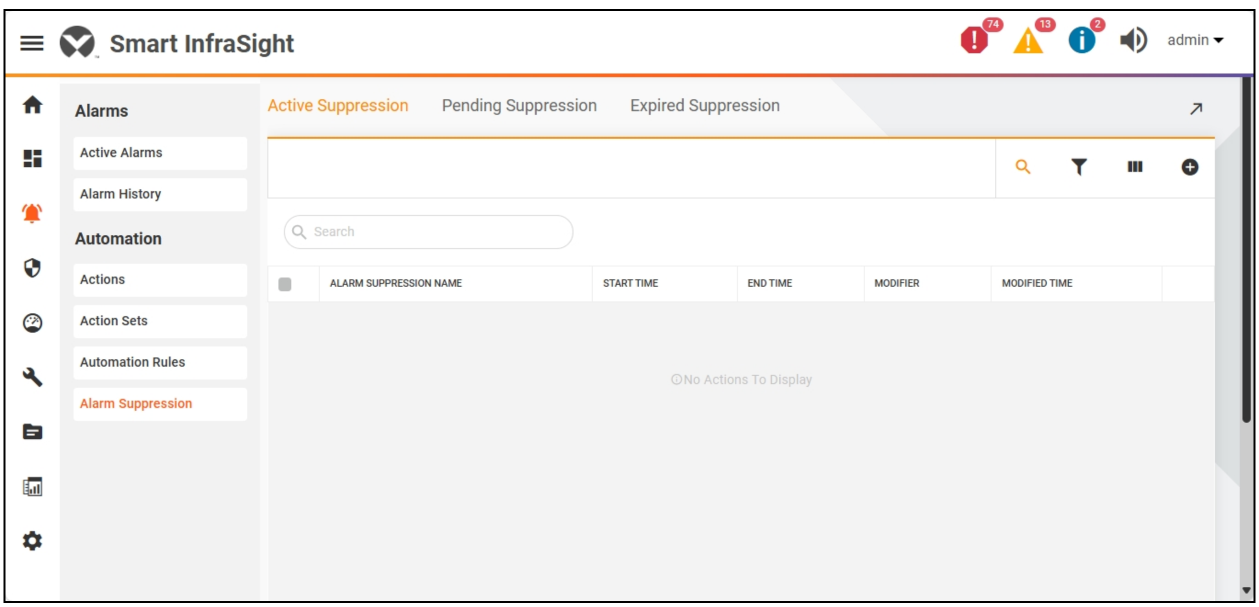


2. Click *Delete*, then the selected alarm binding will be deleted.

11.3.5 Alarm Suppression

If you need to temporarily silence alarm notifications without deleting configured alarm actions, you can create an alarm suppression rule. This is useful when a site or device is undergoing maintenance or has a known issue that might trigger alarms. The suppression rule prevents alarm notifications from being sent for a specified period of time. Navigate to Alarm Suppression page, as shown in **Figure 11.28** below .

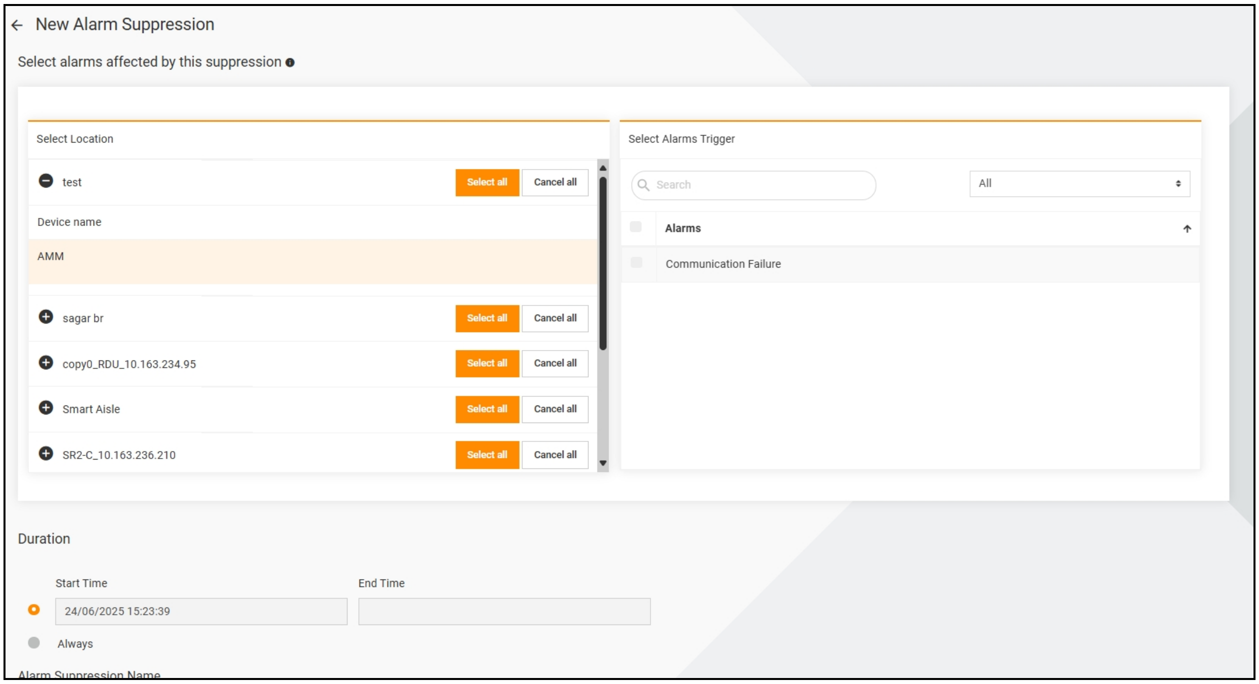
Figure 11.28 Alarm Silence Rules



Alarm Silence Rule is Added.

On the Alarm Suppression page, click Add button to enter the New Alarm Suppression page, as shown in **Figure 11.29** below . Choose the alarm you want to suppress. Once suppressed, you won't receive any notifications or trigger any control actions for this alarm. You can still view the alarm information in **Active Alarms** or **Alarm History**. Set the duration for suppressing, including start and end times. After the end time, notifications will resume. Alternatively, you can choose to silence the alarm indefinitely.

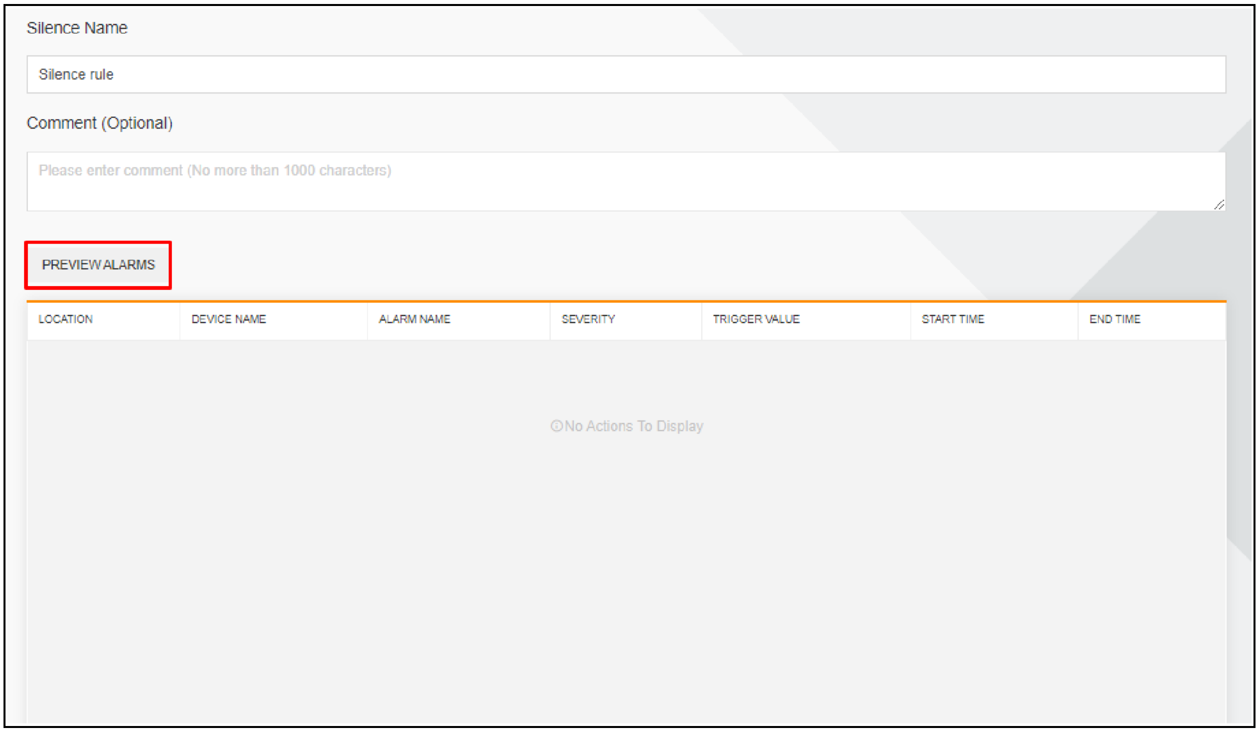
Figure 11.29 New Alarm Suppression Page



Editing the Alarm Suppression Rule

On the Alarm Suppression Rules page, you can click ellipses (...) and select *Edit* to edit the content of the suppression rule. To view alarms suppressed by the rule, click **Preview Alarms** at the bottom of the edit page. As shown in **Figure 11.30** on the facing page .

Figure 11.30 Editing the Alarm Silence Rule



Viewing the Alarm suppression Rule

On the Alarm suppression Rules page, click *ellipses* to open the menu, and if the rule is in effect or not, click *View* to view the suppression rule selected.

Expiring the Alarm Suppression Rules

On the Alarm Suppression Rules page, you can open the menu, and if the rule is in effect or not, click *Expire* to actively expire the suppression rule. After expiration, the rule will automatically become expired and can be viewed in the Expired Suppression Rule.

Copy the Expired Alarm Suppression Rule

On the expired alarm suppression page, click *ellipses* to open the menu, click *View* to view the settings of expired alarm suppression rules, At the top of the page, click *Copy Rule* to access the alarm suppression rule creation page. There, you can copy the configuration of the expired rule, adjust the suppression duration, and enter a new name to create a new alarm suppression rule.

This page intentionally left blank

12 Access Control Management

12.1 Overview

This module manages IP and serial access control devices. Users can connect IP access controllers to the system and view real-time door status. It allows for detailed access card authorization, including setting specific time periods for card access. The module also facilitates easy querying of access control records and equipment operation events.

12.1.1 Functional Modules

Access control management includes the following functional modules, refer to this manual for detailed introduction of each functional module in Detailed Features .

- Access Control
- Access Card Management
- Time Period Settings
- Log Queries

12.2 Quick Start

12.2.1 Rapid Deployment Steps

To deploy access control devices, you need to configure them in the following steps:

1. Add IP access controller and door.
2. Add an access card.
3. Authorization.
4. Time period setting (optional).

12.2.2 Example

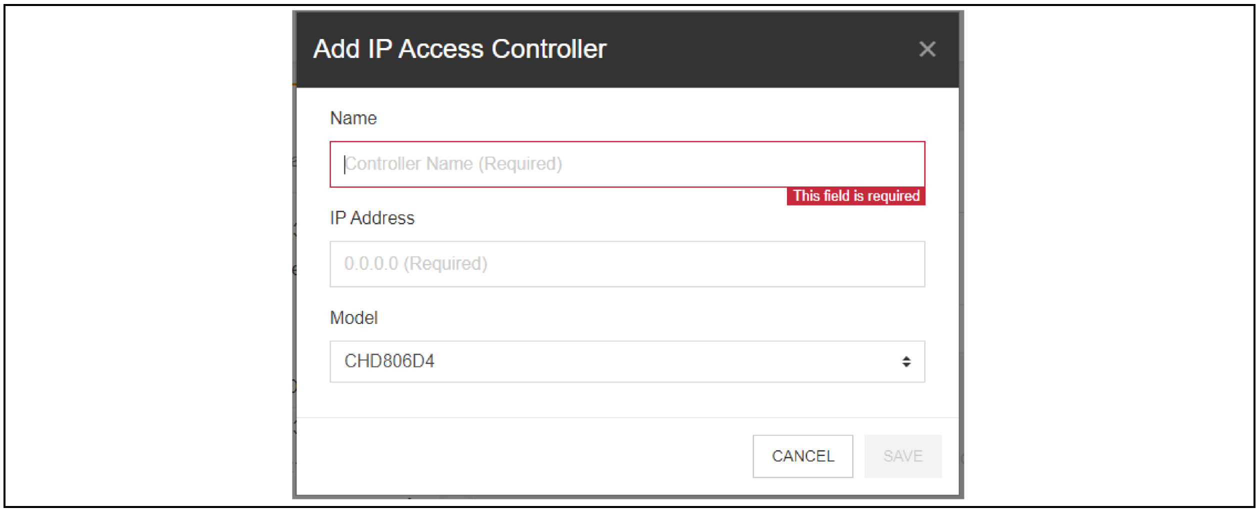
For example, there is an IP access controller with model number **CHD806DX-CHD806-1U** and IP address **10.163.236.129**. You want to connect this access controller into the system through TCP/IP and manage it in the system.

Adding IP Access Controller and Door

Selecting **Security** in the first-level menu will open the monitoring **Access Control** page by default.

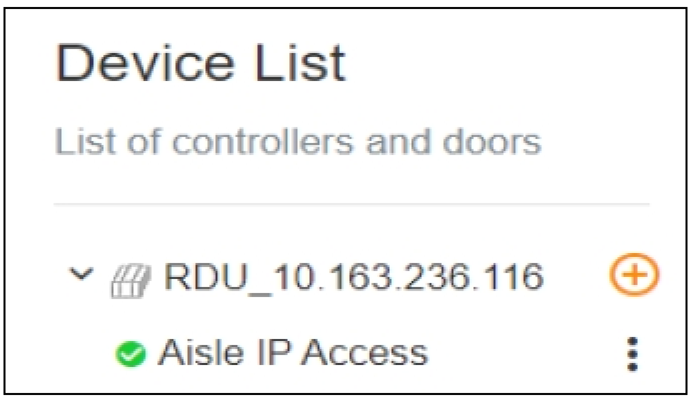
1. On the access control monitoring interface, click the **Add IP Access Controller** to popup the window, as shown in **Figure 12.1** on the next page . Enter the name **Aisle IP Access**, enter the IP address **10.163.236.129**, select the IP access controller model **CHD806DX-CHD806-1U**, and click the *Save* button.

Figure 12.1 Adding an IP Access Control



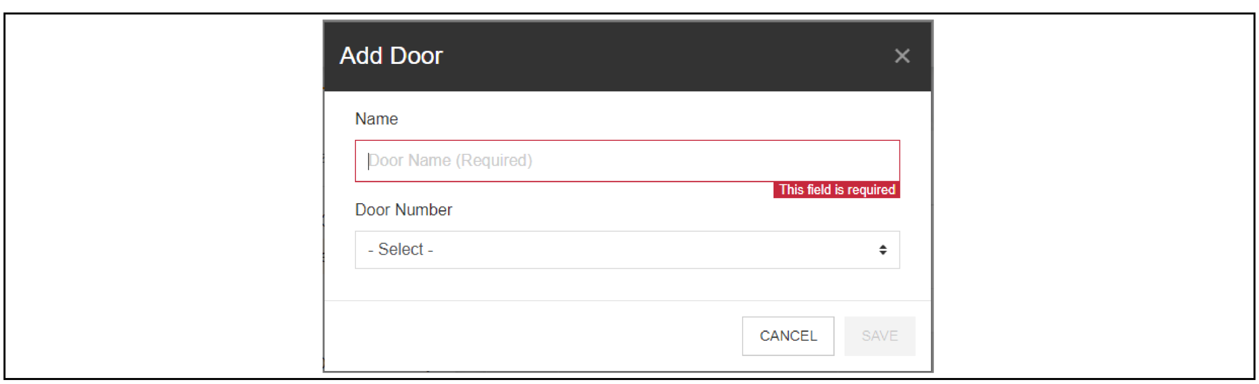
After the IP access controller is successfully added, the interface as shown in **Figure 12.2** below is displayed.

Figure 12.2 The IP Access Controller Added Successfully



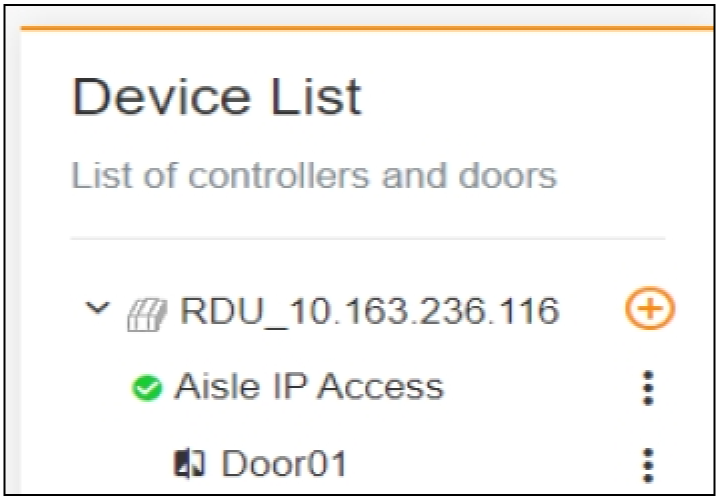
2. In the device list, click *Add* on the right side of the IP access controller name, select **Add Door** in the pop-up drop-down menu, pop up the Add Door interface, enter the name **Door 01**, select the door number **1**, click **Save**, as shown in **Figure 12.3** below .

Figure 12.3 Adding a Door



After the door that is added successfully is displayed in the device list as shown in **Figure 12.4** below .

Figure 12.4 A List of Access Control Devices



Add the corresponding number of doors according to the actual number of doors managed by the IP access controller, and the method is the same as the above method. When adding a door, select the corresponding door number.

The access control device list displays controllers and doors. A green icon next to the controller name indicates normal communication, while a red icon signifies a communication failure.

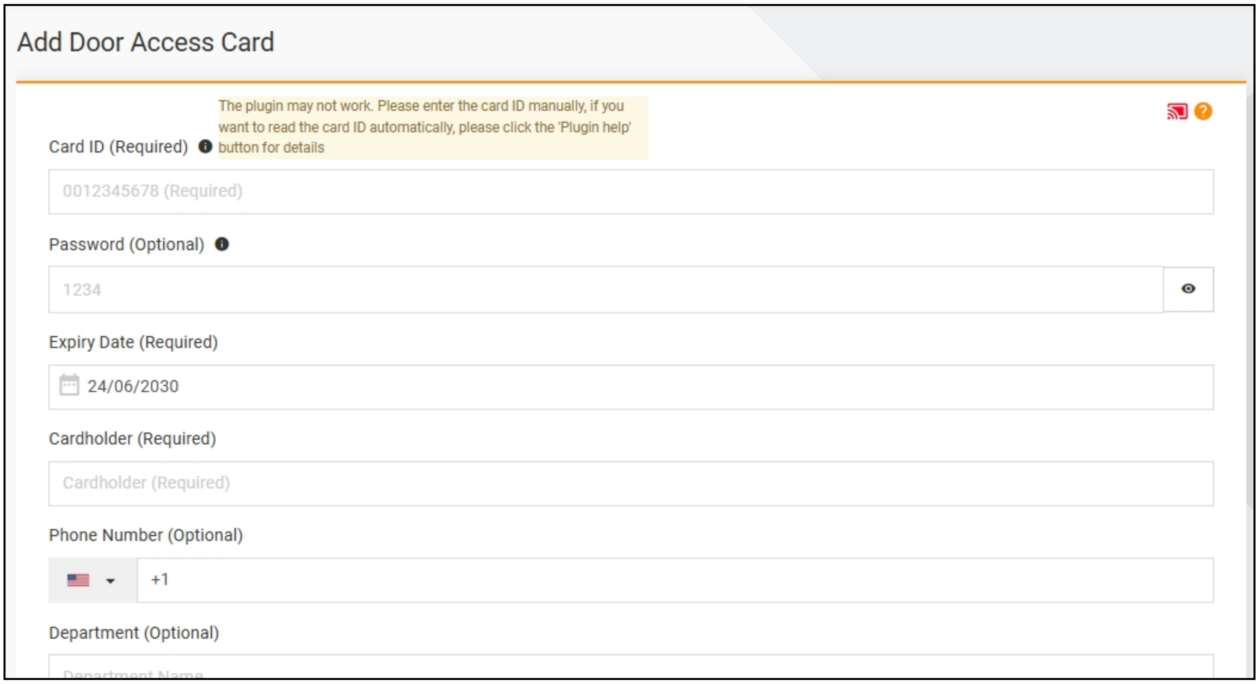
When you select a door from the list, the right panel shows real-time signals, current alarms, and available control commands for that door. To send a command, click the button next to the desired control option, choose **Send Command** from the drop-down menu, select the specific command in the popup window, and click **Send Command**. This will transmit the instruction to the access control device.

Adding an Access Card

Select *Card Management* in the second-level menu to open the access card management page.

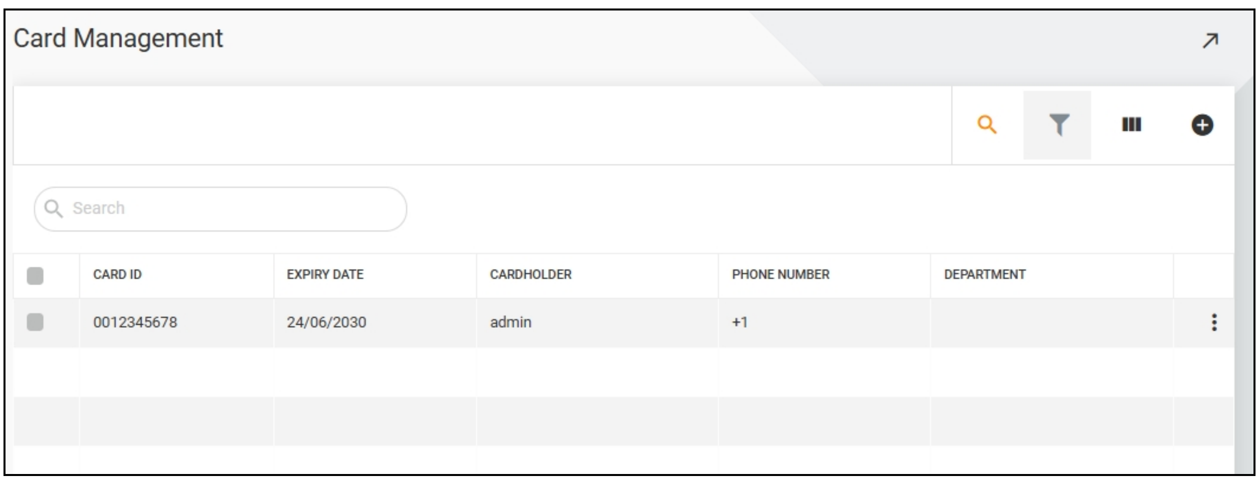
Click the *Add* button from the card table to add a new door access card, as shown in **Figure 12.5** on the next page . Enter the card number 0014781355 and set the validity period to 5 years from today. Select the cardholder from your contacts or address book. Optionally, you can enter a phone number (e.g., 18688888888) and department (e.g., Department One), and collect the user's fingerprint. Once finished, click *Save*.

Figure 12.5 Adding an Access Card



After the access card is successfully added, it is displayed in the list as shown in **Figure 12.6** below . You can add multiple access cards according to your actual needs.

Figure 12.6 Access Card List



Authorization

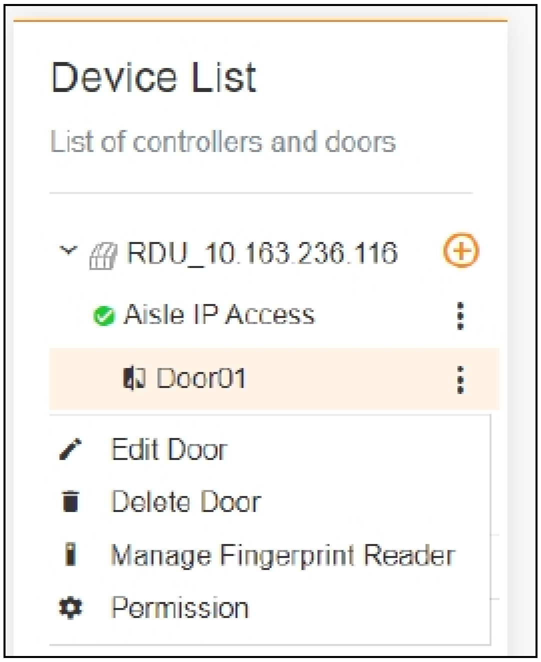
The system offers two methods for authorization:

- From the list of access control devices, select a door, open the authorization page, and choose the access control cards to authorize.
- From the list of access cards, select a card, open the authorization page, and choose the doors to authorize.

Both methods support bulk authorization. The following example demonstrates the first method:

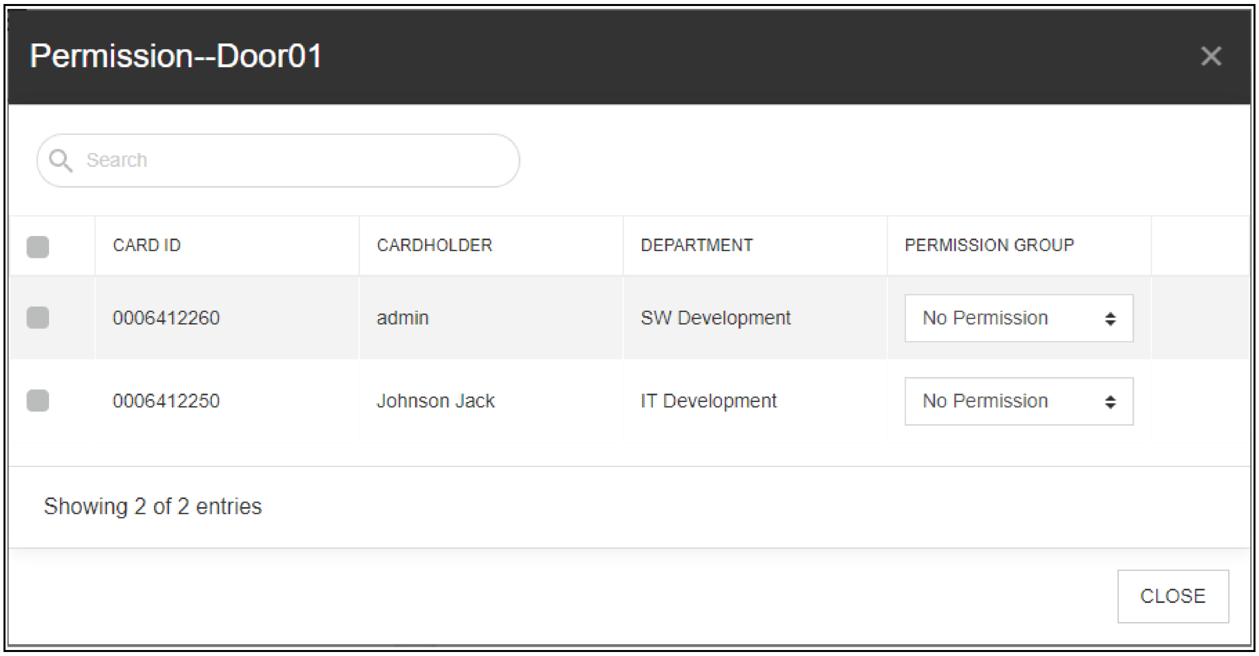
1. Click the button to the right of the door name and select Permission in the pop-up drop-down menu, as shown in **Figure 12.7** below .

Figure 12.7 Selecting Authorization



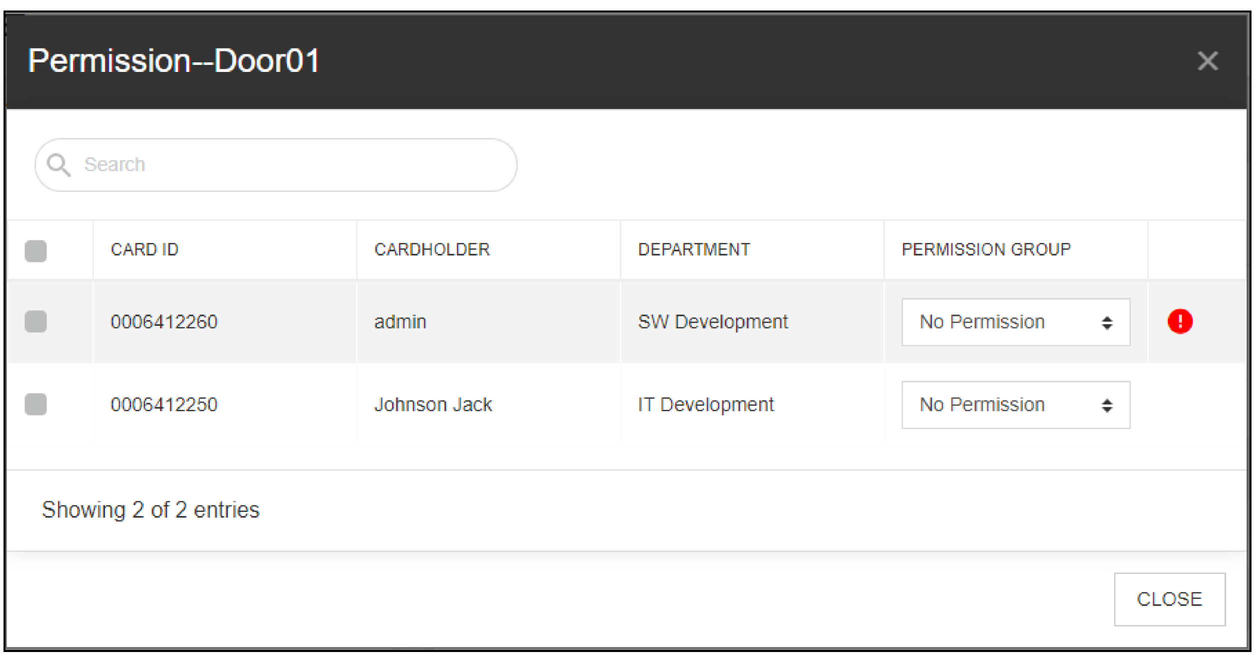
2. **Figure 12.8** on the next page shows the permission setting page, which displays all door access cards and their corresponding permissions to the door. The PERMISSION GROUP column indicates the access level for the selected door, ranging from No Permission to Privilege, and Groups 1 through 4. Cards set to No Permission cannot open the door. Those set to Privilege can open the door at any time. Cards assigned to Groups 1-4 can only open the door within specified time ranges.

Figure 12.8 Permission Popup



3. After selecting *Permission Group 1* in the drop-down list of permission groups, a rotating icon is displayed in the last column, indicating that authorization is in progress. When the authorization is successful, a green icon is displayed. When authorization fails, a red icon is displayed. and the permission group reverts to the options it had before the modification, as shown in Figure 12.9 below .

Figure 12.9 Authorization—Changing the Permission Group

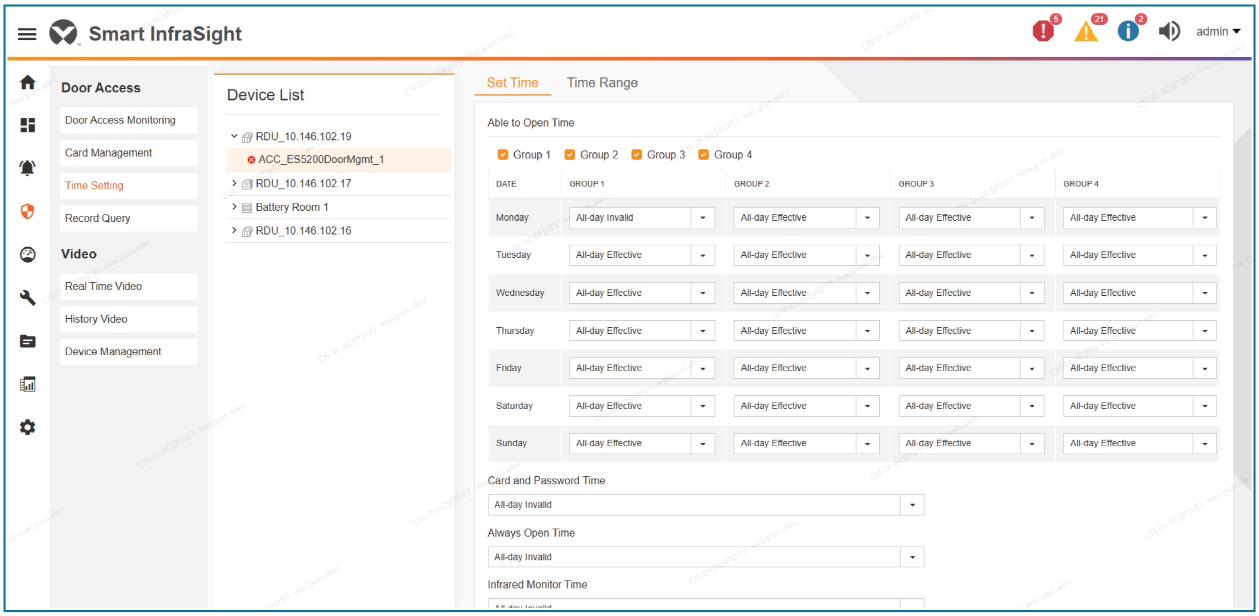


Time Period Setting (Optional)

When adding an IP access controller, the system will set the door opening time of the four permission groups (permission group 1, permission group 2, permission group 3 and permission group 4) of the controller to 00:00-23:59 by default. Therefore, when the user authorizes the access control in the previous step, after selecting a certain permission group, the access card can open the door at any time period. In the following sections, we will explain how to change the default time period so that the access card can only open the door during the set time period.

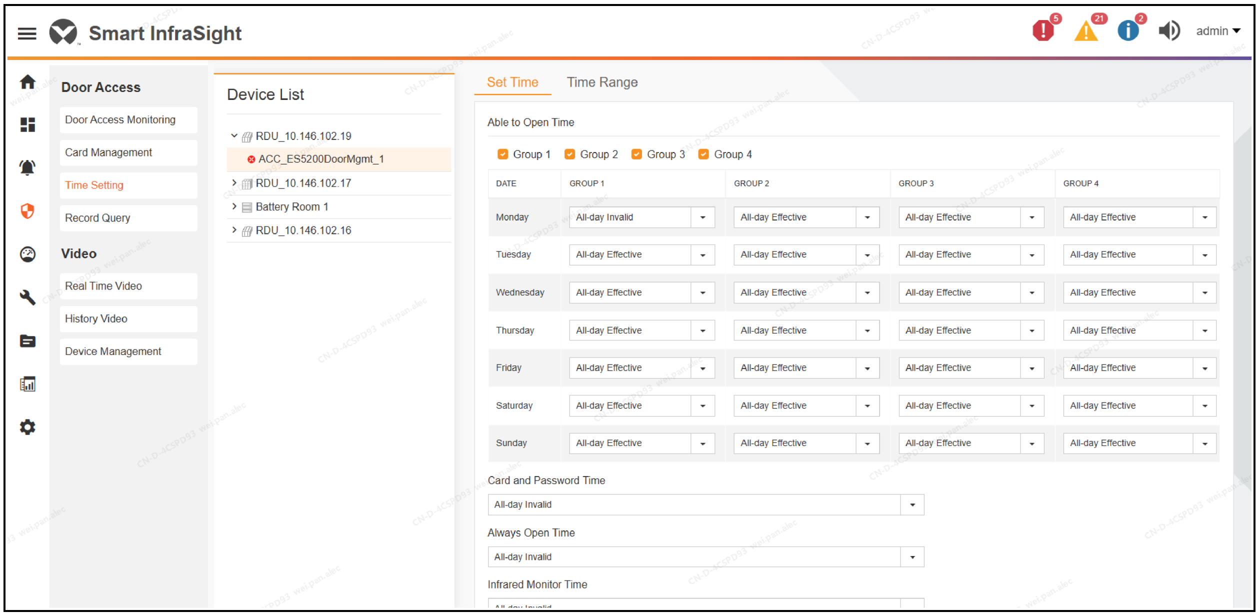
1. Select *Security* in the first-level menu, select *Time Setting* in the second-level menu, open the page of Set Time, and select access controller that require time period control. At the same time, it can be found that by default, the four permission groups are *valid All-Day* from Monday to Sunday, as shown in **Figure 12.10** below .

Figure 12.10 Setting the Time Period



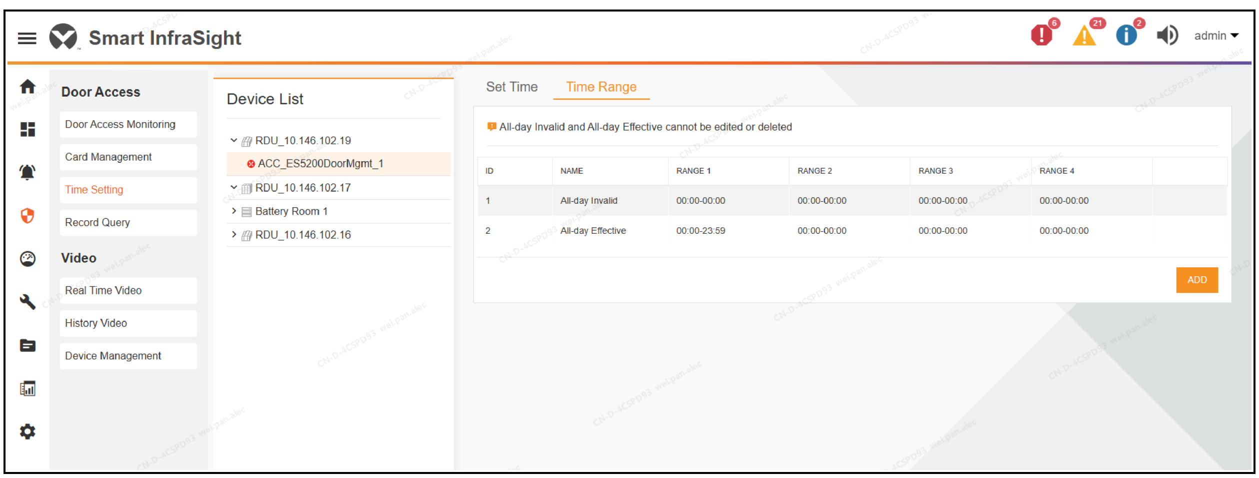
2. If you want to change the opening time of a certain permission group, select the opening time of the permission group. For example, set the permission of *Permission Group 1* to *Invalid All-Day* on Monday, and click the *Save* button to save after the modification is completed, as shown in **Figure 12.11** on the next page .

Figure 12.11 Setting the Time Period



3. When you change the time period of a permission group, only *Valid for All-Days* and *Invalid for all-days* can be selected by default. To change the list of time periods that can be selected, you need to switch to the Time Range page for management, as shown in **Figure 12.12** below . For details on how to operate the time period list, refer to the Time Settings on page 247.

Figure 12.12 Door Opening Time Setting



12.3 Detailed Features

This section outlines the key functions of door access management, which include: Door Access Management, Card Management, Time Setting, Record Query. The system supports two types of access control devices: IP access controllers, which can directly connect to the system; Serial access controllers, which connect through an RDU collector.

12.3.1 Access Control

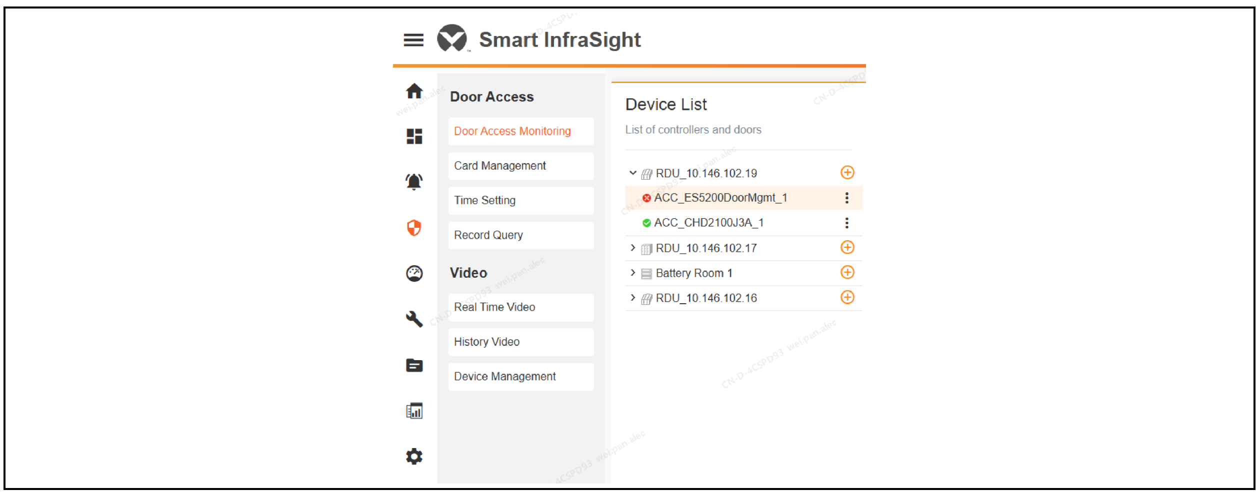
This module introduces the access control monitoring function, mainly including:

- Adding, removing and modifying the IP access controller.
- Add, remove and modify the door that connected to the IP access controller.
- Synchronize data to IP access controllers.
- Configure door access permissions for the access control cards through the IP-based controller.
- Configure door access permissions for the access control cards through the serial-based controller.
- View real-time signals, active alarms, control commands, and setup signals for access controllers.

Access Control Device List

Select *Security* in the first-level menu, and the page of *Door Access Monitoring* will be opened by default. The IP access controller and its door can be added on this page, and the serial access controller connected through the RDU collector will be automatically displayed here. The icon in front of the controller name indicates its communication status, and a green icon is displayed when communication is normal and a red icon is displayed on failure, as shown in **Figure 12.13** below .

Figure 12.13 Access Control Device List

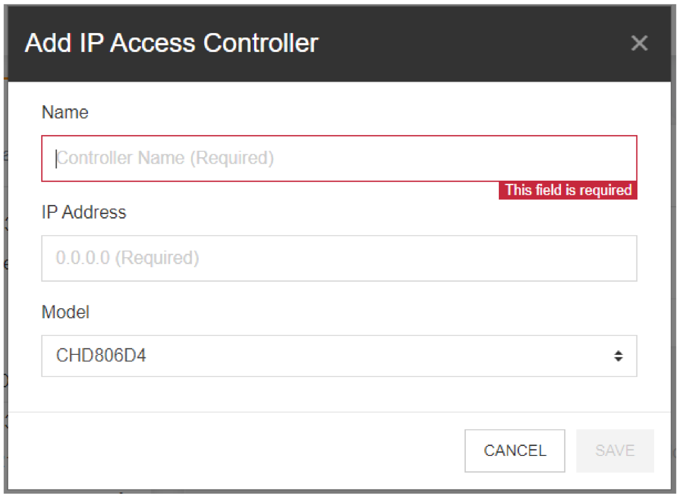


NOTE: When there is no new access controller in the system, the access control device list only shows the site information.

Adding an Access Controller

1. Click *Add* to add an IP access controller as shown in **Figure 12.14** on the next page .

Figure 12.14 Adding an Access Controller



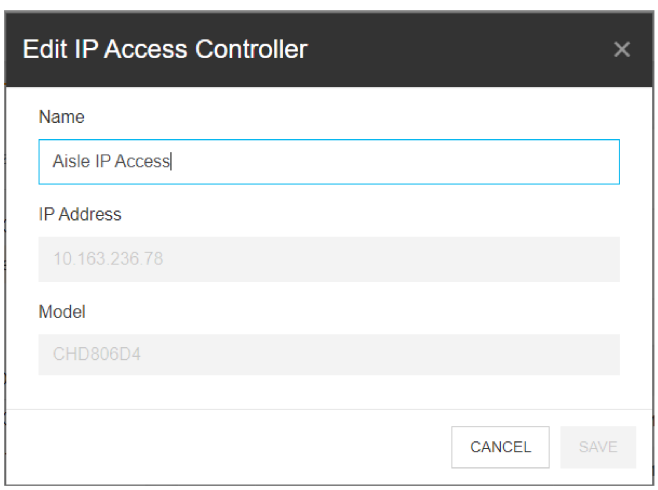
2. Enter the name and IP address of the IP access controller, select the model of the access controller, and click *Save* button.

NOTE: The name of the access controller must be 3-64 characters long and cannot be repeated.

Editing the Access Controller

Click on the *ellipses* to the right of the IP access controller name, and select *Edit IP Access Controller* in the pop-up drop-down menu to pop up the Edit IP Access Controller interface. After modifying the name of the IP access controller, click the *Save*, as shown in Figure 12.15 below .

Figure 12.15 Editing the Access Controller

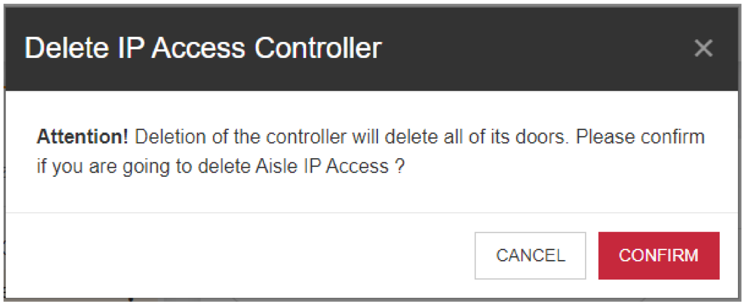


NOTE: The IP address and model of the access controller are not allowed to be modified, if you want to modify it, please delete it and add it again.

Removing the IP Access Controller

1. Click on the *ellipses* to the right of the IP access controller name, and select *Delete IP Access Controller* in the pop-up drop-down menu, which will pop up as shown in Figure 12.16 on the facing page .

Figure 12.16 Removing the IP Access Controller



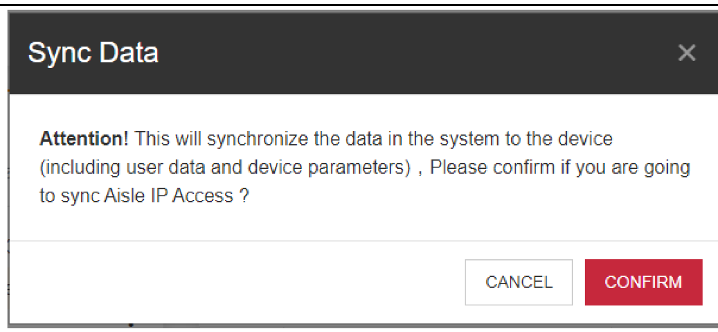
2. Click *Confirm*, and the access controller will be deleted.

NOTE: 1. When you delete an IP access controller, all doors managed by the controller will be deleted synchronously.

Sync data

1. Click the button on the right of the name of the IP access controller, and select *Sync Data* in the pop-up drop-down menu to pop up, as shown in Figure 12.17 below .

Figure 12.17 Sync data



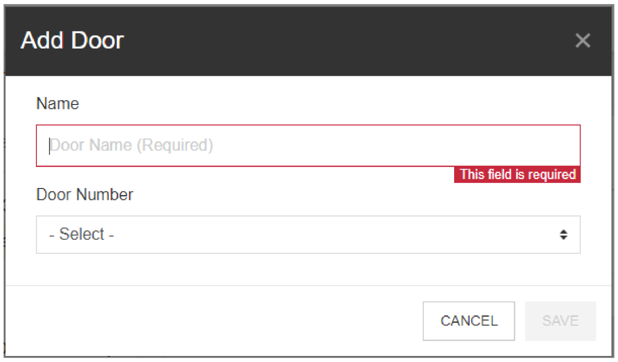
2. Click *Confirm* button, and the data in the system will be synchronized to the IP access controller device, and the synchronized data includes user data and device parameters.

NOTE: The main use scenario of the synchronization data function is: replacing the IP access controller, and synchronizing the original data in the system to the new access control device.

Adding a Door

1. Click on the *ellipses* on the right side of the IP access controller, and select *Add Door* in the pop-up drop-down menu to pop up, as shown in Figure 12.18 on the next page .

Figure 12.18 Adding a Door



2. Enter the name of the door, select the door number, and click the *Save* button.

NOTE: 1. The name of the door must be 3-64 characters, and the name of the door under the same site is not allowed to be repeated.

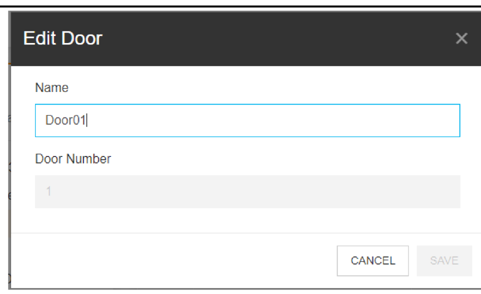
2. Under the same IP access controller, the door number can only be used once, and the door number that has been occupied will not be selected.

3. The name and number of the door are required, and the "Save" button is only allowed to be clicked after the information has been entered completely and the verification has been passed.

Editing a Door

Click on the *ellipses* on the right of the door name and select *Edit Door* in the pop-up drop-down menu to pop up the interface of editing the door. After changing the name of the door, click the *Save* button, as shown in Figure 12.19 below .

Figure 12.19 Editing a Door



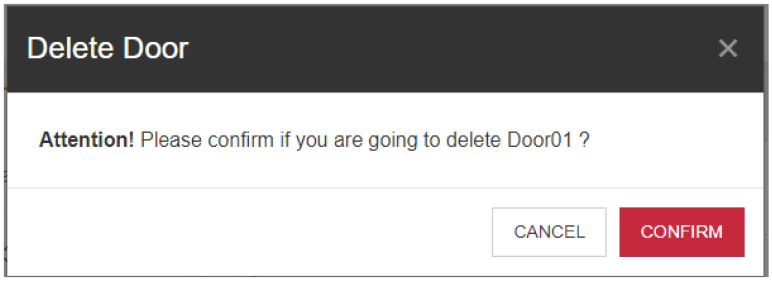
NOTE: 1. The name of the door must be 3-64 characters, and the name of the door under the same access controller is not allowed to be repeated.

2. The door number is not allowed to be edited, if you want to modify the door number, please delete it and add it again.

Deleting the Door

1. Click on the *ellipses* on the right side of the door name and select *Delete Door* in the pop-up drop-down menu to popup as shown in Figure 12.20 on the facing page .

Figure 12.20 Deleting the Door popup



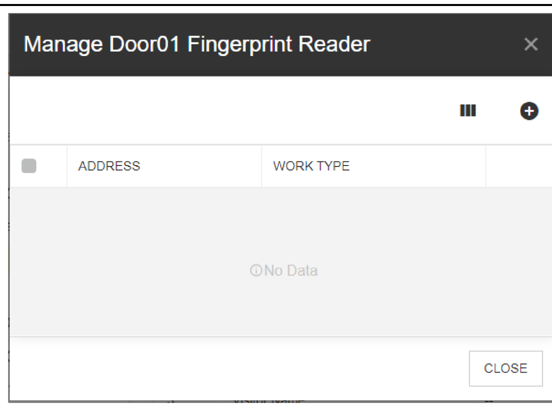
2. Click the *Confirm* button and the door will be deleted.

Managing Fingerprint Readers

The fingerprint reader used to open the door is managed at the IP access controller level.

1. Click the ellipsis (...) next to each door name in the IP access controller. Select **Manage Fingerprint Reader** from the drop-down menu. The fingerprint reader management interface will appear, as shown in **Figure 12.21** below .
2. Click the *Add* button on the interface. A new row will appear in the fingerprint reader table. Select the working mode for the fingerprint reader. A green icon will indicate successful addition, and an address will be automatically generated for the reader.
3. The working mode of a configured fingerprint card reader can be modified, but its address cannot be changed.
4. To delete a configured fingerprint card reader, click the ellipsis (...) next to its record and select *Delete*. You can also select multiple readers for batch deletion.
5. After making changes to the fingerprint reader settings, click *Close* to exit the interface.

Figure 12.21 Managing Fingerprint Readers



NOTE: 1. The baud rate of the access controller must match that of the fingerprint reader for proper communication. If they can't communicate, service personnel should use the manufacturer's debugging tool to set the correct baud rate. After a successful communication test, they can then add or modify the fingerprint reader's operation mode.

2. Each door can support up to two fingerprint readers when using an IP access controller.

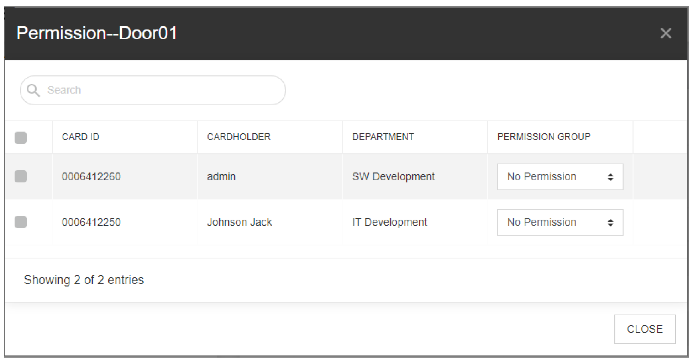
3. The fingerprint reader supports various working modes: independent, card swipe plus fingerprint, card swipe plus password, and fingerprint plus password. When using the card swipe plus password or fingerprint plus password modes, the access controller's swipe plus password function should be disabled.

4. To relocate an in-use fingerprint reader to another door, first delete it from the Manage Fingerprint Reader page. Then, physically move the hardware and re-add the reader on the page, ensuring proper authorization.

Access Control Device Authorization

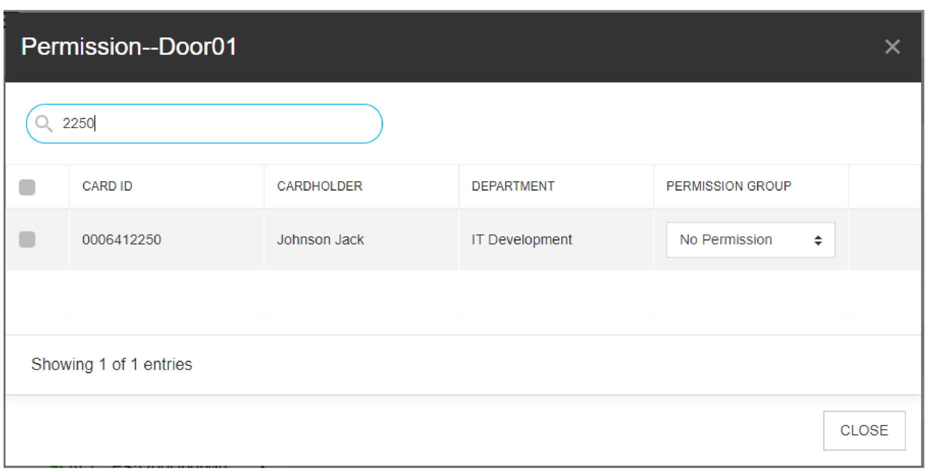
1. Click the ellipsis (...) next to the IP access controller or serial door access device, then select *Permission* from the drop-down menu. The Permission page will appear, as shown in **Figure 12.22** below . This page displays all door access cards and their corresponding permissions in the system. The table includes basic information such as CARD ID, CARDHOLDER, and DEPARTMENT. The PERMISSION GROUP column shows the access level for the selected door, ranging from No Permission to Group 1, 2, 3, or 4.

Figure 12.22 Access Control Device Authorization



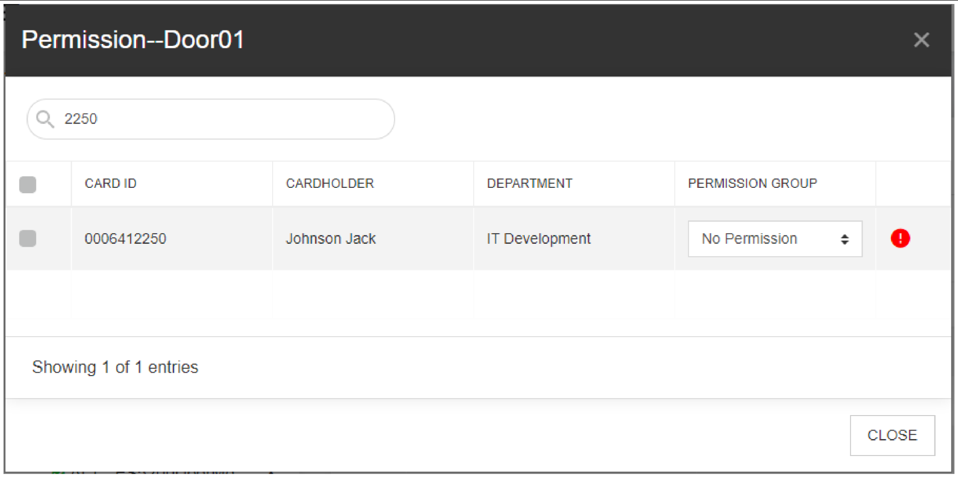
2. Enter the content of the query in the search box above the list, and the system will search for the access control card according to the input content, as shown in **Figure 12.23** below .

Figure 12.23 Searching the Access Card



3. After selecting an option from the PERMISSION GROUP drop-down, a rotating icon appears in the last column, indicating that authorization is in progress. A green icon displays upon successful authorization, while a red icon indicates failure. If authorization fails, the PERMISSION GROUP option reverts to its previous setting. **Figure 12.24** on the facing page shows an example of the page after successful authorization for Group 1.

Figure 12.24 Door Authorization—Changing the Permission Group of the Access Card



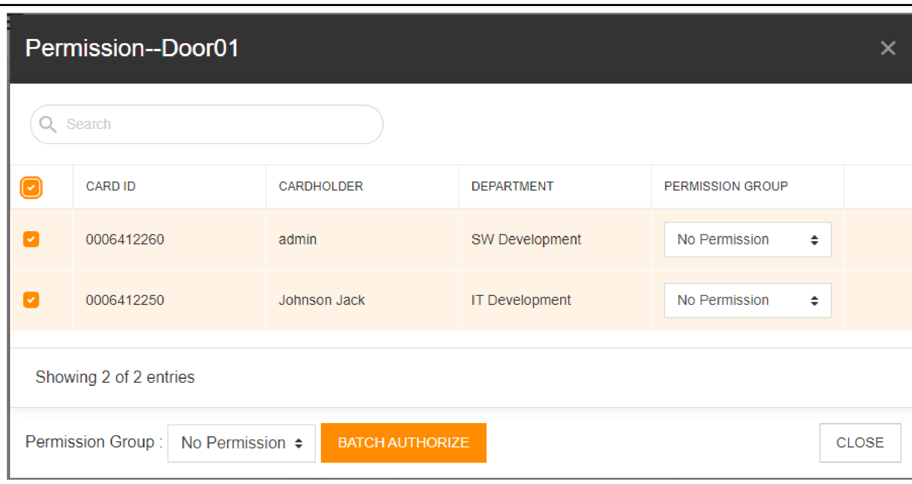
NOTE: When PERMISSION GROUP is set to No Permission, the access card cannot open the door. If set to Privilege, the card can open the door at any time. For settings Group 1 through Group 4, the card can only open the door within specified time ranges.

4. Clicking the checkbox in the table header's first column selects all data. When you select two or more items, the BATCH AUTHORIZE button appears in the lower right corner of the page. After selecting a permission group, click BATCH AUTHORIZE to modify the permissions of selected door access cards in bulk.

The last column displays the authorization result: a green icon for success and a red icon for failure. The PERMISSION GROUP option reverts to its previous setting after the process.

To illustrate, select Group 2 and click BATCH AUTHORIZE. Upon successful batch authorization, the page will appear as shown in **Figure 12.25** below .

Figure 12.25 Door Authorization—Group Modification



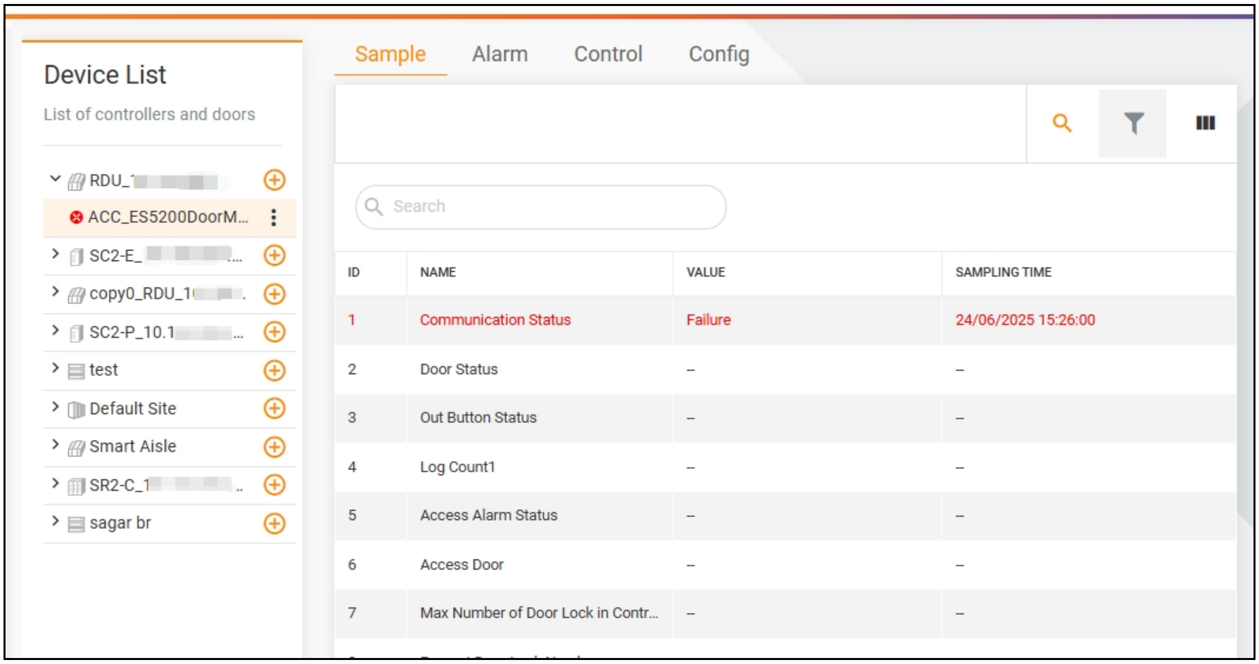
NOTE: 1. For the door of the IP access controller: When modifying the permissions in batches, a maximum of 100 access control cards can be authorized at a time.

2. For serial access control, when modifying permissions in batches, a maximum of 4 access cards can be authorized at a time.

Real-Time Signals

1. On the *Access Control Monitoring* page, when selecting an IP access controller, a door of the IP access controller, or a serial port access control, the system will display the real-time signal list of the device, as shown in Figure 12.26 below .

Figure 12.26 Real Time Signals



2. Enter the query content in the search box above the real-time signal list, and the system will perform a fuzzy search on the real-time signal name according to the input content.

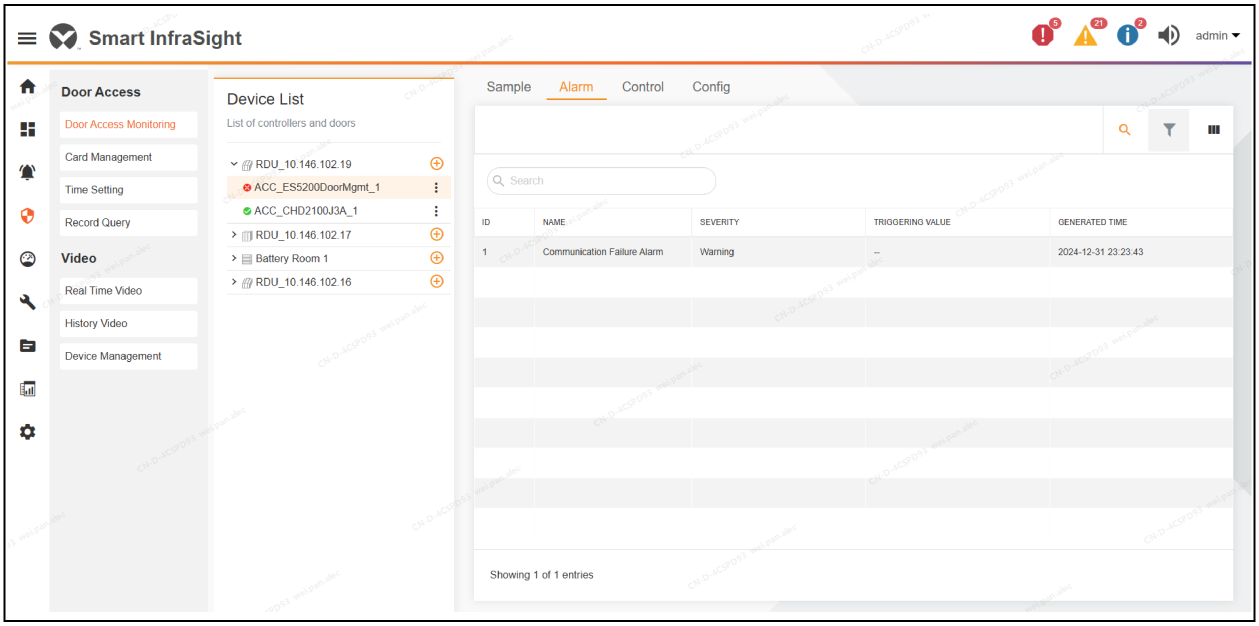
NOTE: 1. Real-time signal data is refreshed every minute.

2. When the real-time signal is unavailable, both the value and acquisition time are displayed as (--).

Current Alarms

1. On the *Access Monitoring* page, when you select an IP access controller, a door of the IP access controller, or a serial port access control, select the alarm tab on the right to display the current alarm list of the selected device, as shown in Figure 12.27 on the facing page . When a new alarm appears, the alarm list is automatically refreshed.

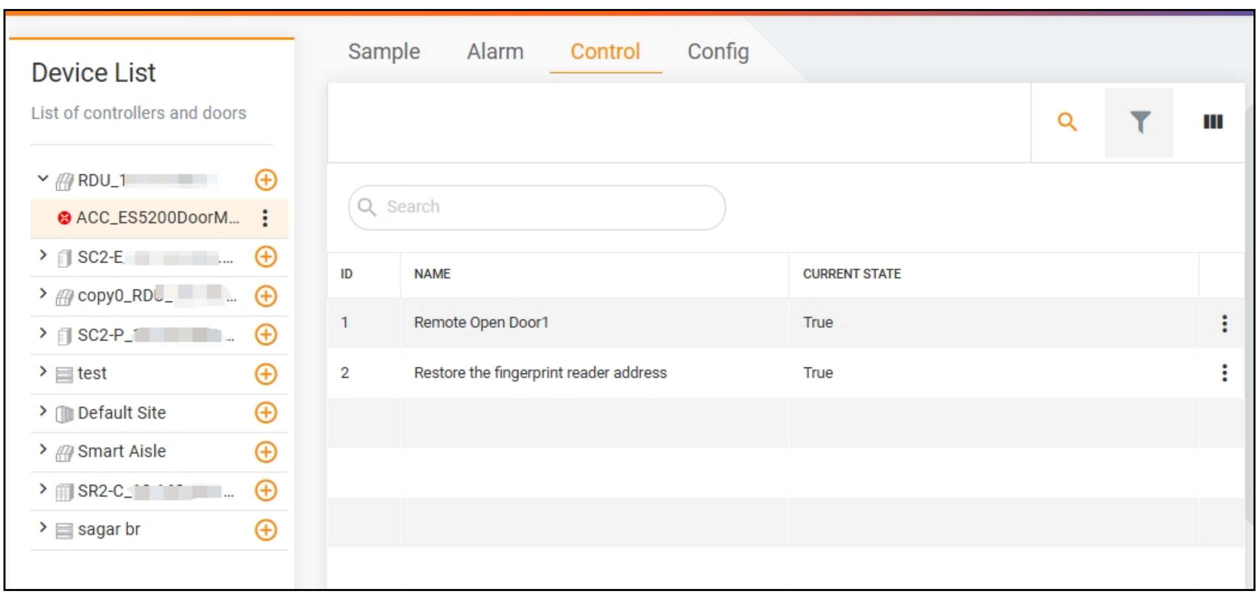
Figure 12.27 Current Alarms



Control Commands

1. On the *Access Monitoring* page, select an IP access controller, a door of the IP access controller, or a serial port access control, and select the control page on the right tab to display the list of control commands for the selected device, as shown in **Figure 12.28** below .

Figure 12.28 Control Command Window



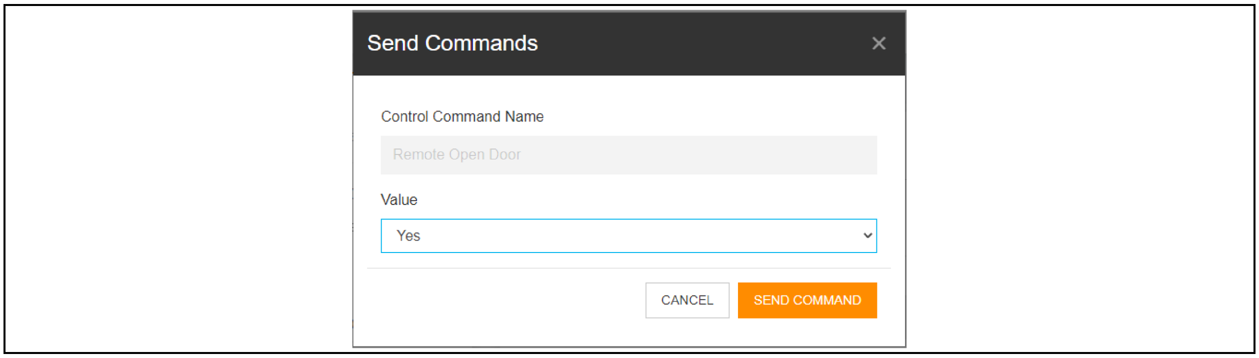
NOTE: 1. When the control commands are unavailable, no data is displayed on the tomb.

2. The command data is refreshed every minute.

2. Click the ellipsis (...) icon next to the control command and select **Send Commands** from the drop-down menu. The Send Commands popup will appear, as shown in **Figure 12.29** below . Choose the desired control command from the drop-down list and click *Send Command*. This will transmit the command to the device.

If successful, the popup window will close, and you'll see an **Operation Successful** message in the lower right corner of the screen. If the command fails to send, you'll see an **Operation Failed** message in the same location.

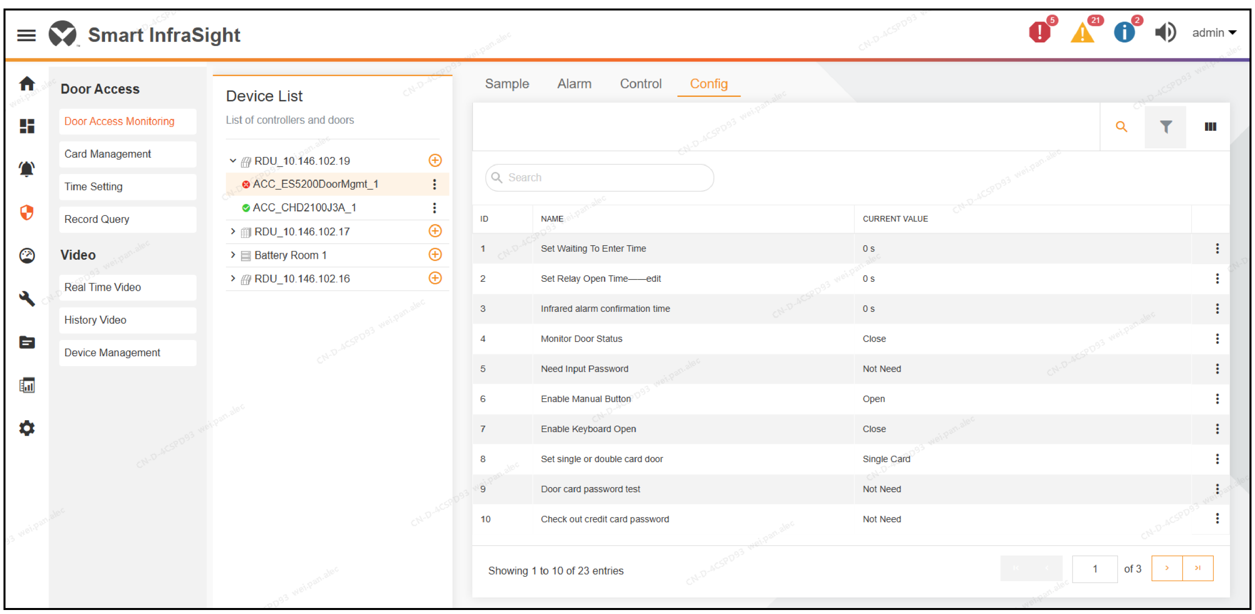
Figure 12.29 Sending Commands



Config Signal

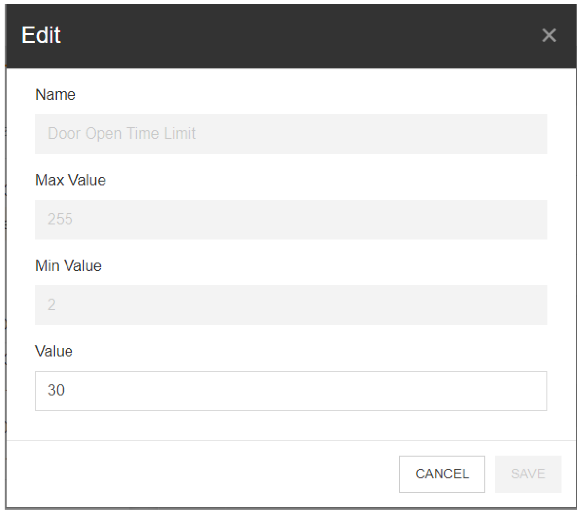
1. On the *Access Monitoring* page, as shown in **Figure 12.30** below , when you select an IP access controller, a door of the IP access controller, or a serial port access control, select the Config tab on the right to display the setting signal list of the selected device.

Figure 12.30 Config Signal - Access controller



2. Click the ellipsis (...) next to the config signal and select *Edit* from the drop-down menu. On the Edit page, enter the new value in the input box or select it from the drop-down list. Click *Save* as shown in **Figure 12.31** below . When the signal is successfully edited by the controller, the pop-up interface closes, and the lower right corner prompts **Operation Successful**. If the editing is successful, the popup window will close, and you'll see an **Operation Successful** message in the lower right corner of the screen. If the edit fails, you'll see a **Configuration Failed** message in the same location.

Figure 12.31 Editing the Setting Signal



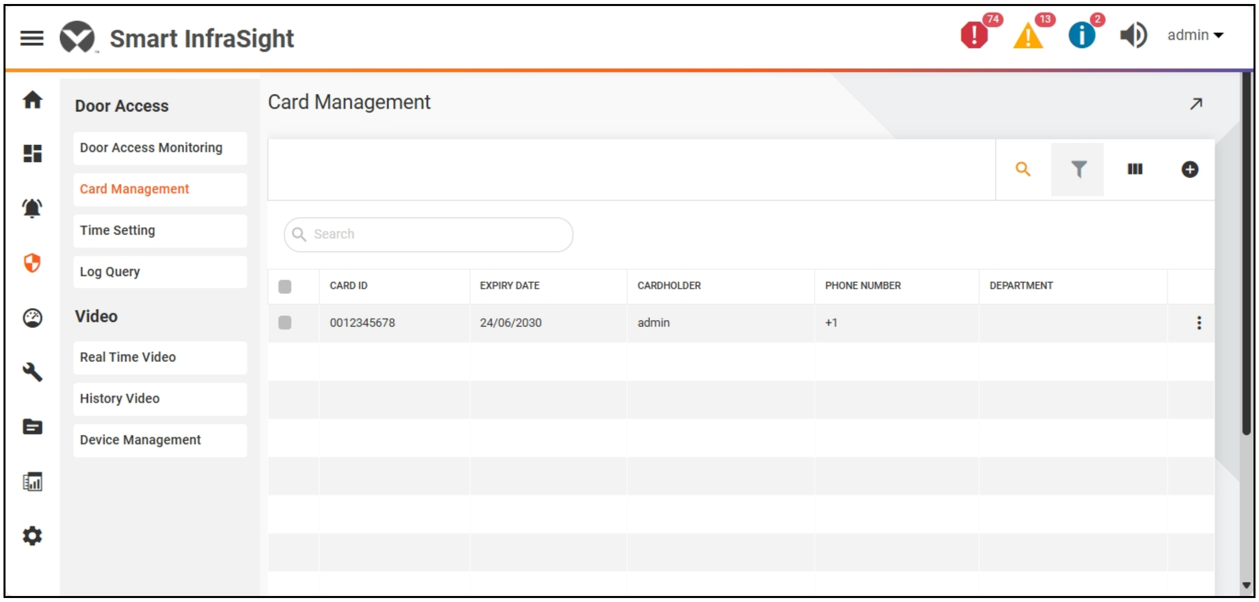
12.3.2 Access Card Management

This module introduces the management functions of the access control card, mainly including: adding, deleting, modifying and querying the access control card. Set the door opening authority of the access control card.

List of Access Cards

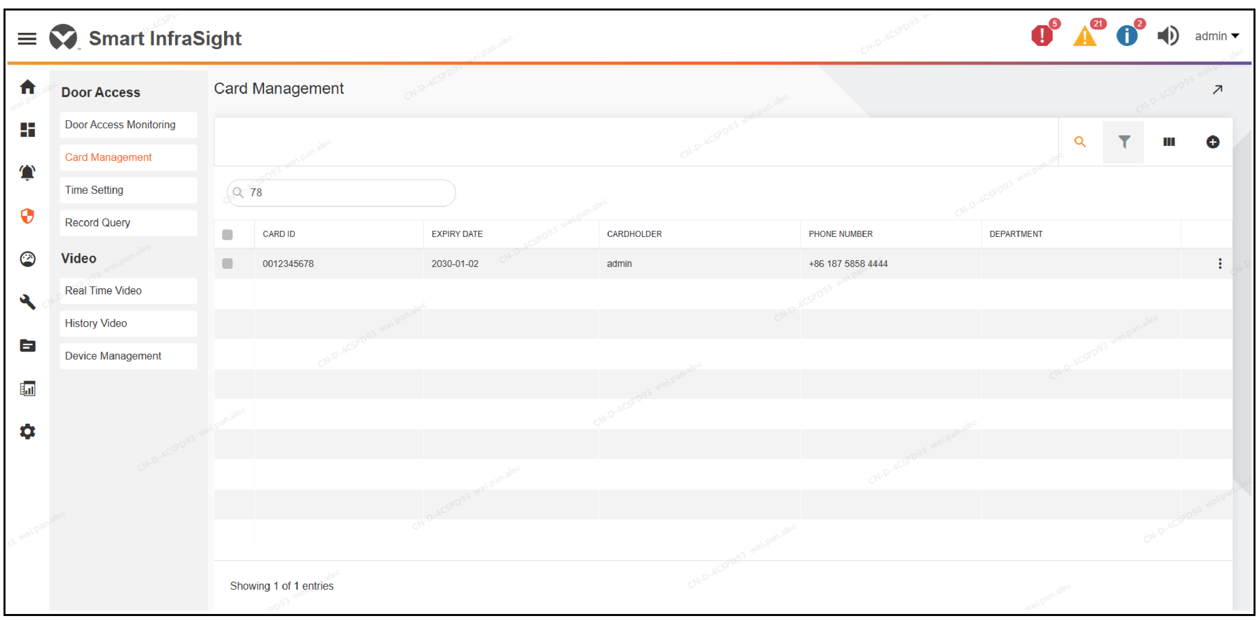
1. Select *Security* in the first-level menu, and select *Card Management* in the second-level menu, and the access card management page will be opened. As shown in **Figure 12.32** on the next page .

Figure 12.32 Access Card List



2. Enter the content of the query in the search box above the list, and the system will search for the access card data according to the input content. The search function supports fuzzy queries of card numbers, cardholders, and department names. Enter **User A** and search results are shown in **Figure 12.33** below .

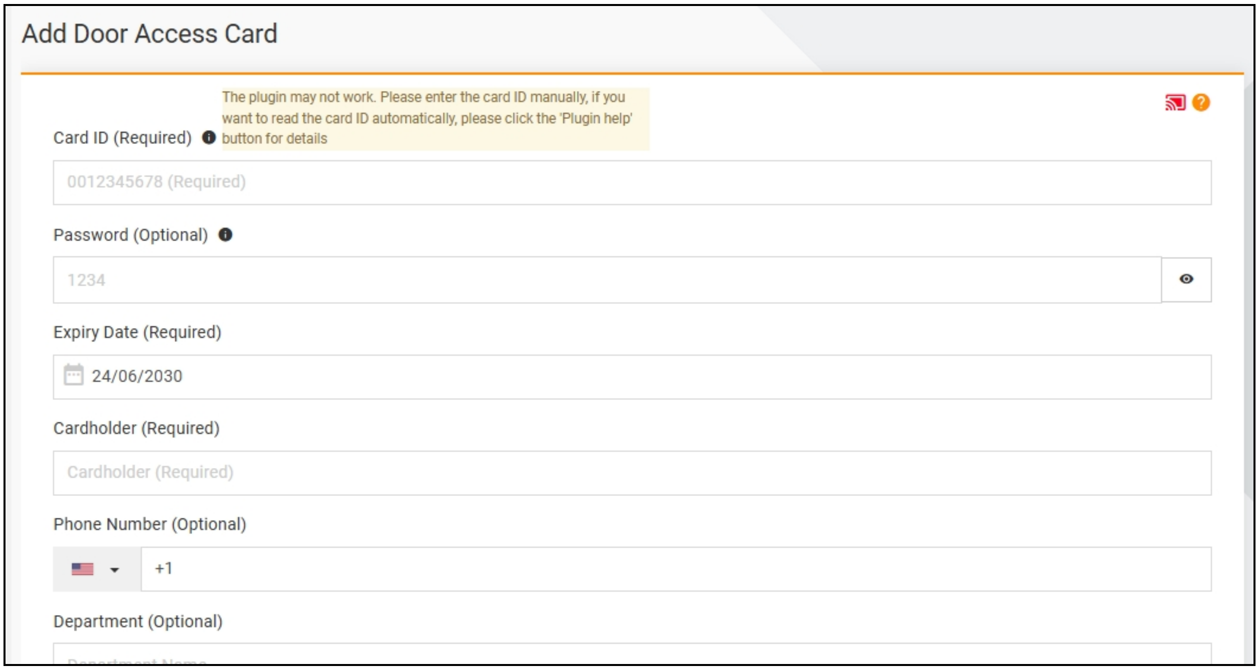
Figure 12.33 Access Card List - Search



Adding an Access Card

1. Click on the *Plus* icon in the upper right corner, to add the Access Card, as shown in **Figure 12.34** on the facing page .

Figure 12.34 Adding Access Cards



2. Enter Card ID (Required), Password (Optional), Cardholder (Required), Phone Number (Optional), and Department (Optional) . Select Expiry Date (Required) and collect Fingerprint (Optional).
3. To set up fingerprint recognition, connect the fingerprint reader to your computer and install the necessary drivers and plugins. Follow the on-screen instructions to register one or two fingerprints. For detailed guidance, refer to the help section in the upper right corner. To delete saved fingerprint data, simply click the **Remove Fingerprint** button.
4. Click *Save*.

NOTE: 1. The card number requires 10 Arabic numerals, and when it is less than 10 digits, it is necessary to fill in 0 before the card number, and the Card ID is not allowed to be repeated.

2. Cardholders are only available as a contact in the address book.

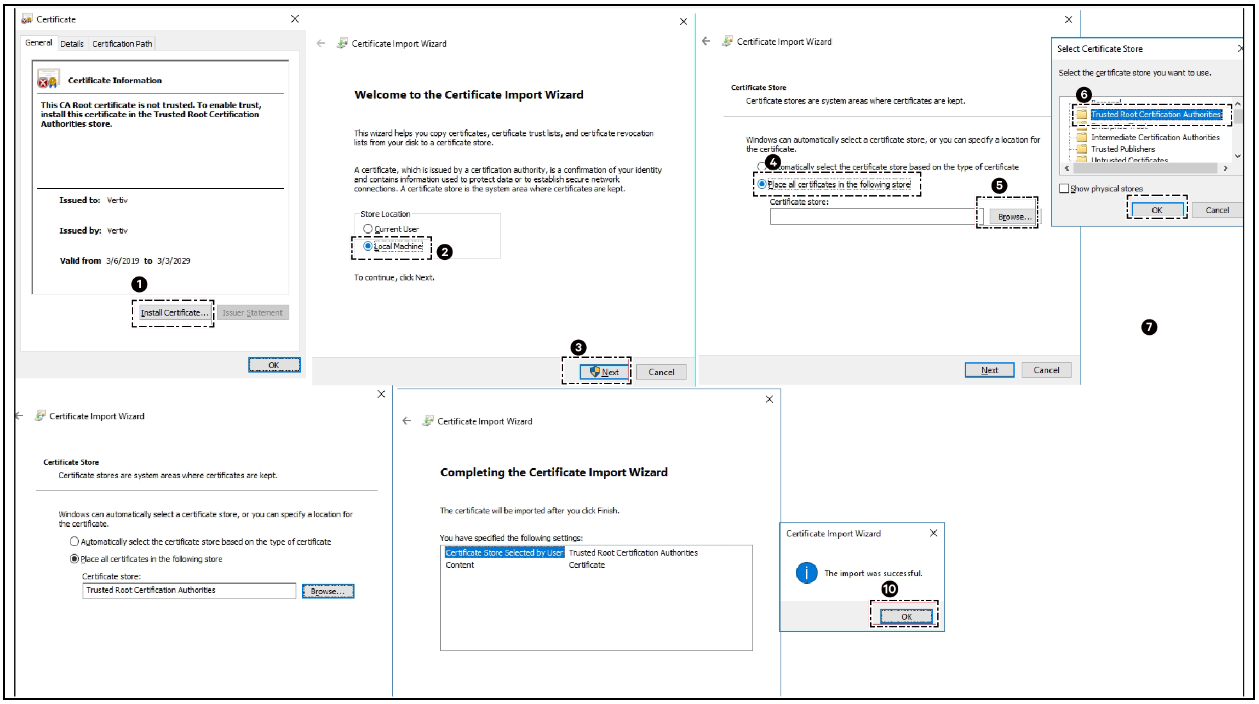
3. The department name must be 1-64 characters.

Access Card Driver

1. On the Card Management page, after you click the Add button and enter Add Door Access Card page, you may see the page displays prompts like this: "The plugin may not work. Please enter the card ID manually, if you want to read the card ID automatically, please click the 'Plugin help' button for details" or "The plugin may not work, please click the 'Plugin help' button for details". In this case, please click the Question mark button in the upper right corner of the current page to assist you in completing the plugin installation.
2. After entering the help page of the plug-in, according to the plug-in help tips, please connect the card reader or fingerprint reader to your computer. If the computer cannot automatically recognize the card reader or fingerprint machine device, you need to install the corresponding plug-in. By clicking Card Reader Driver and Fingerprint Machine Driver, you can download Card Reader Driver USB_CP2102_XP_2000.exe and Fingerprint Machine Driver CH341SER.exe respectively. Then click the card reader and fingerprint machine plug-in to download card_fingerprint_reader_installer.exe and install it.

3. Click on the close icon in the lower right corner. Exit the adding/editing card page. Re-enter the adding/editing card page. Now you can try to read the card number or collect the fingerprint (you can collect one fingerprint or collect fingerprint 1 and fingerprint 2 in sequence).
4. Download Card Fingerprint Reader Server Certificate. After the certificate is downloaded, open card_fingerprint_reader_server.cer. You can click the image in Step2 and install the certificate according to the installation guide, or follow the guide below.

Figure 12.35 Importing the Certificate



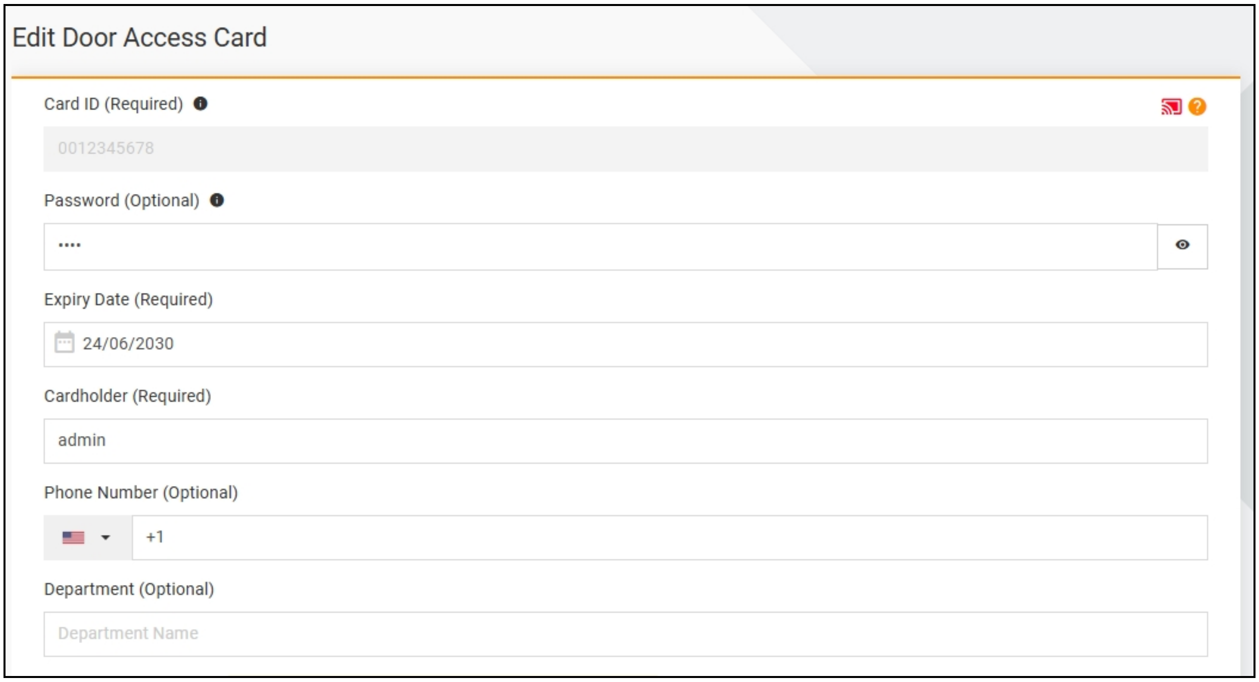
NOTE: 1. Please keep the network connected during the download, if you encounter network problems, please download again.

2. It can connect 1 card reader and 1 fingerprint machine to the computer at the same time.

Editing the Access Card

1. Click on the *ellipses* on the right side of the access card, and select *Edit* in the pop-up drop-down menu as shown in Figure 12.36 on the facing page . After changing the password, expiration date, cardholder, phone number or department information of the access control card, click the *Save* button.

Figure 12.36 Editing the Access Card



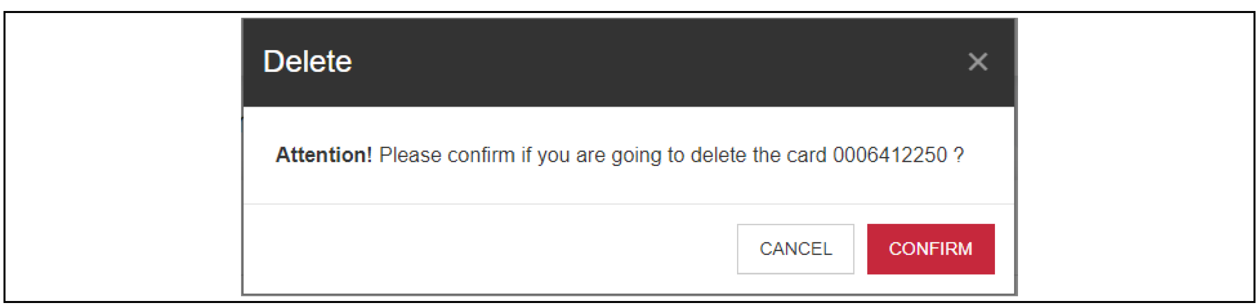
NOTE: 1. The card number cannot be modified, if you want to modify the card number, please delete it and add it again.

2. You can delete the entered fingerprint 1 and fingerprint 2 through the Cancel Fingerprint button.

Deleting the Access Card

Click on the *ellipses* on the right side of the access card and select *Delete* in the pop-up drop-down menu to popup as shown in Figure 12.37 below . Click the *Confirm* button and the access card will be removed.

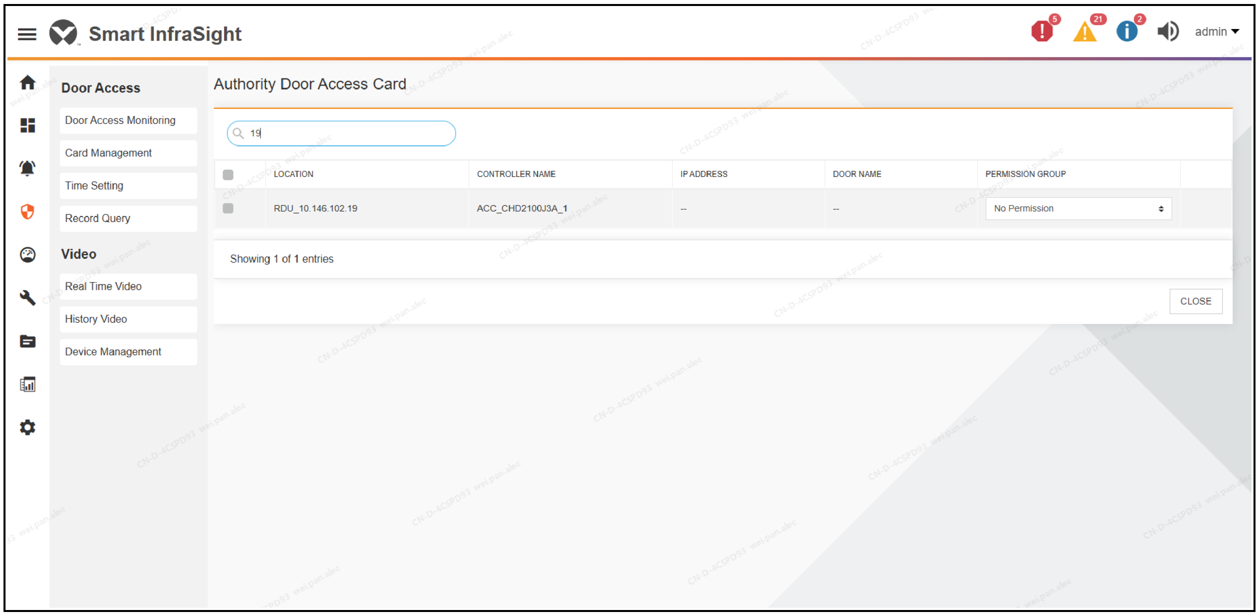
Figure 12.37 Deleting the Access Card Prompt



Access Card Authorization

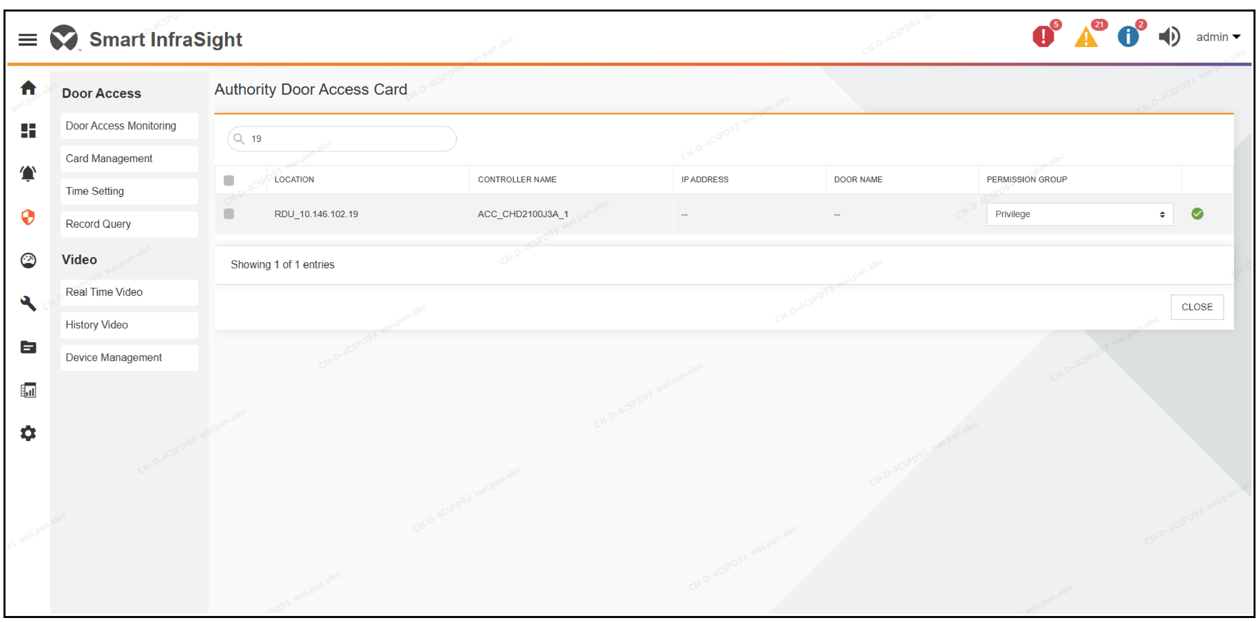
1. Click on the *ellipses* on the right side of the access card and select *Permission* in the pop-up drop-down menu to pop up as shown in Figure 12.38 on the next page . The interface displays all access control devices in the current system and the permission to open the door. The Permission Group column displays the access card permissions for the door (including No Permission, Privileged, Permission Group 1, Permission Group 2, Permission Group 3, and Permission Group 4).

Figure 12.38 Access Card Authorization



2. After selecting an option from the PERMISSION GROUP drop-down, a rotating icon appears in the last column, indicating that authorization is in progress. A green icon displays upon successful authorization, while a red icon appears if it fails. If unsuccessful, the PERMISSION GROUP option reverts to its previous setting, Figure 12.39 below shows an example of the page after successful authorization for Group 1.

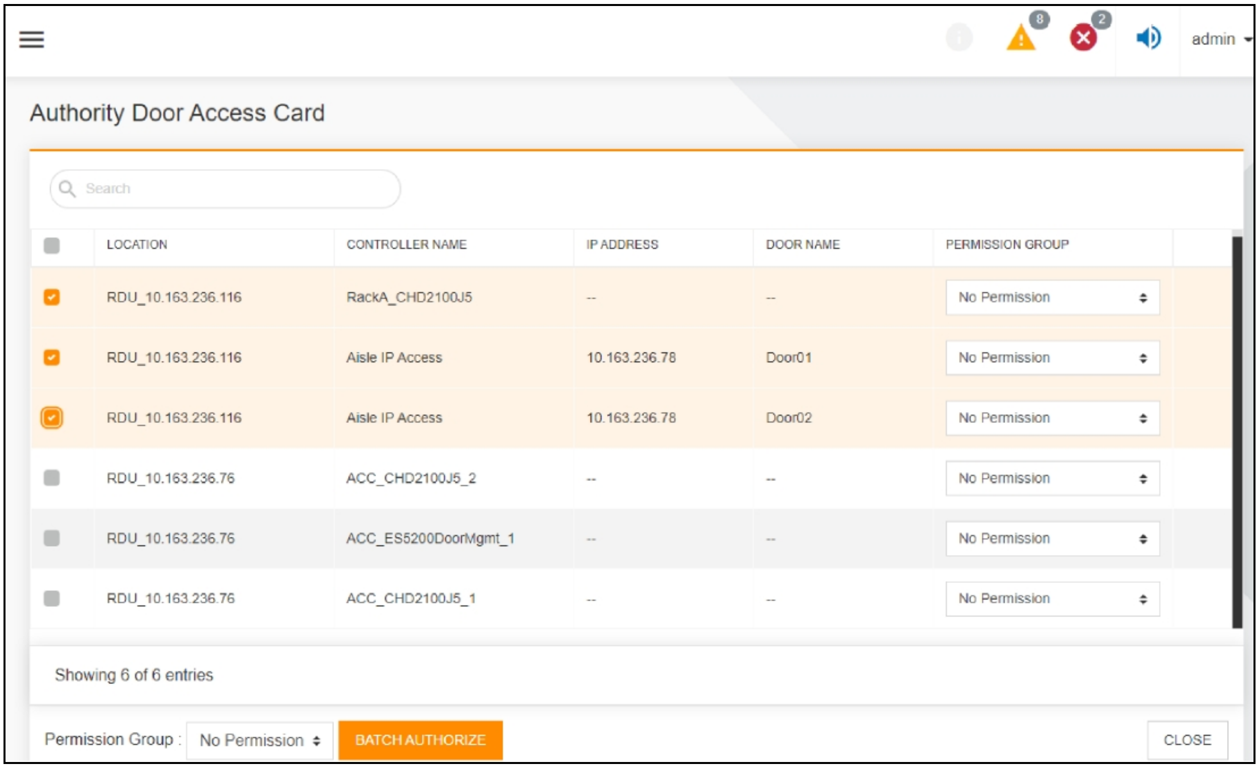
Figure 12.39 Access Authorization - Change Permission Groups



NOTE: When PERMISSION GROUP is set to **No Permission**, the access card cannot open the door. If set to **Privilege**, the card can open the door at any time. For settings **Group 1** through **Group 4**, the card can only open the door within specified time ranges.

3. Clicking the checkbox in the table header's first column selects all data. When you select two or more items, the BATCH AUTHORIZE button appears in the lower right corner of the page. After selecting a permission group, click BATCH AUTHORIZE to modify the permissions of selected door devices in bulk. The last column displays the authorization result: a green icon for success and a red icon for failure. The PERMISSION GROUP option reverts to its previous setting after the change. For example, select door 01 and door 02 under access controller 01, choose Group 2, and click BATCH AUTHORIZE. Upon successful batch authorization, the page will appear as shown in Figure 12.40 below .

Figure 12.40 Door Authorization—Group Modification



NOTE: For IP access controllers: When modifying permissions in batches, a maximum of 100 access control devices can be authorized at a time. For serial access control, when modifying permissions in batches, a maximum of 4 access cards can be authorized at a time.

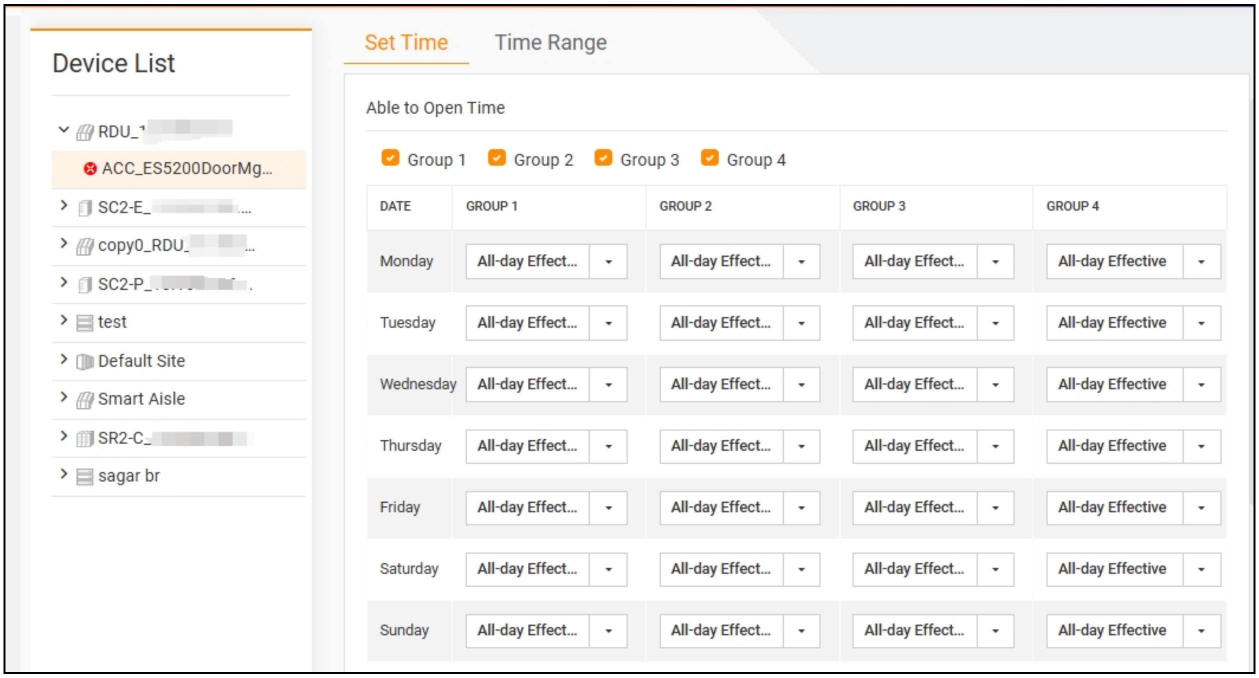
12.3.3 Time Settings

This module explains how to set the time period for the access controller. When you assign a permission group to an access card, the card will only grant entry during the specified time period for that group.

Setting the Time Period

1. Navigate to Security > Time Setting. The Set Time page appears, displaying a list of access controllers on the left and the Set Time tab on the right. The first access controller is selected by default. Icons next to each controller indicate communication status: green for normal, red for failed. Hover over the time range to view specific periods, as shown in Figure 12.41 on the next page .
2. Door opening time ranges differ between serial and IP access controllers. In addition to standard door opening times, you can set ranges for card-and-password entry, constant door opening, and IR door monitoring.

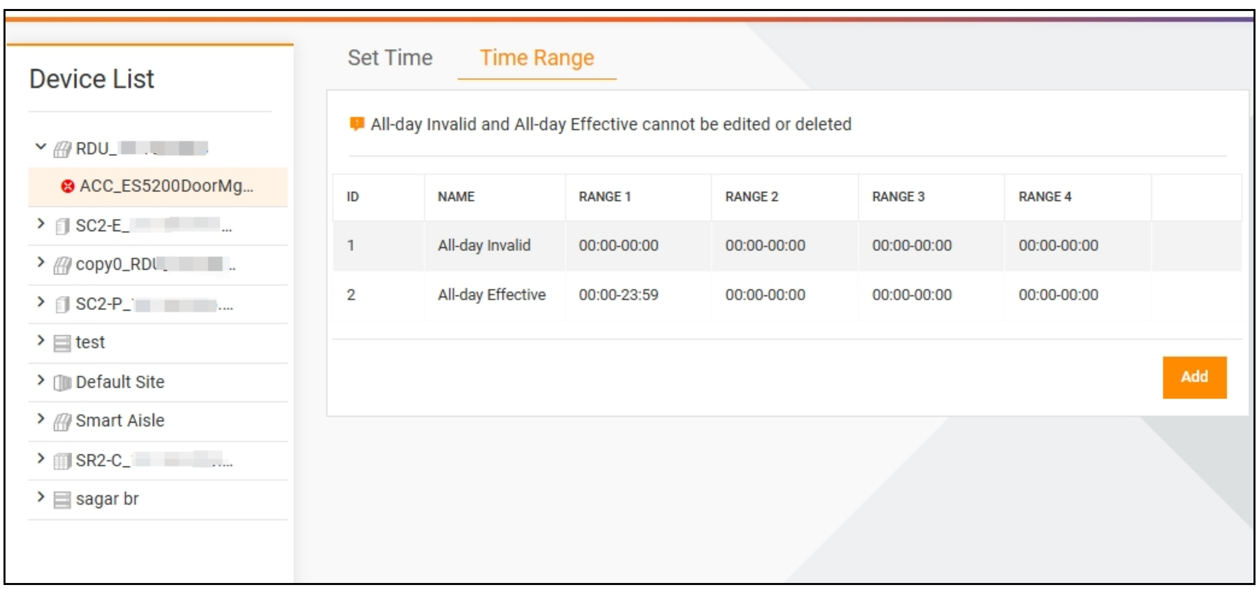
Figure 12.41 Hour List



NOTE: When you add an access controller, the system automatically sets the door opening time range to **All-Day Effective** for four permission groups, while the **Swipe Card with Password** option is set to **All-Day Invalid**. The **All-Day Effective** time range is from 00:00 to 23:59, whereas **All-Day Invalid** is set to 00:00 to 00:00.

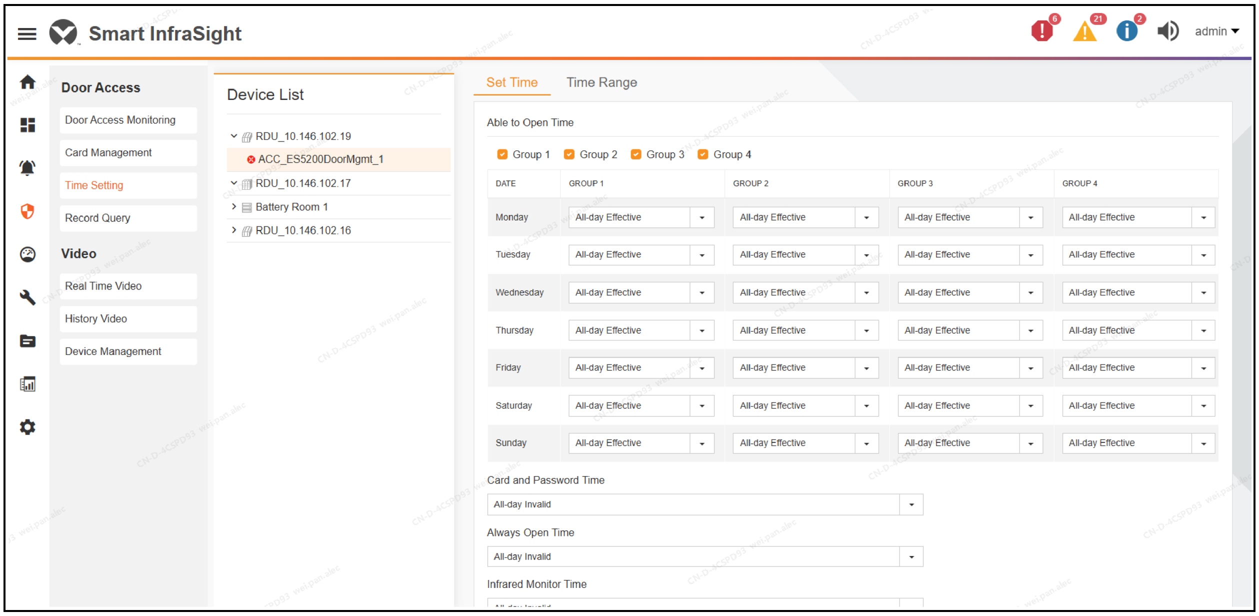
3. To modify the opening time range of a permission group, select the appropriate opening time for the permission group. For example, set the permission of Permission Group 1 to Invalid all day on Monday, and click *Save* after the setting is complete.

Figure 12.42 Modifying the Time Period



4. When you check the checkbox of *Swipe the card with password*, you can configure the time period in which you need to swipe the card and enter password before you can open the door.

Figure 12.43 Modifying the Time Period



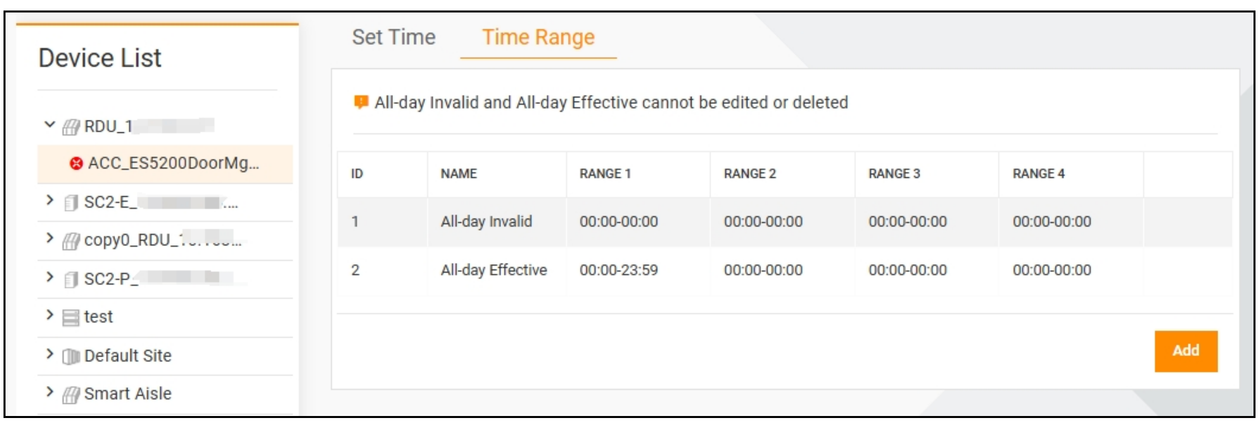
NOTE: 1. Select an access controller, when the Swipe the card with password column of the controller is Invalid all day, the check box of Swipe the card with password will be unchecked automatically.

2 . The Swipe plus password time period takes effect only if the access controller has turned on Swipe plus password in the settings. About the relevant function of modifying the access control controller setting signal.

Time Range

1. On the Time Range tab. The system writes two default time periods. By-default, the system creates two time ranges for each access controller: All-day Effective and All-day Invalid.

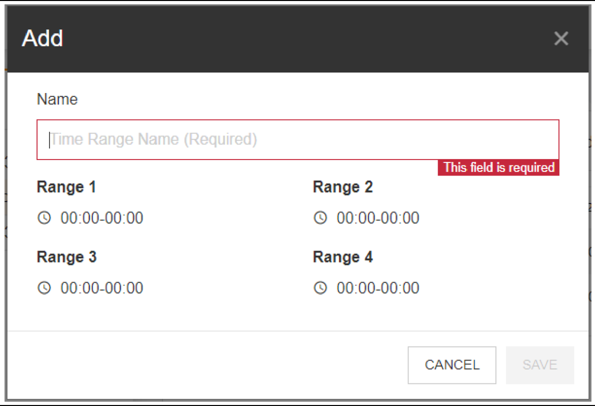
Figure 12.44 Default Time Range



NOTE: Modification and deletion are not allowed for both All-Day Effective and All-Day Invalid time ranges.

2. Click the Add button to pop up the window of adding a time range. On the popup, click the time range you want to modify by selecting the Start Time and End Time. The end time cannot be less than the start time, as shown in Figure 12.45 below .

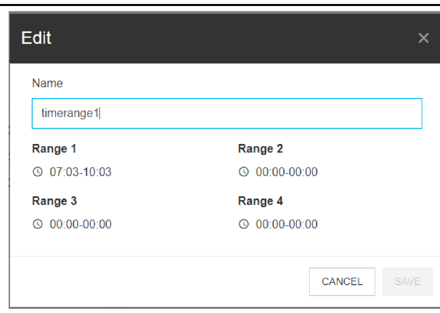
Figure 12.45 Adding/Selecting the Time



2. The access controller with model number CHD806DX-CHD806-1U supports up to 32 range periods.

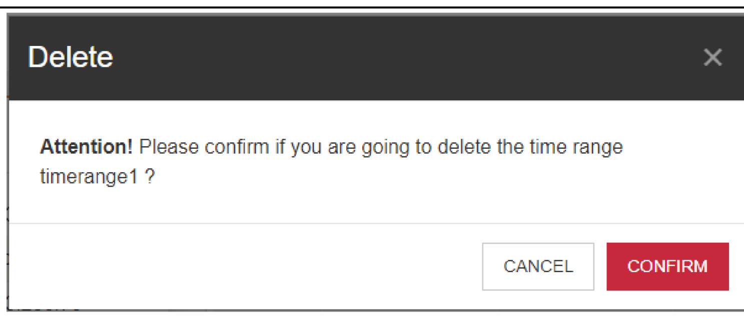
3. After adding a new time range, you can select it when setting permissions for a group.
4. Click the Edit button and you can modify the details of the time range, as shown in Figure 12.46 below .

Figure 12.46 Editing the Time Range



5. When deleting the period data, click the *Delete* button on the right side of the period data as shown in Figure 12.47 below . Click the *Confirm* button and the data will be deleted.

Figure 12.47 Deletion Window Popup



NOTE: 1. If a time range has been used by a permission group, it cannot be deleted

2. Since there is a correspondence between the sequence of the time range and the access controller devices, the time ranges can only be deleted from the back to the front.

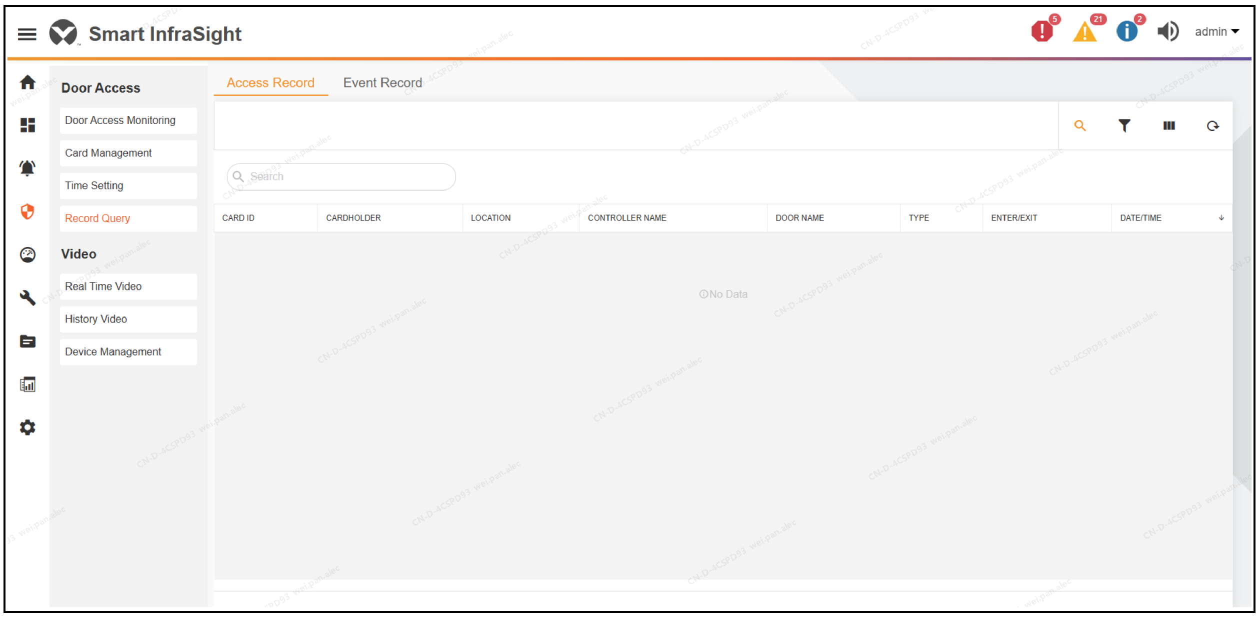
12.3.4 Log Query

This module introduces the display and query functions for access control records. It primarily covers how to view and search card swipe logs and door event logs.

Access Log

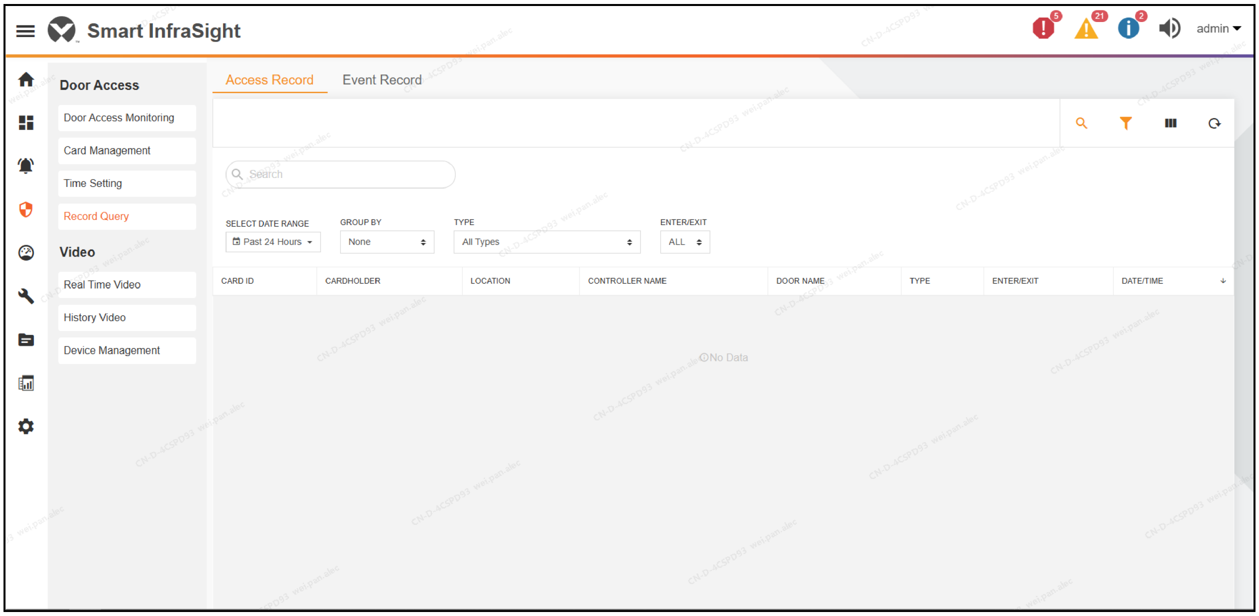
1. Select Log Query in the second-level menu. The Access Log is displayed by-default, and each swiping card log is sorted in reverse order of time, as shown in **Figure 12.48** below .

Figure 12.48 Access Log



2. Enter the content of the query in the search box at the top of the list, and the system will search for the card access history according to the entered content. The search function supports fuzzy queries of card number, cardholder location, access controller, and door name, and supports sorting of time.
3. Click the *refresh* button at the top right of the list. to instantly refresh the list of swipe records.
4. Click the *filter* button at the top right of the list to display the filter. Filters include **Date**, **Group**, **Swipe Type**, and **Door Type**, as shown in **Figure 12.49** on the next page .

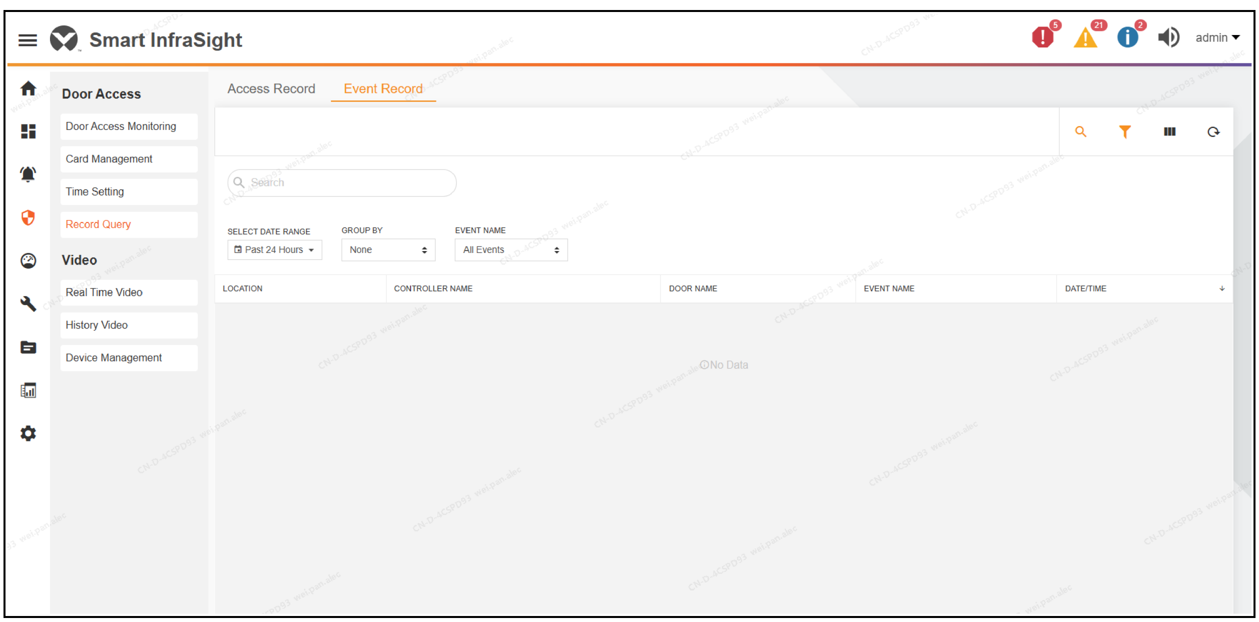
Figure 12.49 Access Log - Filtering



Event Logging

1. Switch to Event Log, the door events are displayed in list. The event logs are sorted in reverse order of time by-default, as shown in **Figure 12.50** below .

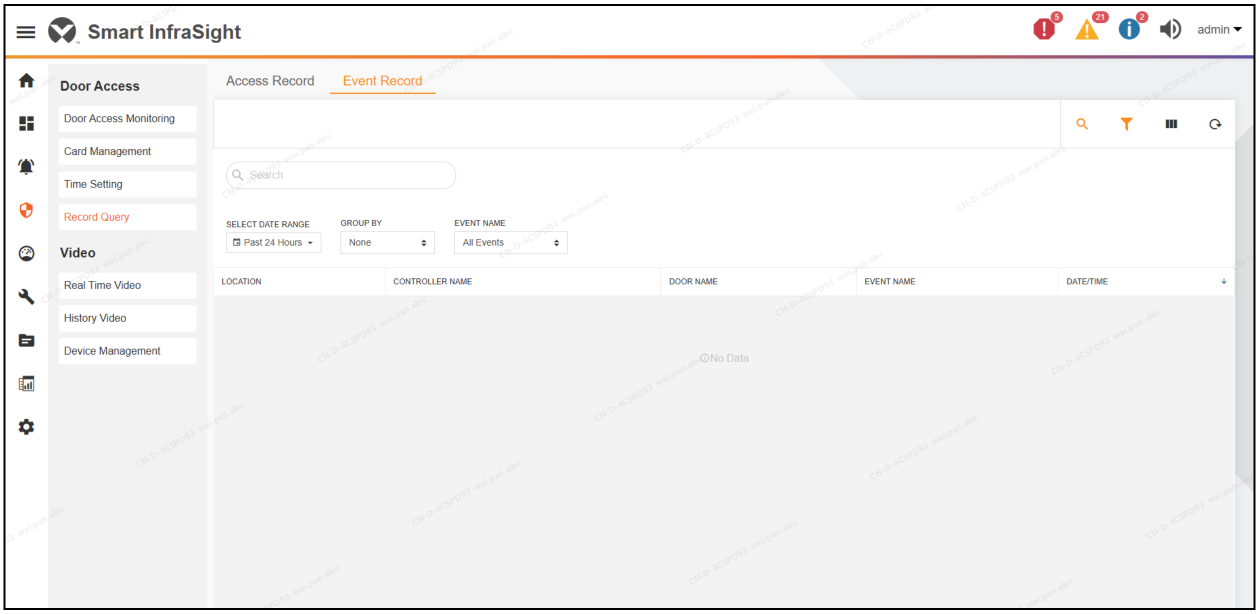
Figure 12.50 Event Log



You can search for event log using location (site) name, access controller name, and door name.

2. Click the refresh button at the top right of the list. to immediately refresh the list of event records.
3. Click the filter button at the top right of the list to display the filter conditions. Filters include **Date**, **Grouping**, and **Event Name.** shown in **Figure 12.51** on the facing page .

Figure 12.51 Filtering the Event Log



This page intentionally left blank

13 Video Management

13.1 General

13.1.1 Overview

This module provides the function of video device management. Users can connect video devices to the system through this module to manage video devices. You can view the live video of the video device; You can search Stored Videos, play Stored Videos, and download Stored Videos based on date and device.

13.1.2 Functional Modules

Video management includes the following functional modules, refer to this manual for detailed functions and detailed information about each functional module, as shown in Detailed Features .

- Device Management
- Live Video
- Stored Videos

13.2 Quick Start

13.2.1 Rapid Deployment Steps

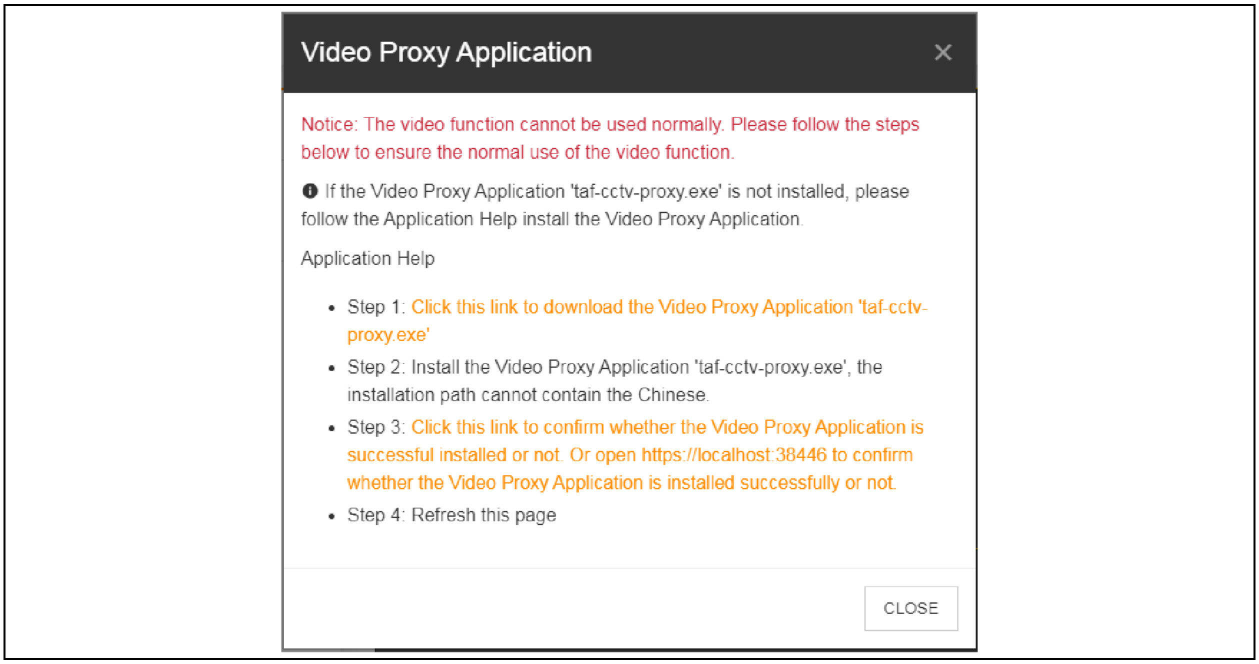
To implement the video management function, perform the following steps:

1. Add an NVR device.
2. Add an IPC device to the NVR channel.

13.2.2 Example

When you use the video module for the first time, you need to install a video plug-in, as shown in Figure 13.1 on the next page .

Figure 13.1 Video Plug-in Help

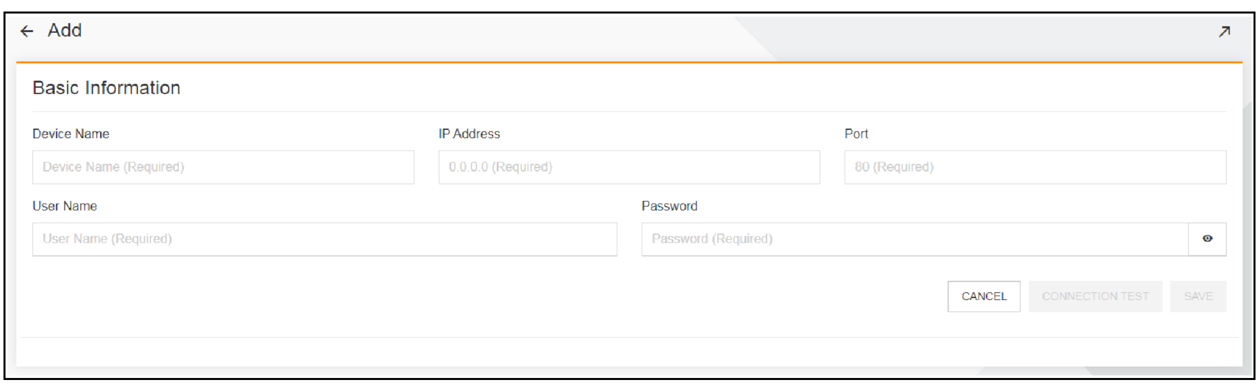


Follow the plug-in help steps. For example, there is currently an NVR device with the IP address **10.163.230.196**. Connect the NVR device to the system to manage the device.

Adding NVR Devices

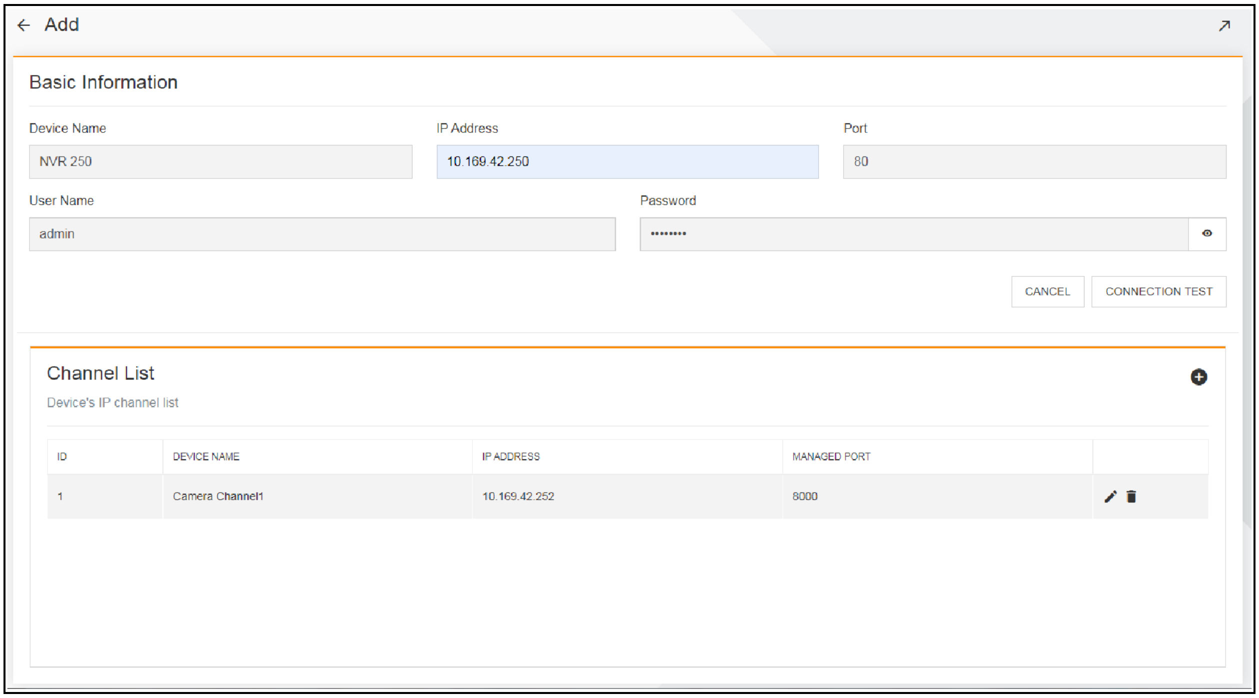
Select Video Management in the first-level menu, and click *Device Management* in the second-level menu. On the device management page, click the *Add* button to open the add NVR device page as shown in **Figure 13.2** below . Enter the device name **NVR 01**, IP address **10.163.230.196**, port **80**, and the username and password of the NVR device. Click on the connection test button, if all the information entered is correct, it will prompt **Connection test successful**. Click the *Save* button to store the device information, and at the same time, the data of the IP channel of the device will be synchronized to the system.

Figure 13.2 Adding an NVR Device



After adding the NVR device successfully, the channel information is displayed.

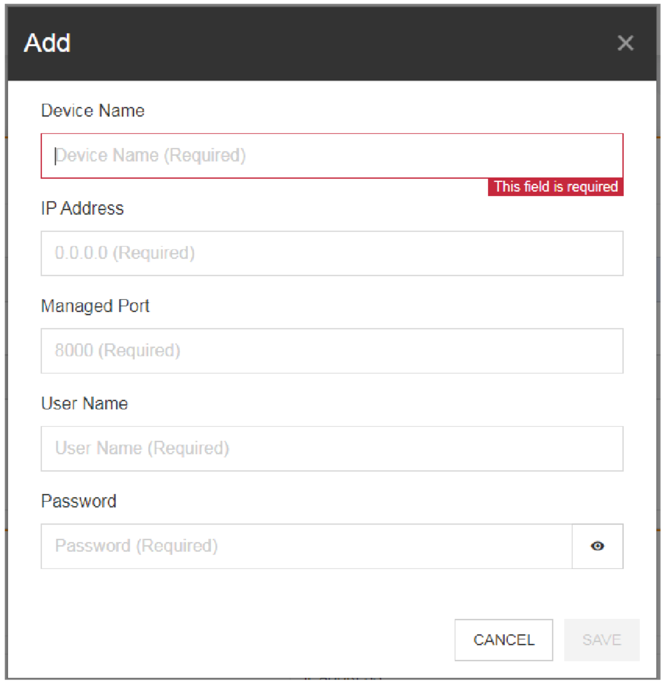
Figure 13.3 NVR Device Information



Adding an IPC Device to the NVR Channel

All IPC devices in the current NVR device channel are displayed in the channel list, if you want to add a new IPC device to the channel, click the **Add** button on the upper-right of the Channel List table and the add IPC popup will show up as shown in Figure 13.4 on the next page . Enter the IPC device name, IP address, management port (the default management port is 8000), the username and password of the IPC device, and click the *Save* button. After the IPC device is added, the channel list is automatically refreshed.

Figure 13.4 Adding an IPC Device



After adding NVR and IPC devices, you can click ***Real Time Video*** and ***Historical Video*** in the secondary menu to preview the live video and play back and download the Historical video.

13.3 Detailed Features

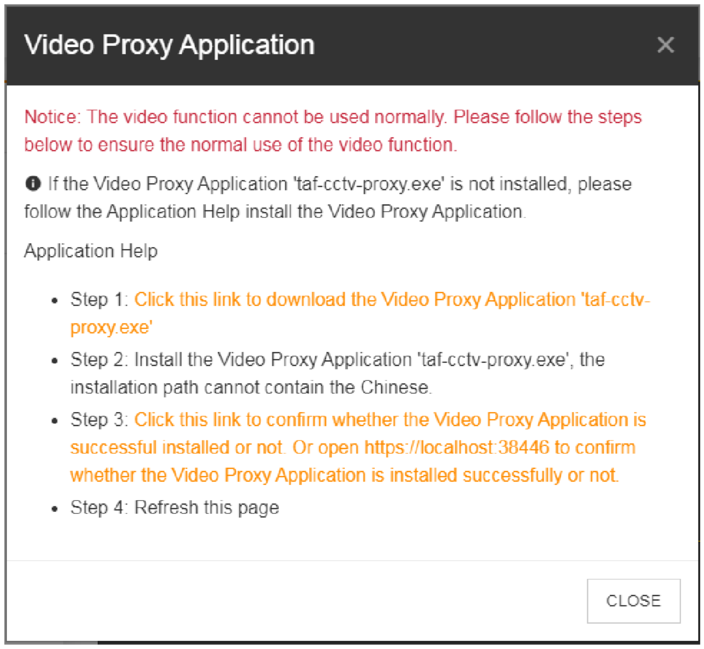
This section describes the detailed features of video management. Video management includes three modules: real-time video, historical video, and device management.

13.3.1 Video Plug-ins

If you are using the video function for the first time, you need to follow the plug-in help guide to install a video plug-in.

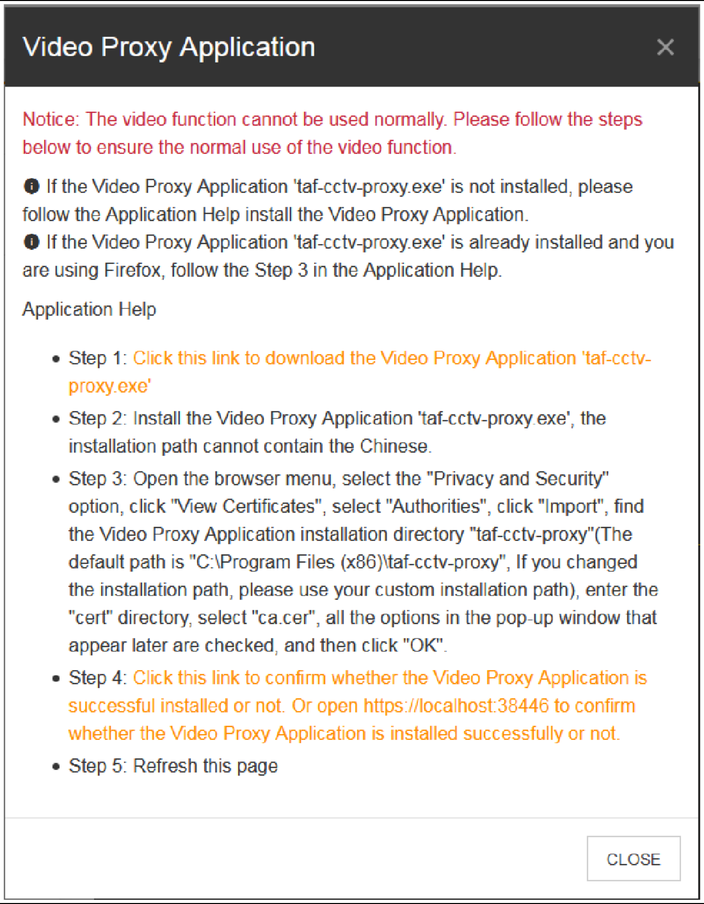
1. The Google Chrome/Edge video plug-in help prompts is shown in Figure 13.5 on the facing page .

Figure 13.5 Google Chrome Video Add-on Help



2. The help prompt of the video plug-in in Firefox browser is as shown in **Figure 13.6** on the next page .

Figure 13.6 Firefox Video Add-on Help



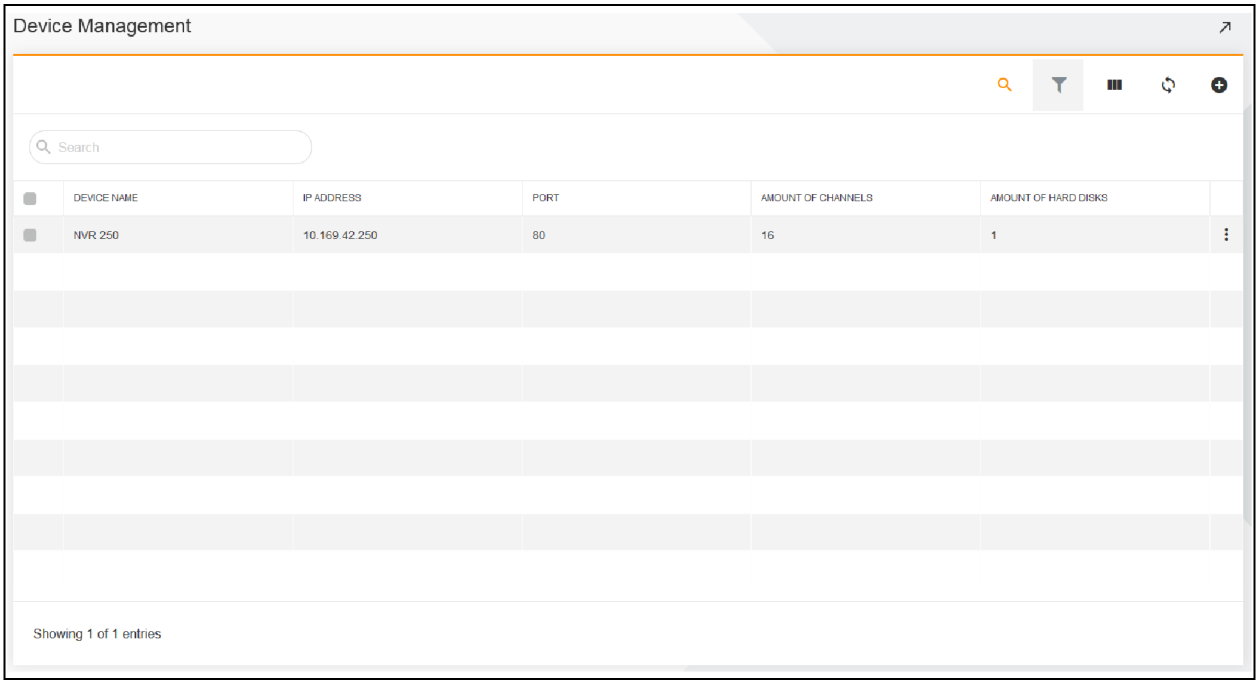
13.3.2 Device Management

This module describes the management functions of video devices, including adding, deleting, and modifying NVR devices, and adding, deleting, and modifying IPC devices in the channel list.

Device List

Select Security in the first-level menu, select Device Management in the second-level menu, and open the device management page, as shown in Figure 13.7 on the facing page.

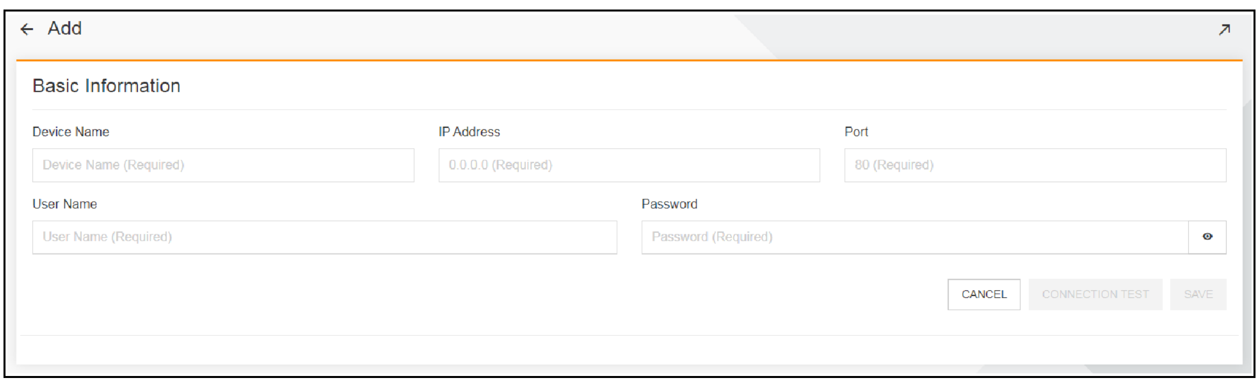
Figure 13.7 List of NVR Devices



Adding a Device

1. Click the Add button. to open the add device page, as shown in **Figure 13.8** below .

Figure 13.8 Adding NVR Device



2. Enter the device name, IP address, port, device username and password.
3. To test whether the information you have entered is correct, you can click the Connection Test button.
4. After confirming that the device information entered is correct, click the *Save* button. After the device information is stored, the data of the IP channel of the device is synchronized to the system.

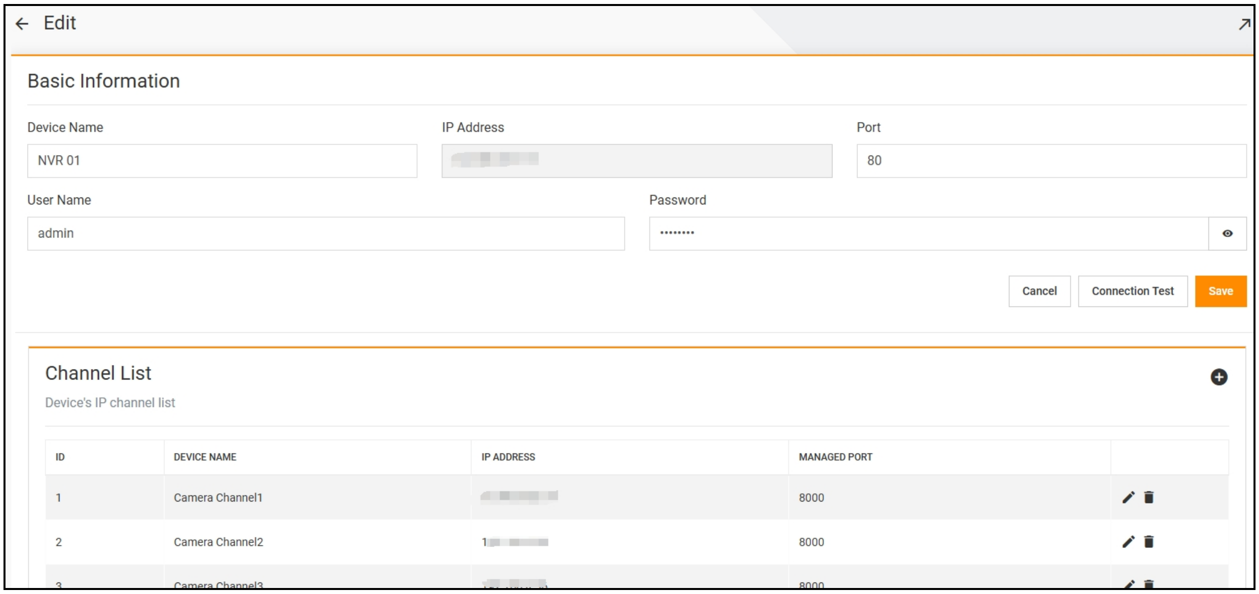
NOTE: 1. The device name must be 3-64 characters long and cannot be repeated.

2. Duplicate IP addresses are not allowed.

Editing the Device

1. Click on the *ellipses* on the right side of the device row, and select *Edit* from the pop-up drop-down menu to open the interface, as shown in Figure 13.9 below .

Figure 13.9 Editing NVR Device



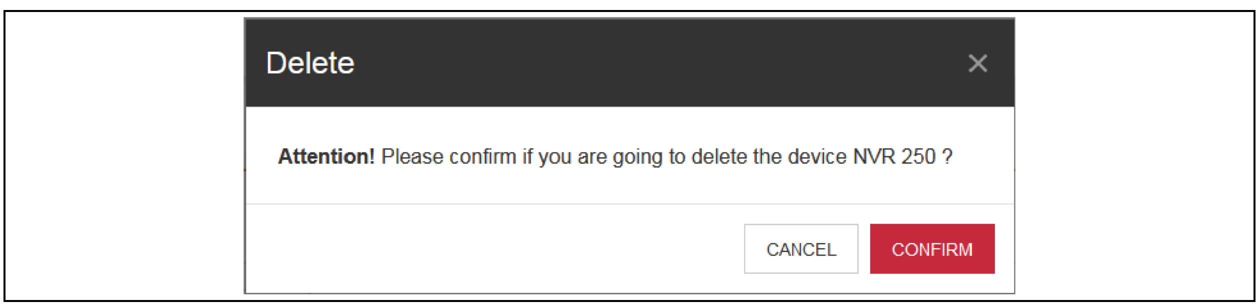
2. After changing the device name or the Username and password of the device, click *save*.

NOTE: The IP address and port of the video device cannot be modified, so if you want to modify the IP address and port, delete it and add it again.

Deleting the Device

1. Click the *ellipses* on the right side of the device data row, select *Delete* in the pop-up drop-down menu, and the prompt interface will popup as shown in Figure 13.10 below .

Figure 13.10 Deletion Popup Window



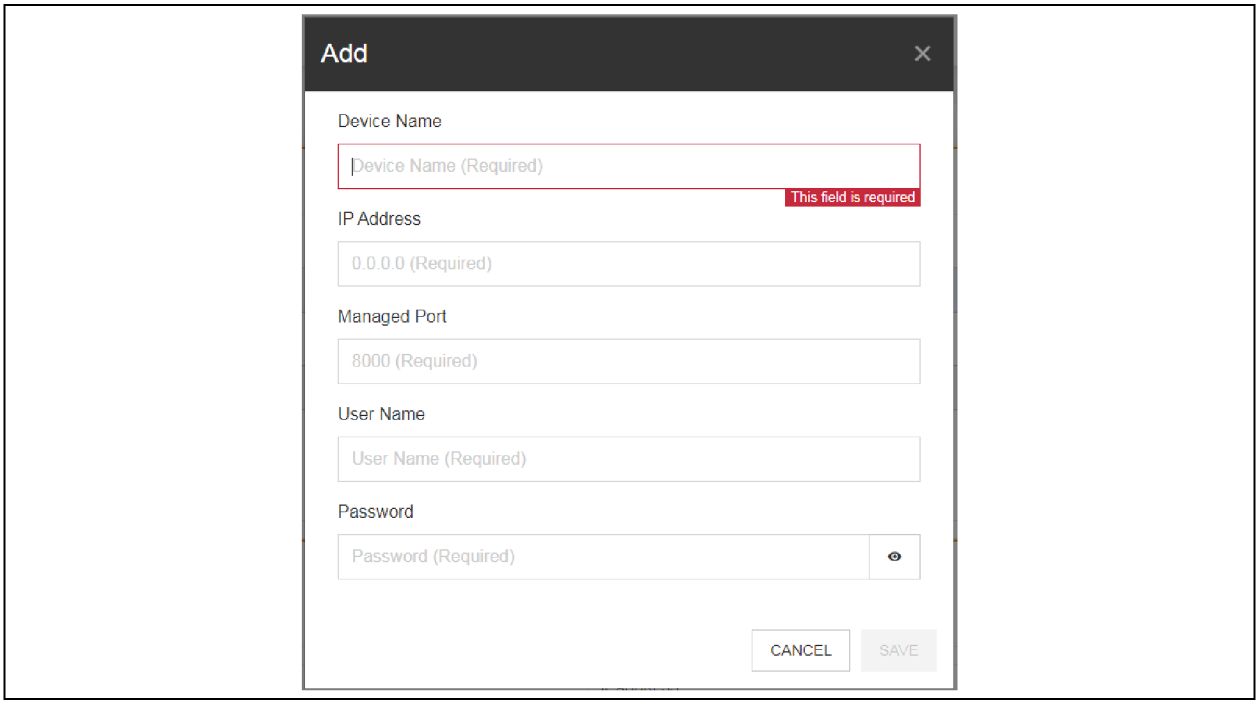
2. Click on *Confirm* and the device will be deleted.

NOTE: When a device is deleted, all IPC device data in the device channel will be deleted synchronously.

Adding an IPC Device to the Channel

1. Select **Security** in the first-level menu, select **Device Management** in the second-level menu, and open the device management page. Click on the *ellipses* on the right side of the NVR device, select *Edit* to open the device editing page, and click the Add button in the channel list table to open the add IPC popup, as shown in **Figure 13.11** below .

Figure 13.11 Adding an IPC Device



2. Enter the IPC device name, IP address, management port (the management port is 8000 by default), the username and password of the IPC device, and click on the *Save*.

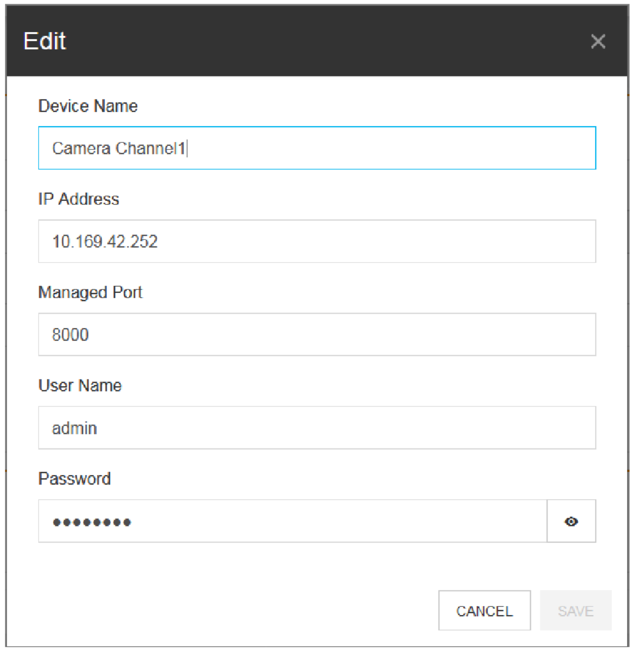
NOTE: 1. The IPC device name must be between 3 and 64 characters, and the name of the IPC device in the same NVR device channel cannot be duplicated.

2. The IP addresses of IPC devices in the same NVR device channel are not allowed to be duplicated.

Editing the IPC Device in the Channel

1. In the channel list, click the *edit* button on the right side of the IPC device information, and the interface will pop up as shown in **Figure 13.12** on the next page .

Figure 13.12 Editing the IPC Device



2. Change the IPC device name, IP address, management port (the default management port is 8000), the Username or password of the IPC device, and click on the *save*.

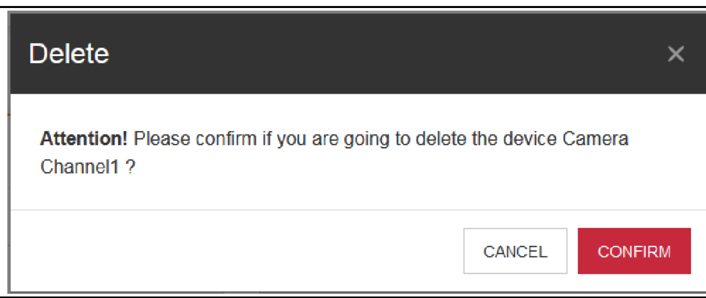
NOTE: 1. The IPC device name must be between 3 and 64 characters, and the name of the IPC device in the same NVR device channel cannot be duplicated.

2. The IP addresses of IPC devices in the same NVR device channel are not allowed to be duplicated.

Deleting the IPC Device in the Channel

1. In the channel list, click on the *delete* on the right side of the IPC device information, and the prompt interface will pop up as shown in Figure 13.13 below .

Figure 13.13 Deleting the IPC Device



2. Click on the *Confirm* and the IPC device will be removed from the channel list.

NOTE: Deleting a device is synchronously deleting the device's data from the current system.

13.3.3 Real Time Video

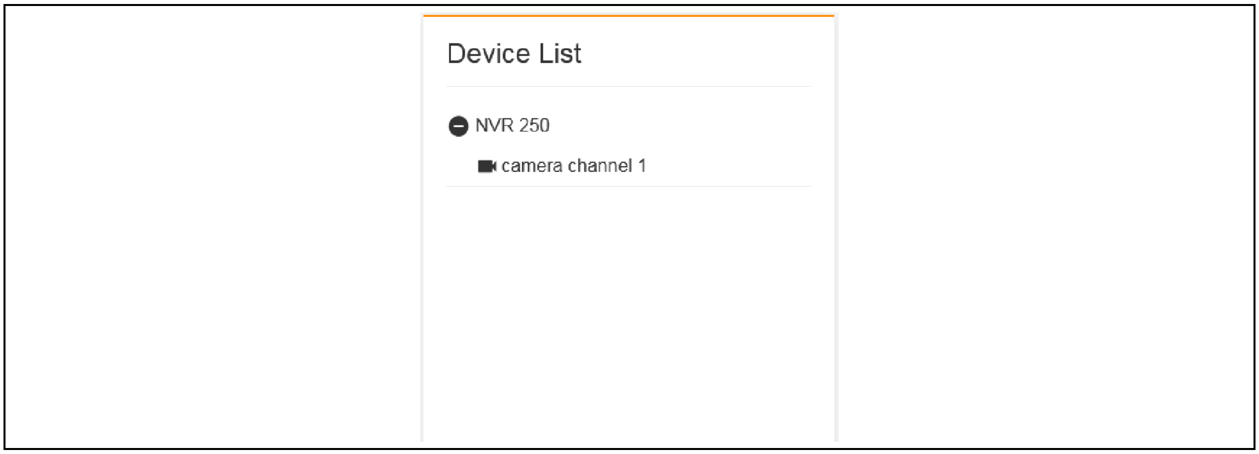
This module introduces the functions of previewing live video.

Limitations: Firefox doesn't support video recording. Internet Explorer 11 lacks support for video preview stopping, video capture, and electronic magnification.

Device List

Select **Security** in the first-level menu, and select **Real Time Video** in the second-level menu to open the page of Real Time Video. The video device is displayed on the left side of the page, and the device is displayed in a tree, the first level displays the name of the NVR device, and the second level displays the name of the IPC device in the IP channel of the device, as shown in **Figure 13.14** below .

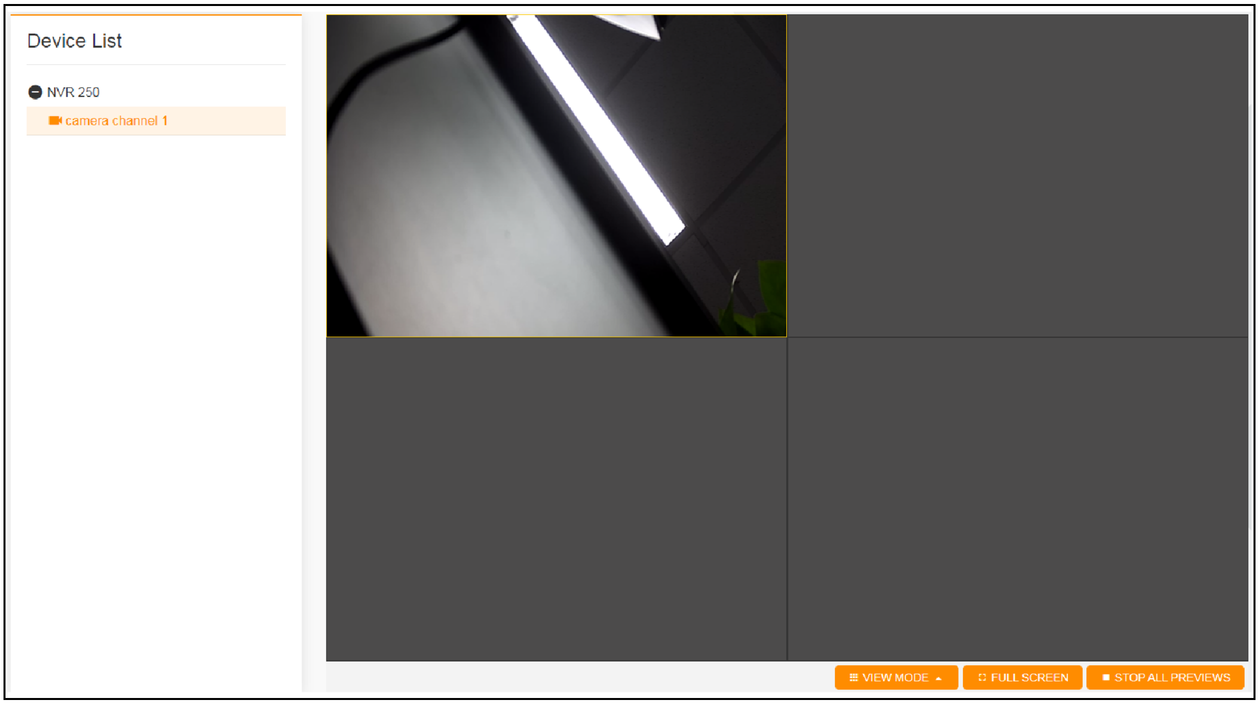
Figure 13.14 Device List



Previewing the Video

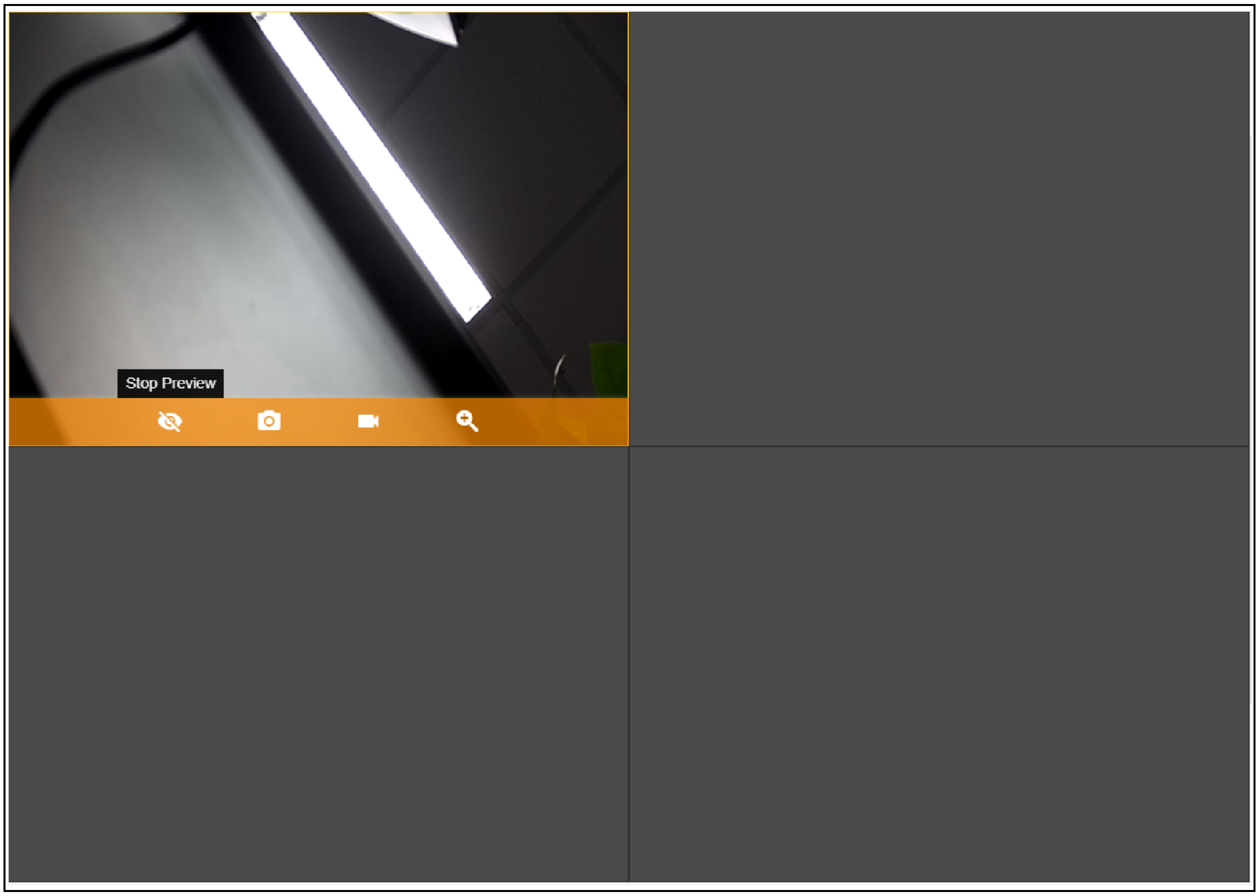
1. To stop previewing a video, hover your mouse over the bottom of the small preview window and click the Stop Preview icon, as shown in **Figure 13.15** on the next page .

Figure 13.15 Previewing the Video



2. To stop previewing a video, hover your mouse over the bottom of the small preview window and click the Stop Preview icon, as shown in **Figure 13.16** on the facing page .

Figure 13.16 Stopping the Preview

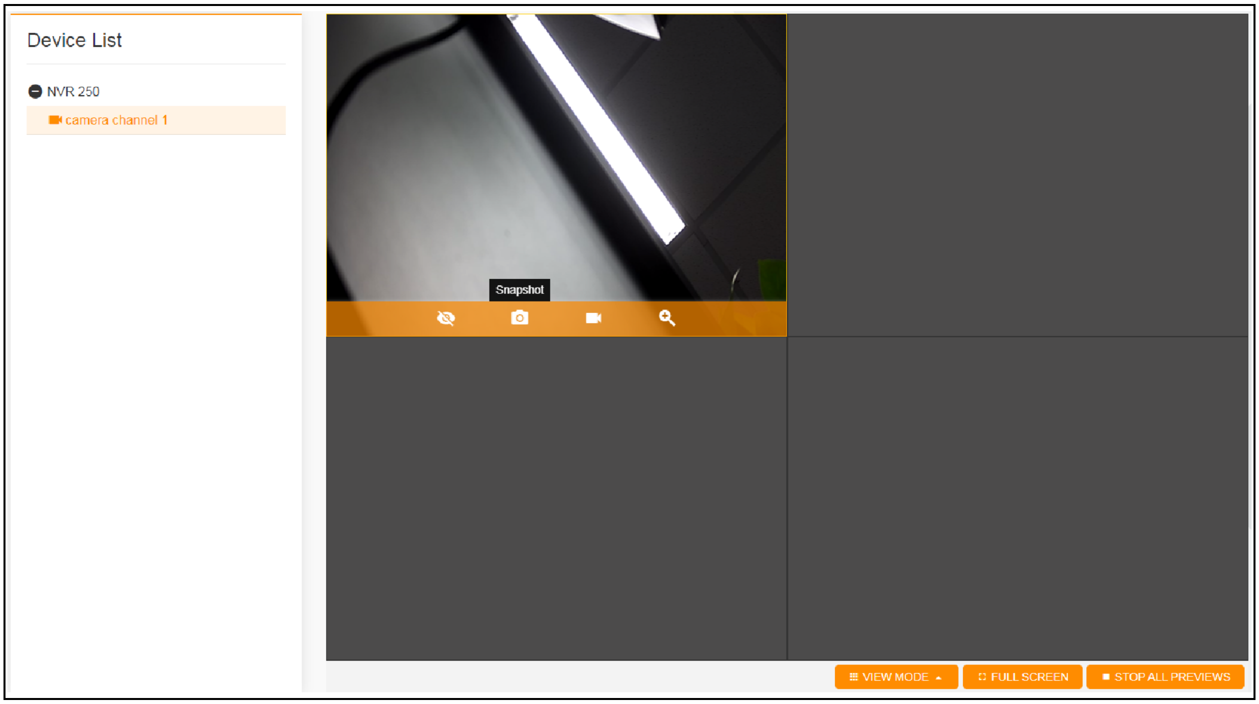


NOTE: The video preview feature is currently supported on Chrome 73+, Firefox 66+, and Edge 87+. It is not available on other browsers.

Capturing the Image

1. Select the small window you want to operate, hover the mouse to the bottom of the window, and click the *snapshot* button, as shown in **Figure 13.17** on the next page .

Figure 13.17 Capturing the Image

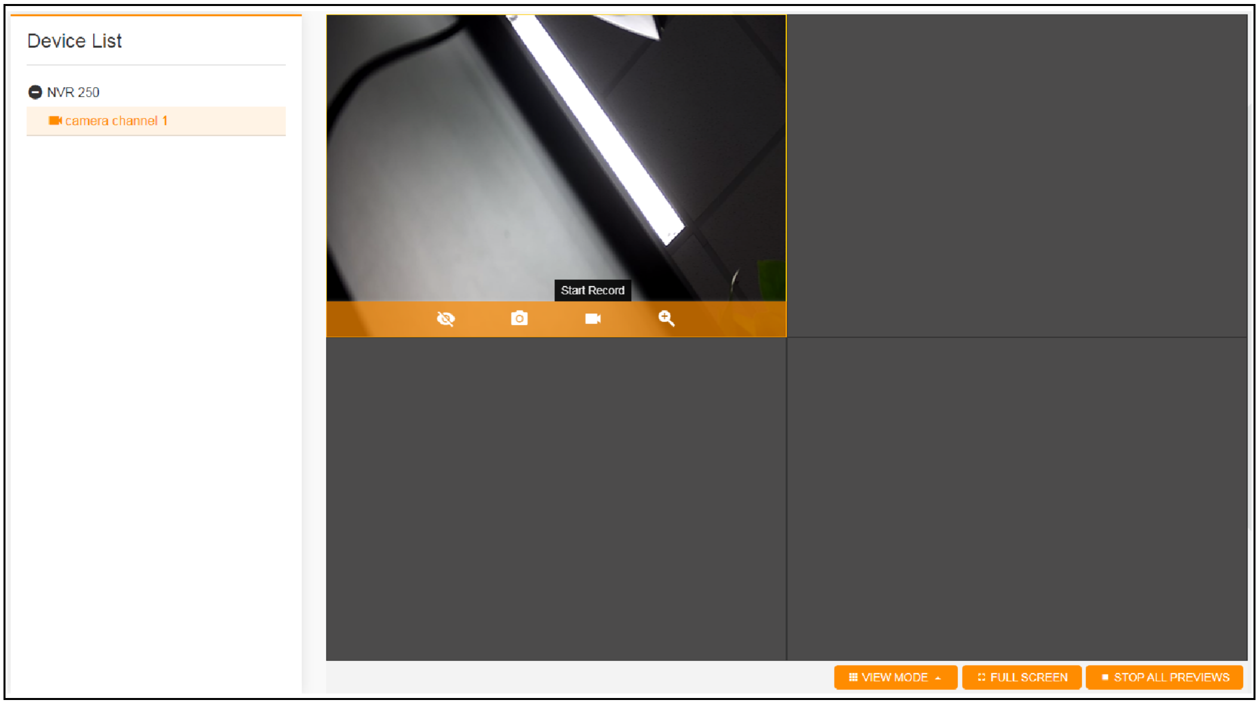


2. After clicking the snapshot button, the currently playing frame will be automatically captured.

Recording the Video

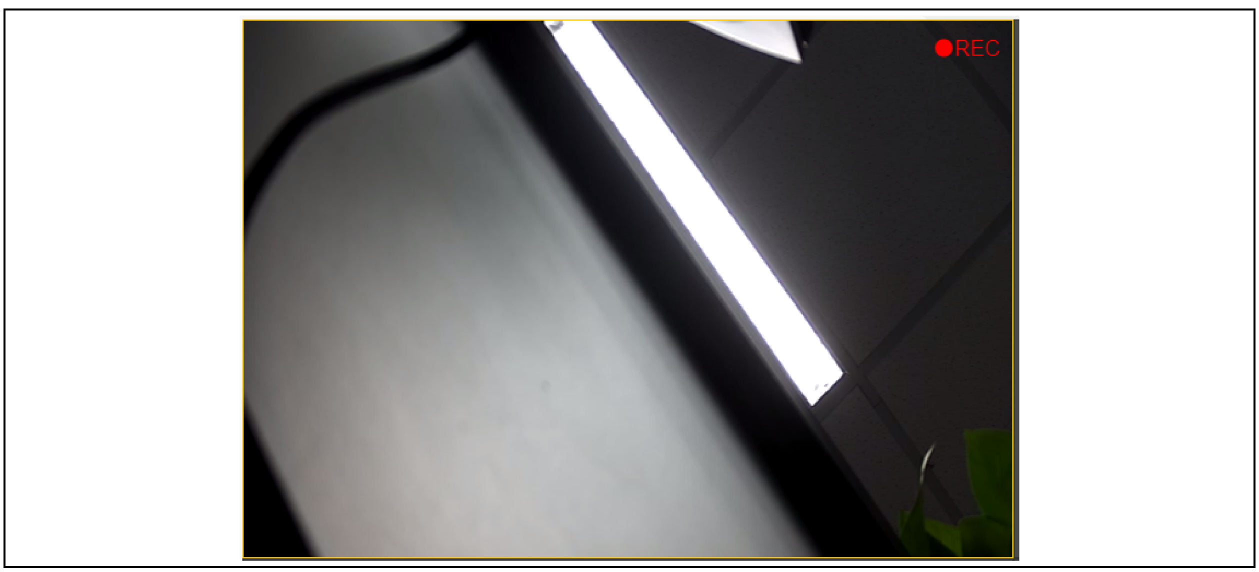
1. Select the small window you want to operate, hover the mouse to the bottom of the window, and click the *Start Record* button, as shown in **Figure 13.18** on the facing page .

Figure 13.18 Recording the Video



2. After clicking the Start Record button, the REC logo will flash in the upper right corner of the video playback window, as shown in Figure 13.19 below .

Figure 13.19 Recording the Video



3. If you want to end the recording, select the small window you want to operate, hover the mouse to the bottom of the window, and click the *End* Record button to end it and download the recording file automatically.

NOTE: 1. After clicking the Start Record button, the button will automatically change to the Stop Record button.

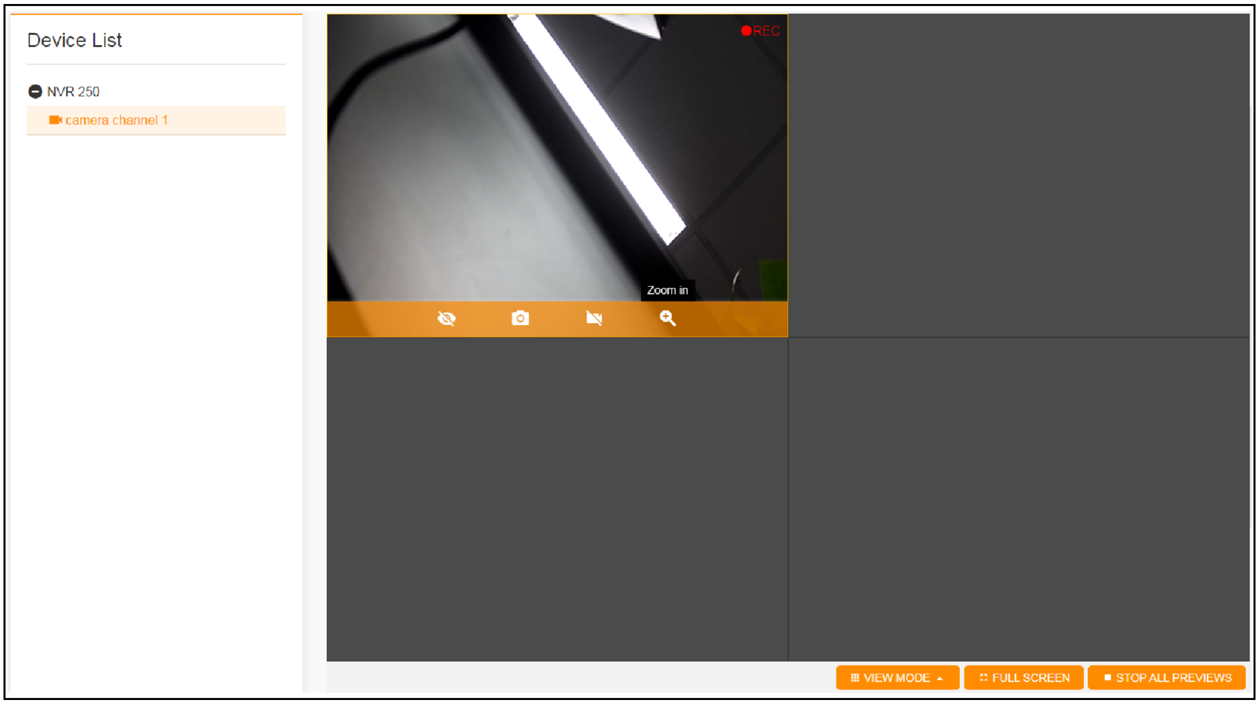
2. Multiple videos can be recorded at the same time.

3. When you stop previewing the live video while recording, the recording will be automatically stopped and the recording file will be downloaded.

Zoom-in

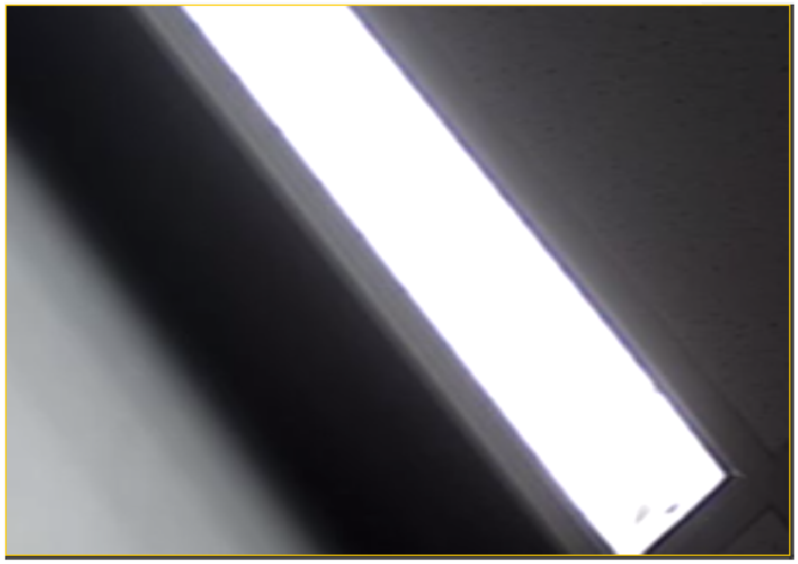
1. Select the small window you want to operate, hover the mouse to the bottom of the window, and click the *Zoom in* button, as shown in **Figure 13.20** below .

Figure 13.20 Zoom-in



2. After clicking the Zoom-in button, use the mouse to select the area to be enlarged in the video window (press the left mouse button and move the mouse position, a red rectangular box will appear in the window, and the rectangular box is the selected area), and the selected area will be enlarged, as shown in **Figure 13.21** on the facing page .

Figure 13.21 Zoom-in View

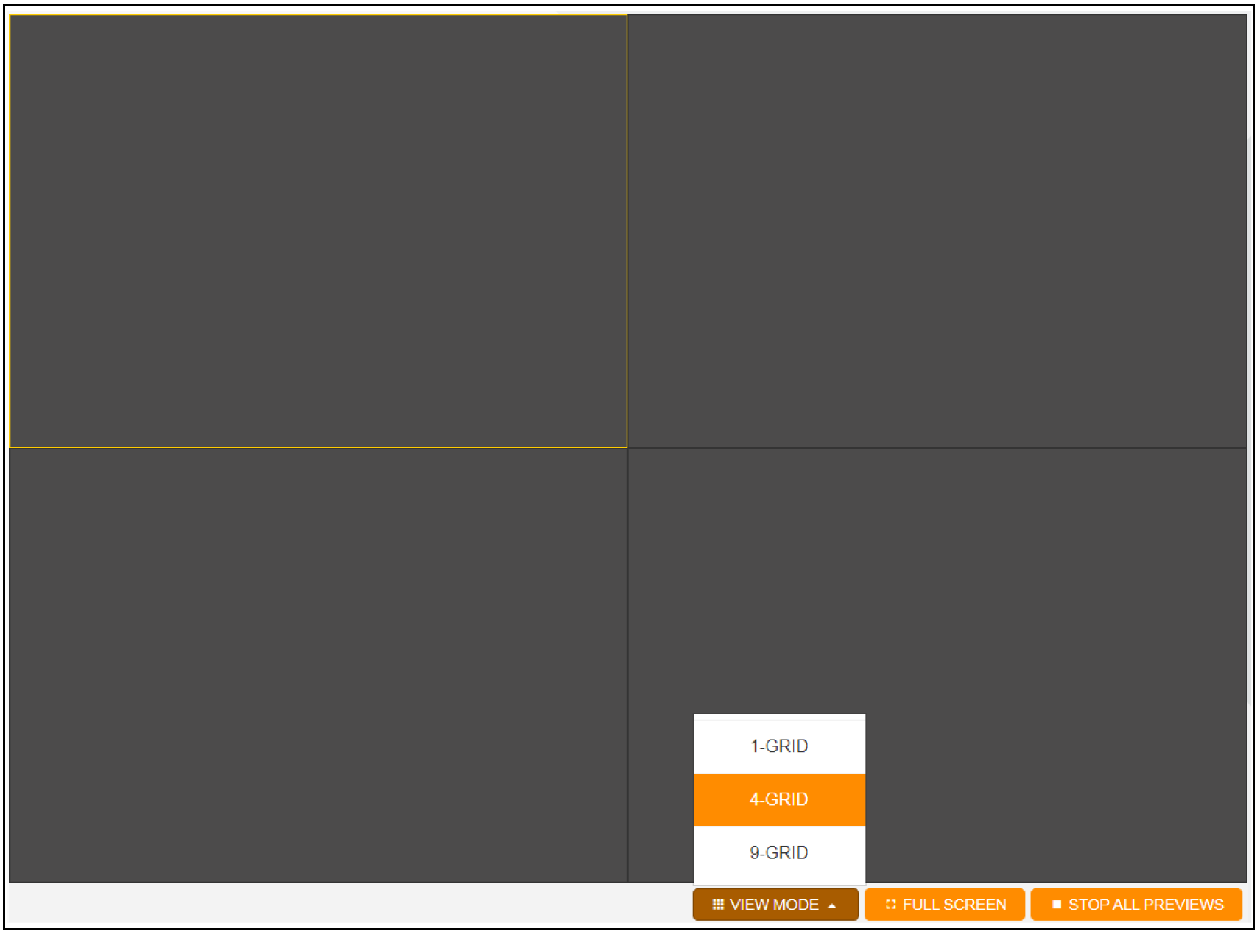


3. To restore a window, hover your mouse over its bottom edge and click the restore button.

Toggle Split-Screen View

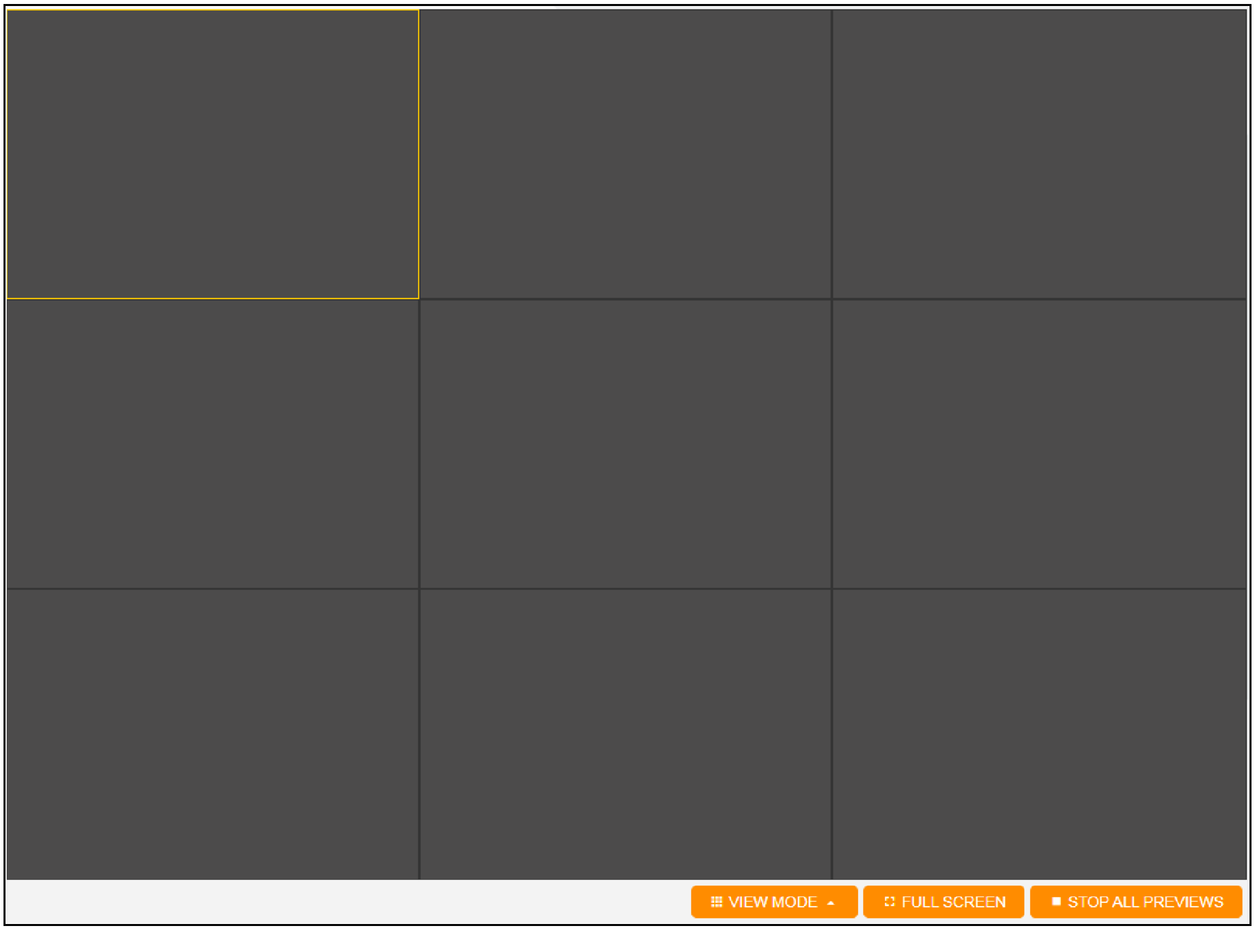
1. Click the View Mode button to choose how many camera feeds to display simultaneously. You can split the screen into one, four, or nine frames, as shown in **Figure 13.22** on the next page .

Figure 13.22 Split-Screen Mode



2. Select from various split-screen options to divide the window into multiple smaller panels. For example, choosing the 9-GRID will change the display, as shown in **Figure 13.23** on the facing page .

Figure 13.23 9 Grid Screen View



Full Screen

1. Double-click any window to display it in full screen mode.
2. Double click again or press the Esc key to exit the full screen mode.

Stopping All Previews

1. Click ***Stop All Previews*** at the bottom of the page to halt camera displays.
2. If a camera is recording, it will automatically stop, save, and download the recording before shutting down.

13.3.4 Historical Videos

This module covers the functions for managing historical Videos. These include querying, playing, and downloading videos, as well as controlling playback features such as changing playback time, pausing, stopping, single-frame viewing, and full-screen mode.

Searching the Historical Videos

Navigate to Security, then select History Videos from the submenu. On the left side of the page, you'll find a date selection box and a video device list. The devices are displayed in a tree structure, with NVR devices at the top level and their associated IPC devices nested underneath, as shown in **Figure 13.24** on the next page.

Figure 13.24 historical Videos

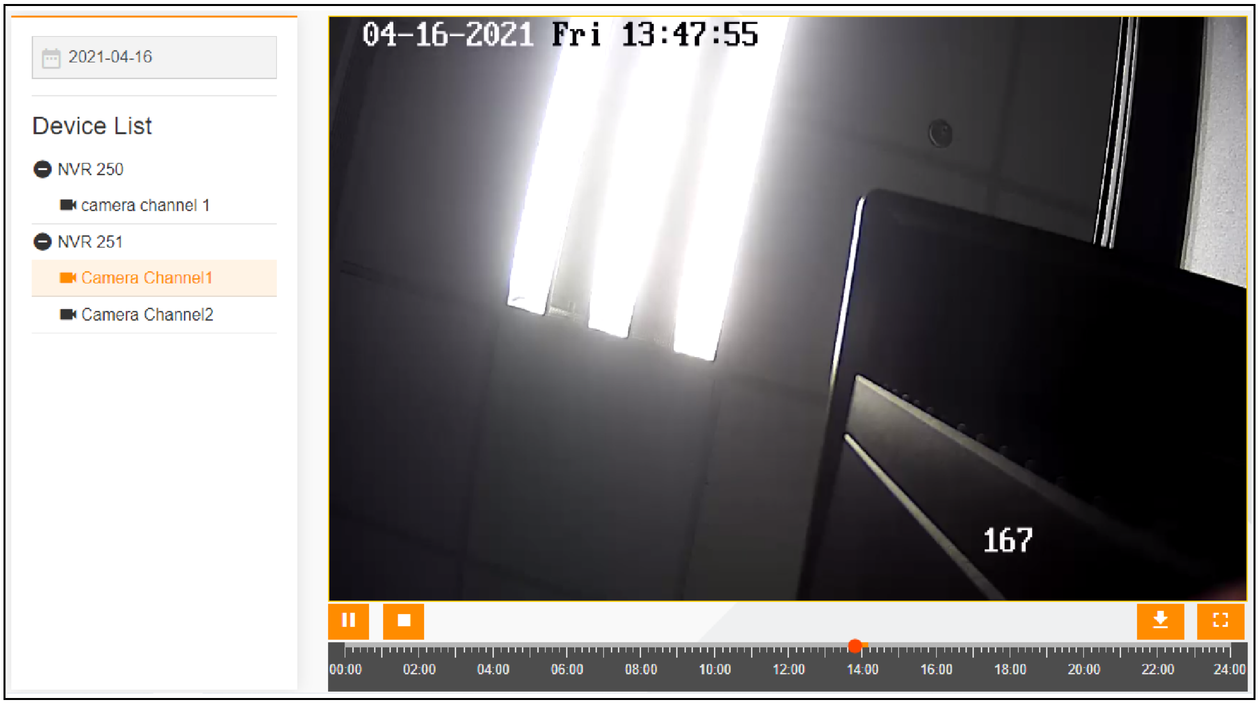
1. The date selection box shows today's date by default. To change it, click the box and choose your desired date.
2. Select the IPC device from the list to view its historical video for the chosen date. The orange bar at the bottom of the playback screen indicates available video segments, as shown in **Figure 13.25** below .

Figure 13.25 Searching the historical Videos

Playing a historical Video

1. After selecting a date or clicking an IPC device in the device list, the play button becomes available if there is a historical video on the device within that time range.
2. When the play button is available, click the *play* button to start playing from the start time of the historical video, as shown in **Figure 13.26** below .

Figure 13.26 Playing a History Video



NOTE: Currently, historical video playback is only supported in Chrome 73+, Firefox 66+, and Edge 87+.

Changing Playback Time

1. A dot on the timeline indicates playback progress. Drag this dot within the orange area to start playing the video from any point.
2. Click anywhere in the orange area of the timeline to move the red playback indicator and start the video from that point.
3. Hovering over the playback indicator displays the current time, as shown in **Figure 13.27** on the next page .

Figure 13.27 Current Time Displayed

Pause

When you click play, the video starts and the button changes to pause. Clicking it again pauses the video.

Stop

Click the stop button and the playing video will be stopped and the time indicator will be back to the starting time of the video.

Full Screen

1. Click the **full screen** button at the bottom of the page to play the right window in full screen, as shown in **Figure 13.28** on the facing page .

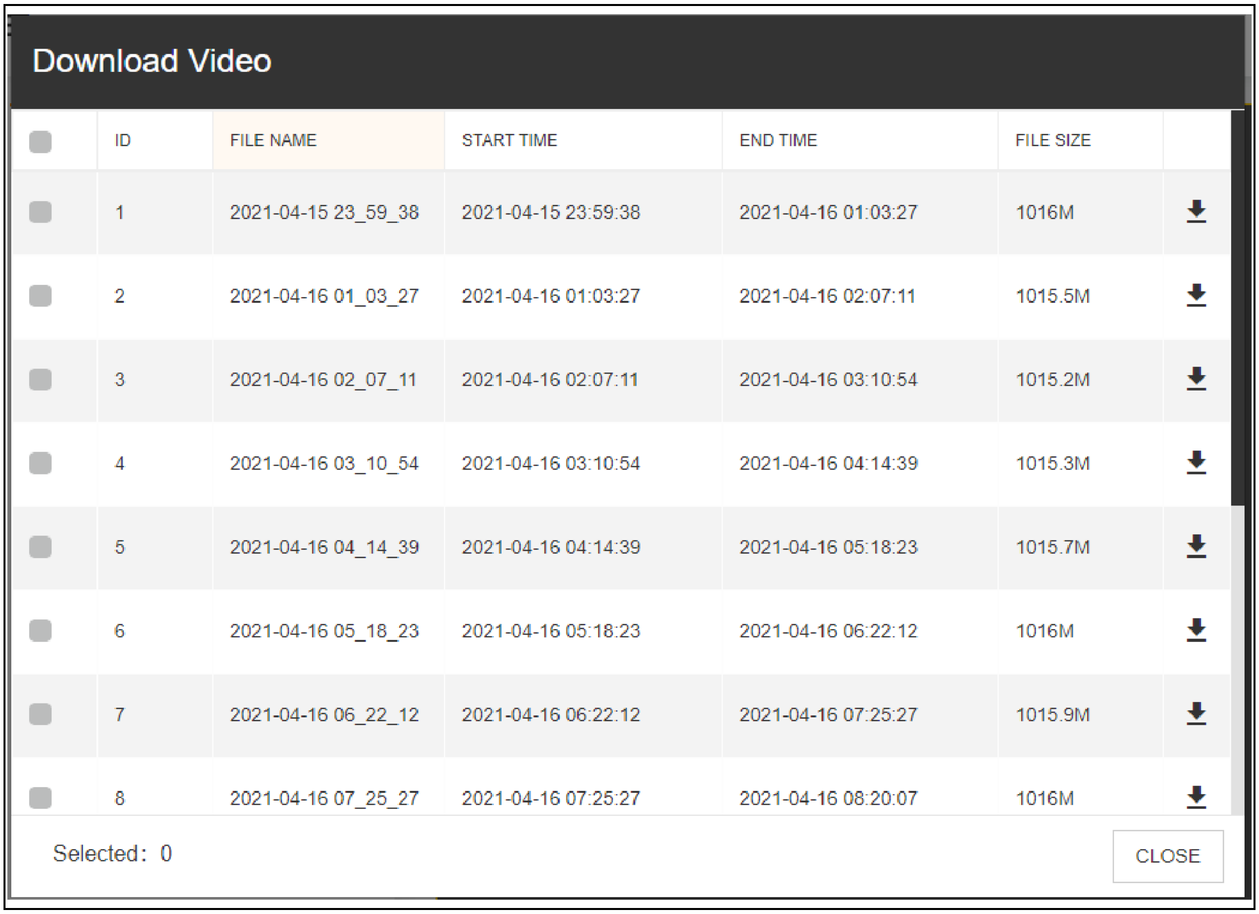
Figure 13.28 Historical Video—Full Screen

2. After the full screen display, press the *Esc* key to exit the full screen mode.

Downloading the History Videos

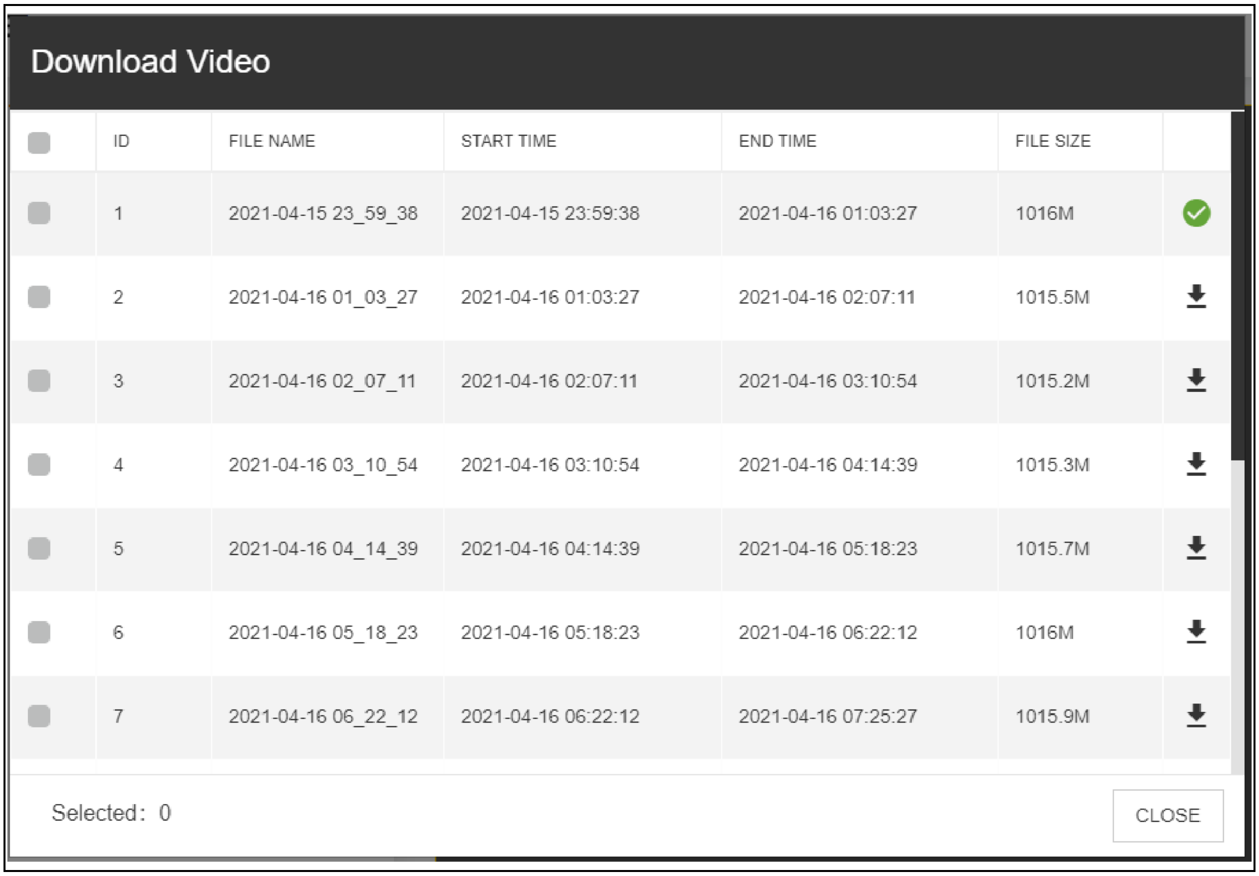
1. When you select a date or click on an IPC device in the list, the Download Video button becomes active if historical videos are available for that period. Downloaded videos are saved to your computer.
2. Click the Download Video button to open the historical videos download page, as shown **Figure 13.29** on the next page .

Figure 13.29 Download Video Popup Window



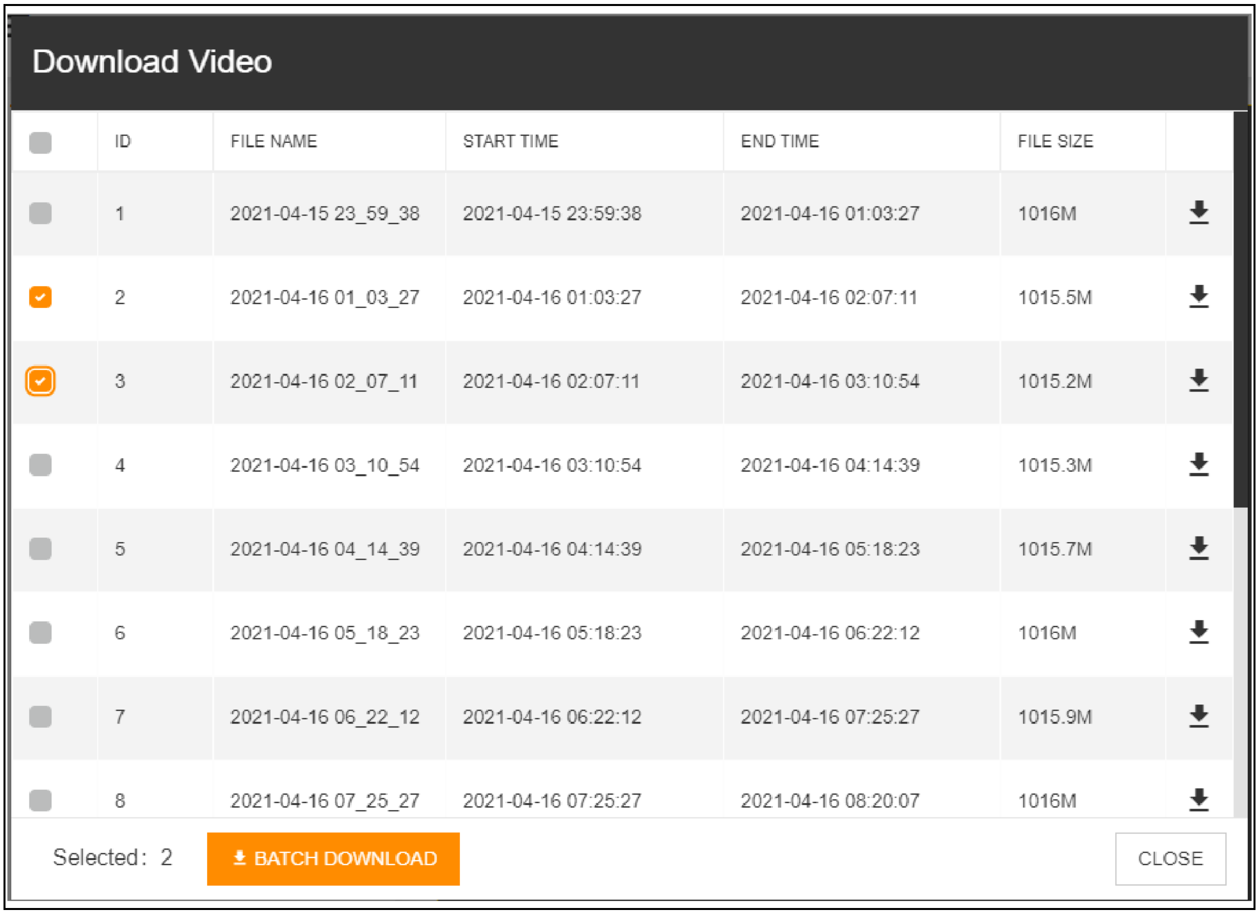
3. On the download video popup, click the download button in the last column of the video file. This will initiate the browser's download function, as shown in **Figure 13.30** on the facing page .

Figure 13.30 Downloading Historical Video



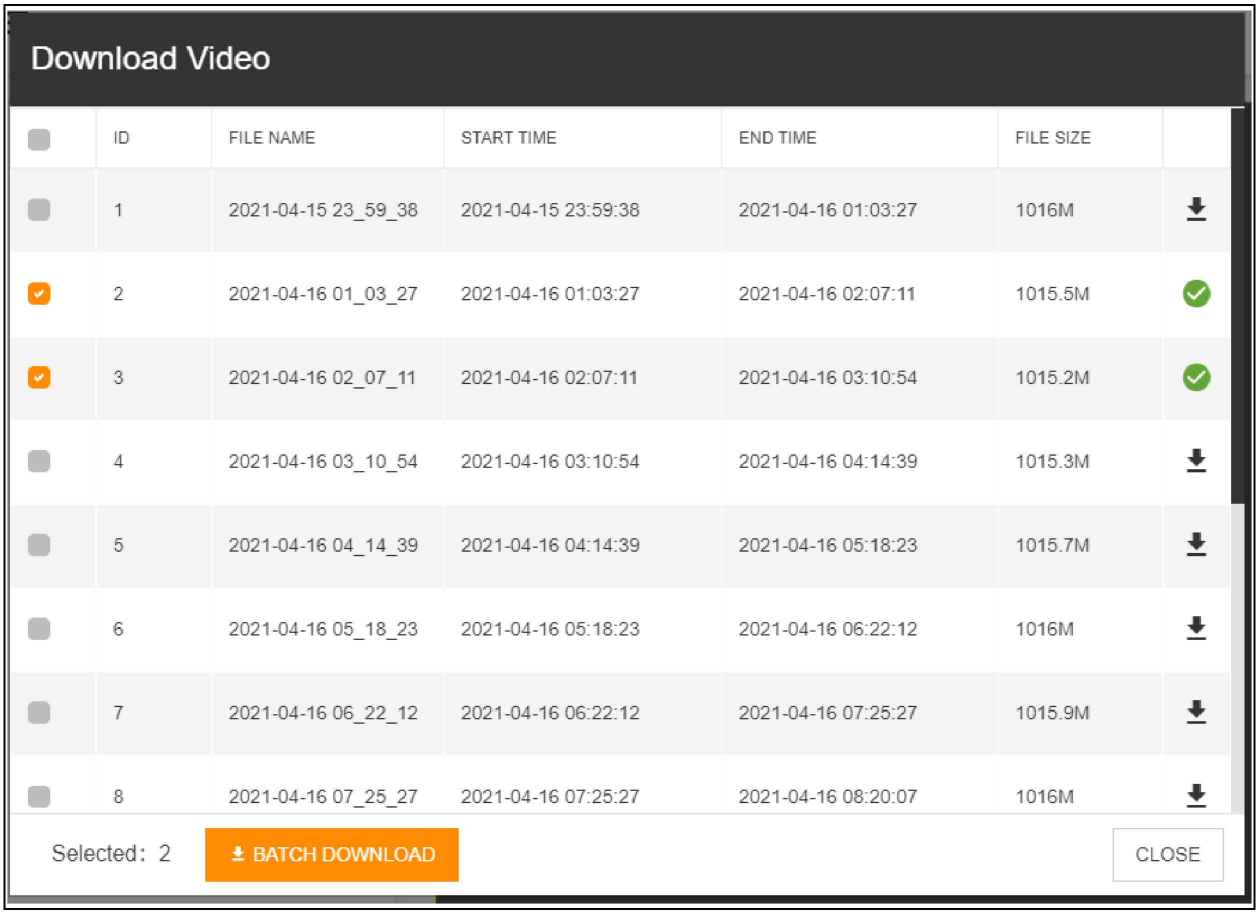
4. You can check the download progress of the file on the download page of the browser.
5. When two or more video files are selected, the batch download button will automatically appear at the bottom of the page, as shown in **Figure 13.31** on the next page .

Figure 13.31 Download Historical Video Popup Window



6. When you click the *batch download* button. The browser will automatically download these video files in turn, as shown in **Figure 13.32** on the facing page .

Figure 13.32 Downloading the Historical Video in Batches



NOTE: 1. Downloading historical videos consumes lots of memory, so avoid downloading many large video files at once.

2. If a prompt appears when batch downloading files, click ***Confirm*** to begin downloading multiple files simultaneously.

This page intentionally left blank

14 Energy Consumption

14.1 General

14.1.1 Overview

The energy consumption module consists of two main components: energy consumption configuration and PUE configuration. The energy consumption configuration calculates the total energy usage for specific combinations of devices, such as for a particular site. PUE (Power Usage Effectiveness) is defined as the ratio of total data center energy consumption to IT equipment energy consumption. This total includes energy used by IT equipment as well as cooling and power distribution systems. PUE values are always above 1, with values closer to 1 indicating higher energy efficiency in the data center due to lower non-IT equipment energy consumption. The PUE configuration can be calculated using various modes, including energy mode, power mode and data retrieval from RDU mode.

14.1.2 Functional Modules

The energy consumption includes the following functional modules, refer to this manual for detailed information about each functional module in Detailed Features on page 287.

- Energy Consumption Configuration
- PUE Configuration

14.2 Quick Start

14.2.1 Rapid Deployment Steps

To set up energy consumption quickly:

1. Navigate to Energy Management.
2. Select Energy Consumption Configuration.
3. Click the Add icon.
4. Add device signals and configure the adjustment value. Optionally, associate the configuration with a site.
5. Save your configuration.

To configure PUE quickly:

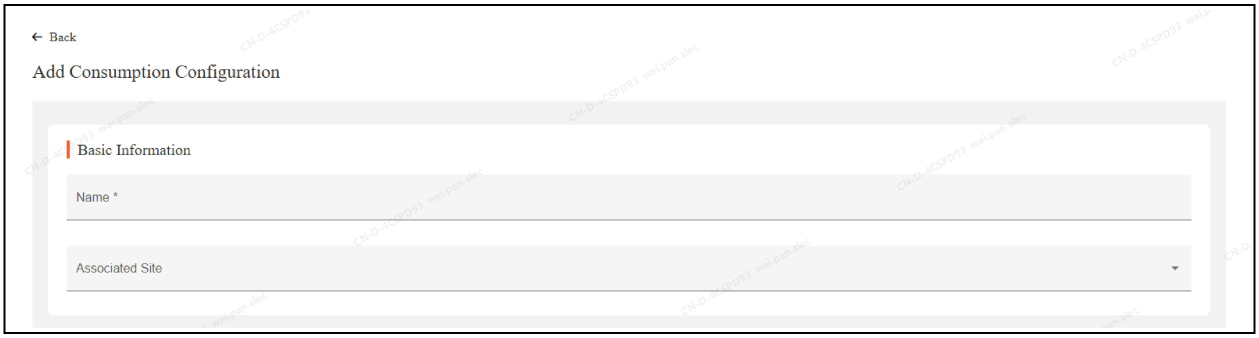
1. Navigate to Energy Management.
2. Select PUE Configuration.
3. Click the Add icon.
4. Select the calculation mode and method.
5. Add device signals (optional) and save.

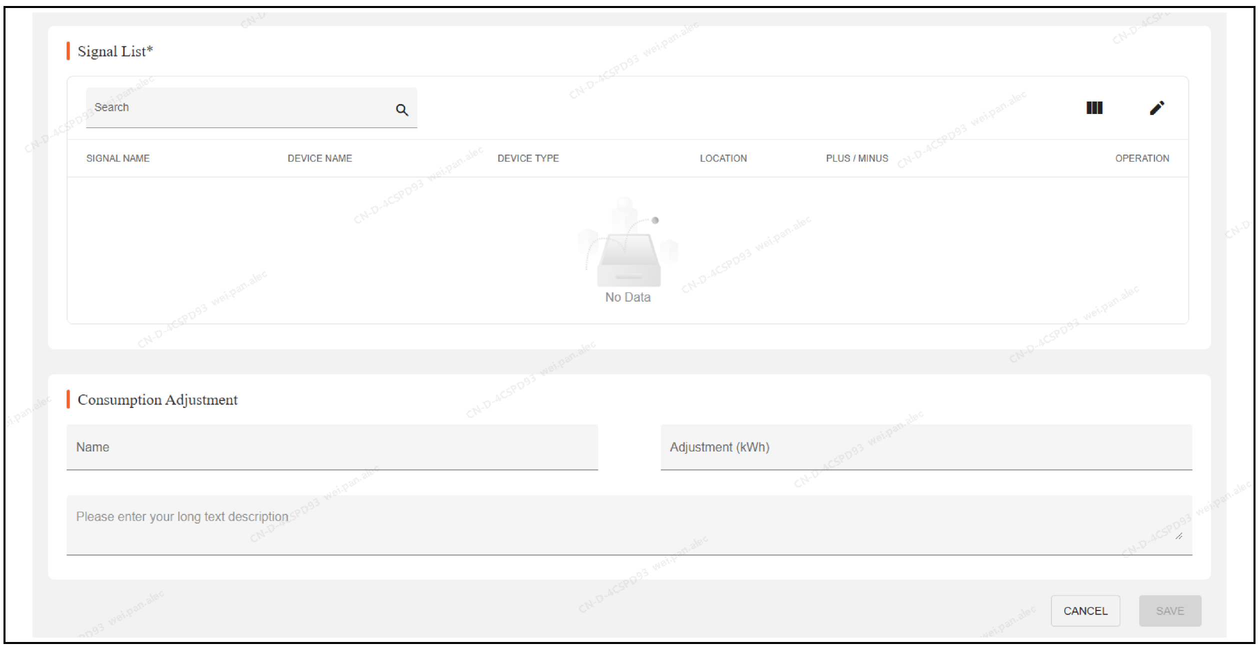
14.2.2 Example

Adding an Energy Consumption Configuration

In the Smart InfraSight™ home page, select and click the *Add* icon in the upper right corner to enter the new energy consumption configuration page, enter a name and select the associated site and configure the adjustment value, as shown in **Figure 14.1** below .

Figure 14.1 Adding an Energy Consumption Configuration

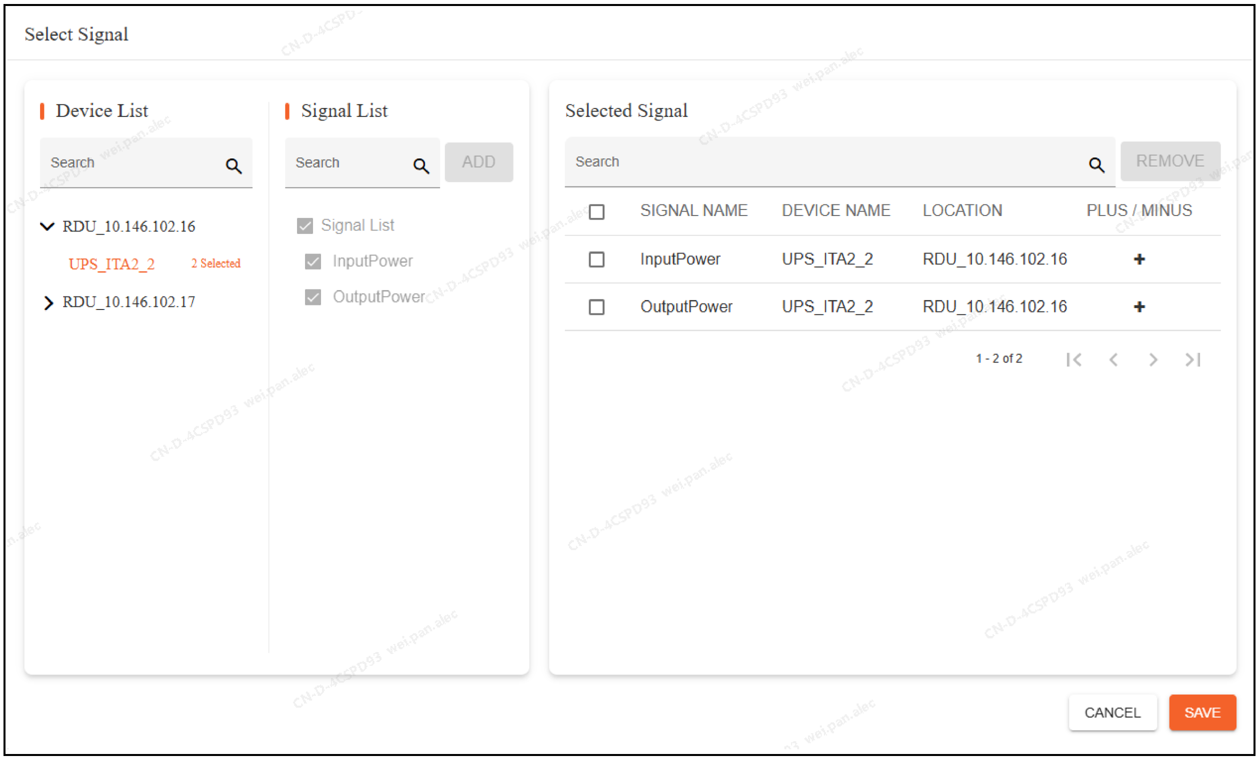




Click on the *list* of signals to add a device signal.

After that, click *Save* to complete the energy consumption configuration, **Figure 14.2** on the facing page . Enable the energy consumption configuration.

Figure 14.2 Selecting the Energy Consumption Calculating Signal

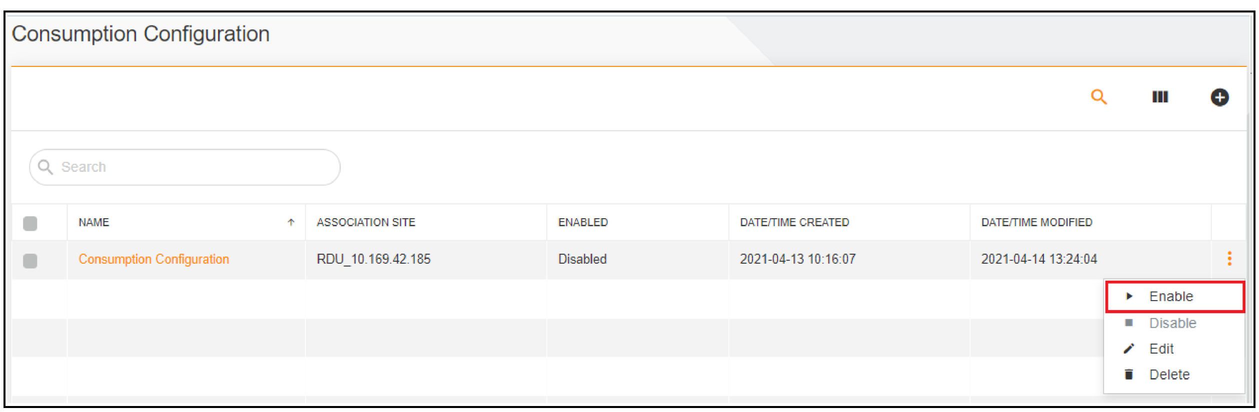


Click on the energy consumption configuration list, and then click *Enable*.

Enabling the Energy Consumption Configuration

Click on the energy consumption configuration list, and then click on the *ellipses*, and then click *Enable*, as shown in **Figure 14.3** below .

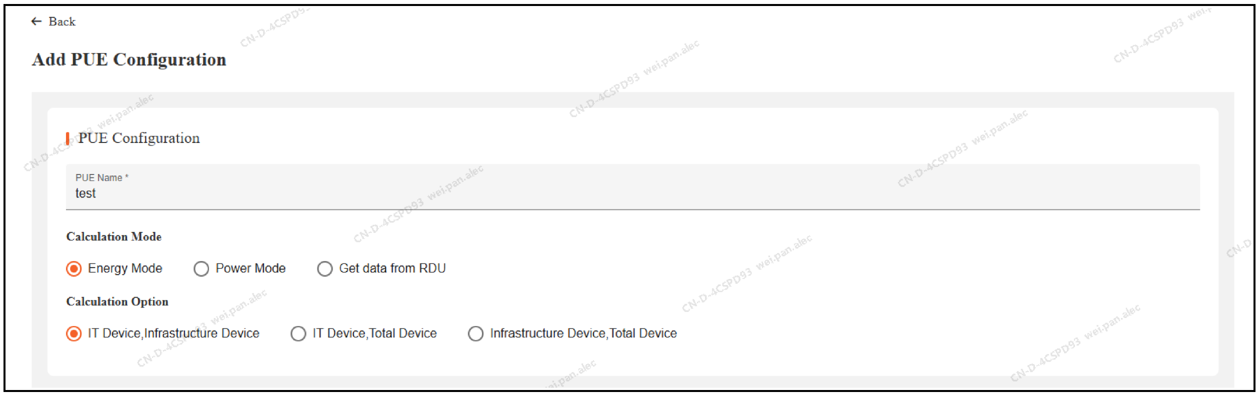
Figure 14.3 Enabling the Energy Consumption Configuration



Adding a PUE Configuration

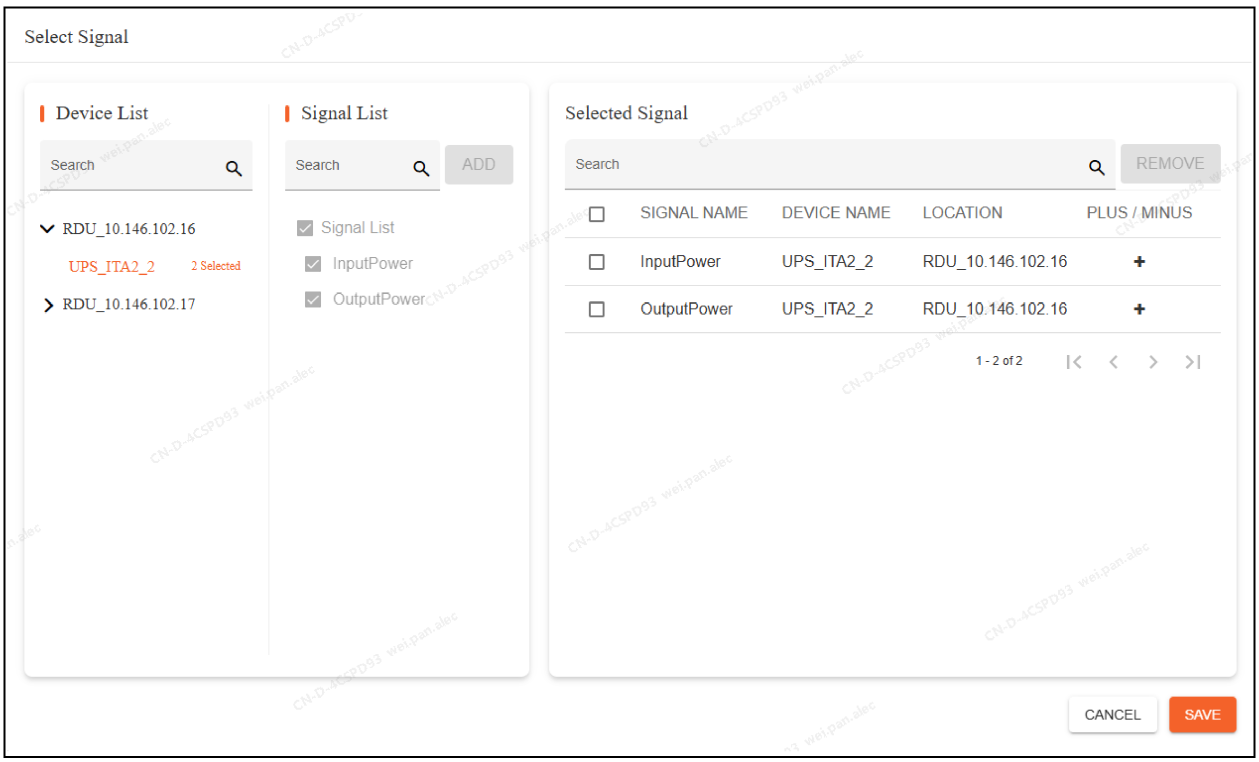
Navigate to PUE Configuration, then click the *Add* icon in the upper right corner to enter the Add PUE Configuration, as shown in **Figure 14.4** on the next page .

Figure 14.4 Adding a PUE Configuration



After configuring the PUE name, calculation mode, and calculation method, as shown in **Figure 14.5** below , click *save* to select the PUE configuration signal (There's no need to configure the signal for **Get data from RDU mode**).

Figure 14.5 PUE Configuration— Selecting the IT Device Energy Consumption Signals



For example, select the IT equipment and infrastructure equipment, enter the calculation adjustment value (optional), and click *Save* to complete the PUE configuration.

14.3 Detailed Features

14.3.1 Energy Consumption Configuration

Adding an Energy Consumption Configuration

Navigate to Energy Consumption Configuration and click the *Add* icon in the upper right corner to enter the Add Energy Configuration page, as shown in Figure 14.6 below .

Figure 14.6 Add Energy Consumption Configuration

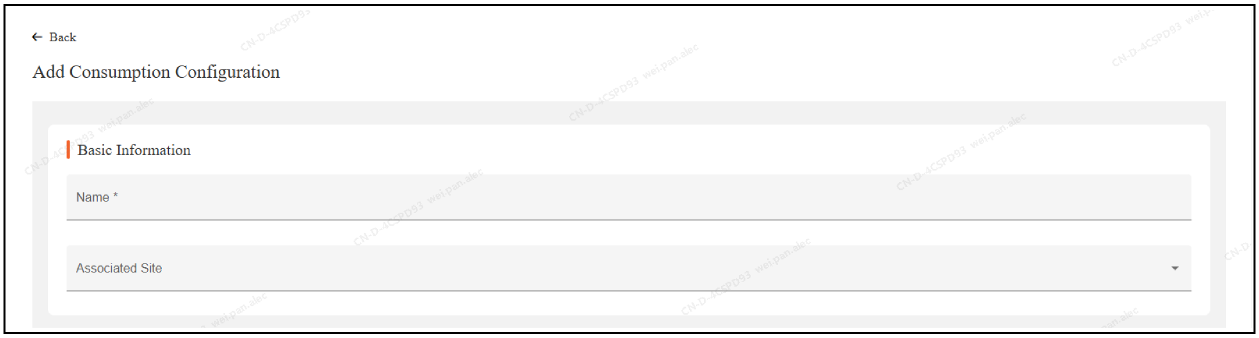
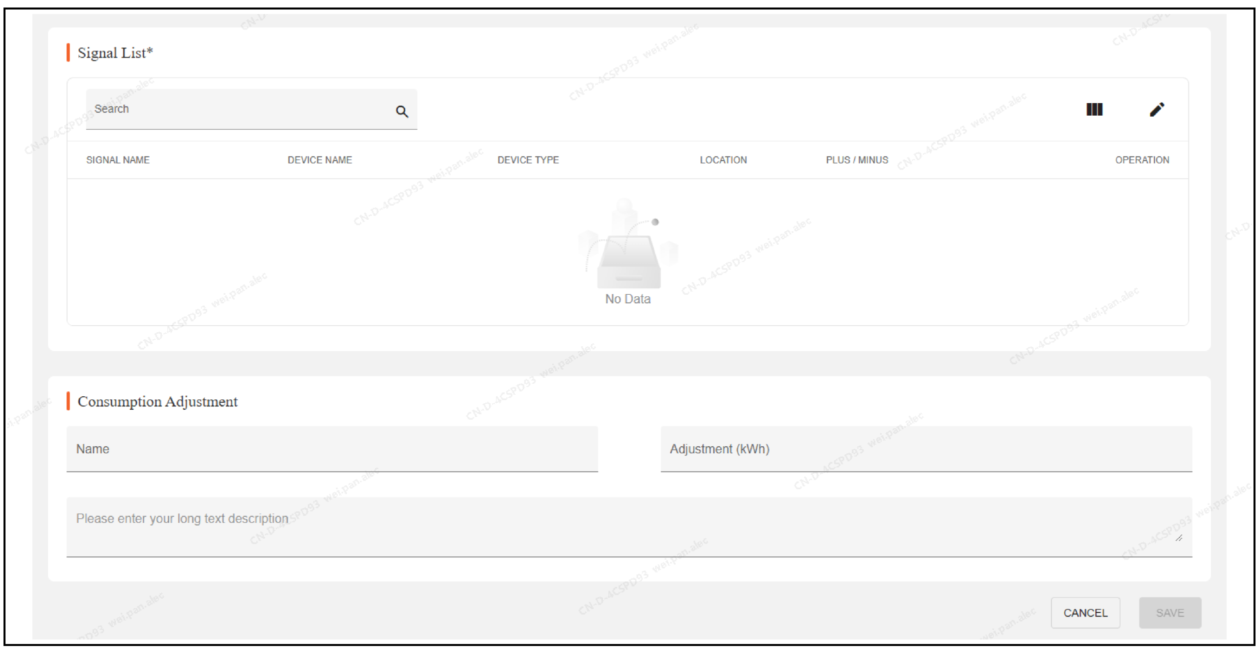


Figure 14.7 Energy Consumption Configuration Added



Enter the energy consumption configuration name and click Edit in the upper right corner of the signal list. Select the device signals you want to use for calculating energy consumption. The formula is:

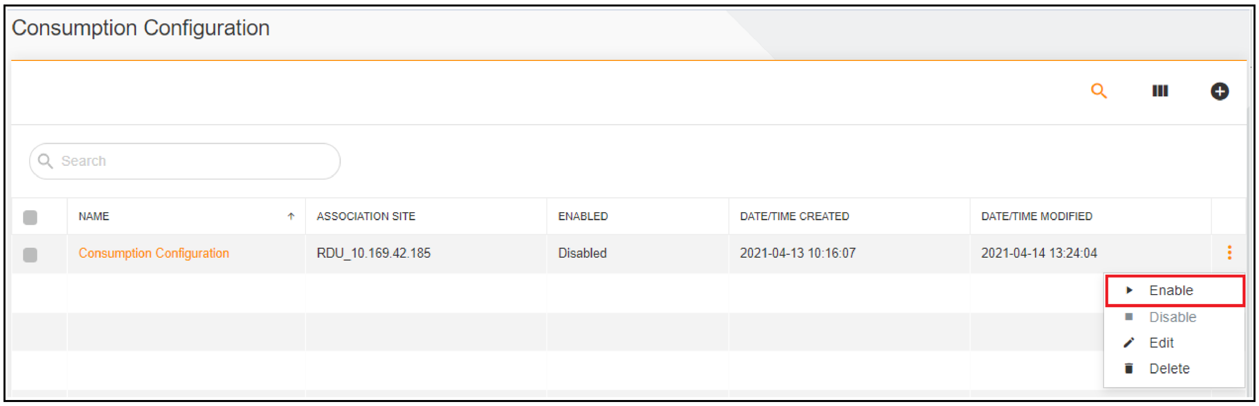
Energy consumption = [Signals marked (+)] - [Signals marked (-)] + Adjustment value

The adjustment value can be flexibly configured based on actual conditions. Once the configuration is complete, you can associate it with a specific site. The calculated result will represent that site's energy consumption. For example, an energy consumption bar chart widget will automatically display the result for the associated site.

Enabling/disabling the Energy Consumption Configuration:

Once energy consumption configuration is enabled, the system calculates and saves the results hourly. To enable or disable this feature, click the ellipsis (...) in the energy consumption configuration list, as shown in **Figure 14.8** below .

Figure 14.8 Enabling/disabling the Energy Consumption Configuration

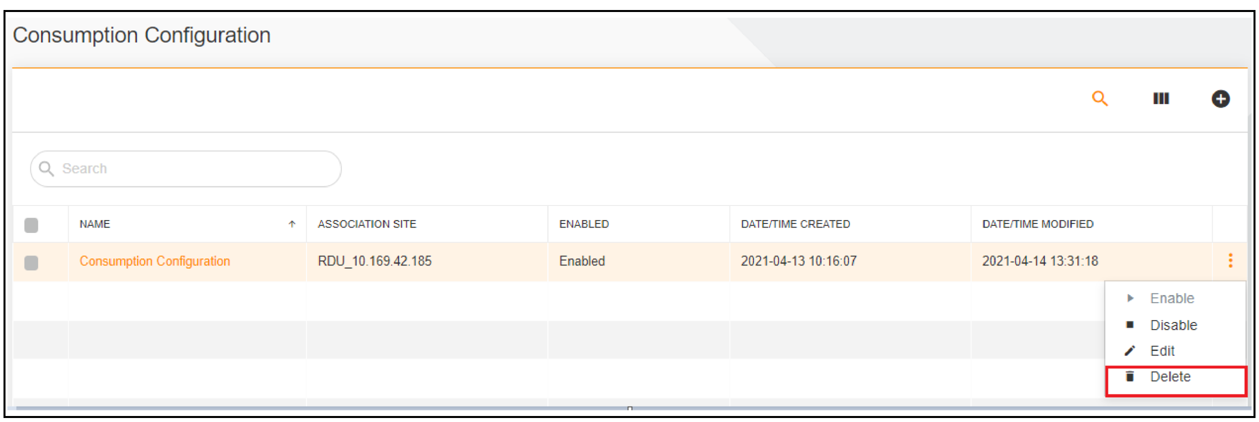


Editing the Energy Consumption Configuration

Click on the *ellipses* for the energy consumption configuration list, and then click *Edit*.

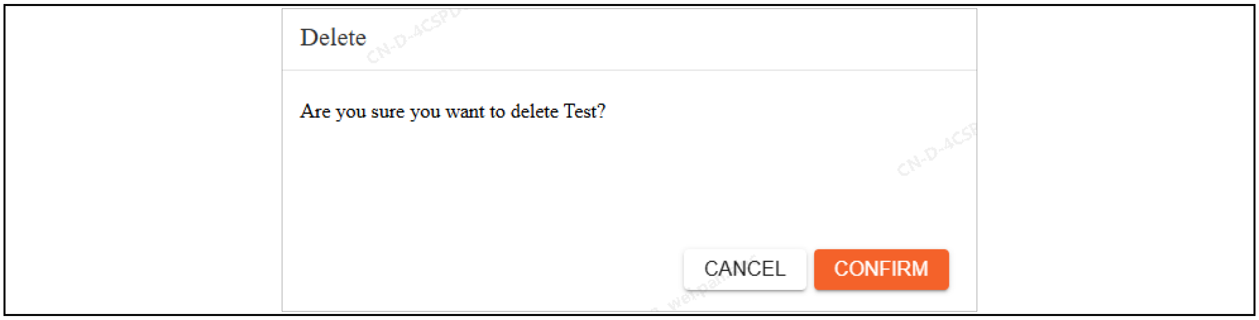
Deleting the Energy Consumption Configuration

Figure 14.9 Deleting the Energy Consumption Configuration



Click on the energy consumption configuration list, and then click *ellipsis* to enter the energy consumption configurations page, click *Delete* and then *Confirm* to delete, as shown in **Figure 14.10** on the facing page .

Figure 14.10 Delete Confirmation Window

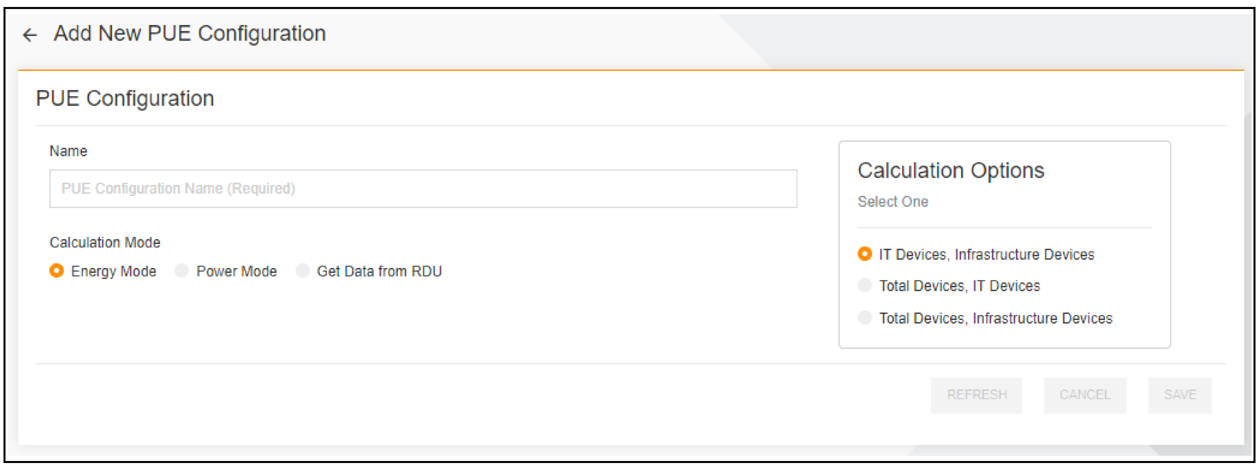


14.3.2 PUE Configuration

Adding a PUE Configuration

Navigate to the PUE Configuration and click the *Add* icon in the upper right corner to enter the Add PUE Configuration page, as shown in **Figure 14.11** below .

Figure 14.11 Adding PUE Configuration



You can choose from 3 PUE modes:

1. **Energy Consumption Mode**: The PUE value is calculated daily at 01:00 based on the previous day's power consumption (kWh). Once saved, it represents yesterday's energy PUE. Calculation example: If IT equipment consumed 20 kWh yesterday and 10 kWh the day before, while total consumption was 50 kWh yesterday and 30 kWh the day before, then PUE = (50-30)/(20-10) = 2.0.

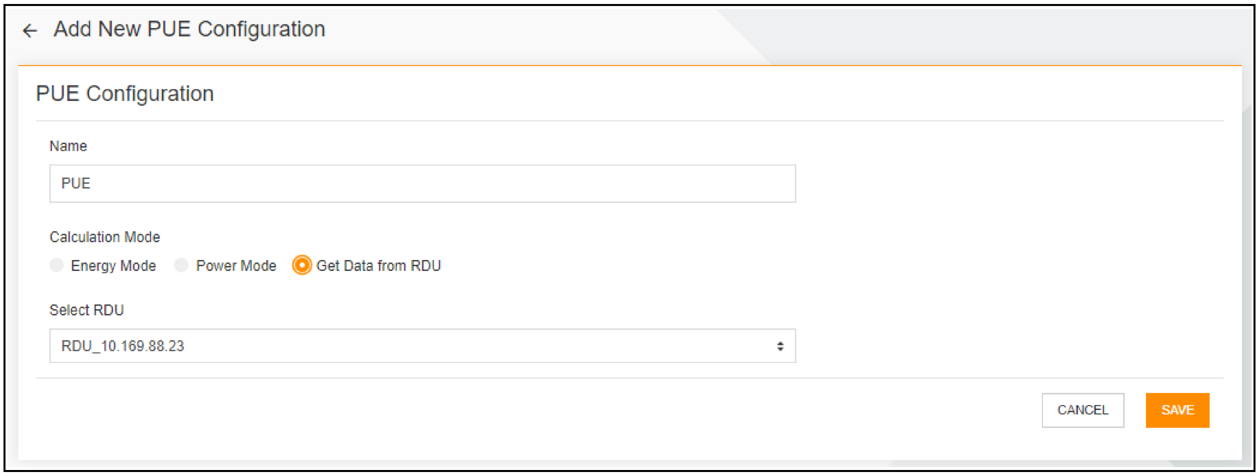
2. **Power Mode**: The PUE value is calculated every 30 seconds based on real-time equipment power (kW). The calculated value is stored hourly. Calculation method is similar to Energy Consumption Mode.

3. **Get data from RDU Mode**: If the selected RDU501 is PUE-configured, the system directly obtains the PUE mode and calculated value from the RDU. The saving strategy and widget display style are determined by the RDU501's PUE calculation mode:

- If RDU501 uses Power Mode: Data is obtained every 30 seconds, and the PUE widget displays as in SI Power Mode.

- If RDU uses Energy Consumption Mode: PUE value is saved hourly, the widget displays as in SI Power Mode, but shows **Energy Consumption Mode**. As shown in **Figure 14.12** below .

Figure 14.12 Getting Data from RDU



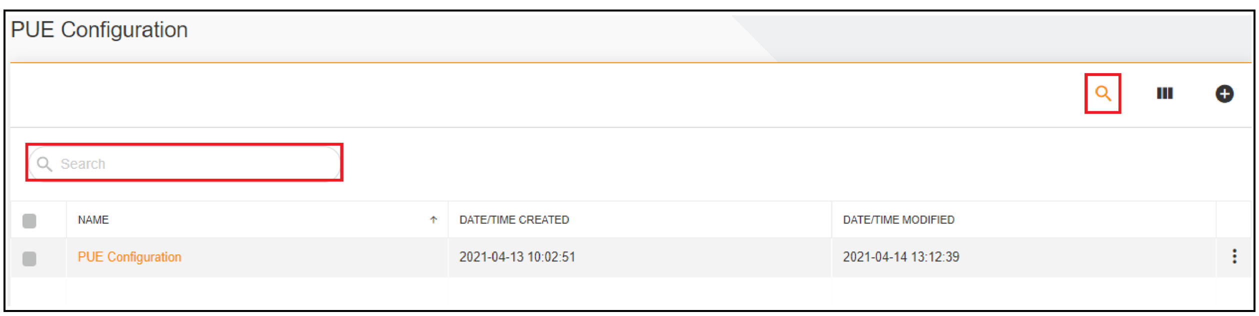
NOTE: To obtain data from RDUs, you need to complete user authentication for RDUs in advance. The path is: Monitoring > Monitoring Tree > Find the site related to the specified RDU501 > Click ellipses(...) and select User Authentication.

After saving the mode selection, if you Energy Mode, you need to select the energy signals(kwh) of the device participating in the PUE calculation. If you select Power Mode, you need to select the power signals(kw).

Searching for the PUE configuration

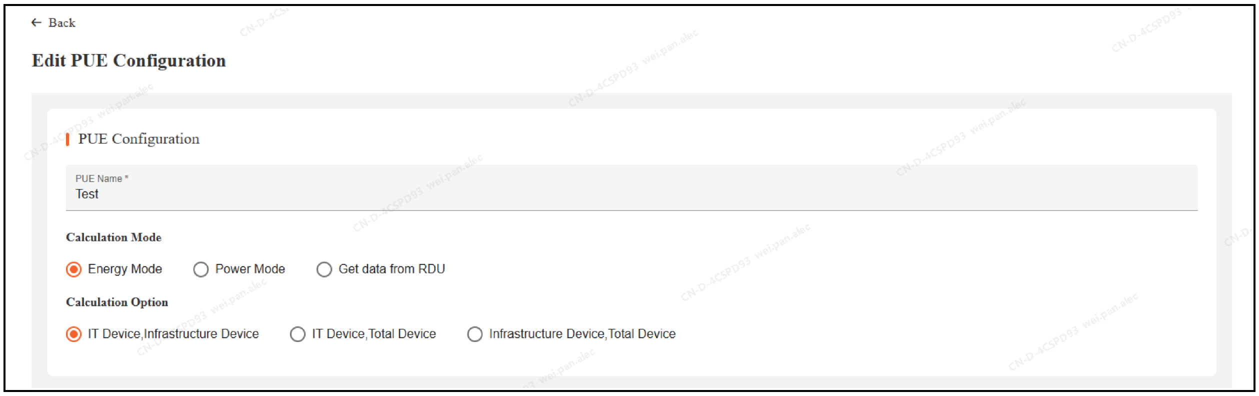
Enter a search keyword in the input box to search, **Figure 14.13** below .

Figure 14.13 Searching for the PUE configuration



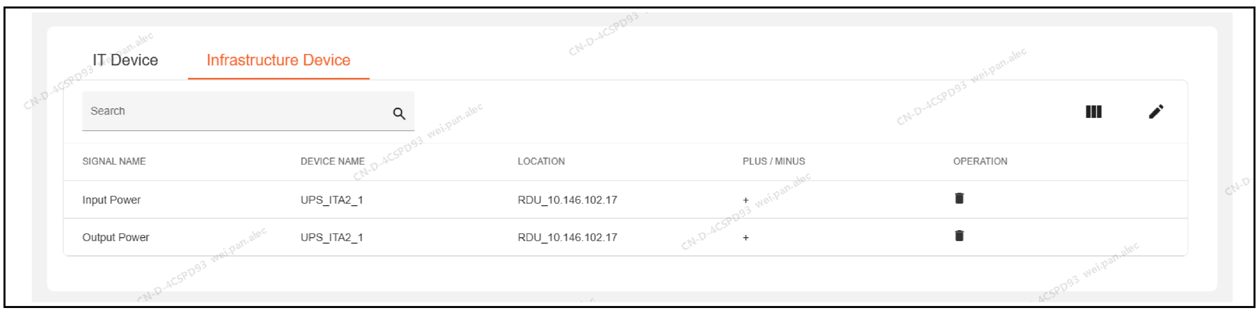
Click on the *ellipses* for the energy consumption configuration list, and then click *edit* to enter the Edit PUE configuration page, you can change the calculation mode, calculation method, and signal for calculating PUE in energy consumption mode and power mode (changing the calculation mode will empty the PUE data calculated by the previous mode).

Figure 14.14 Editing the PUE Configuration



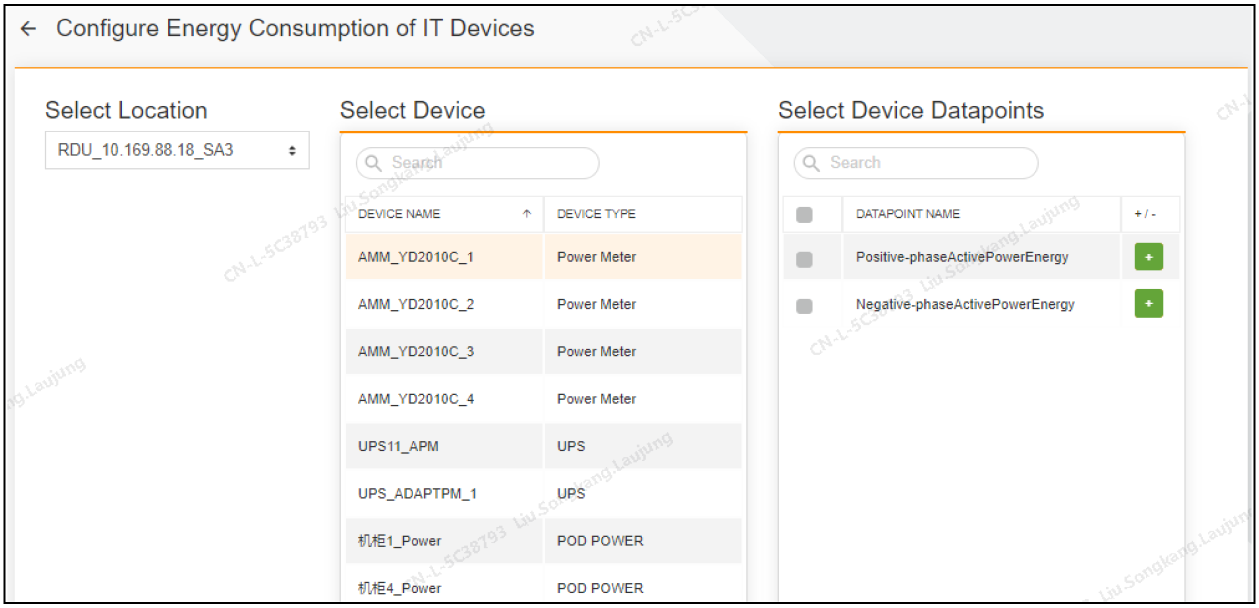
Click on the *edit* icon on the upper right corner of the IT device table to edit signals used to calculate IT devices' energy consumption, as shown in Figure 14.15 below .

Figure 14.15 Configure the Energy Consumption of IT equipment



To calculate the PUE value, select the appropriate signals based on your chosen calculation method. These signals should represent the energy consumption of IT equipment, infrastructure equipment, and all devices combined. Refer to Figure 14.16 on the next page , for a visual representation of this process.

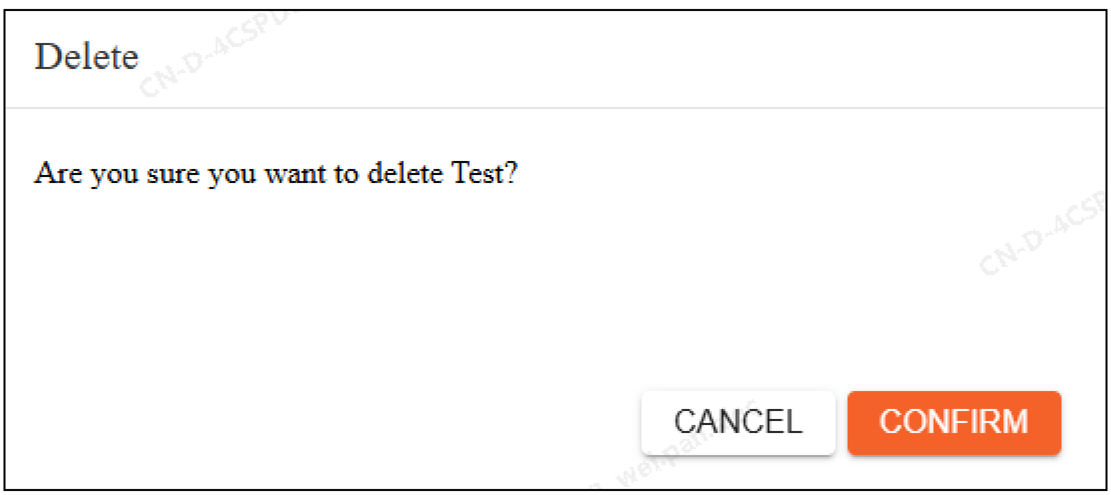
Figure 14.16 Configuring the Energy Consumption of IT Equipment



Deleting the PUE Configuration

Click on the PUE configuration list, and then click *Delete* to delete the PUE configuration. Then confirm the deletion operation, as shown in **Figure 14.17** below .

Figure 14.17 Deletion Confirmation Popup



15 Configuration Tool

15.1 General

15.1.1 Overview

The configuration tool is the core function of the entire Smart InfraSight™ platform, used to monitor and present data. It is also the first function that users interact with. Users can search for SNMP devices or RDUs in the configuration module and add them to monitoring, enabling the underlying data to be officially connected to the Smart InfraSight™ platform, enabling the platform to display and monitor the data normally. The Smart InfraSight™ platform displays a collection of SNMP devices, Smart Aisle (SA2 and SA3), Smart Cabinet2, and Smart Row2, in the structure of a site tree.

SNMP devices are automatically classified into the Default Site after being monitored through communication configuration and device drivers. The monitored devices can edit their own information and configure the key parameters of various collected signals (signals, alarms, control, and settings).

In the RDU configuration, you can customize the multi-dimensional regional structure according to the user's actual geographic deployment, and associate it with the corresponding RDU that is added to the monitoring. The configuration also allows users to synchronize the underlying RDU configuration, jump to the RDU page, customize the list of devices to be monitored under the RDU, configure device storage policies, and configure key parameters of various collected signals (signals, alarms, control, and settings).

15.1.2 Functional Modules

The configuration of Smart InfraSight™ includes the following function modules, and please refer to this manual for details of each function module RDU Detailed Features on page 296.

- Device management
- Comm Profile
- Device Driver

15.1.3 Rapid Deployment Steps

Deploy SNMP

To ensure that SNMP devices can be searched and added to monitoring, perform the following steps:

1. Add Comm Profile (if it hasn't been added already)
2. Add a device driver (if it hasn't been added already)
3. SNMP devices can be added at a single point or in bulk
4. Note for self: Check

Confirm this

To ensure that RDUs can be searched for and added to monitoring, perform the following steps:

1. Set search access permissions in RDU-A
2. RDU search and join monitoring
3. Edit area when adding monitoring (optional)

4. Equipment configuration (optional)

15.1.4 SNMP Device

Add a communication configuration

Before adding an SNMP instance, make sure the corresponding Comm Profile and Device Driver are already in place. If they aren't, add them first. Please refer to the sub-section, see Detailed Functions for more details.

Add a Comm Profile

Click the Plus sign on the Comm Profile page of the configuration tool to add the communication configuration.

Add a Device Driver

Click the *Plus* sign on the device driver interface of the configuration tool to upload and add a device driver.

SNMP search and add SNMP devices for monitoring

Single point of addition

Enter the IP Address, select the Comm Profile and device driver. Then click on **Add Driver** to add the driver.

Bulk Addition

Enter the Starting IP address and Ending IP address, set the number of retries, timeout period, and Comm Profile to search, and add devices in batches after the search is completed.

Device configuration (optional)

If the initial settings of the device do not meet the actual requirements, you can modify the device configuration. Please refer to the for the SNMP Detailed Function specific operation details 316516.0.-1666288320 of device management.

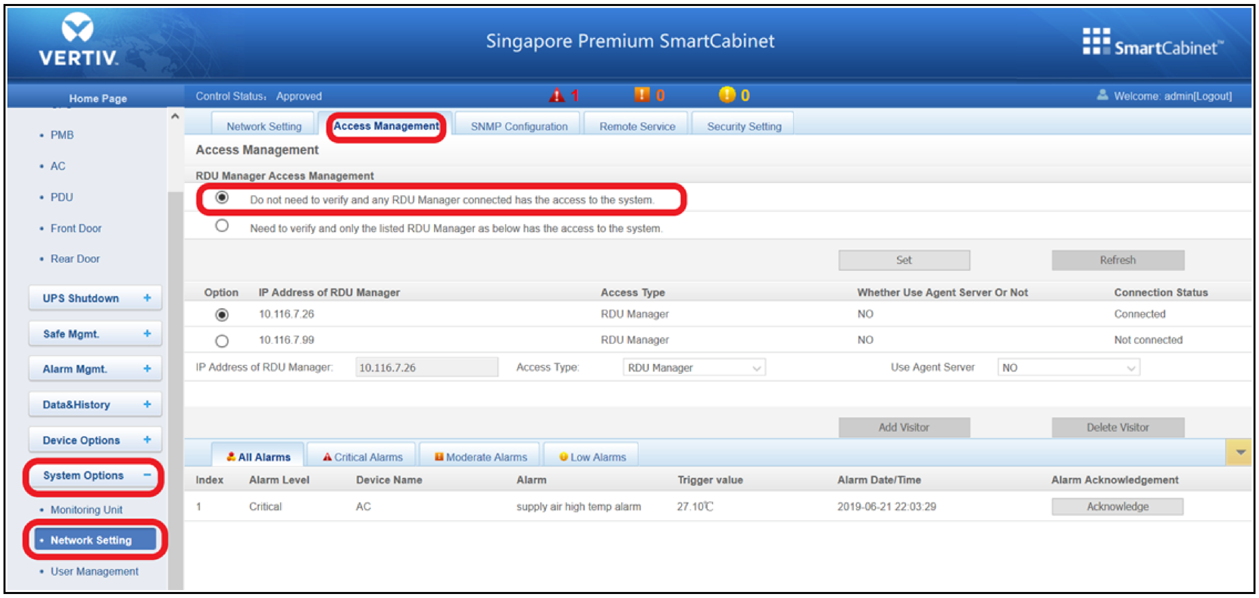
15.1.5 RDU Example

RDU-A

When searching for an RDU, you need to do some basic configuration in the RDU, that is, to allow Smart InfraSight™ to access the current RDU, which is mainly divided into two configurations:

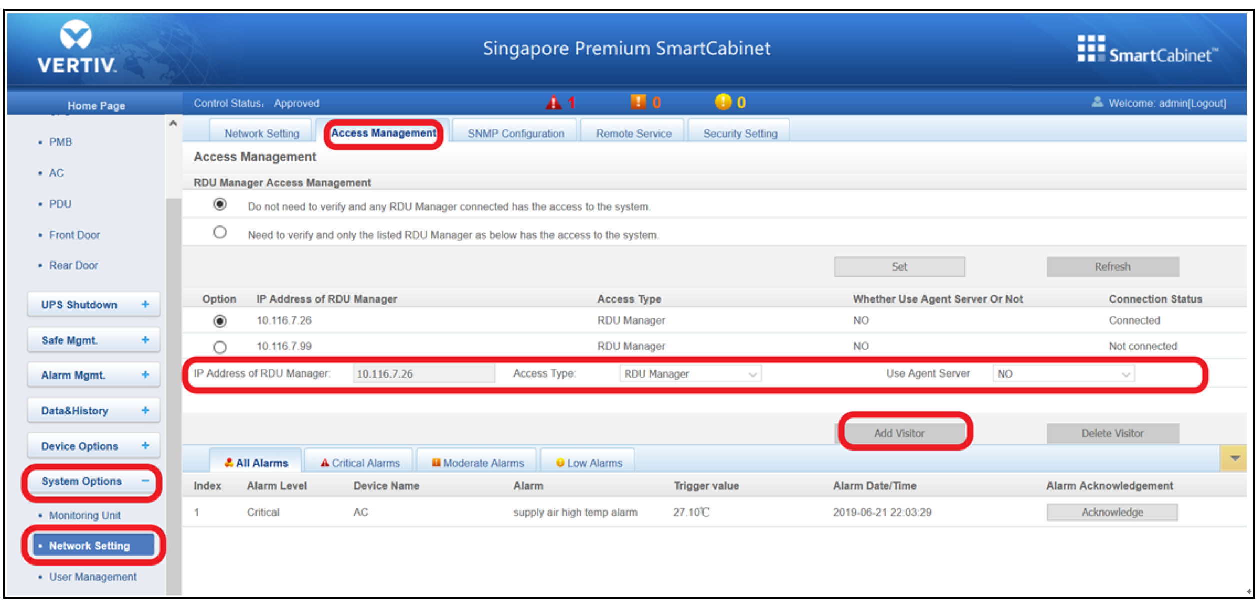
Configuration 1: Allow any Smart InfraSight™ to access the current RDU-A, as shown in **Figure 15.1** on the facing page .

Figure 15.1 Access to the Current RDU-A Configuration is Enabled



Configuration 2: You need to add the IP of the allowed Smart InfraSight™ as an allowed visitor in the RDU, as shown in **Figure 15.2** below .

Figure 15.2 Allowing Visitors IP Address



NOTE: If the pre-search configuration has been confirmed, but the RDU is still not found in Smart InfraSight™, it is possible that the RDU network is interrupted, check whether the network connection of the RDU is normal.

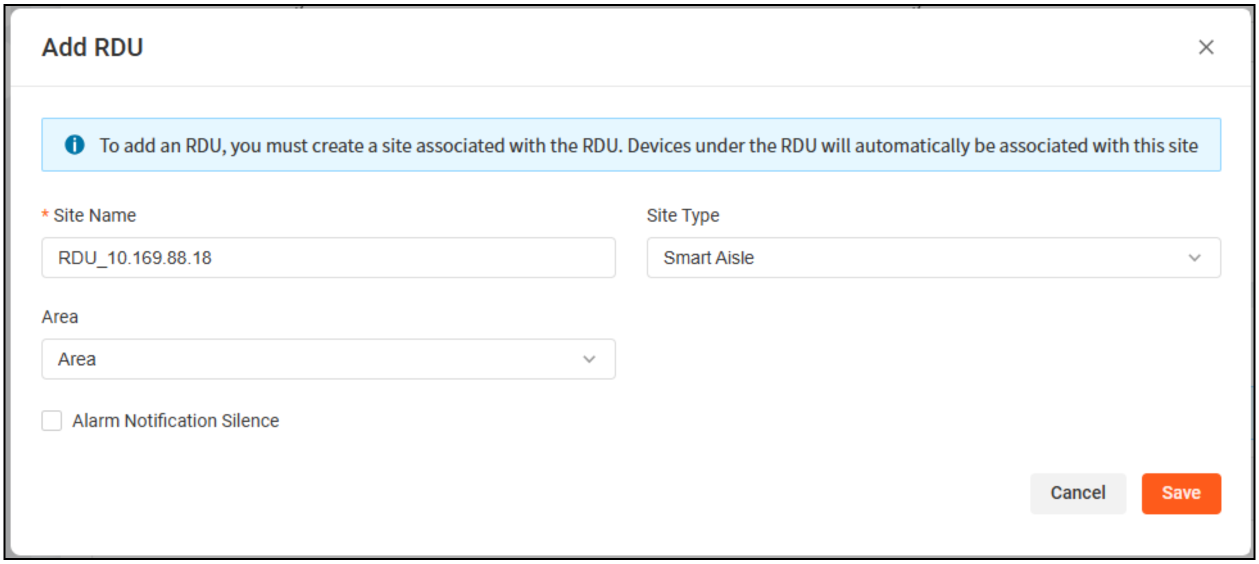
RDU Searching and on-boarding Monitoring:

After completing the above basic configuration work, the user can enter the corresponding IP in the search interface of the configuration tool to search for RDU, and after searching for RDU, you can click the save button of the current RDU region detail line to add it to the monitoring, please refer to the specific operation details in RDU Detailed Features on the next page.

Selecting the Location when Adding RDU Site

Take the searched 10.163.104.121 as an example, you can edit the region here, or you can use the default value as the region name:

Figure 15.3 Editing the Area



Device Configuration (Optional)

If the initial settings of the device do not meet the actual requirements, the user can modify the device configuration, and if the underlying layer of the RDU that has been added changes (some devices are added or removed), the latest RDU configuration can be synchronized through the Synchronize RDU configuration function in RDU Management under Device Configuration. Refer to the specific operation details Device Configuration on page 301.

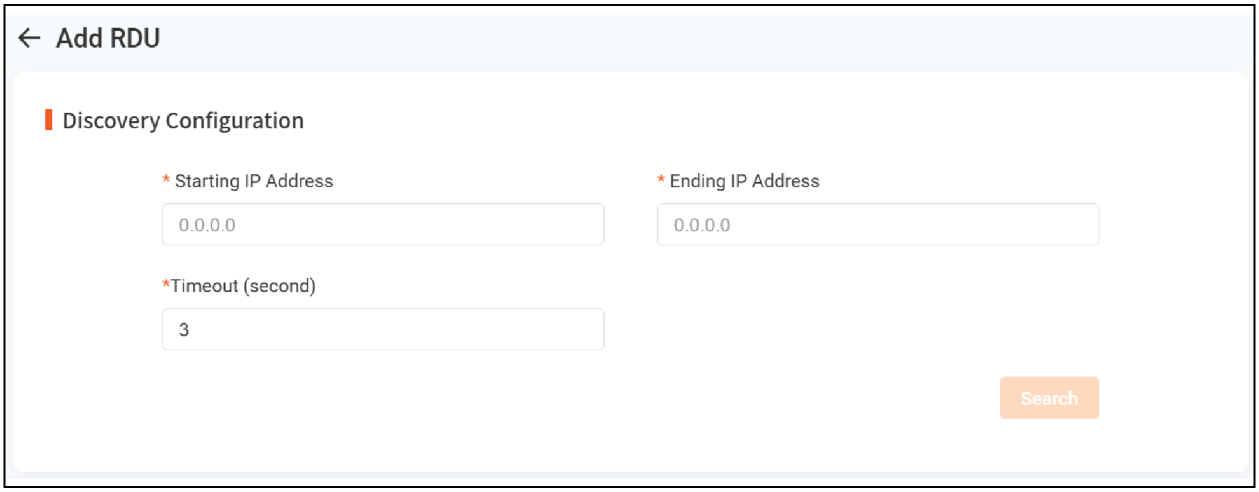
15.2 RDU Detailed Features

15.2.1 Device Management

Go to the Add RDU Page

Go to Configuration → Device Management → RDU Device. Click the '+' icon to add an RDU. The Add RDU screen will appear (See **Figure 15.4** on the facing page .)

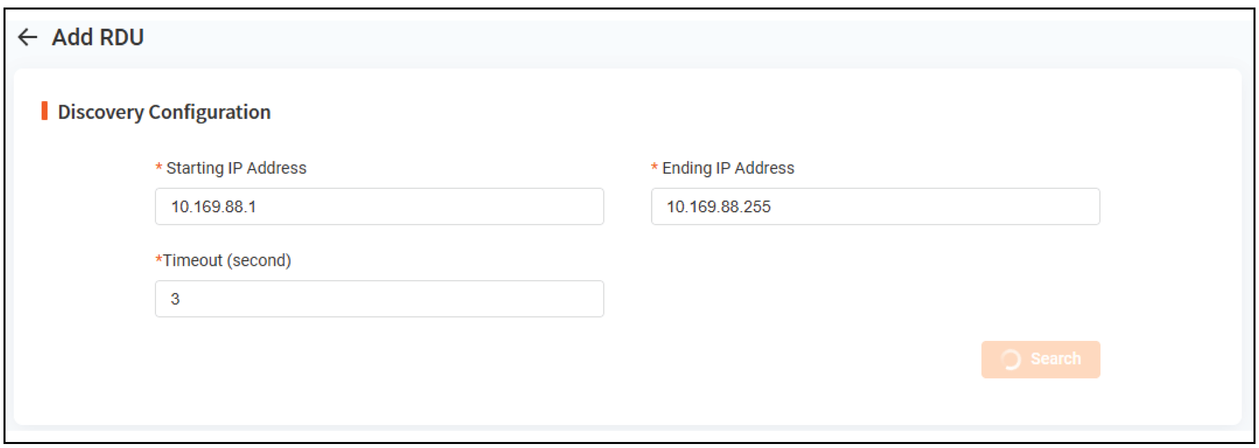
Figure 15.4 Add RDU Page



Search Function

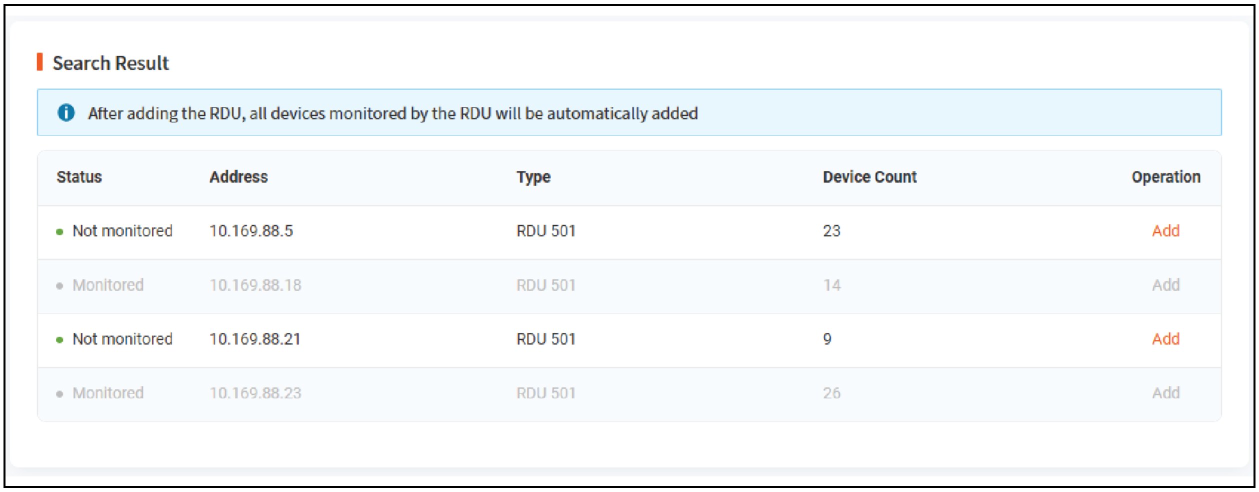
1. Enter the starting IP address, ending IP address, and timeout period, then click the Search button. The system will search for RDUs matching the specified criteria.
2. During the search process, the search button will be disabled, as shown in **Figure 15.5** below .

Figure 15.5 Searching the Device



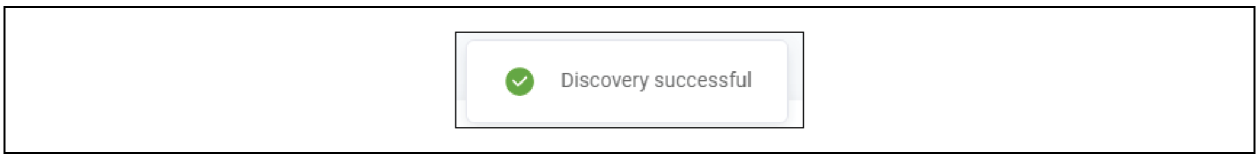
3. After the search is complete, a success message will appear (**Figure 15.7** on the next page)and the search results will be displayed at the bottom of the page, see **Figure 15.6** on the next page . The searched RDU has one of the two statuses: Not Monitored and Monitored. Monitored devices cannot be added again.

Figure 15.6 Search Results



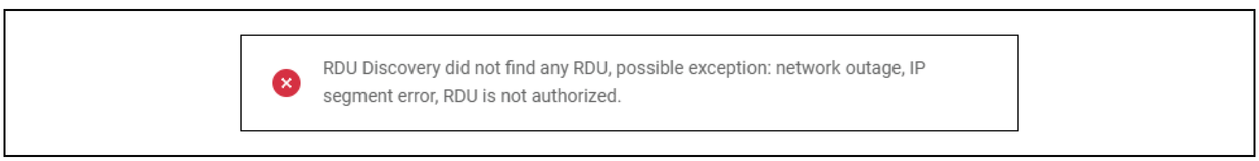
Status	Address	Type	Device Count	Operation
Not monitored	10.169.88.5	RDU 501	23	Add
Monitored	10.169.88.18	RDU 501	14	Add
Not monitored	10.169.88.21	RDU 501	9	Add
Monitored	10.169.88.23	RDU 501	26	Add

Figure 15.7 Success Message after the Search is Completed



If no device is found during the search, a message will be displayed with a description of the information, as shown in **Figure 15.8** below .

Figure 15.8 Message for No RDU Device found



NOTE: 1. The starting IP address must be less than the terminating IP, otherwise the search is not allowed.

2. The range of the starting IP address and the ending IP address cannot exceed 255, otherwise the search is not allowed.

3. When the Search button is clicked, it will be disabled. You must wait for the search to finish before clicking it again.

Timeout

The following **Figure 15.9** on the facing page shows the timeout period of the background setting request of the RDU IP field, which can be set by the user according to the client network conditions. The timeout range is 2-300 Second. It is set to 3 seconds by default.

Figure 15.9 Setting a Search Timeout

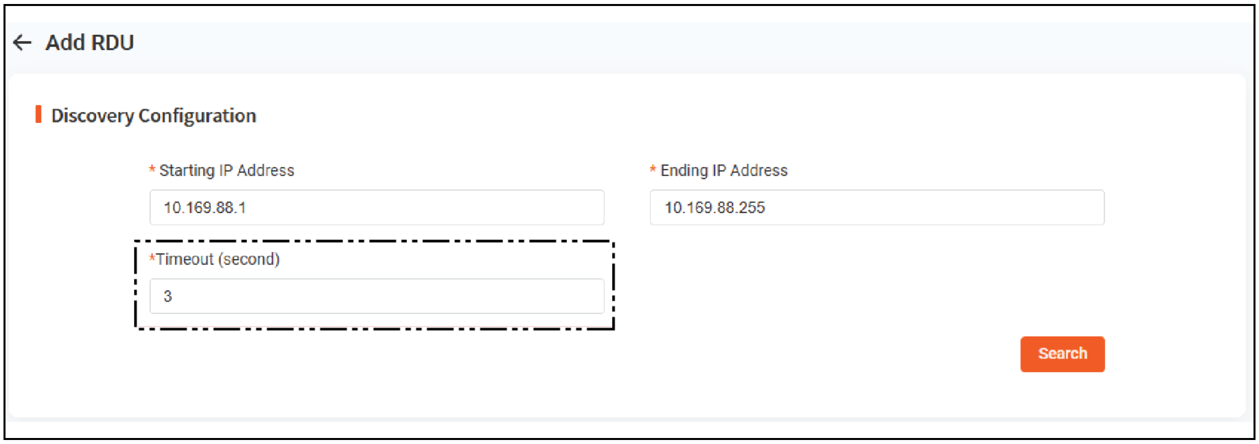
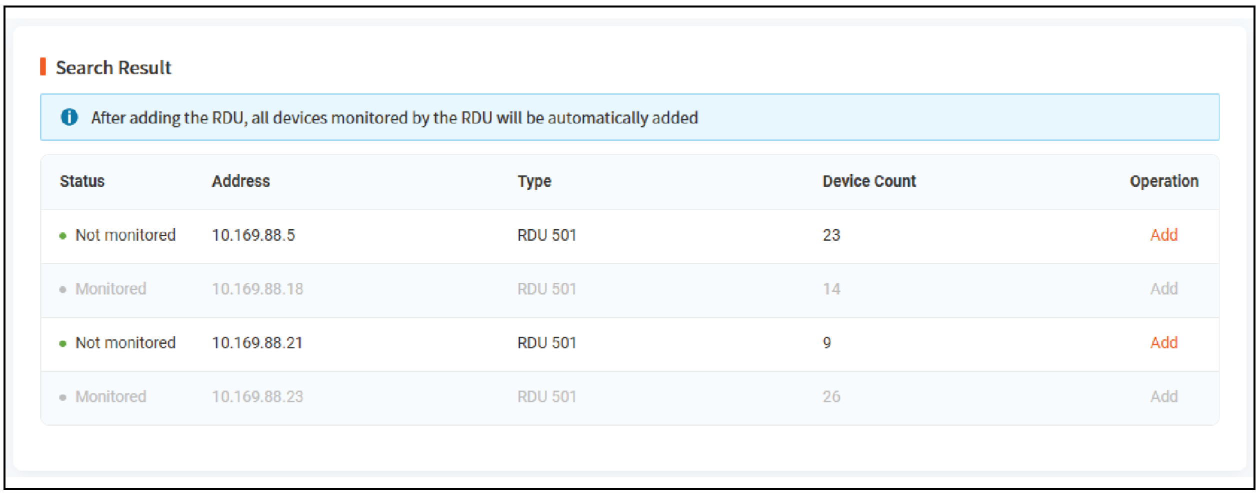


Figure 15.10 Detailed Search Result



Adding a Not Monitored RDU to Monitored

1. After searching for a 'Not Monitored' RDU, click Add under the Operation column to add it to monitoring. A pop-up will appear with the following fields: Site Name, Site Type, Location, and an option to select or deselect Alarm Notification Silence.

By default, the system will:

Set the Site Name to RDU + <RDU IP address>

Set the Site Type to Smart Aisle

Set the Region Name to Default Region

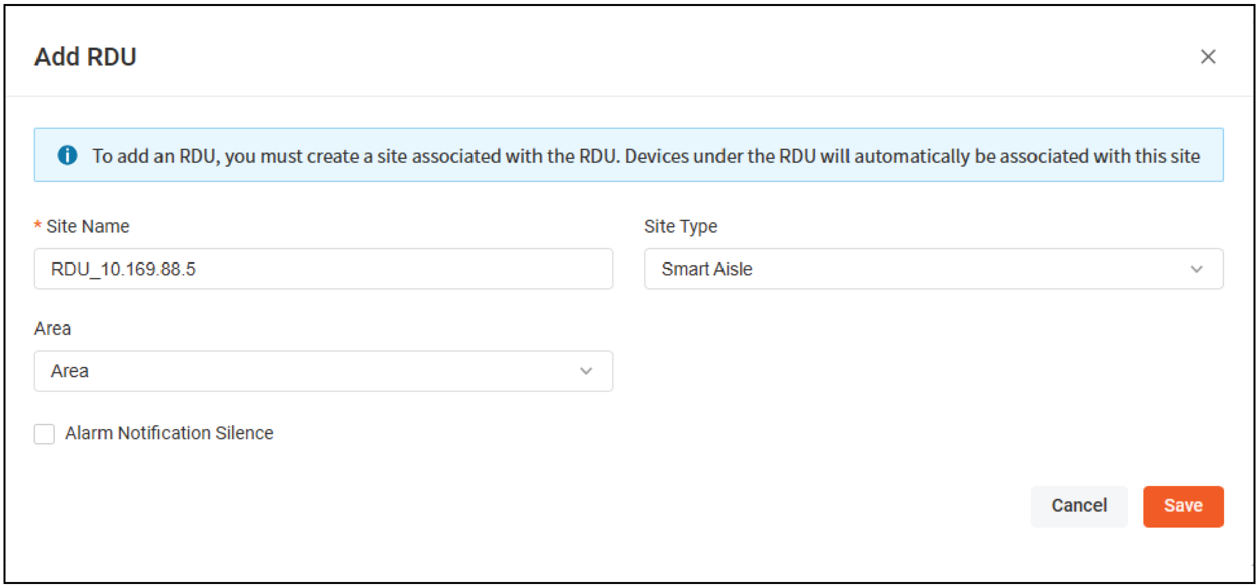
You can modify the Site Name, Site Type, and Region Name as needed.

If the RDU is not yet configured, you can enable Block Alarm Notifications, then later disable alarm notifications in Alarm → Alarm Silence Rule after configuration is complete.

Once you have made the necessary edits, click Save. The system will add the RDU to monitoring and associate it with the newly created site.

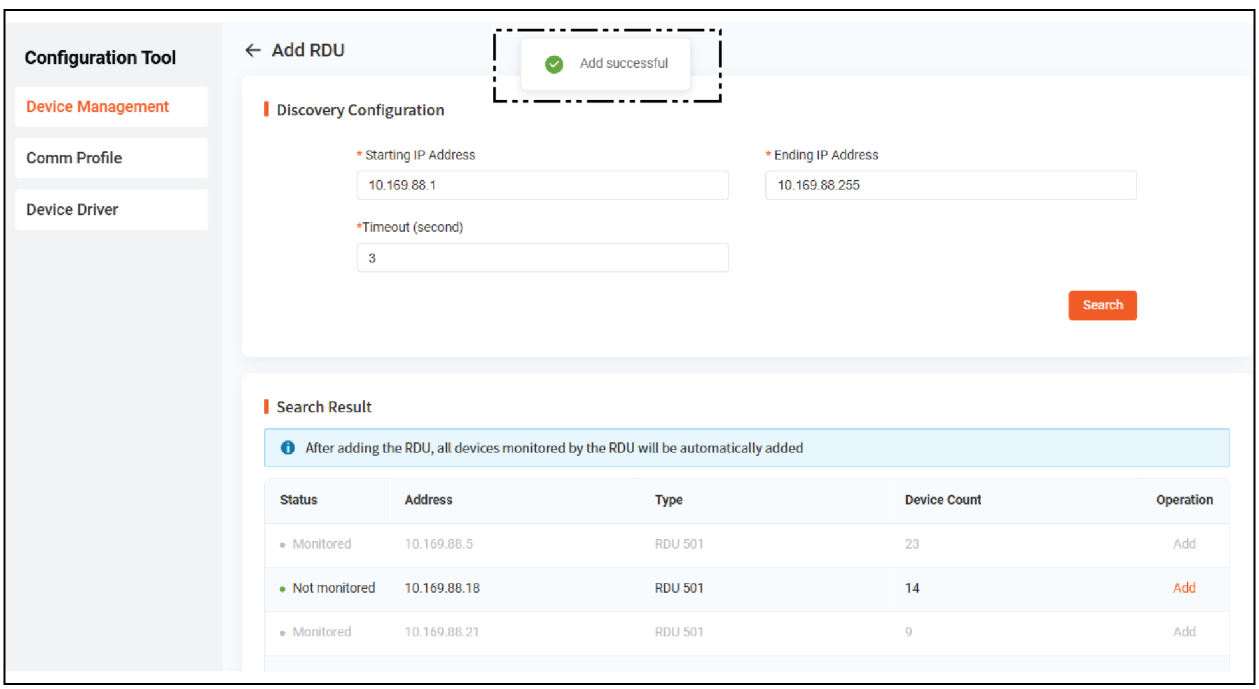
2. Click *Save* to add the RDU to monitoring. The button will then turn gray and become disabled.

Figure 15.11 Adding to Monitoring



3. After monitoring is complete, a notification will appear at the top of the page indicating the result of the addition (Refer to **Figure 15.12** below). If successful, the message will automatically close after 5 seconds. If the configuration fails, an error message will be displayed with details. The status will be updated to **Monitored**, and repeated attempts to **Add** to Monitoring will not be allowed (Refer to **Figure 15.12** below).

Figure 15.12 Monitoring Configuration



NOTE: 1. Once the searched RDU is added to monitoring, the detailed row for the associated site will no longer appear in subsequent searches, meaning it cannot be added to monitoring again.

2. For RDUs that are Not monitored, click Save. The button will remain disabled until the save process is complete.

3. The site name must be entered, otherwise the save button cannot be clicked.

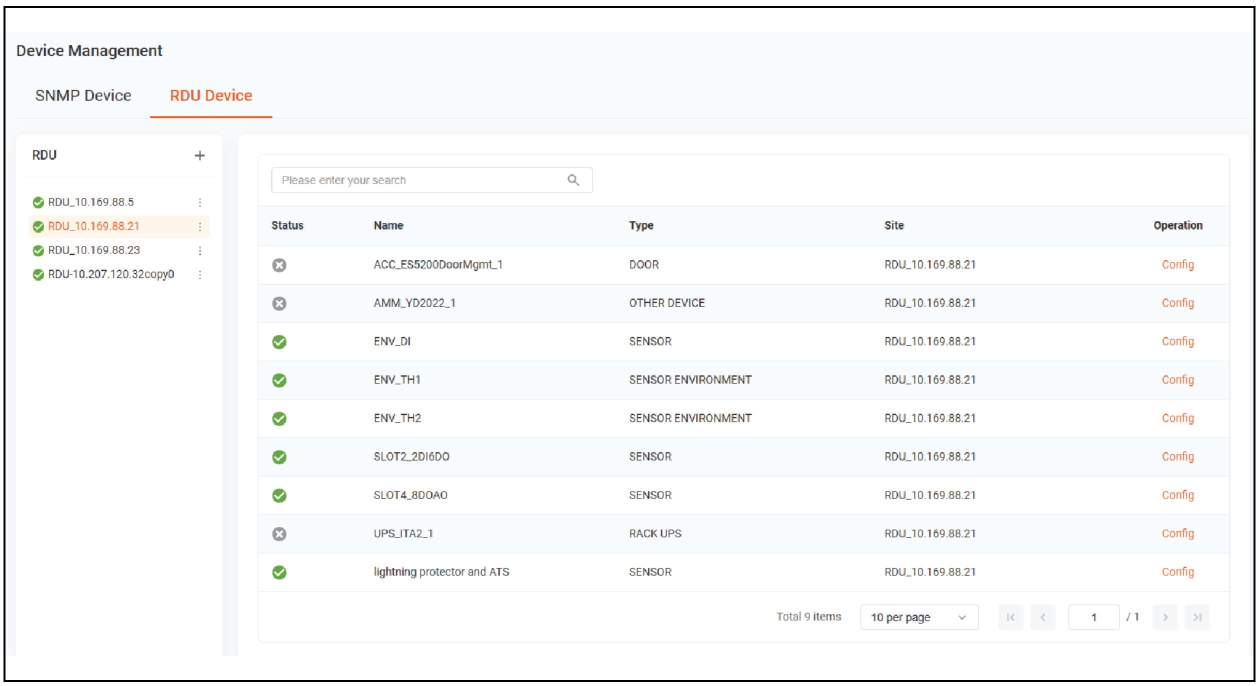
4. The site name must be unique within the entire center and cannot duplicate any other name, including region names.

5. The site name requires 3-64 characters.

15.2.2 Device Configuration

In the Configuration Tool, go to the RDU Device tab and select the required RDU. All devices under this RDU will be displayed in the table, as shown in Figure 15.13 below .

Figure 15.13 RDU Device Configuration Page

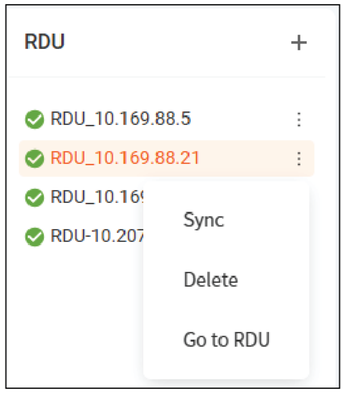


RDU Management

1. Synchronizing the RDU Configurations

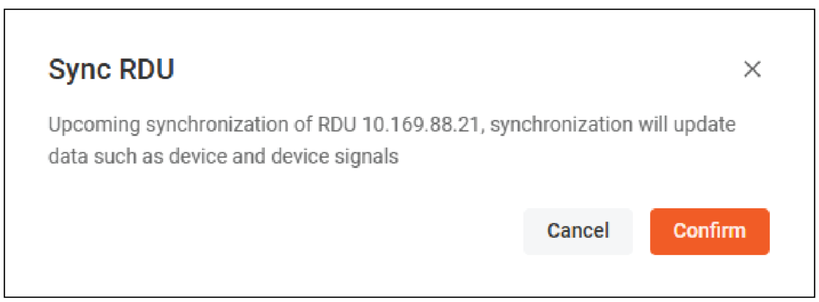
1. In RDU management, select an RDU and click the three dots to open the options. Then, click the Sync button to synchronize the current RDU configuration with the RDU device, as shown in Figure 15.14 on the next page .

Figure 15.14 RDU Management



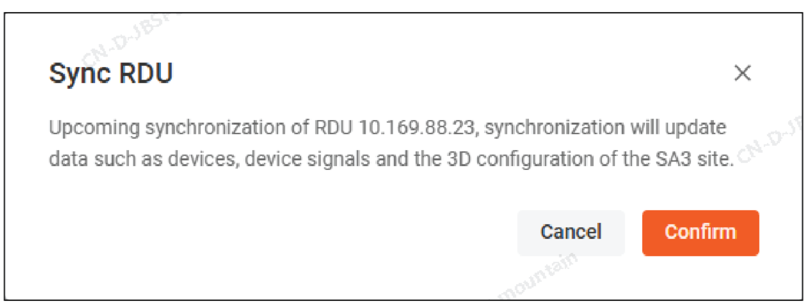
2. Since the current RDU may have been configured in the 3D configuration or widget, after clicking the Synchronize Configuration button, a confirmation message will pop up, and you can choose to confirm or cancel according to the actual situation. If you choose to cancel, the configuration will not be synchronized. If you select *Confirm*, the configuration of the RDU is synchronized, please refer to **Figure 15.15** below for the confirmation message.

Figure 15.15 Confirming the Synchronization Popup



If the site is of type SA3, you will see the popup as shown in **Figure 15.16** below .

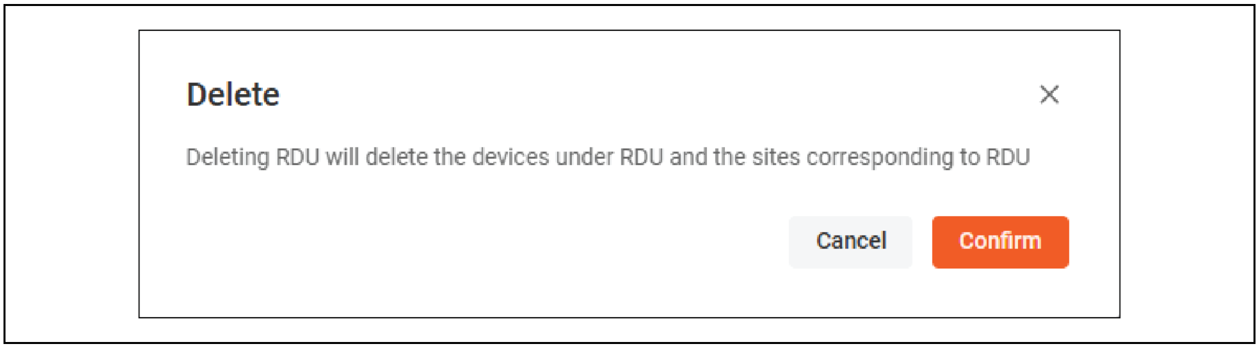
Figure 15.16 Confirming the Synchronization Configuration



2. Deleting the RDU

a) In the RDU list, click the three dots, then select the Delete button in the RDU management pop-up (as shown in **Figure 15.17** below), to delete the entire RDU along with all devices under it.

Figure 15.17 Deletion Confirmation Popup



3. Go to RDU

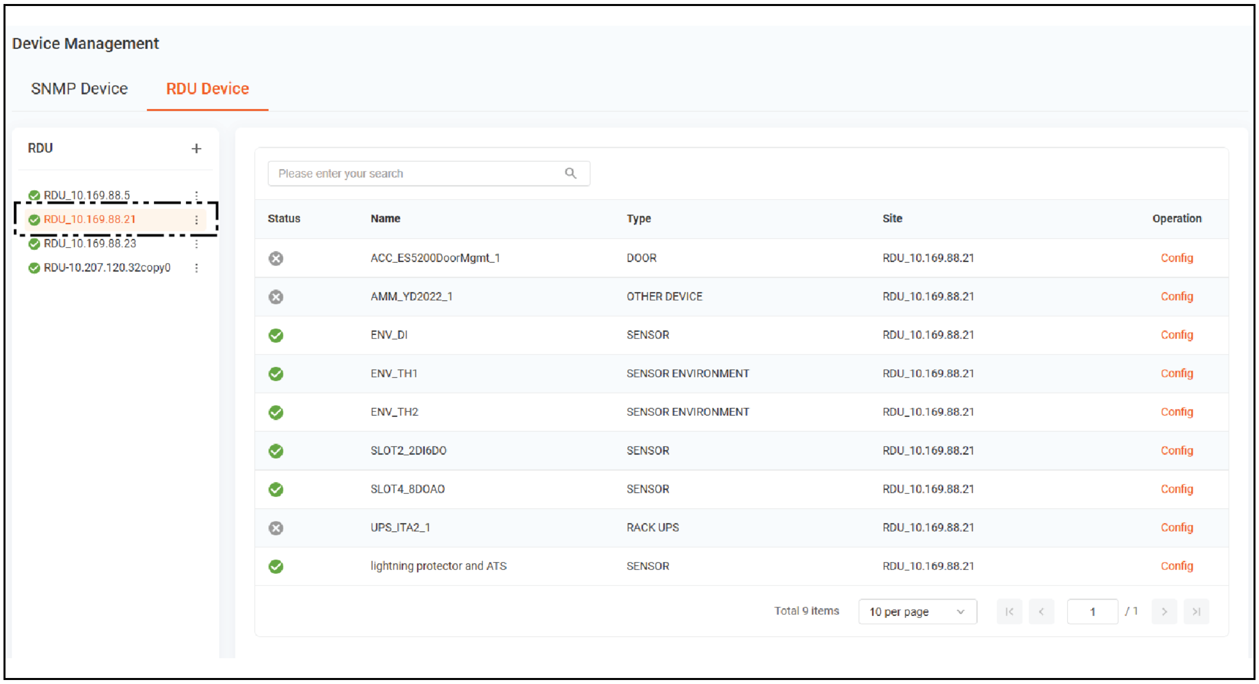
Click the three dots, then select the Go to RDU button to open a new browser tab for the RDU management system, as shown in **Figure 15.18** below .

Figure 15.18 Go to the RDU Page

4. View the devices associated with the RDU

a) To view the devices associated with the RDU, click on an RDU on the left and the related devices will be displayed on the right, as shown in **Figure 15.19** on the next page .

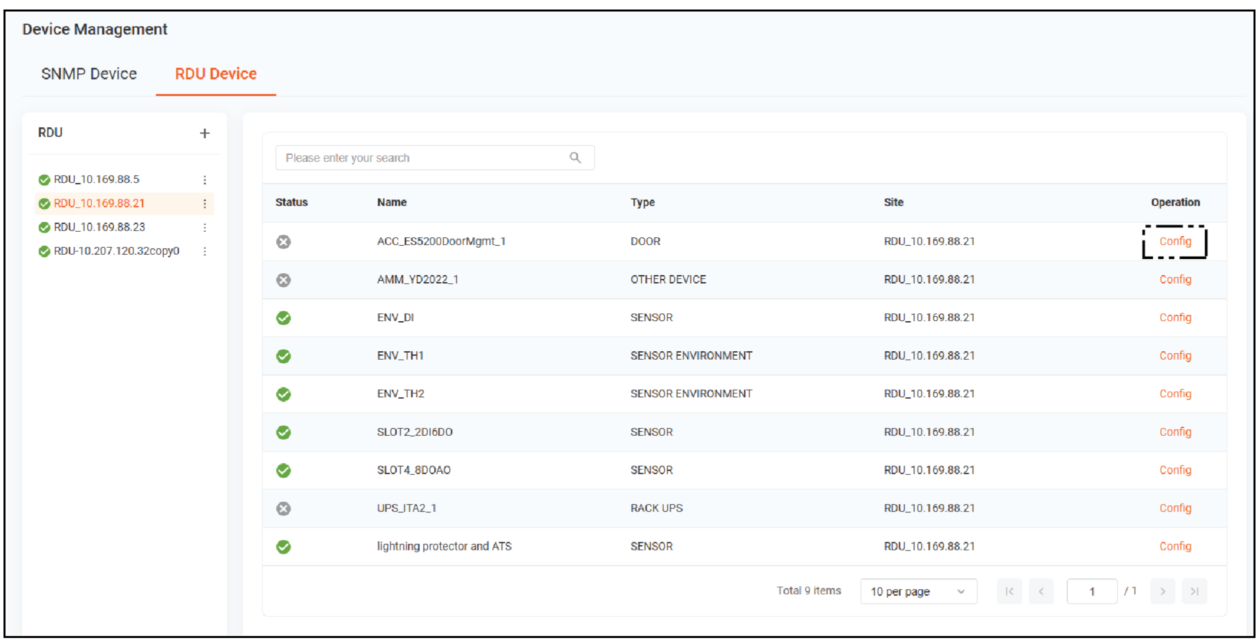
Figure 15.19 RDU Associated Devices



5. Device Configuration

1. Click the Config button in the Operations column for any device, as shown in **Figure 15.20** below .

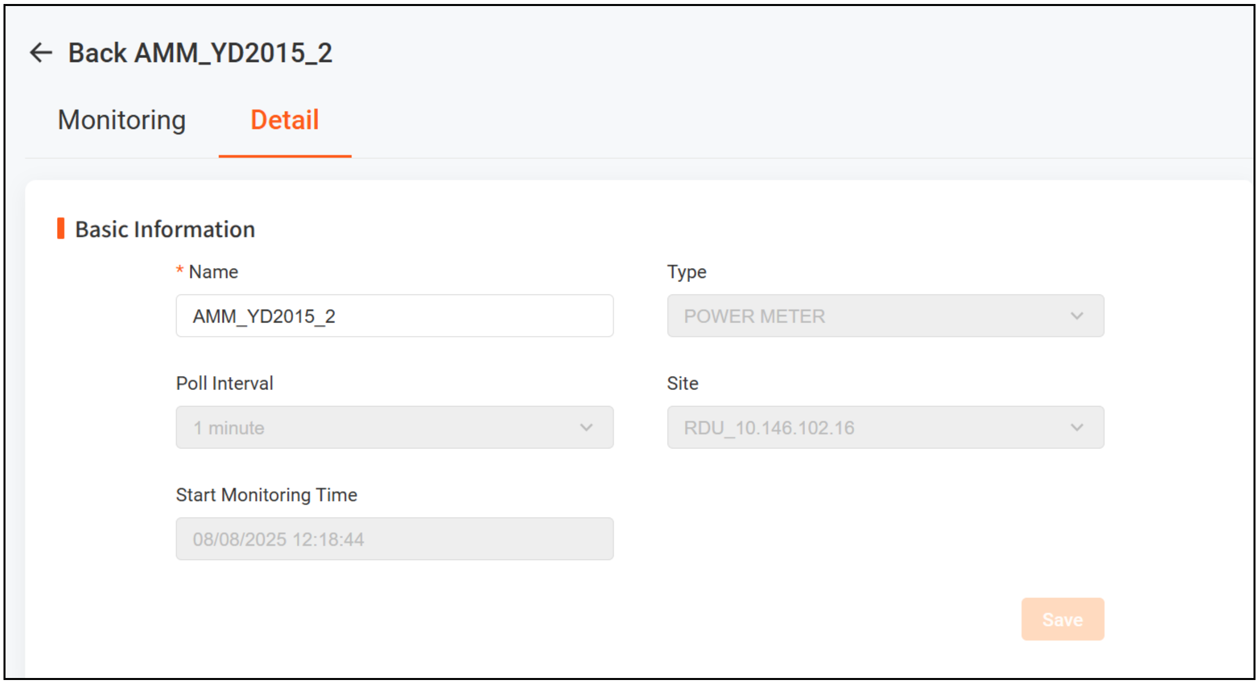
Figure 15.20 Device Configuration



2. After entering the device configuration page, it is mainly composed of two tabs: **Monitoring** and **Detail**. The function of the **Monitoring** tab can also be described in **15.3.1** on page 318 .

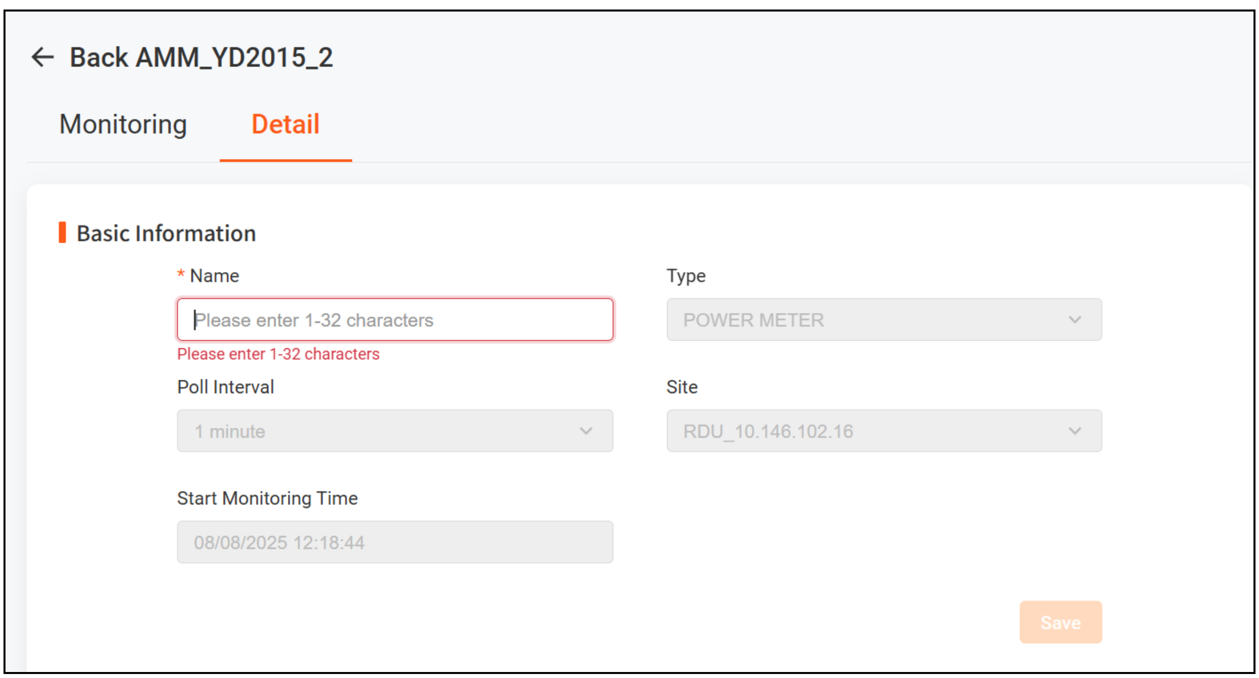
3. When you click the *Details* tab, the basic information of the device details is displayed. You can modify the name of the device. If no changes are made, the save button will remain disabled, as shown in RDU Detailed Features .

Figure 15.21 The Device Configuration Modification



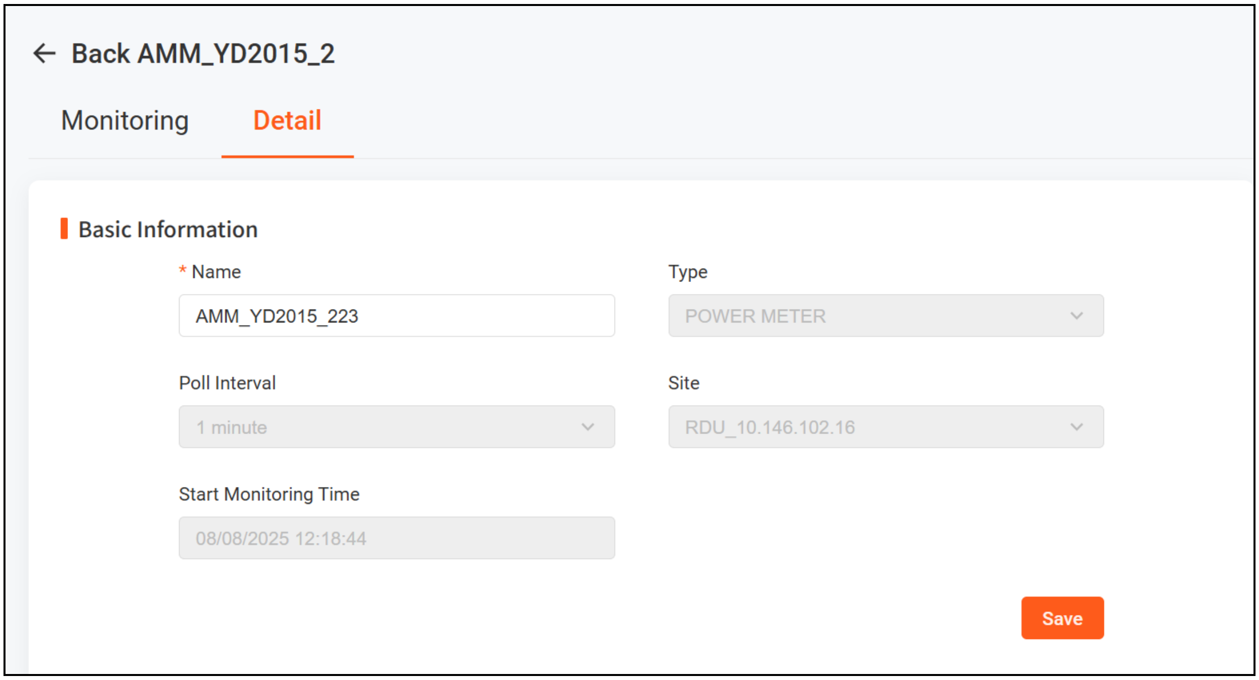
4. If the format is incorrect, a message will be displayed below, as shown in , the edit box and the save button will be disabled, as shown in Figure 15.22 below .

Figure 15.22 Incorrect Input Format Window



5. The user can modify the device name, and the save button becomes enable to click, and after modifying the device name, click *Save*, as shown in Figure 15.23 below .

Figure 15.23 Modifying the Device Configuration



NOTE: 1. The device name is required to be at least 1 character.

2. In the editing window, clicking the Save button is only allowed after the information has been modified.

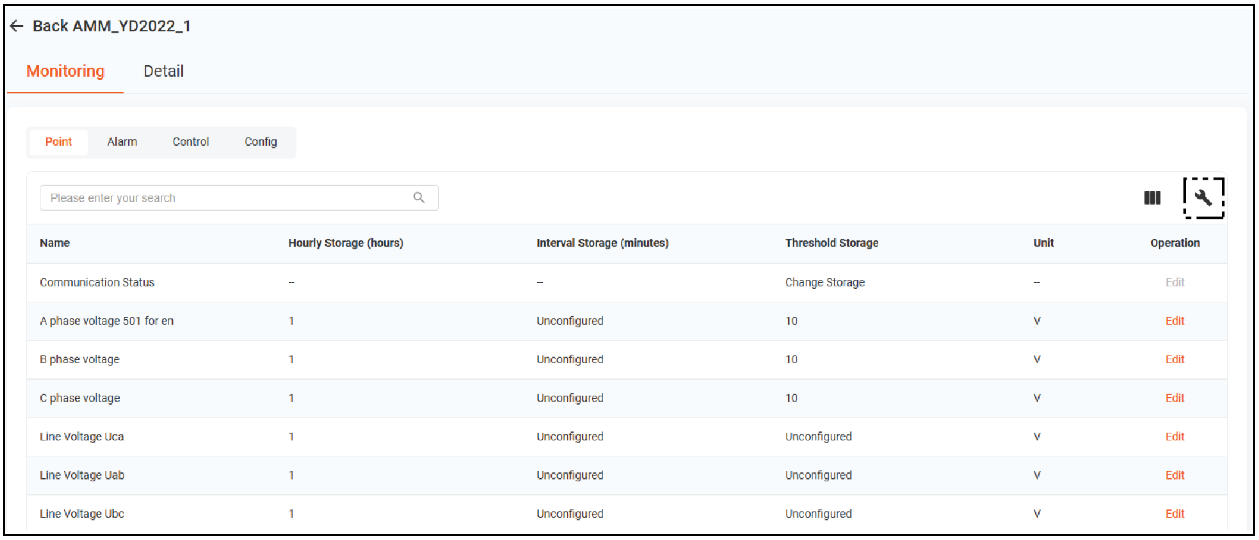
Signal Standardization

If the equipment monitored by the RDU is a non-standard device, or its signal is not standardized, use the Signal Standardization function to map the device's non-standard signal to a standardized signal. You can manually configure the signal standardization, and once standardized, the signal will be displayed in the 3D view and on the dashboard. (It is recommended that non-professionals consult the on-site configuration personnel in advance before carrying out signal standardization operations).

1. Standardizing Configuration Signals

1. On the Device Configuration page, under the Monitoring - Point tab, click the Signal Normalization button to open the Signal Normalization pop-up window, as shown in Figure 15.24 on the facing page .

Figure 15.24 Device Signal Normalization

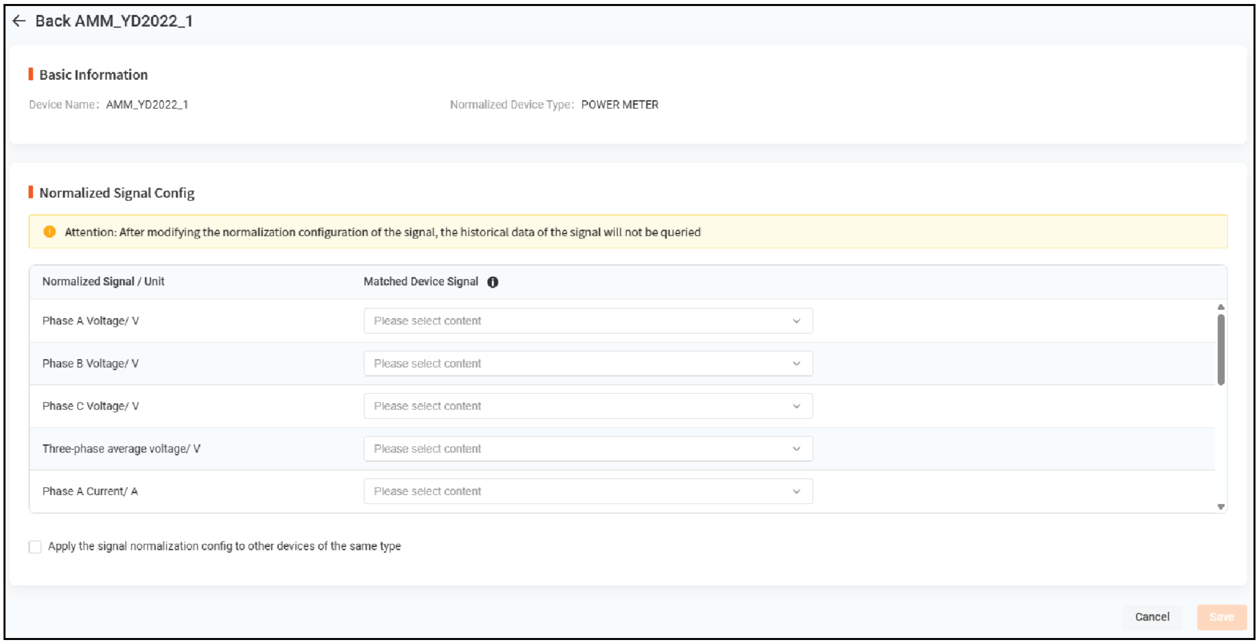


2. In the signal normalization pop-up window, the device type will be automatically set to the standardized device type (only UPS, CRAC, and Power meter devices are supported).

NOTE: If the signal is not standardized, click *save* directly, and the non-standard device type (the default type is Other) will also be changed to the corresponding device type.

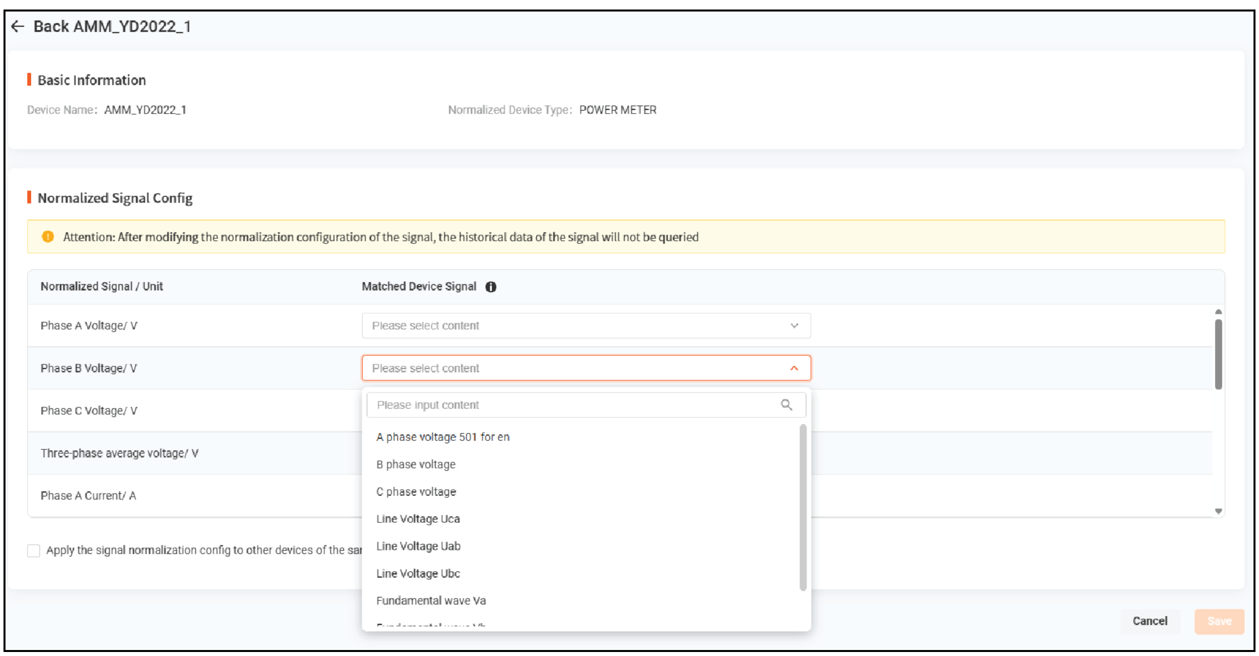
3. According to the standardized signal name in the list on the left, select the actual device signal corresponding to the standardized signal on the right to match them one by one to achieve standardized device signal configuration. For example, if the name of the normalized signal on the left is **phase A input voltage**, you need to select the actual signal corresponding to phase A input voltage under the current device in the drop-down box on the right, as shown in **Figure 15.25** on the next page . (If the device does not have a corresponding signal, you can leave it blank).

Figure 15.25 Signal Normalization Configuration Pop-up Window



4. When selecting a matching device signal, click to open the device signal drop-down box to query the signal name, and only the device signal with the same standardized signal unit will be filtered, as shown in **Figure 15.26** below .

Figure 15.26 Signal Standardization Configuration Drop-down



5. Once you have completed all or part of the signal standardization configuration, click *Save* to complete the standardization of the device type and the selected device signal.

NOTE: 1. After the signal normalization configuration is modified, the history before the signal normalization of the modified signal can no longer be queried based on the device signal in the historical signal report.

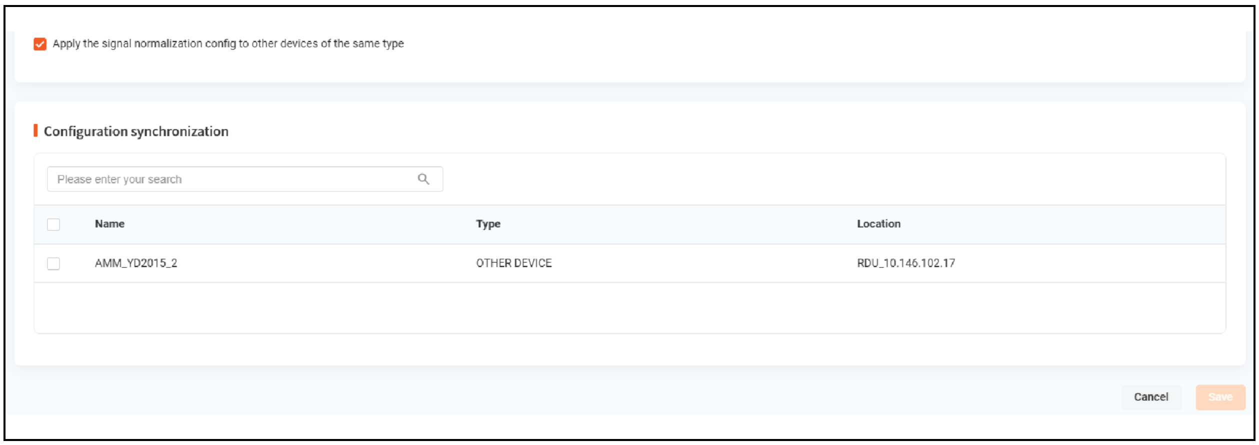
2. After the device driver is updated on the RDU linked to the device, synchronizing the RDU in SI will reset the device's signal standardization configuration. Whether the signal is standardized will then depend solely on the updated driver.

After selecting the required option from the drop-down to match the Matched Device Signal with the Normalized Signal/Unit, check the box to apply the signal normalization config to other devices of the same type. This will open the Configuration Synchronization section.

In this section, you can select other devices of the same type to apply the signal standardization configuration (only for devices in SI that use the same device driver model and driver version as the current one). Once selected, click Save to apply the configuration to the chosen devices.

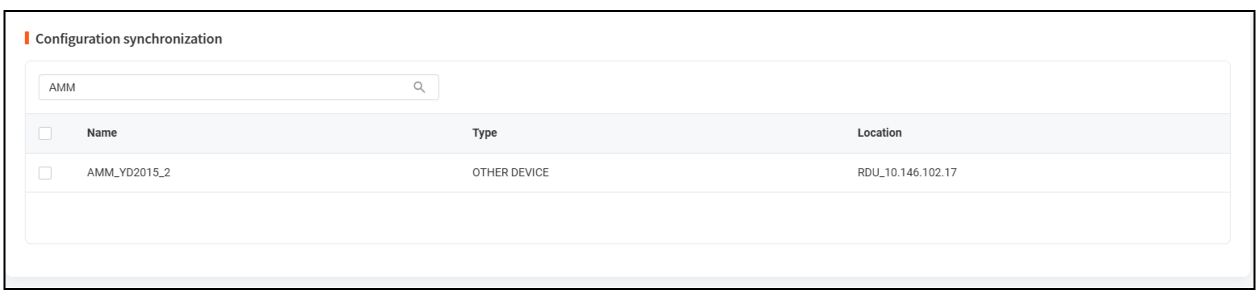
Note: Applying Configuration Synchronization is optional. (See Figure 15.27 below).

Figure 15.27 Signal Normalization - Synchronization to Other Devices



2. In the Synchronization Signal Normalization Configuration section, you can enter the device name, device type, and site to perform fuzzy query and filter devices, as shown in Figure 15.28 below .

Figure 15.28 Signal normalization—Synchronization to Other Devices

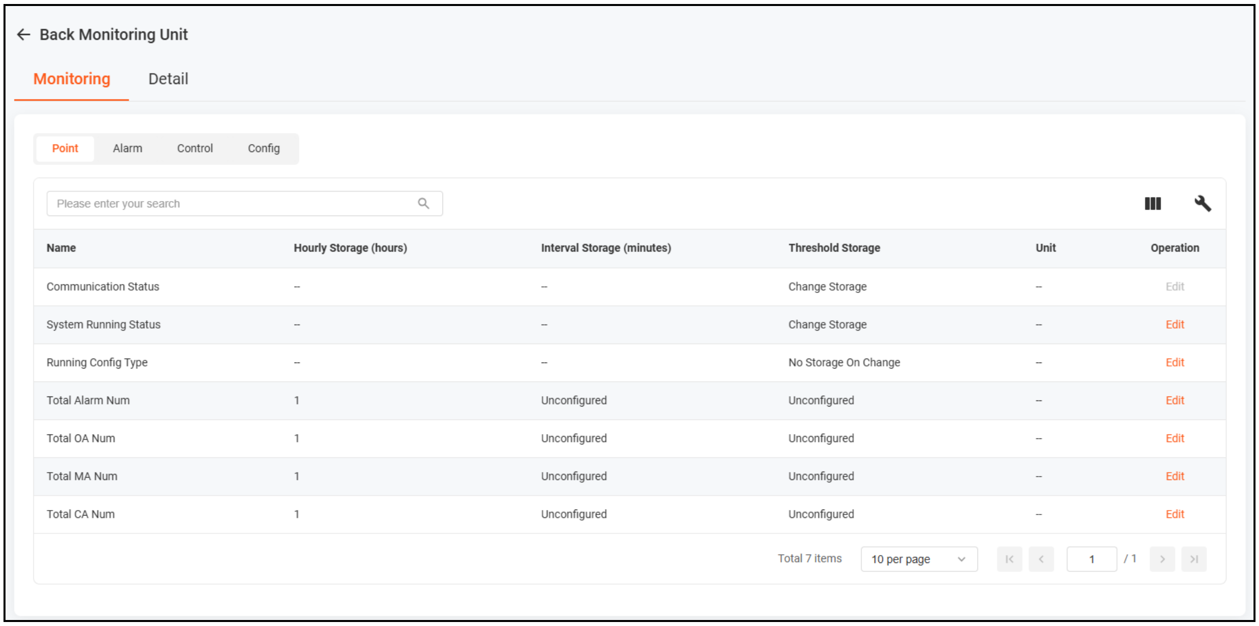


Signal Configuration

1. Displays a List of Signals

Clicking the *Config* button on the device associated with the RDU will dynamically display the corresponding signal list in the Monitoring-Point tab, as shown in Figure 15.29 on the next page .

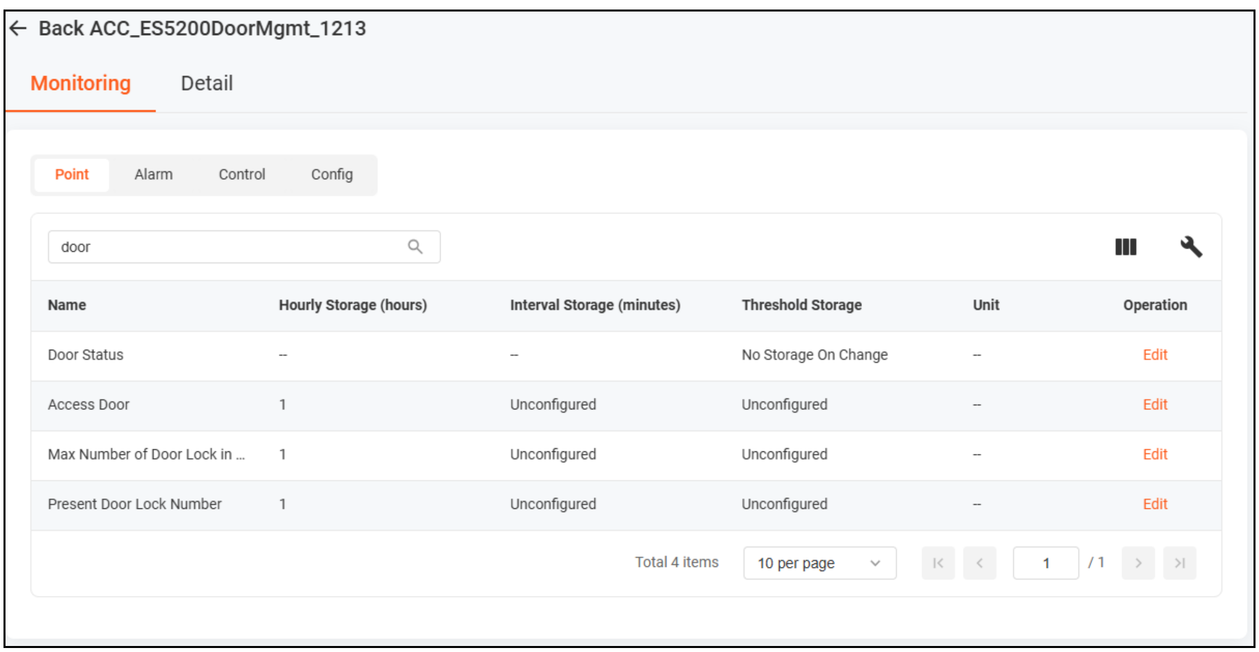
Figure 15.29 A List of Signals



2. Signal Abnormal Search

In the search box on the Signal page, enter the name of the signal you want to quickly find, and the system will immediately filter out the corresponding signal, as shown in **Figure 15.30** below .

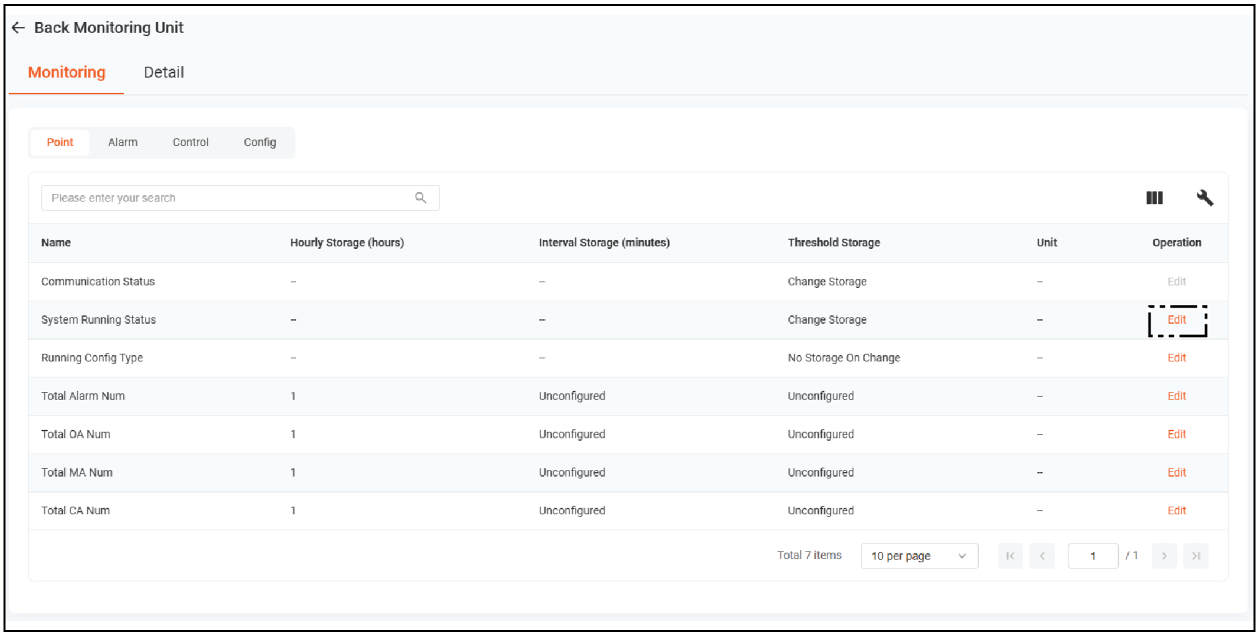
Figure 15.30 Abnormal Search



3. Signal Editing

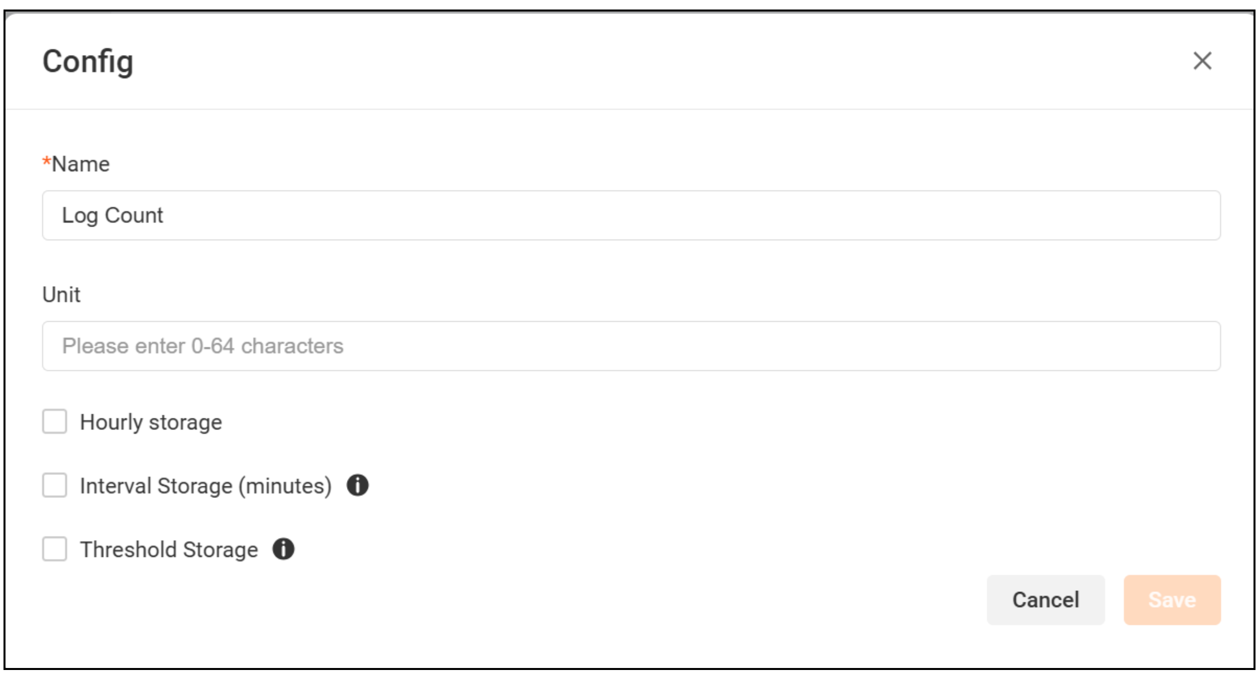
1. Click the *edit* icon on the right of the signal you want to edit, as shown in **Figure 15.31** on the facing page .

Figure 15.31 Editing the Signals



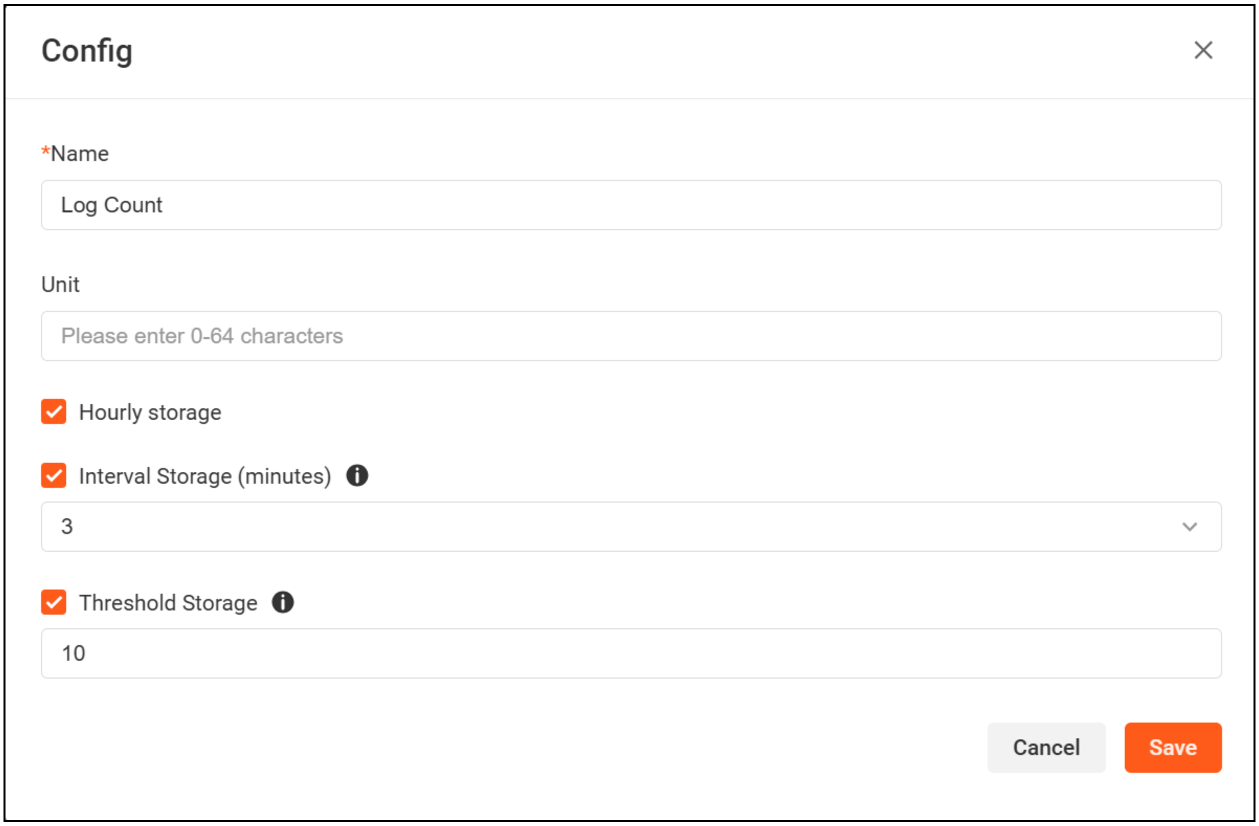
2. The signal configuration page will pop up, and if no changes have been made, the Save button is disabled. Click the *cancel* button to close the pop-up, as shown in **Figure 15.32** below .

Figure 15.32 Signal Configuration



3. The user can edit the signal name and click *save*.
4. Configure the storage strategy of the signal. The default value is Hour-Point Storage, and the Hour-Point Storage Policy is the same as that of the device. If you select Threshold Storage, it will be stored when the signal is greater than or equal to the threshold, as shown in **Figure 15.33** on the next page .

Figure 15.33 Signal Configuration—Modifying the Storage Threshold



NOTE: 1. The signal name must be at least 1 character.

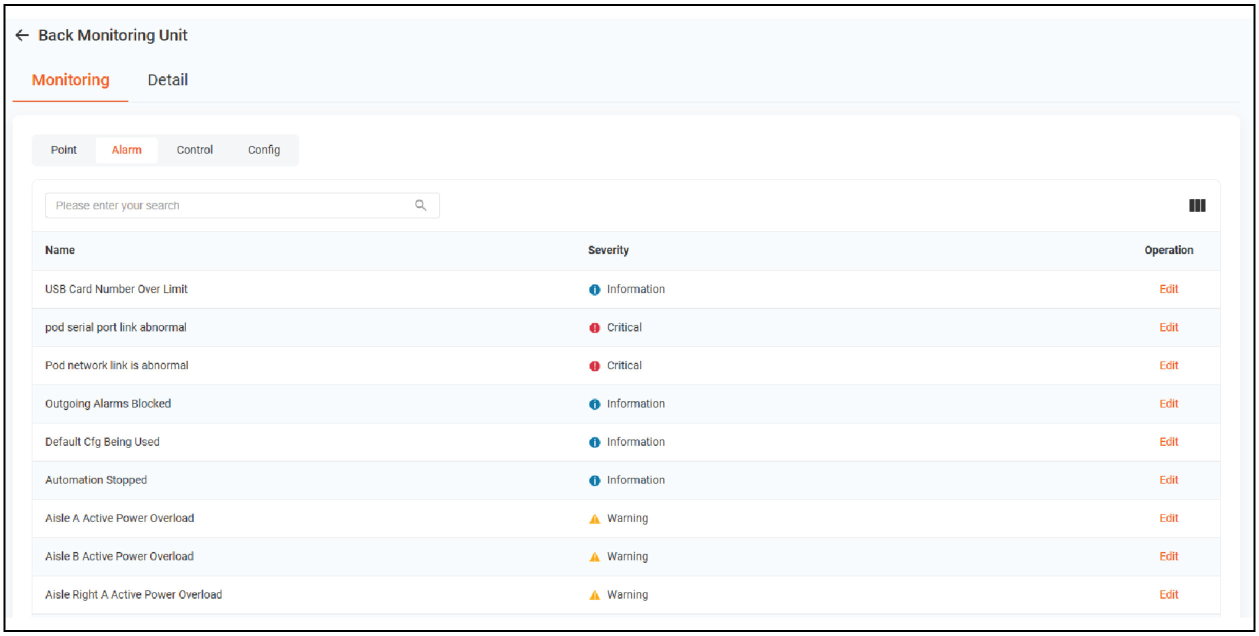
2. In the editing window, clicking the Save button is only allowed after the information has been modified.

Alarm Configuration

1. A list of alarms is displayed

Go to the configuration page of the device associated with the RDU and switch to the Monitoring-Alarm tab, and the Alarm list for the device will be displayed. As shown in Figure 15.34 on the facing page .

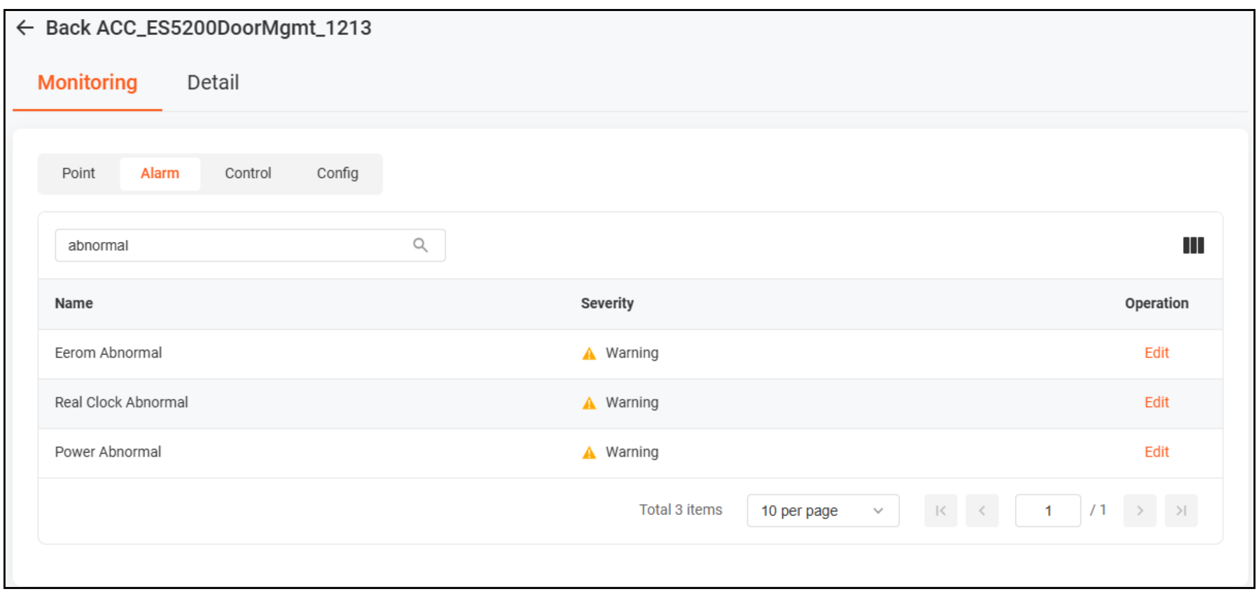
Figure 15.34 A List of Alarms



2. Searching the Abnormal Alarm

In the search box of the Alarm tab, enter the name of the alert you want to quickly find, and the system will immediately filter out the corresponding alert. As shown in **Figure 15.35** below .

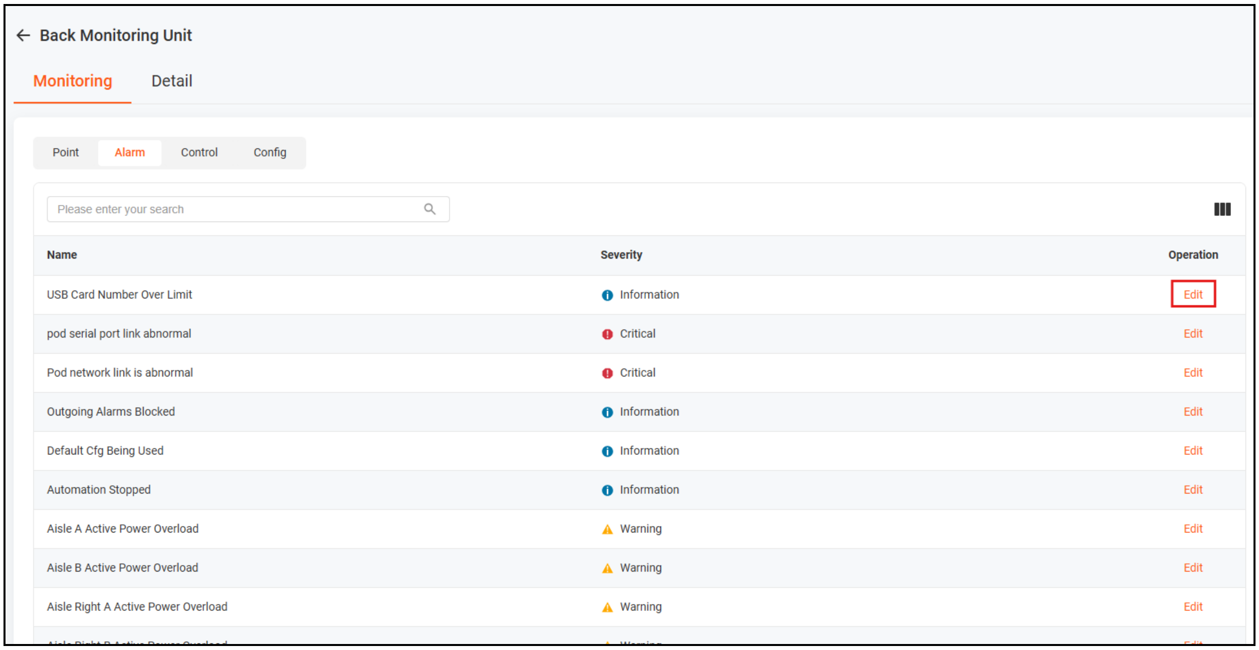
Figure 15.35 Abnormal Alarm Search



3. Alarm Editing

1. Click the *Edit* button in the Operations column for the alarm you want to edit, as shown in **Figure 15.36** on the next page .

Figure 15.36 Alarm Editing



2. The signal configuration page will pop up, and if no changes have been made, the Save button will be disabled. Click the *cancel* button close the pop-up, as shown in **Figure 15.37** below .

Figure 15.37 Alarm Configuration

3. Users can edit the alarm name, Severity, and then click *save* to complete the editing of the alarm.

NOTE: 1. The alert name must be at least 1 character long.

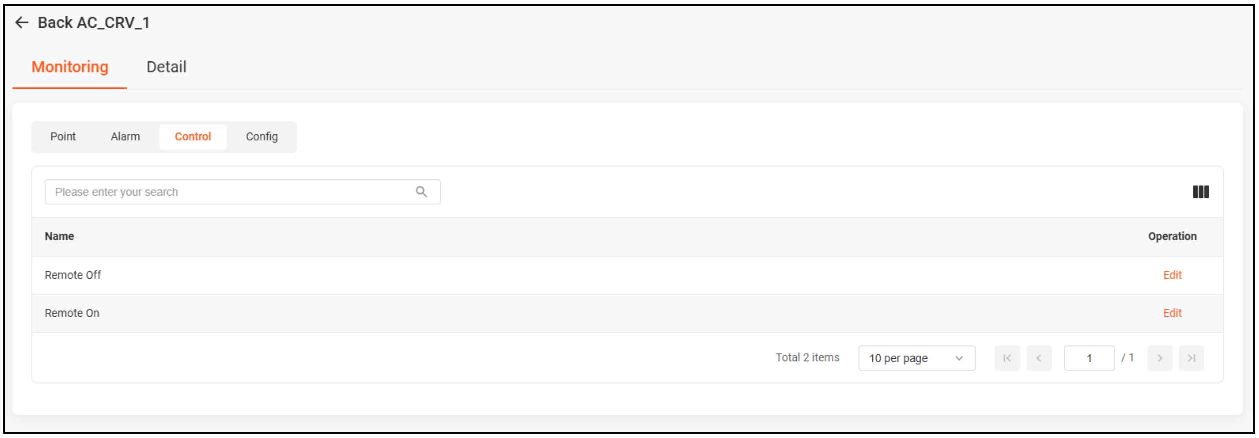
2. In the editing window, clicking the Save button is only allowed after the information has been modified.

Controlling the Configuration

1. Displays the control list

Go to the configuration page of the device associated with the RDU and switch to the Monitoring-Control tab, and the control list for the device will be displayed. As shown in **Figure 15.38** below .

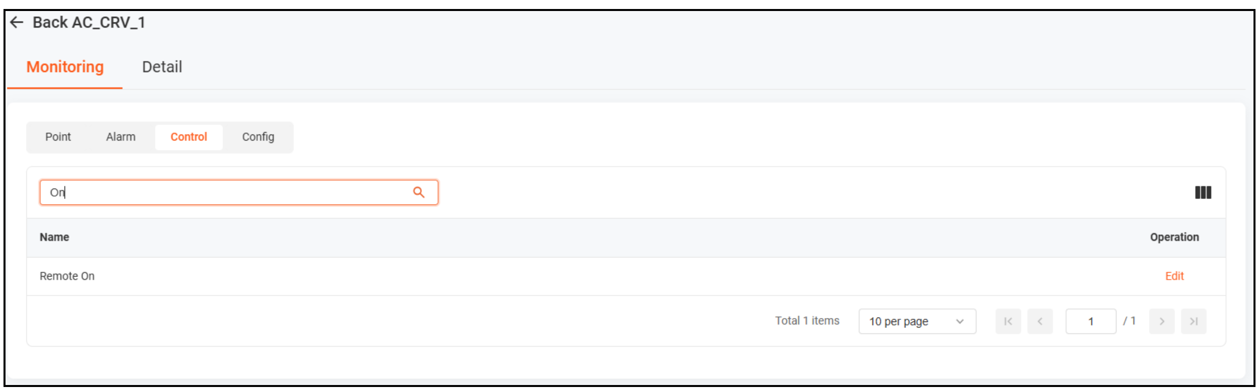
Figure 15.38 A List of Controls



2. Control name Abnormal Queries

In the search box on the Control TAB page, enter the name of the control you want to quickly find as shown in **Figure 15.39** below , and the system will immediately filter out the corresponding control action.

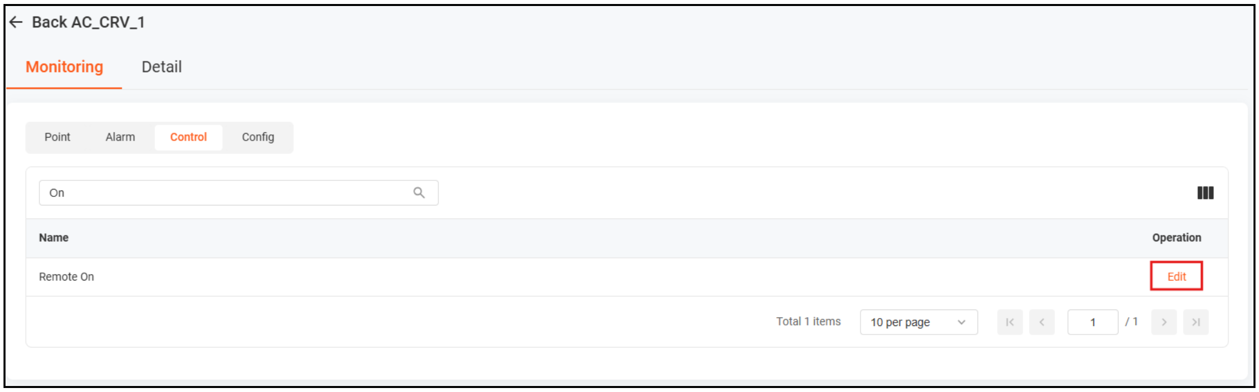
Figure 15.39 Controlling the Abnormal Queries



3. Control Editing

1. Click the *Edit* button under the operations columns for the Control to edit, as shown in **Figure 15.40** on the next page .

Figure 15.40 Control Editing Page



2. If no changes have been made, the Save button is disabled. Click the *cancel* button to exit the edit page, as shown in Figure 15.41 below .

Figure 15.41 Control the Editing Popup

3. Users can edit the name, and then click *save* to complete the editing of the control.

NOTE: 1. The control name requires a minimum of 1 character.

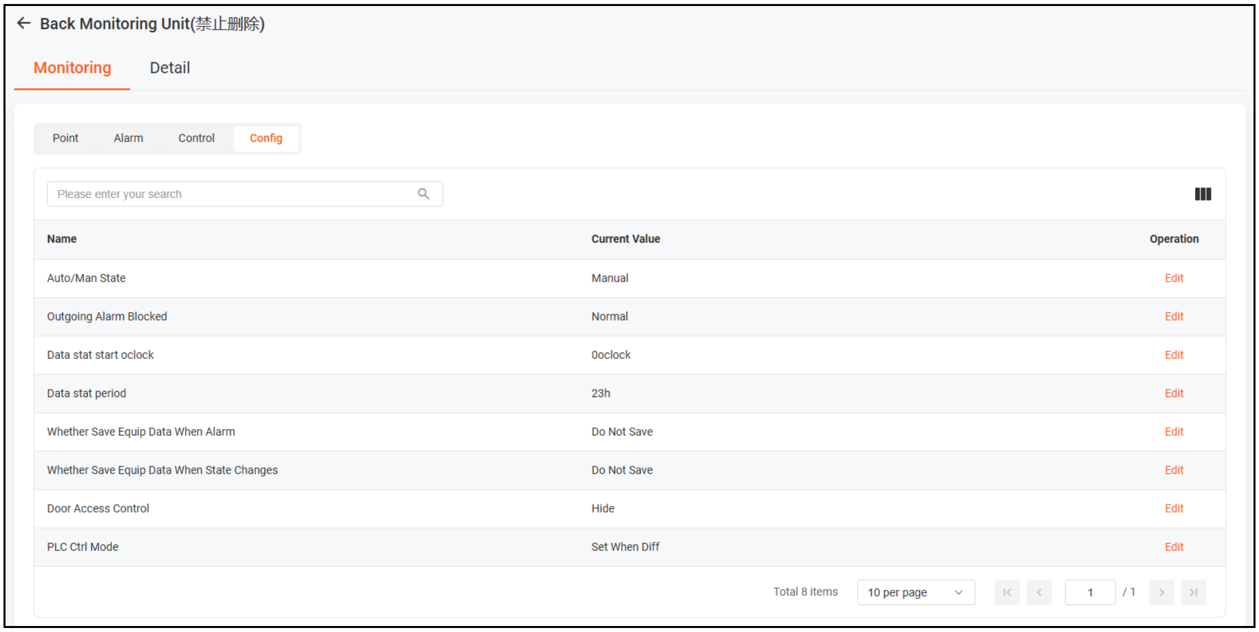
2. In the editing window, clicking the Save button is only allowed after the information has been modified.

Setting up the Configuration

1. A list of settings is displayed

Go to the configuration page of the device associated with the RDU and switch to the Monitoring-Config tab, and the Config list for the device will be displayed , as shown in Figure 15.42 on the facing page .

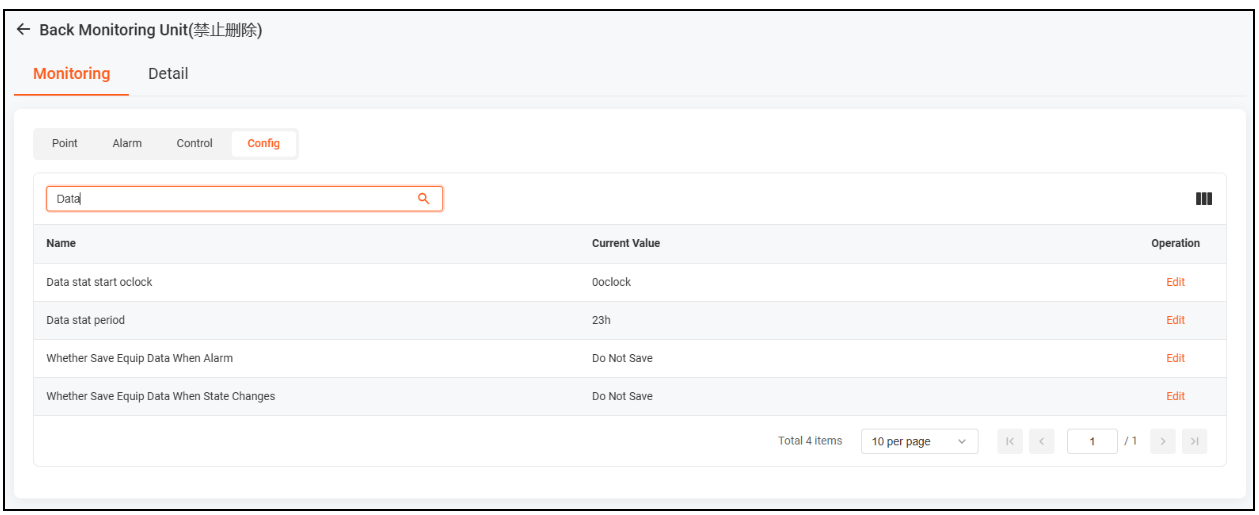
Figure 15.42 Settings List



2. Setting a name for Abnormal Query

In the search box on the Settings tab page, enter the name of the setting you want to quickly find, and the system will immediately filter for that setting, as shown in **Figure 15.43** below .

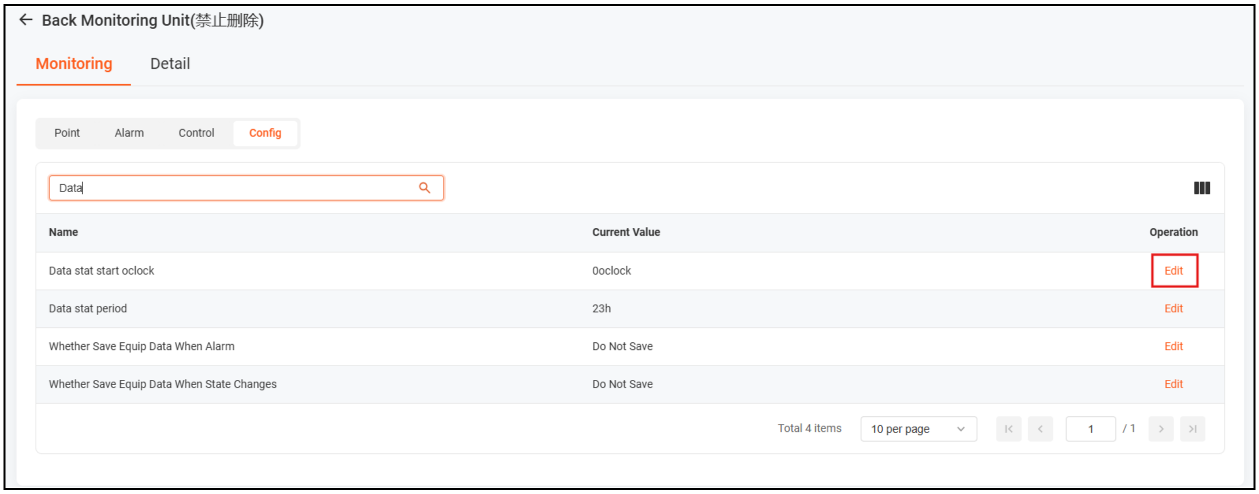
Figure 15.43 Setting an Abnormal Query



3. Editing Settings

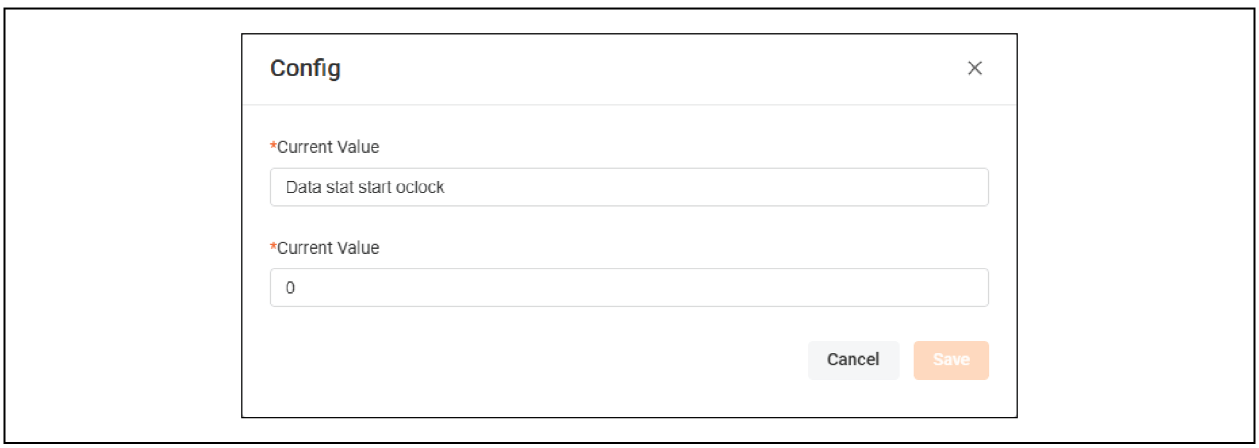
1. Click the *Edit* button under the operations columns for the Config to edit, as shown in **Figure 15.44** on the next page .

Figure 15.44 Settings Editing



2. The setting configuration page will popup as **Figure 15.45** below , and if no changes have been made, the Save button is disabled. Click the *cancel* button to exit the editing pop-up.

Figure 15.45 Setting up the Editing Page



3. Users can edit the name, the value of the control and then click *save* to complete the editing of the control.

NOTE: 1. The control name requires a minimum of 1 character.

2. In the editing window, clicking the *Save* button is only allowed after the information has been modified.

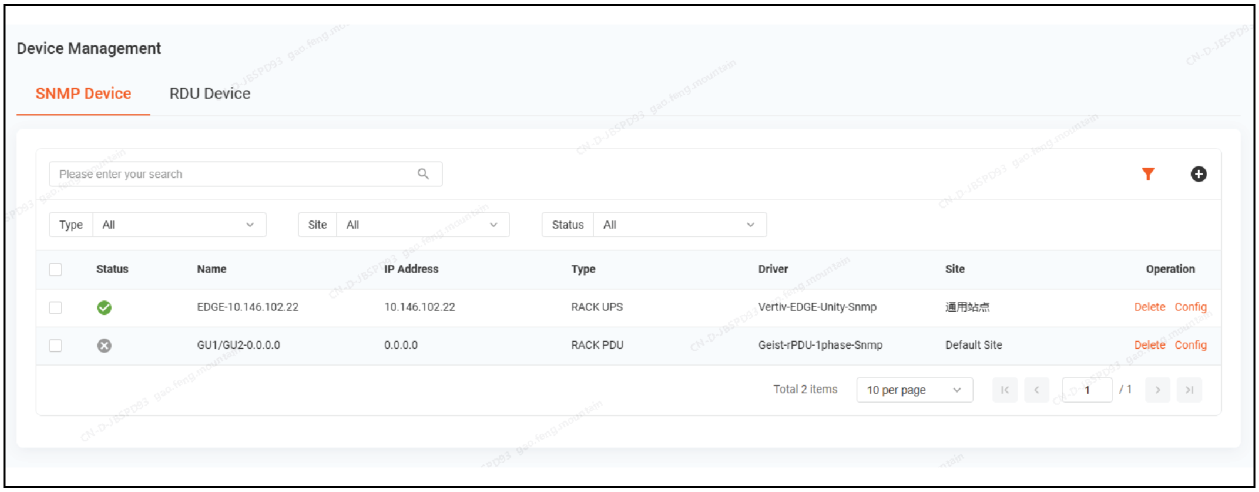
15.3 SNMP Detailed Function

15.3.1 Device Management

Go to the SNMP device page

Click Configuration Tool on the Smart InfraSight to go to the Device Management page, you will enter the SNMP device list, as shown in **Figure 15.46** on the facing page .

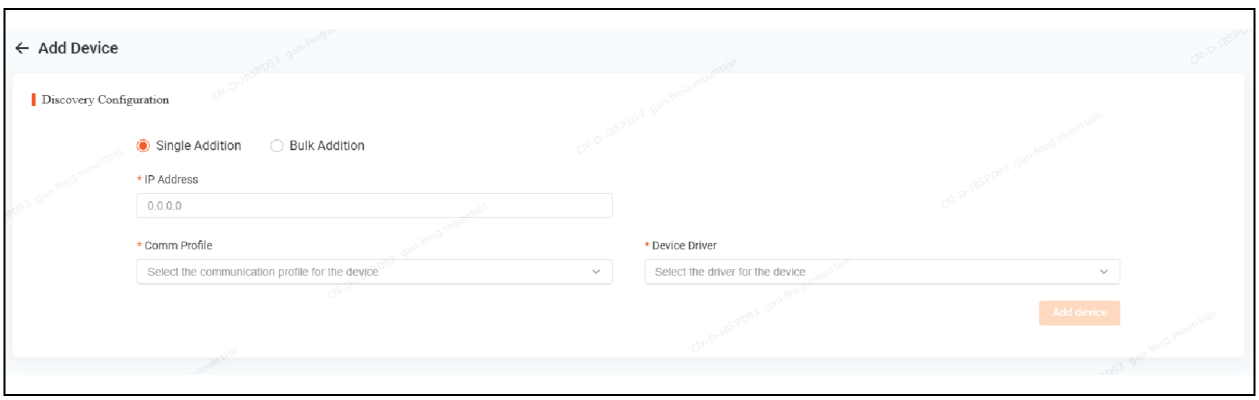
Figure 15.46 List of SNMP Devices



Add a new device

Click the *add* button in the upper right corner of the table to enter the Add Device page, you can choose to add a single device or add a batch of devices, as shown in Figure 15.47 below .

Figure 15.47 Adding Devices Page



Single Addition

- Enter an IP address, which cannot be the same as an existing device's IP address
- Select a comm profile (refer to the SNMP Detailed Function)
- Select the device driver

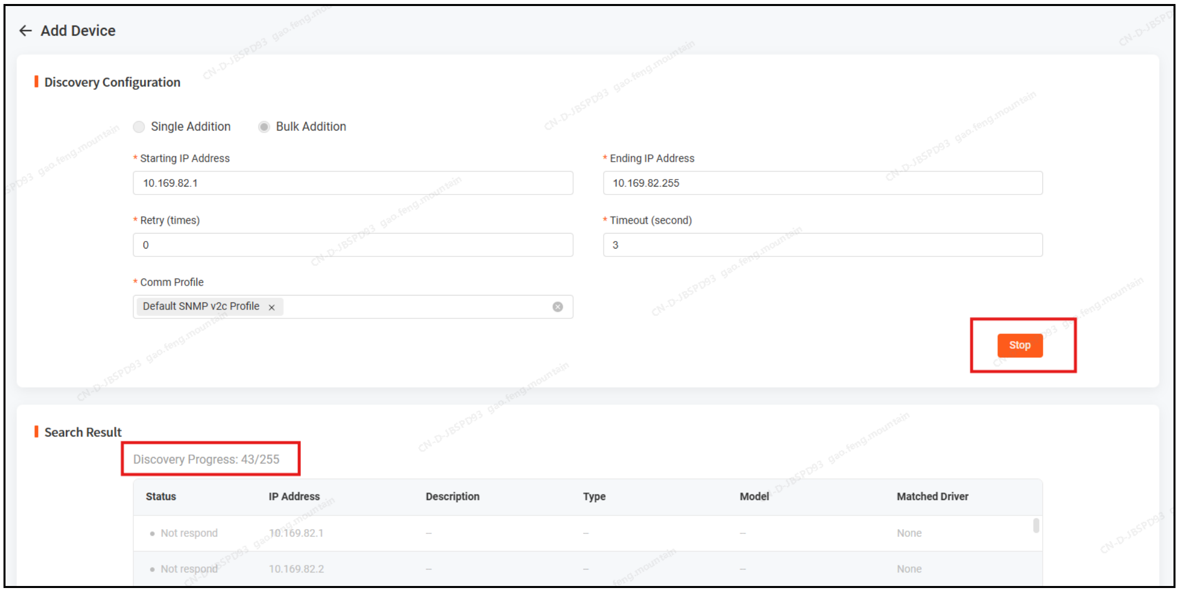
Click the Add Device button to add a device.

Bulk Addition

- Enter the starting IPv4 address and the ending IPv4 address, where the devices will be searched for.
- Enter the number of retries, when the system fails to communicate with an IP address, the system will retry the communication.

- Enter a timeout period, When the system tries to communicate with an IP address, it waits for the timeout period before considering the communication a failure.
- Select a communication profile. In SNMP Detailed Function the comm profile is default for device search, it will be selected by default in the bulk addition configuration.
- After filling in the required information, click the search button. The search progress will be displayed in the results section. You can click the stop button at any time to halt the search. Note that you cannot interact with the search results while the search is in progress, as shown in **Figure 15.48** below .

Figure 15.48 Device Searching Process



After the search is completed, the results are categorized into the following statuses:

- Not responding: The device is disabled, and no action can be taken.
- Driver missing: This status means the system cannot match an appropriate driver with the device. Clicking **Select Driver** in the operation column to manually select a driver for the device. The status will change to **Unmonitored**.
- Unmonitored: You can either select **Add to Monitor** directly or click **Modify Driver** in the operation column to change the matching driver of the device.

Figure 15.49 Search Result

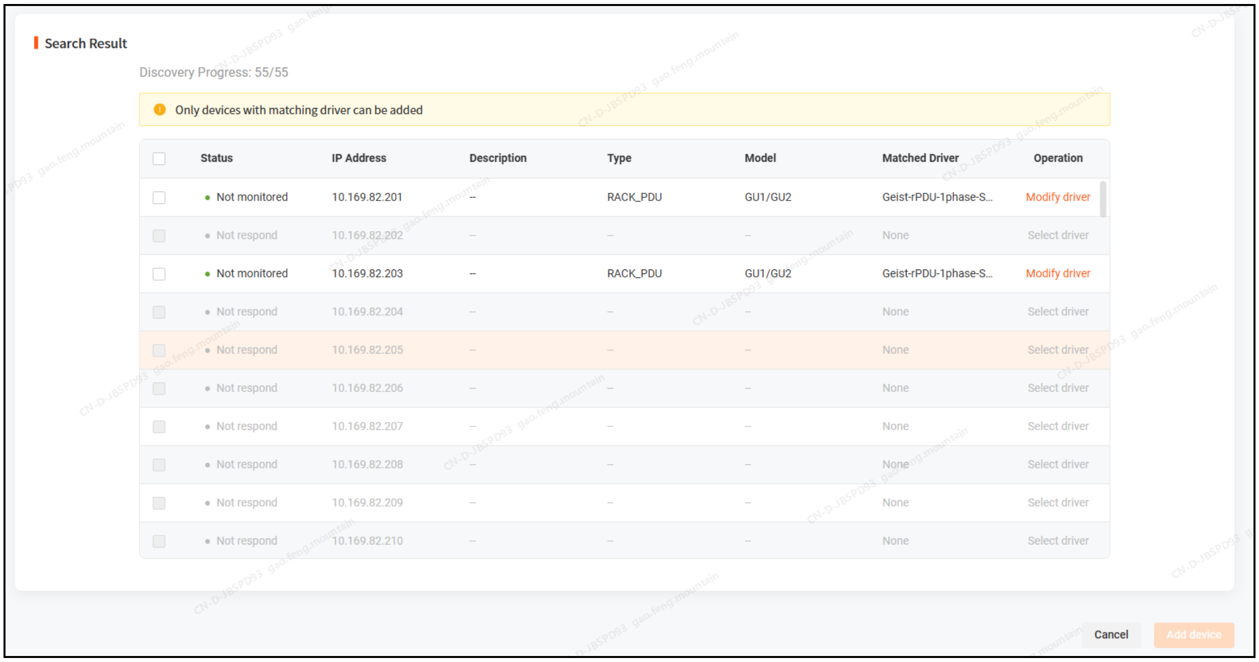
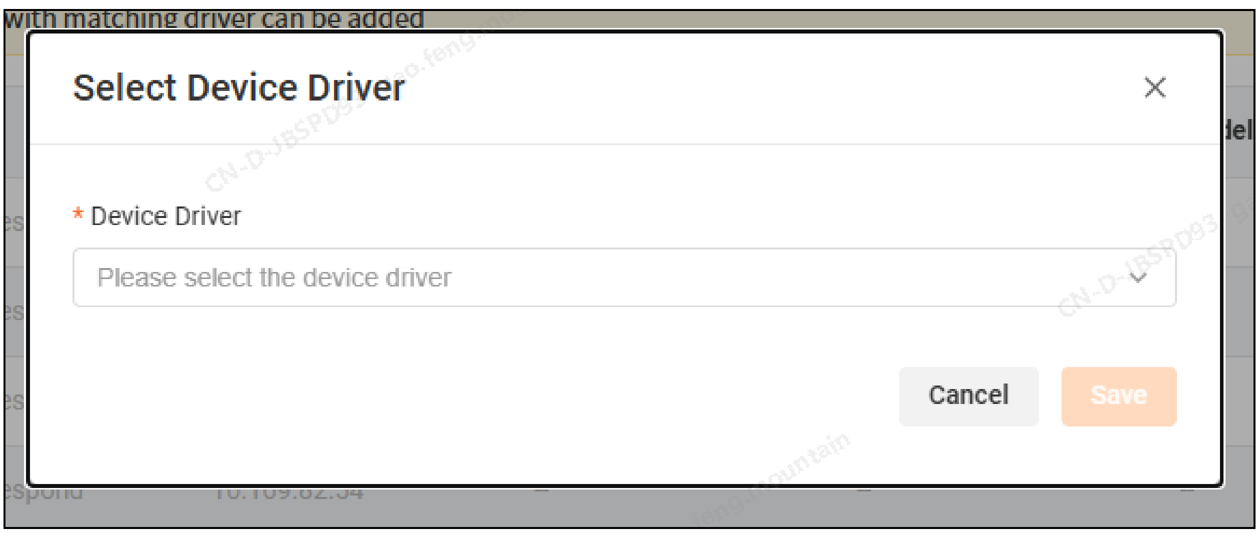


Figure 15.50 Selecting the Device Driver



After the search is completed, you can select the devices that are not monitored in batches and click the Add Device button to add them, as shown in **Figure 15.51** on the next page .

The newly added devices belong to the Default Site, as shown in **Figure 15.52** on the next page .

Figure 15.51 Adding Devices

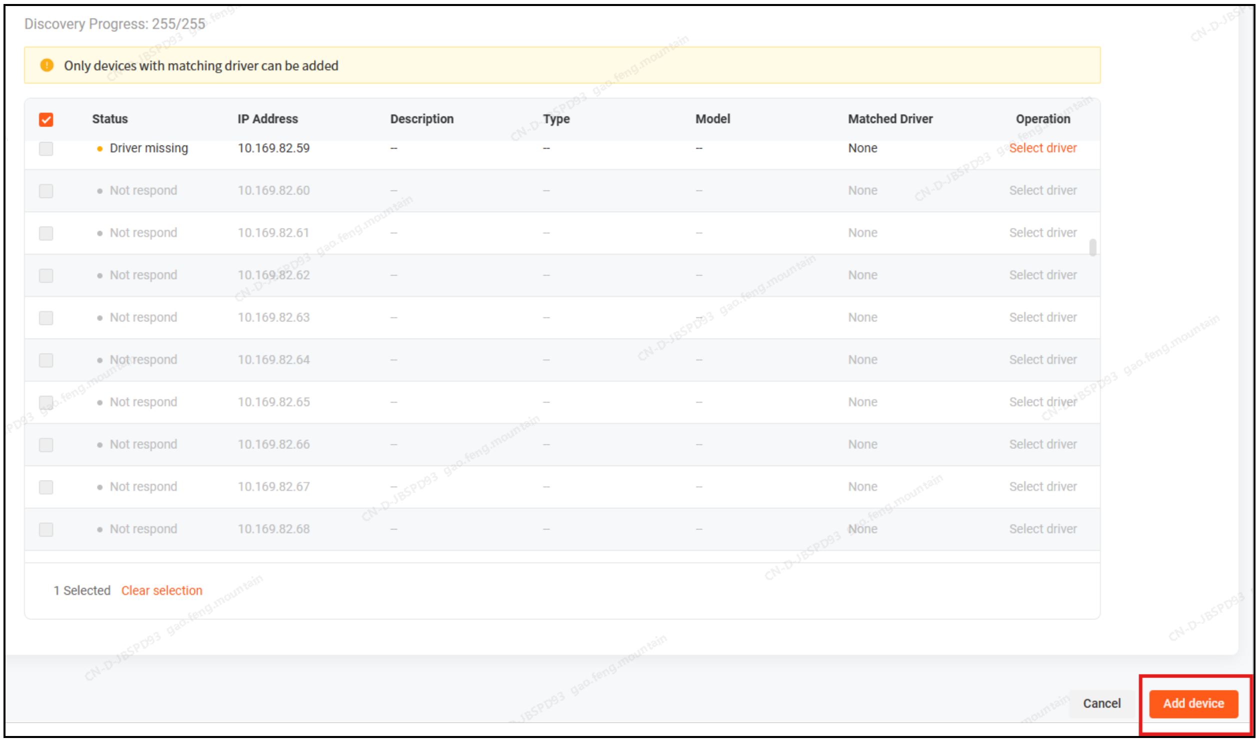
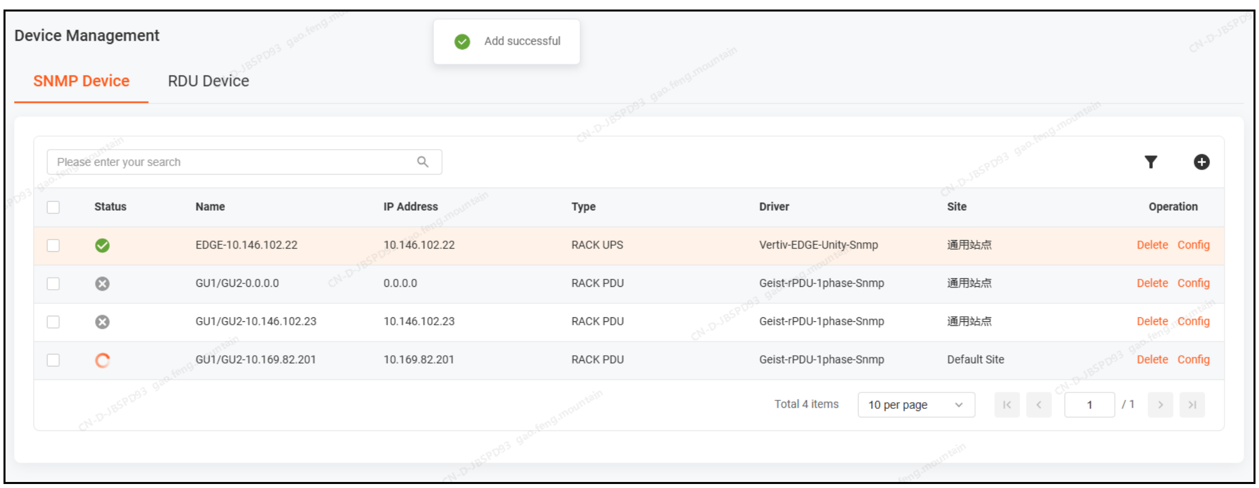


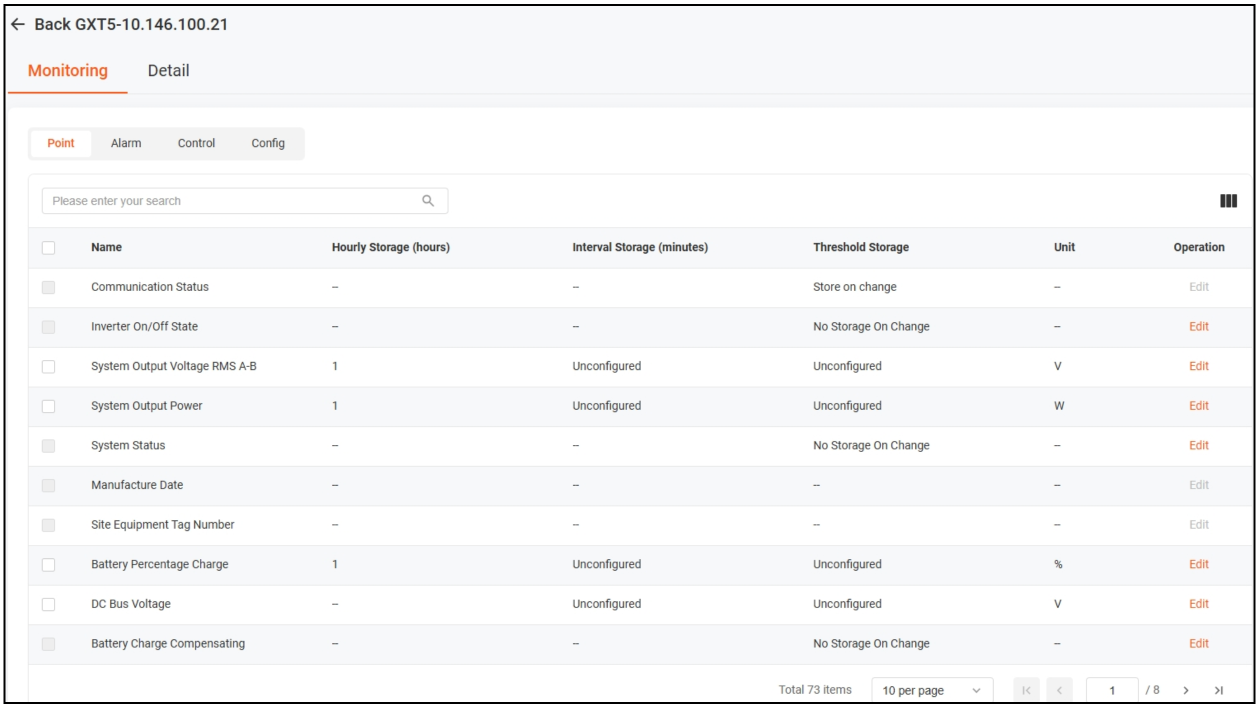
Figure 15.52 Added Successfully



Device Configuration

Click the Config button in the Operation column of the SNMP device list to enter the device configuration page, as shown in **Figure 15.53** on the facing page .

Figure 15.53 Device Configuration Page



Points

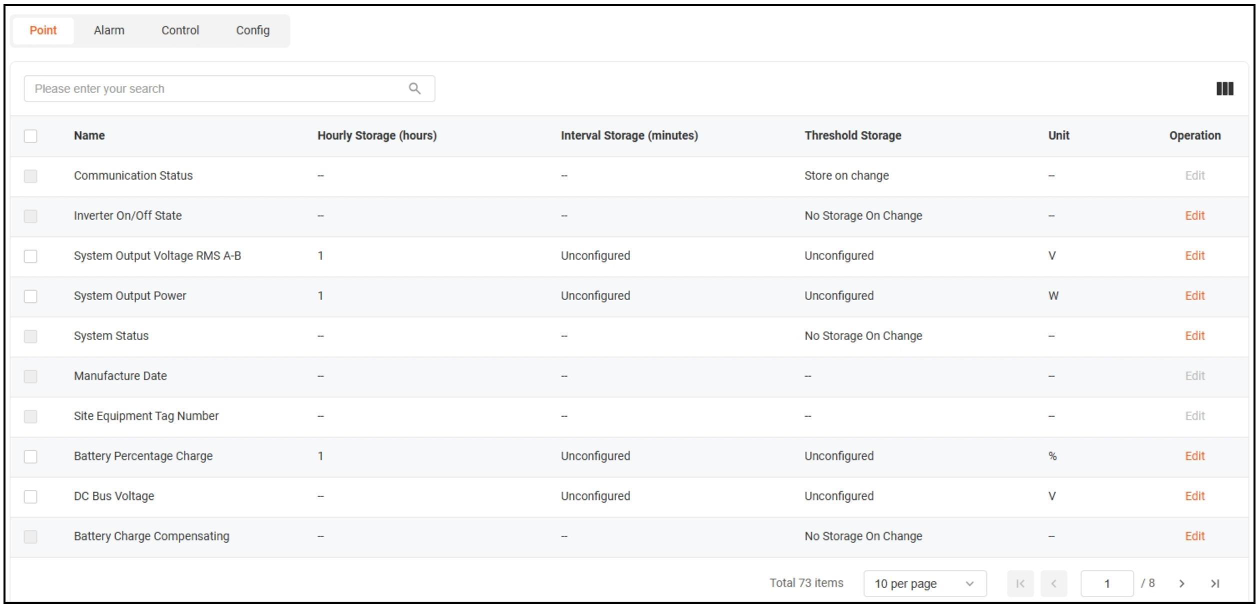
Click the Edit button on a point to open its configuration popup:

1. For enumerated points, you can edit the point name and "store on change" setting, as shown in **Figure 15.55** on the next page

2. For numeric points, you can edit the point name and unit, as shown in **Figure 15.56** on page 325 . Additionally, you can modify the storage policy:

- Hourly storage: Fixed at a 1-hour interval (unchangeable). You can also select multiple numeric points in the point list and modify the hourly storage policy in batch.
- Periodic storage: Default is unset (displayed as "--"). Options include 3 minutes (default when selected), 10 minutes, or 30 minutes. Data is stored at the chosen interval.
- Threshold storage: Stores the signal value when it changes beyond the specified threshold. The default threshold is 10.

Figure 15.54 Measuring Points



Point Alarm Control Config

Please enter your search

Name	Hourly Storage (hours)	Interval Storage (minutes)	Threshold Storage	Unit	Operation
Communication Status	–	–	Store on change	–	Edit
Inverter On/Off State	–	–	No Storage On Change	–	Edit
System Output Voltage RMS A-B	1	Unconfigured	Unconfigured	V	Edit
System Output Power	1	Unconfigured	Unconfigured	W	Edit
System Status	–	–	No Storage On Change	–	Edit
Manufacture Date	–	–	–	–	Edit
Site Equipment Tag Number	–	–	–	–	Edit
Battery Percentage Charge	1	Unconfigured	Unconfigured	%	Edit
DC Bus Voltage	–	Unconfigured	Unconfigured	V	Edit
Battery Charge Compensating	–	–	No Storage On Change	–	Edit

Total 73 items 10 per page 1 / 8

Figure 15.55 Enumerate Point Configuration Popup

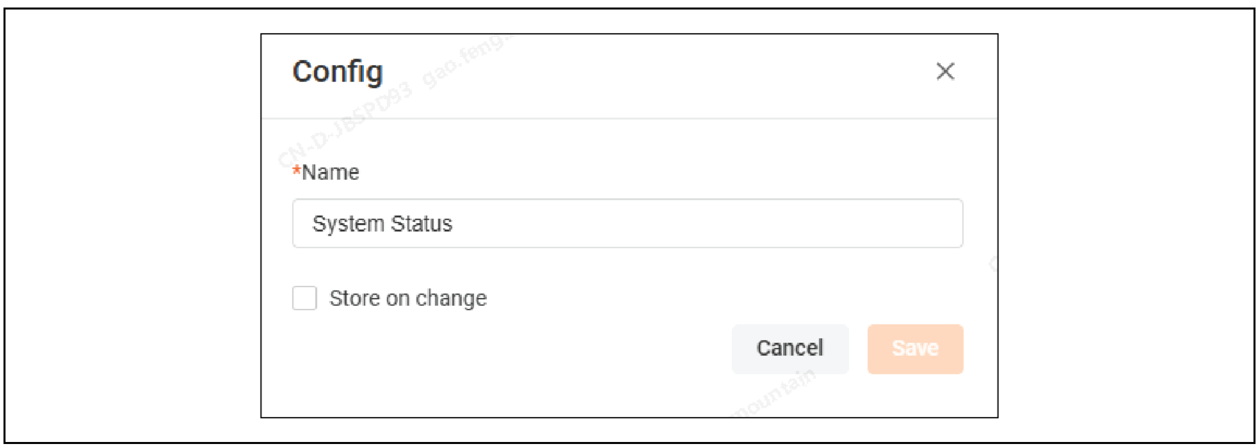


Figure 15.56 Numeric Point Configuration Popup

Alarm

As shown in **Figure 15.57** on the next page , to edit an alarm, click the Edit button in the table's operation column. This opens the edit pop-up window, as illustrated in **Figure 15.58** on the next page . Here, you can modify the alarm name and severity.

Click the Edit button in the table operation column to open the edit pop-up window, as shown in **Figure 15.58** on the next page .

Figure 15.57 Alarm

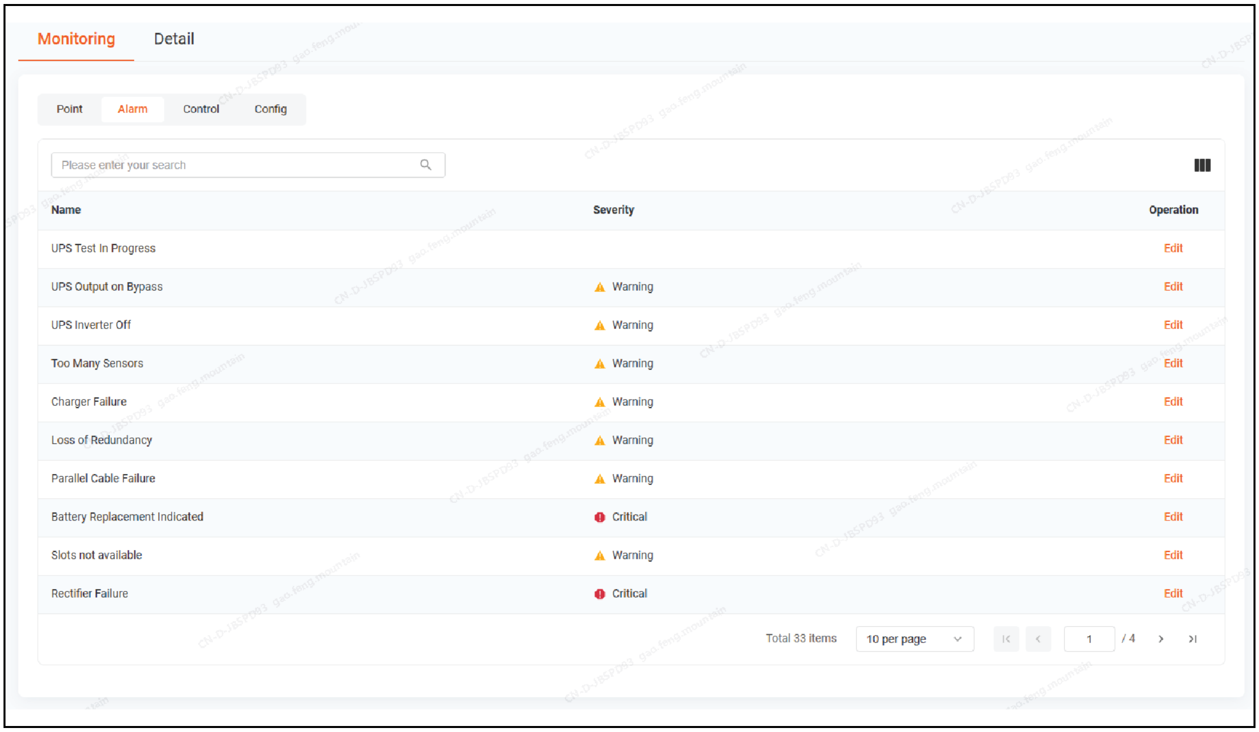


Figure 15.58 Alarm Edit Popup Window

Control

The control page primarily displays controllable signals that can be used to send to the device, as shown in **Figure 15.59** on the facing page .

To modify a control name, click the Edit button in the operation column, which opens an edit window (see **Figure 15.60** on the facing page).

Figure 15.59 Control

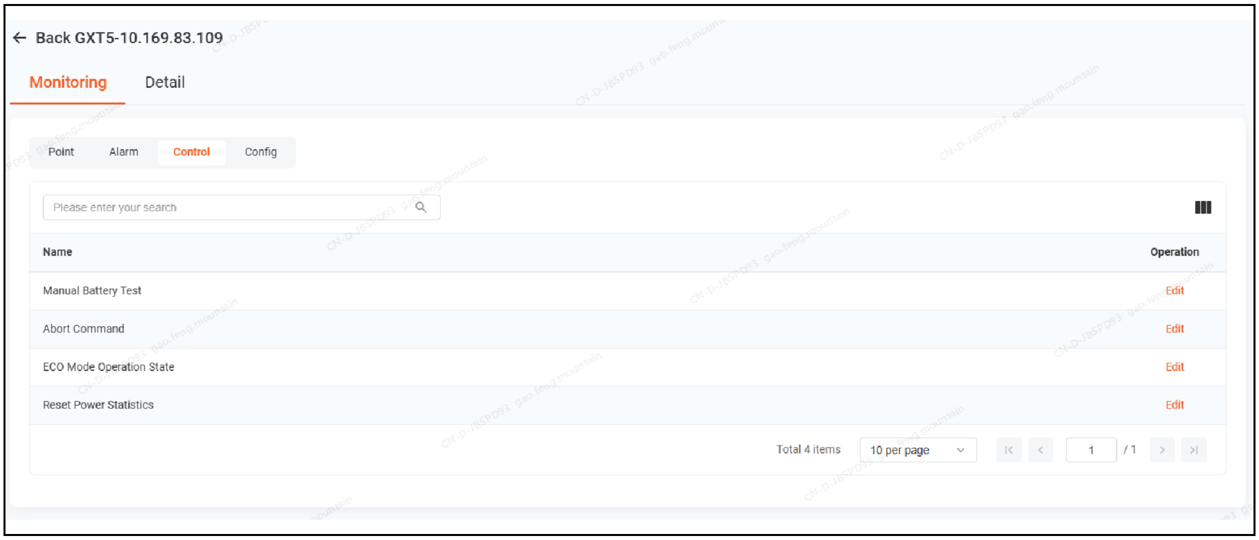


Figure 15.60 Control Edit Popup Window

Config

The config page mainly displays config signals that can be used to send to change the device's settings, as shown in **Figure 15.61** on the next page .

Click the Edit button in the Operation column of the table to open the edit pop-up window, as shown in **Figure 15.62** on the next page .

Figure 15.61 Config

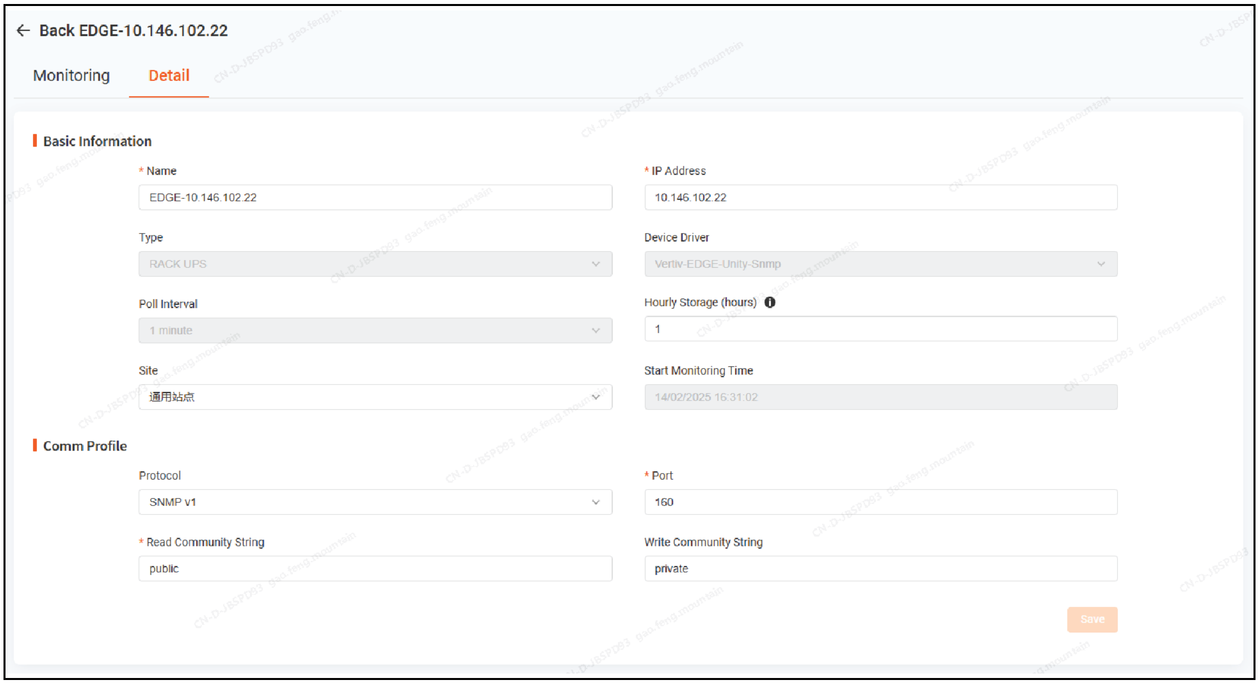
Figure 15.62 Config Edit Popup Window

Detail

The details page contains two parts: basic information and communication configuration, as shown in **Figure 15.63** on the facing page .

If you change the communication configuration, the device will be reconnected with the new protocol after saving.

Figure 15.63 Device Details Page



15.3.2 Comm Profile

Click *Comm Profile* under Configuration Tool to enter the communication profile list, as shown in **Figure 15.64** below . When the system is initialized, a default communication configuration is created, as follows:

1. Name: Default SNMP v2c Profile

2. Communication protocol: SNMP v2c

3. Port: 161

4. Read the word communication: public

5. Write the communicator: private

6. Defaults to device search: Check

You can search by name in the search input box.

Figure 15.64 Communication Profile Page

Add/Edit Communication Profile

To add a communication Profile:

Click the *Add* button in the upper right corner of the table to open the Add Communication Profile pop-up window, as shown in **Figure 15.65** below . If "Default for device search" is checked, this comm profile will be automatically selected when adding SNMP devices in batches in SNMP Detailed Function .

Figure 15.65 Adding Communication Profile

Select SNMP v1 or SNMP v2c as the protocol

You need to input the read community string so that Smart Infrasight can use it to read data from devices.

Select SNMP v3 as the protocol

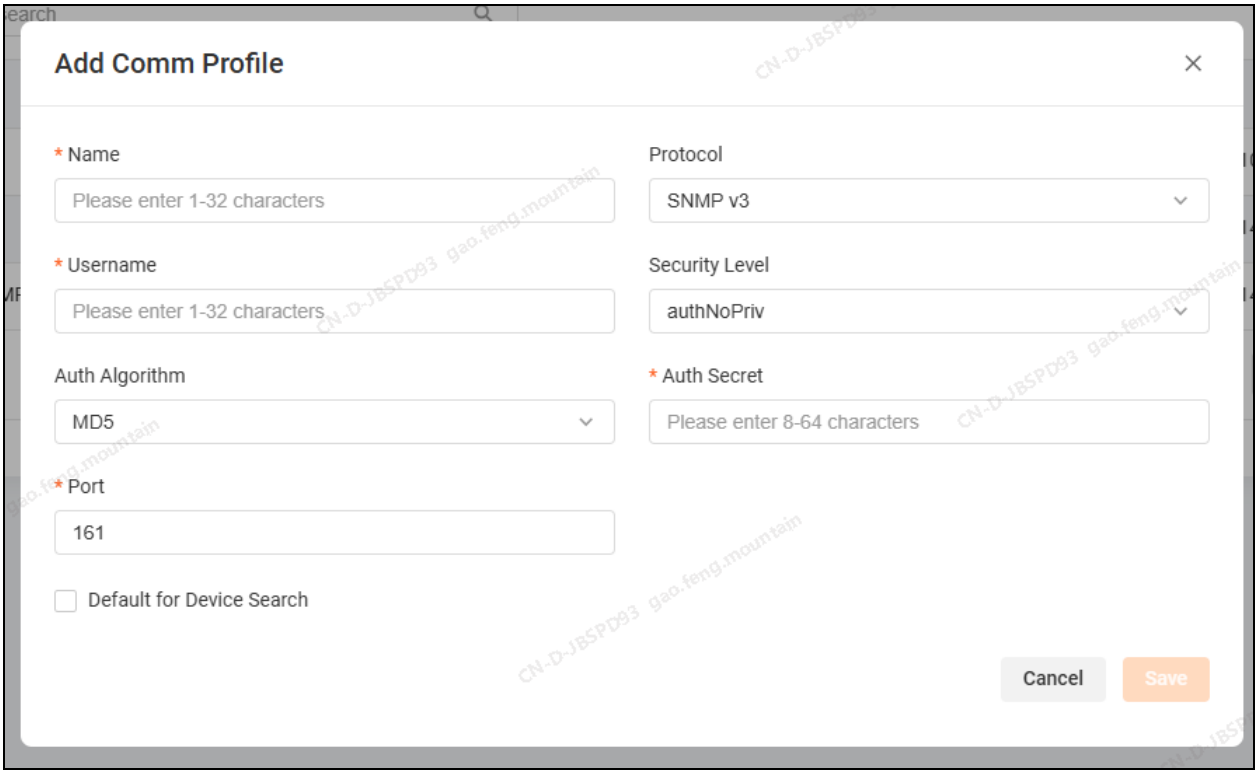
Extra security fields need to be input to make sure Smart Infrasight can communicate with the device safely.

There are 3 types of security levels:

- noAuthNoPriv
- authNoPriv
- authPriv

In this security level, authentication secret and privacy secret are both required, as shown in **Figure 15.66** on the facing page .

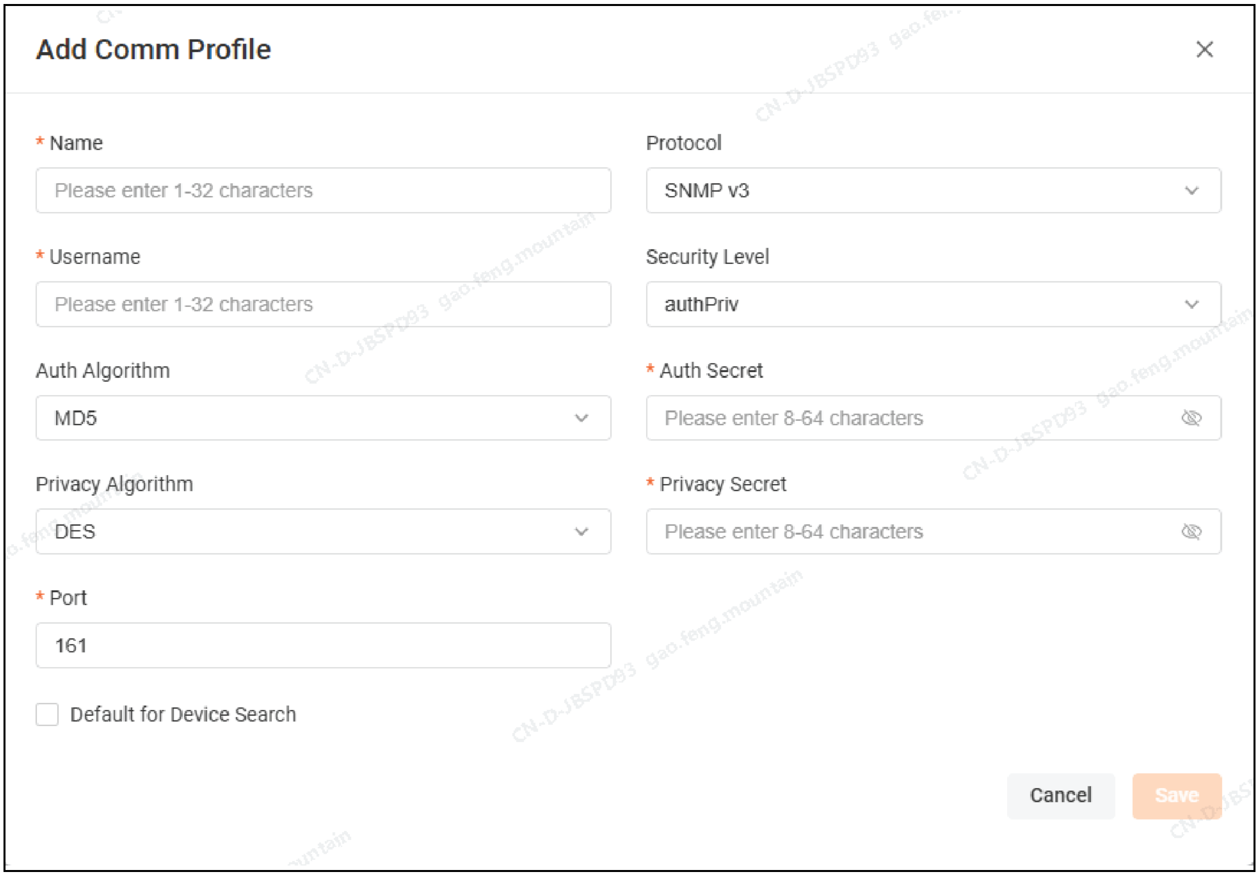
Figure 15.66 Adding the authNoPriv Comm Profile



authPriv

The authentication algorithm, authentication password, encryption algorithm, and encryption authorization password are added, as shown in **Figure 15.67** on the next page .

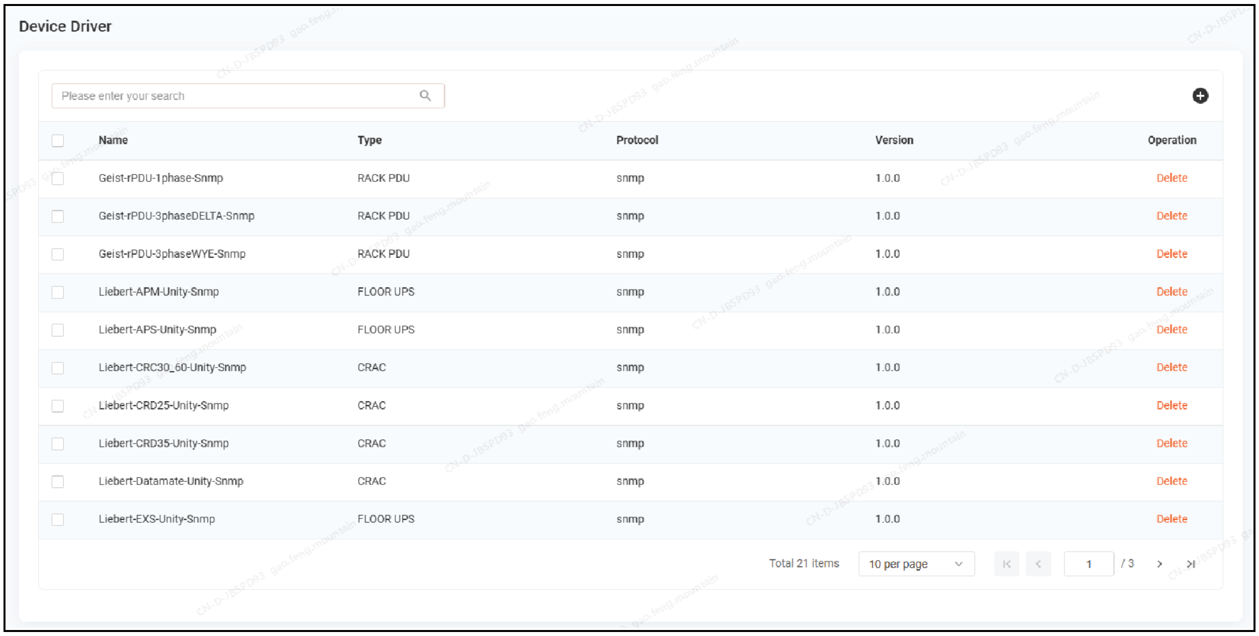
Figure 15.67 Added authPriv communication configuration



15.3.3 Device Drivers

Click Device Driver under the Configuration Tool to enter the device driver's page, as shown in **Figure 15.68** on the facing page .

Figure 15.68 Device Driver page



Device Driver

Please enter your search

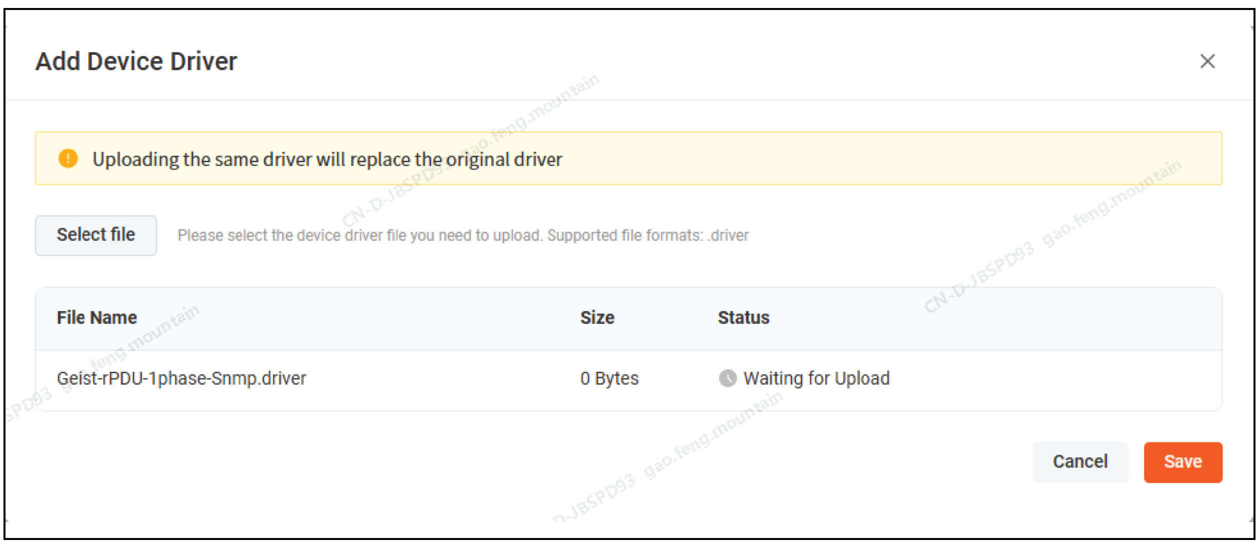
	Name	Type	Protocol	Version	Operation
	Geist-rPDU-1phase-Snmp	RACK PDU	snmp	1.0.0	Delete
	Geist-rPDU-3phaseDELTA-Snmp	RACK PDU	snmp	1.0.0	Delete
	Geist-rPDU-3phaseWYE-Snmp	RACK PDU	snmp	1.0.0	Delete
	Liebert-APM-Unity-Snmp	FLOOR UPS	snmp	1.0.0	Delete
	Liebert-APS-Unity-Snmp	FLOOR UPS	snmp	1.0.0	Delete
	Liebert-CRC30_60-Unity-Snmp	CRAC	snmp	1.0.0	Delete
	Liebert-CRD25-Unity-Snmp	CRAC	snmp	1.0.0	Delete
	Liebert-CRD35-Unity-Snmp	CRAC	snmp	1.0.0	Delete
	Liebert-Datamate-Unity-Snmp	CRAC	snmp	1.0.0	Delete
	Liebert-EXS-Unity-Snmp	FLOOR UPS	snmp	1.0.0	Delete

Total 21 items 10 per page 1 / 3

Adding a Device Driver

Click the *Add* button in the upper right corner of the table to open the Add Device Driver pop-up window, and upload the driver as required, only one driver can be uploaded at a time, as shown in **Figure 15.69** below .

Figure 15.69 Added Device Drivers



Deleting the Device Driver

Individual Deletions

Click the *Delete* button in the action column of the corresponding item in the table to delete it.

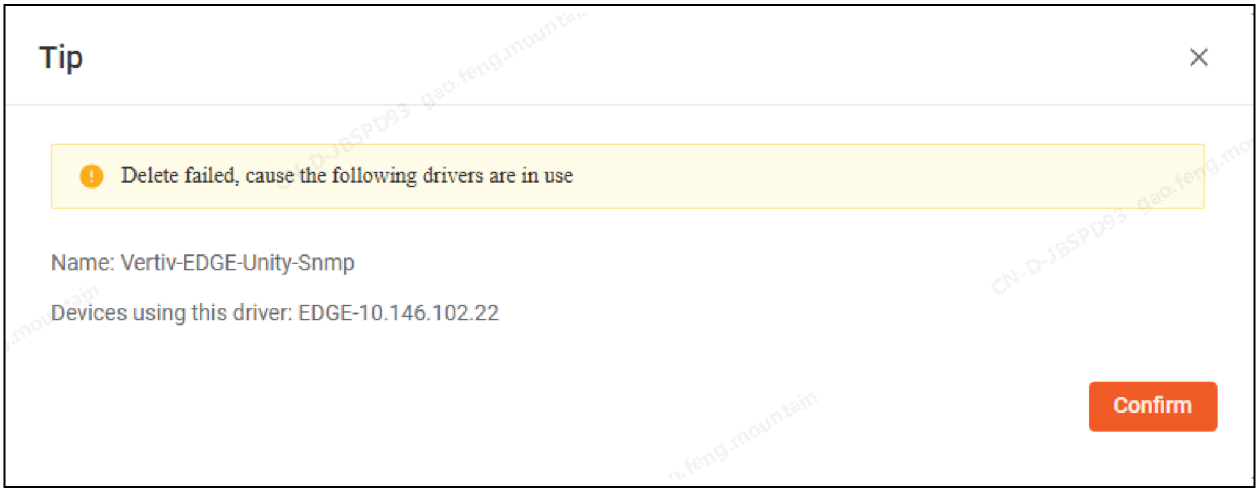
Multiple Deletions

After checking the selection box in the first column, click the *Batch Delete* button to delete in batches.

If the deletion fails, as shown in **Figure 15.70** below .

- The most likely reason is that the driver you are trying to delete is currently in use by one or more devices.
- Another reason could possibly be database interruptions during deletion

Figure 15.70 The pop-up cannot be deleted



16 Asset Management

16.1 Overview

Asset management in Smart InfraSight™ allows users to monitor, view, and modify assets and devices across all sites. This feature enables users to add, edit, or remove asset information as needed.

16.1.1 Functional modules

Refer to this manual for the detailed description of the following functional modules of asset management in Detailed Features on page 343

- Add an Asset
- Asset Import
- Asset Export
- Review Assets
- Edit the Asset
- Delete the Asset
- Warranty Notifications
- Asset rack and de-rack records

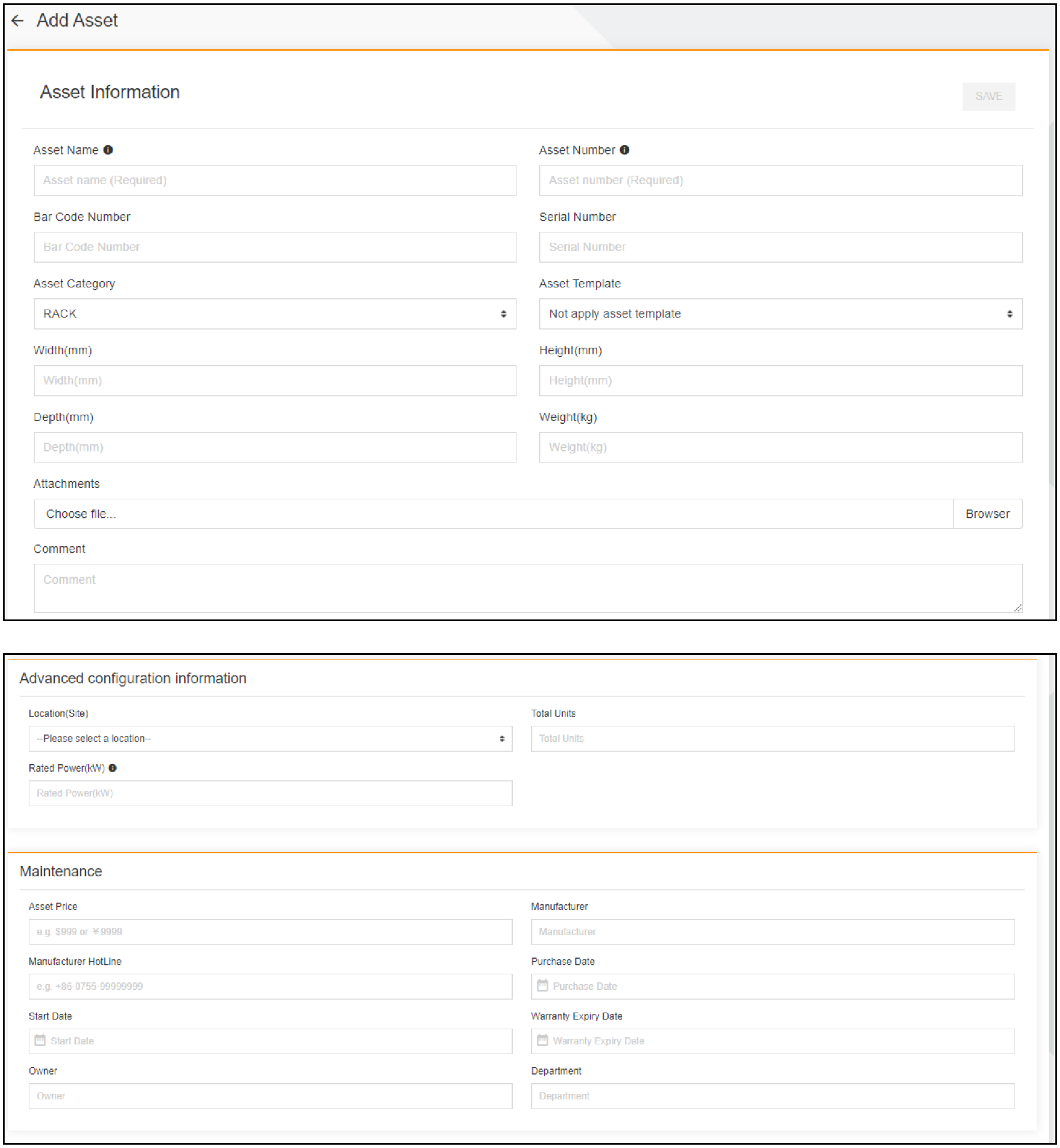
16.2 Quick Start

16.2.1 Example

Adding an Asset

In Assets feature, navigate to Asset Management, click *Add* button in the upper right corner to enter the Add Asset page, as shown in **Figure 16.1** on the next page .

Figure 16.1 Adding an Asset



Asset Name and **Asset Code** are mandatory, and the rest are optional. Once you have filled in the asset information, click the *save* button in the upper right corner.

Asset Import

Asset import is another way to add new assets. Click on the *import* button in the upper right corner of Asset Management to enter the asset import page, and you can choose to upload from the asset template or import from RDU, as shown in **Figure 16.2** on the facing page .

Figure 16.2 Importing an Asset

To upload from an asset template:

1. Click *Next* to access the **Upload From Asset Template** page.

2. In the upper right corner, click *Download Asset Template*.

3. Open the downloaded Excel file and fill in the asset information.

4. Click *Browse* to select your completed Excel file.

5. Click *Import* to upload the file.

6. Check for a confirmation message to ensure the import was successful.

Figure 16.3 Import Assets

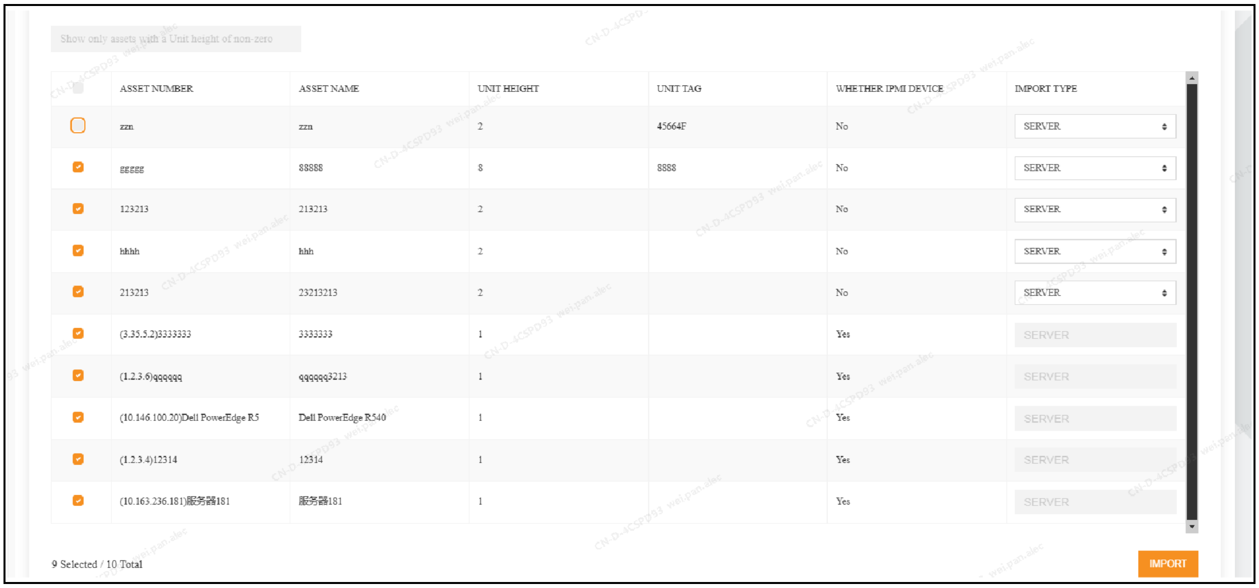
If you choose to import from RDU, click Next to enter the **Import from RDU page**, there is a RDU selection box at the top, you can import asset data from different RDU501, and the asset list only shows assets with U position height above 0. As shown in **Figure 16.4** below .

Figure 16.4 Import from RDU

In the asset list, select items for import by checking the boxes next to them. Choose the asset types (servers, switches, or rack PDUs) from the right-hand menu. The number of selected assets appears in the lower left corner, as shown in **Figure 16.5** on the next page , Click the import button to complete the process.

When importing assets from RDU501, the system will update existing asset information if the assets have already been imported. For assets not previously imported, new entries will be created.

Figure 16.5 Importing from RDU



Show only assets with a Unit height of non-zero

	ASSET NUMBER	ASSET NAME	UNIT HEIGHT	UNIT TAG	WHETHER IPMI DEVICE	IMPORT TYPE
☐	zzn	zzn	2	45664F	No	SERVER
☑	ggggg	88888	8	8888	No	SERVER
☑	123213	213213	2		No	SERVER
☑	hhhh	hhh	2		No	SERVER
☑	213213	23213213	2		No	SERVER
☑	(3.35.5.2)3333333	3333333	1		Yes	SERVER
☑	(1.2.3.6)qqqqqq	qqqqqq3213	1		Yes	SERVER
☑	(10.146.100.20)Dell PowerEdge R5	Dell PowerEdge R540	1		Yes	SERVER
☑	(1.2.3.4)12314	12314	1		Yes	SERVER
☑	(10.163.236.181)服务器181	服务器181	1		Yes	SERVER

9 Selected / 10 Total

IMPORT

NOTE: 1. The asset list can fetch up to 1000 pieces of data at a time.

2. Only assets can be imported from RDU501, if RDU authentication fails, please check the user's authentication configuration. Refer to Detailed Configuration

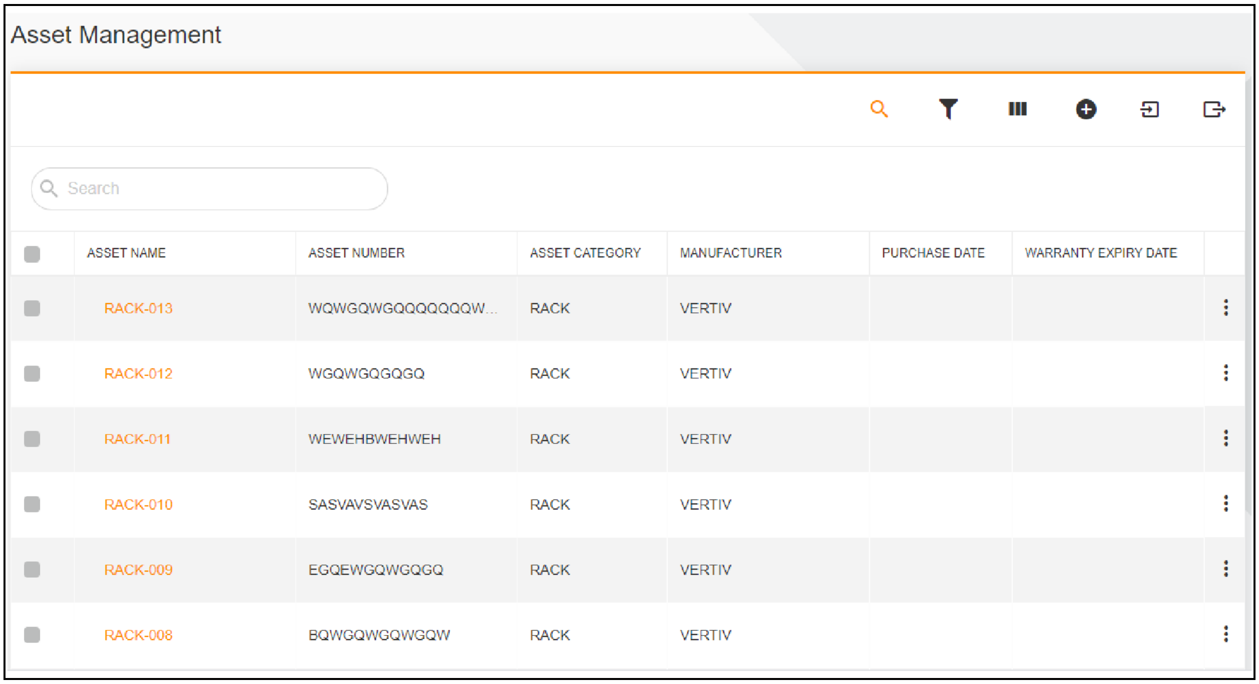
Asset Export

Click the *Export* icon in the upper right corner of the asset management list to export all assets in excel format.

Asset List

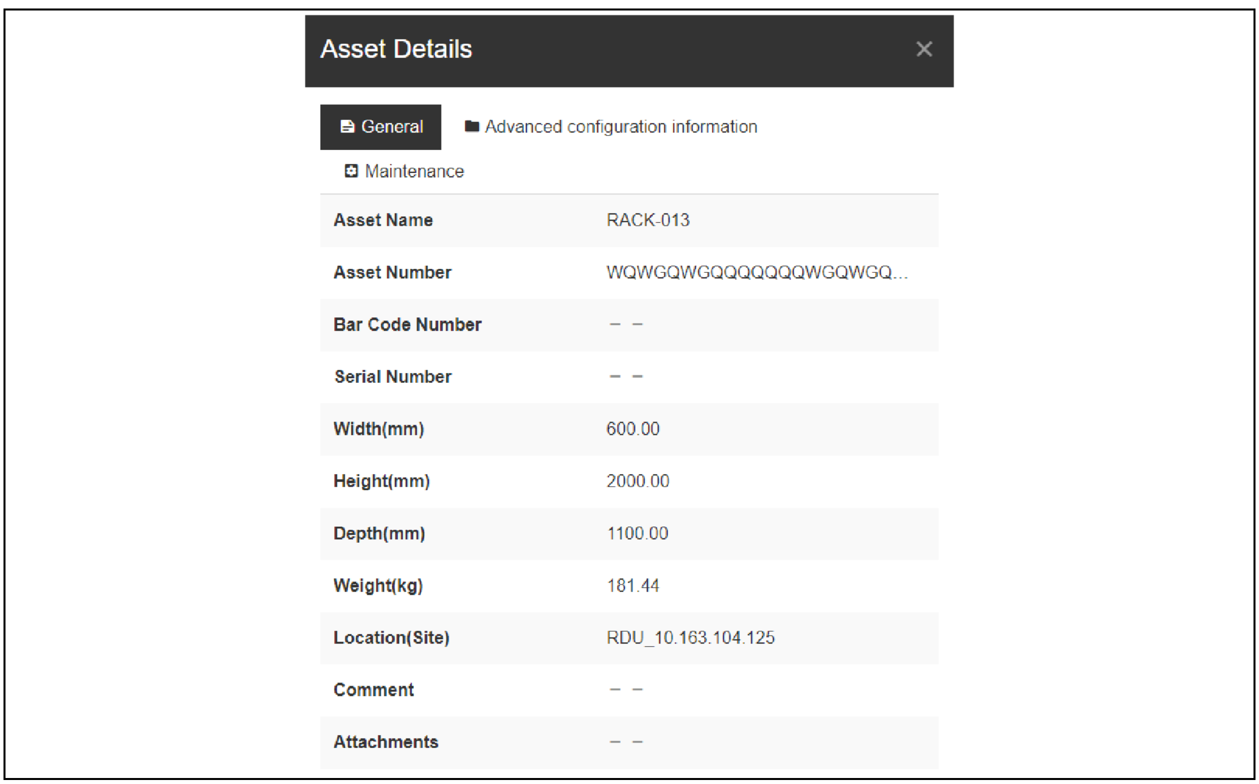
The list of assets is shown in **Figure 16.6** on the facing page .

Figure 16.6 List of Assets



Click on the **Asset Name** to see the asset details, as shown in **Figure 16.7** below .

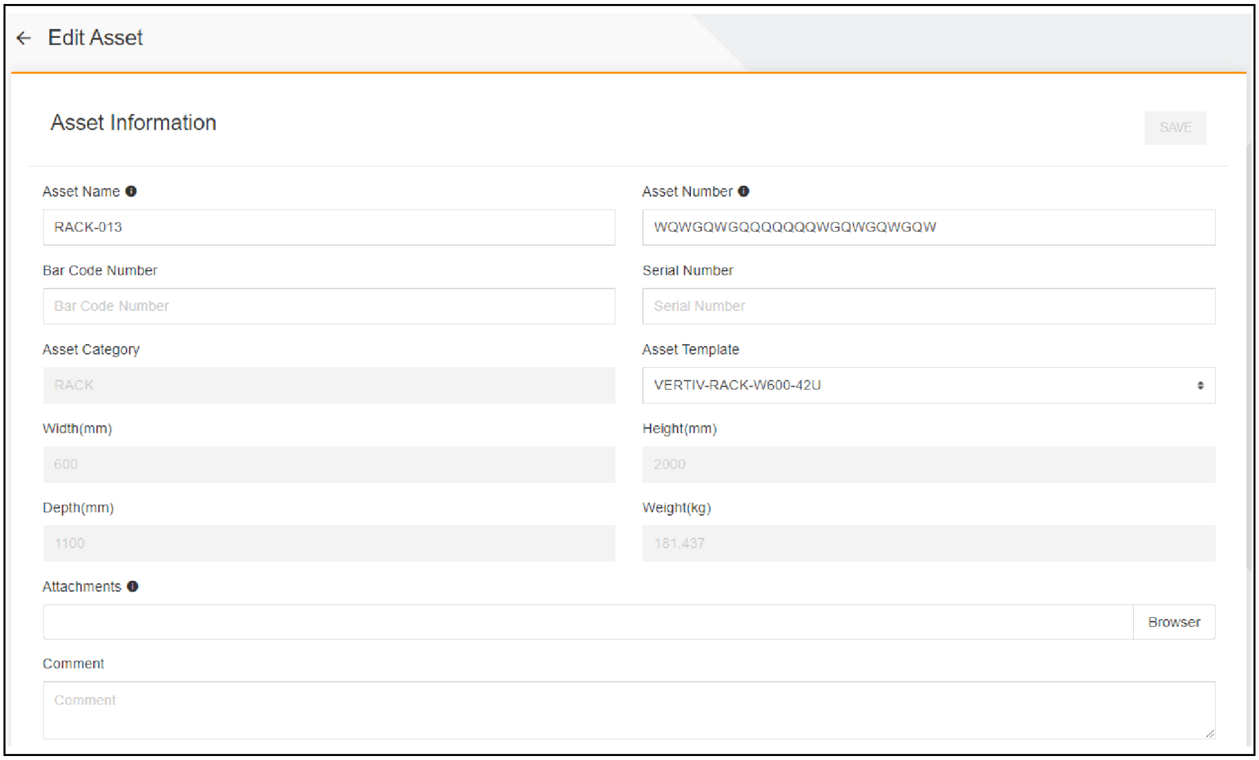
Figure 16.7 Asset Details

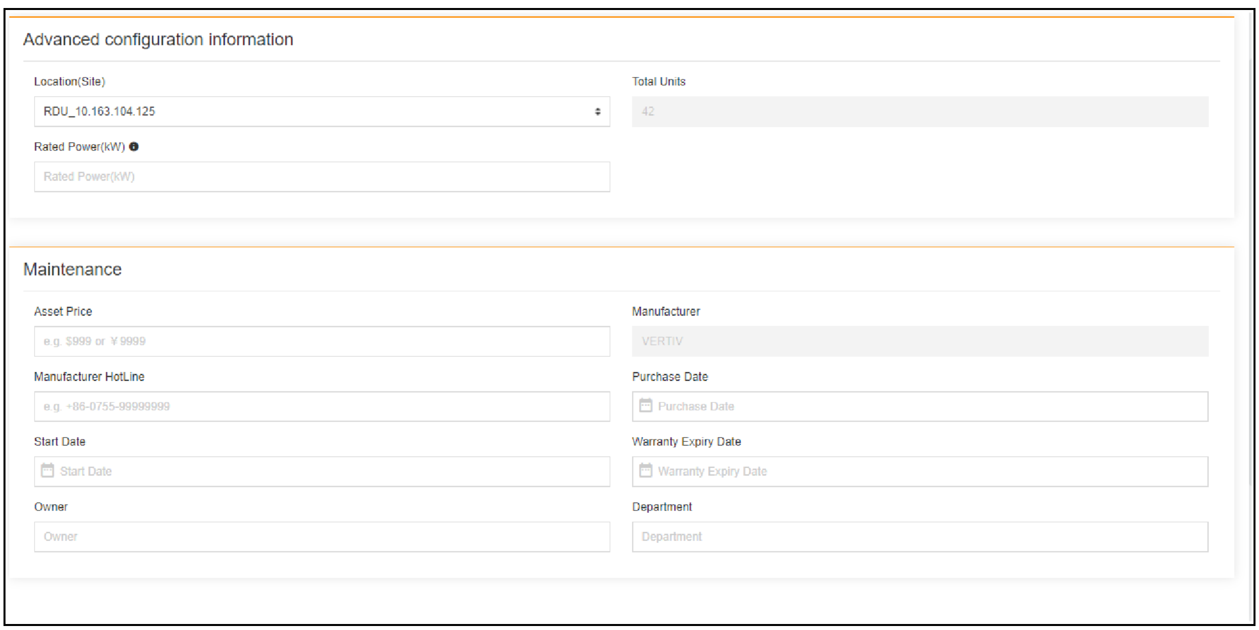


Editing the Asset

Click on the ellipses (...) on the right side of the asset and select Edit to enter Edit Asset page, as shown in **Figure 16.8** below .

Figure 16.8 Editing the Asset



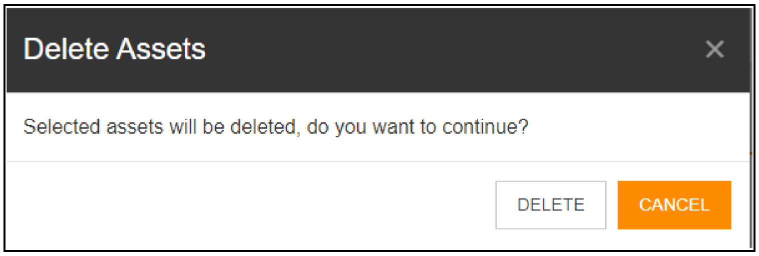


When you have done editing the asset information, click the *save* button in the upper right corner.

Deleting the Asset

Click ellipses (...) on the right side of the asset and select Delete to delete the asset, as shown in **Figure 16.9** below .

Figure 16.9 Deleting the Asset



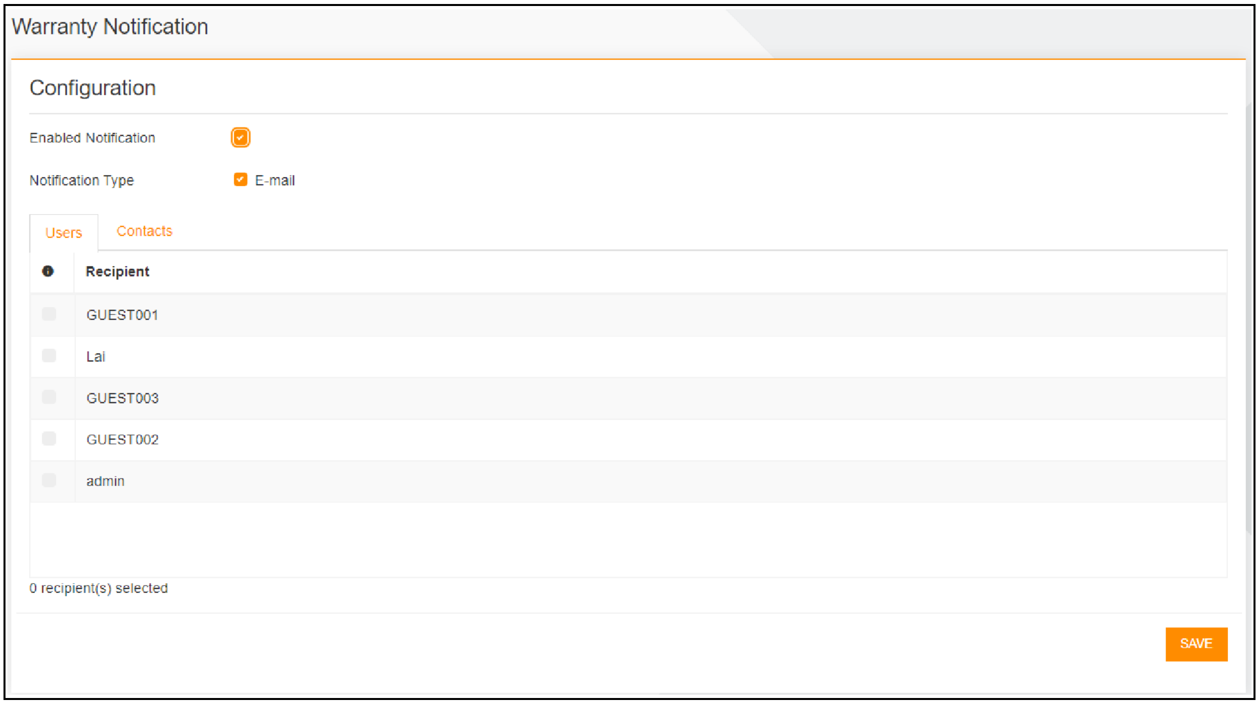
16.2.2 Warranty Notifications

If you need the Warranty Notification function, click the asset menu and select the **Warranty Notification** menu to enter the Warranty Notification page. As shown in Figure 16.10 below .

Figure 16.10 Warranty Notification

To enable notifications, check the corresponding box and select the recipient from the pre-configured email list. Click 'Save' and activate the Warranty Notification function, as shown in Figure 16.11 on the next page . Note that for this feature to work correctly, you must have already set up the asset maintenance expiration time.

Figure 16.11 Enabling the Warranty Notifications

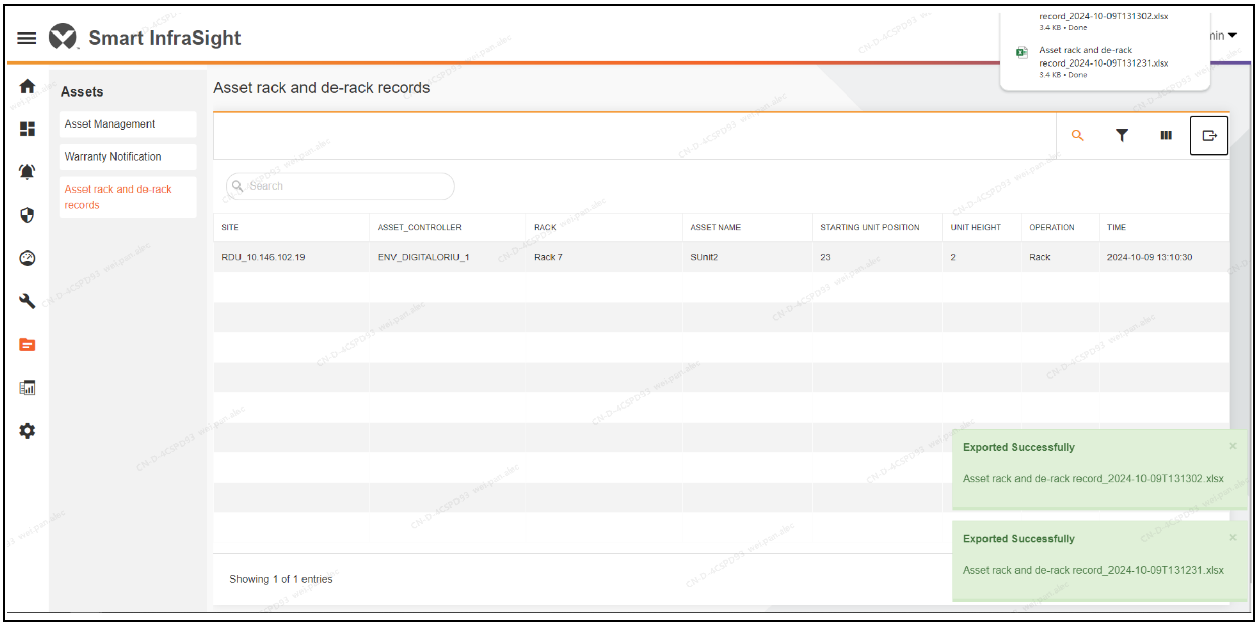


Warranty Notification's email reminder policy is as follows: You will receive one reminder on the 1st of each month, starting three months before your asset's expiration date. If the initial email fails to send, we will attempt to resend it on the same day. No further reminders will be sent after that date.

16.2.3 Records of Assets Rack and De-rack

This function primarily records asset position changing log from the U-position Asset Manager. It tracks changes in asset locations and allows users to export and view asset records, as shown in Figure 16.12 on the facing page.

Figure 16.12 Asset Rack and De-rack Records



16.3 Detailed Features

16.3.1 Adding an Asset

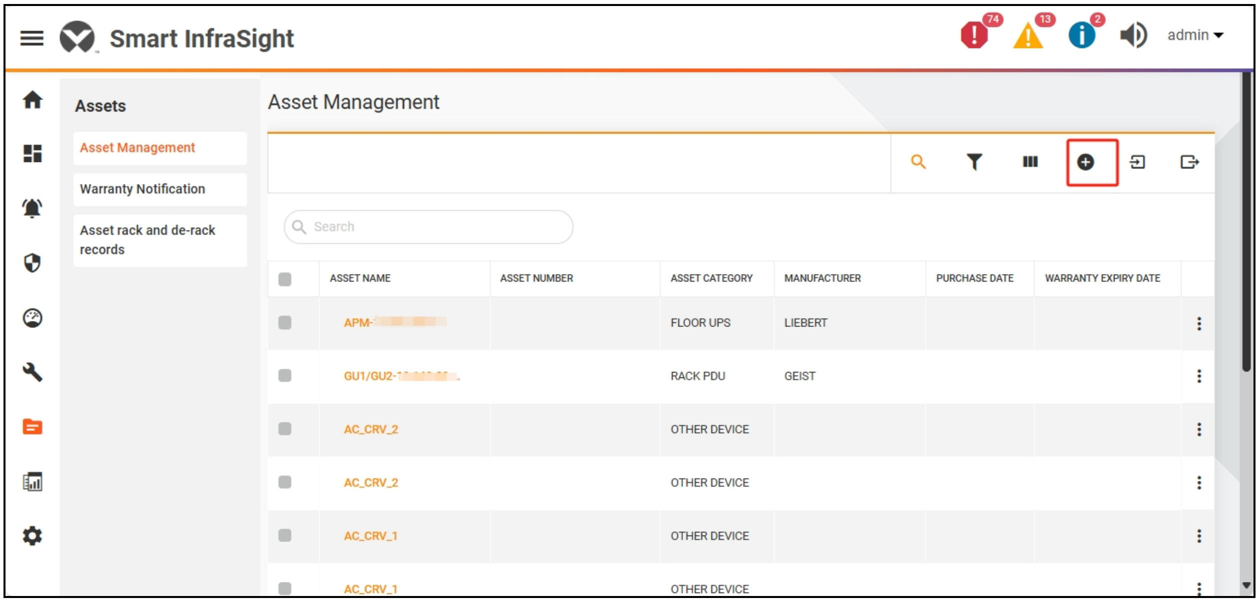
Users can add assets and devices as needed. To add a new asset, click the asset menu and then the Add icon in the upper right corner (Figure 16.13 on the next page). Available asset types include cabinets, rack PDUs, servers, switches, and battery cabinets. Note that cabinets and battery cabinets cannot be added to sites of Smart Aisle3.

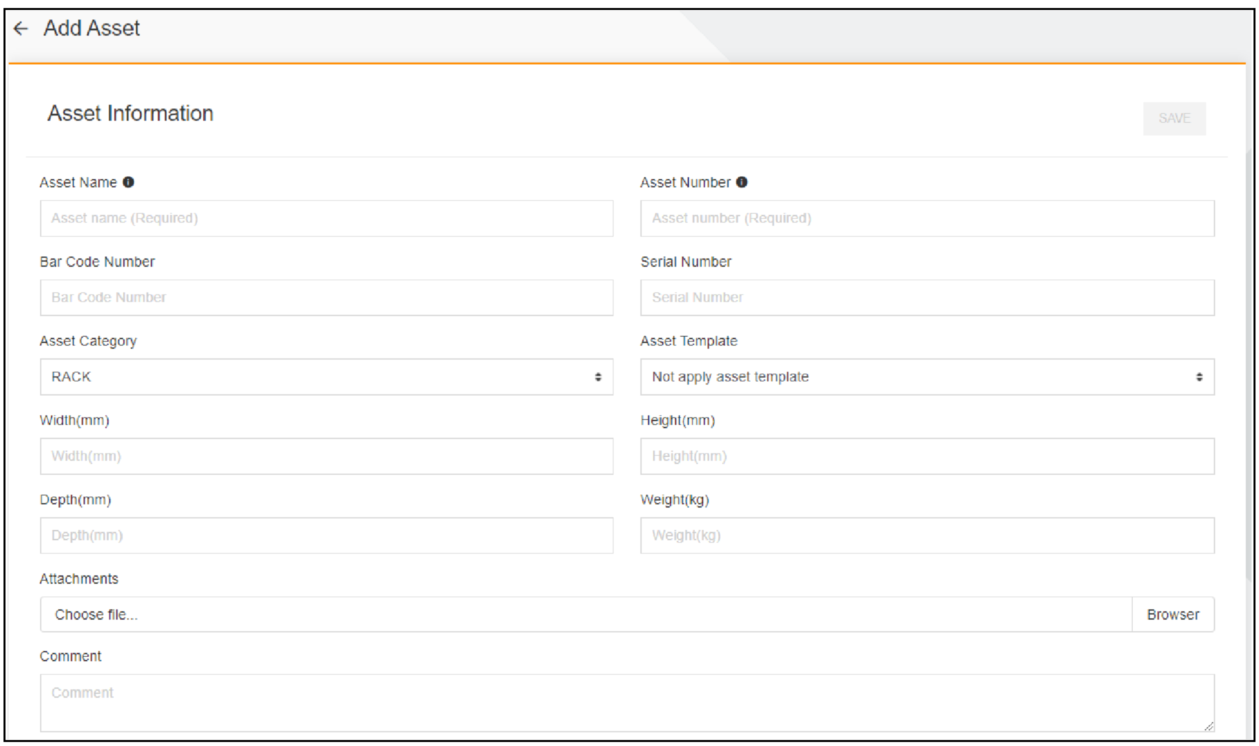
When adding an asset, the Asset Name and Asset Number fields are required, while others are optional. Each Asset Number must be unique. If you enter an existing asset code, an error message will appear, and the Save button will be disabled.

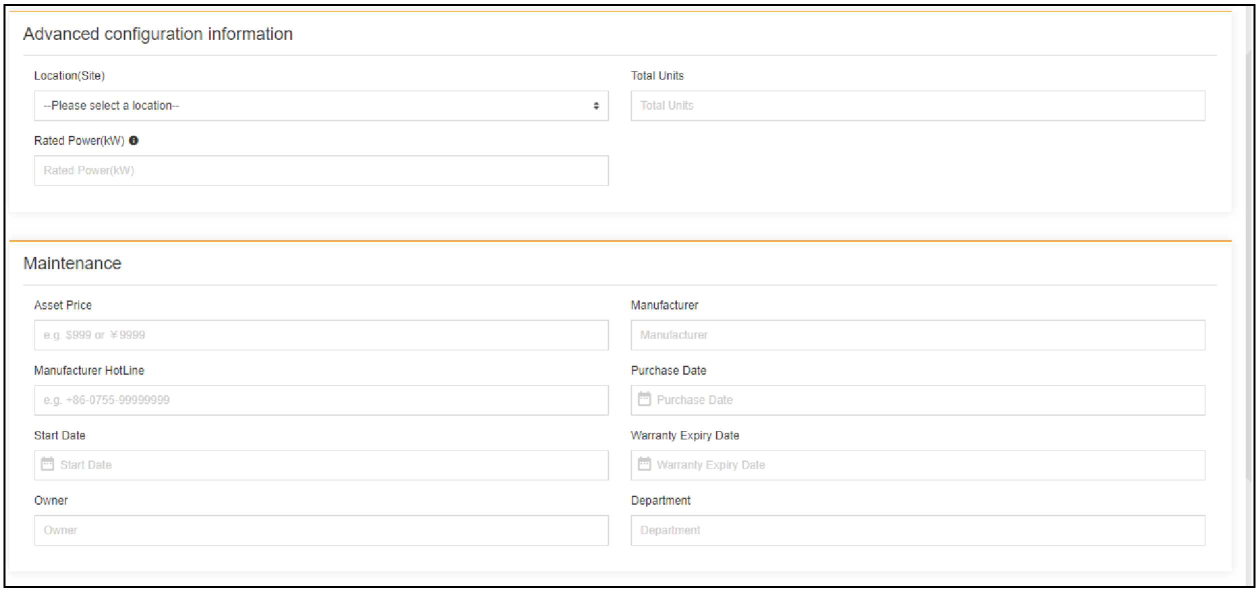
You can attach files (such as descriptions or related documents) to an asset. Supported file types include .doc, .docx, .pdf, .xls, .xlsx, .ppt, .pptx, .txt, .jpg, .jpeg, .gif, and .png.

The Location field links an asset to a specific site. When entering dates, ensure that the maintenance date and activation time are not earlier than the purchase time; otherwise, an error message will appear, and the Save button will be disabled.

Figure 16.13 Adding an Asset



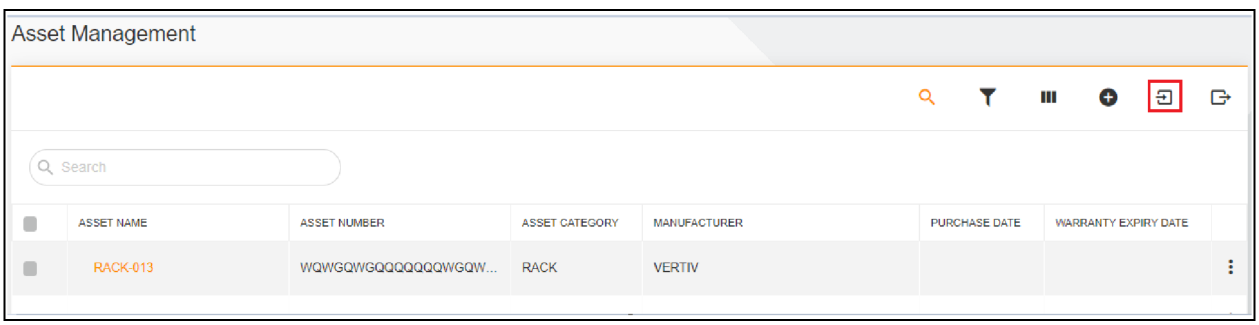




16.3.2 Asset Import

Asset import is another way to add new assets. Click the *asset menu* and click the *Import* button in the upper right corner to enter the asset import page, as shown in **Figure 16.14** below .

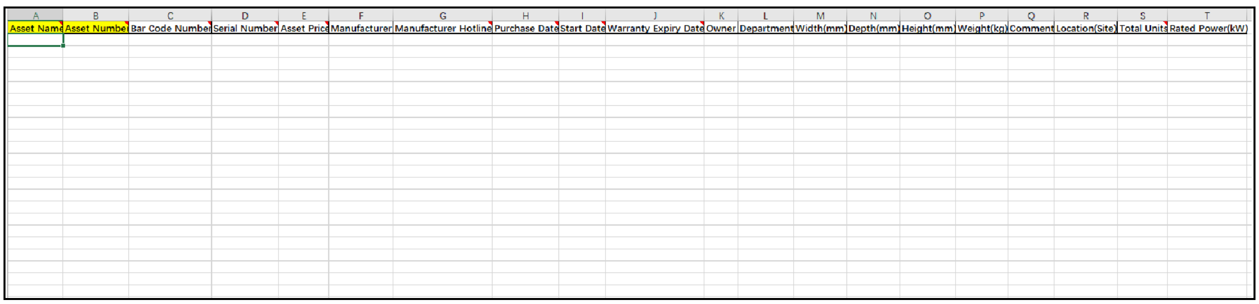
Figure 16.14 Importing an Asset



Download the asset template by clicking the **Download Asset Template** button in the top right corner. Open the Excel file and fill in the asset information. Ensure asset names and codes are unique. And then click "Browse" to select your completed Excel file, then click **Import**.

NOTE: The cabinet\battery cabinet cannot be imported to the Smart Aisle sites.

Figure 16.15 Importing Asset Information

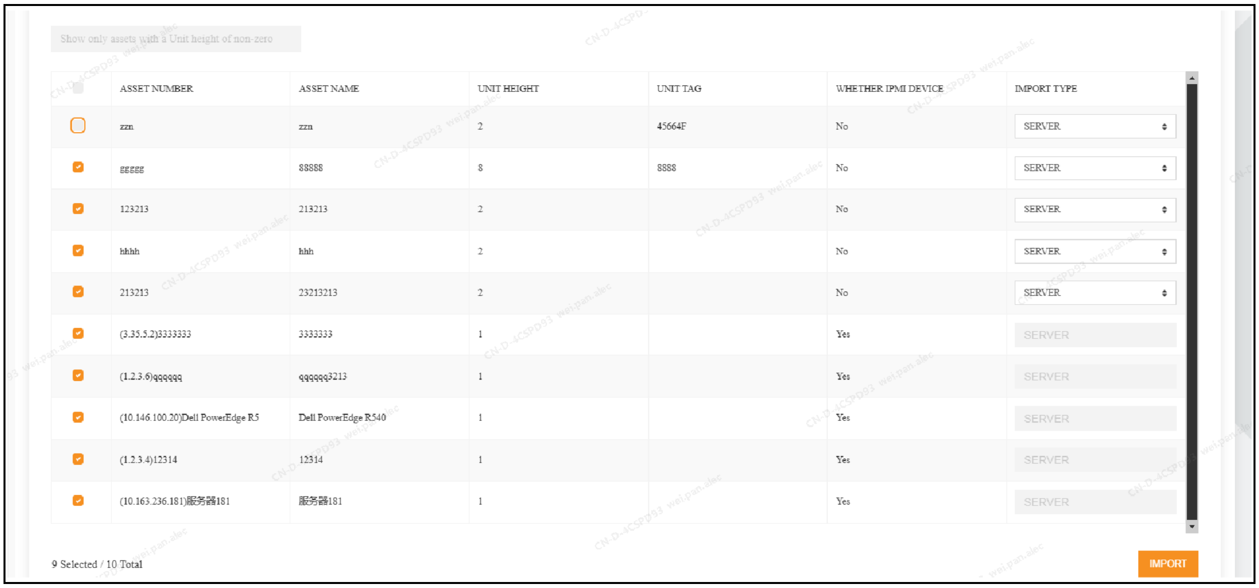


If you choose to import from RDU as shown in **Figure 16.16** below , click Next to enter the import from RDU interface, there is a RDU selection box at the top, you can import assets from different RDUs, and the asset list only shows assets with U-position height above 0.

Figure 16.16 Importing Assets from RDU

In the asset list, check the boxes next to the items you want to import. On the right, choose the asset type (servers, switches, or rack PDUs). The number of selected assets appears in the lower left corner. Once you've made your selections, click the import button to complete the process, as shown in **Figure 16.17** on the facing page .

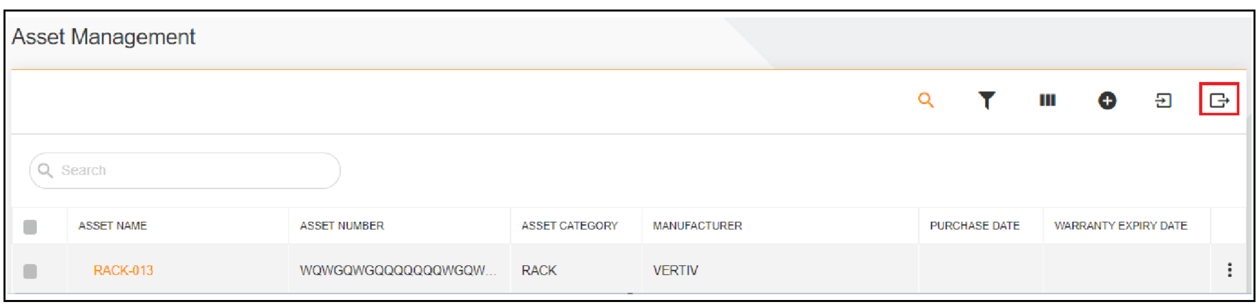
Figure 16.17 Selecting Assets



16.3.3 Asset Export

Click the filter button in the upper right corner of the asset management list to view different assets by filter. The filtered asset list can be exported to an Excel file. Note that this exported Excel file cannot be used for asset import. The export file format is as shown in **Figure 16.18** below .

Figure 16.18 Exporting Assets



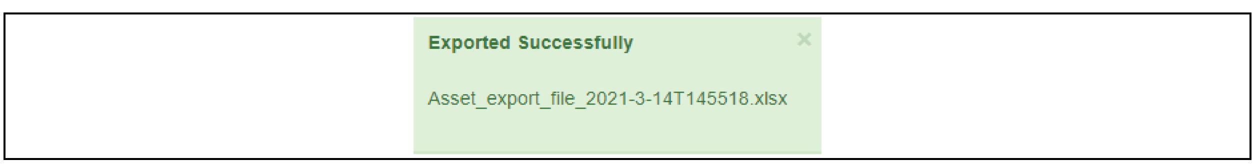
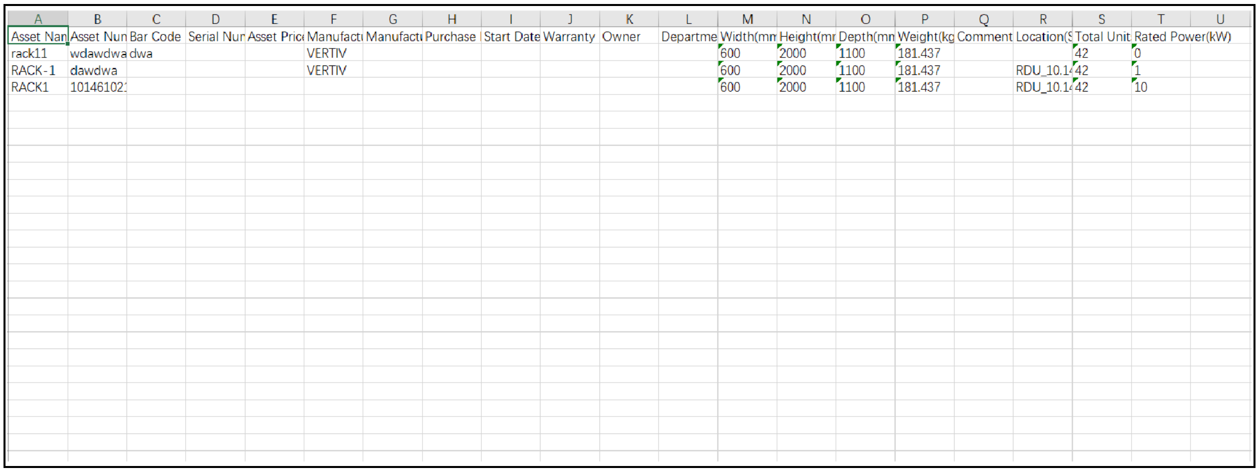


Figure 16.19 Exported Asset File

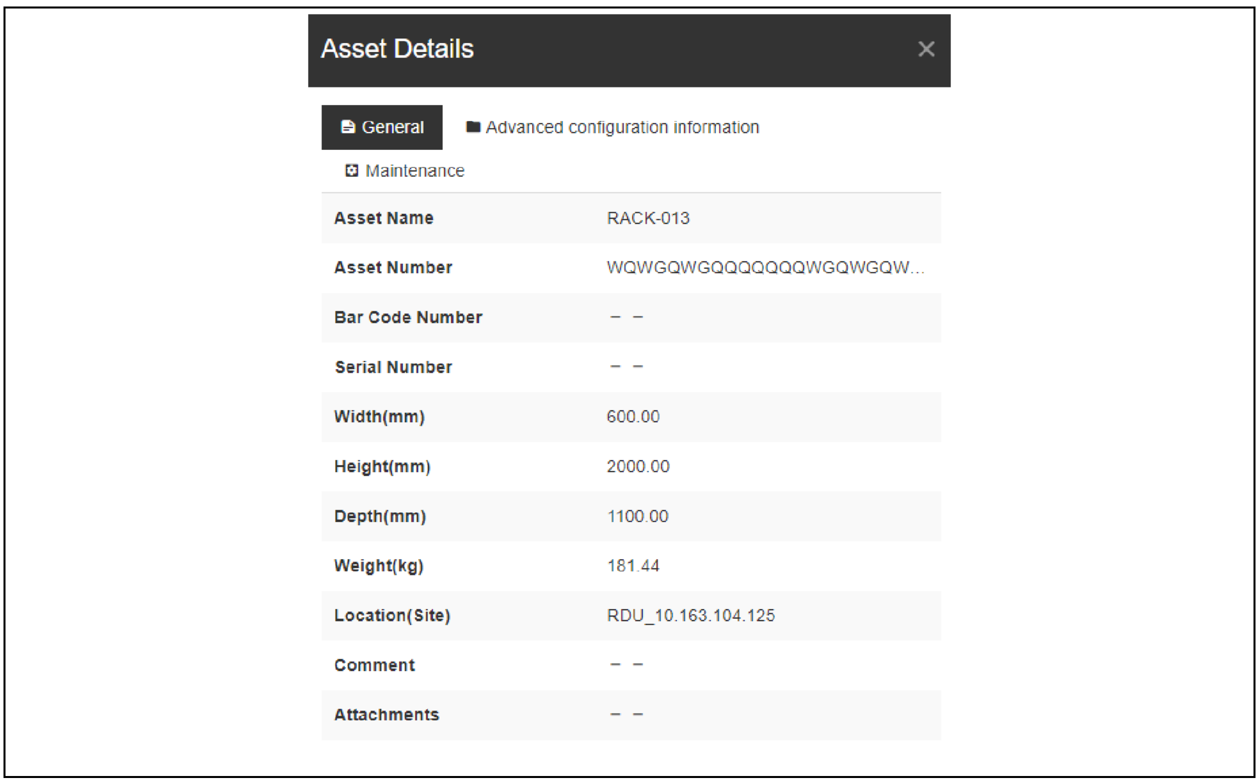


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
Asset Nan	Asset Nun	Bar Code	Serial Nur	Asset Pric	Manufactı	Manufactı	Purchase	Start Date	Warranty	Owner	Departme	Width(mn	Height(mr	Depth(mn	Weight(kg	Comment	Location(S	Total Unit	Rated Power(kW)	
rack11	wdawdwa	dwa			VERTIV							600	2000	1100	181.437			42	0	
RACK-1	dawdwa				VERTIV							600	2000	1100	181.437		RDU_10.1	42	1	
RACK1	10146102											600	2000	1100	181.437		RDU_10.1	42	10	

16.3.4 Review Assets

In Asset Management, click the asset name to view the asset details, as shown in **Figure 16.20** below

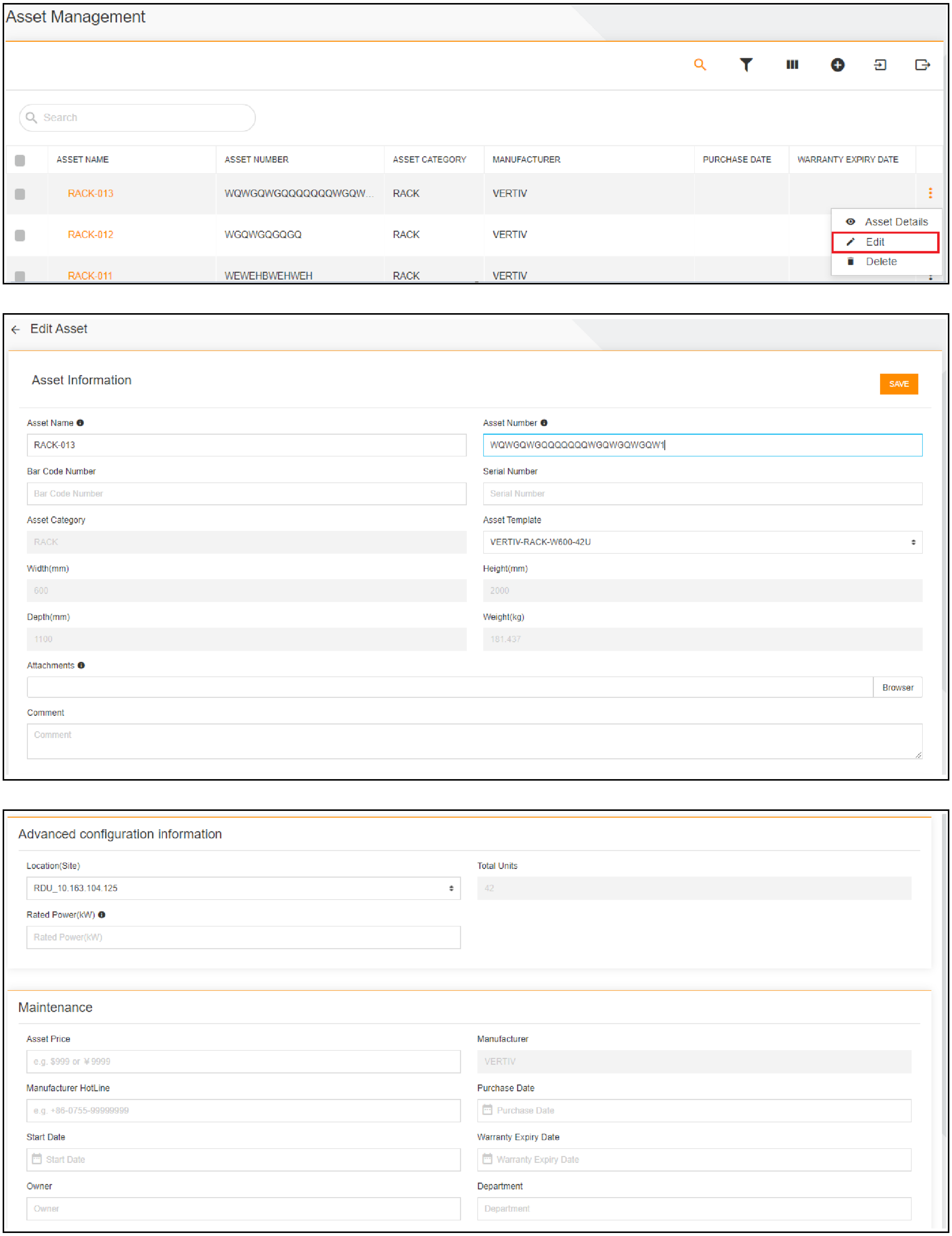
Figure 16.20 Asset Details



16.3.5 Editing the Asset

Click ellipse (...) on the right side of the asset and select Edit to open the Edit Asset page, as shown in **Figure 16.21** on the facing page .

Figure 16.21 Editing an Asset



Click the save button in the upper right corner after the editing.

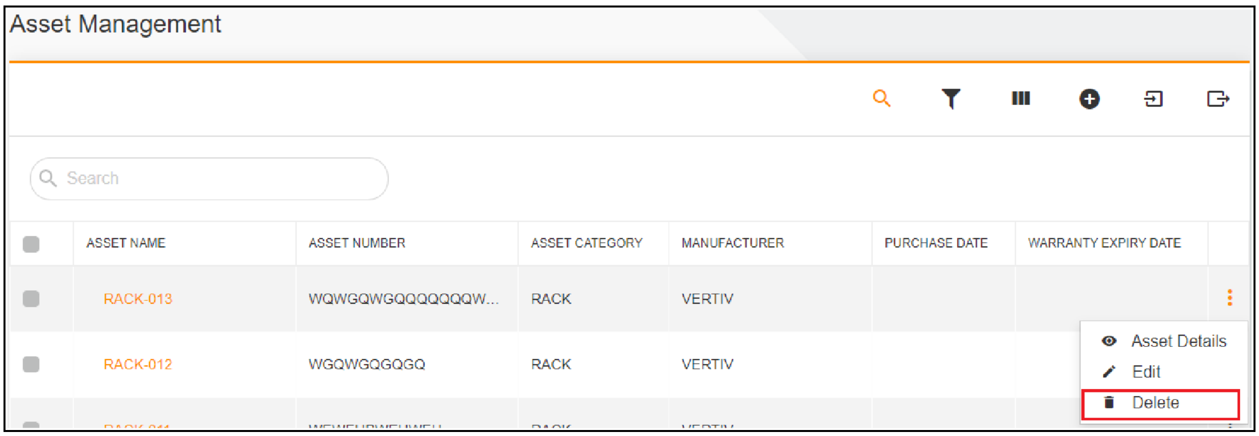
NOTE: For devices located at an SA3.0 site, editing dimensional fields (length, width, height), total U-position, or rated power is prohibited. This applies to devices including air conditioners, UPS systems, and cabinets.

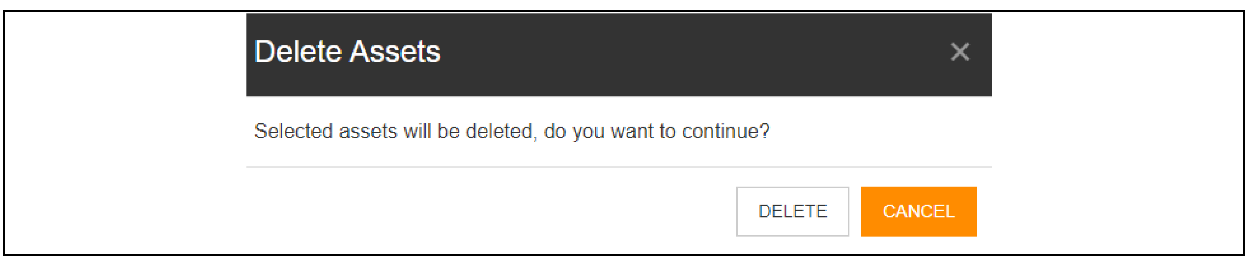
On the asset editing page, if you're using U-position Asset Manager, you can configure the U-position tag field (Unit tag) in the advanced settings. Enter the six-digit code obtained by scanning the U-position tag, then click Save to complete the setup. Once configured, U-position Asset Manager can automatically inventory supported assets, including servers, console devices, and rack PDUs.

16.3.6 Deleting the Asset

Click the ellipses(...) on the right side of the asset in the asset list and select Delete as shown in **Figure 16.22** below .

Figure 16.22 Deleting an Asset



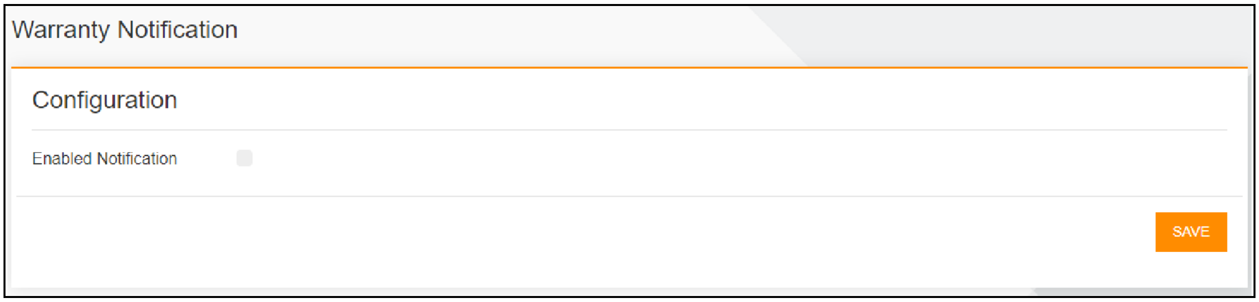


Click the *Delete* icon to delete the asset.

16.3.7 Warranty Notifications

If you need the Warranty Notification function, click the asset menu and select the **Warranty Notification** menu to enter the Warranty Notification page, as shown in **Figure 16.23** on the facing page .

Figure 16.23 Warranty Notification



Enable notifications by checking the box shown in, as shown in **Figure 16.24** below , Select the person to be notified by email (ensure email addresses are pre-configured), then click save to activate the Warranty Notification function. Note that for this feature to work, the asset maintenance expiration time must be set up in advance.

The Warranty Notification email reminder system operates as follows:

1. Starting three months before the asset maintenance expiration date, an email is sent to the designated person on the 1st of each month.

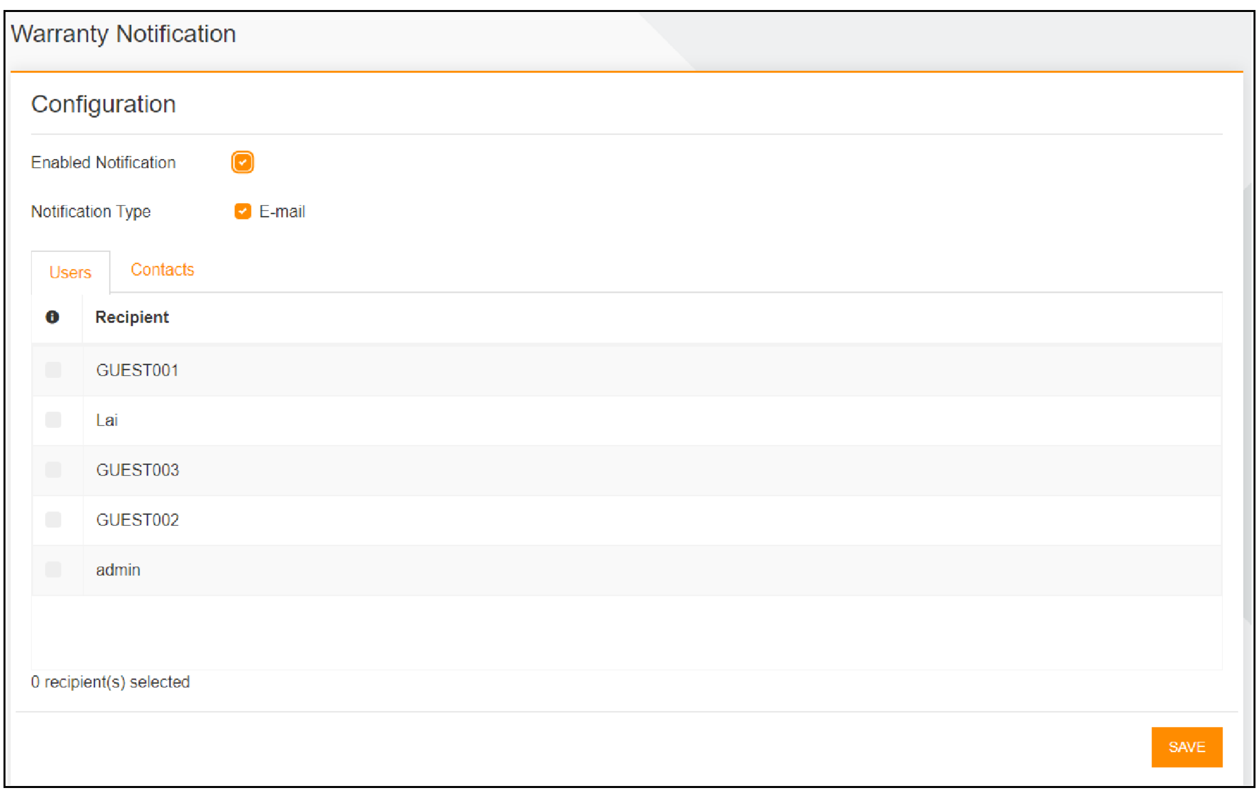
2. If the initial send fails, one retry attempt is made.

3. If both attempts fail, no further emails are sent that month.

The process repeats on the 1st of the following month.

.

Figure 16.24 Enabling Warranty Notifications



16.3.8 Rack and De-rack Record of Assets

The U-position Asset Manager allows users to monitor and track changes in rack-mounted assets through racking and de-racking records. It supports multiple sites and U-level Asset Managers, and offers an export function for these records.

17 Report

17.1 Overview

Reports are divided into basic reports and custom reports, which are mainly used by users to query or analyze the data and alarms generated by the data center monitoring system.

17.1.1 Functional modules

The report is divided into the following functional modules, please refer to this manual for the detailed description of each functional module Detailed Features on page 355.

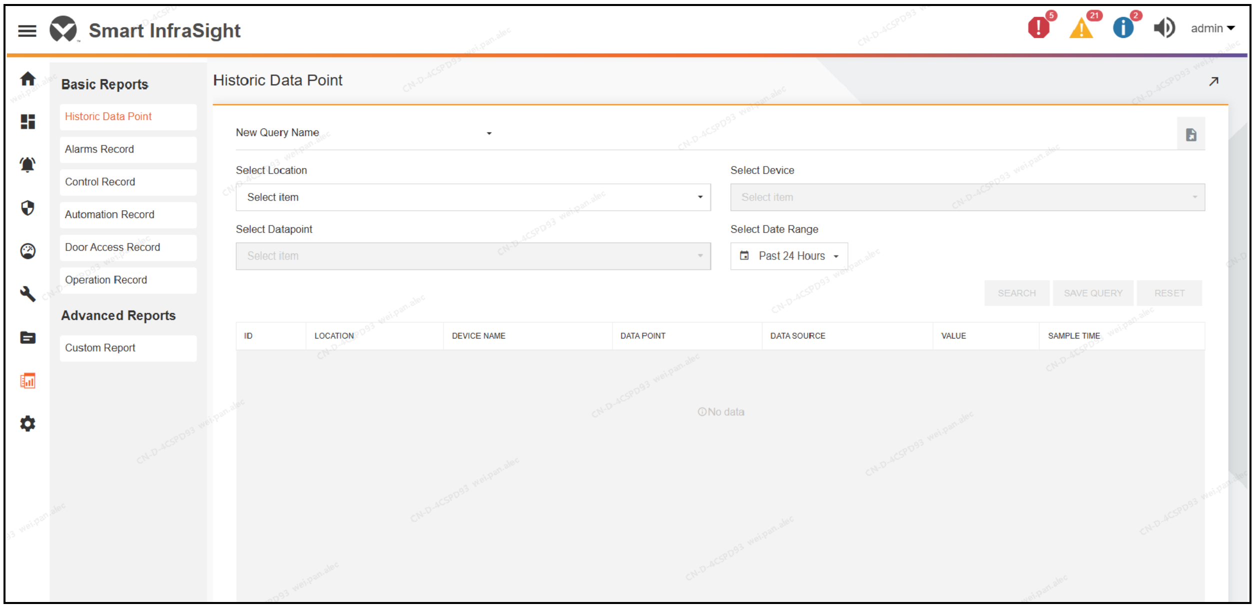
- Device History Report
- Alarm History Report
- Device Control Report
- Automation Report
- Door Access Report
- System Report
- Custom Line Chart
- Custom Column Chart
- Custom Alarm Analysis Report

17.2 Quick Start

17.2.1 Example

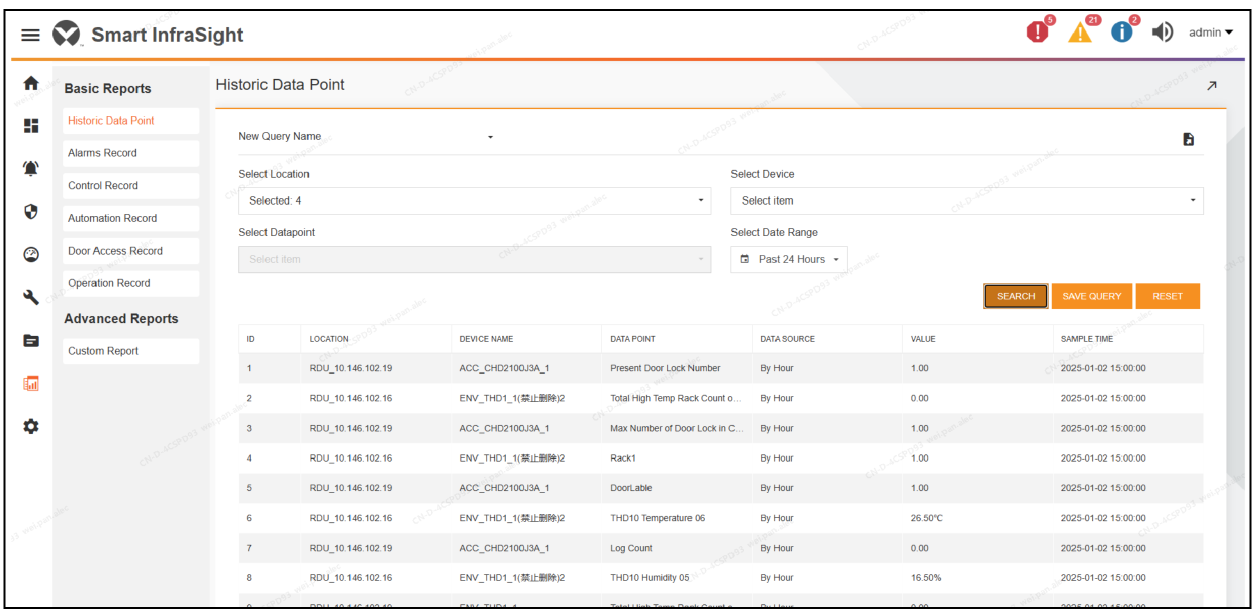
Taking the history signal report as an example, navigate to Report, and select Device History Report, as shown in **Figure 17.1** on the next page .

Figure 17.1 Historic Report Page



Select a site from the Select Location drop-down list. Then, choose devices from the **Select Device** list, and select signals from the **Select Datapoint** list. Finally, choose a query time period from the **Select Date Range** and click *Save*, as shown in **Figure 17.2** below .

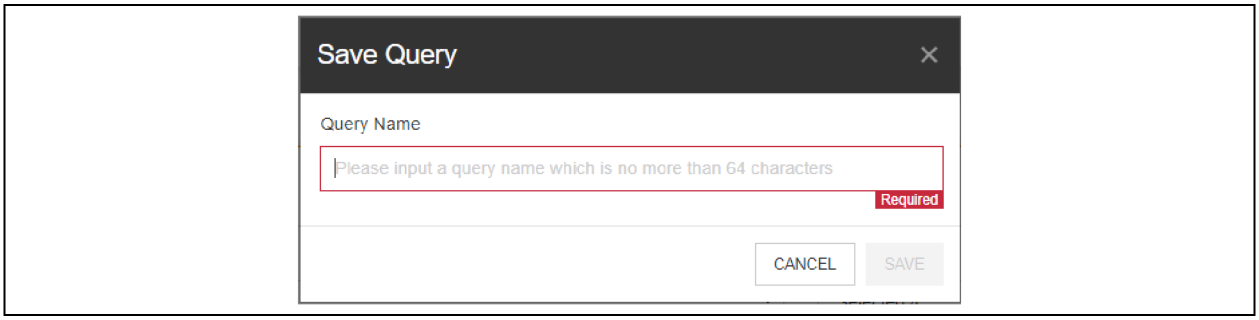
Figure 17.2 The Result Page based on the Query Condition



Saving the Query Condition

Click on the *Query Condition*, enter a name for the query condition to save the current query rule, as shown in **Figure 17.3** on the facing page .

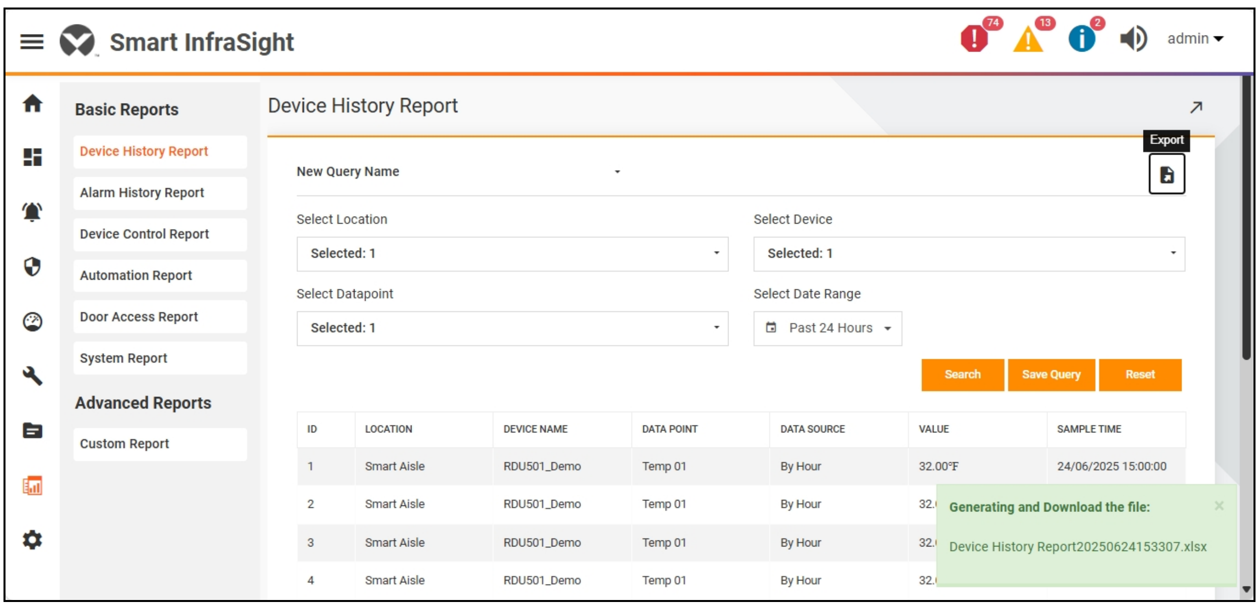
Figure 17.3 Saving the Query



After saving, the query condition will be retained in the drop-down list of New Query Condition, and you can reuse the query condition for filtering later. When the user does not need to save the query condition, he needs to click the delete button on the right side of the query condition.

Click *Query* and the selected query condition has the query result, then click the **Export button** in the upper right corner to download. As shown in **Figure 17.4** below .

Figure 17.4 Downloading the Historical Report



17.3 Detailed Features

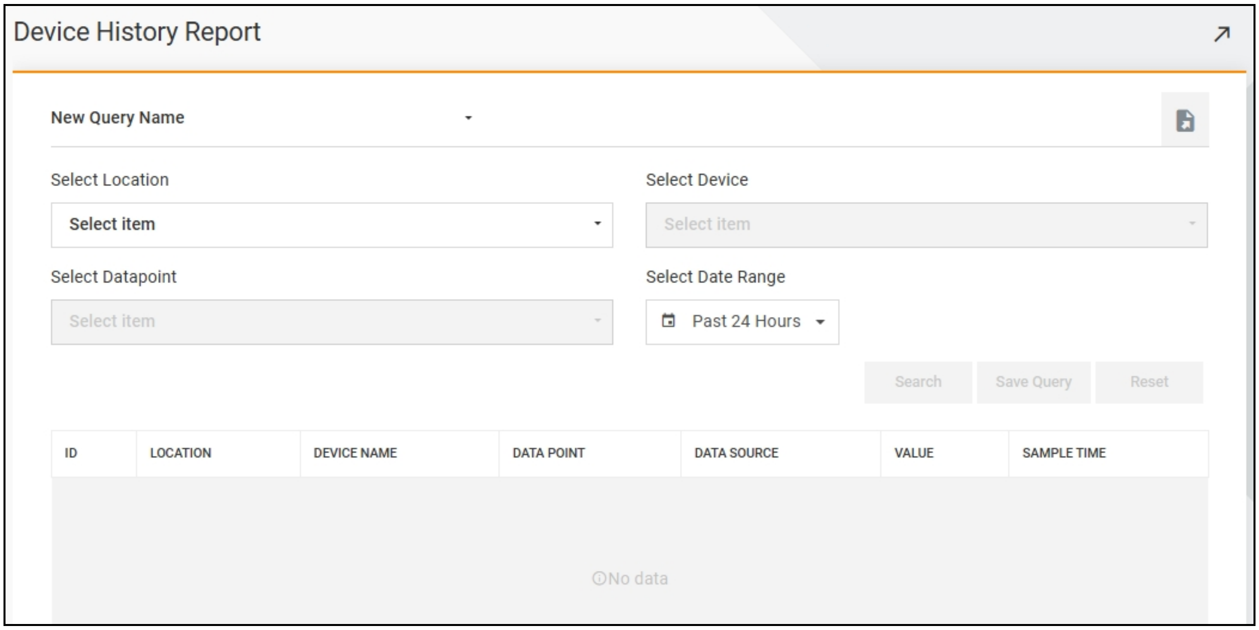
17.3.1 Basic Reports

The basic report is mainly for the monitoring system generated by the signal, alarm, control, automation , access control and other data aggregate statistics, mainly covering history signals, alarm records, automation records, control records, access control card records and other data.

Device History Report

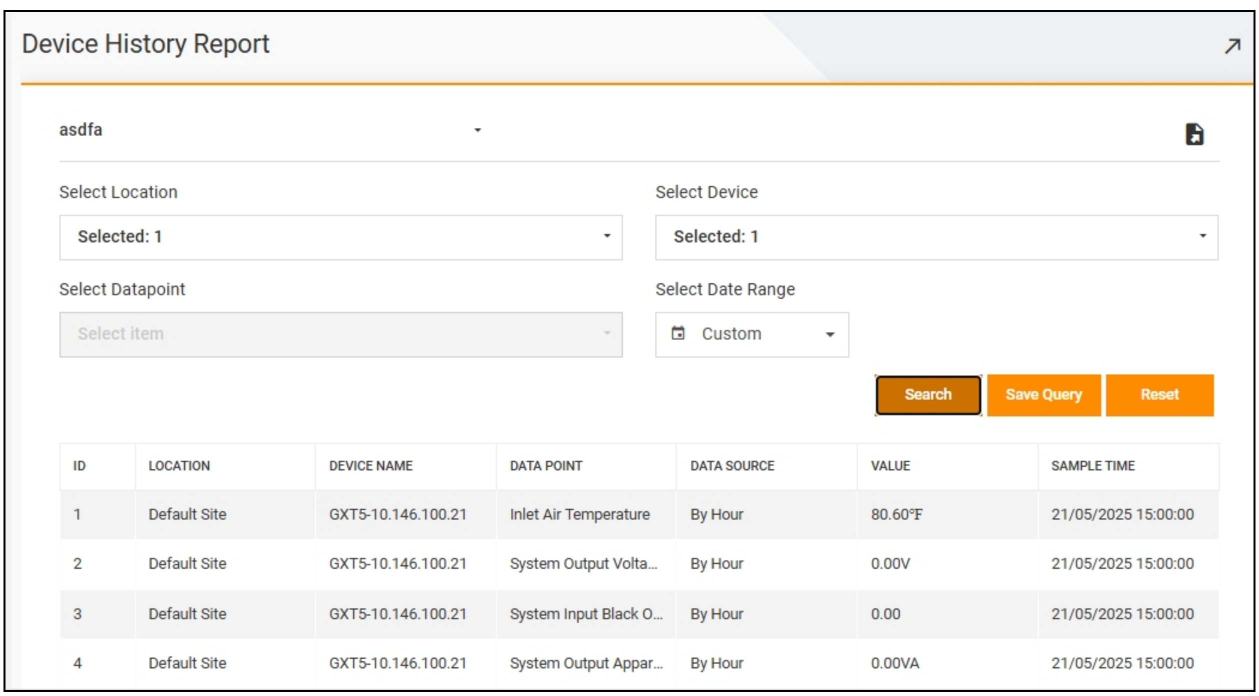
To find the device history of the device under any site, click *Report*, then click on the *Basic Report*, then *device history* to enter the device history page, as shown in **Figure 17.5** on the next page .

Figure 17.5 Device History Report



Select the site from the select location drop-down list, select the device in the selected site from the select device drop-down list, select the signal under the selected device from the select signal drop-down list, select a query time period from the select date drop-down list, and finally click the *Search* icon, as shown in **Figure 17.6** below .

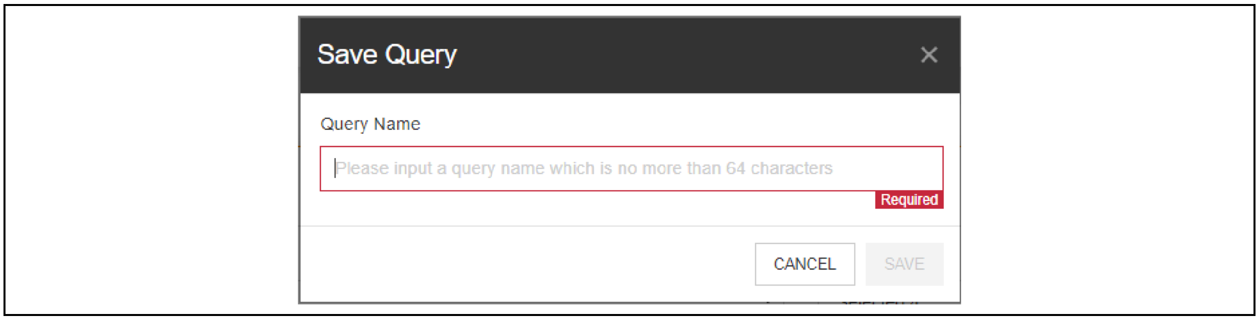
Figure 17.6 Device History Report Query Results



To Save the Query Criteria:

Click the button to pop up the save query condition dialog box, enter a name for the query condition to save the current query condition, as shown in Figure 17.7 below .

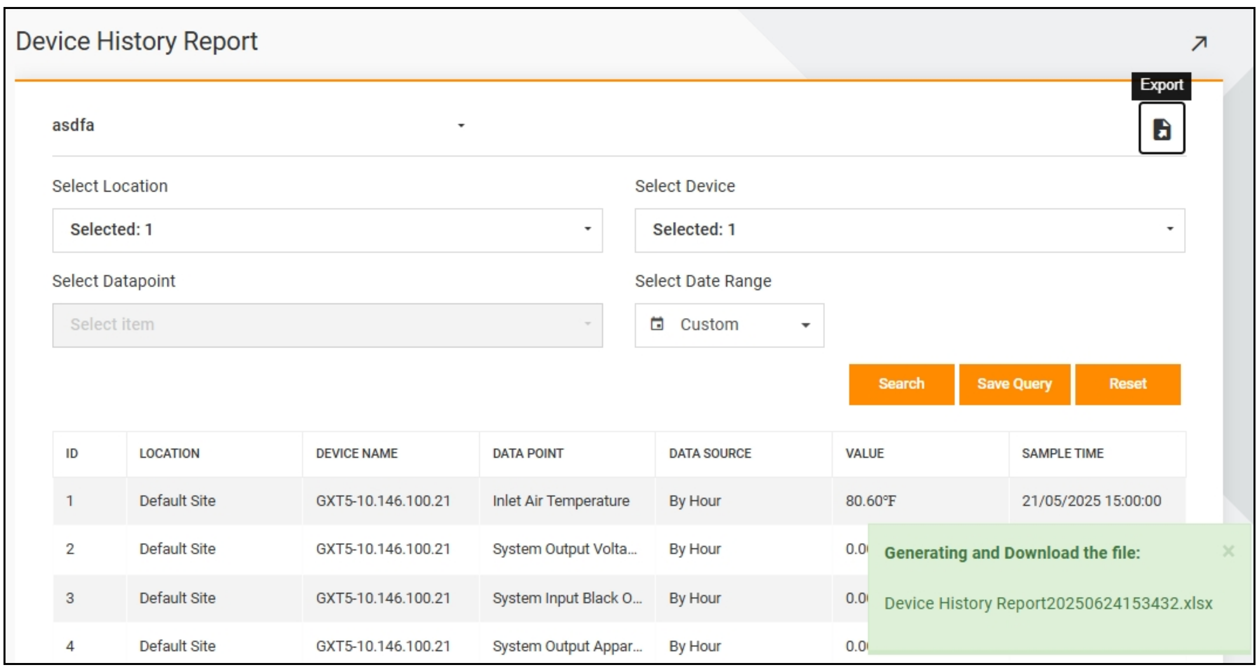
Figure 17.7 Saving the Query Criteria



After saving, the query condition will be retained in the drop-down list of new query condition, and you can reuse the query condition for filtering later. When you do not need to save the query condition, you have to click the *delete* on the right side of the query condition.

Download History Signal Report: When you click *Query* and the selected query condition has query results, you can click the *Export button* in the upper right corner to download, as shown in Figure 17.8 below .

Figure 17.8 Downloading the Historical Signals



NOTE: 1. Select no more than 30 locations, devices, and signals.

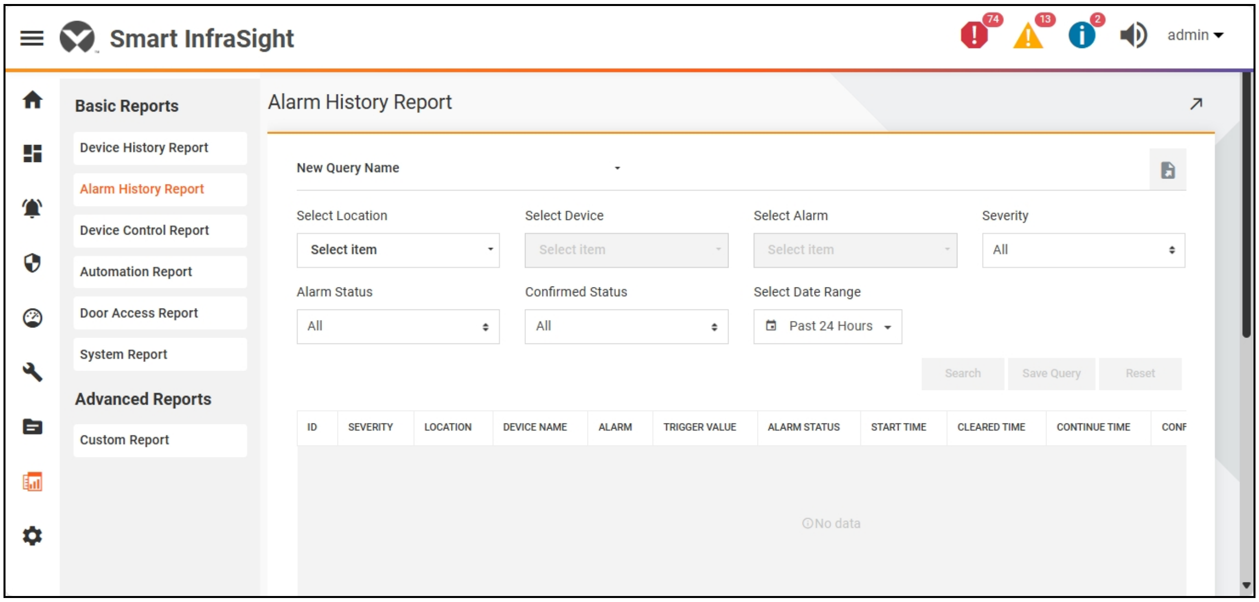
2. By-default, the signal value is displayed in two decimal places.

3. Normallized Floor_PDU and UPS devices will display non-tributary signals, not all signals.

Alarm Record Report

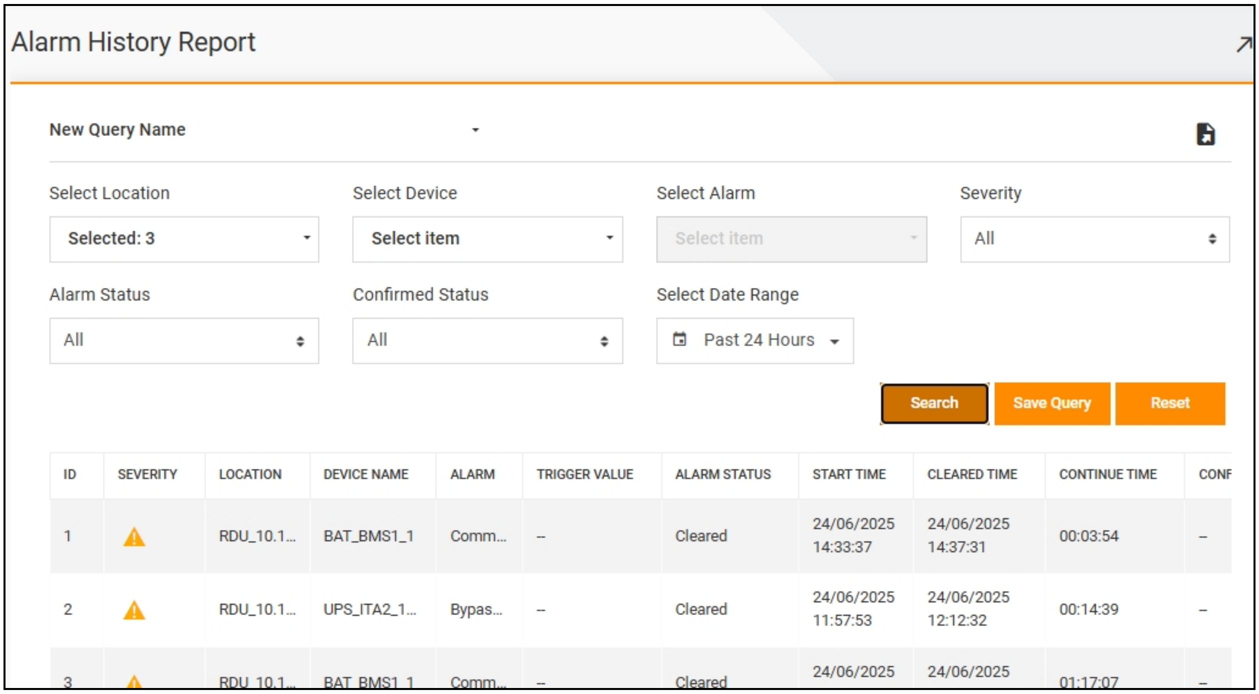
To query the Stored signal value of the device under any site, click *Report*, Click on the *Basic Report*, then *Alarm Record* to enter the alarm record report page, as shown in **Figure 17.9** below .

Figure 17.9 Alarm Record Report



Select a site from the Select Location drop-down list (mandatory), select the device in the selected site from the Select Device drop-down list, select the alarm under the device from the Select Alarm drop-down list, select the level of the desired alarm, the status of the alarm and whether the alarm has been confirmed (single-select) from the Alarm Level, Alarm Status and Acknowledgment Status drop-down lists, if not, the default result is all, select the query time period from the Select Date drop-down box, and the default time is in the past 24 hours. Click the *Search* button to query the selected location, device, alarm, alarm level, alarm status, confirmation status, and statistics within the specified date, as shown in **Figure 17.10** on the facing page .

Figure 17.10 Query Result of Alarm Record Report



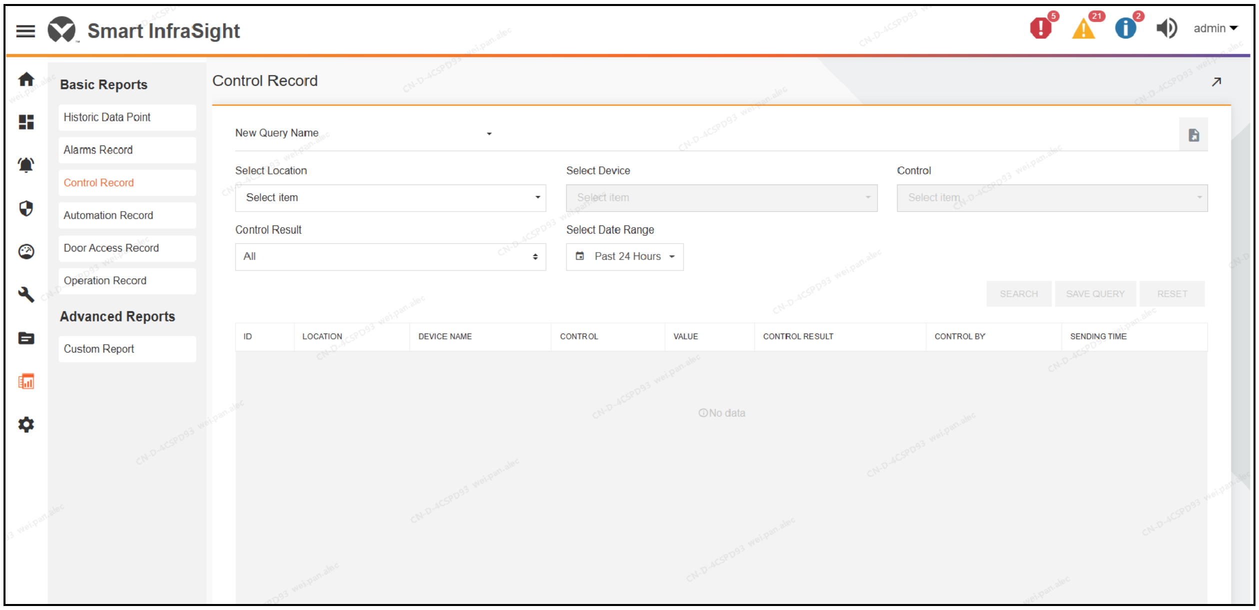
NOTE: 1. Location is mandatory, and all other items are returned by default if no selection is made.

2. After clicking on the *Query* and returning the query results, you can save the query conditions and download the alarm record report.

Control Record Reports

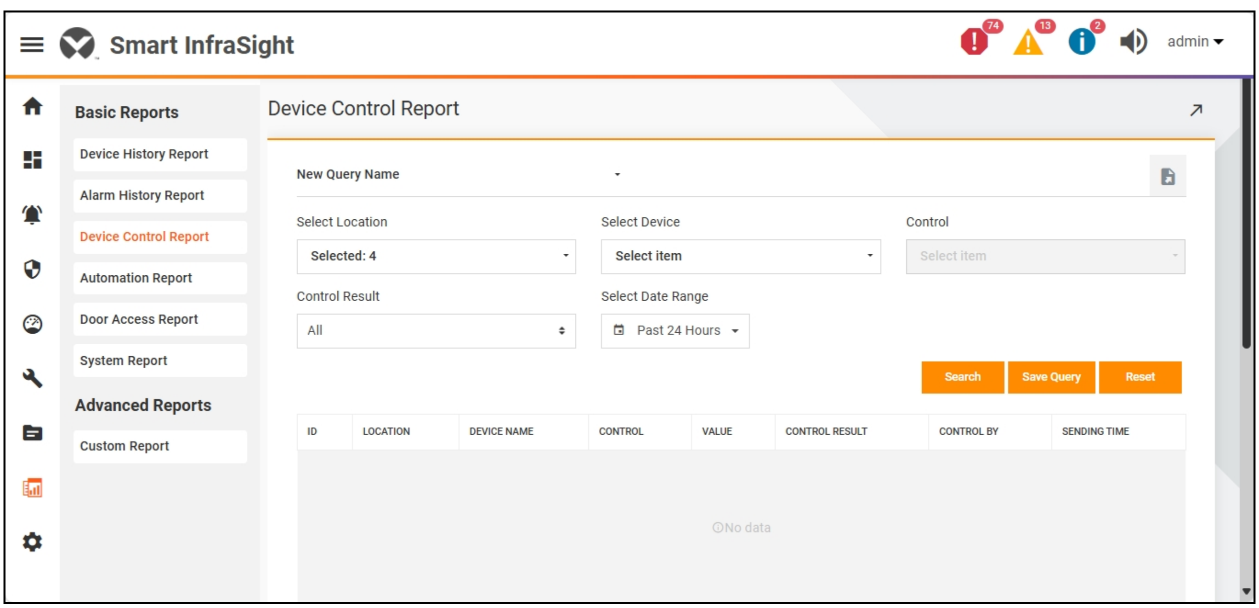
Used to query the control signal records sent by the user of the SI system to the devices under any site. click *Report*, then click on the *Basic Report*, then *Stored Signal* to enter the control record report page, as shown in **Figure 17.11** on the next page
.

Figure 17.11 Control Record Reports



Select the site item from the select location drop-down list (mandatory), select the device in the selected site from the select device drop-down list, select the control signal of the device from the Control Signal drop-down list, select the record of control success or control failure from the Control Result drop-down list (single selection), if not, the default result returned is all, and select the time period of the query from the select date drop-down box, the default time is the past 24 hours. Click the *search* button to query the selected location, equipment, control signal, control result within the specified date of the control record, as shown in Figure 17.12 below .

Figure 17.12 Control Record Report—Query Results



NOTE: 1. Select no more than 8 locations, devices, and signals.

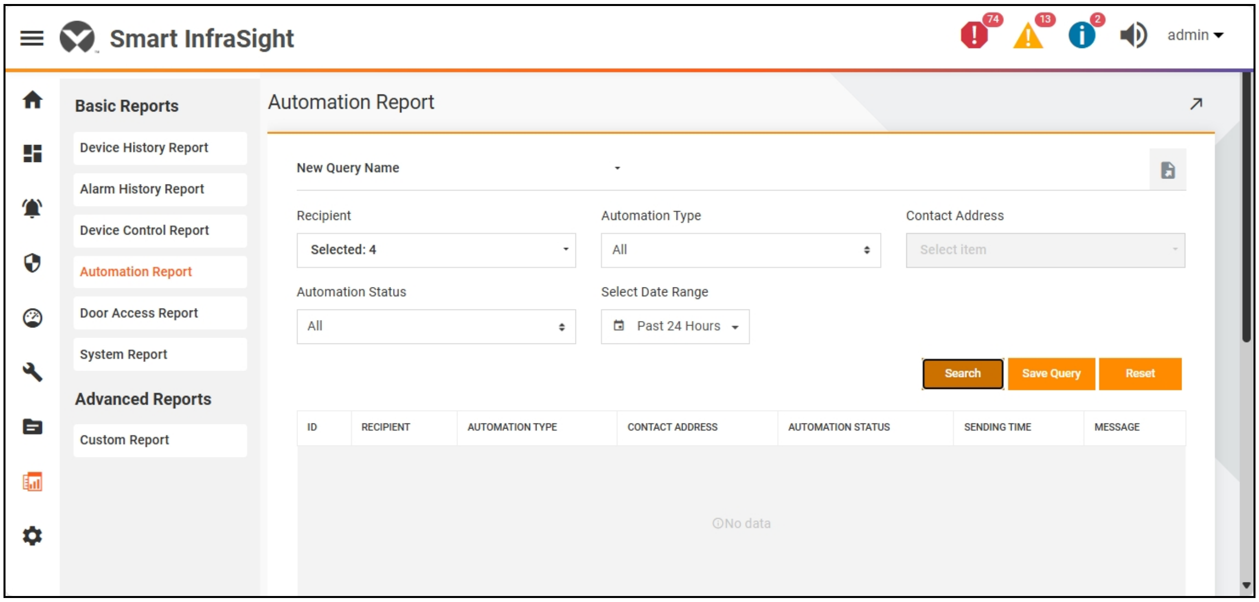
2. Location is mandatory, and all other items are returned by default if no selection is made.

3. **After clicking on the *Query* and returning the query results, you can save the query conditions and download the Control record reports.**

Automating the Records Report

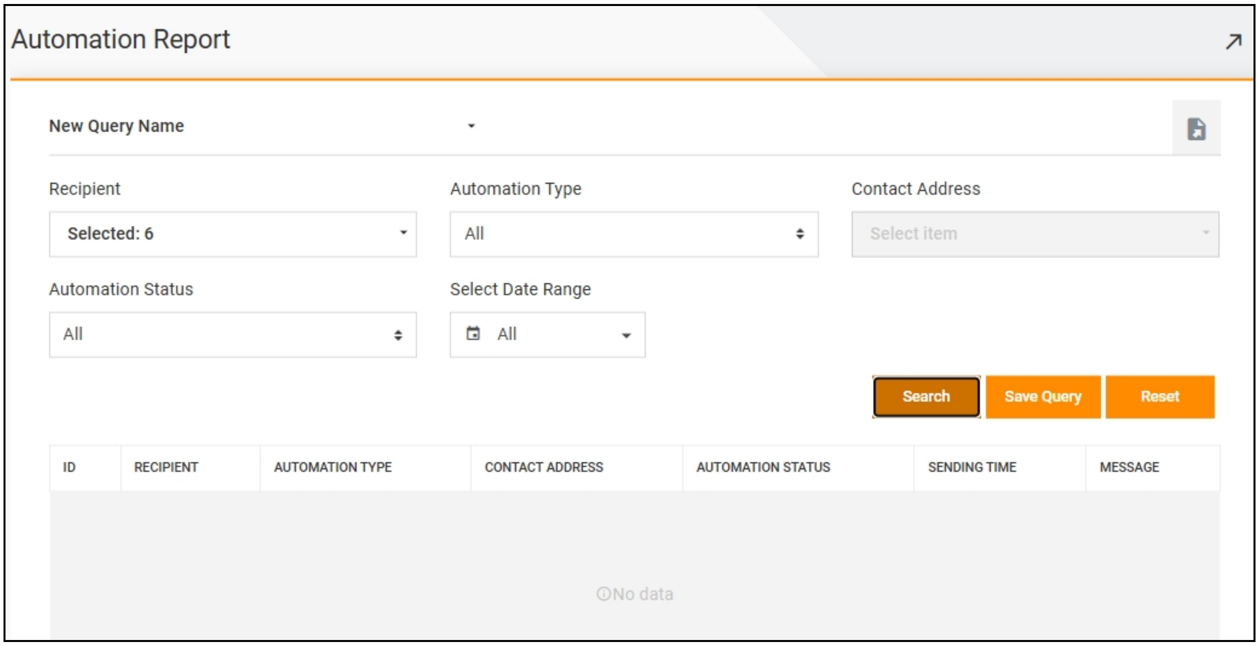
Used to query the alarm notification records (including email, SMS, and voice) sent by the SI system. Click *Report*, then click on the *Basic Report*, then *Notification Sending Record* to enter the Stored signal report page to enter the automation record report page, as shown in **Figure 17.13** below .

Figure 17.13 Automation Records Report



Select the recipient from the Recipient drop-down list (mandatory), select the notification type from the Notification Type drop-down list, select the desired sending status from the Sending Result drop-down list according to the recipient's address from the Sending Address drop-down list (single-select), if not, the default result is all, and select the time period from the Select Date drop-down box. Click the *Search* icon to query the selected recipients, notification type, sending address, sending result, and statistics within the specified date, as shown in **Figure 17.14** on the next page .

Figure 17.14 Notification Sending Records Report—Query Results



NOTE: 1. You can select not more than 8 recipients and send notification to not more than 8 addresses.

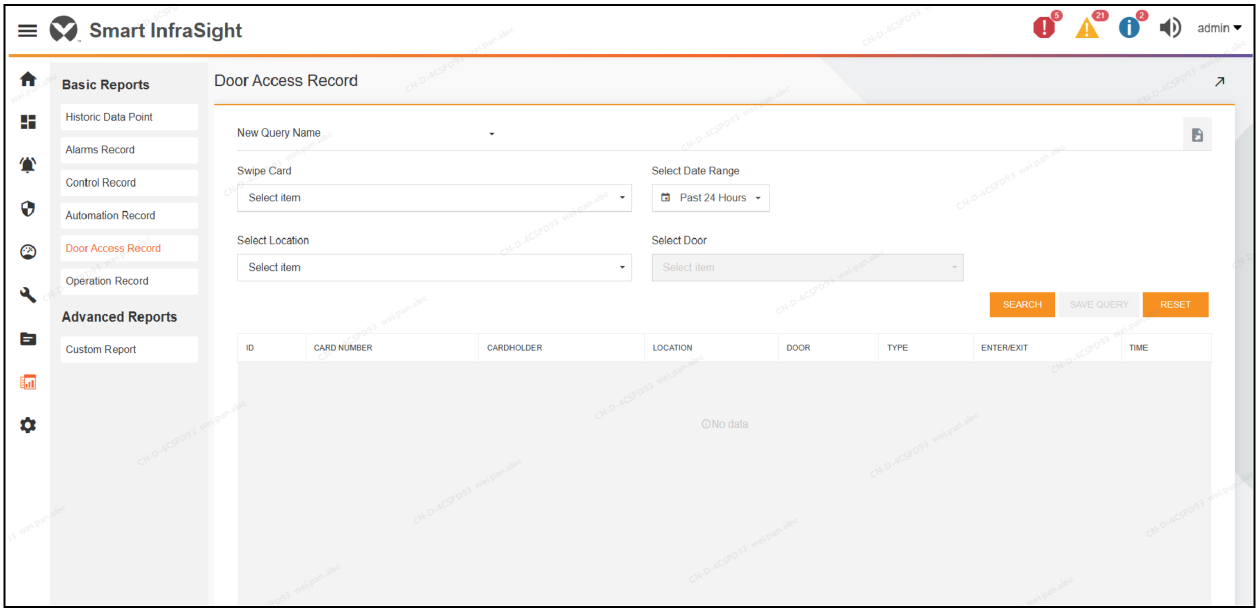
2. Recipient is mandatory, and all other items are returned by default if no selection is made.

3. After clicking on the *Query* and returning the query results, you can save the query conditions and download the automation history report.

Door Access Card Record Report

Used to query the card record of the access control device under the SI system. Click *Report*, then click on the *Basic Report*, then *Access Control Card Record* to enter the access control card record report, as shown in Figure 17.15 on the facing page.

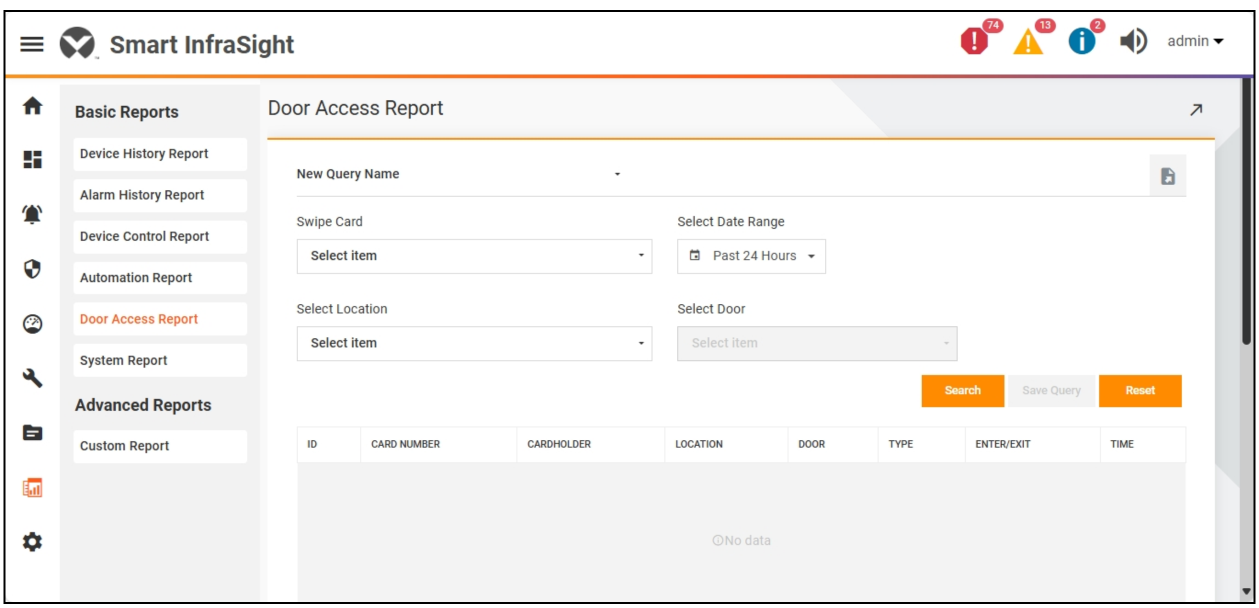
Figure 17.15 Access Control Card Record Report



Select the user from the person drop-down list, select site information from the select location drop-down list, select the door device based on the site from the select door drop-down list, and select the time period for the query from the select date drop-down box, the default time is the last 24 hours.

Click on the *Query* to query the selected user, door, location, and statistics for the specified date, as shown in **Figure 17.16** below .

Figure 17.16 Access Control Card Record Report—Query Results



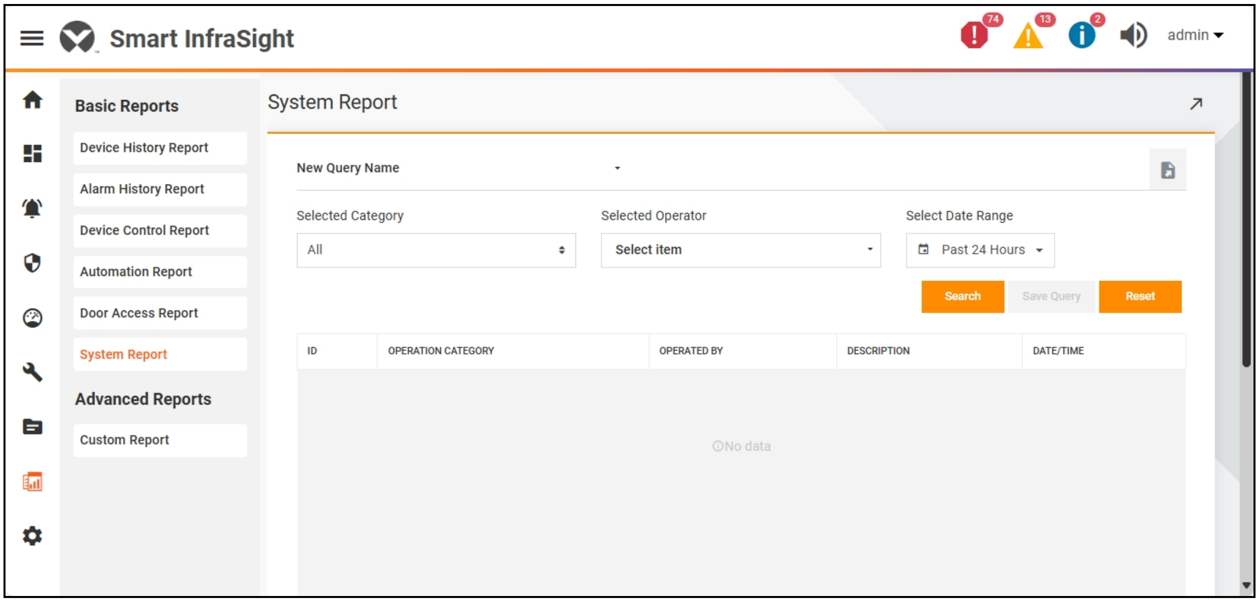
NOTE: 1. Select no more than 8 users, doors, or locations.

2. **After clicking on the *Query* and returning the query results, you can save the query conditions and download the automation history report.**

Operation Record Report

Used to query the operation records of the SI system administrator. Click *Report*, then click on the *Basic Report*, then *Operation Record* to enter the operation record report, as shown in Figure 17.17 below .

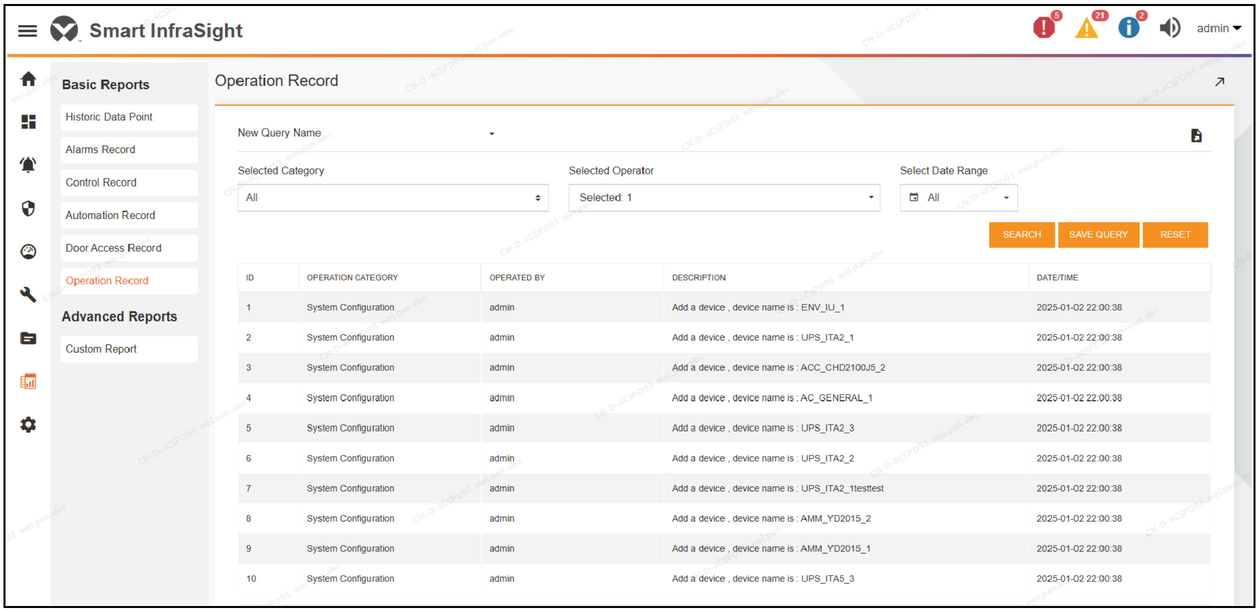
Figure 17.17 Operation Record Report



Click the *Query* button and return the query result to save the query conditions and download the operation record report.

Select the operation type (All (default), System Configuration, User Login/Logout, Service Management from the Select Operation Category drop-down list, select the operation selector from the Select Operator drop-down list, if not, the default result returned is All, and select the query time period from the Select Date drop-down box, the default time is the past 24 hours. Click the *Query* button to query the selected operation classification, operator, description and statistics within the specified date, as shown in Figure 17.18 on the facing page .

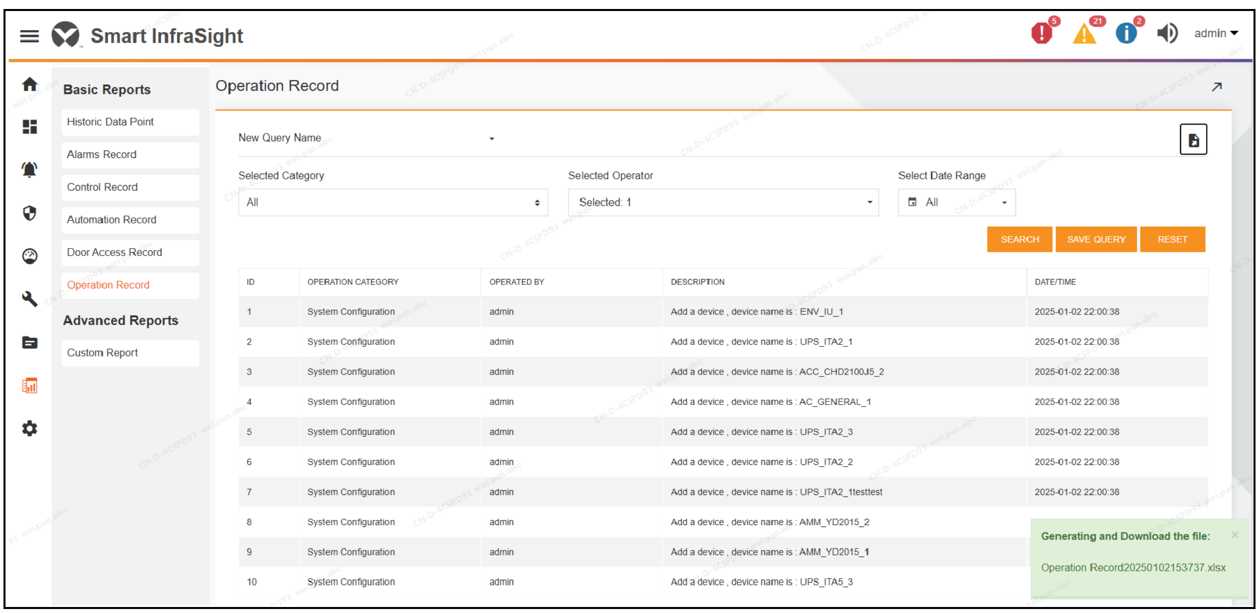
Figure 17.18 Operation Record Report—Query Result



NOTE: 1. The number of operators selected cannot exceed 8.

2. After clicking the *Query* button and returning the query result, you can save the query conditions and download the operation record report, as shown in **Figure 17.19** below .

Figure 17.19 Operation Record Report—Query Result Downloading



17.3.2 Custom Reports

Custom reports include three types of analytic reports, each of which can be used in different scenarios:

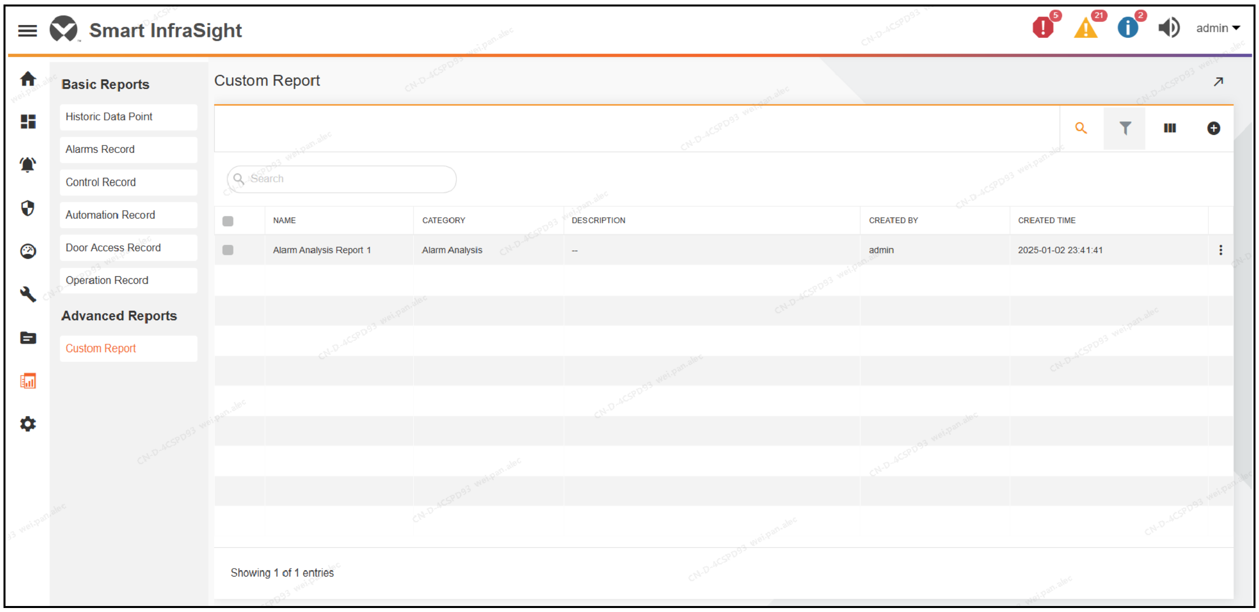
Line chart: You can analyze the change of signal value, the number of alarms, and the change of PUE value over time.

Bar Chart: You can analyze the number of alarms at the site, the energy consumption at the site, and the number of alarms by device type.

Alarm analysis report: The alarm analysis report can be used to analyze the number of alarms from the three dimensions of site, device type, and device.

Click *Report*, then click on the *Custom Report* to enter the custom report list page, which will by default display all the custom reports recently created in the system, as shown in **Figure 17.20** below .

Figure 17.20 Custom Report List



1. Click the *Search* button, and a search box will appear on the page, and you can search for a custom report by entering the report name. Click the button again and the page will hide the search box.
2. Click the *Control* button to control whether the page displays the report name, report type, description, creator, and creation time columns of the report.
3. Click the *Add* button to enter the new custom report page and create a new custom report, see the detailed introduction of specific types of reports below.
4. Click the *ellipses* button behind each report to edit, delete, and preview the report, and you can modify, delete, or preview the specified report.

Line Chart Report

The horizontal axis of the report is time, and the data source type is signal analysis, alarm analysis, and PUE analysis. You can select the time to collect statistics on device signals, alarm numbers, and PUE values by hour, day, month, quarter, or year on the horizontal axis of the line chart, and display the signal value on the Y axis. When the data source is configured as the acquisition signal of the device, the virtual signal can be configured to perform four operations based on the device signal.

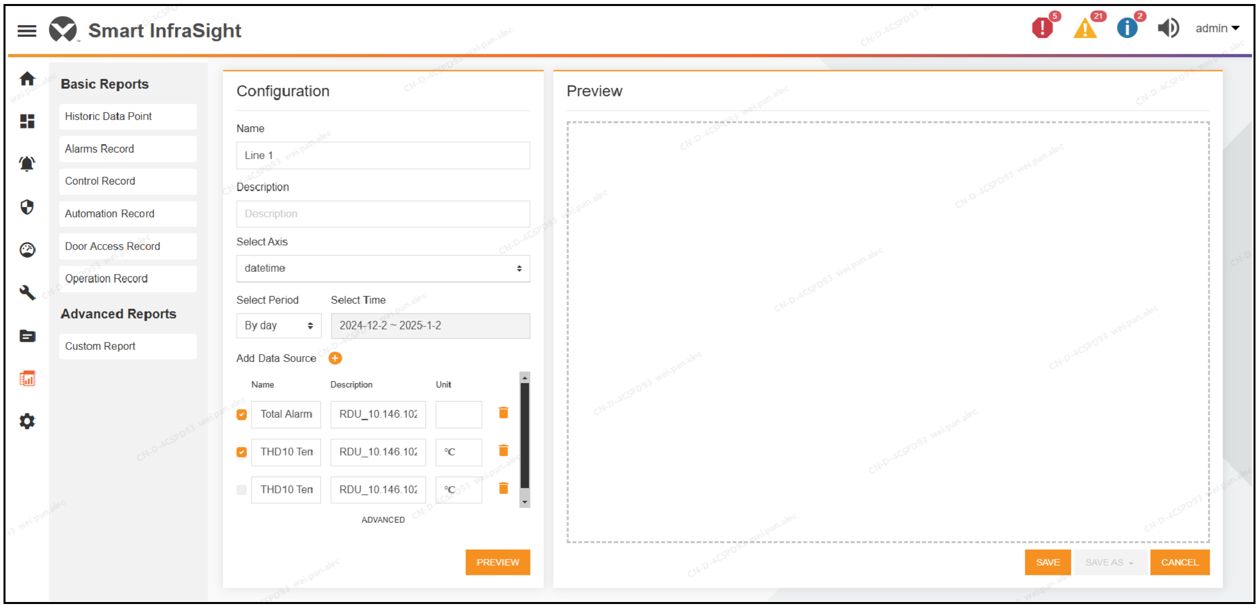
Click on the *Report*, then *Custom Report*, and the custom report list page will open. Click the *Add* button on the custom report list page to jump to the report selection page. Click the *Add* button under Custom Report-Line Chart to jump to the line chart report configuration interface, as shown in **Figure 17.21** on the facing page .

Enter a report name and description, select Time as the horizontal axis, select Hourly/Daily/Monthly/Quarterly/Yearly for the select period, and then select a specific time range.

Signal Analysis

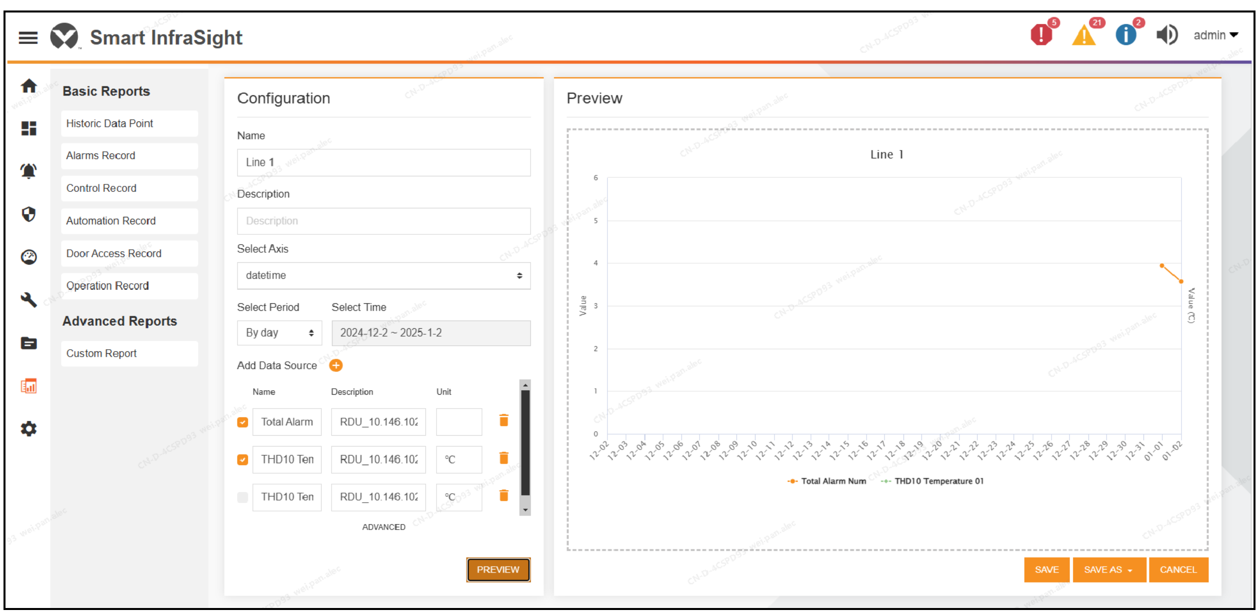
After clicking **Add Data Source**, select the **Signal Analysis** data source, and the **Add Data Source** window will pop up. In the **Add Data Source** window, select the site, select the device, select the signal, or click the **Configure Virtual Signal** button to configure a virtual signal based on the signal selected above in the pop-up **Custom Formula** window. Then click on the *Save* button, and the selected signal or the configured virtual signal will appear in the list of data sources on the left.

Figure 17.21 Creating a Line Chart and Signal Analysis Report



Select one or more signals from the list of data sources on the left (up to 8), click the ***Preview*** button, and the report preview area on the right is for users to preview the effect of the report (as shown in **Figure 17.22** below). After previewing the report, you can click the *Save As* button at the bottom right to export the report as a PDF or PNG image.

Figure 17.22 Preview of the Time-Signal Analysis Report



Click the *Save* button to generate a new custom report to the system, and return to the custom report list page, the newly created report will appear in the list.

NOTE: 1. The report name is required and can be up to 32 characters.

2. The report description is optional, up to 64 characters.

3. Each report can only be configured based on the Signal Analysis data source.

4. After configuring the data source entries, you must select at least 1 data source entry and a maximum of 8 data source entries, otherwise you cannot preview or save them.

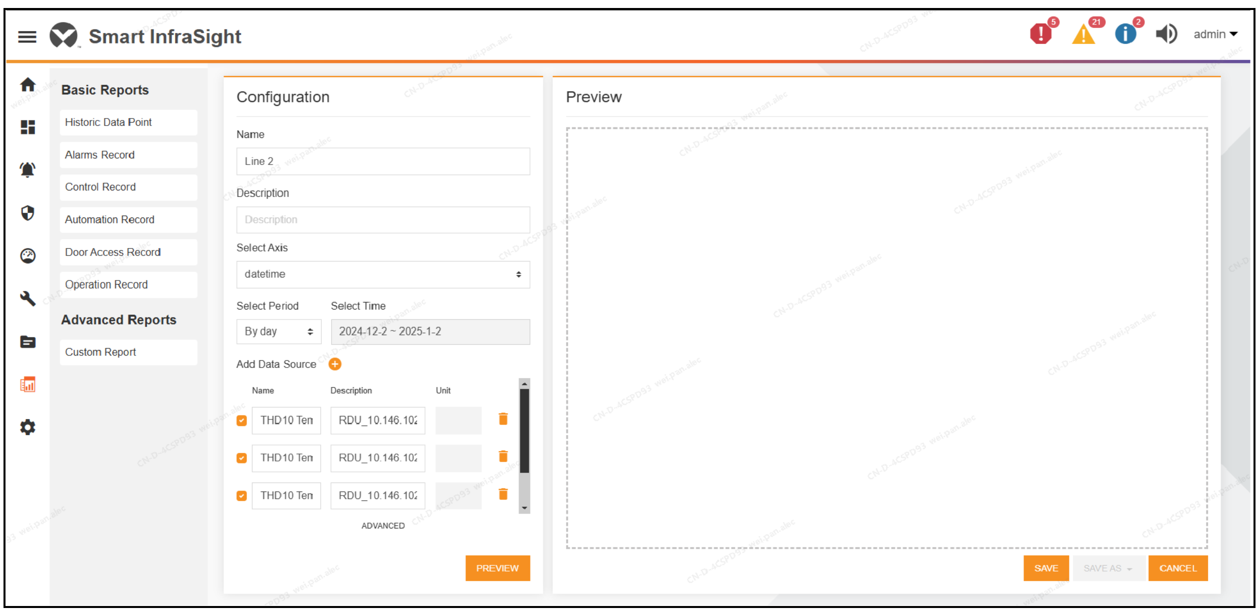
5. During the report configuration process, the report can only be exported when the report is displayed after the user clicks Preview.

6. The report supports axis unit checking, which displays a dual Y-axis coordinate system when two units appear for the selected signal. The selected signal must not appear in more than two units, otherwise it cannot be previewed and saved.

Alarm Analysis

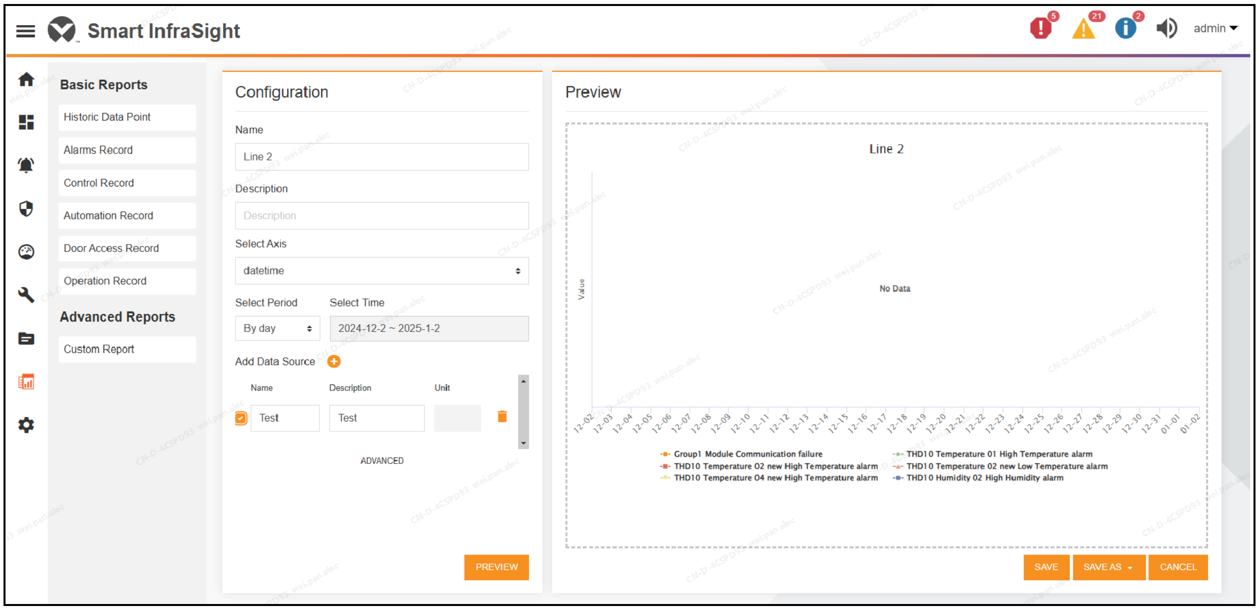
After clicking on *Add Data Source*, select the Alarm Analysis data source, and the Add Data Source window will pop up. In the **Add Data Source** window, select Site, select Device, select Alarm, and then click *Save*, the alarm selected above will appear in the data source list on the left.

Figure 17.23 Creating a Time-Alarm Analysis Report



Select one or more alarms in the data source list on the left (up to 8), click the *Preview* button, and the report preview area on the right is available for users to preview the effect of the report, as shown in **Figure 17.24** on the facing page . After previewing the report, you can click the *Save As* button at the bottom right to export the report as a PDF or PNG image.

Figure 17.24 Time-Alarm Analysis Report Preview



Click *Save* to generate a new custom report to the system, and return to the custom report list page, the newly created report will appear in the list.

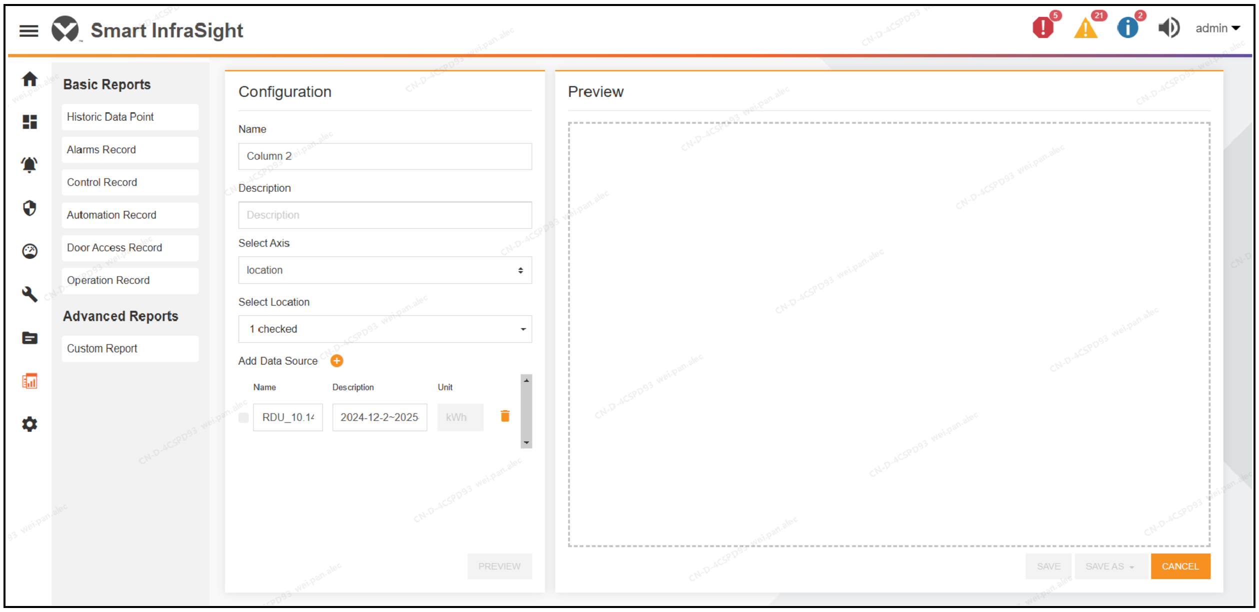
NOTE: 1. After configuring the data source entries, you must select at least 1 data source entry and a maximum of 8 data source entries, otherwise you cannot preview or save them.

2. During the report configuration process, the report can only be exported when the report is displayed after the user clicks Preview.

PUE Analysis

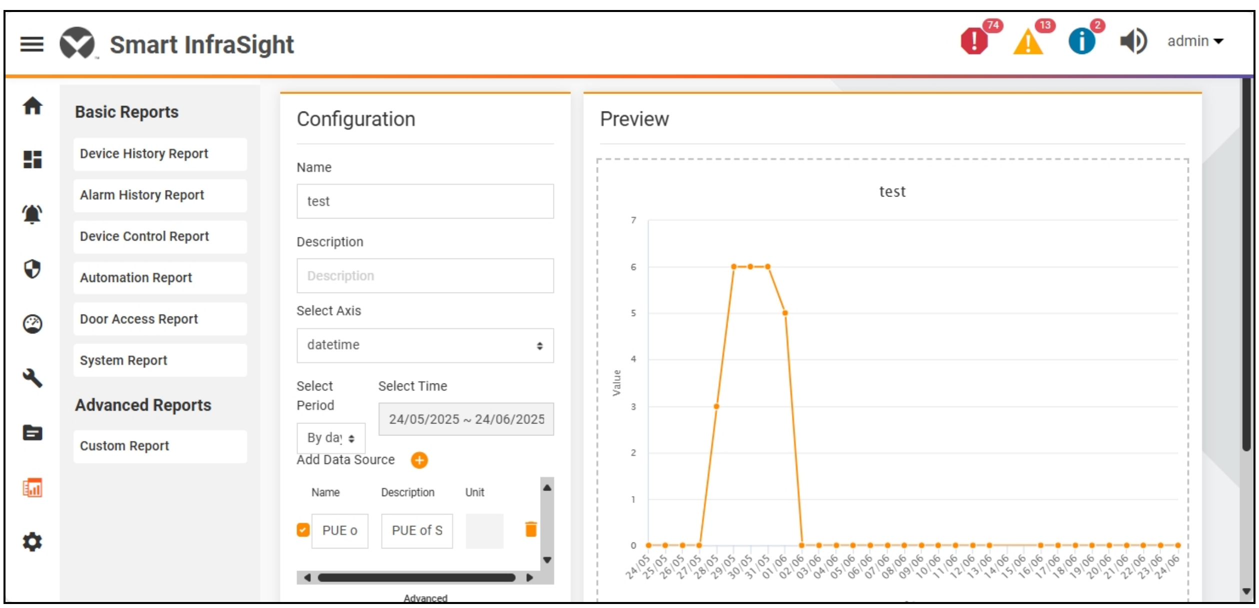
After clicking Add Data Source, select PUE Analysis data source, and the Add Data Source window will pop up. In the *Add Data Source* window, select the PUE scheme that has been created in the system, or click the *Configure Virtual Signal* button to configure a virtual signal based on the PUE scheme selected above in the *Custom Formula* window. Then click the *Save* button, and the PUE scheme or virtual signal you have selected above will appear in the list of data sources on the left, as shown in Figure 17.25 on the next page .

Figure 17.25 Creating a Time—PUE Analysis Report



Select one or more PUE schemes in the data source list on the left (up to 8). Click the *Preview* button, and the report preview area on the right is for users to preview the effect of the report, as shown in **Figure 17.26** below . After previewing the report, you can click the *Save As* button at the bottom right to export the report as a PDF or PNG image.

Figure 17.26 Preview of the Time—PUE Analysis Report



Click on the *Save* to generate a new custom report to the system, and return to the custom report list page, the newly created report will appear in the list.

NOTE: 1. After configuring the data source entries, you must select at least 1 data source entry and a maximum of 8 data source entries, otherwise you cannot preview or save them.

2. The report can only be exported during the report configuration process if the user clicks Preview and the report is displayed.

Bar Chart Report

The horizontal axis of the Bar Chart is the device type or site. The number of alarms on a device can be counted by device type, with one column for each device type on the X-axis and one alarm for each device type on the Y-axis. You can compare the number of alarms or energy consumption of different sites, where the X-axis of the Bar Chart is the number of sites and the Y-axis is the number of alarms or energy consumption of each site in a certain period of time.

Click on the *Report*, then *Custom Report*, and the custom report list page will open. Click the button on the custom report list page to jump to the report selection page. Clicking the button under Custom Report-Bar Chart will jump to the custom report configuration interface. As shown in 17.3.2 on page 365 .

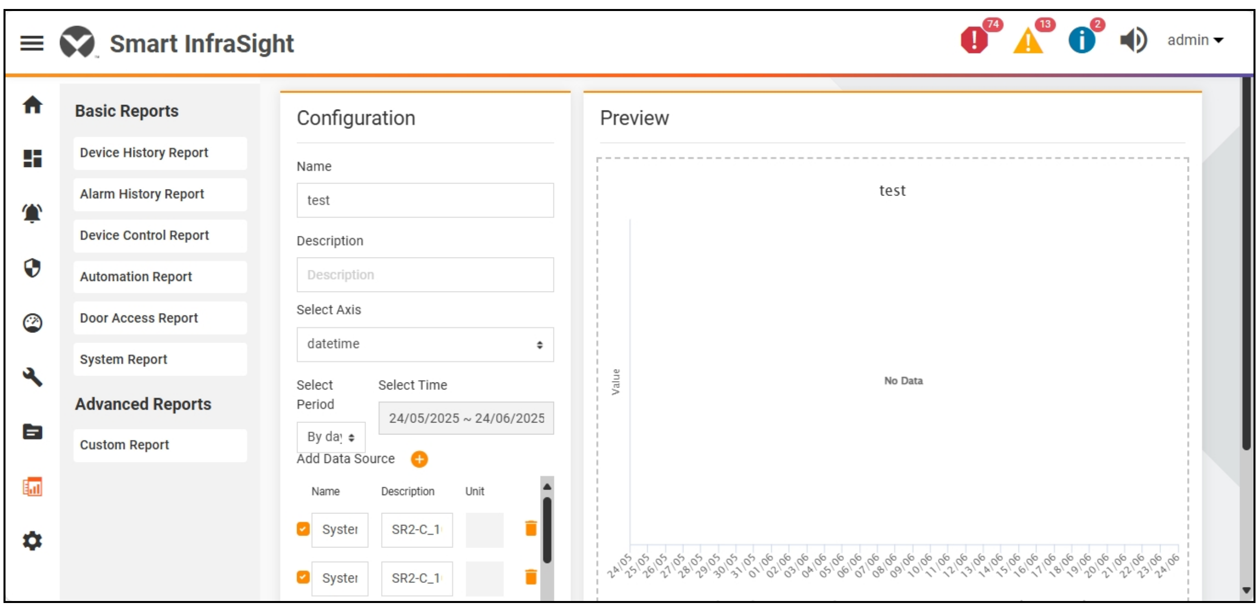
Enter a report name, description, and select from Site or Device Type on the horizontal axis.

- Analyze alarms based on device type

Select Device Type for the horizontal axis, select at least one device type for Select Device Type, and configure the data source as the condition for filtering the device types on the horizontal axis, including the site, alarm level, and time range. After clicking Add Data Source, select the Alarm Analysis data source, and the Add Data Source window will pop up. In the Add Data Source window, select the site, select the alarm level (optional), select the time range, and click the *Save* button, these conditions are combined into a single data source entry, which will appear in the data source list on the left.

Select the entries in the data source list on the left, click the *Preview* button, and the report preview area on the right is for users to preview the effect of the report. After previewing the report, as shown in Figure 17.27 below , you can click the *Save As* button at the bottom right to export the report as a PDF or PNG image.

Figure 17.27 Preview of the Alarm Analysis Report by Device Type



Click on the *Save* button to generate a new custom report to the system, and return to the custom report list page, the newly created report will appear in the list.

NOTE: 1. The report name is required and can be up to 32 characters.

2. The report description is optional, up to 64 characters.

3. Reports can only be configured based on the Alarm Analysis data source.

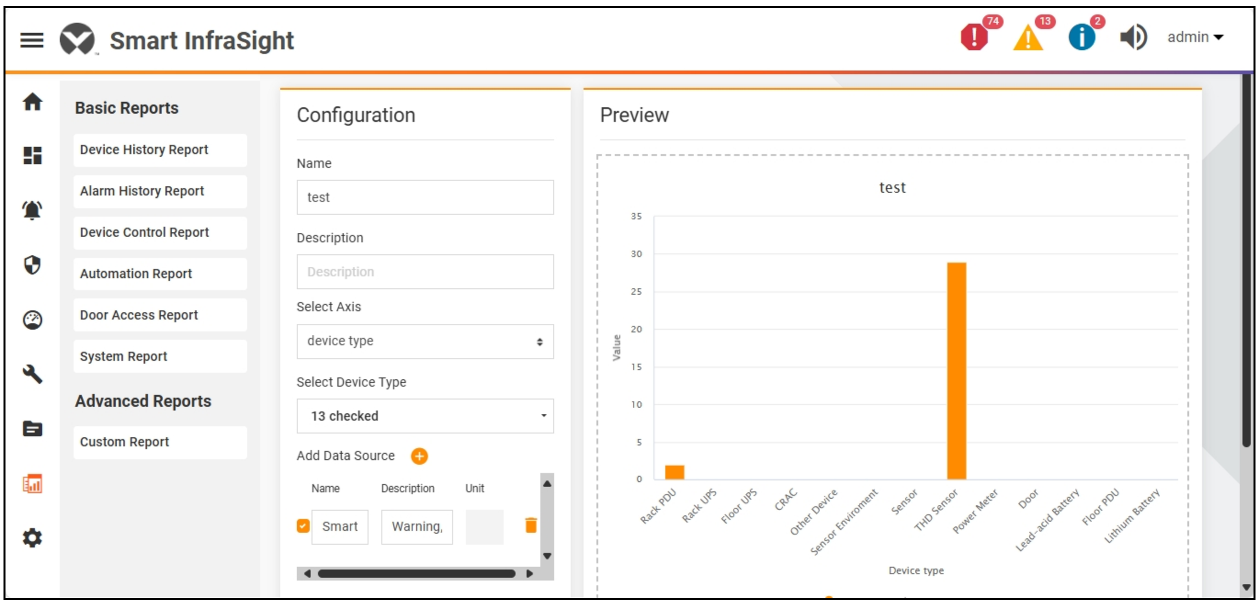
4. After you configure the data source entries, you must select the data source entries before you can preview or save them.

5. During the report configuration process, the report can only be exported when the report is displayed after the user clicks Preview.

Analyzing Alarms based on Site

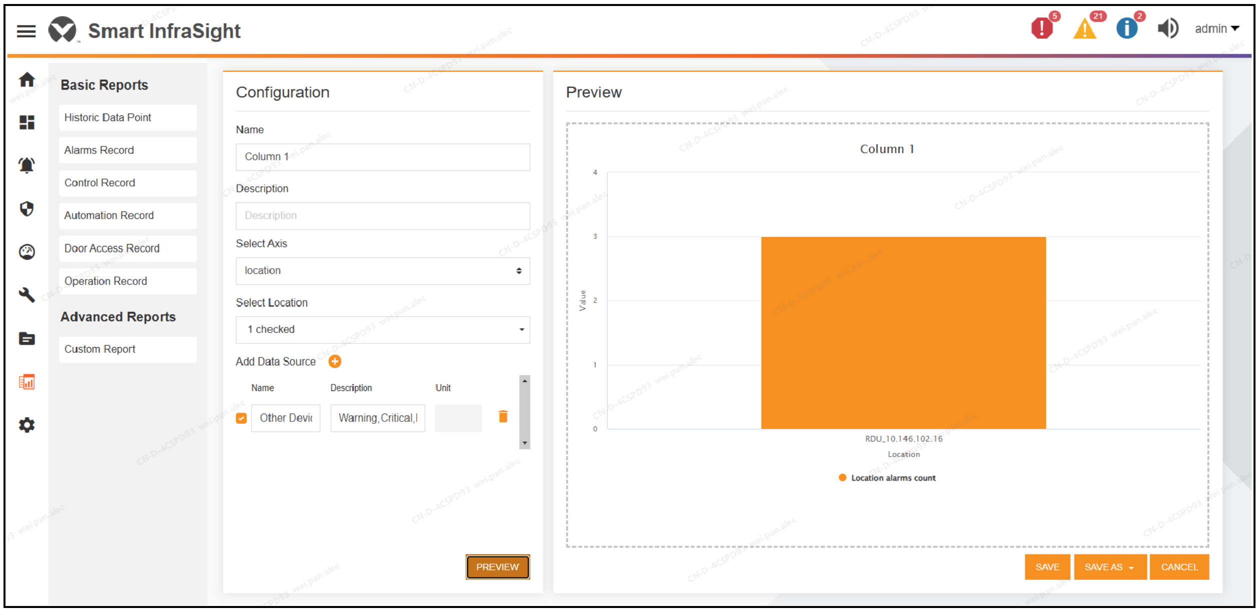
Select Site as the horizontal axis, select at least one site in Select Site, click Add Data Source, and then select Alar m Analysis data source, and the Add Data Source window pops up. In the **Add Data Source** window, select the site, select the alarm level (optional), select the alarm status (optional), select the time range, and then click the *Preview* button, these conditions are combined into a single data source entry, which will appear in the data source list on the left, as shown in **Figure 17.28** below .

Figure 17.28 New Site—Alarm Analysis Report



Select the entries in the data source list on the left, click the *Preview* button, and the report preview area on the right is for users to preview the effect of the report, as shown in **Figure 17.29** on the facing page . After previewing the report, you can click the *Save As* button at the bottom right to export the report as a PDF or PNG image.

Figure 17.29 Preview of the Site-Alarm Analysis Report



Click on the *Save* button to generate a new custom report to the system, and return to the custom report list page, the newly created report will appear in the list.

NOTE: 1. The report name is required and can be up to 32 characters.

2. The report description is optional, up to 64 characters.

3. Reports can only be configured based on the Alarm Analysis data source.

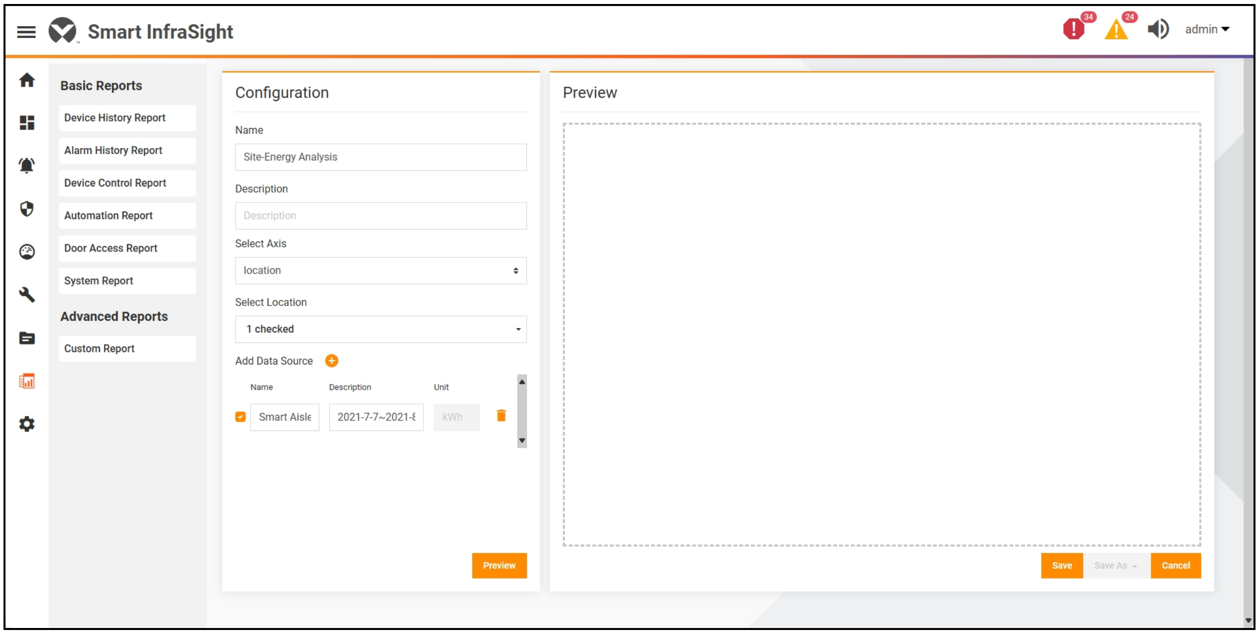
4. After you configure the data source entries, you must select the data source entries before you can preview or save them.

5. During the report configuration process, the report can only be exported when the report is displayed after the user clicks Preview.

Analyzing Energy Consumption by Site

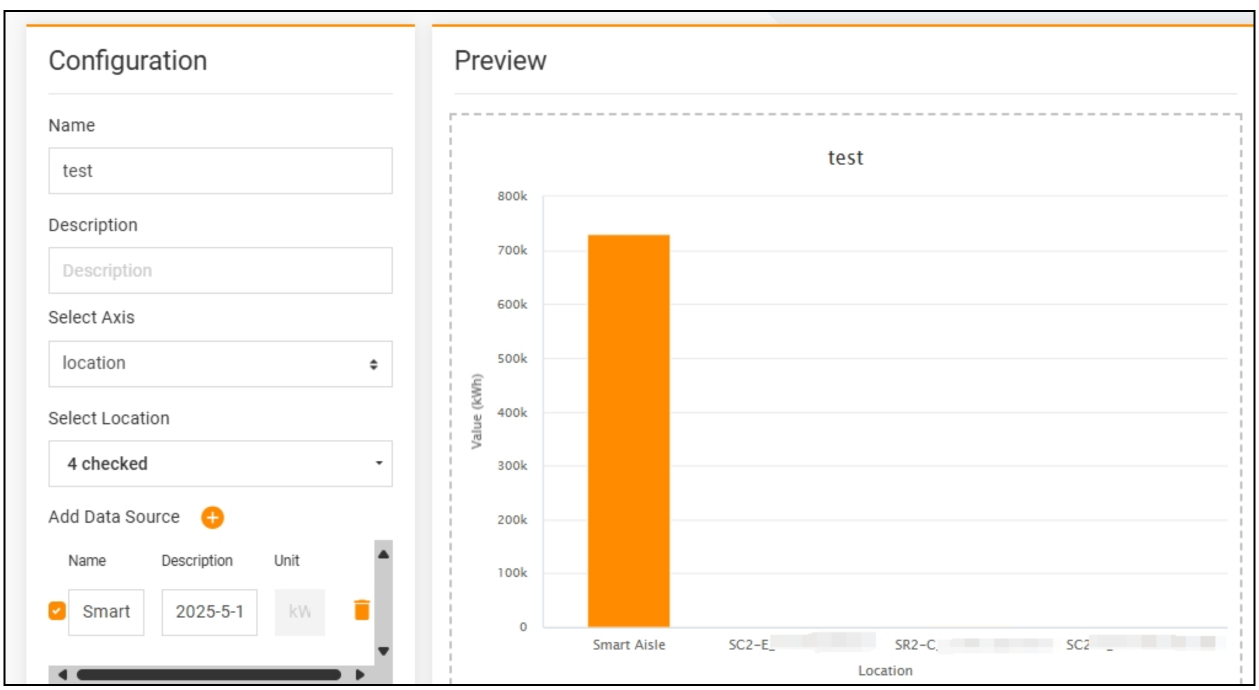
Select **Site** as the horizontal axis, select at least one site in **Select Site**, then you need to configure the data source, click *Add Data Source*, select the **Energy Consumption Analysis** data source, and the **Add Data Source** window will pop up. In the Add Data Source window, select a time range. Then click the *Save* button, and the time condition selected above will appear in the list of data sources on the left. As shown in **Figure 17.30** on the next page .

Figure 17.30 New Site—Energy Consumption Analysis Report



Select the entries in the data source list on the left, click the Preview button, and the report preview area on the right is for users to preview the effect of the report, as shown in **Figure 17.31** below . When calculating the energy consumption of a site, search for the energy consumption configuration bound to the site in the data source configuration based on the selected site on the horizontal axis, and then calculate the energy consumption. After previewing the report, you can click the *Save As* button at the bottom right to export the report as a PDF or PNG image.

Figure 17.31 Preview of the Site—Energy Analysis report



Click on the *Save* button to generate a new custom report to the system, and return to the custom report list page, the newly created report will appear in the list.

NOTE: 1. The report name is required and can be up to 32 characters.

2. The report description is optional, up to 64 characters.

3. Reports can only be configured based on the Alarm Analysis data source.

4. After you configure the data source entries, you must select the data source entries before you can preview or save them.

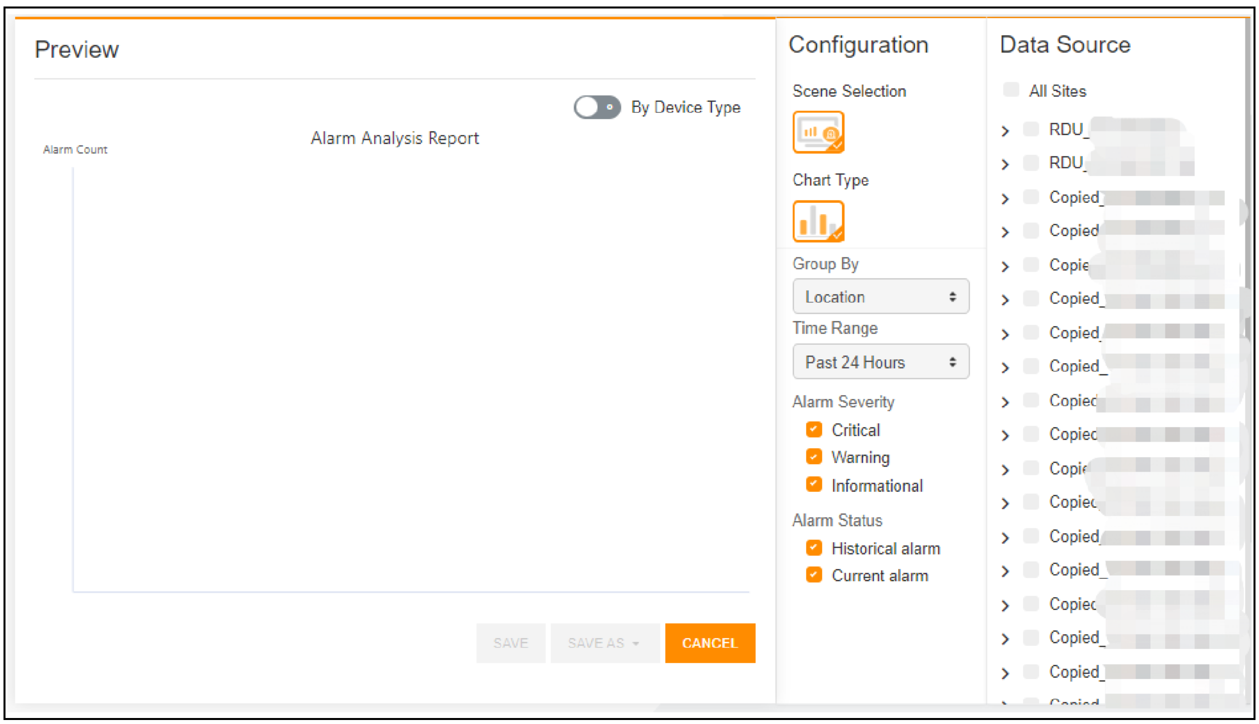
5. During the report configuration process, the report can only be exported when the report is displayed after the user clicks Preview.

Alarm Analysis Report

The report can flexibly select the number of alarms for different sites and device types in a specific time period for analysis, and filter the results of the Bar Chart based on the alarm level and alarm status.

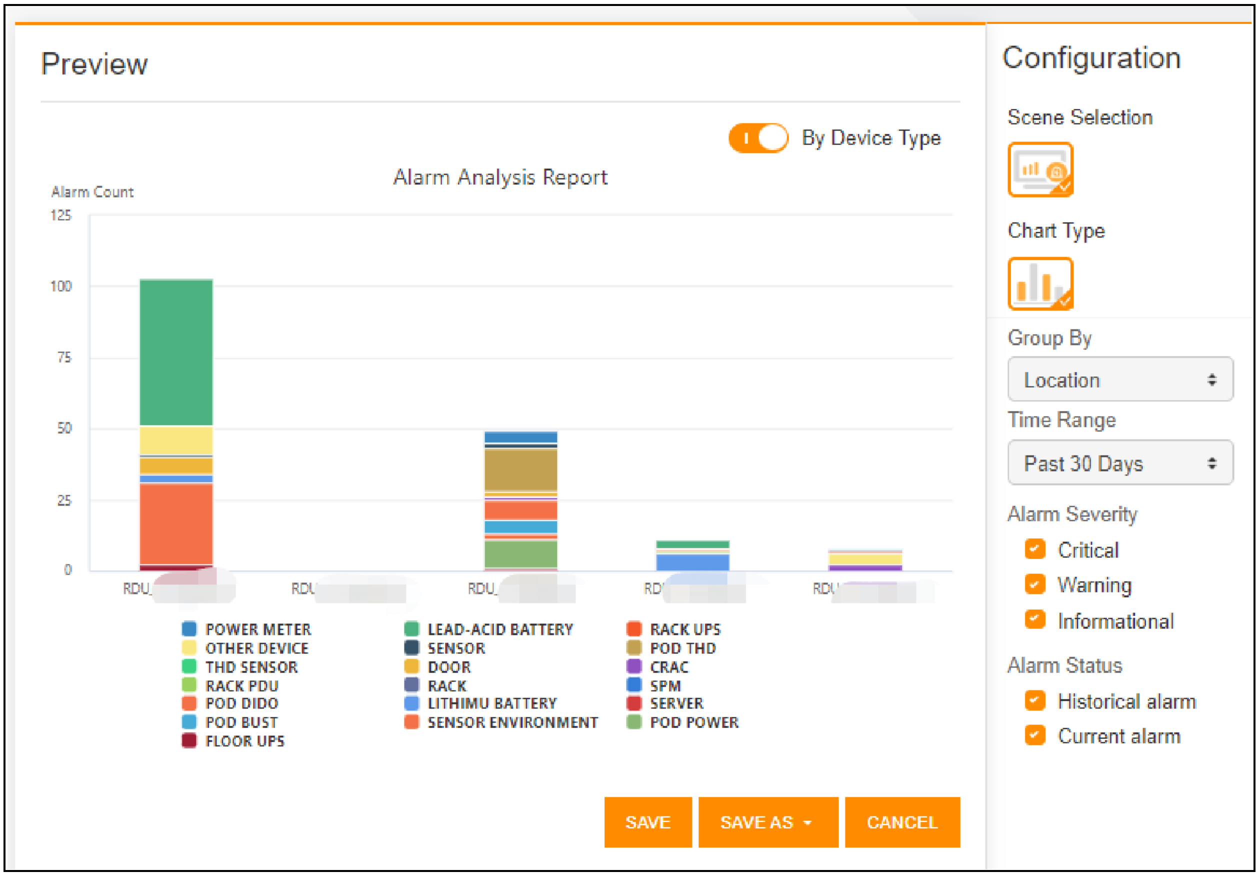
Enter the custom report list from Reports-Custom Reports, click *Add* to jump to the report type selection page, and click the button in the Alarm Analysis Report option to open the alarm analysis report configuration page, as shown in Figure 17.32 below .

Figure 17.32 Configuring an Alarm Analysis Report



From the data source option on the right, you can filter the alarm data source from the three levels of site-device type-device, and you can select different time ranges, alarm levels, and alarm status in the visualization options. If you turn on **By Device Type**, the column of the number of alarms at the site in the preview image will display the number of alarms of each device type under the site, as shown in Figure 17.33 on the next page .

Figure 17.33 Number of Alarms at a Site by Device Type



Click in the lower right corner to save the report of this query to the list of custom reports. You can also choose to save the report as a PDF or PNG. The file is downloaded locally.

NOTE: 1. If the device type is changed after the device is standardized, the alarms generated before the device is standardized will still be classified under the Other Devices category.

2. The custom alarm analysis report cannot count alarms for IPMI devices.

18 System Settings

18.1 Overview

The system settings mainly cover the management of users and permissions, notifications, server settings, and the management of policies such as authorization and backup upgrades. Through the relevant settings, the system administrator can uniformly assign the users, user groups, roles, and contacts existing in the overall management system, and modify the notification settings, security, time, network, authorization, backup and upgrade policies. Only the system administrator has the administrative privilege to upgrade the policies set for users, user groups, and roles, and other users cannot access them.

18.1.1 Functional Modules

- User
- User groups
- Role
- Contacts
- Notification settings
- Server settings for authorization management
- Backups and upgrades

How the notifications are set is described in the Automation Notification on page 203 and will not be repeated in this chapter. License management will be described in detail in License Management on page 401 and the backup and upgrade functions will be described in the following sections Backups and Upgrades on page 405, the server settings will be set in Server Settings on page 393. User management. For more information on other features of user management, refer to the Detailed Features on page 382.

18.2 Quick Start

18.2.1 Rapid Deployment Steps

The steps to use the user management quick start are as follows:

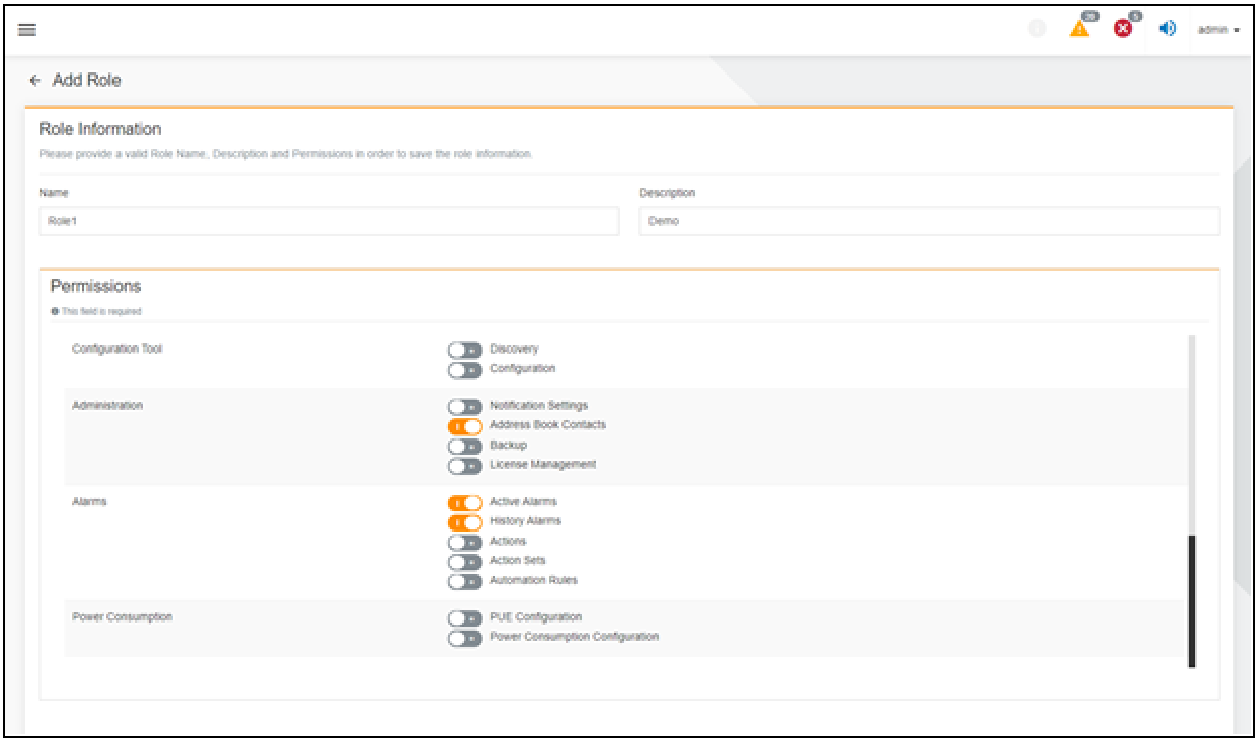
1. Click on the *User* to create and edit user information.
2. Click on the *User Group* to create and edit user group information.
3. Click on the *Role* to create and edit user group information.

18.2.2 Example

Add a custom role and assign the role to a user through a user group.

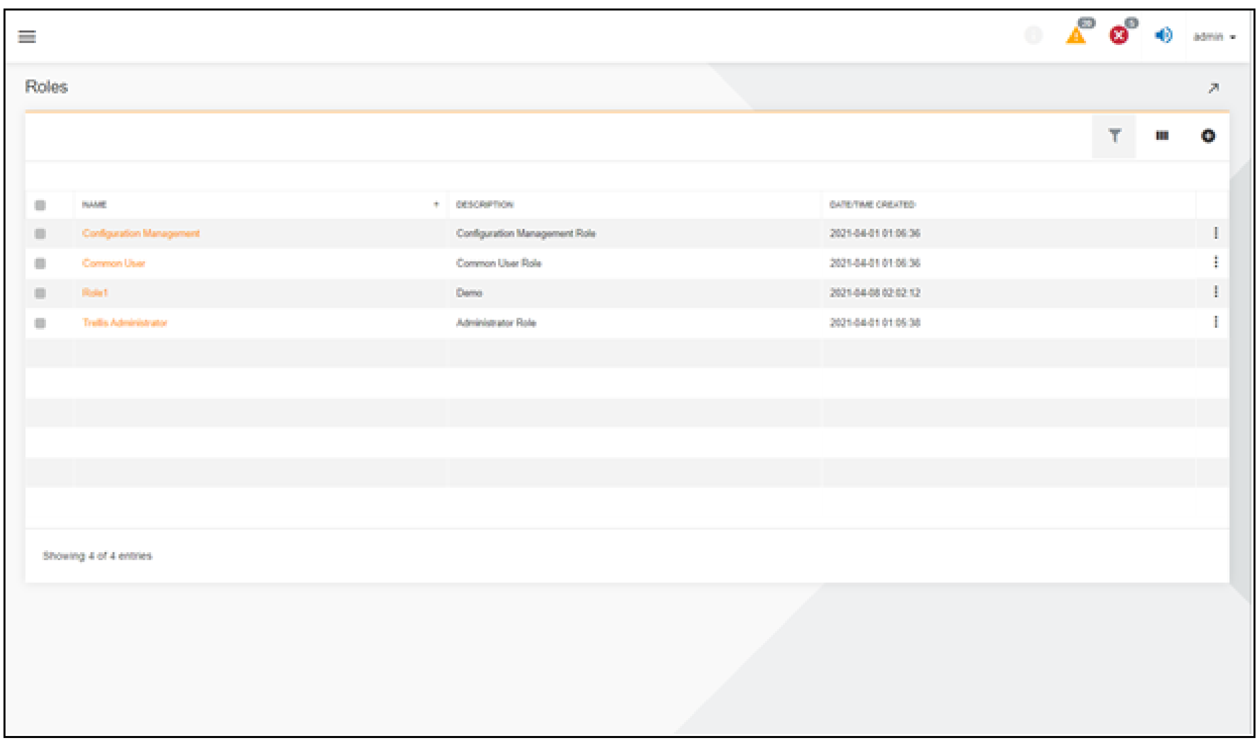
Click the menu system settings, open the role interface, click the *Add* button in the upper right corner, and enter the name (required, no more than 64 characters), description (optional, no more than 128 characters), and permission (required, the default selection of contacts, current alarms, Stored alarms, and monitoring page permissions) to add a role, as shown in **Figure 18.1** on the next page .

Figure 18.1 Adding a Role



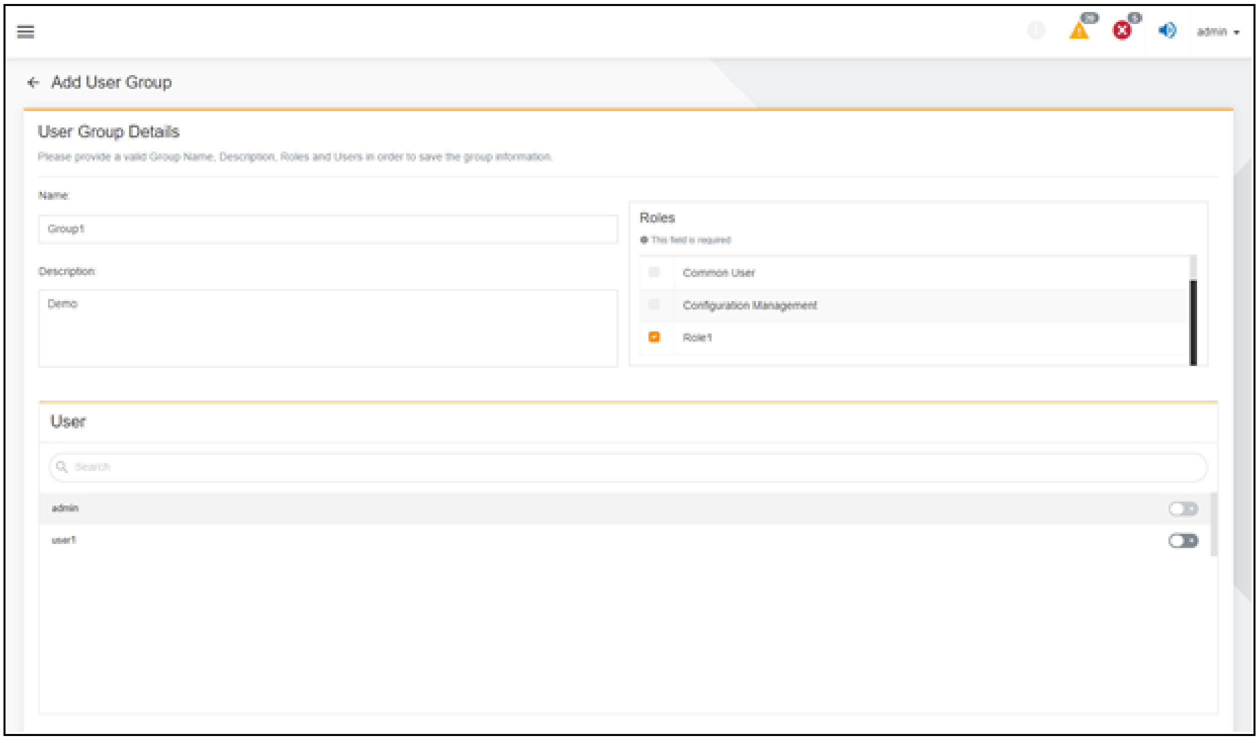
After clicking *Save*, it will be displayed in the list of roles, as shown in **Figure 18.2** below .

Figure 18.2 List of Roles



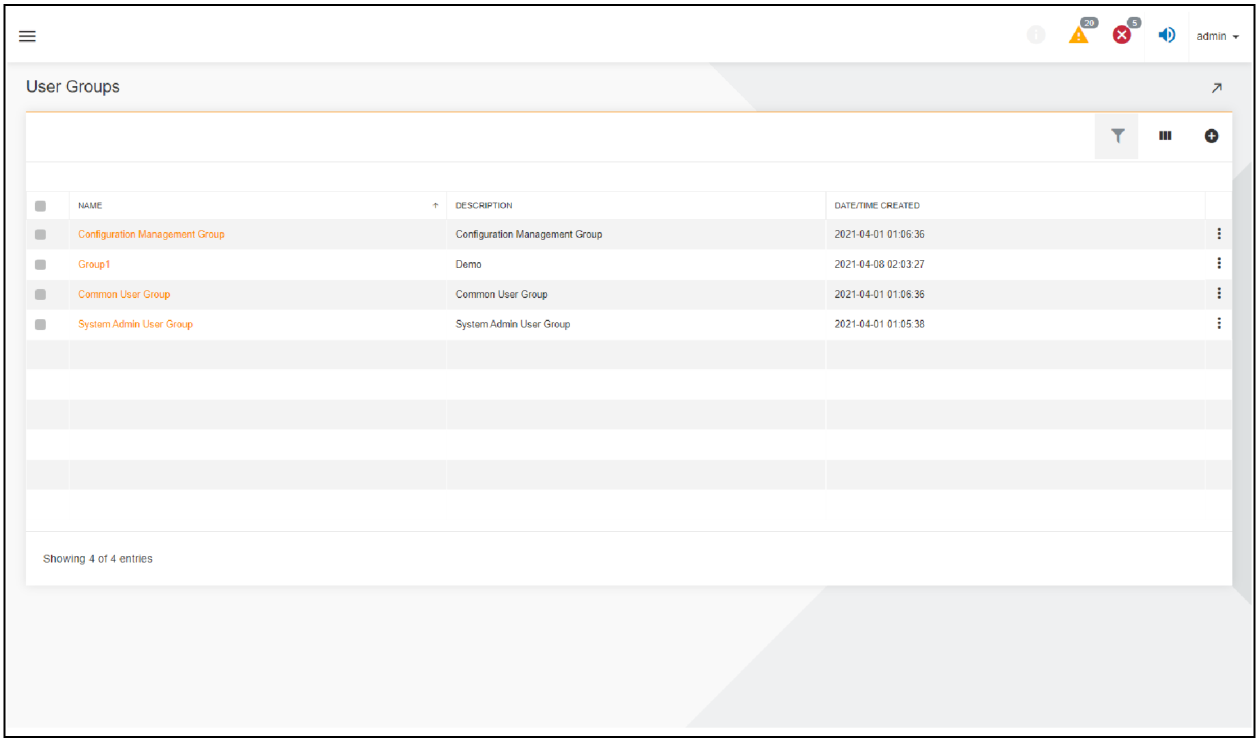
Click the first-level menu system settings, open the user group interface, click the *Add* button in the upper right corner, and enter the name (required, no more than 64 characters), description (optional, no more than 128 characters), select the new role you just created (required, multiple selections are supported, administrator role cannot be selected by default), and user (optional) to add a user group, as shown in **Figure 18.3** below .

Figure 18.3 Adding a User Group



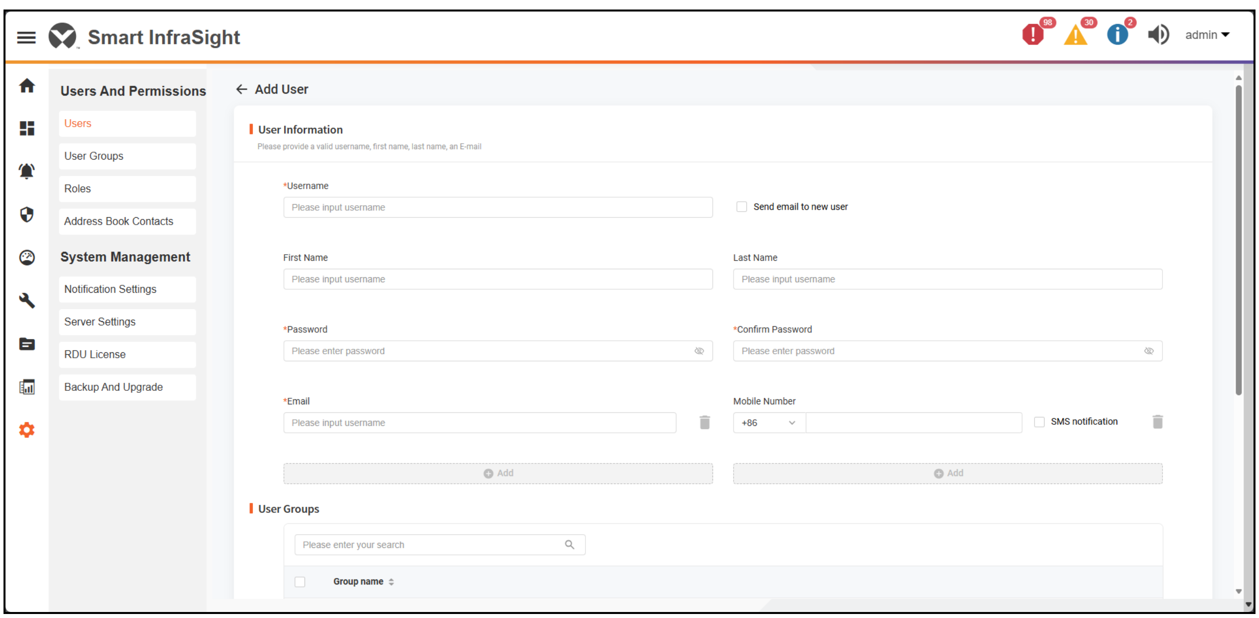
After clicking *Save*, the list of user groups is displayed as shown in **Figure 18.4** on the next page .

Figure 18.4 A List of User Groups



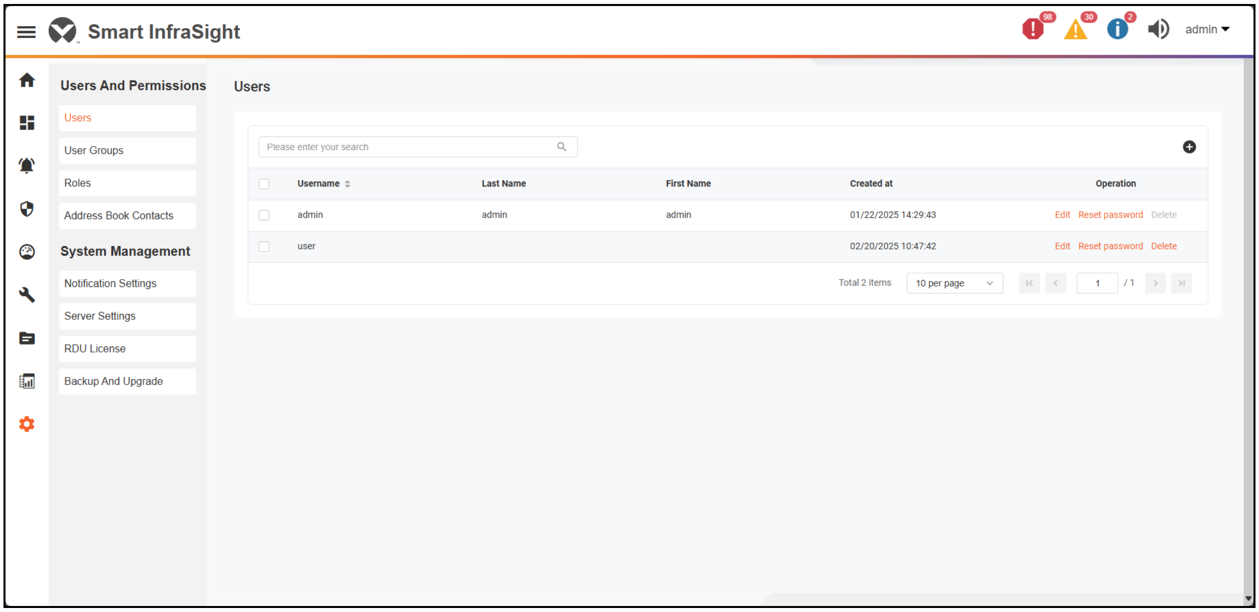
Click the first-level *Settings* menu, the user interface will be opened by default, click the *Add* button in the upper right corner, enter the user account name (required), email (required), and select the newly created user group (optional) to add the user in the pop-up Add User Information interface, as shown in **Figure 18.5** below .

Figure 18.5 Adding a User



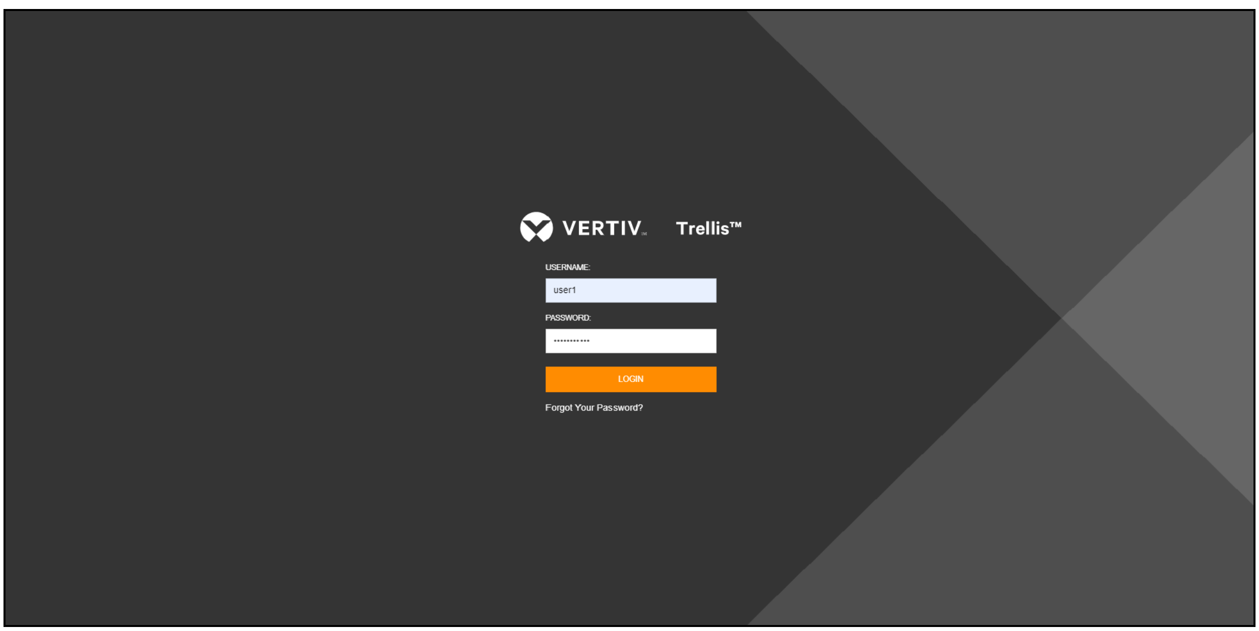
When you click *Save*, the list of users will appear as **Figure 18.6** on the facing page .

Figure 18.6 User List



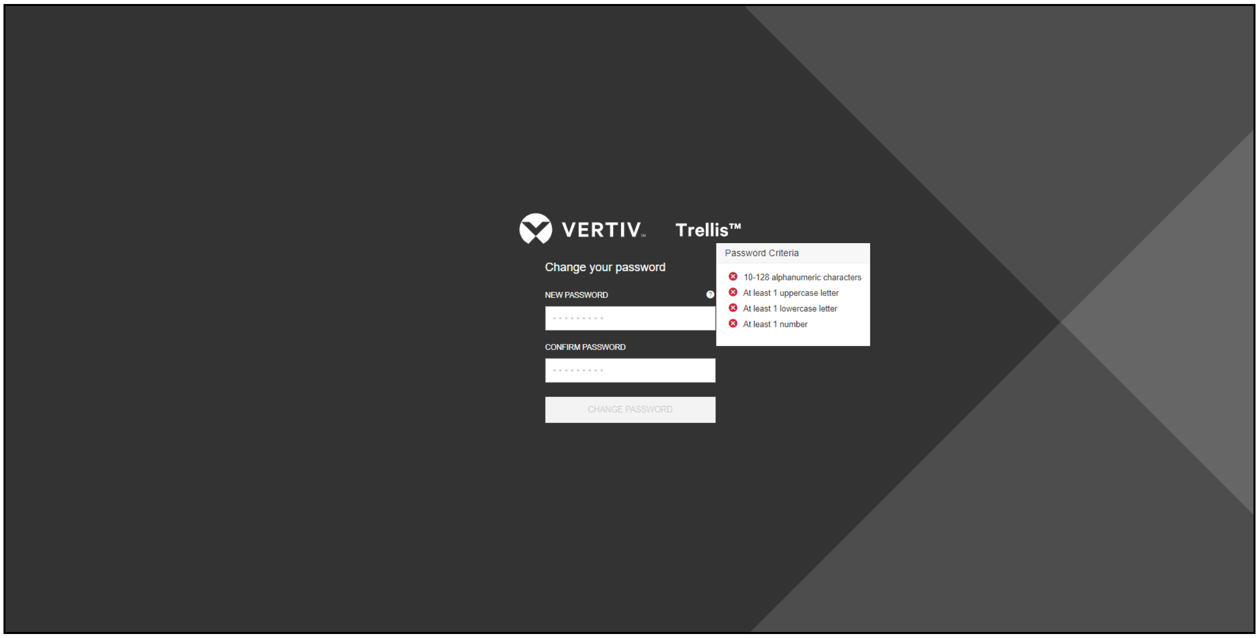
Click *Log-in* to reset your password, as shown in **Figure 18.7** below .

Figure 18.7 User Login



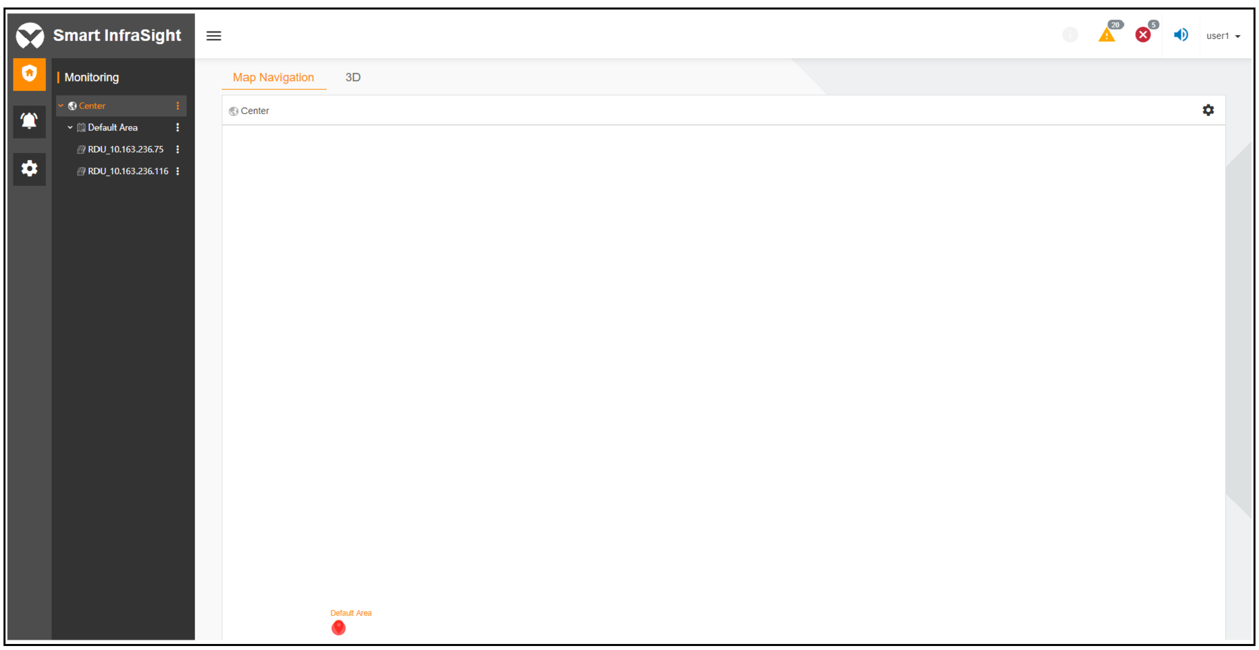
Change your password and login again, as shown in **Figure 18.8** on the next page .

Figure 18.8 Resetting the Password



After the user successfully logs in, you will get the privileged access to the specified role, as shown in **Figure 18.9** below .

Figure 18.9 Defining the Role Access Permissions



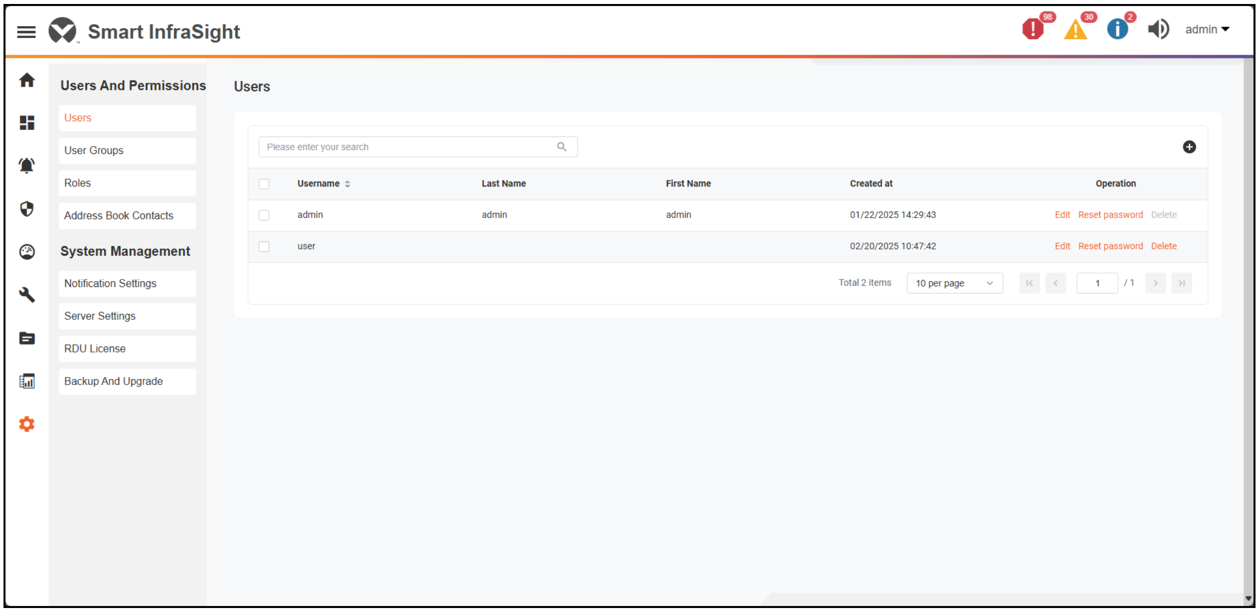
18.3 Detailed Features

In the system settings interface, users, roles, user groups, and system settings can only be configured by admin.

18.3.1 List of Users

Click the first-level *System Config* menu, the user interface will be opened by default, and the list of users currently in the system will be displayed, among which only admin is the administrator user by default, and the other users are ordinary users. The details like username, first name, and last name are displayed in the list, as shown in **Figure 18.10** below .

Figure 18.10 List of Users



18.3.2 Adding the Users

Click the *Add* button from the user list in the upper right corner, and enter the user's username (required), first name (optional, no character limit), surname (optional, no character limit), password (required), confirm password (required), email (required), phone number (optional), user group (optional), localization settings to add users on the Add User Information page.

The account name cannot be repeated, at least 1-64 characters are required for full English, 1-64 characters for Chinese, and 1-64 characters for first and last name.

The password must be in 10-108 characters in length and must contain uppercase and lowercase characters and numbers. Confirm that the password input must be the same as the password. If the **Send Password Change Email** option is selected, the username and password will be sent to all email addresses of the current user when saving, and the email content will be in the language following the **Notification Language Setting** in the **Notification Settings**, and the email content is as follows:

Topic: New to Smart Infrasight

Content: User XXX in your Smart Insight system (XX.XX.XX.XX) has been created by the system administrator, please login with a temporary password XXXX, and set a new password after logging in. Don't share your temporary password with others.

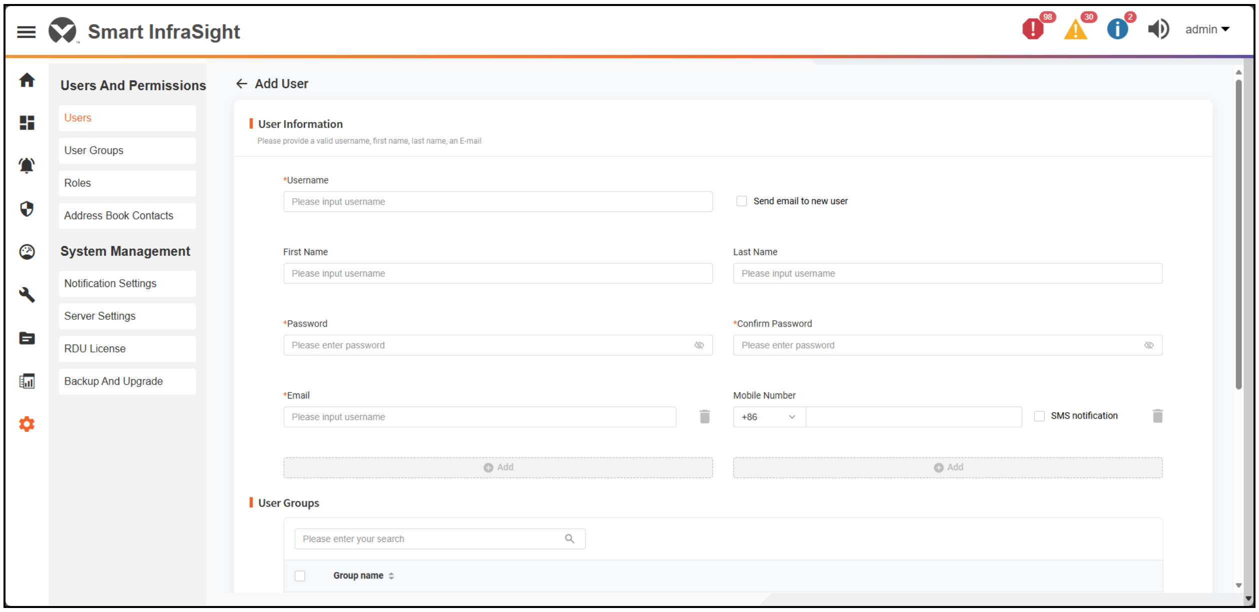
After the user logs in with the initial password, the system automatically redirects the user to the Change Password page to guide the user to change the password. As shown in **Figure 18.11** on the next page .

Among them, the account name cannot be repeated, if it is full English, it needs at least 1-64 characters, the Username cannot be mixed in Chinese and English, and Chinese needs 1-64 characters, surname and name 1-64 characters.

The email format needs to meet: standard email format, the mailbox prefix can be numbers, letters, full stops in English, underscores and connecting lines, the mailbox suffix needs to have at least two words, the top-level domain name is 2~4 digits, and the default prefix and suffix do not start with underscore (_) or hyphen (-). At the end, the default password is **Password123**.

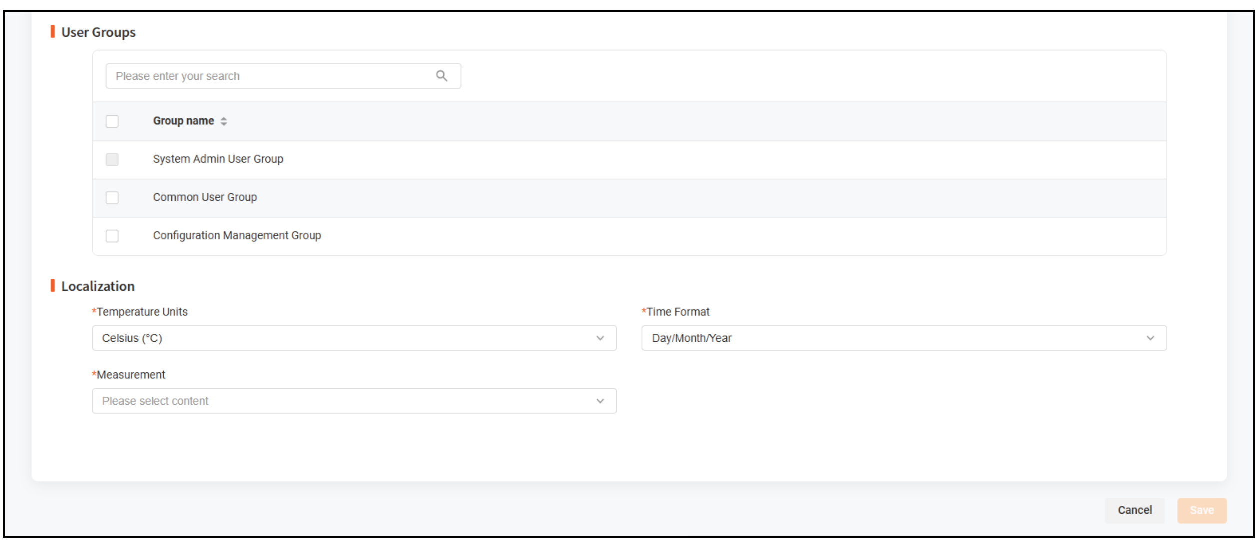
NOTE: Once saved, the account name cannot be modified. If the Username is not filled, it will be prompted that the Username is required and cannot be clicked to save. If the e-mail address is not entered, you cannot click the Save button. If you do not select a user group, you cannot click *Save*.

Figure 18.11 Adding the User



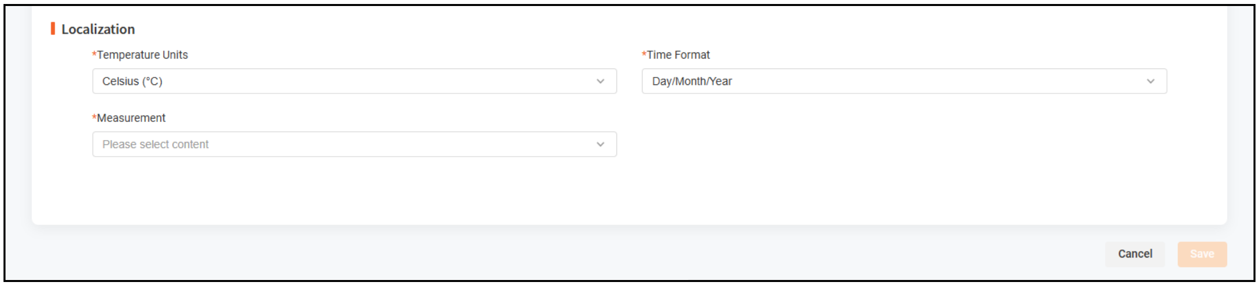
Select the user group to which the user needs to be assigned: Select the checkbox on the left side of the user group to be assigned, as shown in **Figure 18.12** below .

Figure 18.12 Selecting the User Group



Localized Configuration: Select the localized configuration required by the user, including temperature units (Fahrenheit and Celsius), time format (month/day/year, day/month/year), and measurement units (imperial and metric), as shown in **Figure 18.13** below . After the preceding content is configured, the temperature unit, time format, and measurement unit (length, width, height, weight, area, volume, etc.) are displayed on the page. The default localization configuration for new users is the localization configuration of the admin account, which can be modified again by clicking the username in the upper right corner of the system.

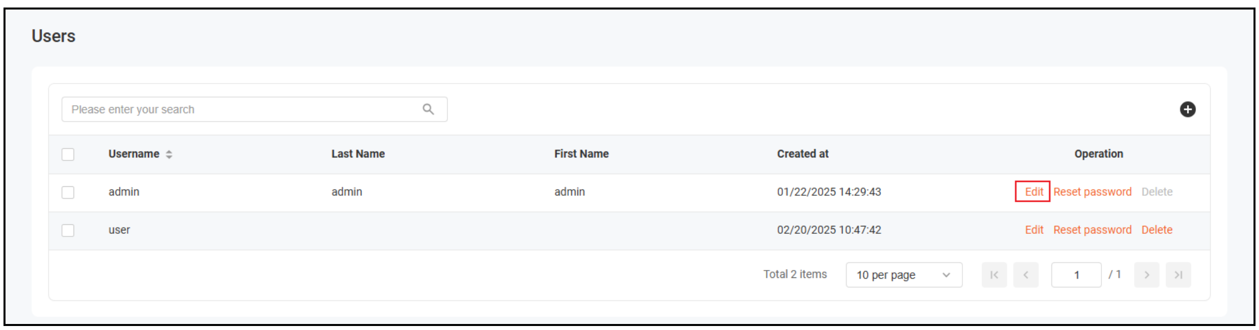
Figure 18.13 Localized Configuration



18.3.3 Editing the User

Click the edit button of the operation column on the right side of the user list row to enter the editing page, as shown in **Figure 18.14** below , modify the user information to be edited, and then click Save to complete the update of the user.

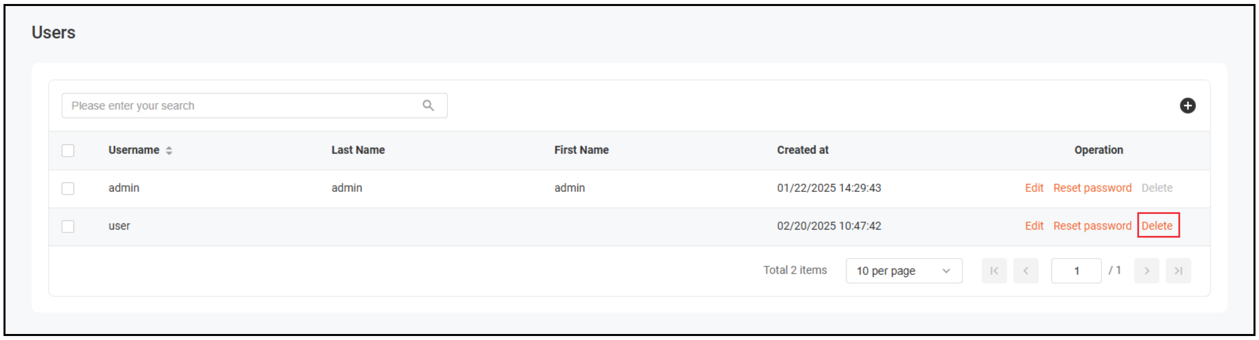
Figure 18.14 Editing the User



18.3.4 Deleting the User

Click the first-level menu, the user interface will open by default, click the delete button in the operation column on the right side of the user list row, as shown in **Figure 18.15** on the next page , and select confirm in the pop-up window.

Figure 18.15 Deleting the User



NOTE: The admin cannot delete himself, but can only delete other users.

Reset the User's Password

Figure 18.16 Reset the user's password

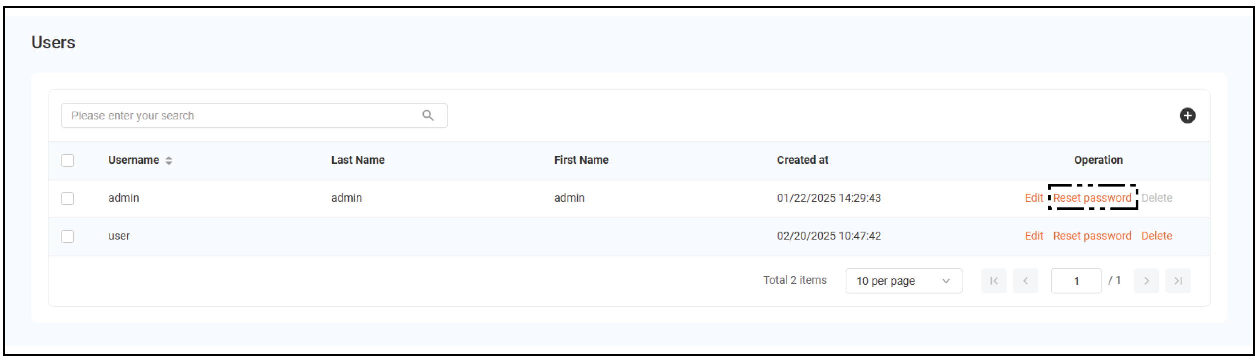
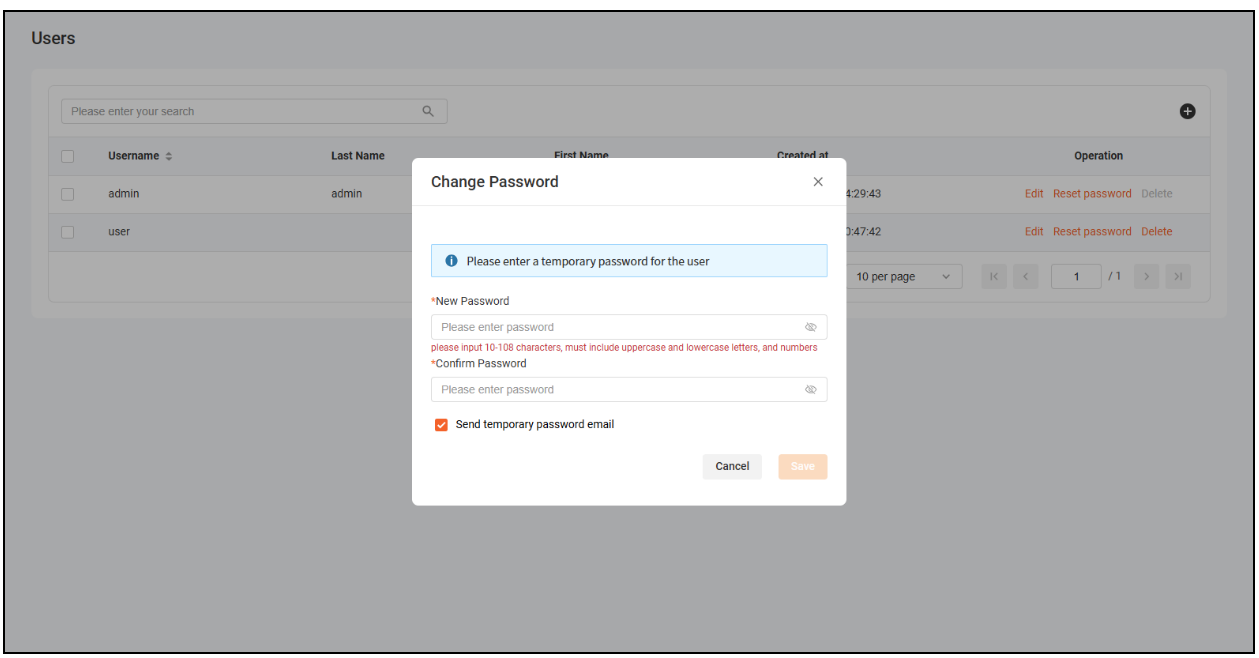


Figure 18.17 Reset the User's Password



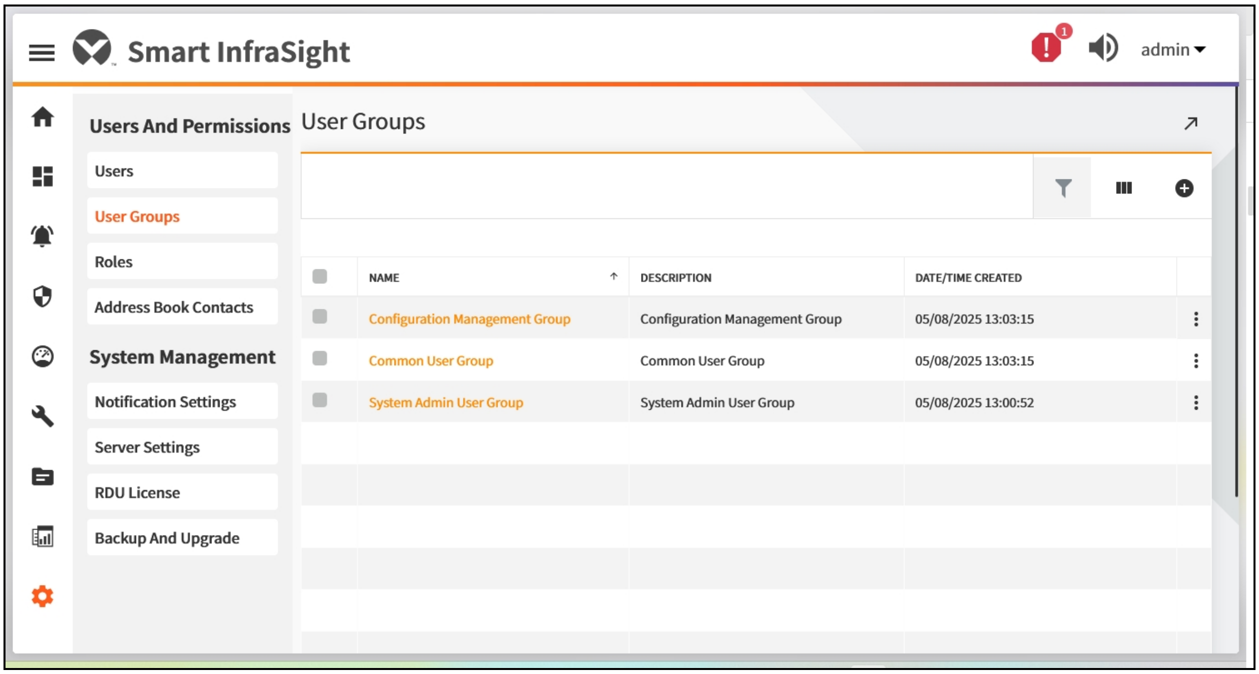
Click the reset password button in the operation column on the right side of the user list row, enter the temporary password in the pop-up window, confirm the password and save it to change the user password to the entered temporary password, if the **Send password change email** option is checked, the temporary password will be sent to all mailboxes of the current user when saving, and the language used in the email content follows the **Notification Language Setting** in the **Notification Settings**.

After the user successfully logs in with the temporary password, the system automatically redirects the user to the Change Password page to guide the user to change the password.

18.3.5 List of User Groups

Click on the Level 1 *Settings* menu, which shows the 3 user groups that exist by default in the current system, as shown in **Figure 18.18** below . The default user group cannot be deleted, and the system administrator user group cannot be edited.

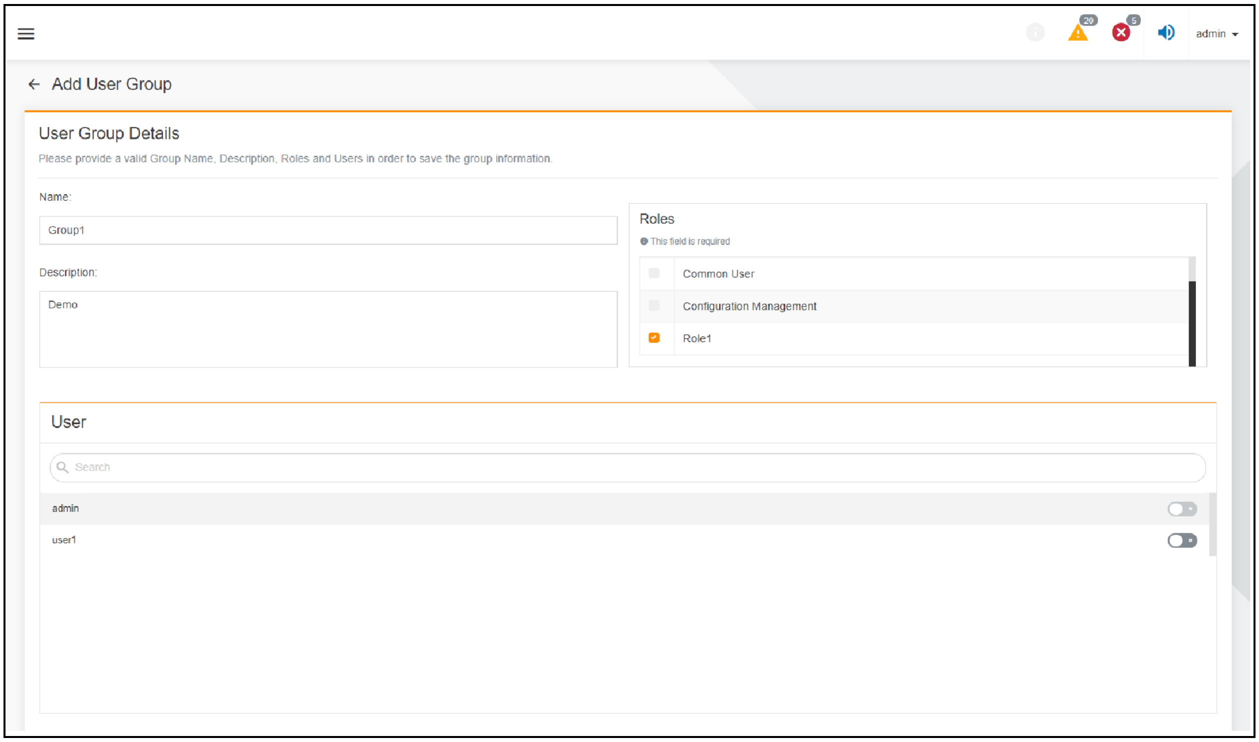
Figure 18.18 User Group List



18.3.6 Adding the User Group

Click the first-level system settings menu, open the user group interface, click on *add* in the upper right corner, and enter the name (required, no more than 64 characters), description (optional, no more than 128 characters), role (required, multiple selections are supported, administrator role cannot be selected by default), and user (optional) to add a user group.

Figure 18.19 Adding a User Group



NOTE: 1. The name of the user group cannot be repeated.

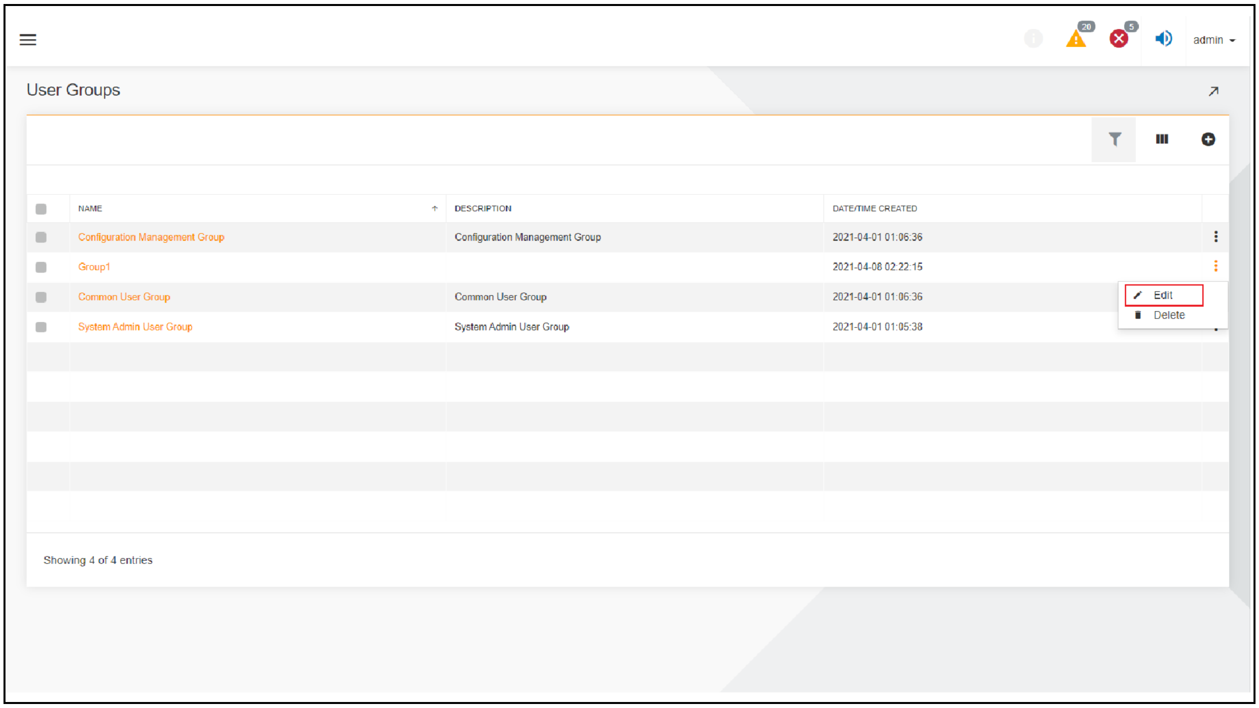
2. In English, it is not allowed to contain special characters such as vertical lines, single and double quotation marks, and slashes.

3. Special characters such as vertical lines, spaces, and slashes cannot be included in the Chinese environment.

18.3.7 Editing the User Group

On the User List page, click on the *ellipses* on the right side of the user group list, select Edit Options, jump to the Edit User Group page as shown in Figure 18.20 on the facing page , enter the information of the user group you want to edit, including the user group name and role as mandatory, and then click *Edit* to edit the user group.

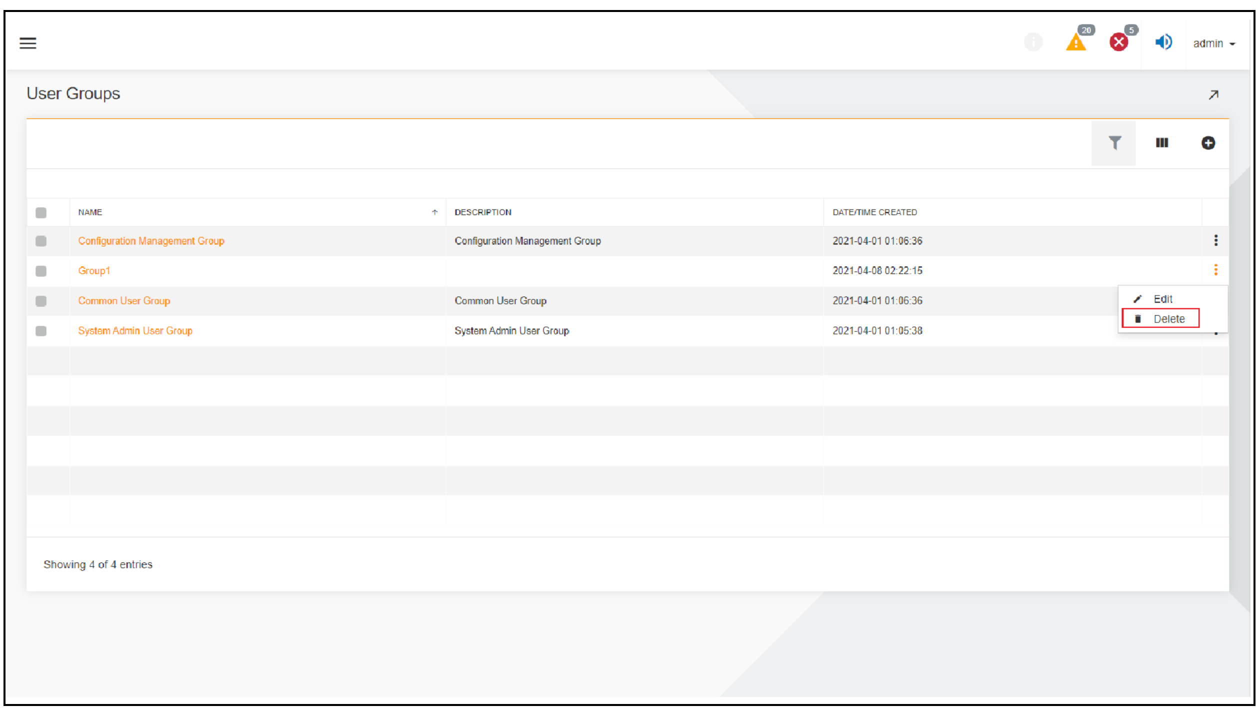
Figure 18.20 Editing the User Group



18.3.8 Deleting a User Group

On the User Group List page, click on the *ellipses* on the right side of the user group list row and select the *Delete* option. As shown in Figure 18.21 below .

Figure 18.21 Deleting a User Group

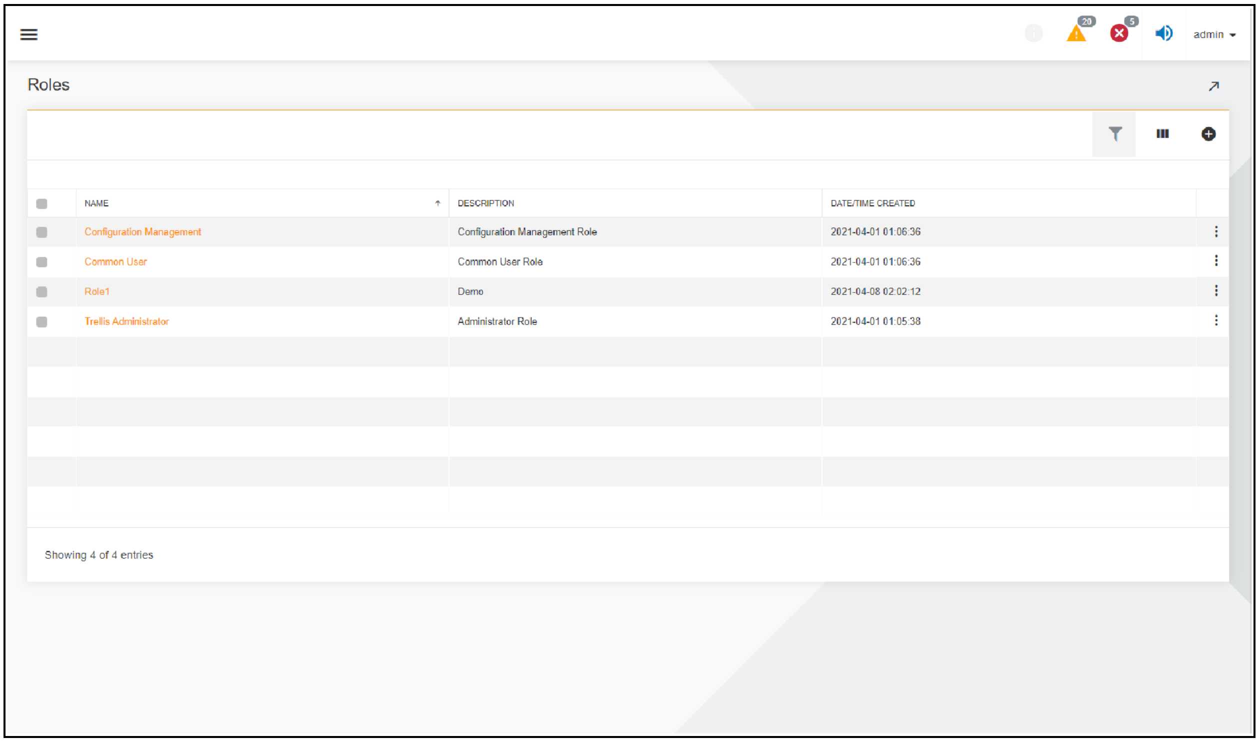


NOTE: The three default user groups cannot be deleted, and custom user groups can be deleted.

18.3.9 List of Roles

Click on the menu System Settings. The role menu shows the 3 roles as shown in Figure 18.22 below that exist by default in the current system, and the default roles cannot be deleted or modified.

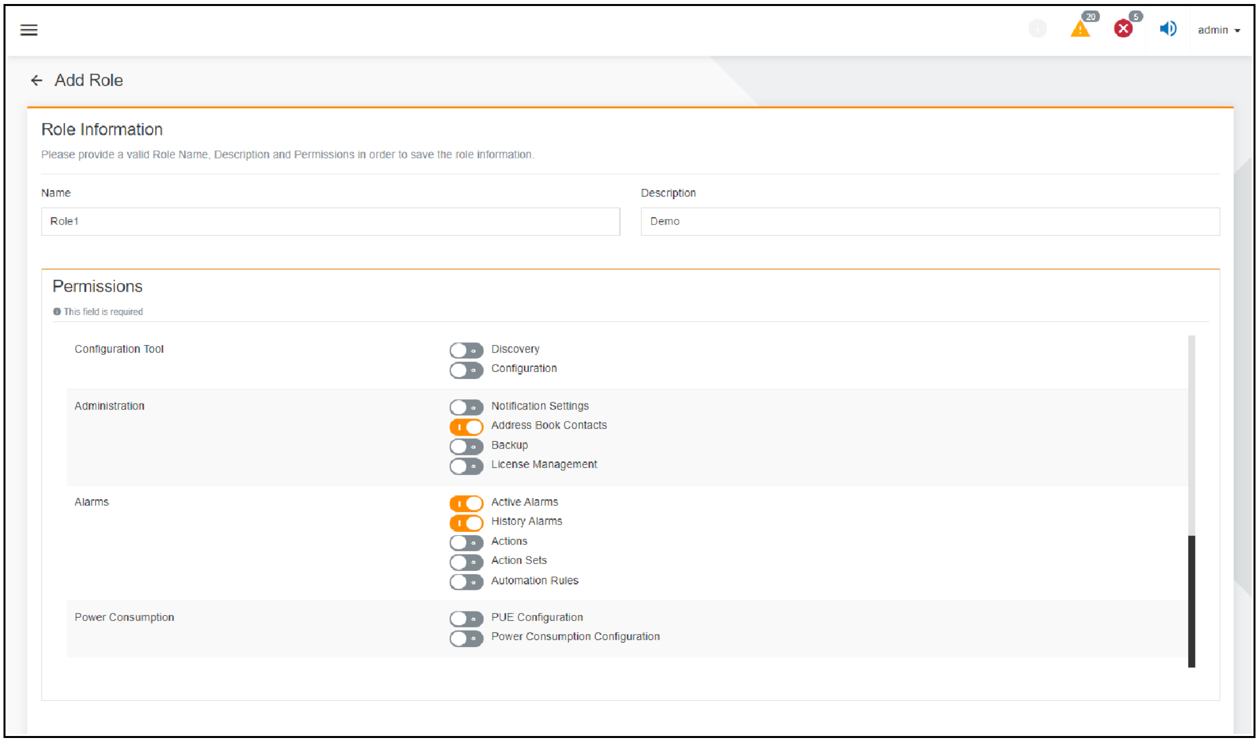
Figure 18.22 List of Roles



18.3.10 Adding a Role

Click the menu system settings, open the role interface, click on *add* in the upper right corner, and enter the name (required, no more than 64 characters), description (optional, no more than 128 characters), and permission (required, the default selection of contacts, current alarms, Stored alarms, and monitoring page permissions) to add a role, as shown in Figure 18.23 on the facing page .

Figure 18.23 Adding a Role



NOTE: 1. The role name cannot be repeated.

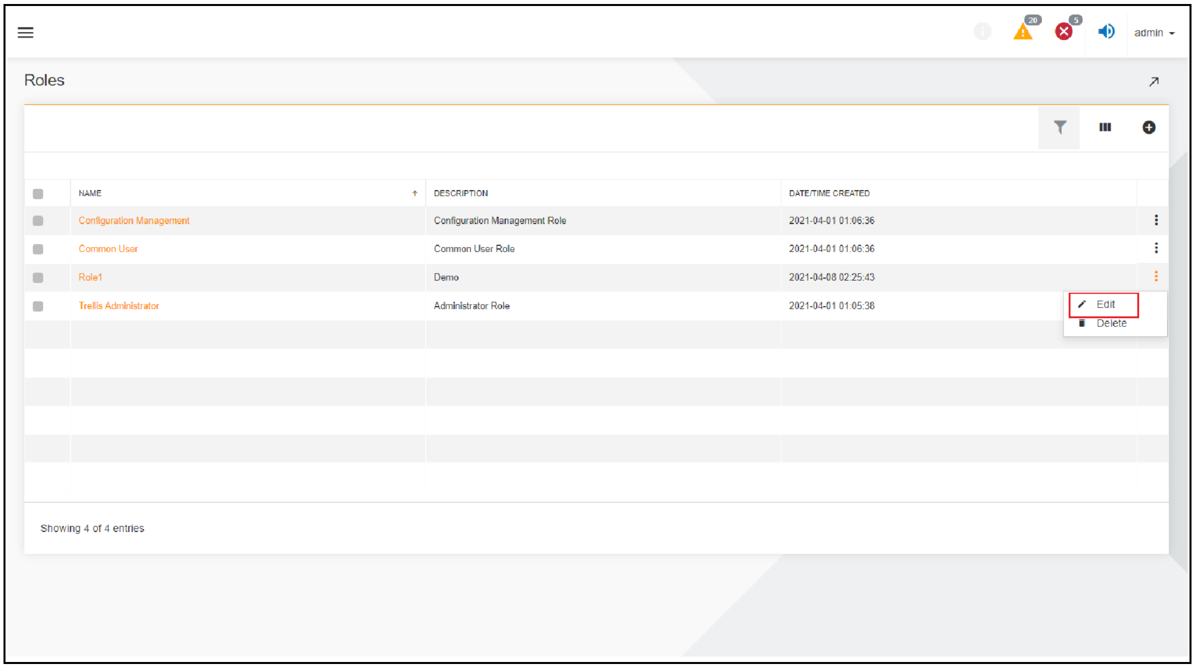
2. Character names cannot contain special characters such as vertical lines, single and double quotation marks, and slashes in English.

3. The default permissions cannot be edited, and the user must have the default permissions.

18.3.11 Editing the Role

On the role list page, click on the *ellipses* on the right side of the role list row, then select *Edit* Options, as shown in Figure 18.24 on the next page , the Edit Role interface pops up, enter the information of the role you want to edit, where the role name is mandatory, and then click *Save* to update the role.

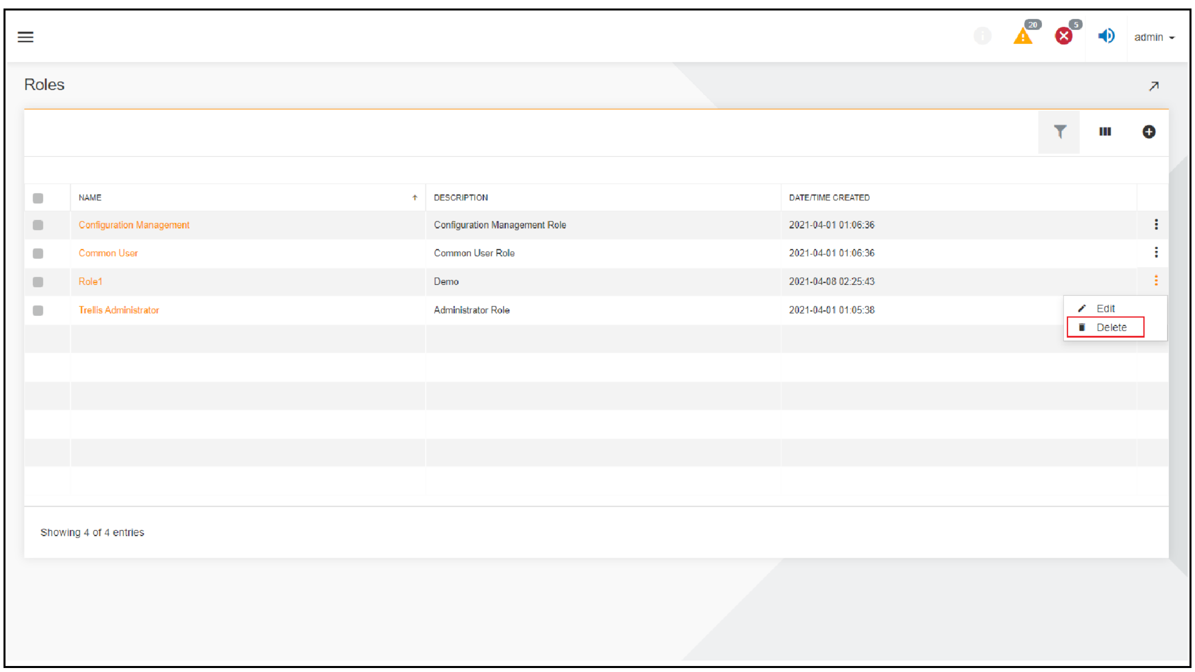
Figure 18.24 Editing the Role



18.3.12 Deleting the Role

On the Role List screen, click on the *ellipses* to the right of the list row, and then click the *Delete* option, for the role you wish to delete, as shown in **Figure 18.25** below .

Figure 18.25 Deleting a Role



NOTE: The three default roles cannot be deleted, and custom roles can be deleted.

19 Server Settings

19.1 Overview

Server settings include three functions: security settings, time settings, and network settings. In the security settings, you can set the login user timeout logout time and replace the system SSL certificate, and the user can replace the system's self-signed SSL certificate with a certificate verified by the user to provide network access security. The automatic system time calibration in the time setting can make the time of the server match the time of the client, and the time zone setting can set the time zone information of the server. The time setting ensures that the server and the client maintain the same time zone and time. Avoid inconsistencies between time zones and times, such as the time when the notification is sent and the time information received by email or SMS. Network settings: You can set the configuration of the system NIC.

19.2 Quick Start

19.2.1 Rapid deployment steps

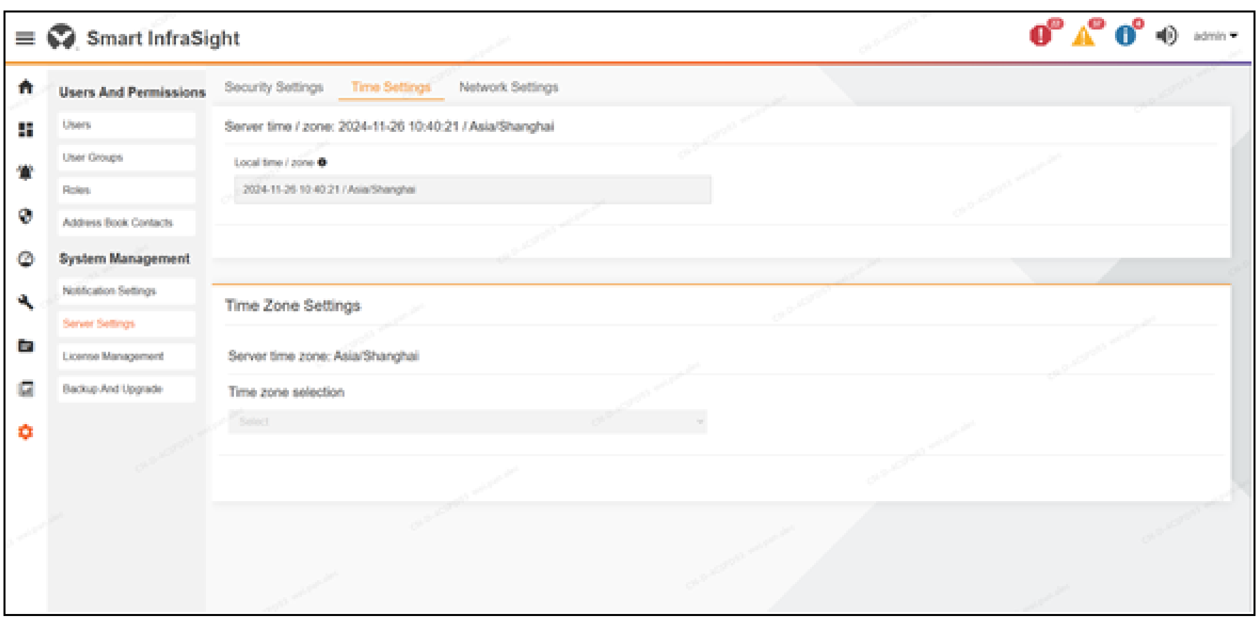
The steps to set up the system quickly are as follows:

1. Click on the *Security Settings* tab to configure the session timeout and replace the SSL certificate.
2. Click on the *Time Settings* to proofread the server time and set the time zone.
3. Click on the *Network Settings* to set the NIC information.

19.2.2 Example

Time setting Path: System settings --> Server settings--> Time setting, as shown in Figure 19.1 below .

Figure 19.1 Time Setting



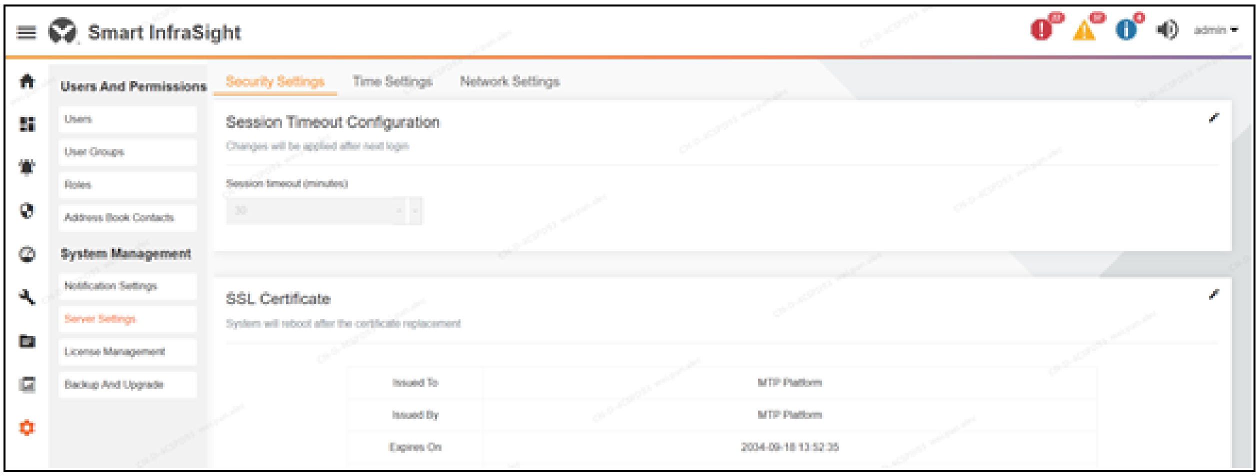
19.3 Detailed Features

19.3.1 Security Settings

Session Timeout Settings

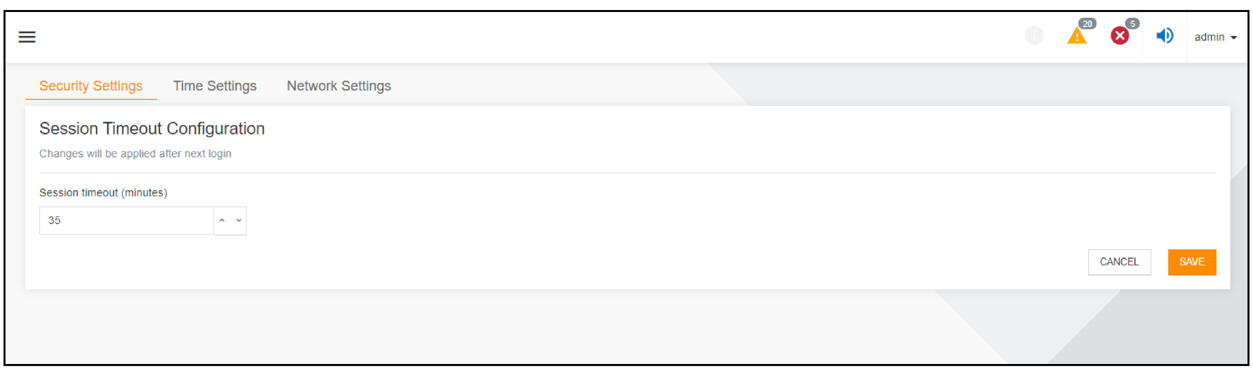
Click on the menu *System Settings*. Then click on the *Server settings*, with the Security Settings tab selected as default. As shown in **Figure 19.2** below .

Figure 19.2 Security Settings



To set the session timeout, click on *Edit* in the upper-right corner to enter the editing settings, as shown in **Figure 19.3** below .

Figure 19.3 Session Timeout Configuration



Set the session timeout period, which can be set to a maximum of one day (1440 minutes), and click Save to take effect immediately after the setting is completed.

Replacing the SSL Certificate

The SI system uses a self-signed certificate by default, and users can upload a trusted certificate signed by the certification authority as shown in **Figure 19.4** on the facing page and replace the original certificate. Click *edit* on it in the top right corner to open the Replace Certificate window, as shown in **Figure 19.5** on the facing page .

Figure 19.4 SSL Certificate Window

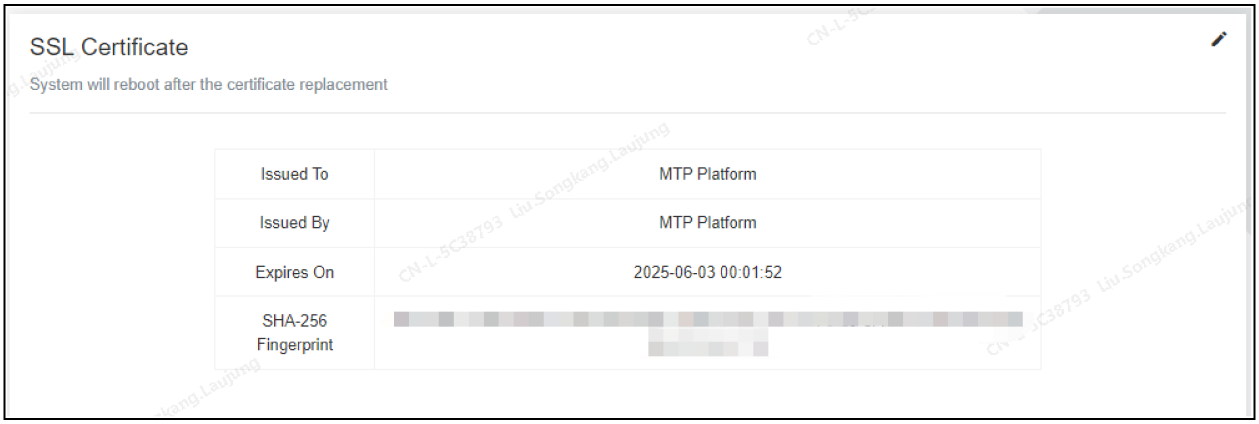
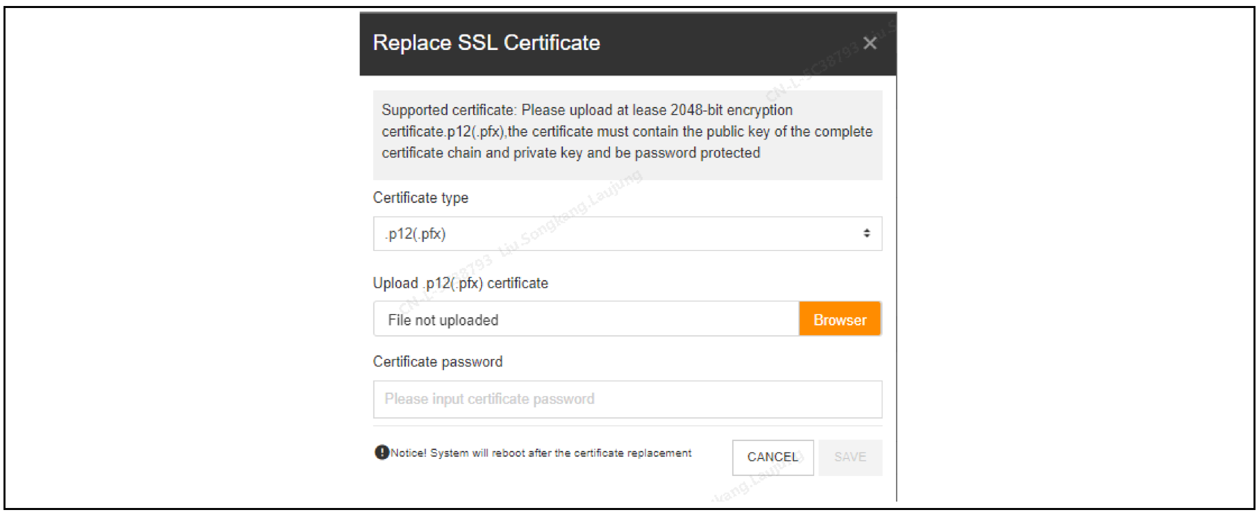


Figure 19.5 Replacing SSL Certificate Window



You need to merge the public key and private key of the replacement certificate into a certificate file in .p12 format in advance, click *Upload* to the system, enter the certificate password, click *Save*, and the SI system will restart after saving successfully.

NOTE: 1. The uploaded certificate encryption requirements need to meet RSA 2048.

2. The uploaded .p12 certificate file can contain only one certificate and needs to contain matching public and private keys.

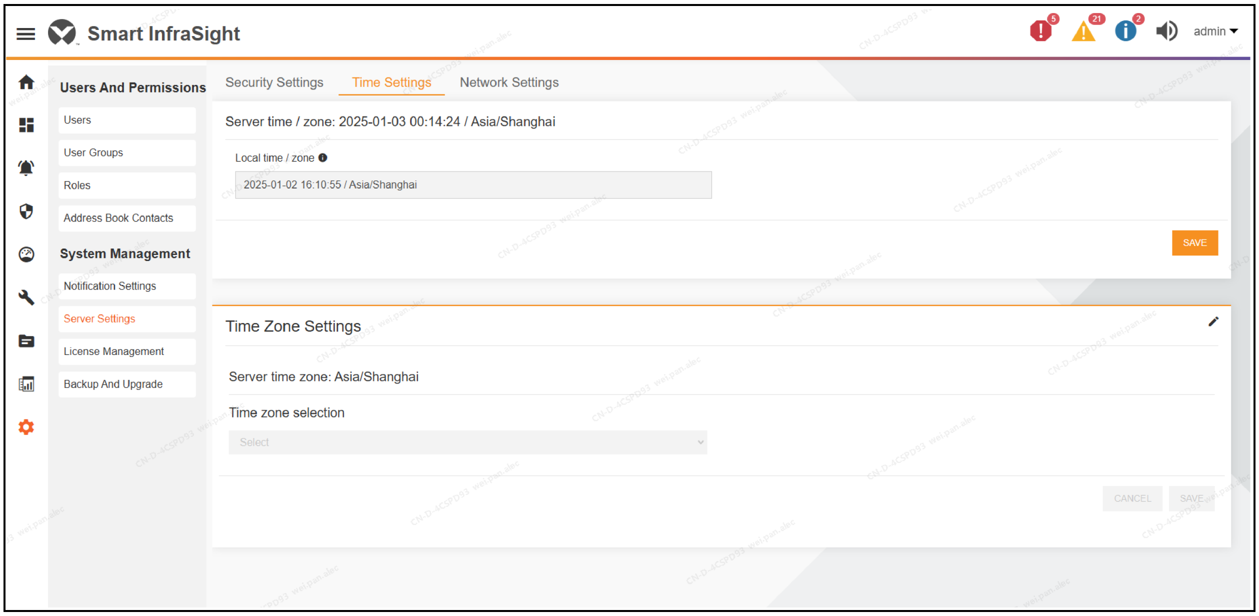
3. The uploaded certificate needs to ensure that it has not expired.

19.3.2 Time Setting

Correcting the Server Time

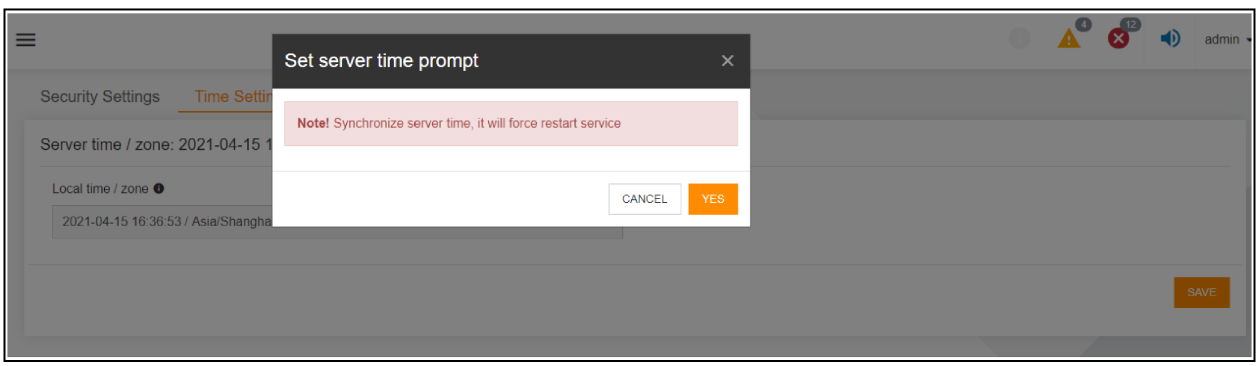
Click on the menu *System Settings*. Then click on the *Server settings*, then click on *Time setting*, as shown in **Figure 19.6** on the next page .

Figure 19.6 Using the Local Time Calibration



1. Click *Save*, which will prompt you to set up the server to restart the service, as shown in **Figure 19.7** below .

Figure 19.7 Setting the Server Time Prompt



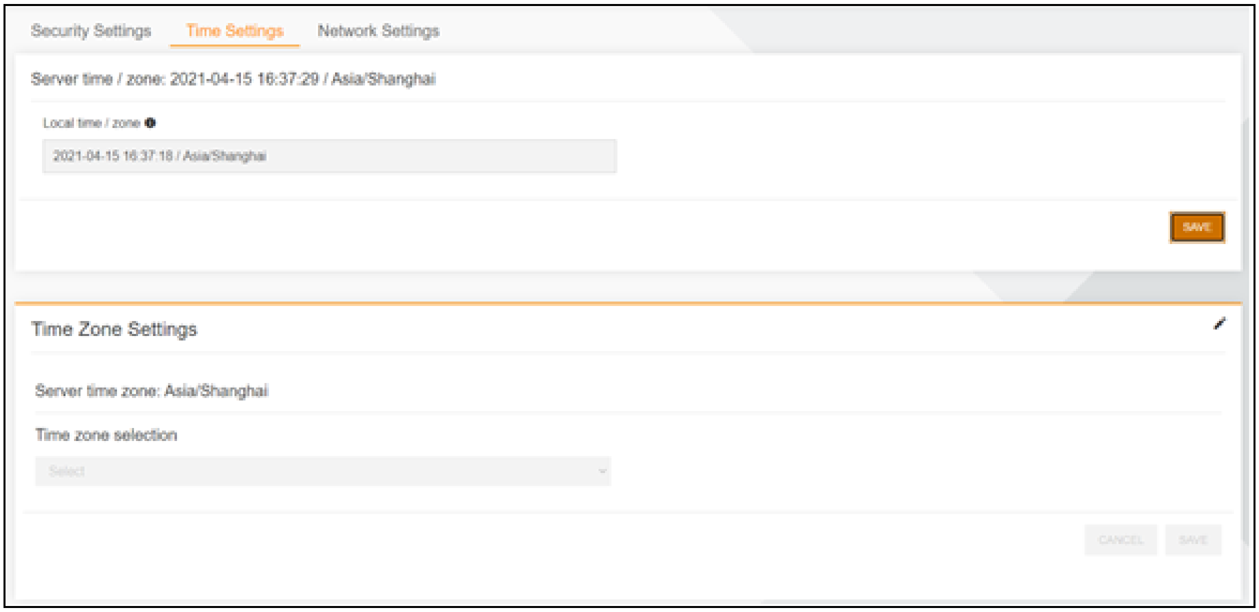
NOTE: When the system calibrates the operation, please do not perform other configuration operations, otherwise the correctness and reliability of the data will be affected. At the same time, keep it on.

2. Confirm that you need to click *Save*, the system will restart, wait, and log in again.

Time Zone Setting

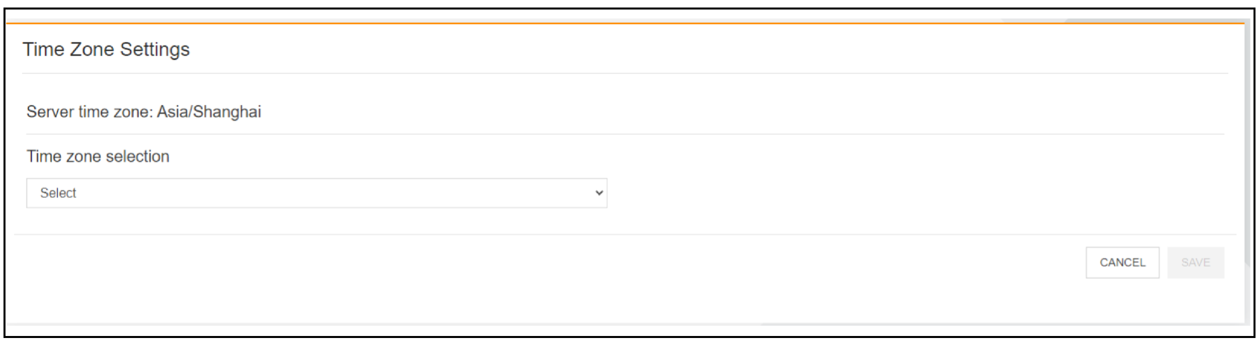
Click on the menu *System Settings*. Then click on the *Server settings*, then click on *Time setting*, as shown in **Figure 19.8** on the facing page .

Figure 19.8 Setting the Server Time Zone



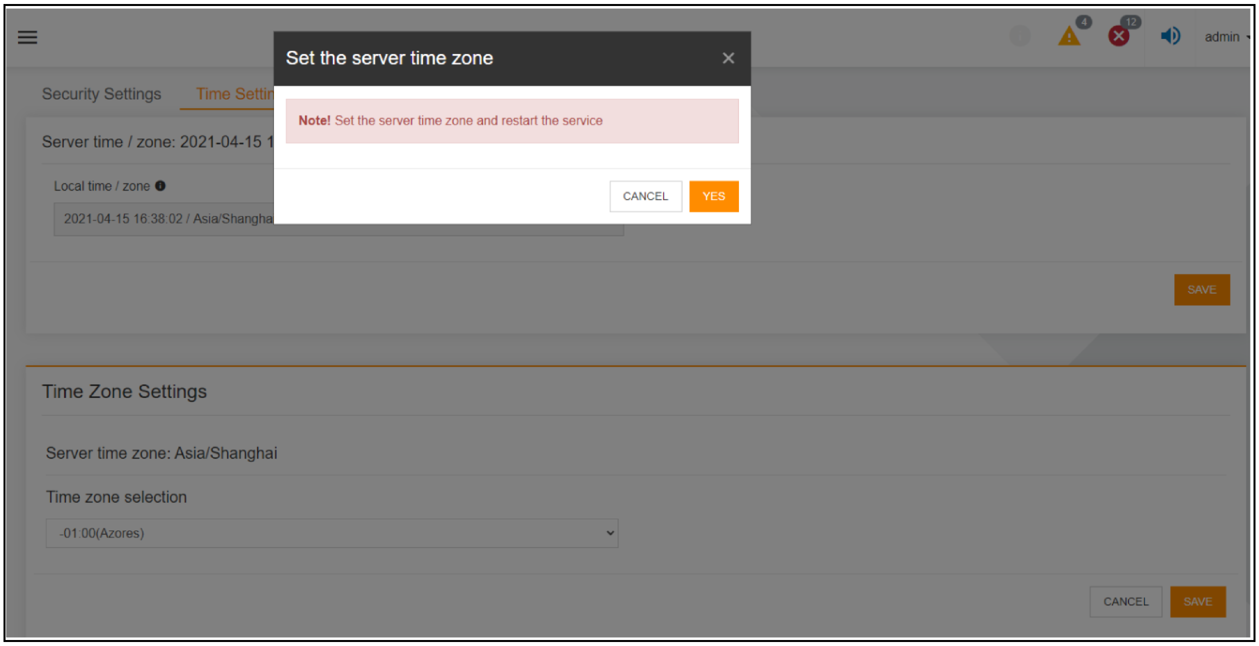
1. Click on the right to make the time zone setting editable and select the time zone you want to set, as shown in Figure 19.9 below .

Figure 19.9 Selecting a Server Time Zone



2. After selecting the time zone, click *Save*, which will remind you to set up the server to restart the service, as shown in Figure 19.10 on the next page .

Figure 19.10 Setting the Server Time Zone

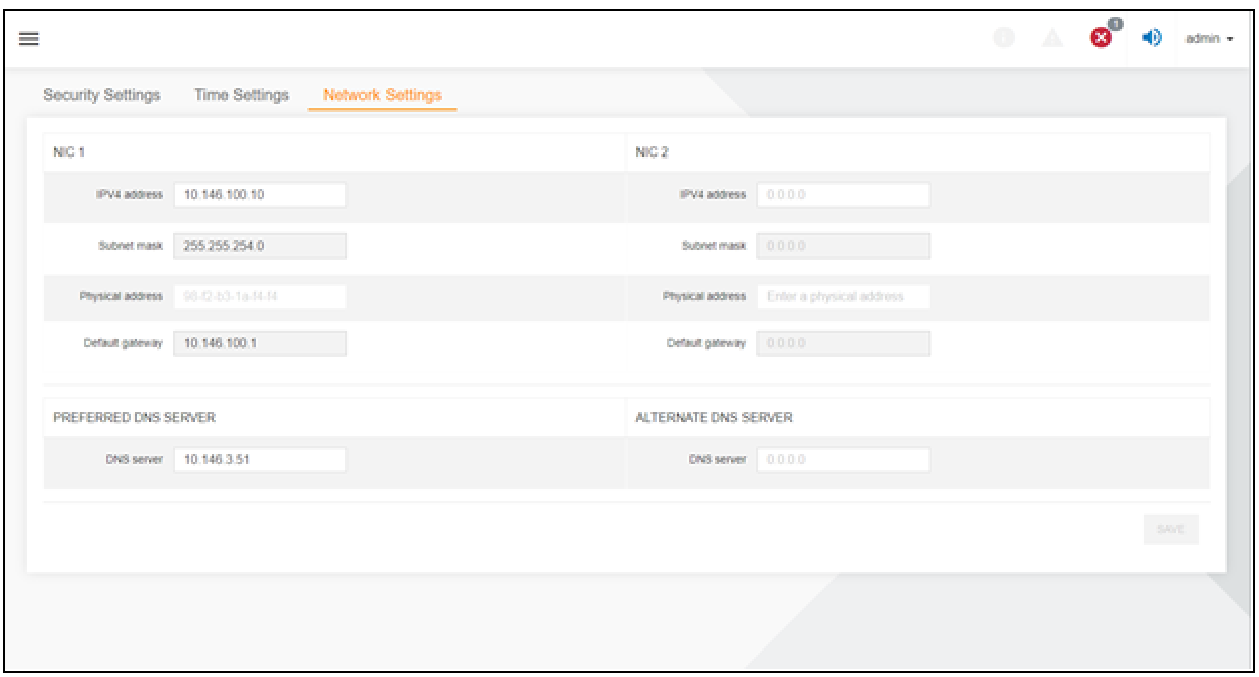


3. Click on the *Save* in the prompt box to restart the server, and log in to the system again after the reboot is successful.

19.3.3 Network Settings

Click on the menu *System Settings*. Then click on the *Server settings*, then click on *Time setting*. check the Network Settings tab. As show in **Figure 19.11** below .

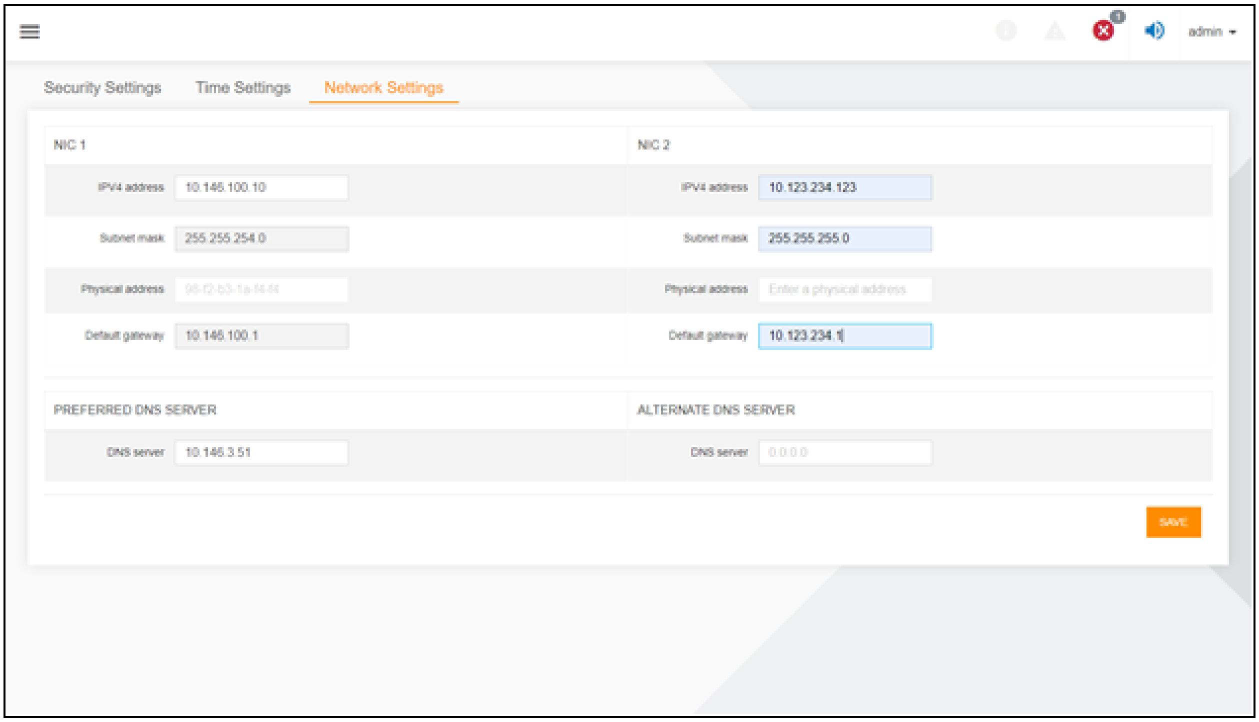
Figure 19.11 Network Settings



Set the IPV4 ADDRESS, SUBNET MASK, DNS SERVER, AND DEFAULT GATEWAY OF NIC 1 AND NIC 2. (IPV4 ADDRESS, SUBNET MASK, DEFAULT GATEWAY are required, the DNS server optional). As shown in **Figure 19.12** below .

The physical address is automatically obtained from the physical address of the server, which cannot be changed and is not required. The entered IP address must be formatted correctly, otherwise it cannot be saved.

Figure 19.12 Configuring a NIC



The above input is in the correct format to save, click the *save* button.

This page intentionally left blank

20 License Management

20.1 Overview

License management has two main functions: one is to display the number of RDUs, the number of access controls, the number of cameras, the number of monitorable devices, and their usage; The second is to upgrade the system authorization (License Upgrade) to expand the upper limit of the number of access RDUs, access controls, and cameras. According to the product model, Smart InfraSight™ is provided with licenses for the number of access RDUs, access control, cameras, and monitorable devices. Specifically, there are three types of licenses:

1. **Basic**: The default number of RDUs that can be connected is 32. After the license upgrade, the number of RDUs that can be connected is expanded to 96. The number of devices that can be monitored by the system is 500. The default number of accessible access controllers is 32. The number of access controller connections can be upgraded up to 500. The default IP address that can be accessed

The number of video devices is 32. The maximum number of IP-based video devices can be upgraded to 500.

2. **Essential**: The default number of RDUs that can be connected is 128. After the license upgrade, the number of RDUs that can be connected is expanded to 384. The number of devices that can be monitored by the system is 800. The default number of accessible access controllers is 64. The maximum number of access controller connections can be upgraded to 800. The default number of IP video devices that can be accessed is 64. The maximum number of IP-based video devices can be upgraded to 800.

3. **Premium**: The default number of RDUs that can be accessed is 256. After the license upgrade, the number of RDUs that can be connected is expanded to 768. The number of devices that can be monitored by the system is 1500. The default number of accessible access controllers is 256. The maximum number of access controller connections can be upgraded to 1,500. The default number of IP video devices that can be accessed is 256. The maximum number of IP-based video devices can be upgraded to 1,500.

20.1.1 Functional modules

The following functional modules are authorized to be managed, and please refer to this manual for detailed information about each functional module Detailed Features .

- Usage
- License Upgrades

20.2 Quick Start

20.2.1 Rapid Deployment Steps

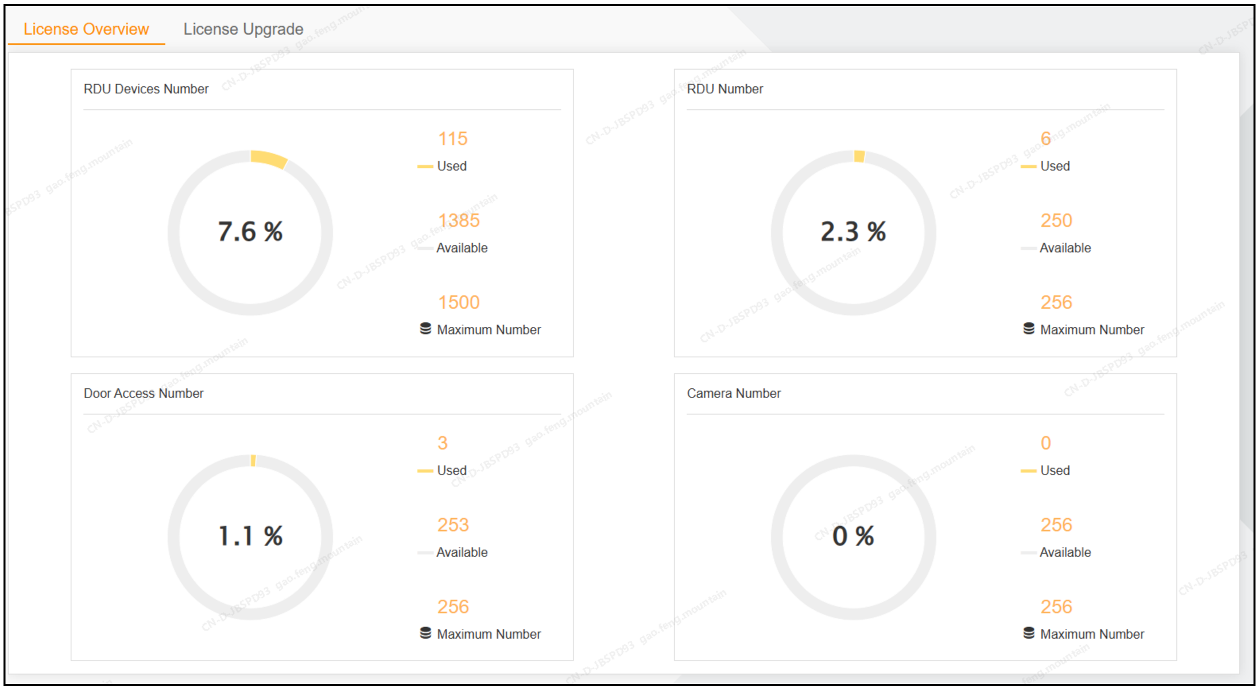
The steps to use the authorization management quick start are as follows:

1. Click on the *Usage* tab to view the device usage.
2. If you have an authorization file, select Upload the authorization file and click on the *Upgrade*.

20.2.2 Example

Usage

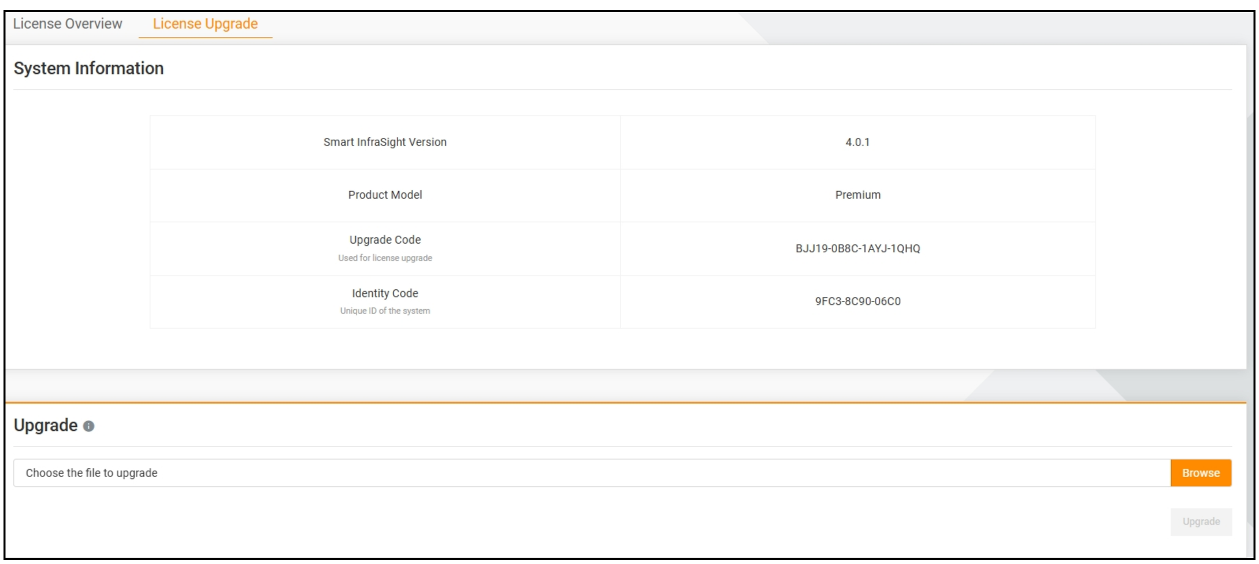
Figure 20.1 License Management—Usage Page



License Upgrades

Upload the authorization file obtained from Vertiv Technical Support Service personnel, as shown in Figure 20.2 below .

Figure 20.2 License Management—License Upgrade Page

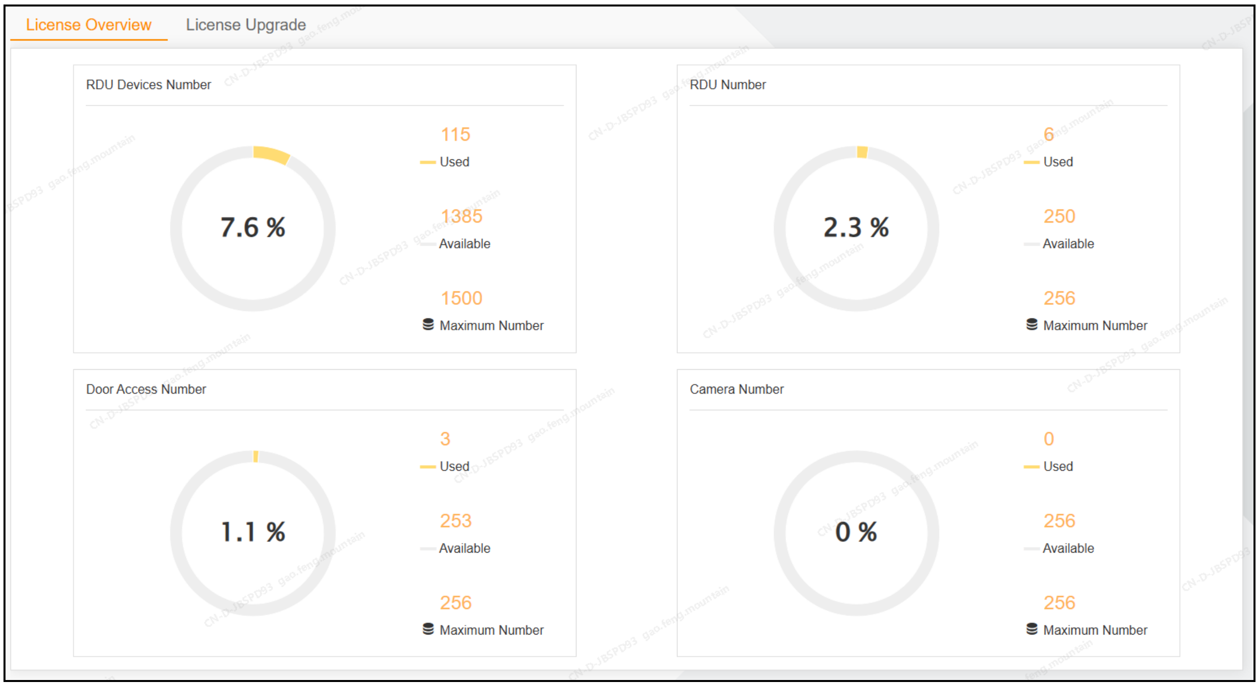


20.3 Detailed Features

20.3.1 Usage

Figure 20.3 below shows the number of RDUs, the number of access controls, the number of cameras, the number of RDU devices that the system can monitor and SNMP devices that the system is monitoring, and how they are being used. For each device, the number of devices that have been used, the number that can be used, and the maximum capacity are displayed. The scale value in the graph is the ratio of (Used Quantity to Maximum Capacity Quantity).

Figure 20.3 License Overview

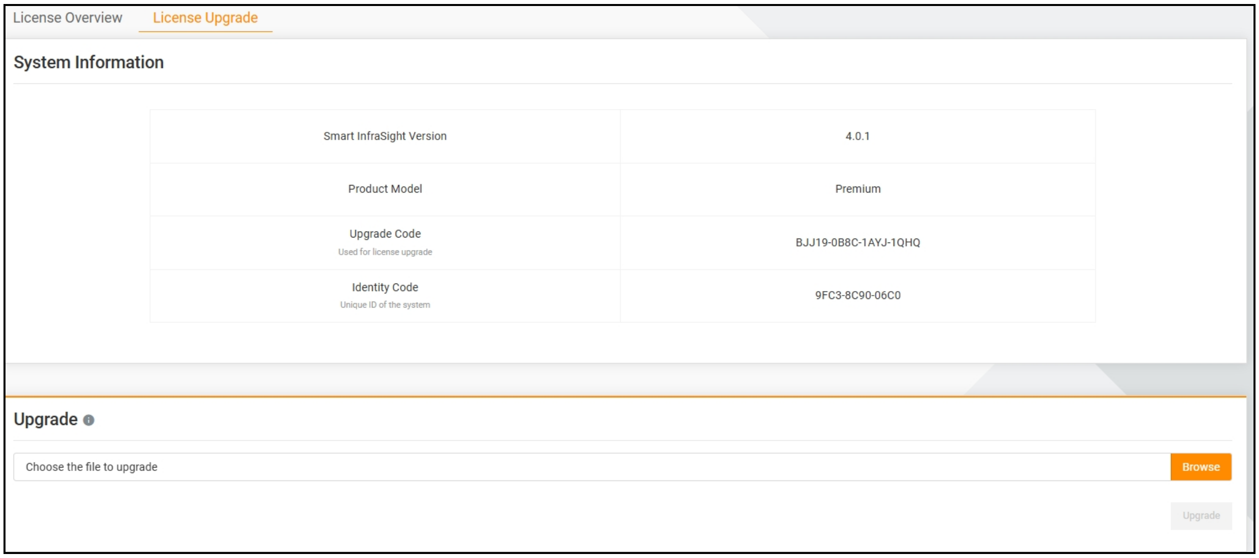


20.3.2 License Upgrades

License upgrade expands the number of access RDUs, access controls, and cameras. This page is divided into two parts as shown in Figure 20.4 on the next page , the upper part displays the system information: system version number (i.e., software version number), product model, and feature code (corresponding to the product). The next part is the authorization upgrade area, where after uploading the authorization file, click the *confirm upgrade* button to upgrade. If there is no content in the input field, confirm that the upgrade button is not enabled.

NOTE: The authorization file is generated based on the signature code. When obtaining the authorization file, you need to provide the feature code to Vertiv technical support personnel.

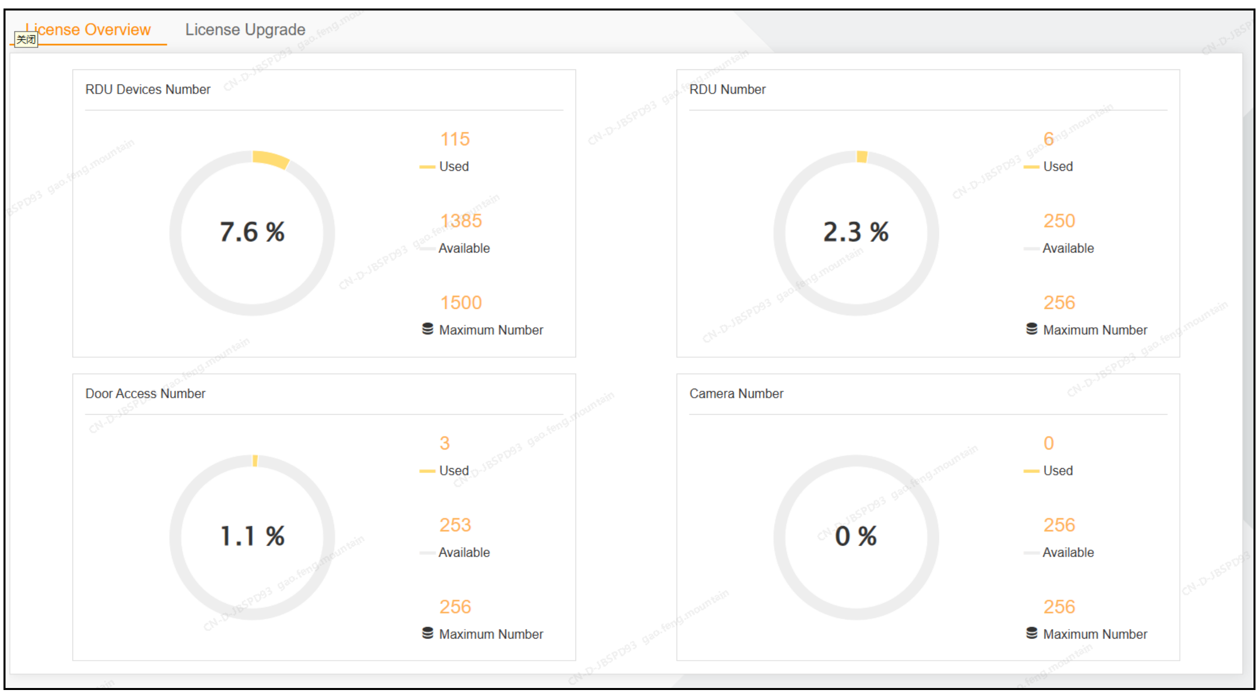
Figure 20.4 License Upgrades



If the authorization file is correct, the upgrade is successful, and a prompt box appears in the lower right corner with the following message: **Authorization upgrade successful**.

After a successful upgrade, the maximum capacity changes. As shown in **Figure 20.5** below .

Figure 20.5 Maximum Capacity Expansion



The Upgrade Failed

If the authorization file is invalid, the authorization upgrade fails, and a dialog box appears in the lower right corner indicating that the upgrade failed. Please contact Vertiv technical support staff in time.

21 Backups and Upgrades

21.1 Overview

There are 3 main functions of backup and upgrade: backup, recovery and system upgrade. This part of the function provides a basic guarantee for the system data, and at the same time, provides an interface for the system upgrade, which is convenient for the subsequent modification of new functions and problems.

Backup and recovery is divided into remote backup and recovery and local backup and recovery. The target of remote backup and recovery operations is remote, that is, backing up files to a remote Windows host and restoring the database from the backup files of the remote host. Local backup and recovery is targeted at the server installed on Smart InfraSight™. Back up the files to the server where Smart InfraSight™ is installed, and perform database recovery from the backup files in the Smart InfraSight™ server.

The backup method is a full backup, and each backup is to back up the data of all databases. The recovery method is full coverage recovery, the content of the recovered file is written to the database, and the original data in the database is emptied, the recovery has certain risks, please make a backup of the original data before recovery, in case there is an abnormality in the recovery process.

System upgrade is an interface to upgrade the system, and the system is upgraded by uploading the upgrade package.

21.1.1 Functional modules

Backup and upgrade includes the following functional modules, refer the Detailed Features on the next page for details of each functional module.

- Backup & Restore
- System Upgrades

21.2 Quick Start

21.2.1 Rapid Deployment Steps

The steps to use the backup and upgrade are as follows:

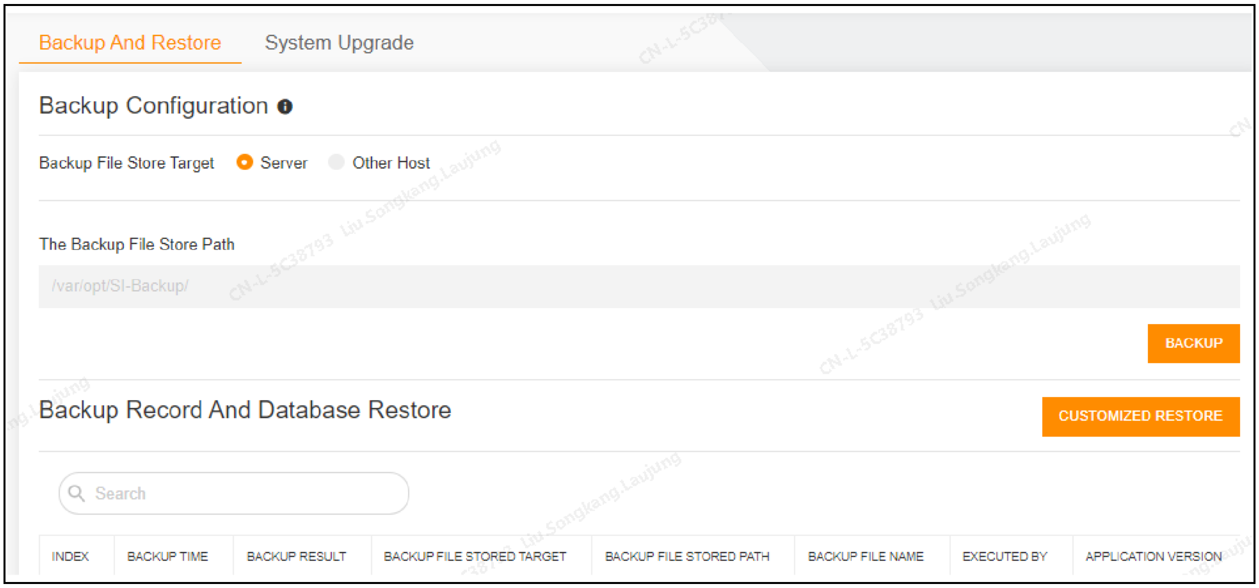
1. Enter the backup and upgrade interface.
2. Click on the *Backup & Restore tab*.
3. Click on the *System Upgrade* tab.

21.2.2 Example

Backup and Restore

Path: System Config --> Backup And Upgrade --> Backup and Restore. As shown in **Figure 21.1** on the next page .

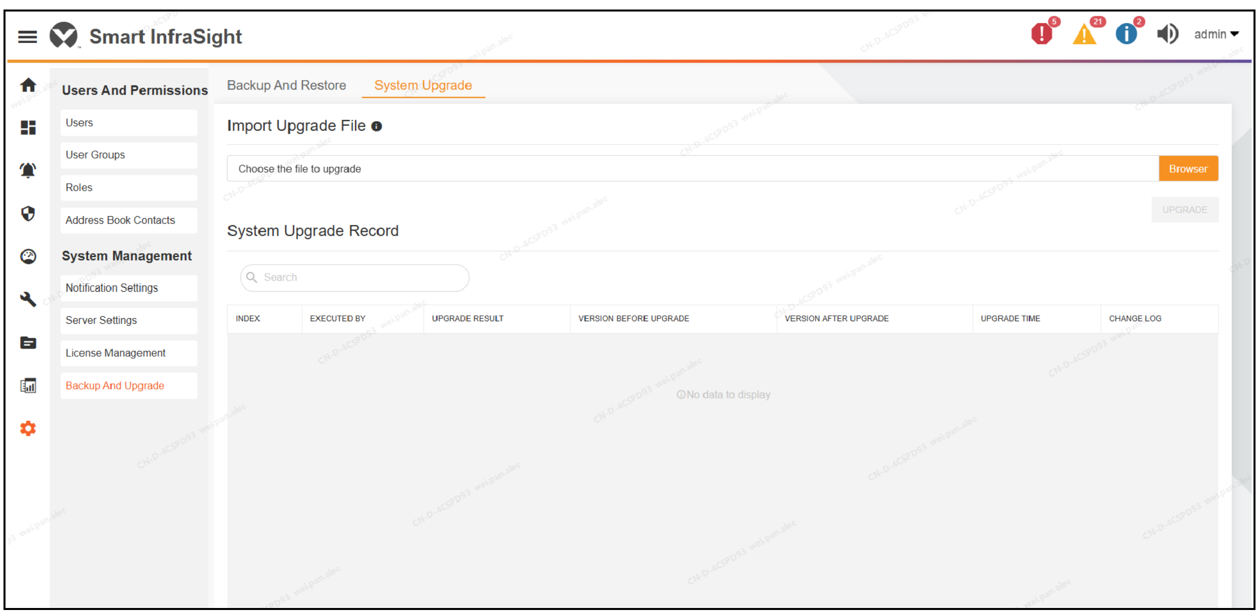
Figure 21.1 Backup and Restoration Page



System Upgrades

Path: System Config --> Backups And Upgrade --> System Upgrades. As shown in **Figure 21.2** below .

Figure 21.2 System Upgrade Page

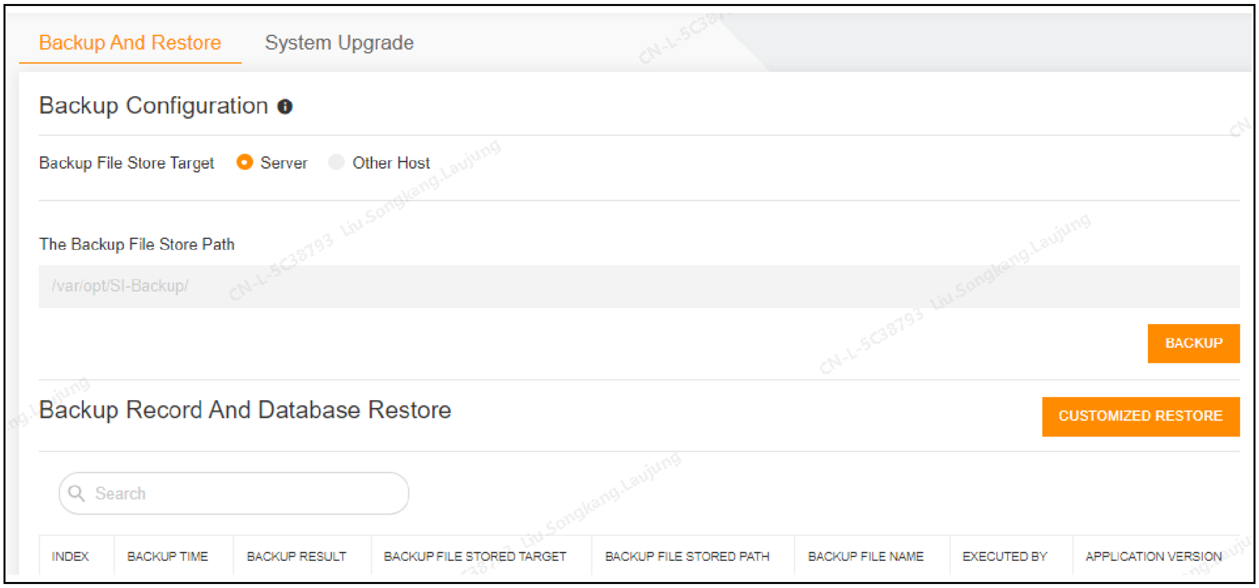


21.3 Detailed Features

21.3.1 Backup and Restore

Go to the System Config and select the Backups And Upgrade. As shown in **Figure 21.3** on the facing page .

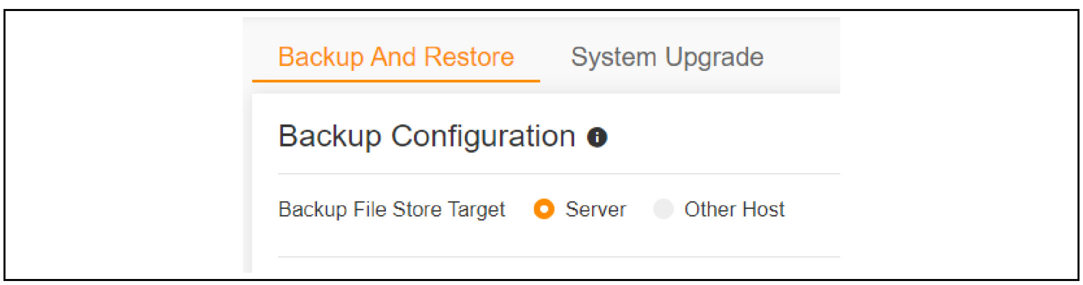
Figure 21.3 Backup and Upgrade Page



Backup

Path: System Config --> Backups and upgrades--> Backup and Restore: Select the backup type, as shown in **Figure 21.4** below .

Figure 21.4 Backup and Restore



There are two types of backups:

Type 1: Back up to the server installed by Smart InfraSight™, select the **Server** button.

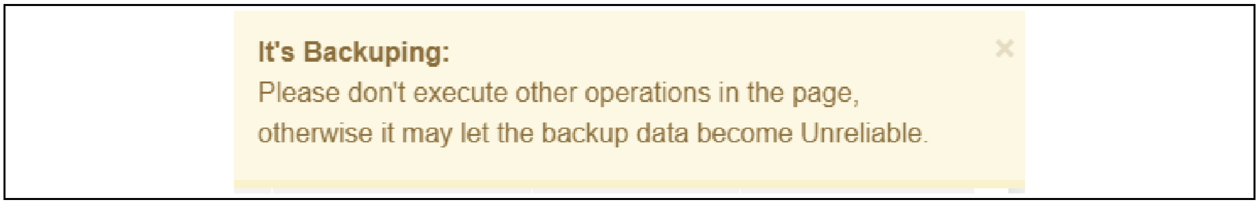
Type 2: Back up to a remote Windows host, back up by sharing a folder, and select the button **Other Host.**

1. Local backup

Figure 21.5 Local Backup

The system automatically configures the default path, click the *Backup* to back up, and the backup file will be automatically saved to the /var/opt/SI-Backup/ path of the SI server. And the prompt will be as shown in Figure 21.6 below .

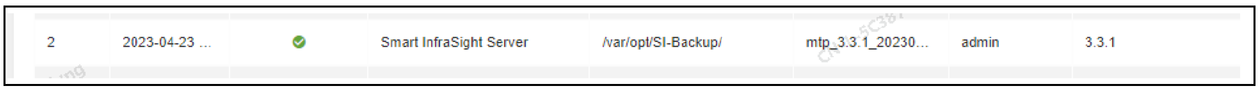
Figure 21.6 Backup Prompt



NOTE: Do not perform other configuration operations during backup operations, otherwise the correctness and reliability of the data will be affected. At the same time, keep it on.

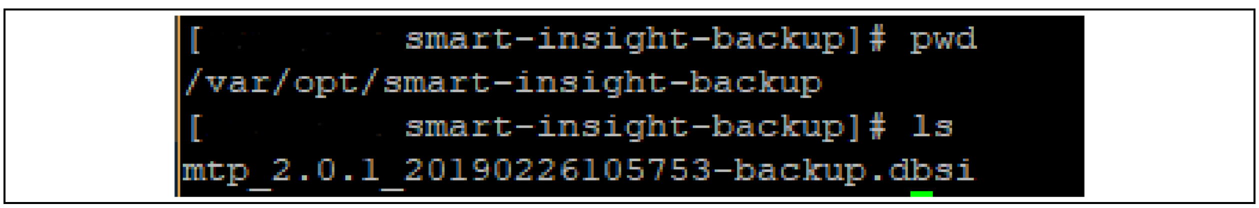
Result 1: Interface, a record of the backup will be saved, as shown in Figure 21.7 below .

Figure 21.7 Back up Records



Result 2: To back up the file, log in to the Smart InfraSight™ server and go to the configured file path to view the backup file, as shown in Figure 21.8 below . Files that are backed up are suffixed with .dbsi.

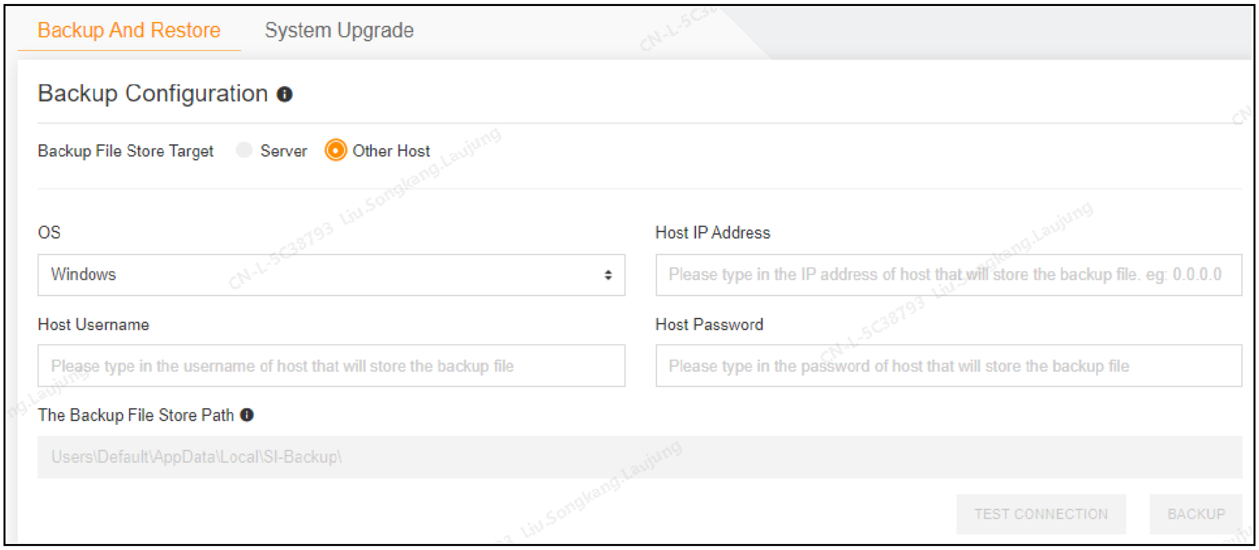
Figure 21.8 Backup popup



2. Remote Backup

Step 1: Configure the input information. As shown in Figure 21.9 on the facing page .

Figure 21.9 Remote Backup Configuration



The remote host system only supports Windows, and the backup file storage path is fixed to Users\Default\AppData\Local\SI-Backup.

Configure the remote host IP: for example, 10.123.123.123

Configure the remote host Username: The Username that needs to be entered to log in to the remote host.

Configure the password of the remote host: The password that you need to enter to log in to the remote host.

NOTE: 1. Do not perform other configuration operations during backup operations, otherwise the correctness and reliability of the data will be affected. At the same time, keep the power on and the network is unblocked.

2. Since remote backup transmits data through shared folders, you need to configure the shared folder of the remote host and enable the writable permission of the shared folder.

Restore

Path: System Config --> Backup And Upgrade --> Backup And Restore

NOTE: 1. The restoration operation will overwrite all the local data, and there is a risk of losing the local data.

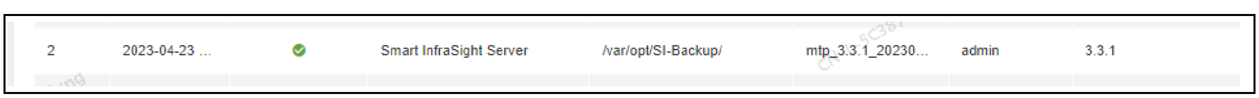
2. When restoring, do not perform other configuration operations, otherwise the correctness and reliability of the data will be affected. At the same time, keep the power on and the network is unblocked.

3. Only admin users can perform recovery operations.

1. Local Restore

1. Select the target local backup file and click the **Convenient Restore** button.

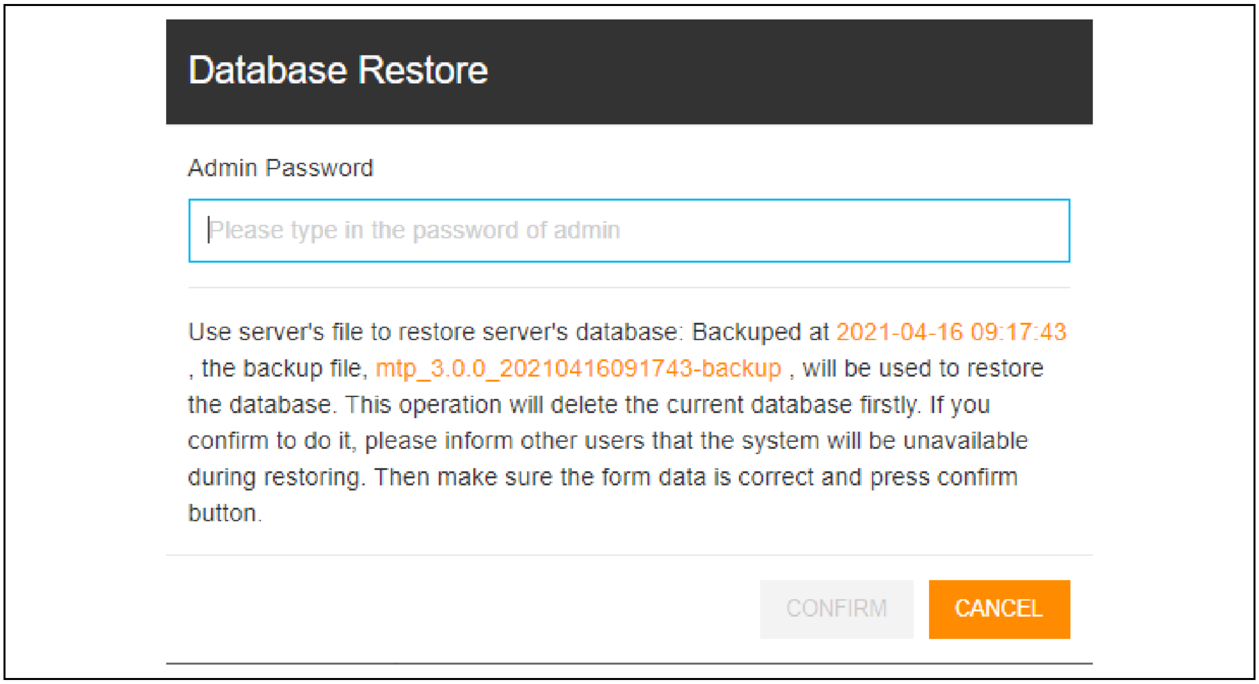
Figure 21.10 Backup Record



2	2023-04-23 ...	✓	Smart InfraSight Server	/var/opt/SI-Backup/	mtp_3.3.1_20230...	admin	3.3.1

2. Enter the admin password as shown in **Figure 21.11** on the next page and click Confirm.

Figure 21.11 Entering the Administrator Password

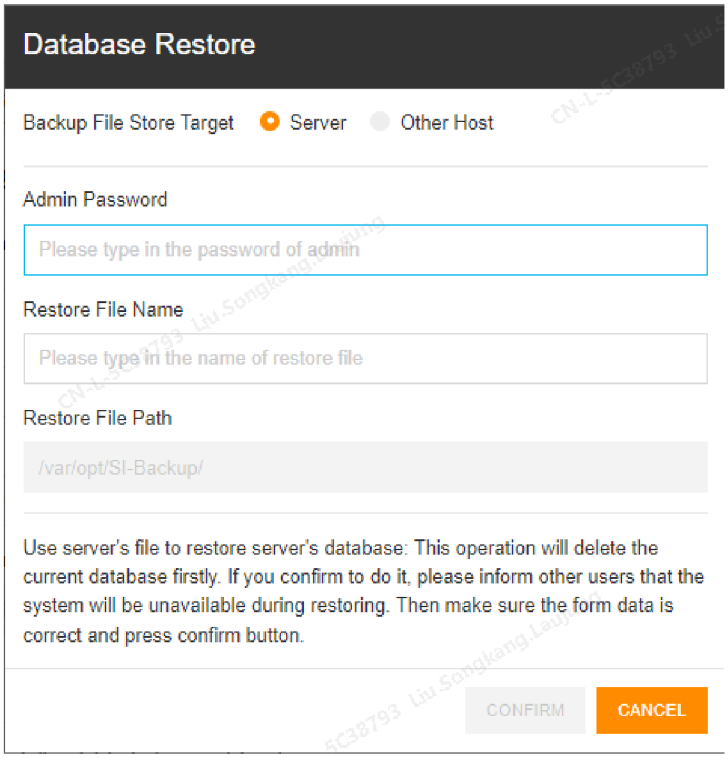


2. Customized Restore from a Local File

Use this method to restore from a custom backup file stored on the Smart Infrasight server's hard drive

Path: System Config --> Backups And Upgrade --> Backup And Restore --> Button: Customized recovery. Open the Database Restore popup as shown in Figure 21.12 on the facing page .

Figure 21.12 Database Restore Popup



1. Enter system administrator password.
2. Enter the name of the restore file, for example, mtp_2.0.1_20190226112432-backup.dbsi
3. Click the CONFIRM button.

3. Customized Restore from a Remote File

Use this method to restore from a custom backup file stored on the remote server's hard drive

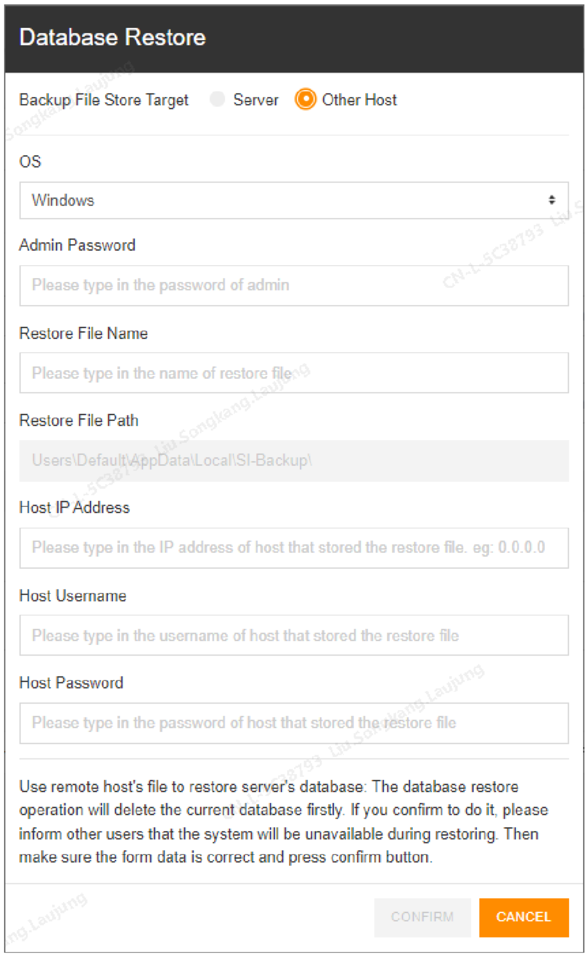
Path: System Config -> Backup And Upgrade -> Backup And Restore -> Button: Customized Restore

Noted: Restoring from a remote server is significantly slower than using a local file, resulting in extended downtime for Smart Infrasight. For faster restoration, we recommend manually copying the restore file from the remote server to the Smart Infrasight server's designated path. Then, use the "Customized Restore from Local File" method to restore the system.

.

1. Enter the configuration information page as shown in **Figure 21.13** on the next page .
2. Click Confirm Recovery.

Figure 21.13 Custom Configuration for Remote Restoration

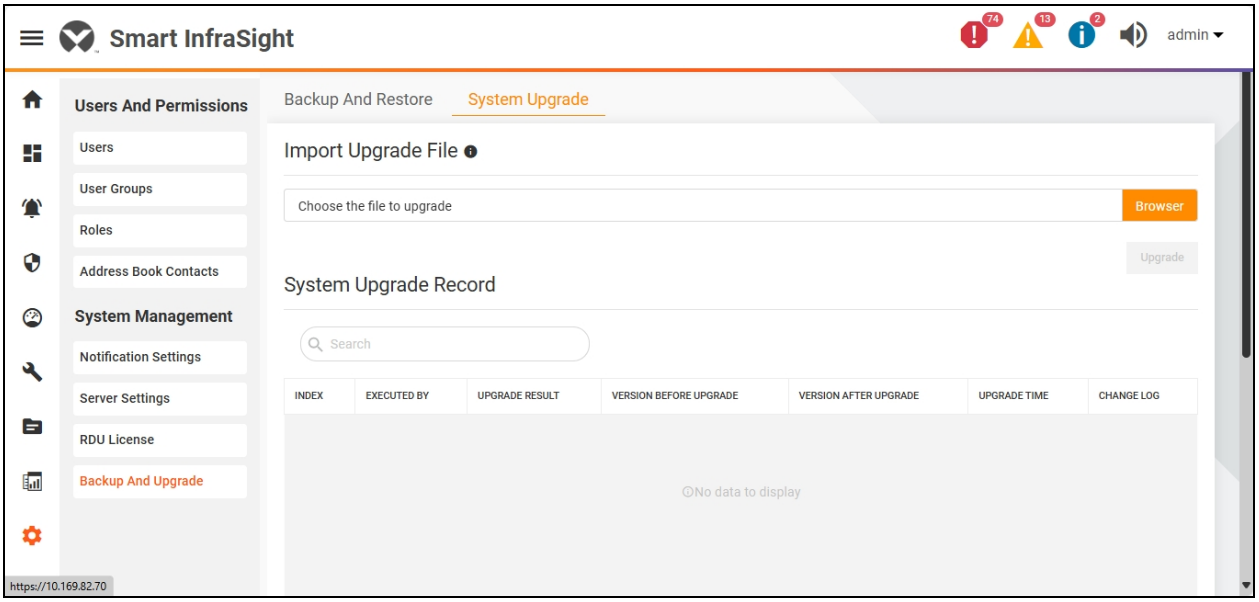


21.3.2 System Upgrades

Path: System Config -->Backups And Upgrade -->System upgrades, as shown in Figure 21.14 on the facing page .

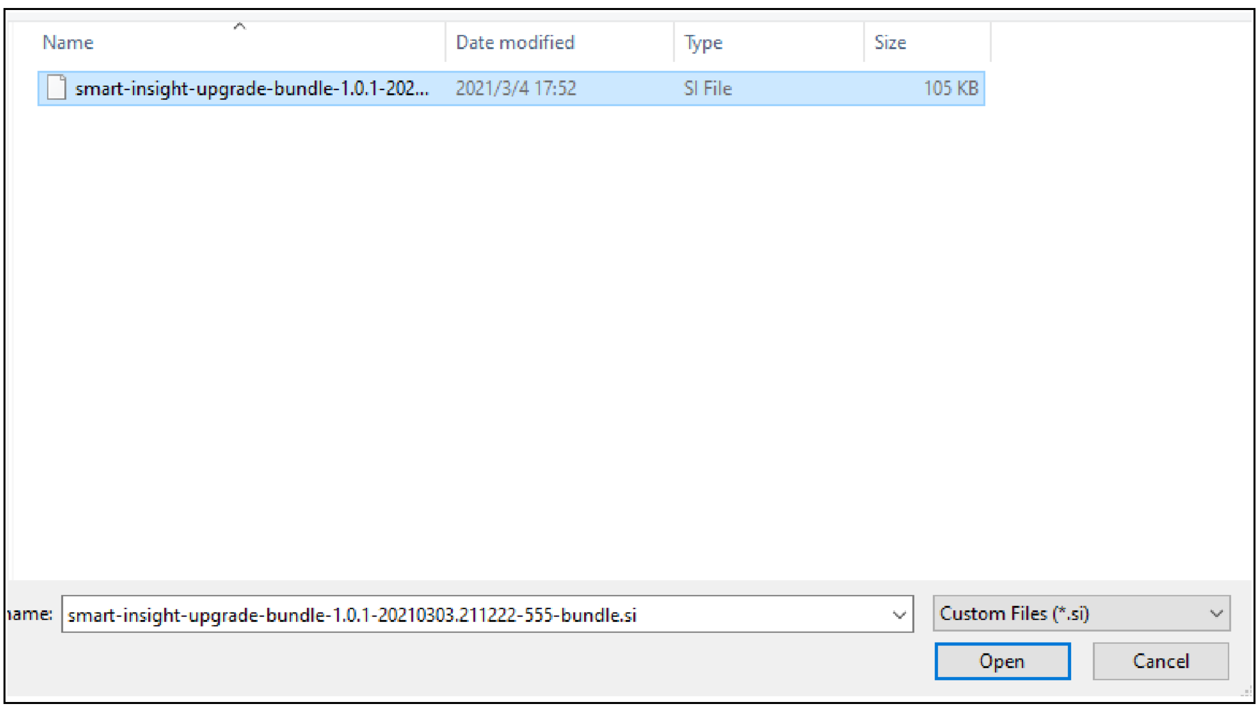
NOTE: Perform the upgrade operation, all services will be stopped, the page will not be operational, please wait for the system upgrade to be completed.

Figure 21.14 System Upgrade



1. Click *Browse*, select the upgrade file as shown in Figure 21.15 below , and the upgrade file ends in .si.

Figure 21.15 Selecting the Backup File



2. Click the on the *Upgrade* icon to upgrade.

3. The system starts the upgrade, please wait.

22 Frequently Asked Questions

22.1 Browsers Supported by Smart InfraSight™

Table 22.1 Browser list

Browser	Version
Google Chrome	Google Chrom73 and above
Firefox	Firefox 66 and above
Edge	Edge 87 and above
The same browser does not support multiple users to log in at the same time.	
Recommended resolution: 1920x1080, minimum resolution: 1600x900	

22.2 RDU Software Upgrade Issues

After RDU upgrades the software, the access card cannot be edited and deleted: When the RDU is in the process of upgrading, Smart InfraSight™ will need to delete the site and then rediscover and add the site before it can edit and delete the access card.

22.3 IPMI User Authentication Configuration Issues

After an administrator user is added to the IPMI user authentication configuration page, the device list on the IPMI device management page remains empty, and the system prompts **Unable to load device configuration, please check whether the user authentication configuration information is correct**.

When Smart InfraSight™ is connected to the RDU 501, disable the two-factor authentication login of the RDU 501 to prevent users from being asked to enter a dynamic password every time they log in.

22.4 Fingerprint Reader Setup Issues

The fingerprint card reader is set to swipe + fingerprint mode, when using an unauthorized card to swipe the card, it will prompt the unauthorized card but no card swiping record:

When the fingerprint card reader is set to a combination mode, such as card swiping + fingerprint, when using an unauthorized card to swipe the card, the unauthorized card will be prompted, and the fingerprint will not be prompted to enter, and the verification on the fingerprint reader side will fail, and there will be no Wigan output, so there is no card swipe record.

22.5 Set the BMC Time of the Server, but the Power on and off Fails

Possible causes and solutions are:

1. If the account password entered in the IPMI user authentication configuration page is incorrect, RDU 501 will ask for a verification code after the first authentication. Please check the authentication configuration.

Check whether the account and password of the RDU 501 are correct, or log in to the RDU 501 page to check whether you need to manually enter the verification code.

2. Check whether the Smart InfraSight™ system and the RDU 501 system network are interoperable.
3. Unexpected downtime of the Smart InfraSight™ or RDU 501 may result in the invalidation of the authenticated information, please re-authenticate in the IPMI User Authentication Configuration Interface.

22.6 Home Temperature Difference Issues

There is a difference between the temperature configuration temperature of the home page heat map and the temperature range displayed on the page:

Because the heat map plug-in adaptively adjusts the temperature display interval for the temperature range display height and the user-set temperature range, the display is different from the user's input.

22.7 Engineering Considerations when Connecting Smart InfraSight™ to the RDU

Smart InfraSight™ is based on the Smart Solution (Smart Aisle/Smart Row/Smart Cabinet) application scenario. Dashboard and Widget are displayed visually, and their tables are as follows:

Table 22.2 Standardized Equipment Scope

Standardized Equipment Scope : 2019-04-23					
Device type	**TAF type**	**Model**	**The name of the driver** **SmartAisle(SA2，SA3) SmartRow2 SmartCabinet2**	**SmartAisle(SA2，SA3) SmartRow2 SmartCabinet2**	**SmartAisle(SA2，SA3) SmartRow2 SmartCabinet2**
Device type	TAF type	Model	The name of the driver		
			SmartAisle(SA2，SA3)	SmartRow2	SmartCabinet2
Temperature and humidity are transmitted Sensors	SENSOR_ ENVIR ONMENT	TH1/TH 2	ENP_ENV_TH1/ENP_ENV _TH2	ENP_ENV_THD/ENP_ ENV _THD2	ENP_ENV_TDI [SENSOR]
Serial access control	DOOR	ACC	ENP_ACC_ES5200DoorMgmt[COM★]		
			ENP_ACC_CHD2100J5[COM☆]		
ammeter	POWER_ METER	AMM	ENP_AMM_CPM3310_C OM☆	ENP_AMM_YD2015 [CO M]]★	-

Table 22.2 Standardized Equipment Scope (continued)

Standardized Equipment Scope : 2019-04-23					
Device type	TAF type	Model	The name of the driver		
			SmartAisle(SA2，SA3) SmartRow2 SmartCabinet2	SmartAisle(SA2，SA3) SmartRow2 SmartCabinet2	SmartAisle(SA2，SA3) SmartRow2 SmartCabinet2
air conditioning	COOLING	CRV+	ENP_AC_CRV+[COM☆]	ENP_AC_SRVII [COM★]]	ENP_AC_SMC[COM]
		CRV	ENP_AC_CRV[COM]		
		PEX+	Not sure how to access, so it can't be provided (I haven't received this kind of equipment, section.) Do not do it in the first stage)		
		DME		ENP_AC_DME3000 [COM]	
UPS	UPS	APM15 0	ENP_UPS_ADAPTPM[CO M]☆		
		GXT4		ENP_UPS_GXT4G[COM]???	
		ITA2		ENP_UPS_ITA2 [COM★]]	ENP_UPS_ITA2[COM]
		ITA		ENP_UPS_ITA5_10K [CO M]	

Table 22.3 Standardized Equipment Scope Continued

Standardized Equipment Scope 2019-04-23					
Device type TAF type Model	Device type TAF type Model	Device type TAF type Model	The name of the driver		
			SmartAisle(SA2，SA3) SmartRow2 SmartCabinet2	SmartAisle(SA2，SA3) SmartRow2 SmartCabinet2	SmartAisle(SA2，SA3) SmartRow2 SmartCabinet2
Equipment standardization equipment scope: 2019-04-23					
Device type	TAF type	Model	The name of the driver		
			SmartAisle(SA2，SA3)	SmartRow2	SmartCabinet2
				ENP_UPS_ITA16_20K[CO M]	
					ENP_UPS_ITA1_3K[CO M]

Table 22.3 Standardized Equipment Scope Continued (continued)

Standardized Equipment Scope 2019-04-23					
			The name of the driver		
Device type TAF type Model	Device type TAF type Model	Device type TAF type Model	SmartAisle(SA2, SA3) SmartRow2 SmartCabinet2	SmartAisle(SA2, SA3) SmartRow2 SmartCabinet2	SmartAisle(SA2, SA3) SmartRow2 SmartCabinet2
				ENP_UPS_ITA30_40K[COM]]★	
		eXL	Drivers are not provided and no plans are made (no equipment has been taken, not done in the first phase)		
UPS	UPS	eXM	ENP_UPS_EXM[COM]		
		HIU	ENP_UPS_HIPULSE [COM]		
PDU	RACK_PDU	MPS	ENP_MPDU_MPS[COM★]]		
		MPI	ENP_MPDU_MPI [COM]		ENP_MPDU_MPSC[COM]
		MPH2		We are not sure how to access the information, so we cannot provide it In addition, Xiyan feedback: there is no way to standardize, because the signal points provided by the MIB library of the device cannot correspond to the standardized signal points one-to-one (without receiving this kind of equipment, the first stage will not be done)	
Integrated power distribution cabinet	FLOOR_ PDU	SPM	ENP_PDU_SPM2 [COM]] ★		
			ENP_PDU_SPM [COM★]]		

When upgrading the old Smart Solution, some precautions for Smart InfraSight™ to connect to the RDU:

1. Follow the table in the RDU to upgrade the old drive.
2. The access control service is managed by Smart InfraSight™, so the access control information in the RDU and access control hardware in the original project, including card information (including fingerprint and other information), authorization information, 501 access control and G2 information, may be cleared, and these information must be re-entered in Smart InfraSight™.

22.8 The Configuration Content of Serial Port Access Control

To implement the management function of serial port access control (taking ES5200 as an example), perform the following steps:

1. Diagram of the Configuration Process and Device

1. 220V mains power supply to power supply.
2. The RS485 terminal port of the connector connects the serial port and card reader of the RDU501 respectively.

3. The two electrically controlled locking ports of the connector can be selected according to your needs (several ports can be connected to control several doors at the same time).
4. The reader's two interfaces can be selected as required (one for one-sided opening, two for double-sided opening). The door can be set from the terminal block wiring, refer to the illustration for details.

The core components of the power supply (left) and connector (right) are shown in **Figure 22.1** below .

Figure 22.1 Power Supply (Left) and Connector (Right)

2. RS485 Wiring

Enter the configuration tool in the left menu, then click Device Settings, RDU Management, and click *ellipses* on the right side of the RDU you want to operate, select and jump to RDU, and enter the RDU login page.

After logging in successfully, select Configuration Management on the left menu, add the ES5200 driver, and click to edit the COM, and the managed COM port should be the same as the COM port connected to the RS485 RDU.

After the addition is complete, select Green icon under ACC is normal communication status, orange is unsuccessful connection, and red is alarm status.

3. Card Reader Wiring

It is a power cable, which is a signal cable, which is connected to the RS485 interface of the connector, and the power cable is connected to either of the two interfaces of the card reader.

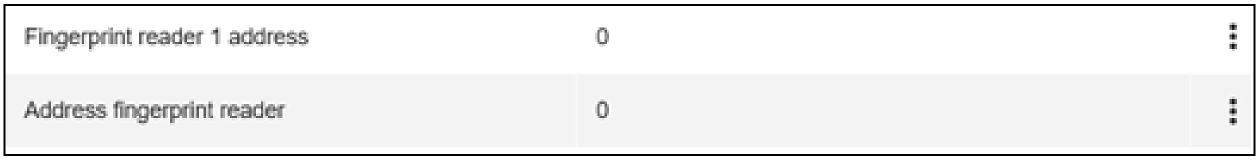
4. Card Reader Address Settings

1. Select ES5200 (example) under Security, Access Control, Device List.

Click Settings on the right navigation bar, and select the *ellipses* on right to set the address of the card reader to set the address of the card reader itself.

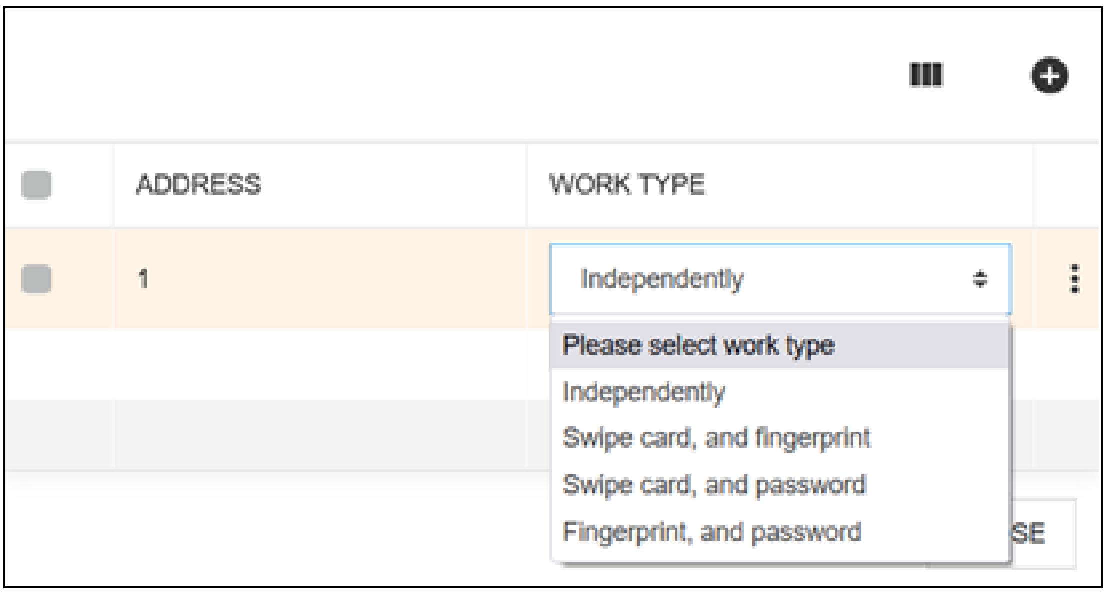
2. Set the address of the fingerprint reader to be the same as the location of the reader itself, as shown in the following figure.

Figure 22.2 Setting the Address of the Card Reader



3. The working mode of the fingerprint reader can also be set as shown in the image below.

Figure 22.3 Setting the Working Mode of the Card Reader



22.9 Unable to Find the Lithium Battery Device Issue

Question: Why I cannot find a lithium battery device in the custom line chart widget and alarm analysis report?

Answer: At present, these two functions do not support lithium battery devices, if you need it, you can contact Vertiv Technical Services.

22.10 Power Link Diagram: Right-Click and Hold the Page to Move Forward and Backward

Issue: Right-clicking and dragging the Edge browser causes the page to move forward/backward.

Solution: Edge browser has a mouse shortcut set by default, and pressing and dragging with the right mouse button will make the page forward/backward.

If you want to use the energy link diagram normally, you can turn off mouse gestures in Settings -->Appearance-->Customize Browser-->Enable Mouse Gestures in Edge browser.

22.11 There is no Record of Assets being Put on and off the Shelves

Issue: A U-level Asset manager is bound, but no record of the location change of the related asset is found in the asset listing record.

Scenario: When you use the SI management U-level Asset manager to implement automatic on-shelf loading and unloading of assets, the **location** of the assets (servers, switches, etc.) needs to be the same as that of the U-level Asset manage.

22.12 CCTV Clicks to Download the Video, and the Username and Password Input Box will popup

Problem: When CCTV clicks to download a video in Firefox, the username and password input box will pop up

Solution: On Firefox, turn off **Enhanced Tracking Protection** to download it smoothly.

22.13 When Querying or Exporting Stored Signals, the U-digit Tag Value is Displayed as a Decimal Value

Tip: When querying or exporting Stored signals, the U-level Asset tag value of the U-level Asset manager is displayed as a decimal number, and you need to manually convert it to a hexadecimal number to restore the U-level Asset tag value.

22.14 When the Working Mode of Swipe + Password is Selected, the Door Cannot be Opened

Problem: The fingerprint reader cannot open the door when selecting the working mode of **Swipe + Password**.

Solution: When the fingerprint reader selects the working mode of **swipe + password**, the user needs to enter the fingerprint into the card before using the swipe + password to open the door.

22.15 Error Message is Displayed: The Alarm Push is Blocked

Problem: Occasional alarm push will be blocked, and the abnormal message **Alarm push blocked** will be displayed.

Solution: After the page is refreshed, the page can receive alarms normally (the current alarm, Stored alarm list, and alarm notification are not affected).

After 20 seconds, the page will be automatically refreshed.

This page intentionally left blank

Connect with Vertiv on Social Media

https://www.facebook.com/vertiv/

https://www.instagram.com/vertiv/

https://www.linkedin.com/company/vertiv/

https://www.x.com/Vertiv/

SL-50012_REVA_09-25