Smart InfraSight™

User Manual

Version 4.1.0

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages result from use of this information or for any errors or omissions.

Refer to local regulations and building codes relating to the application, installation, and operation of this product. The consulting engineer, installer, and/or end user is responsible for compliance with all applicable laws and regulations relation to the application, installation, and operation of this product.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use, or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

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.

Proprietary and Confidential ©2026 Vertiv Group Corp.

TABLE OF CONTENTS

1 Activation **1**
1.1 Overview 1
1.1.1 Appliance 1
1.1.2 Virtual Machine 1
1.1.3 Functional Modules 1
1.2 Onboarding Process 2
1.2.1 Activating the Vertiv™ Smart InfraSight™ 2
2 User Login **9**
2.1 General 9
2.1.1 Overview 9
2.2 Detailed Functions 9
2.2.1 User Login 9
2.2.2 User Profiles and Help Information 10
3 Monitoring **19**
3.1 General 19
3.1.1 Overview 19
3.1.2 Functional Modules 19
3.2 Detailed Features 19
3.2.1 Monitoring Tree 19
3.2.2 Location 19
3.2.3 Site 25
3.2.4 Location: Map Navigation 30
3.2.5 Location: 3D 32
3.2.6 Site: Monitoring Center 33
3.2.7 Site: Monitoring Battery Devices 42
4 3D Configuration **47**
4.1 General 47
4.1.1 Overview 47
4.1.2 Functional Modules 47
4.2 Detailed Functions 47
4.2.1 Enter the Site/Location 3D Configuration 47
4.2.2 Dragging and Dropping the Device to Edit the Canvas Size 50
4.2.3 Editing or Adding the Devices 52
4.2.4 Preview or Save 3D Configuration 56
4.2.5 Configuring the Rack 58
4.2.6 Configure the Power Distribution Cabinet 70
4.2.7 3D Configuration of the Battery Room 72

© 2026 Vertiv Group Corp. All Rights Reserved.

4.2.8 Lithium Battery 3D Configuration 73
4.2.9 Lead-Acid Battery 3D Configuration 74
4.2.10 Configure the U-level Asset Manager 75
5 Power Train 79
5.1 General 79
5.1.1 Overview 79
5.1.2 Functional Modules 79
5.2 Detailed Functions 79
5.2.1 Creating a Power Train Diagram 79
5.2.2 Asset List and Operations 80
5.2.3 Canvas and Operations 84
5.2.4 Power Configuration 85
5.2.5 Circuit Configuration 88
6 3D Visualization 95
6.1 General 95
6.1.1 Overview 95
6.1.2 Functional Modules 95
6.2 Detailed Features 95
6.2.1 Smart Aisle2 Site 3D Visualization 95
6.2.2 Smart Aisle3 Site 3D Visualization 115
6.2.3 Smart Row2 Site 3D Visualization 121
6.2.4 CREMS Site 3D Visualization 137
6.2.5 Location 3D Visualization 138
6.2.6 Battery Room Site 3D Visualization 140
6.2.7 Power Train Diagram 3D Visualization 141
7 Single-Site Power Distribution and Thermal Management 143
7.1 General 143
7.1.1 Overview 143
7.1.2 Functional Modules 143
7.2 Detailed Features 143
7.2.1 Power Distribution Professional Interface 143
7.2.2 Thermal Management Professional Interface 147
8 IT Management 151
8.1 General 151
8.1.1 Overview 151
8.1.2 Functional Modules 151
8.2 Detailed Configuration 151
8.2.1 User Authentication Configuration 151
8.2.2 Server Management Detailed Functions 152
8.2.3 Console Management Detailed Function 159

© 2026 Vertiv Group Corp. All Rights Reserved.

9 Dashboard **163**
9.1 Overview 163
9.1.1 Functional Modules 163
9.2 Detailed Features 163
9.2.1 Dashboard 163
9.2.2 Adding a Visualization 164
9.2.3 Move, Resize, and Delete a Visualization 165
9.2.4 Deleting a Dashboard 167
10 Alarm **169**
10.1 General 169
10.1.1 Overview 169
10.1.2 Functional Modules 169
10.2 Detailed Functions 169
10.2.1 Active Alarms 169
10.2.2 Alarm History 170
10.2.3 View Alarm Details 171
10.2.4 Alarm Notes 171
10.2.5 Action History 172
10.2.6 Alarm Status Records 172
10.2.7 Export Alarms 173
10.2.8 Automations 175
10.2.9 Alarm Suppression 180
11 Security **187**
11.1 General 187
11.1.1 Overview 187
11.1.2 Functional Modules 187
11.2 Detailed Features 187
11.2.1 Door Access Monitoring 187
11.2.2 Access Card Management 200
11.2.3 Time Settings 208
11.2.4 Log Query 212
11.2.5 Real Time Video 214
11.2.6 Stored Videos 222
11.2.7 Device Management 230
12 Energy Management **235**
12.1 General 235
12.1.1 Overview 235
12.1.2 Functional Modules 235
12.2 Detailed Features 235
12.2.1 Energy Consumption Configuration 235

© 2026 Vertiv Group Corp. All Rights Reserved.

12.2.2 PUE Configuration 238
13 Configuration Tool 247
13.1 General 247
13.1.1 Overview 247
13.1.2 Functional Modules 247
13.2 Detailed Features 247
13.2.1 Device Management 247
13.2.2 Communication Profile 282
13.2.3 Template 284
13.2.4 Firmware 308
14 Asset Management 315
14.1 General 315
14.1.1 Overview 315
14.1.2 Functional modules 315
14.2 Detailed Features 315
14.2.1 Asset Management 315
14.2.2 Warranty Notification 320
14.2.3 Asset Rack and De-Rack Records 321
15 Reports 323
15.1 General 323
15.1.1 Overview 323
15.1.2 Functional modules 323
15.2 Detailed Features 323
15.2.1 Device History Report 323
15.2.2 Alarms Record 325
15.2.3 Device Control Report 327
15.2.4 Automation Report 329
15.2.5 Door Access Report 331
15.2.6 Custom Reports 333
16 Visualization 343
16.1 General 343
16.1.1 Overview 343
16.1.2 Functional Modules 343
16.2 Detailed Features 344
16.2.1 Visualization List 344
16.2.2 Creating a Visualization 348
16.2.3 Export to Excel 353
16.2.4 Visualization Usage 355
16.3 Visualization Type 357
16.3.1 Bar Chart 357

© 2026 Vertiv Group Corp. All Rights Reserved.

16.3.2 Gauge 359
16.3.3 Image 361
16.3.4 Pie Chart 361
16.3.5 Simple Value 363
16.3.6 Table 365
16.3.7 Text 375
16.3.8 Time Series 377
17 Notification Hub 381
17.1 Overview 381
17.1.1 Functional modules 381
17.2 Detailed Features 381
17.2.1 Outbound Notifications 381
17.2.2 Notification History 387
17.2.3 Notification Settings 390
18 System Configuration 399
18.1 General 399
18.1.1 Overview 399
18.1.2 Functional Modules 399
18.2 Detailed Features 399
18.2.1 Users 399
18.2.2 List of User Groups 405
18.2.3 Roles 409
18.2.4 Address Book Contacts 412
18.2.5 Password Policy 414
18.2.6 Server Settings 416
18.2.7 License 418
18.2.8 Backup and Upgrade 421
18.2.9 Audit Logs 426
18.2.10 AD/LDAP 428
18.2.11 Data Retention 433
19 Frequently Asked Questions 439
19.1 Browsers Supported by Smart InfraSight™ 439
19.2 RDU Software Upgrade Issues 439
19.3 IPMI User Authentication Configuration Issues 439
19.4 Fingerprint Reader Setup Issues 439
19.5 Set the BMC Time of the Server, but the Power on and off Fails 439
19.6 Home Temperature Difference Issues 440
19.7 Engineering Considerations when Connecting Smart InfraSight™ to the RDU 440
19.8 The Configuration Content of Serial Port Access Control 441
19.9 Unable to Find the Lithium Battery Device Issue 443

© 2026 Vertiv Group Corp. All Rights Reserved.

19.10 Power Link Diagram: Right-Click and Hold the Page to Move Forward and Backward 443
19.11 There is no Record of Assets being Put on and off the Shelves 444
19.12 CCTV Clicks to Download the Video, and the Username and Password Input Box will popup 444
19.13 When Querying or Exporting Stored Signals, the U-digit Tag Value is Displayed as a Decimal Value 444
19.14 When the Working Mode of Swipe + Password is Selected, the Door Cannot be Opened 444
19.15 Error Message - Alarm Push Blocked 444
19.16 SI IP Change Causes Firmware Upgrade Unavailability for resolution 444
19.17 Failed to Set IP Door Access Wait Time 447

© 2026 Vertiv Group Corp. All Rights Reserved.

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 Vertiv™ Smart InfraSight™. After Vertiv™ 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 Vertiv™ Smart InfraSight™. After Vertiv™ Smart InfraSight™ is successfully activated, users can continue to use the relevant features of Smart InfraSight™.

1.1.3 Functional Modules

Refer to Onboarding Process on the next page.

Recommended Configuration for Client Hardware

Refer to AV-50015 Vertiv™ Smart InfraSight™ v4.1.0 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 Vertiv™ Smart InfraSight™ not being able to obtain data correctly, as shown in the Table 1.1 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Table 1.1 Recommended Configuration for Power Train

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

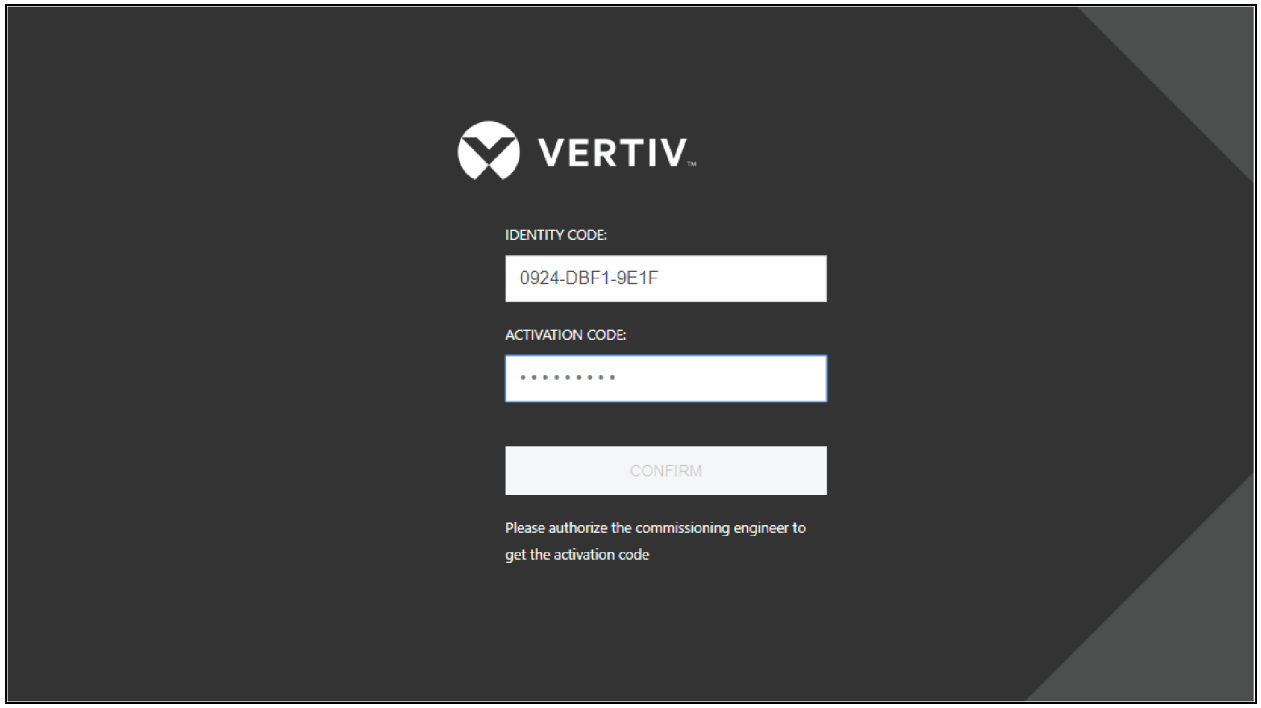
1.2 Onboarding Process

1.2.1 Activating the Vertiv™ Smart InfraSight™

Getting an Activation Code

When accessing the Vertiv™ 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 below shows the activation page.

Figure 1.1 Activation Page



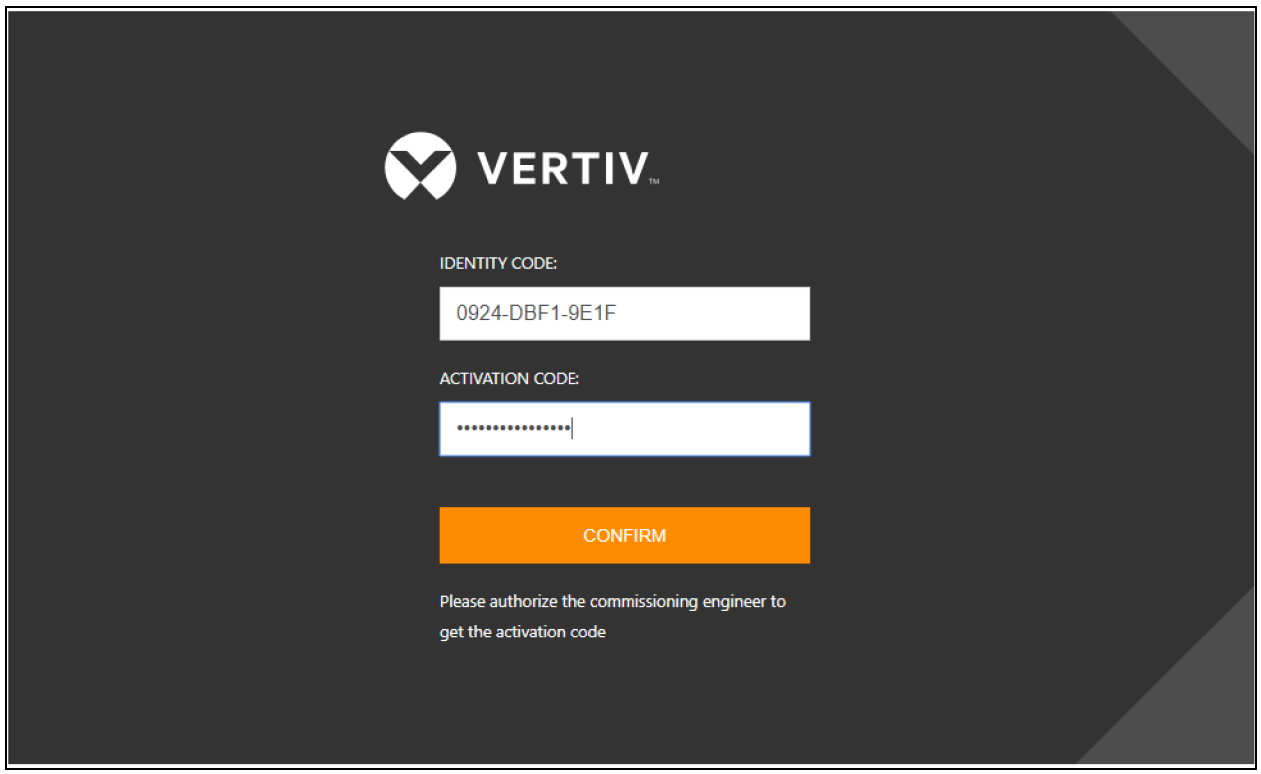
NOTE: The Activation code is unique to each Smart InfraSight™.

© 2026 Vertiv Group Corp. All Rights Reserved.

Activation

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

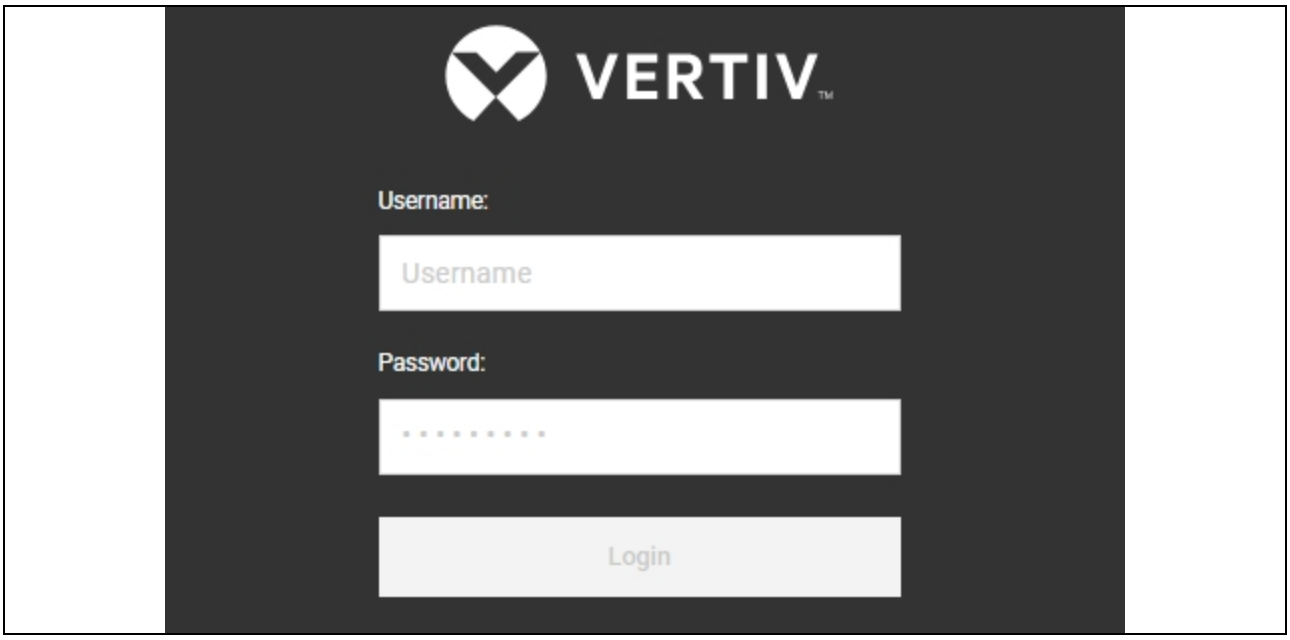
Figure 1.2 Activation Screen



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** on the next page .

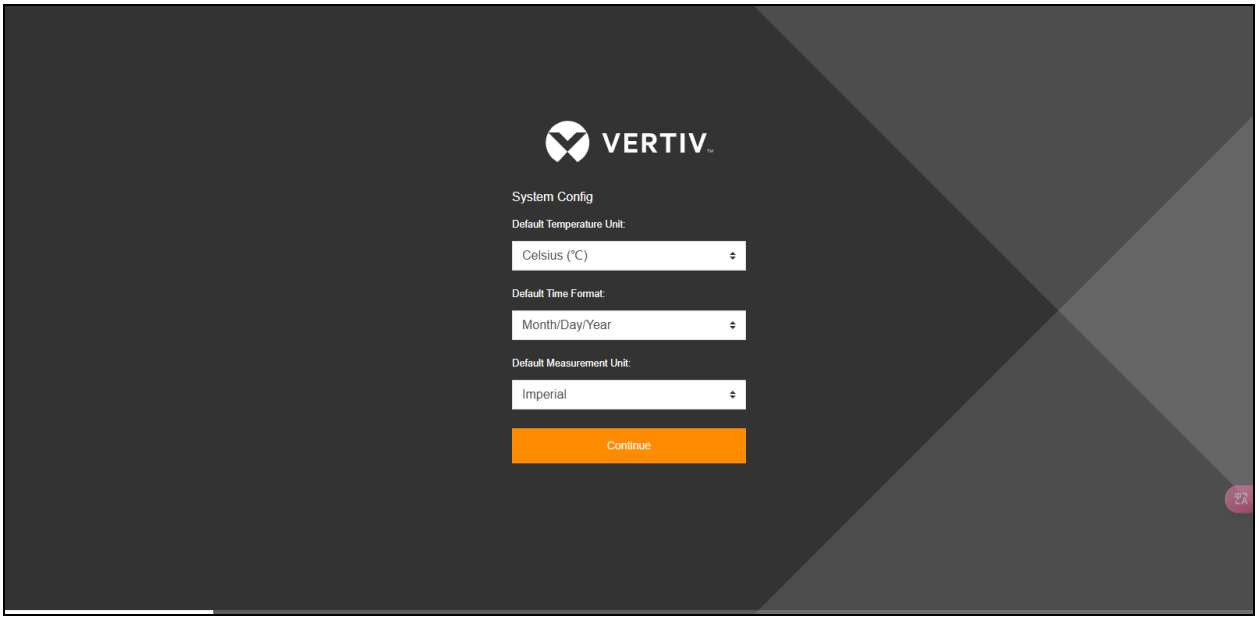
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 1.3 User Login Screen



3. Log in with the preset account. The default **username** is **admin** and the default **password** is **Vertiv@123**. If the password is correct, the system localization configuration page opens, as shown in **Figure 1.4** below .

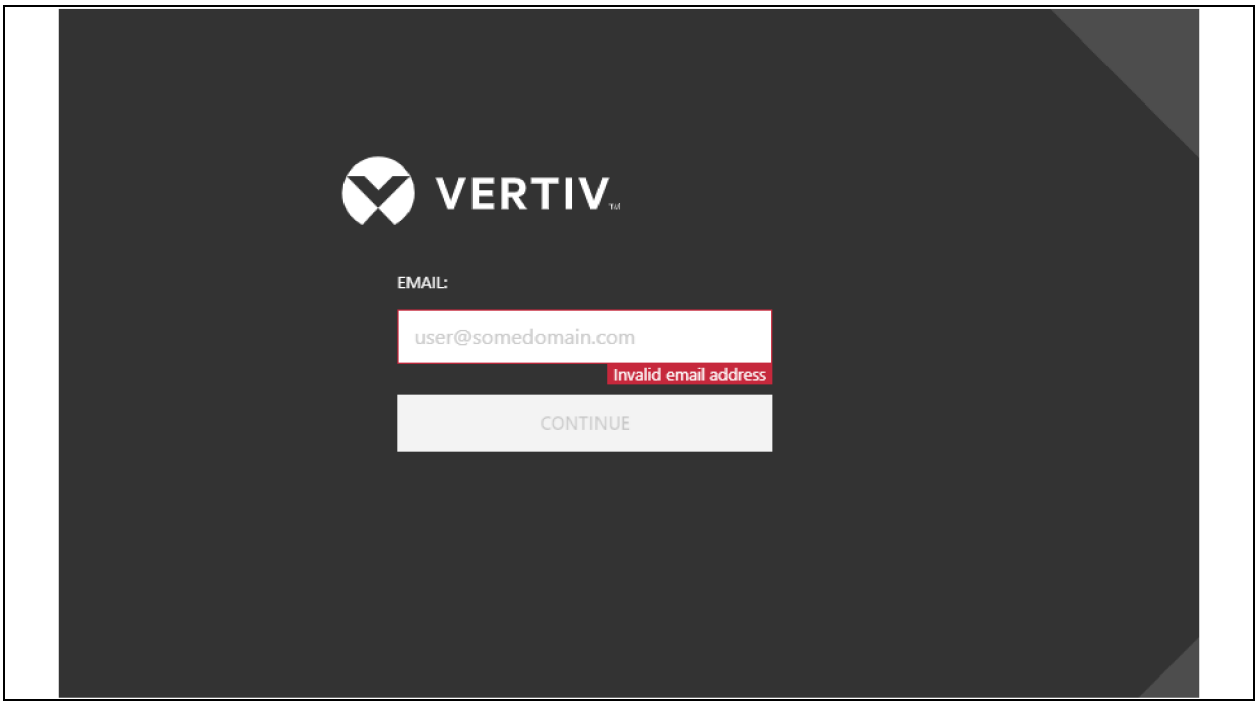
Figure 1.4 System Configuration



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** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

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 .

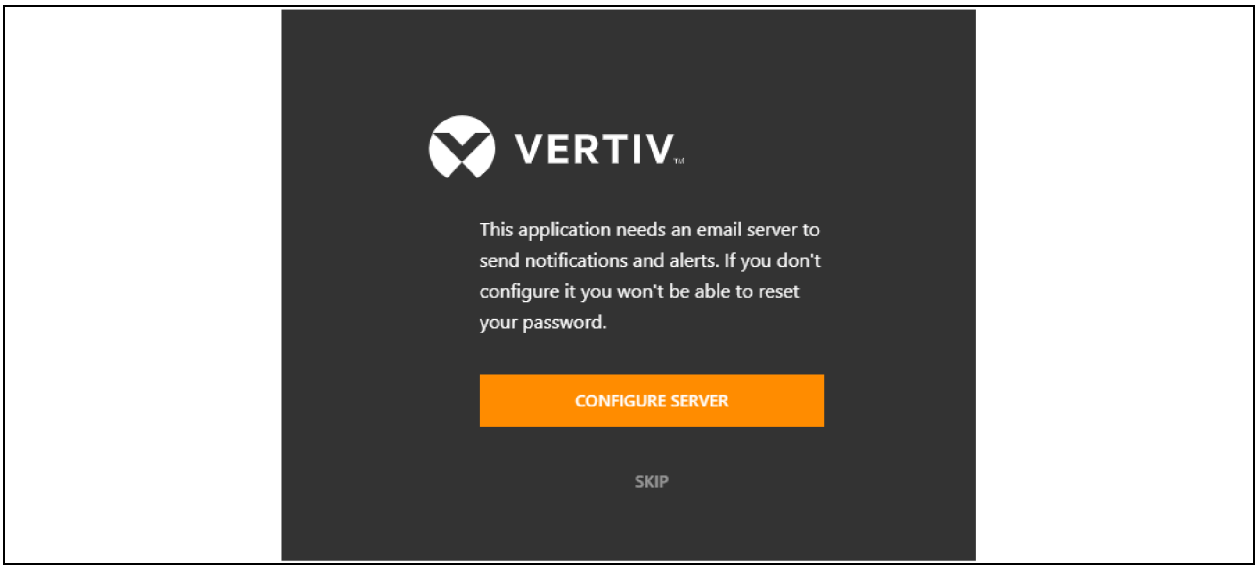
Figure 1.6 Setting up the Login Password for the System Administrator (Admin)



© 2026 Vertiv Group Corp. All Rights Reserved.

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 on the facing page . 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

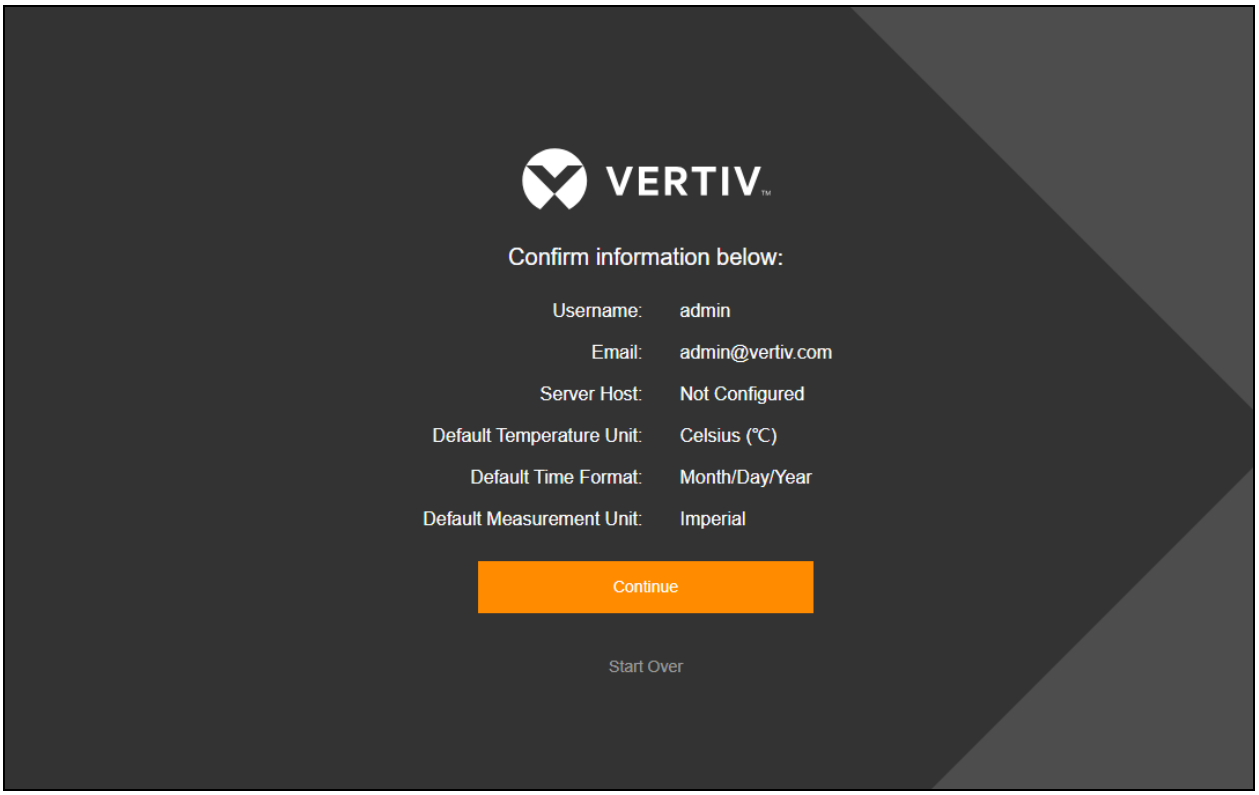
Figure 1.8 Configuring the Mail Server



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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 1.9 System Configuration Interface



© 2026 Vertiv Group Corp. All Rights Reserved.

2 User Login

2.1 General

2.1.1 Overview

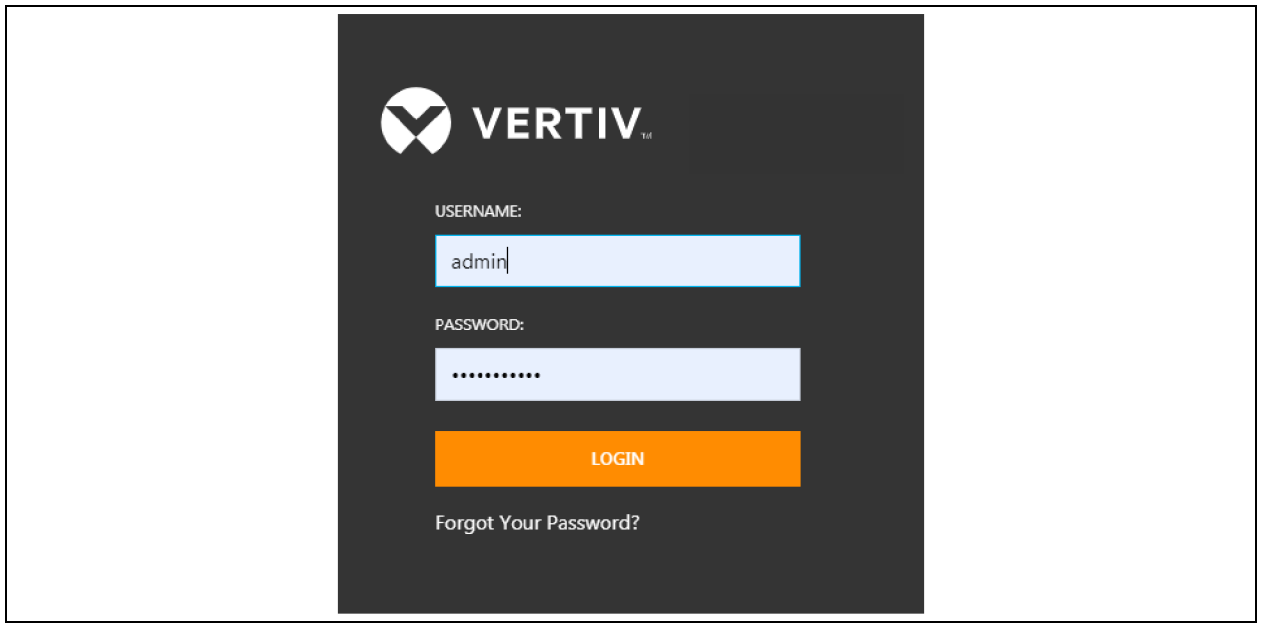
After Vertiv™ Smart InfraSight™ is activated and the initialization information is configured, users can now log in to the Smart InfraSight system.

2.2 Detailed Functions

2.2.1 User Login

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

Figure 2.1 User Login



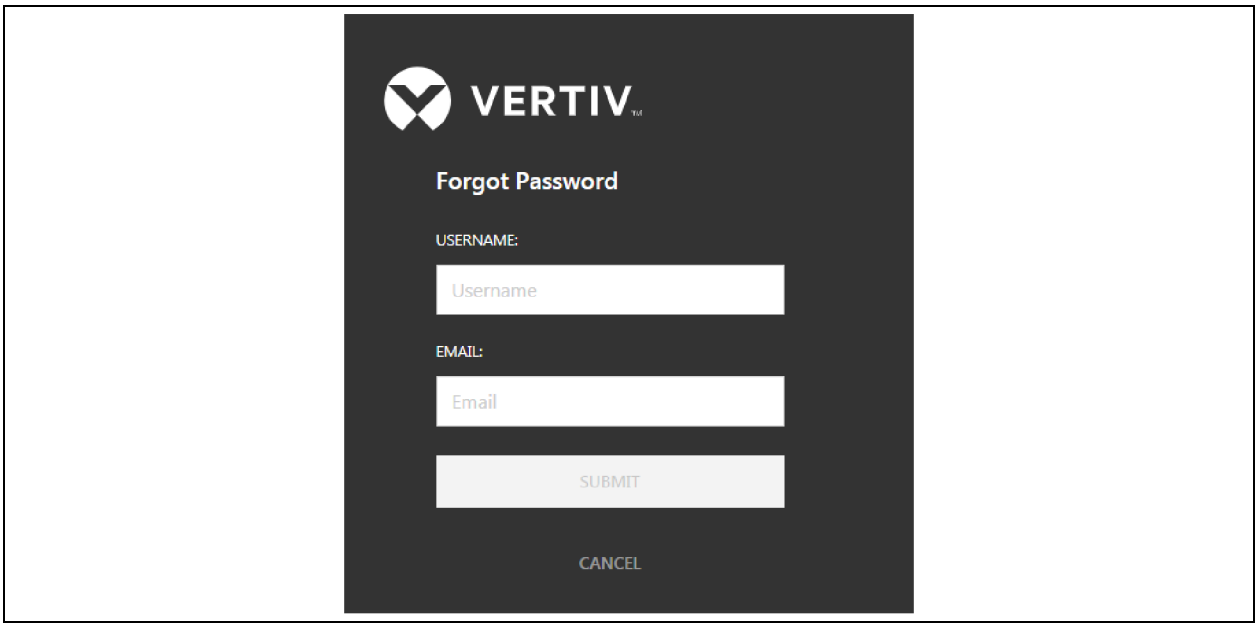
Forgot Password

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

NOTE: If the username or password is entered incorrectly 5 times, the account is locked for 2 hours.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 2.2 Forgot Password Window



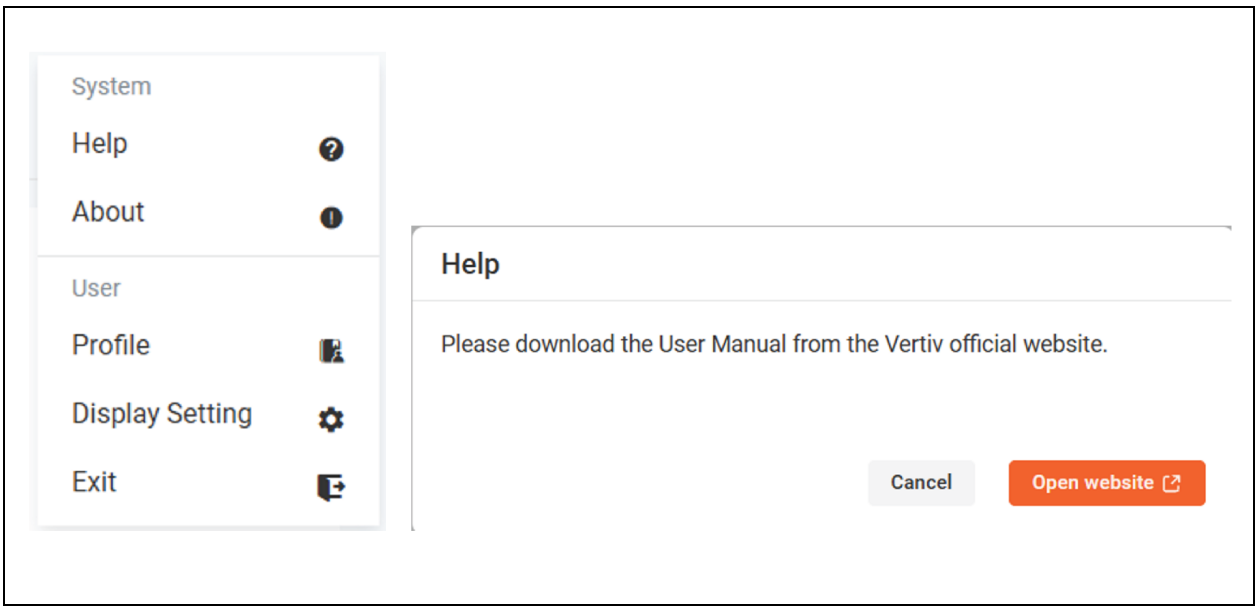
NOTE: You need to enter a correct username and the corresponding email address or the verification code email will not actually be sent.

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 Menu



© 2026 Vertiv Group Corp. All Rights Reserved.

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.

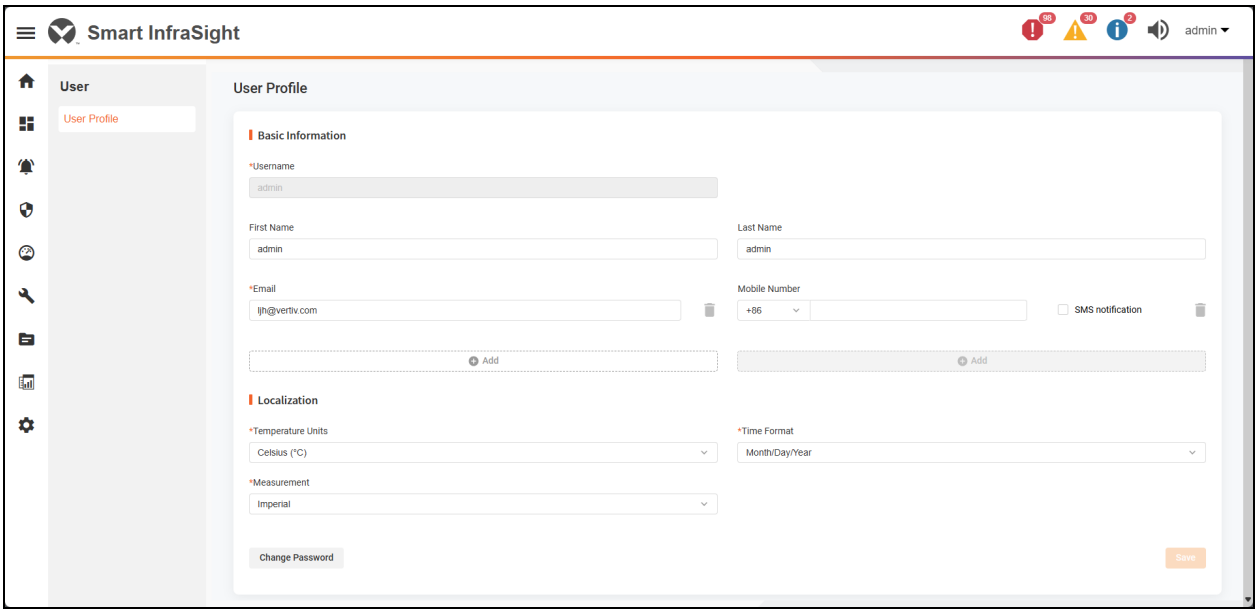
Figure 2.4 About Section



User Profile

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



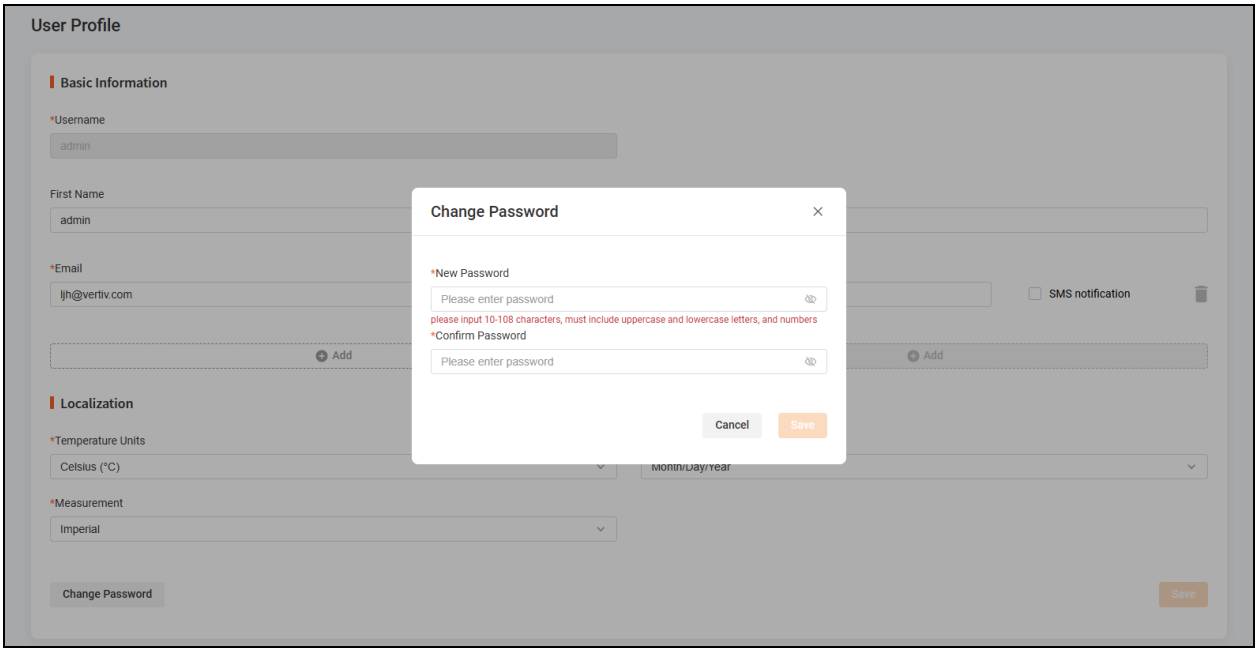
Changing the User Password

Click the *Change Password* button 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

After saving, you will be logged out and redirected to the login page.

Figure 2.6 Changing the User Password

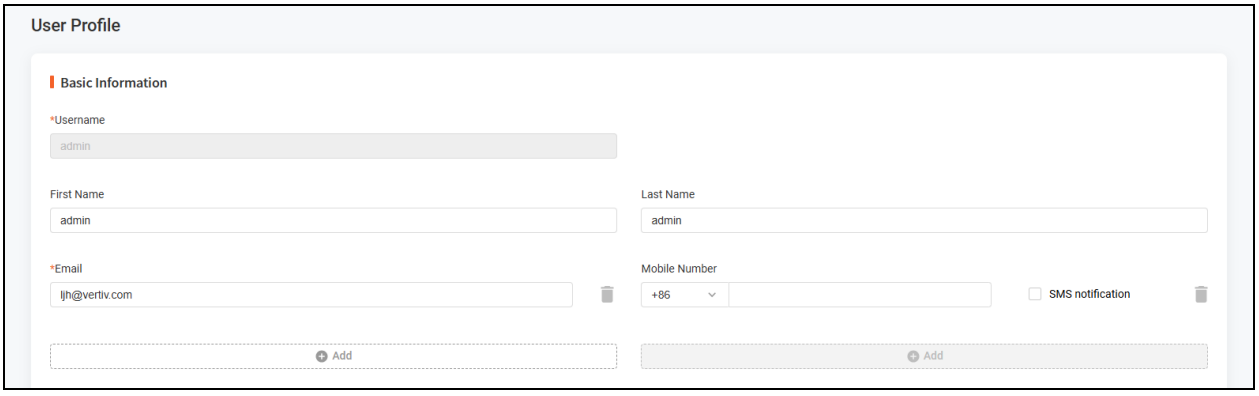


Modifying the Contact Information

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 apply the changes.

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.

Modifying the Localization Configuration

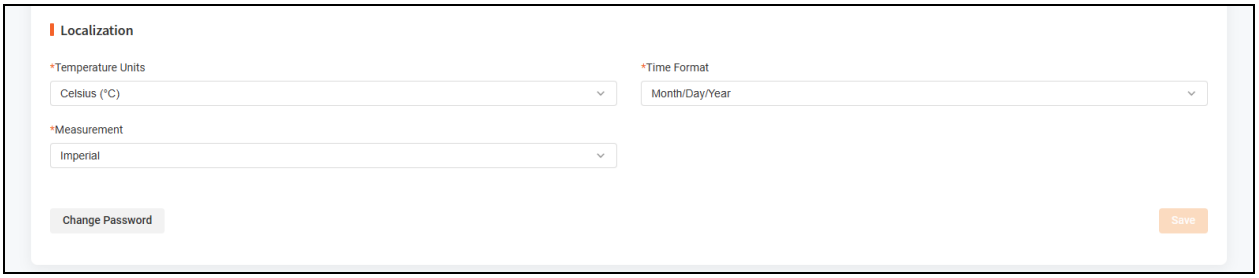
In the user profile each user can change their own regional settings, (as shown in Figure 2.8 on the facing page). This includes:

© 2026 Vertiv Group Corp. All Rights Reserved.

- Temperature units (Fahrenheit or Celsius)
- Time format (month/day/year or day/month/year)
- Measurement units (imperial or metric)

After you save the settings, the system will display information using your selected units and time format.

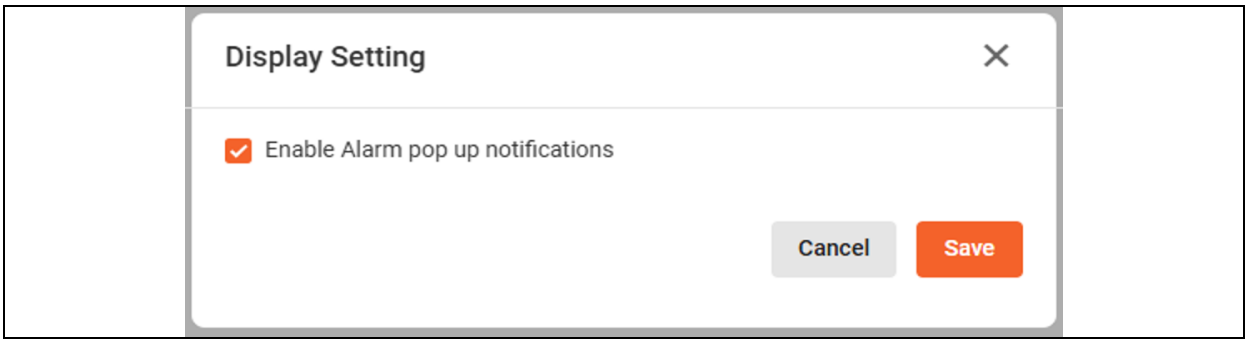
Figure 2.8 Modifying the Localization Configuration



Display Setting

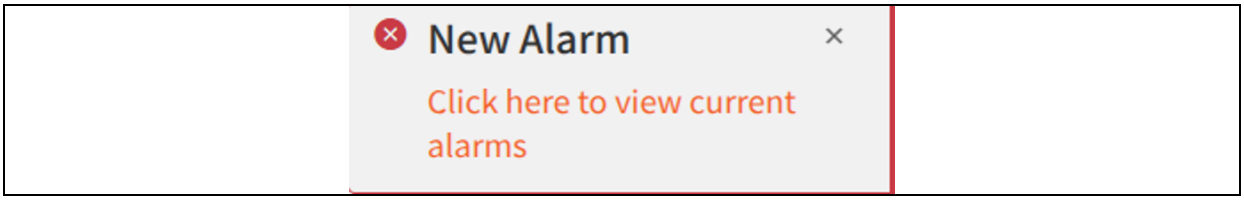
Click Display Settings from the drop-down menu to the right of your Username , as shown in Figure 2.9 below , and the display settings dialog will open.

Figure 2.9 Display Setting



Clear Enable alarm pop-up notification, then click *Save*. New alarms reported to the system will no longer appear in a pop-up in the lower-right corner of the interface. Select Enable alarm pop-up notification again and click *Save*. New alarms will again appear in a pop-up in the lower-right corner. As shown in Figure 2.10 below .

Figure 2.10 Alarm Popup Notifications

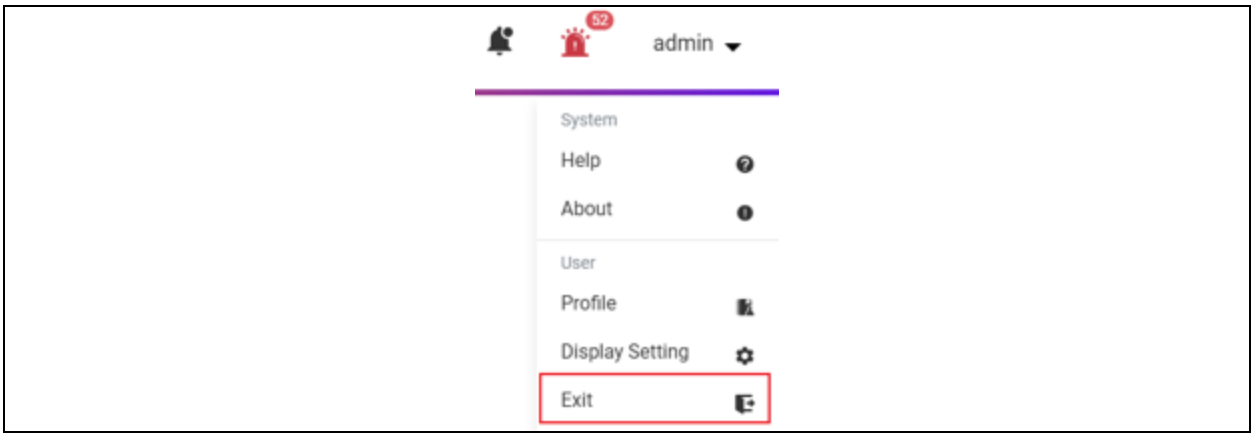


Signing Out

Click the *Exit* option from the drop-down menu to the right of your Username, as shown in Figure 2.11 on the next page , and the system will log you out of the current user.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 2.11 Signing Out



Alarm Icon

In the top-right corner of the header, next to the Notification Bell, there is an Alarm icon that is always visible.

When there are active alarms, a number appears on the top-right corner of the icon. This number shows the total count of active alarms, including:

- Critical
- Warning
- Information

If there are no active alarms, the number is hidden.

The alarm count updates automatically in real time as alarms are triggered or cleared.

Figure 2.12 Alarm Icon

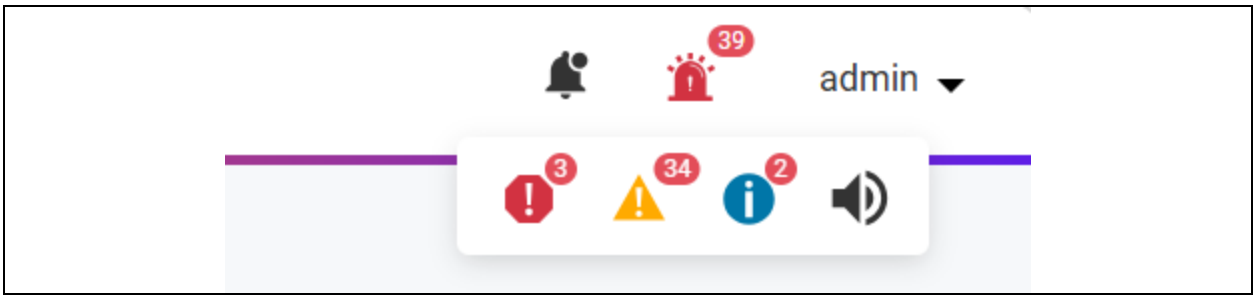


Click the Alarm Icon to open the alarm overview pop-up. The pop-up displays the following four icons side by side (as shown in **Figure 2.13** on the facing page)

- **Critical**: Shows the current count of active Critical-level alarms.
- **Warning**: Shows the current count of active Warning-level alarms.
- **Information**: Shows the current count of active Information-level alarms.
- **Alarm Sound**: Shows the current state of the alarm sound, either On or Off.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 2.13 Alarm Overview Popup



In the alarm overview pop-up:

- Click ***Critical***, ***Warning***, or ***Information*** to go directly to the Alarms page. The system will automatically show only alarms of the selected type.
- You can close the pop-up by clicking anywhere outside it.

To control sound, click the *Alarm Sound* icon to turn the alarm sound on or off. The icon will update to show the current status.

NOTE: Alarm sound settings will be saved in the user's configuration and won't be reset after the next login.

Notification Bell

The **Notification Bell** icon is located in the top-right corner of the header and is visible on all pages.

When there are unread notifications, a number appears on the icon to show how many are unread. If there are no unread notifications, the number is hidden.

There are 2 types of notifications:

1. Fleet Management

2. Asset Warranty Expire Reminder

Click the Notification Bell to open the Notifications panel. The panel displays notification cards grouped by date in the following sections:

Today: Timestamp displayed in HH:MM AM/PM format.

Yesterday: Timestamp displayed in HH:MM AM/PM format.

Older: Date displayed in DD MMM YYYY format.

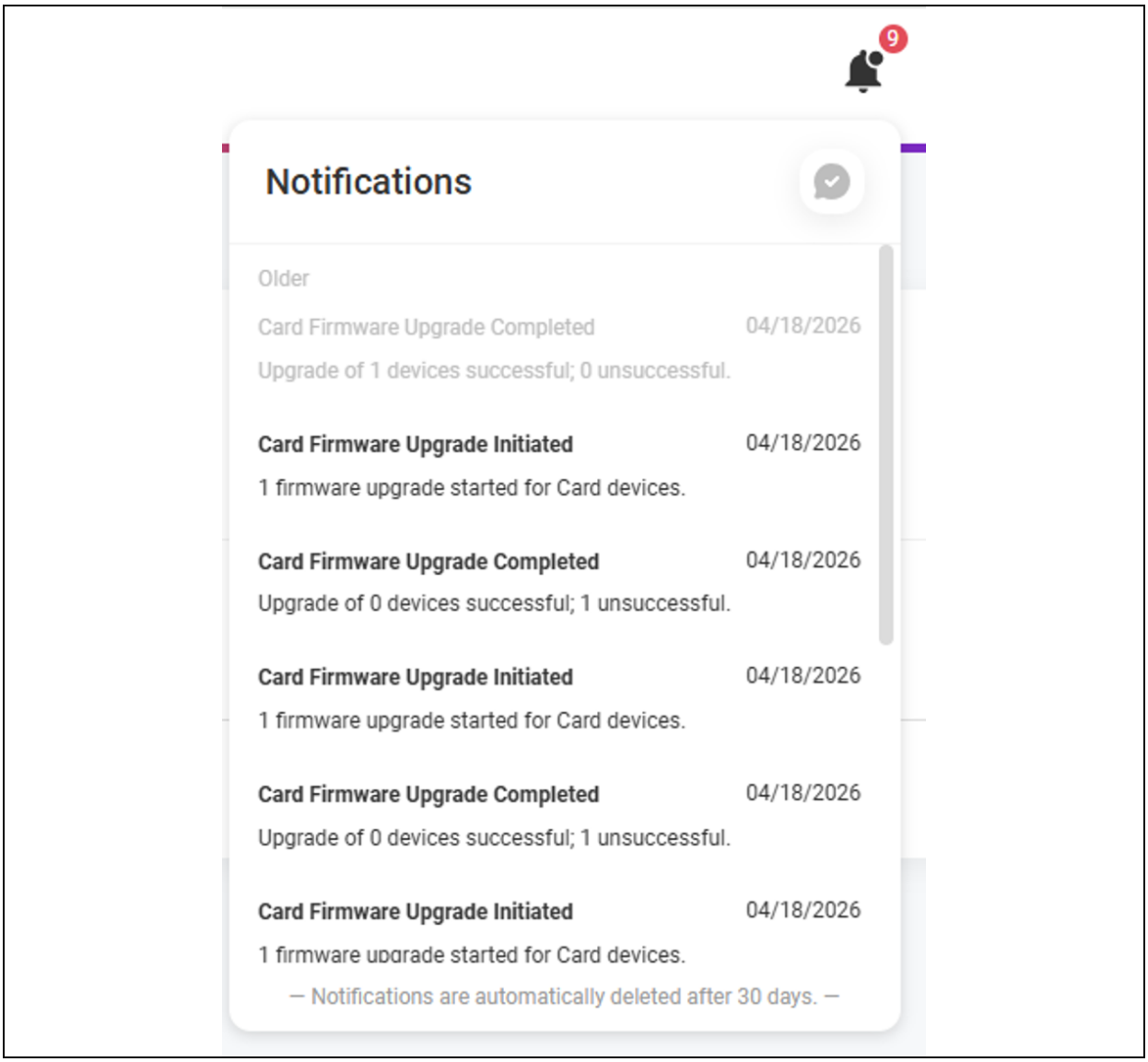
Within each group, notifications are listed in descending order, with the most recent appearing first. Unread notifications appear in bold text. Notifications that have been viewed appear in light grey text.

To mark all notifications as read, click Mark All as Read in the top-right corner of the panel. A confirmation message will appear.

- Click *Yes* to confirm. All notifications will be marked as read, and the unread count will reset to zero.
- Click *No* or *X* to cancel without making any changes.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 2.14 Alarm Overview Notification

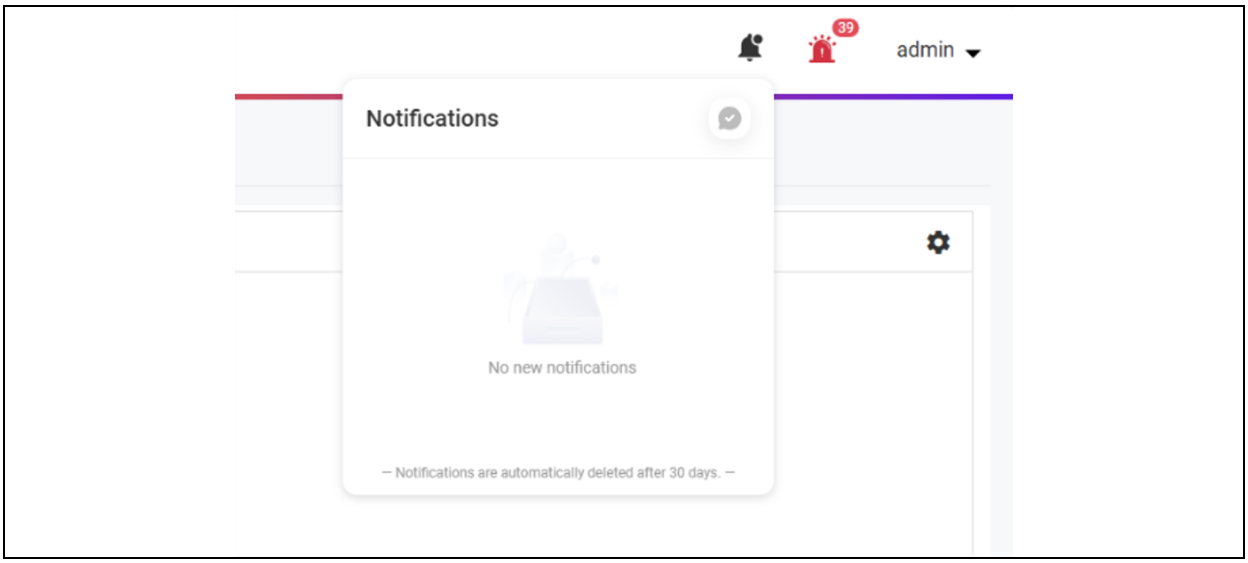


NOTE:

- Read status is tracked for each user individually. Marking a notification as read will not affect other users.
- Notifications are automatically deleted after 30 days. Only notifications from the past 30 days are visible. The retention period can be configured by users in Section 18.2.11 Data Retention. If the retention policy is set to **Never Delete**, this field shall be hidden.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 2.15 Notification Bell Popup when No Notifications



© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

3 Monitoring

3.1 General

3.1.1 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.

3.1.2 Functional Modules

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

3.2 Detailed Features

3.2.1 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.

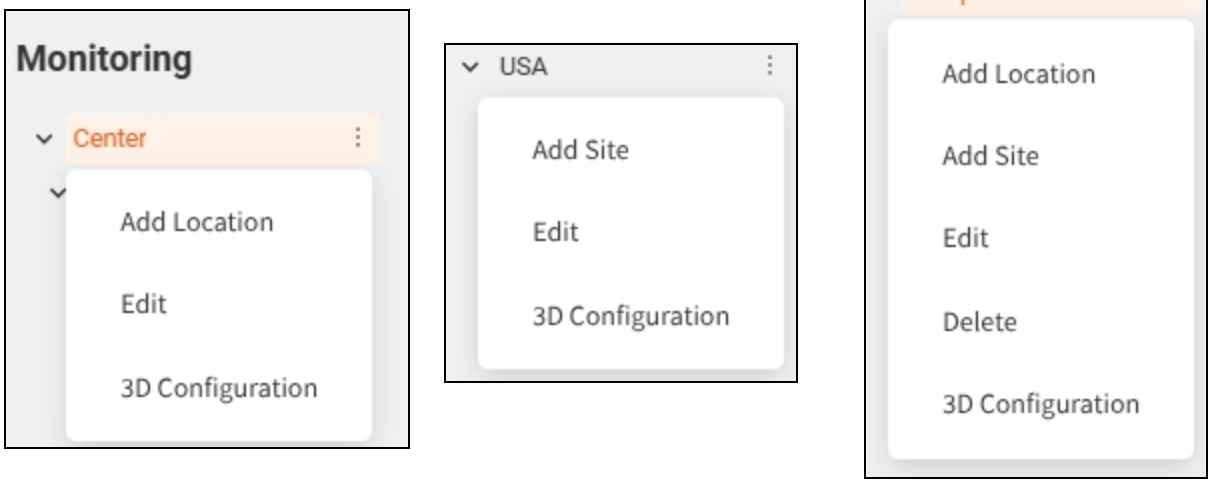
3.2.2 Location

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.)

© 2026 Vertiv Group Corp. All Rights Reserved.

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 ellipses (⋮) icon the right side of center, click *Add Location*, as shown in Figure 3.2 below .

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 on the facing page .

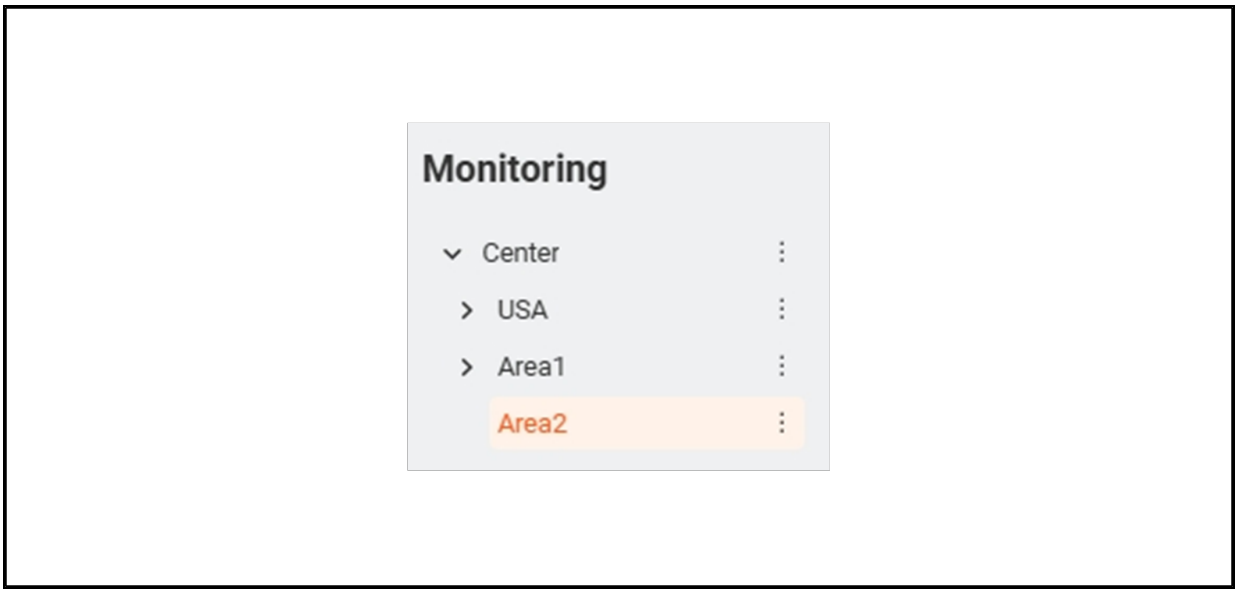
© 2026 Vertiv Group Corp. All Rights Reserved.

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 below .

Figure 3.4 After Editing Location



If you need to add a location under location Area2, click on the ellipses (⋮) on the right side of location name and repeat steps 1 to 3 .

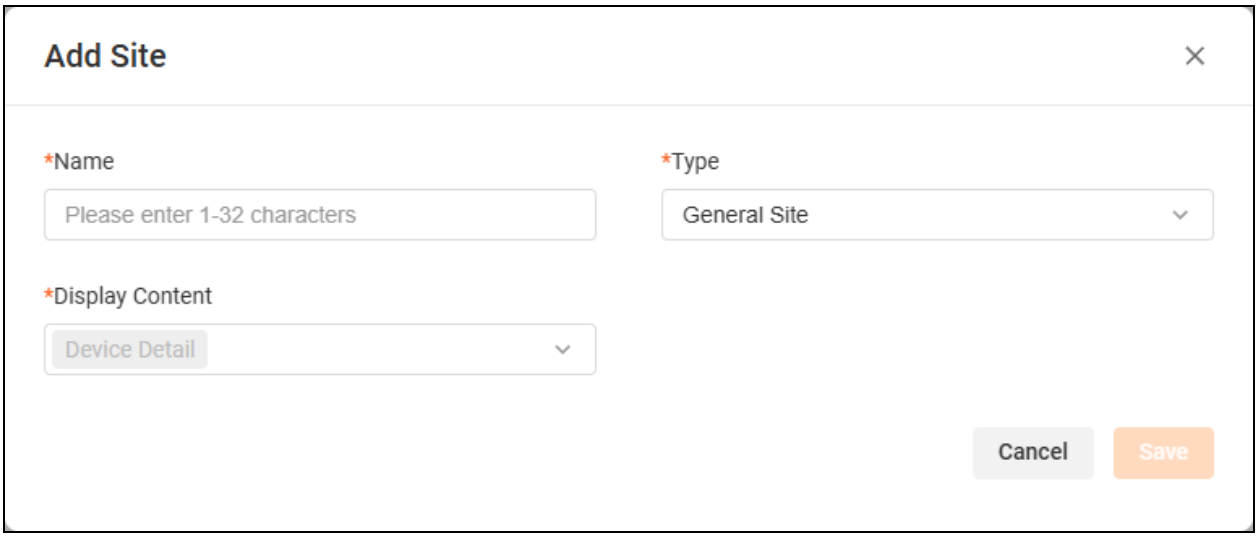
2. Adding a Site

2.1 Adding a General Site

1. Take the Area2 Location as an example, click the ellipses (⋮) 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 on the next page .

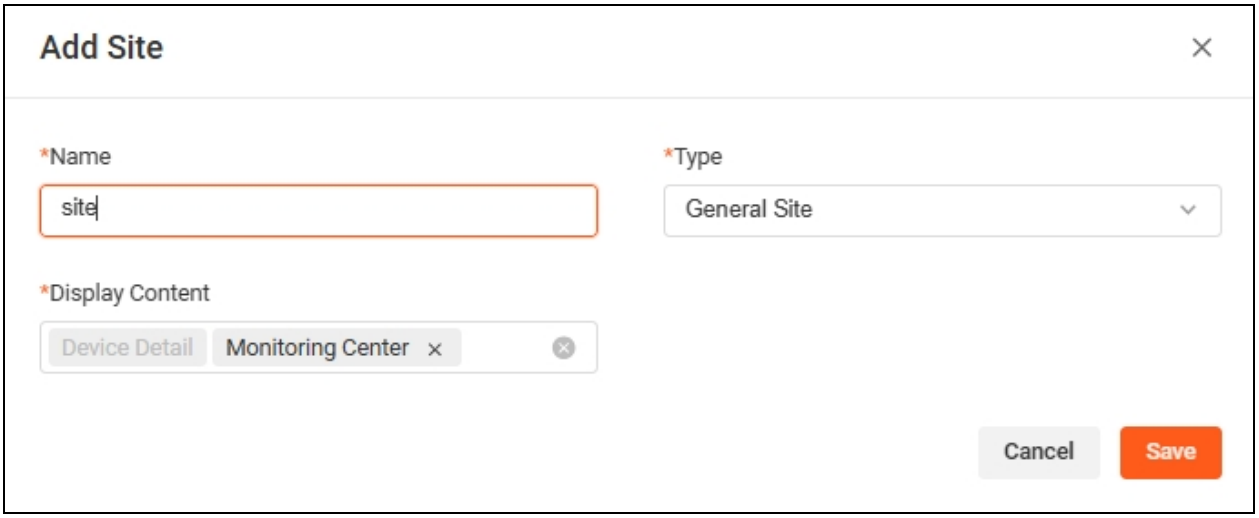
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.5 Adding a General Site



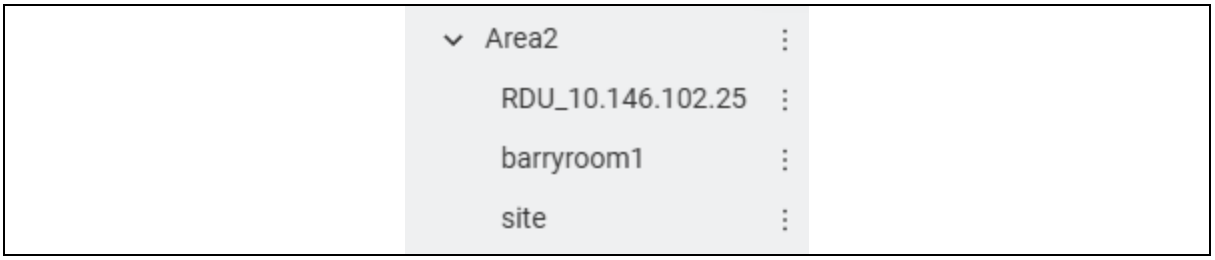
2. Enter the name of the site, for example, as **Site**. The Display Content field controls the displaying tab on this site's homepage. Device Detail is selected by default, as shown in **Figure 3.6** below .

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

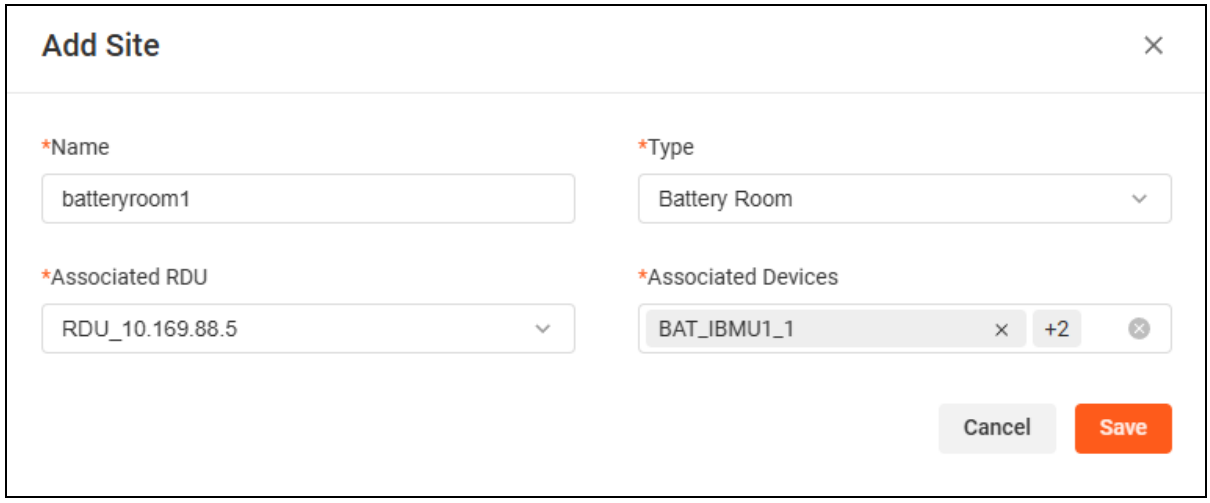


© 2026 Vertiv Group Corp. All Rights Reserved.

2.2 Adding Battery Room Sites

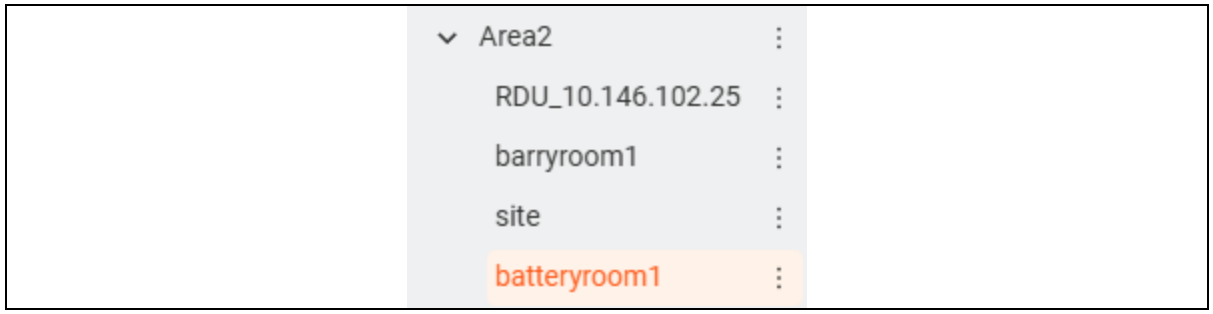
1. To add a new battery room site, select Battery Room for the site type in the Add Site pop-up window, and select the associated RDU and device. When you select the associated devices, you can move lithium battery devices, lead-acid battery devices, UPS and power meter devices from the RDU site to the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

Figure 3.8 Added a 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

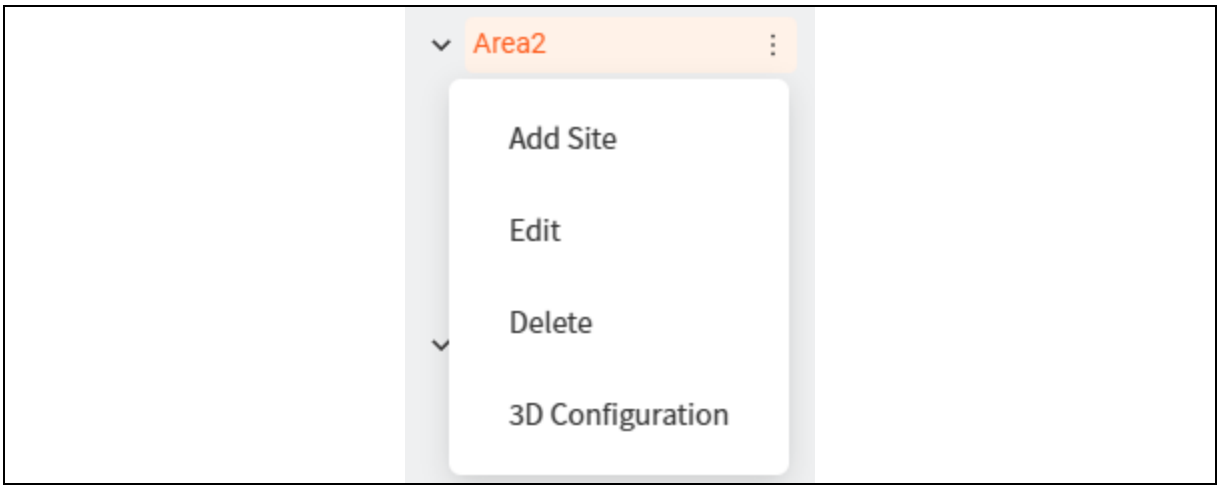


3. Editing Location:

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

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.10 Action Menu



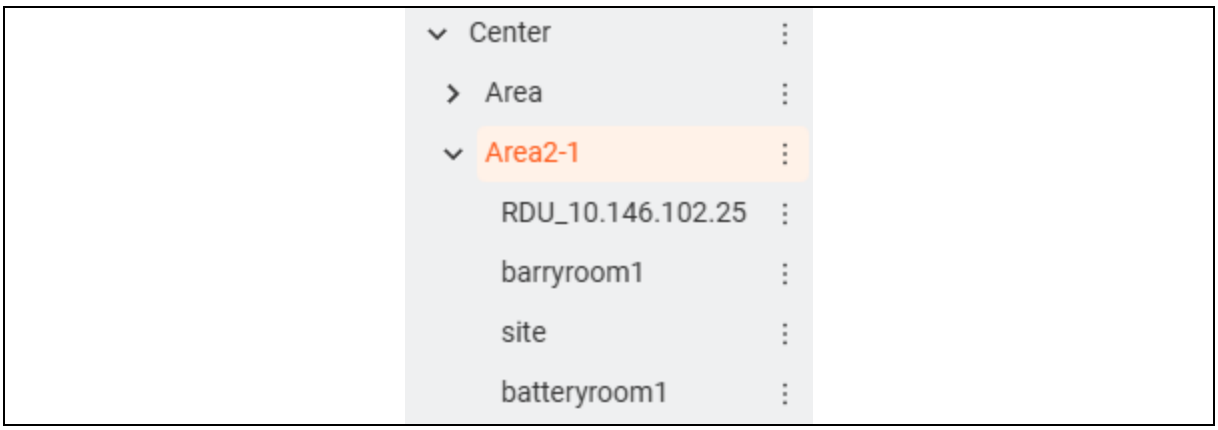
You can modify the name of the location, as shown in Figure 3.11 below .

Figure 3.11 Edit Location



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

Figure 3.12 Location Management Page



© 2026 Vertiv Group Corp. All Rights Reserved.

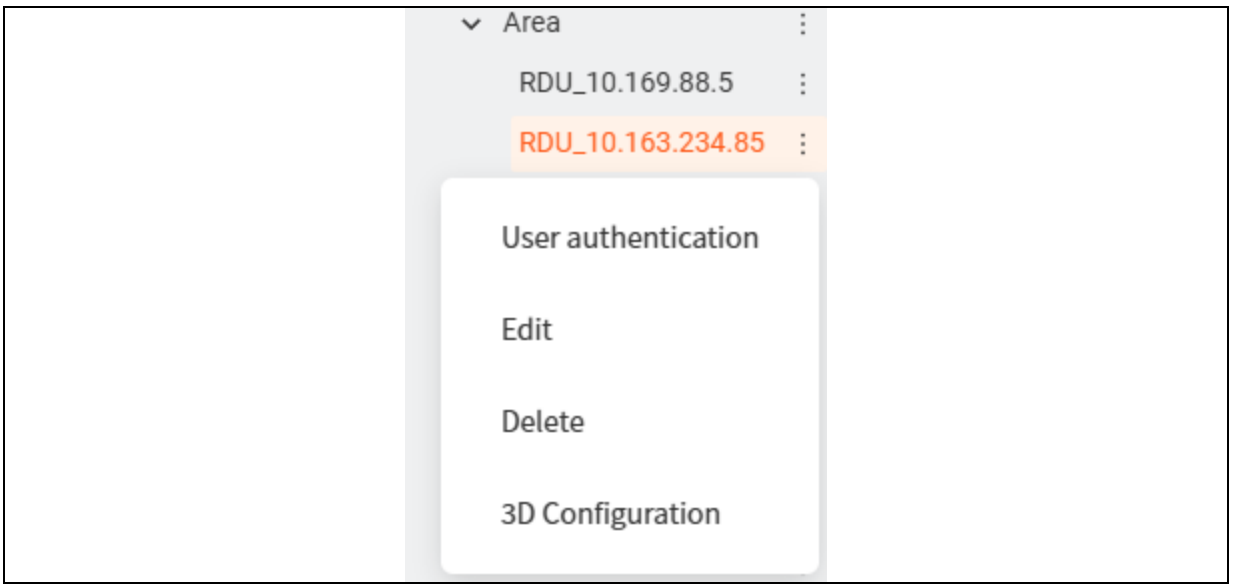
3.2.3 Site

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 ellipses (⋮) 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 below .

Figure 3.13 RDU Site Action Menu

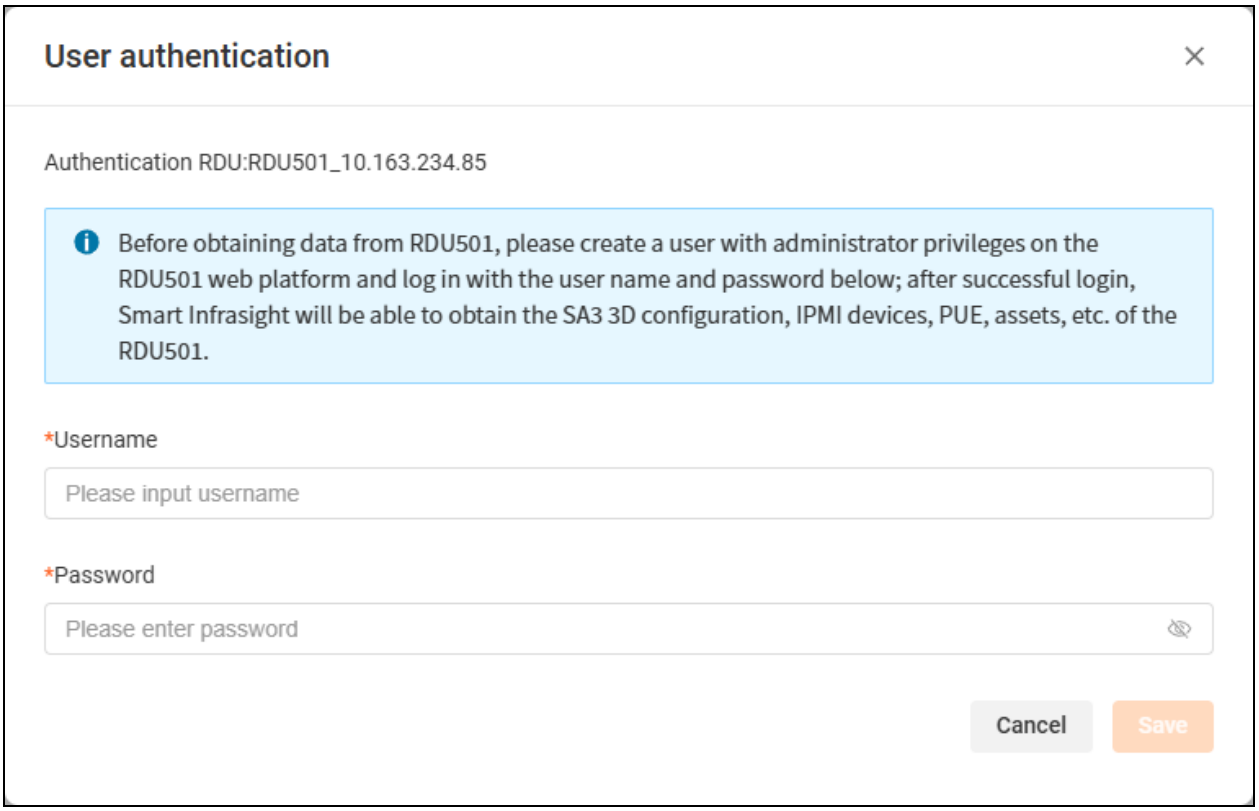


By clicking the User authentication button, you can enter the administrator account and password for the corresponding RDU. Once authentication is successful, Smart InfraSight can retrieve data from the RDU, including the 3D layout of Smart Aisle, Smart Row, Smart Cabinet, IPMI device information, PUE,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

NOTE: It is recommended not to use the default RDU administrator account. Smart InfraSight may repeatedly log that account out. Create a second administrator account on the RDU and enter those credentials here.

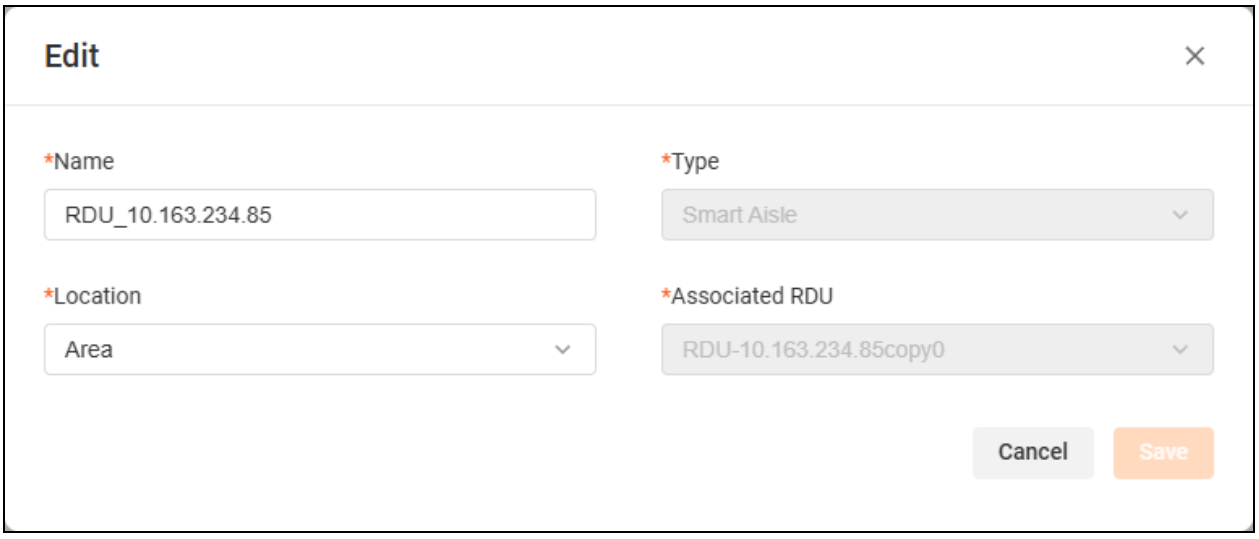
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.14 Pop-up interface — User Authentication



1. 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 .

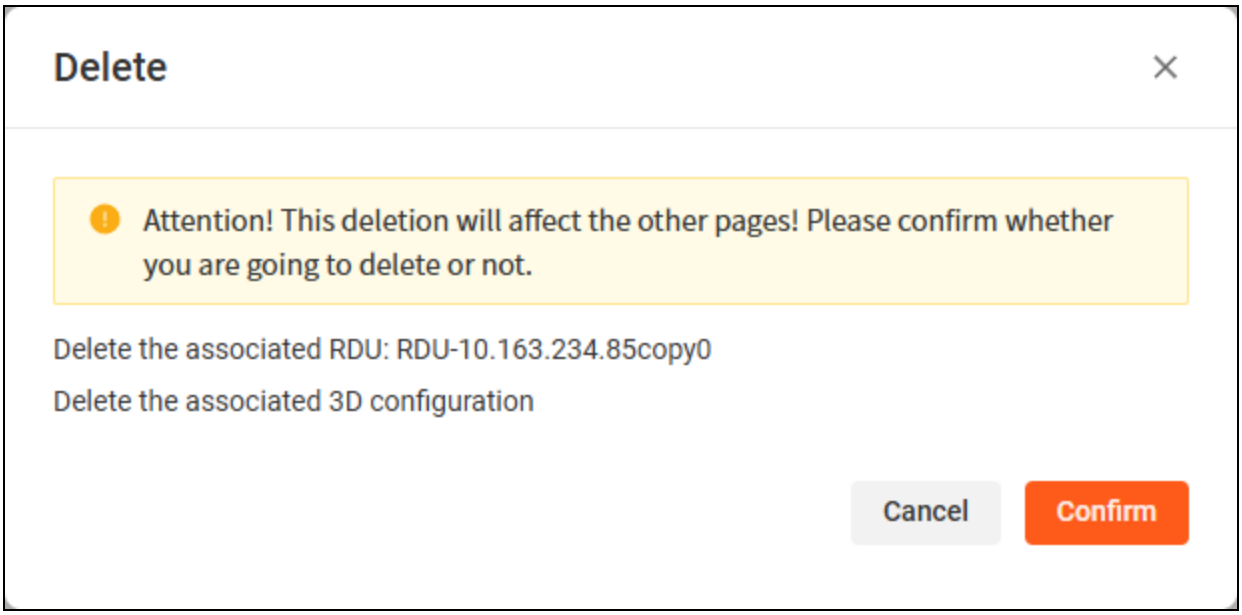
Figure 3.15 Editing the Site



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

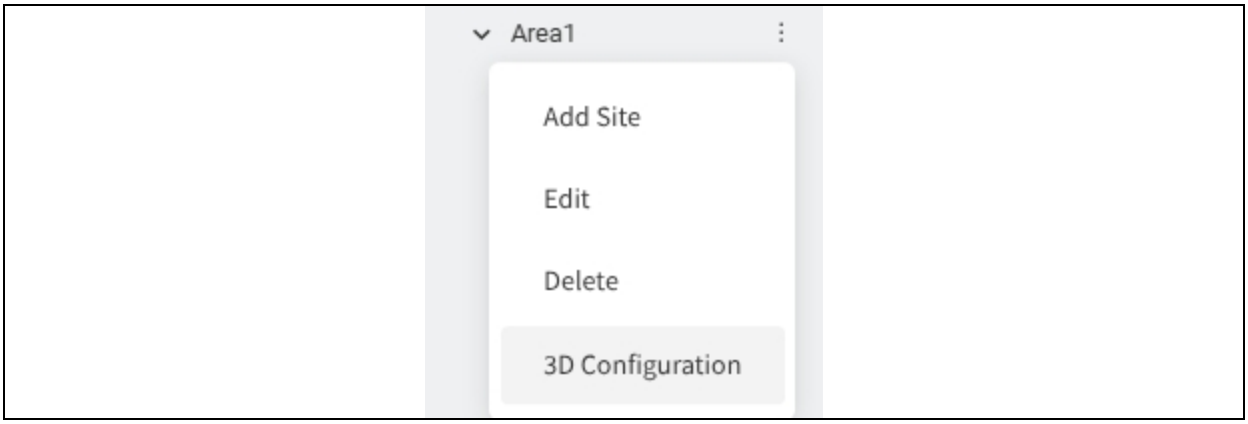
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.16 Site Deletion Popup Box



3. Click the *3D configuration* button to enter the 3D configuration interface of the current site. Refer to Chapter 3D Configuration for details.

Figure 3.17 3D Configuration Interface Selection



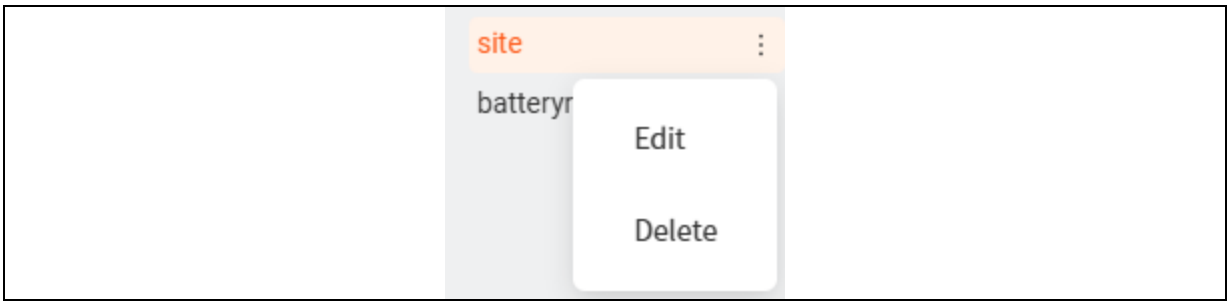
NOTE: 3D configuration currently supports Smart Aisle2, Smart Aisle3, Smart Row2 and CREMS Site, and Battery Room Site.

2. General Site

By default, SNMP devices monitored by users are attached to the Default Site, which cannot be deleted. Any manually created general sites can be deleted by the user. Click the ellipses (⋮) on the right side of the site to open the action menu, as shown in Figure 3.18 on the next page .

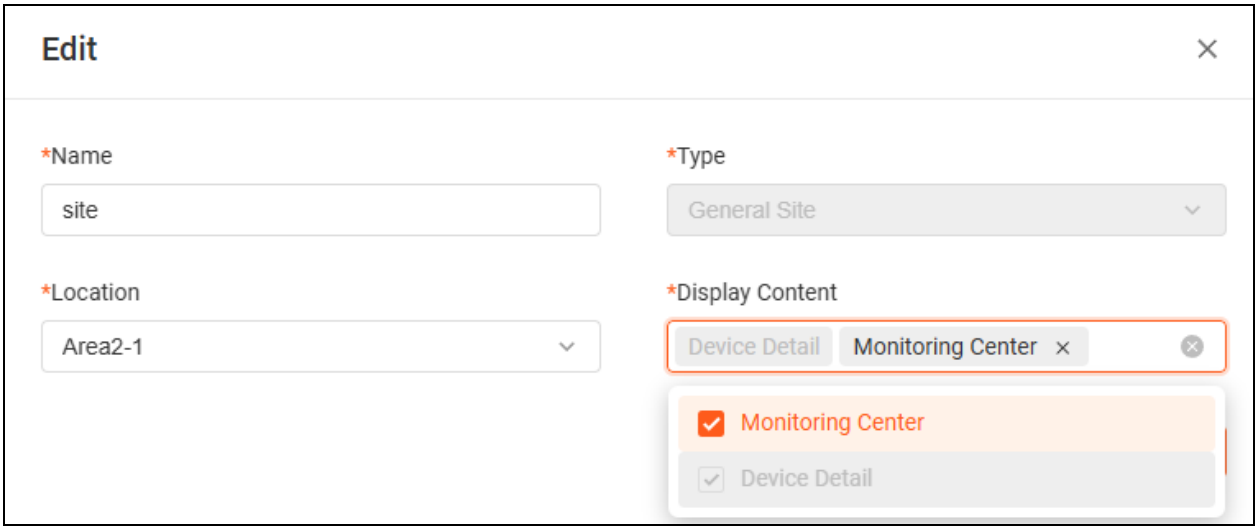
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.18 General Site Action Menu



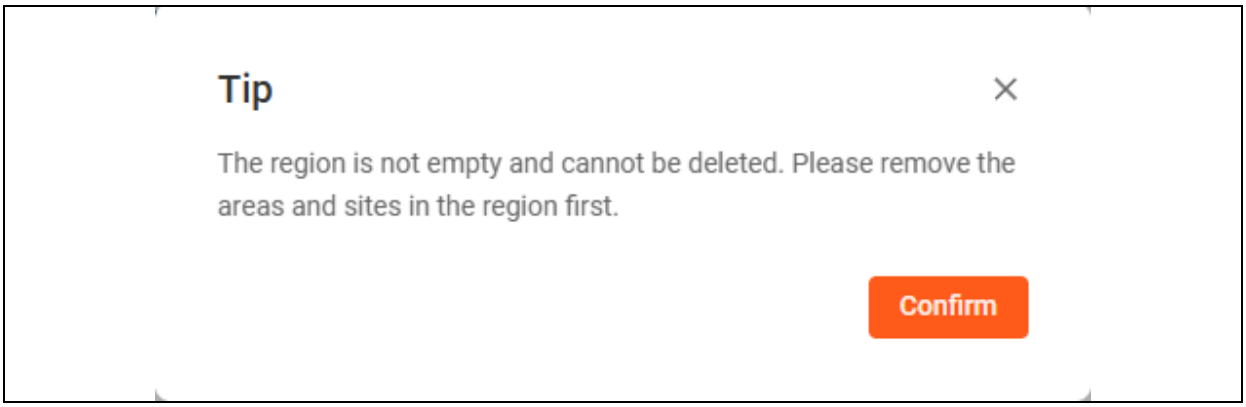
1. Click the *Edit* button to modify the current site name, location, and display content. By changing the Display Content, you can display or hide the Monitoring Center of the site, as shown in Figure 3.19 below

Figure 3.19 The General Site Edit Popup Box



2. Click on *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

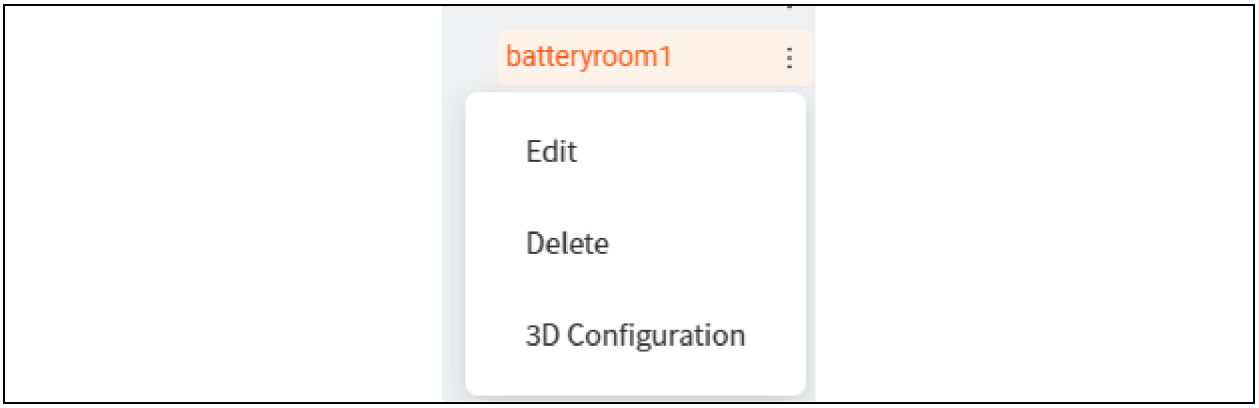


© 2026 Vertiv Group Corp. All Rights Reserved.

3. Battery Room Site

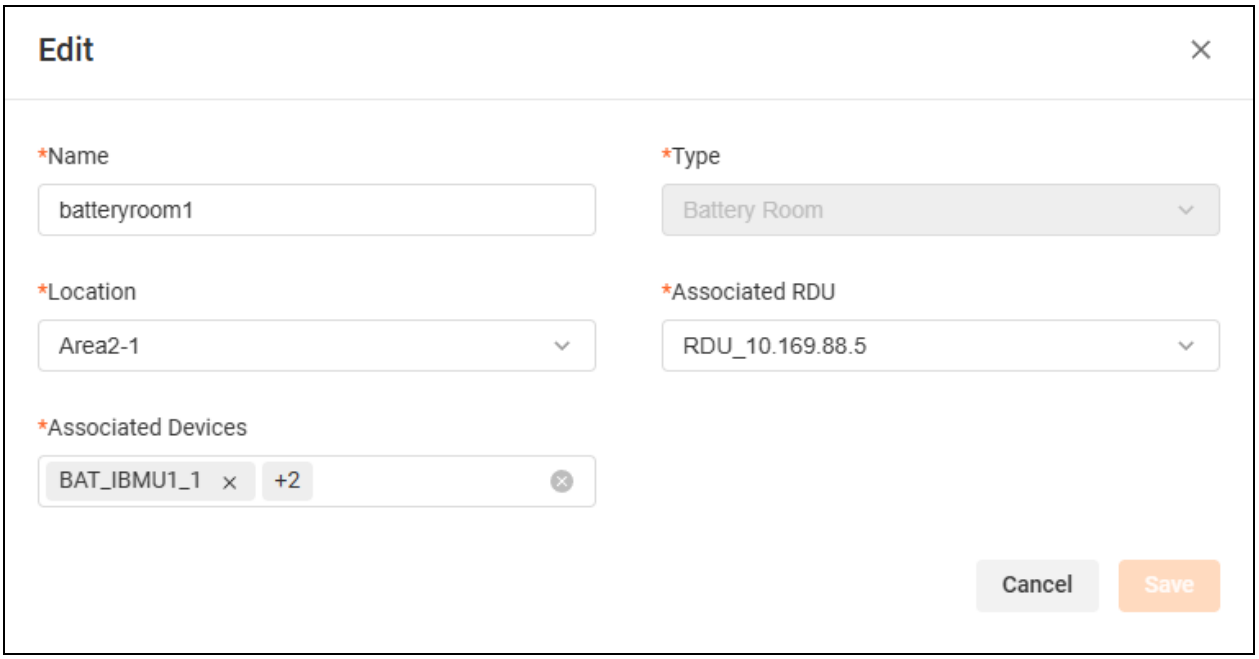
The user-created battery room site can be associated with the corresponding RDU site. Battery and other devices can then be moved from the RDU site to be managed under the battery room site. Take a battery room site as an example, click the ellipses (⋮) on the right to pop up the action menu. As shown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

Figure 3.21 Battery Room Site Action Menu



1. 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 .

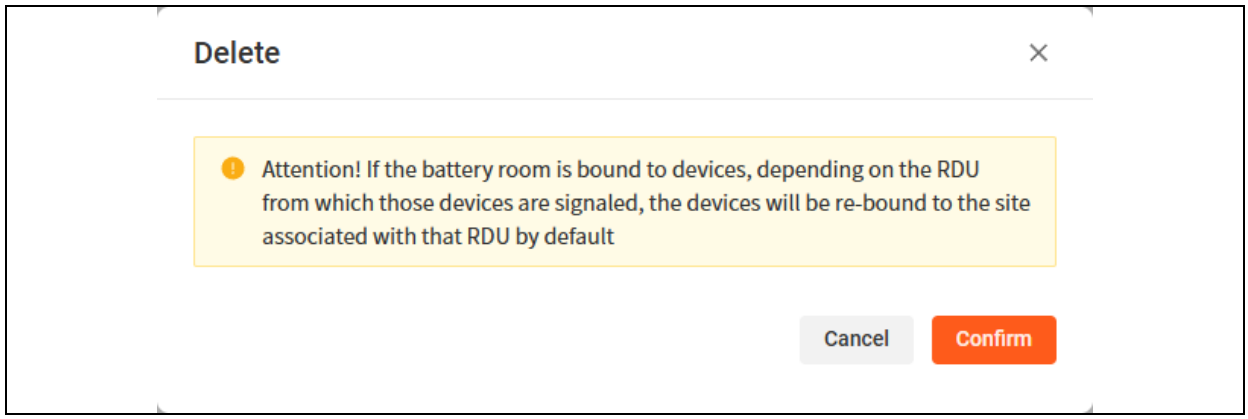
Figure 3.22 Editing Battery Room Site



2. Click the *Delete* button. Once the battery room site has been deleted, the devices bound to the battery room will be rebound to the RDU site where the devices were originally monitored, as shown in Figure 3.23 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.23 Popup Box for the Battery Room for Deletion



3.2.4 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

1. 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



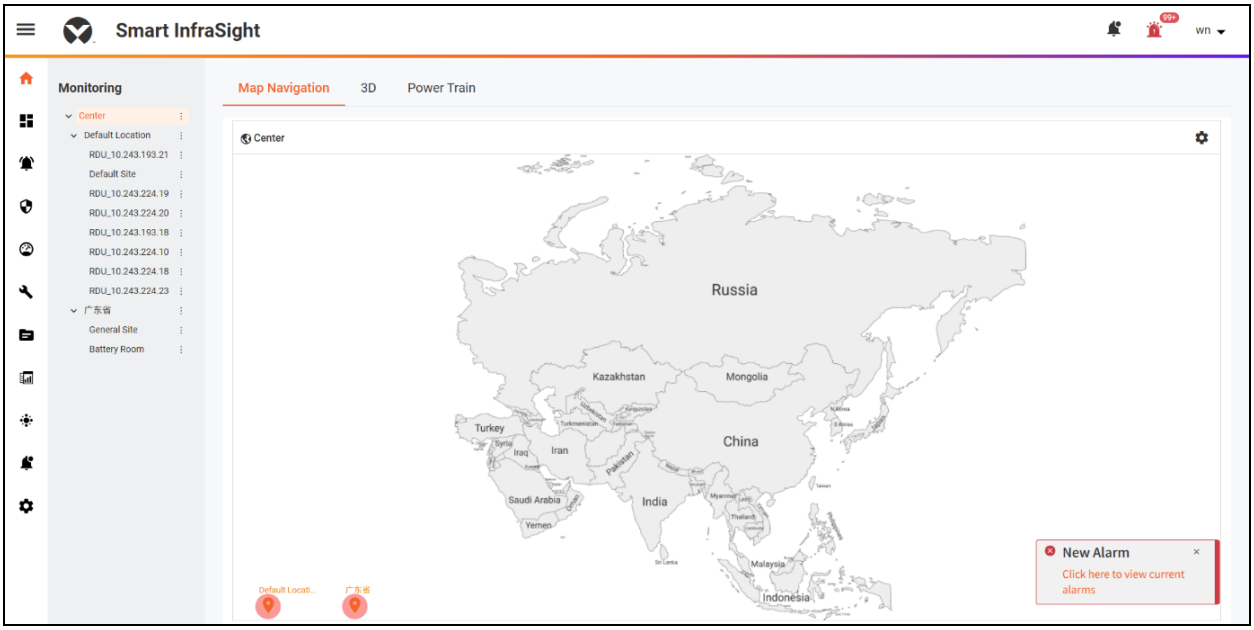
2. Select a background image and click *Save* to set the background image.

© 2026 Vertiv Group Corp. All Rights Reserved.

2. Editing the Site Position

1. 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 3.2 on page 19 .

Figure 3.25 Editing the Site Position

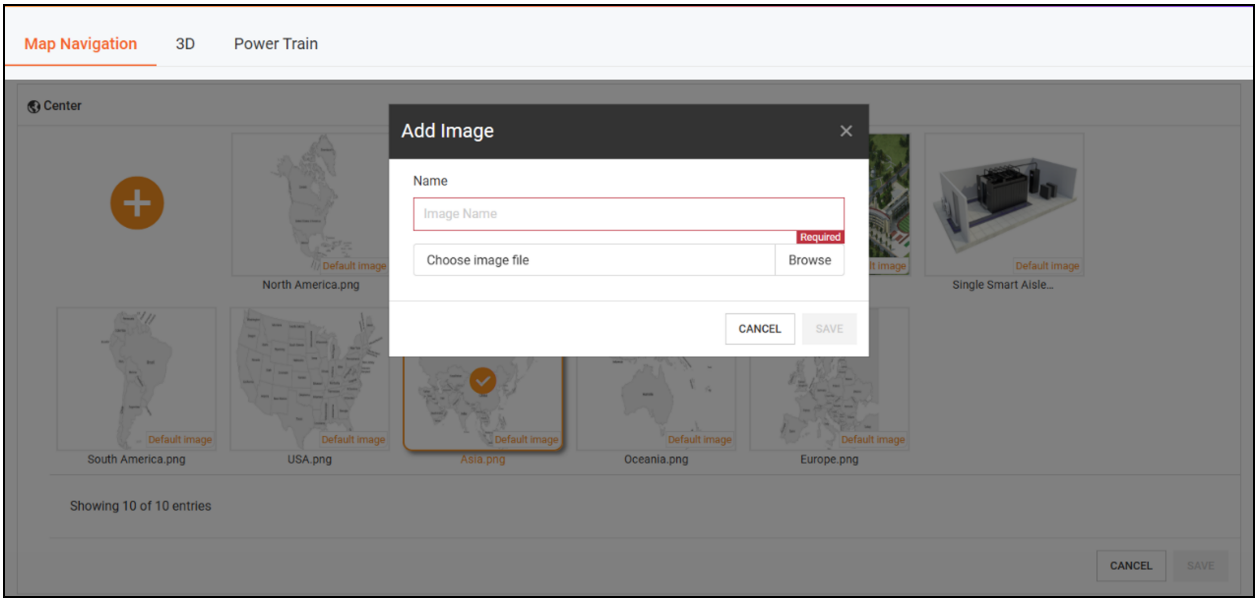


2. Drag the site icon to a target position and click *Save* in the bottom right corner.

3. Uploading a Custom Background Image

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

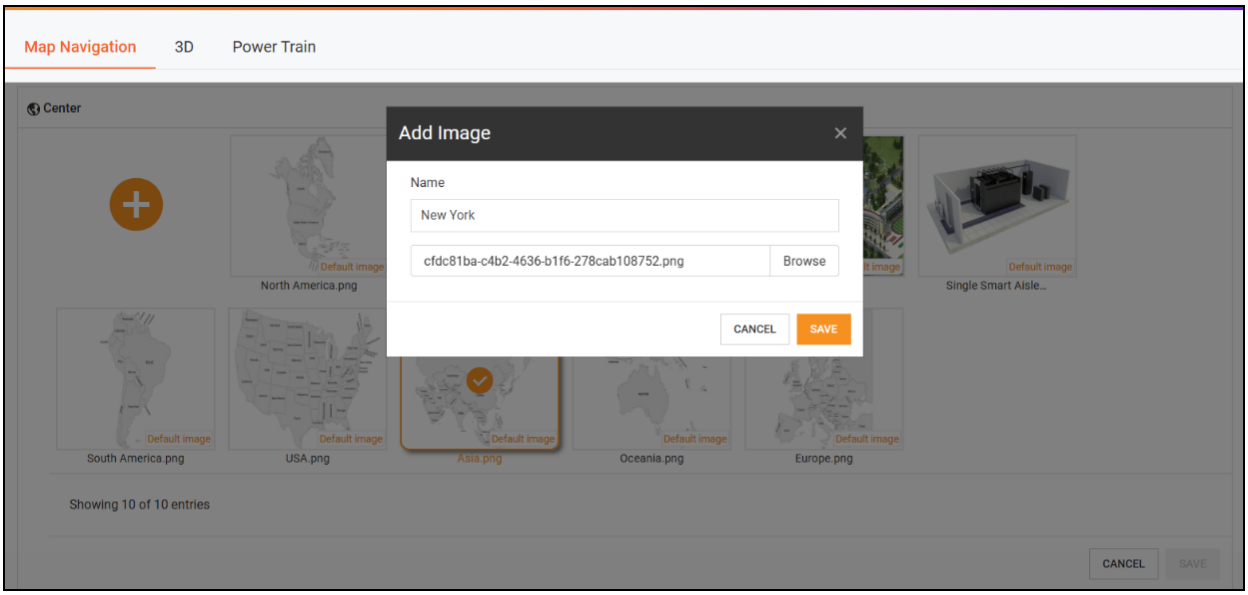
Figure 3.26 Adding Image Popup Window



© 2026 Vertiv Group Corp. All Rights Reserved.

2. Enter a name for the image, select a path for the image as shown in Figure 3.27 below , 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:

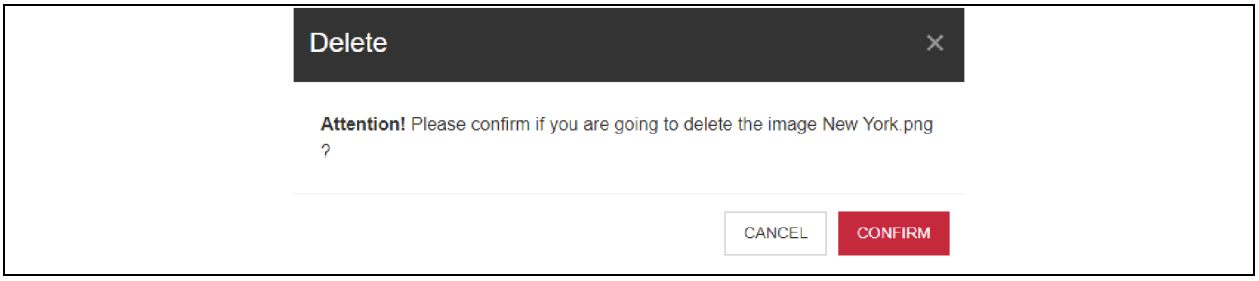
1. Image names support only the following special characters: -, _, and ..

2. Only PNG, JPG, and GIF formats are supported.

4. Deleting the Background Image

1. 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.

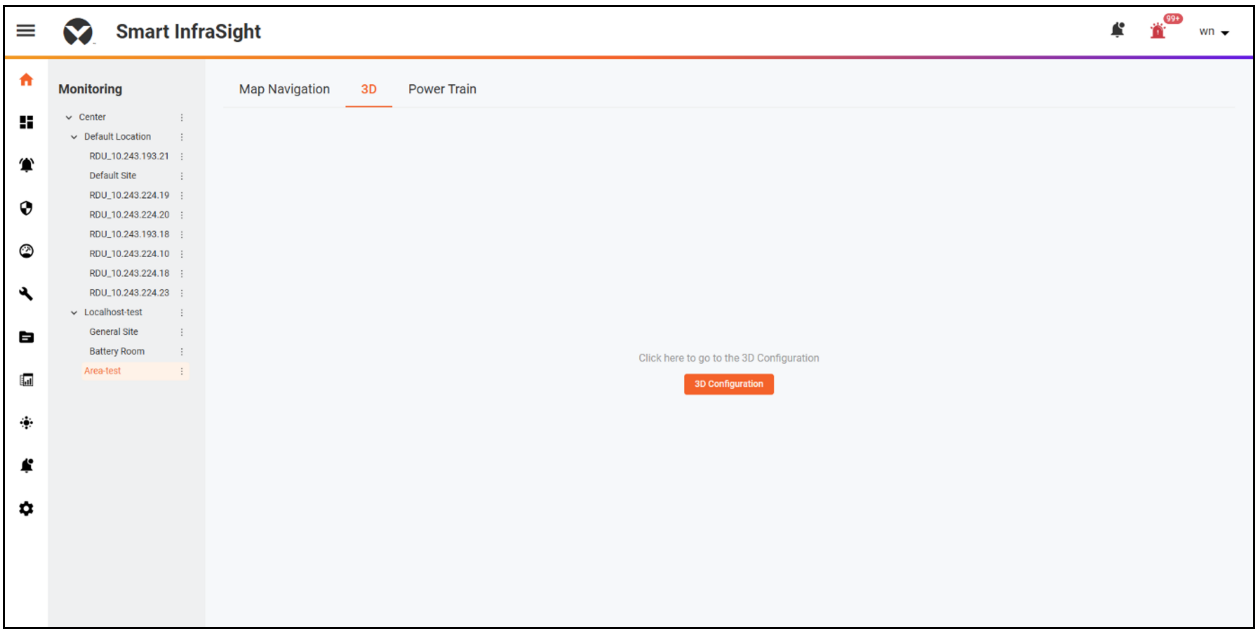
3.2.5 Location: 3D

There are two ways to enter the 3D configuration.

1. If the location has not initialized 3D, you can click the 3D tab and jump to 3D configuration following the instructions, as shown in Figure 3.29 on the facing page .

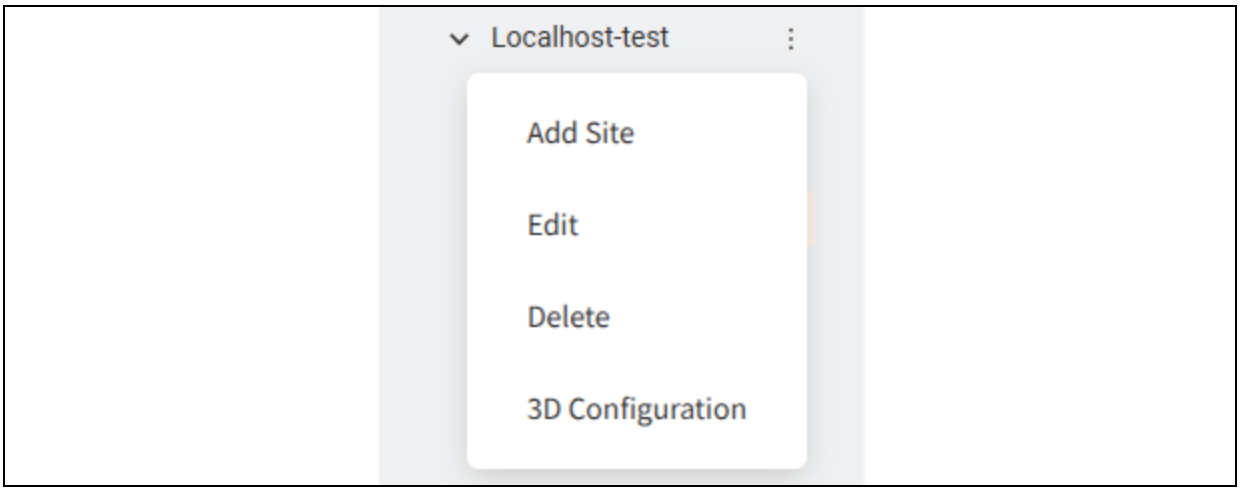
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.29 Entering Location 3D Configuration Path 1



2. Click on the ellipses (⋮) 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



Refer to Detailed Functions on page 47 in 3D Configuration on page 47.

3.2.6 Site: Monitoring Center

The site monitoring home page at most includes 5 parts:

- Monitoring Center
- 3D
- Power

© 2026 Vertiv Group Corp. All Rights Reserved.

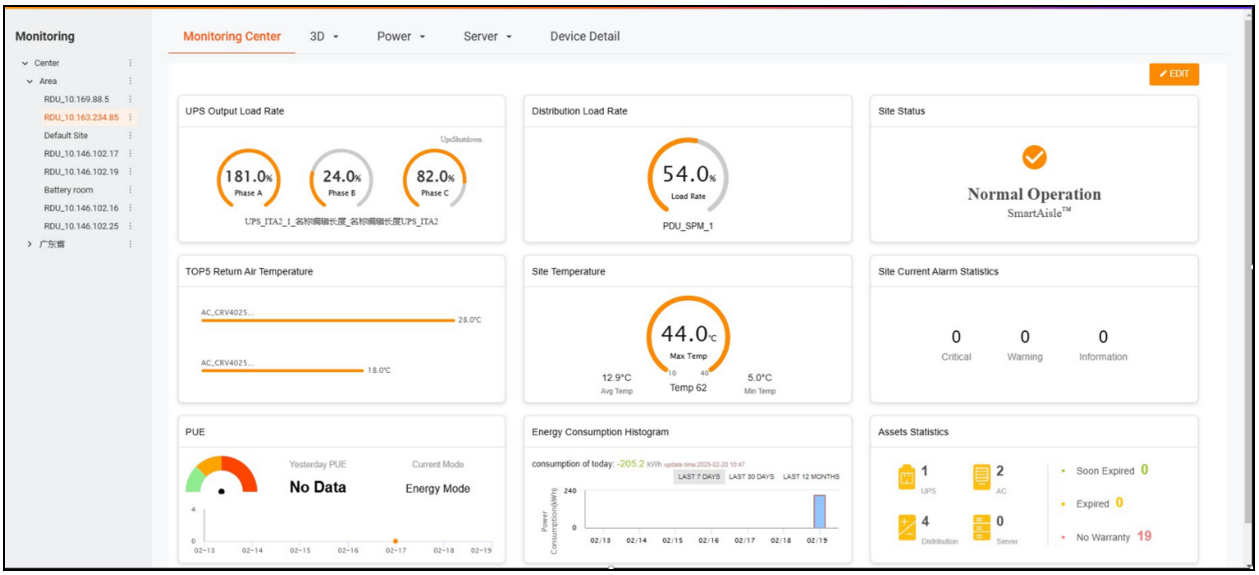
- Server
- Device Details

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 Dashboard on page 163 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 Histogram
- Asset Statistics

Figure 3.31 Monitoring Home Page



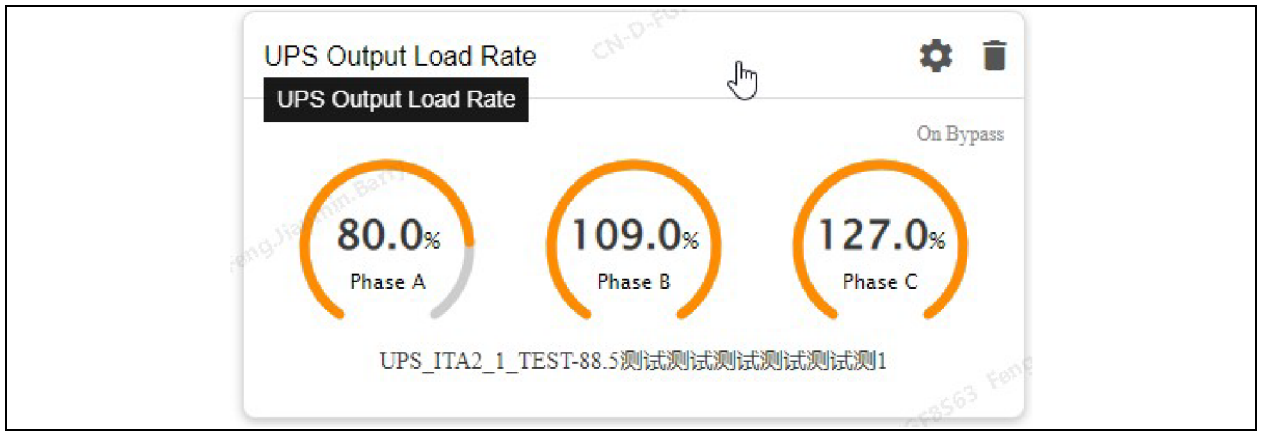
By default, the monitoring home page displays the nine widgets of the current site, and the user can delete, edit, add, and drag the nine widgets by selecting the Edit button in the upper right corner.

1. Deleting the Widgets

1. Hover over the widget's header to display the config button and delete button, as shown in **Figure 3.32** on the facing page .

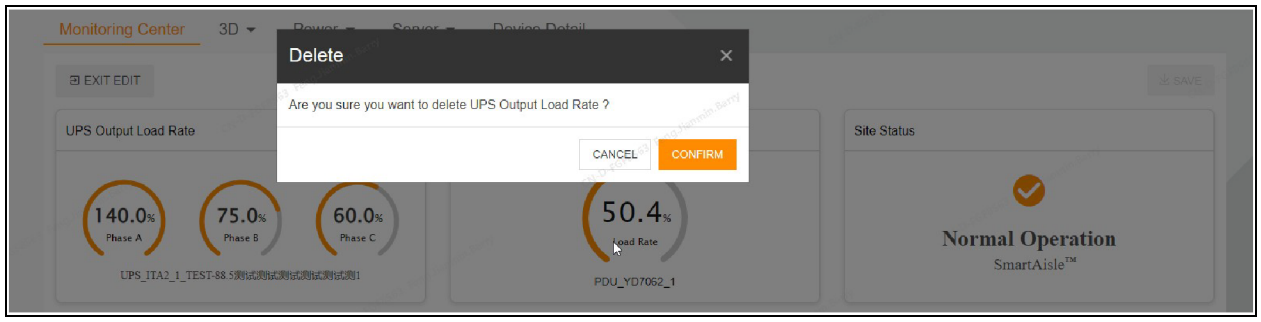
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.32 Deleting the Widget



2. Click the *Delete* icon, and a pop-up box prompts the user to decide whether to delete the widgets.
3. Click *Confirm* to delete the current widgets, as shown in Figure 3.33 below .

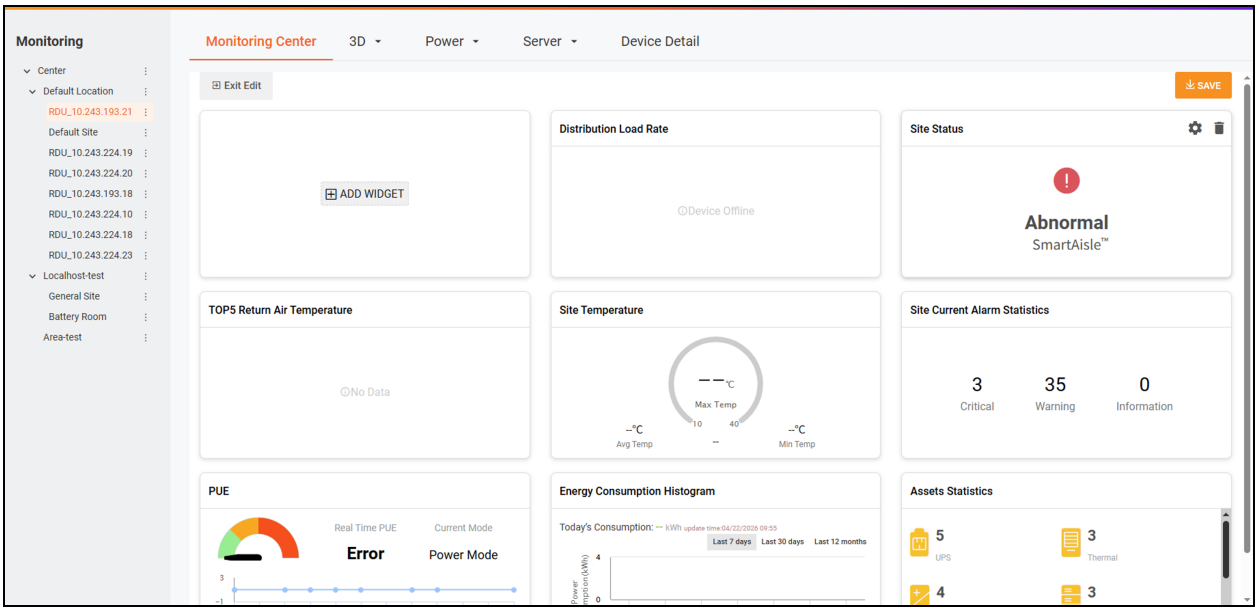
Figure 3.33 Deletion Popup Window



4. After the modification is completed, click *save* in the upper right corner edited monitoring homepage.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.34 The Monitoring Home page after Deletion



2. Editing the Widgets

1. Hover over the widget, and you can click the *Edit* button to display the widget's Config pop-up window, as shown in **Figure 3.35** below .

Figure 3.35 Editing a Widget

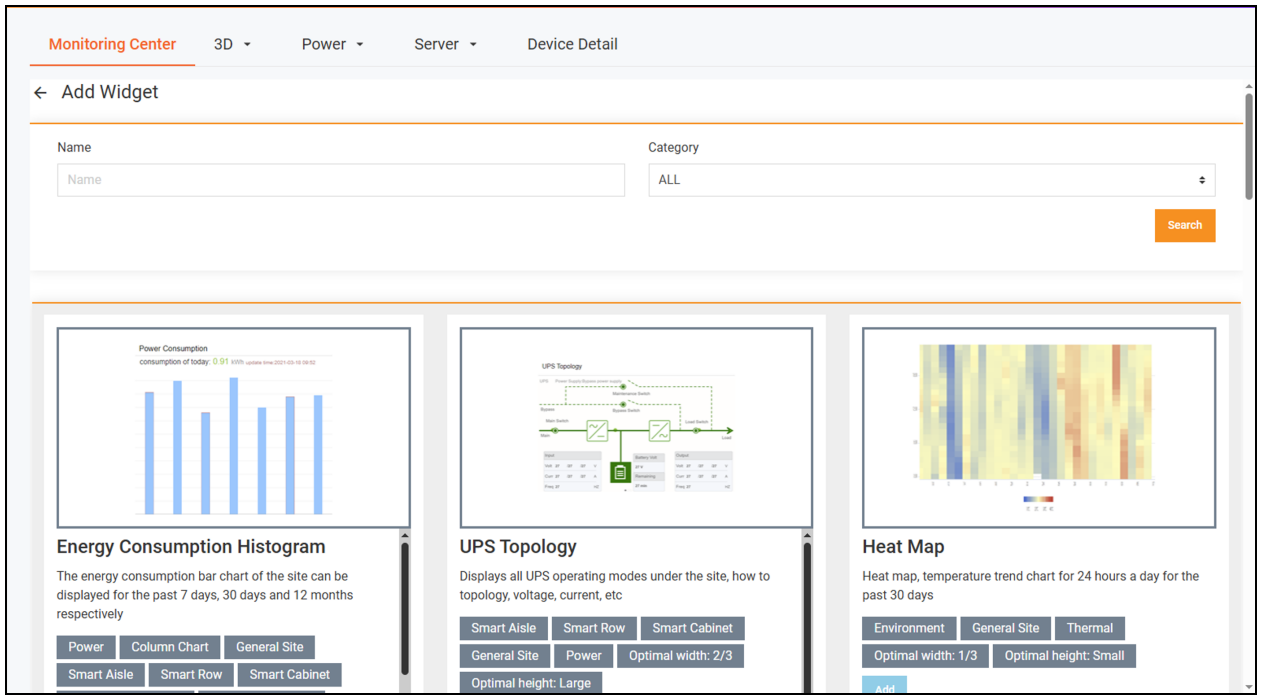


3. Adding New Widgets

2. 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 facing page .

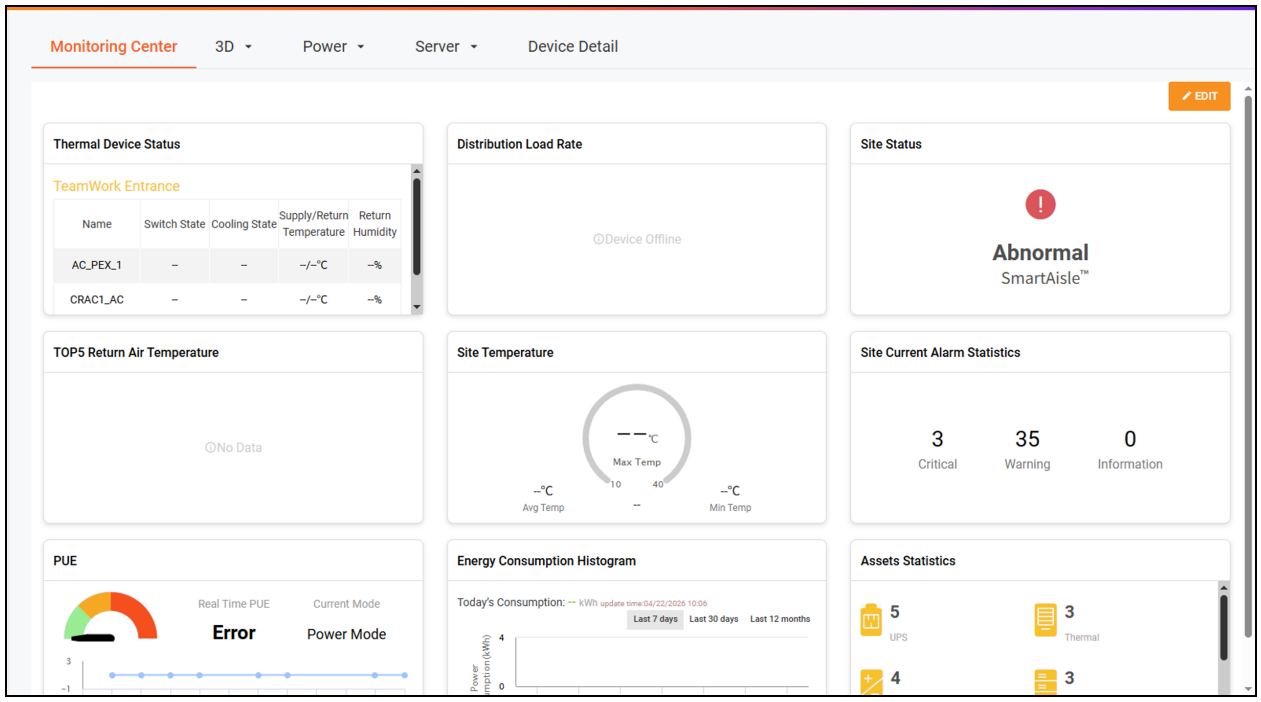
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.36 Adding Widgets Page



You can select the target widget. Click *Add* to add the new widgets on the monitoring homepage. As shown in **Figure 3.37** below .

Figure 3.37 After Adding the Widgets



© 2026 Vertiv Group Corp. All Rights Reserved.

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 widget. 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 Management on page 143.

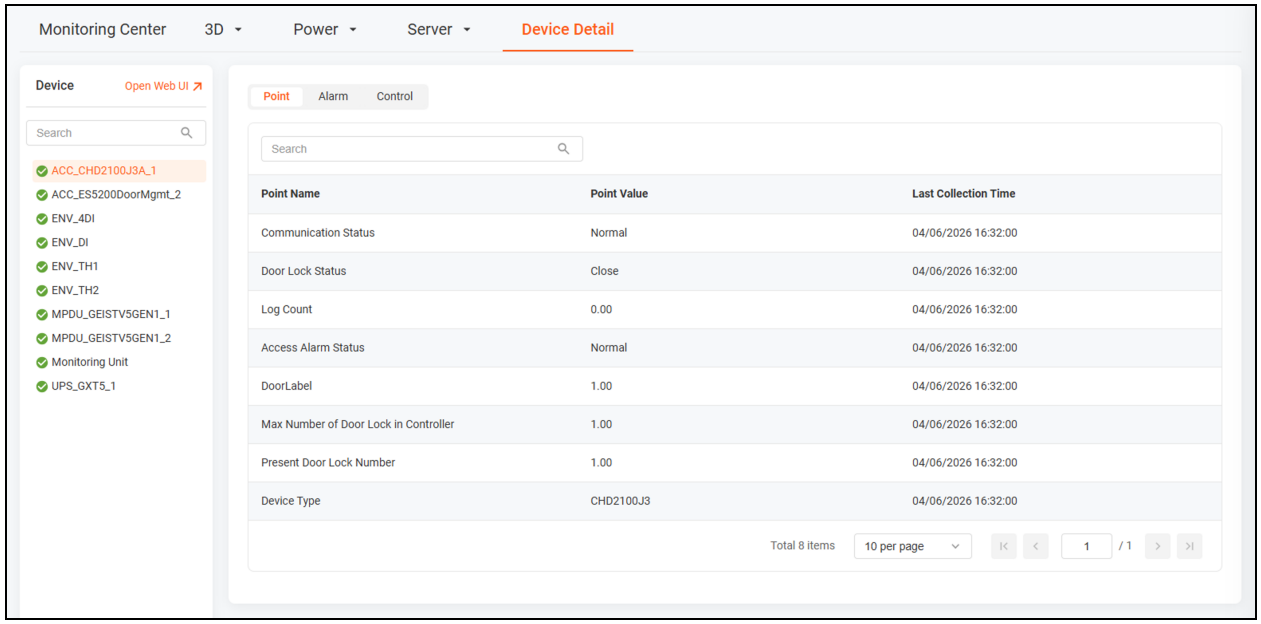
Server

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 151.

Device Details

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

Figure 3.38 Device Details Page



Click *Open Web UI* to go to the corresponding RDU management site. HTTPS on port 443 is used by default.

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 facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.39 Device Point Page

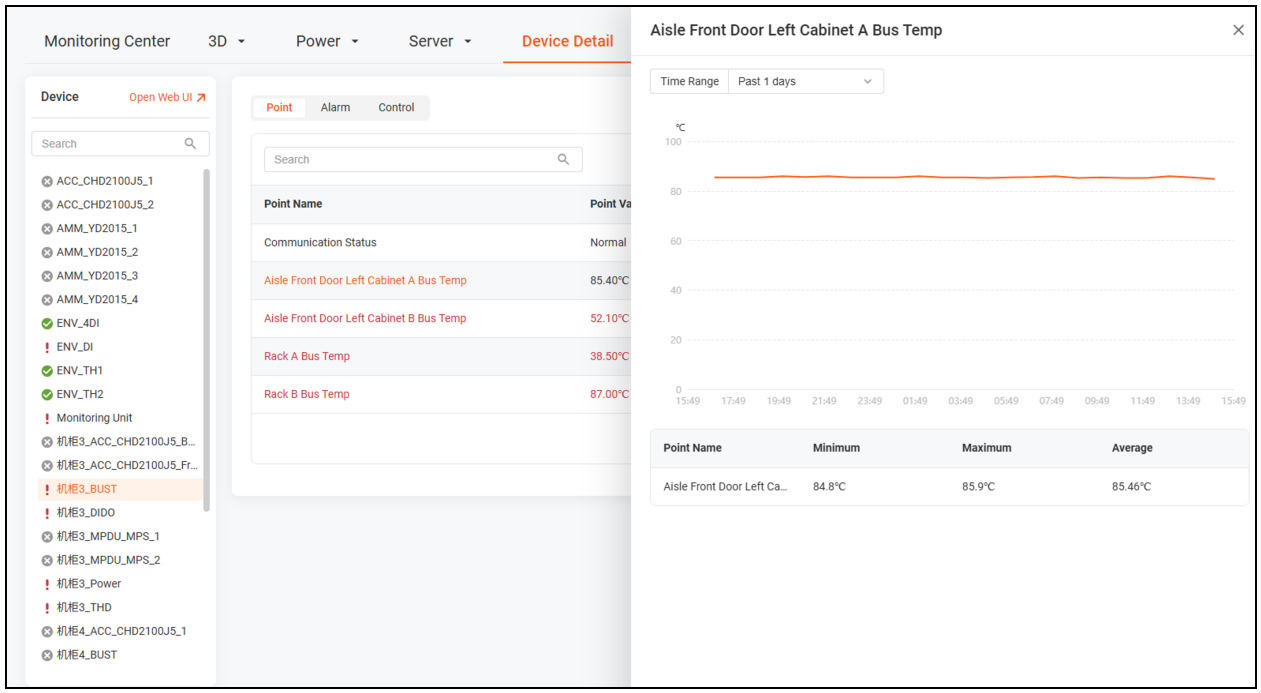
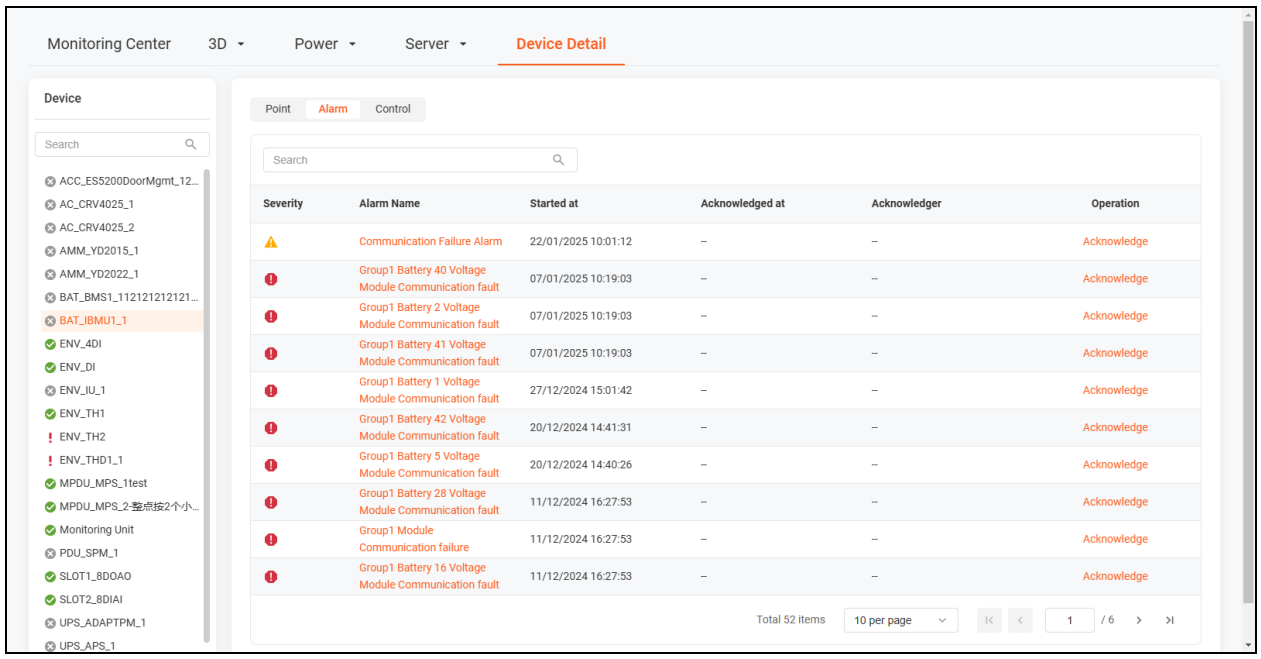
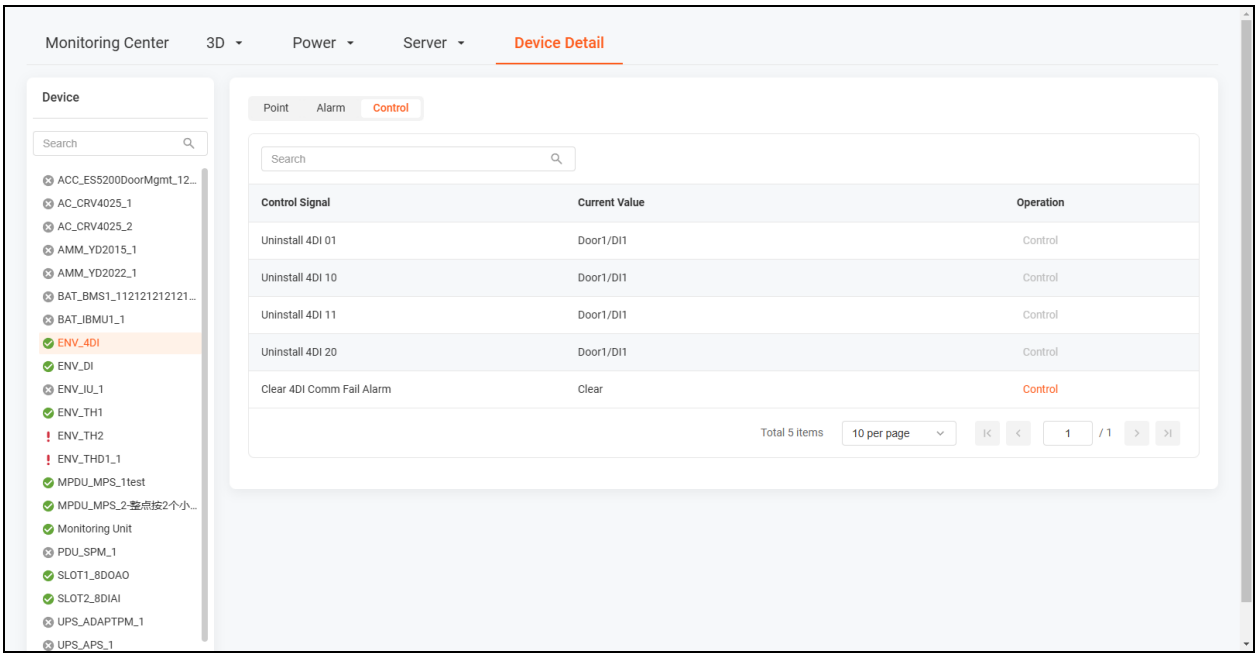


Figure 3.40 Device Alarm Page



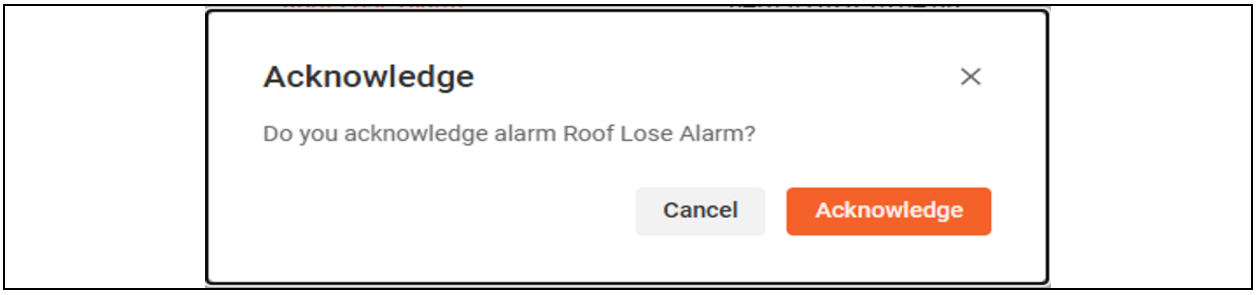
© 2026 Vertiv Group Corp. All Rights Reserved.

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 .

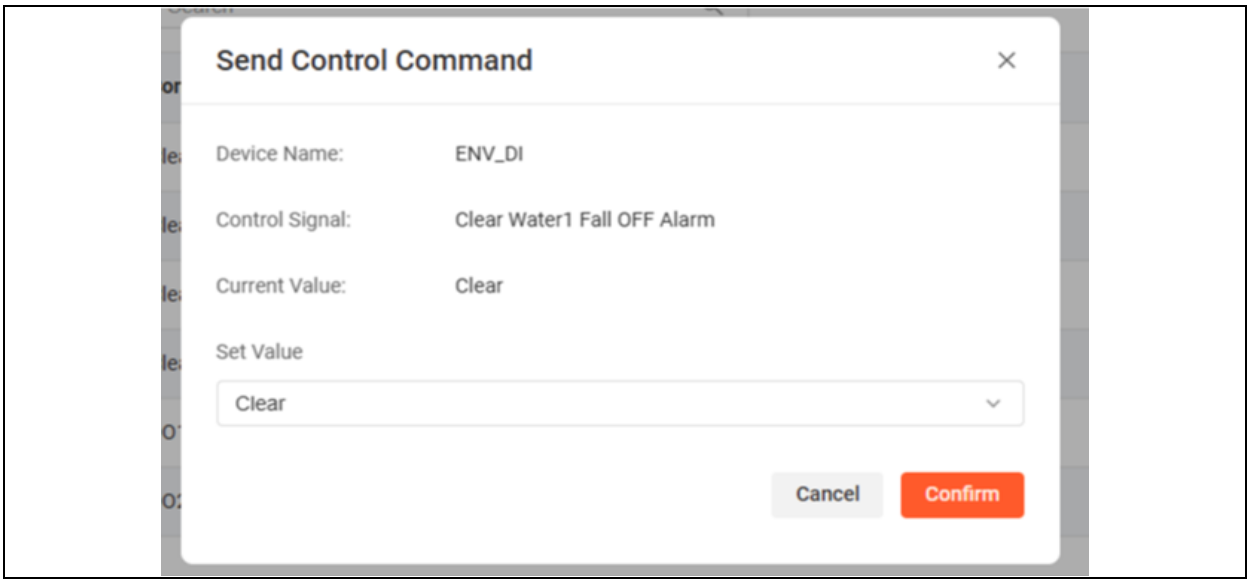
Figure 3.42 Alarm Acknowledging



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

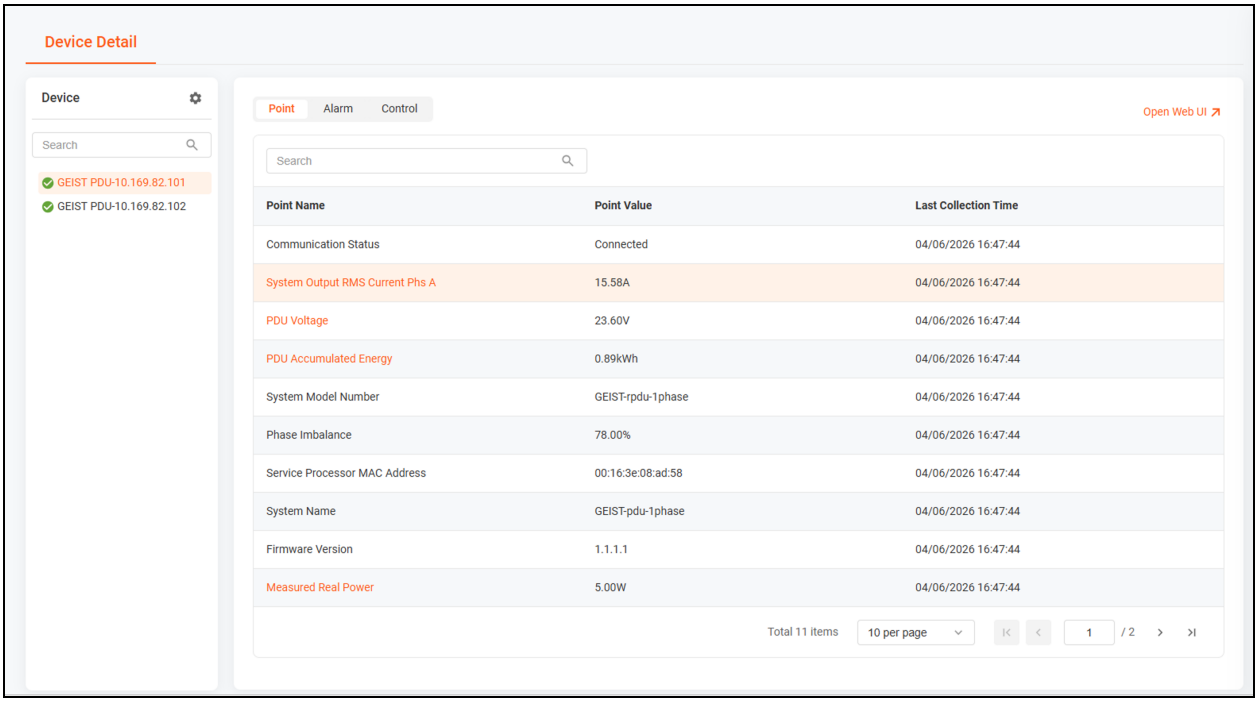
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.43 Device Control sends Control Commands



For the General Site or Default Site that manages SNMP devices, you can manage SNMP devices under the 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

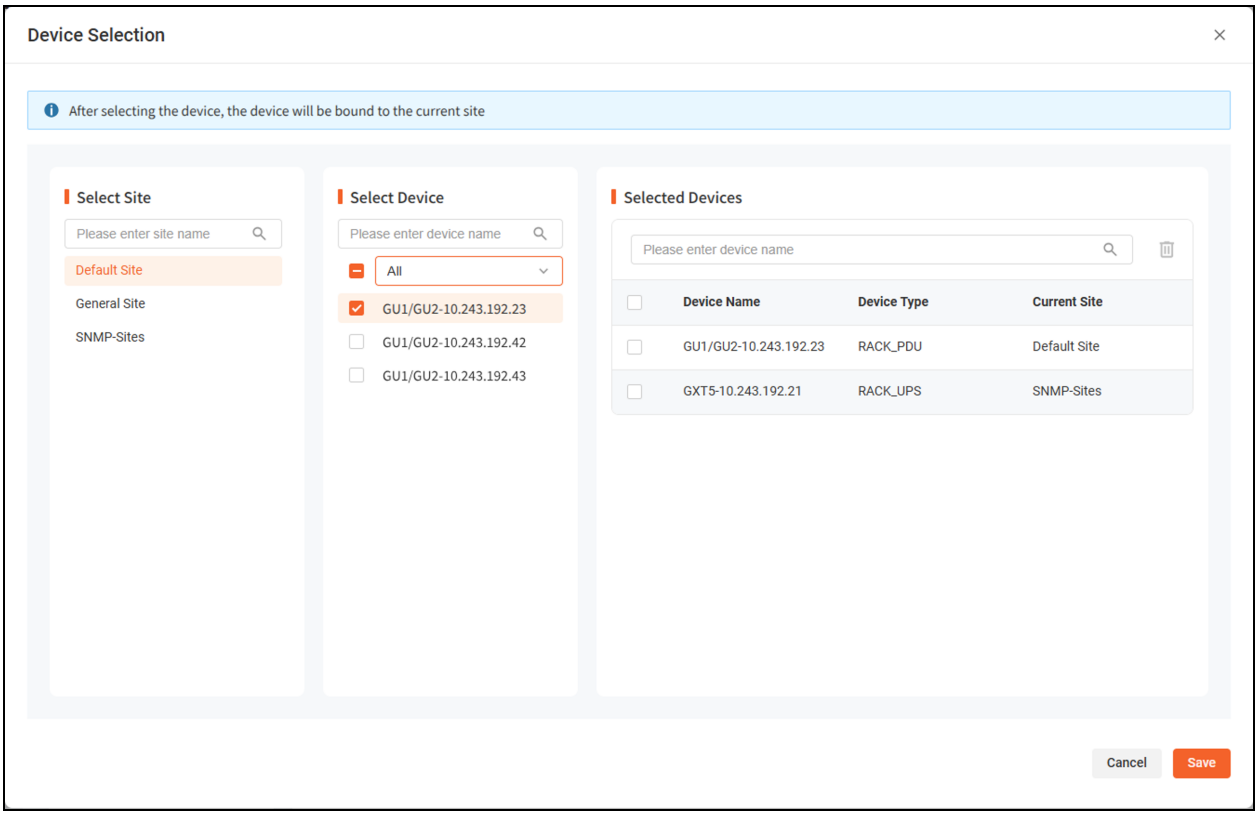


Click the *Open Web UI* button in the upper-left corner. The page opens the management interface for the currently selected device. Hover over the button to preview the navigation URL. If the URL is incorrect, go to Device Management → Device Properties, then under Card Access Settings update Protocol and Port to set the correct link.

© 2026 Vertiv Group Corp. All Rights Reserved.

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 below .

Figure 3.45 Device Selection Popup Window

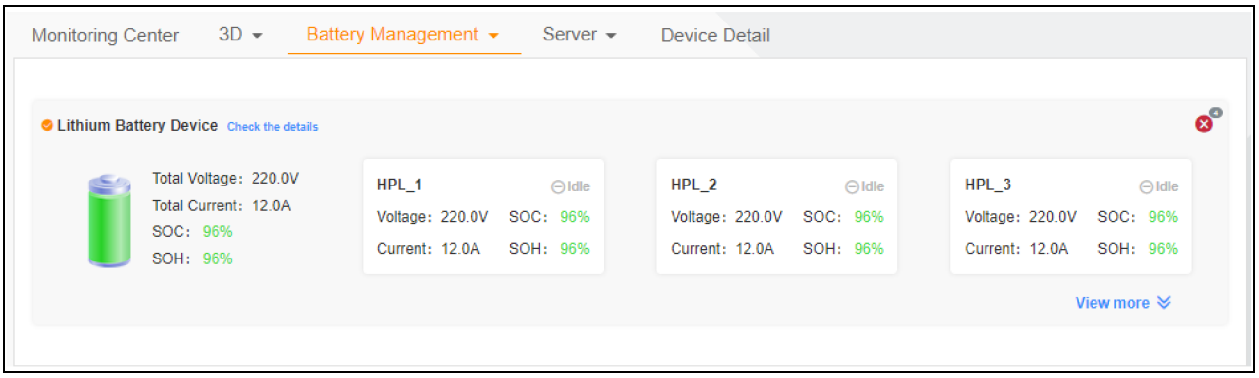


3.2.7 Site: Monitoring Battery Devices

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.

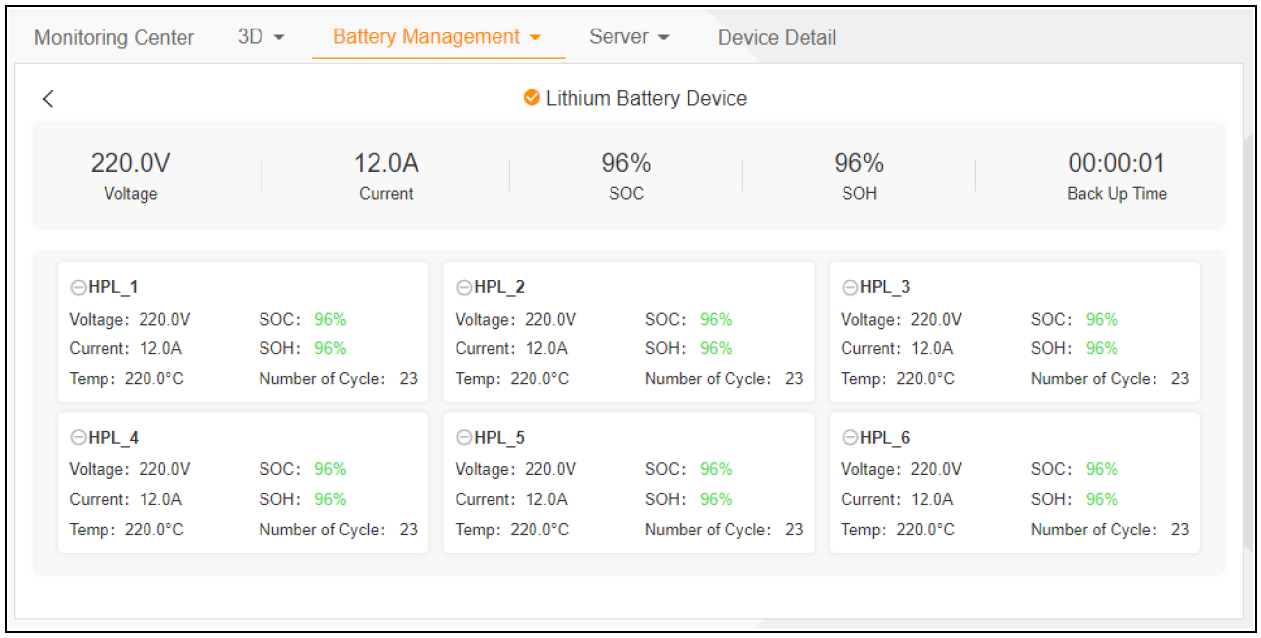
Figure 3.46 Battery Device Overview



© 2026 Vertiv Group Corp. All Rights Reserved.

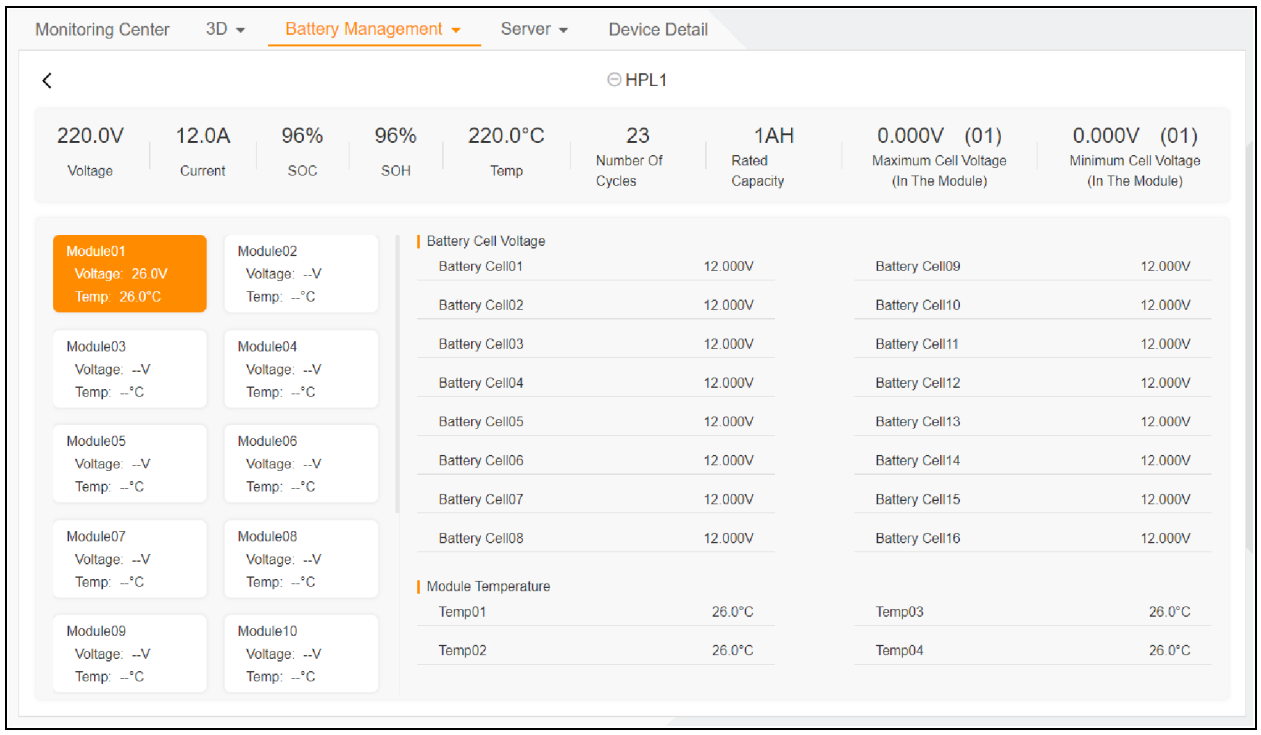
The overview page displays information about the lithium battery systems connected to the current site as shown in **Figure 3.47** below , This includes total voltage, current, state of charge (SOC), state of health (SOH), and alarm counts for each severity level. The page also provides a summary of 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 one of the *lithium battery cabinets* to view the lithium battery cabinet details pag, as shown in **Figure 3.48** below .

Figure 3.48 Lithium Battery Cabinets Details



© 2026 Vertiv Group Corp. All Rights Reserved.

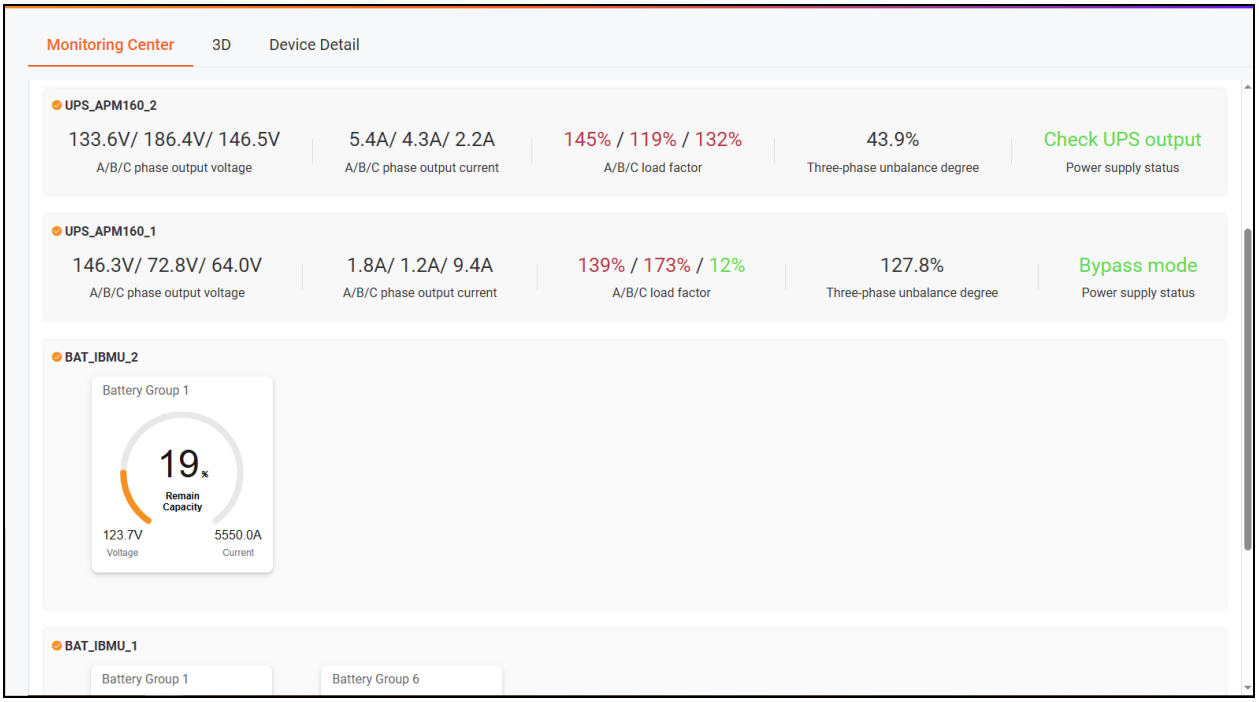
On the details page of the lithium battery cabinet, the summary information of the current lithium battery cabinet is displayed at the top, and the different battery modules in the battery cabinet are displayed on the left.

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 .

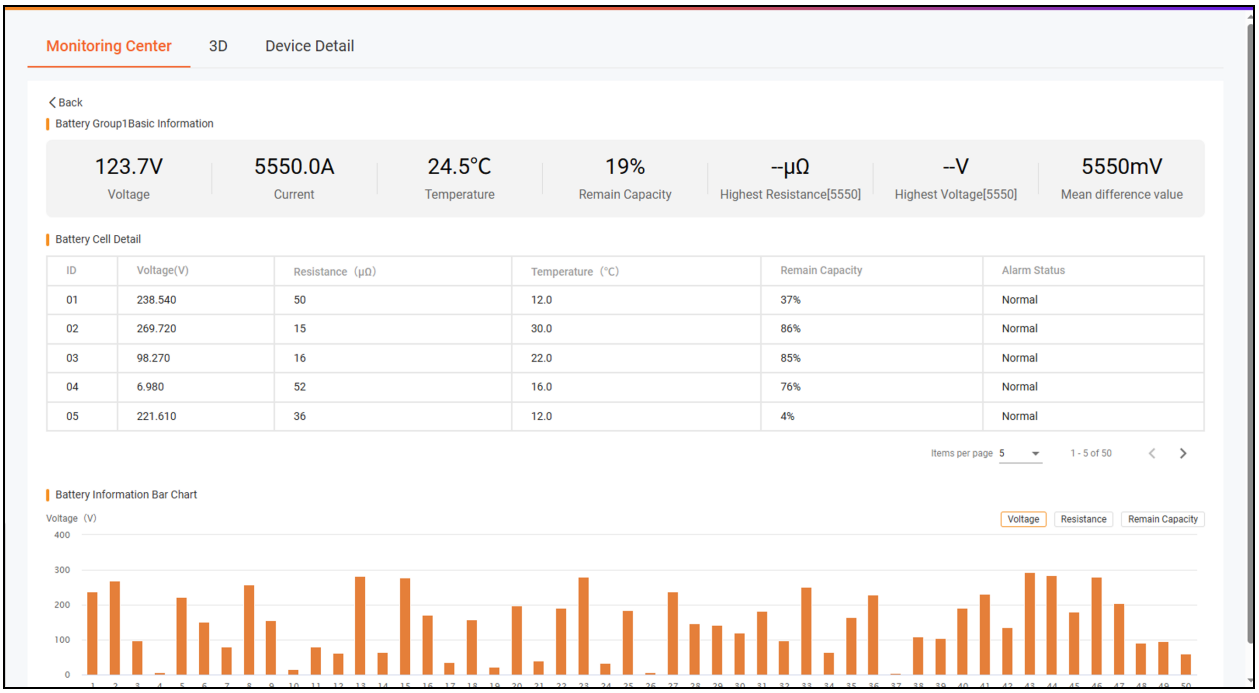
Figure 3.49 Battery Room Monitoring Home Page



Click *Device Detail* to view the detailed signal values, as shown in Figure 3.50 on the facing page .

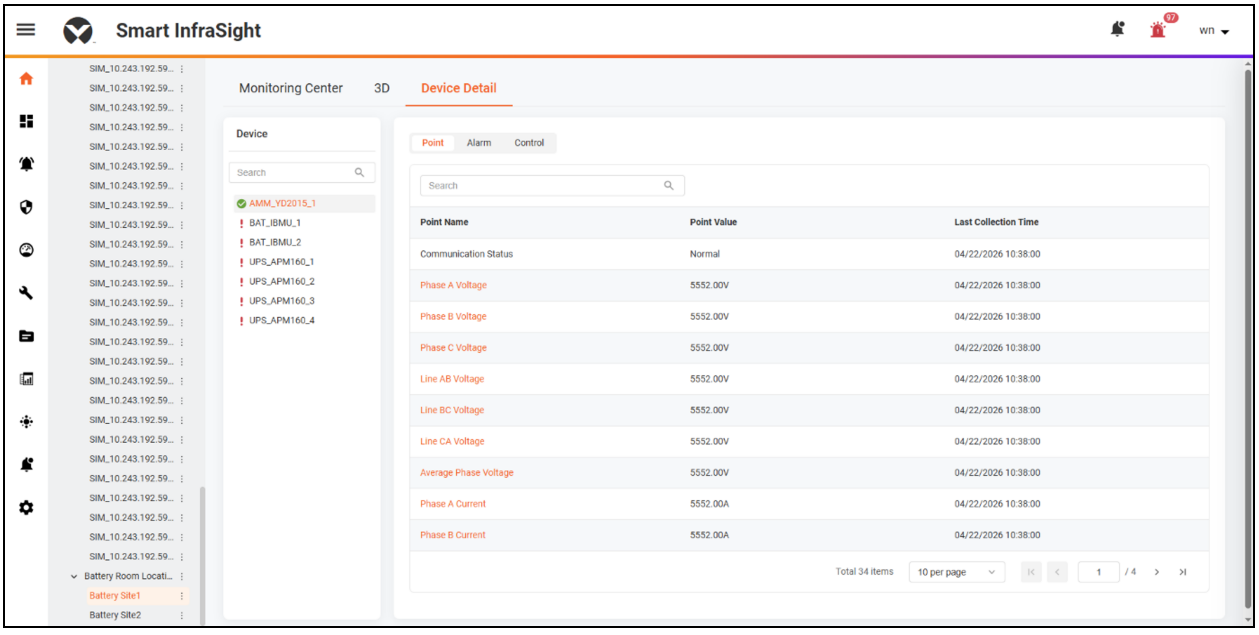
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 3.50 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, and you can click on the IBMU card to view the IBMU details, as shown in Figure 3.51 below .

Figure 3.51 IBMU Device Details



© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

4 3D Configuration

4.1 General

4.1.1 Overview

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

4.1.2 Functional Modules

- Enter the Site/Location 3D Configuration
- Dragging and Dropping the Device to Canvas
- Editing or Adding the Devices
- Preview and Save 3D Configuration
- Configuring the Rack
- Configure the Power Distribution Cabinet
- 3D Configuration of the Battery Room
- Lithium Battery 3D Configuration
- Lead-Acid Battery 3D Configuration
- Configure the U-level Asset Manager

4.2 Detailed Functions

4.2.1 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 4.1 on the next page and Figure 4.2 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.1 Site 3D Configuration Entrance

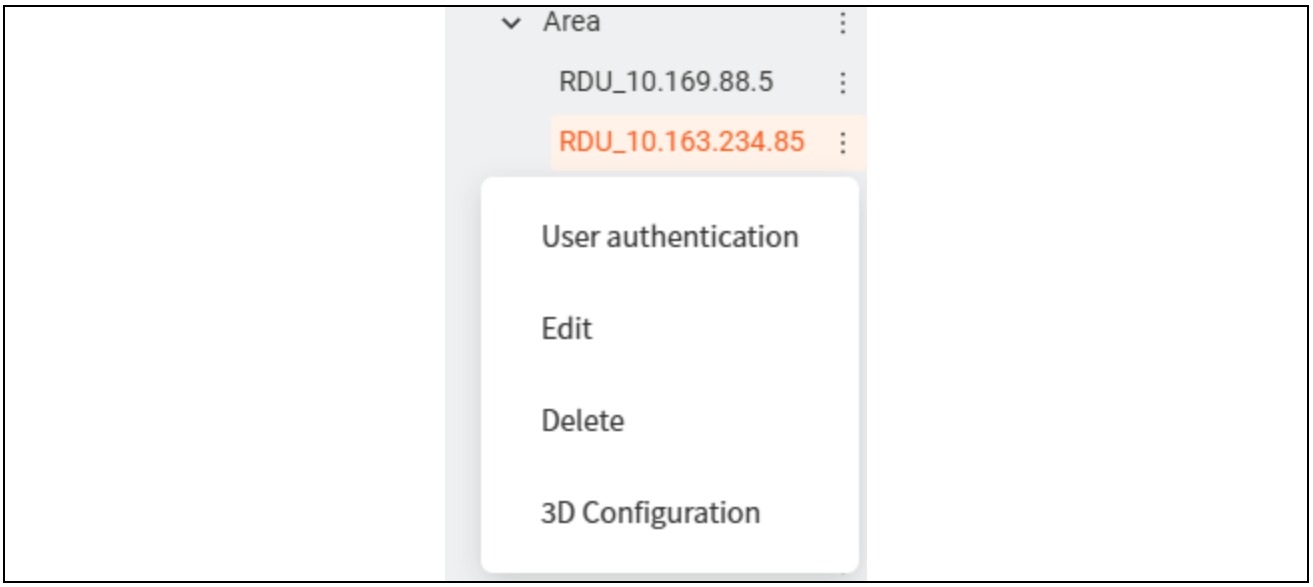
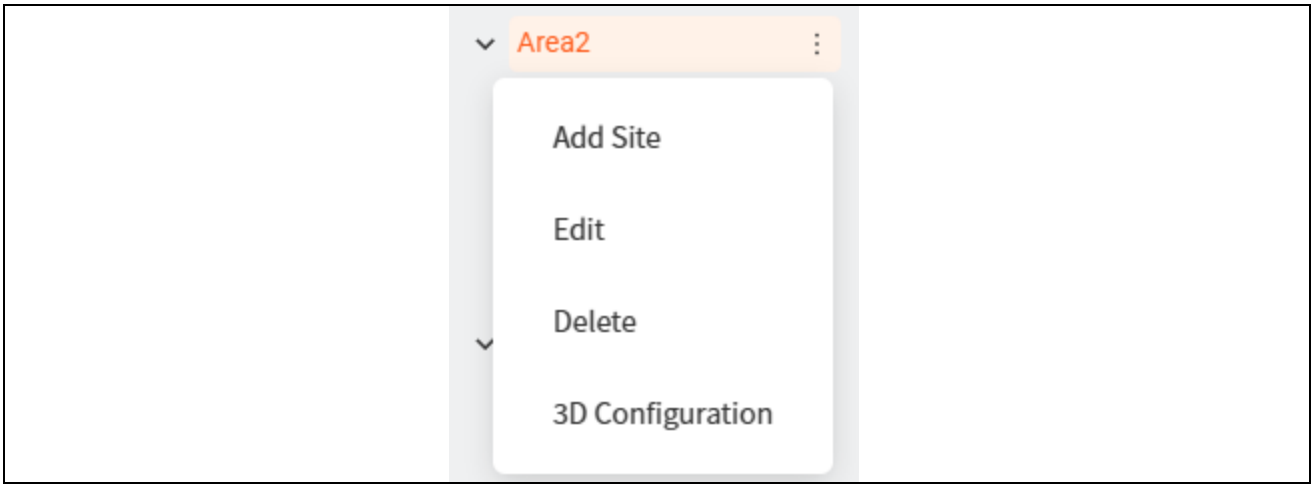


Figure 4.2 Location 3D Configuration Entrance

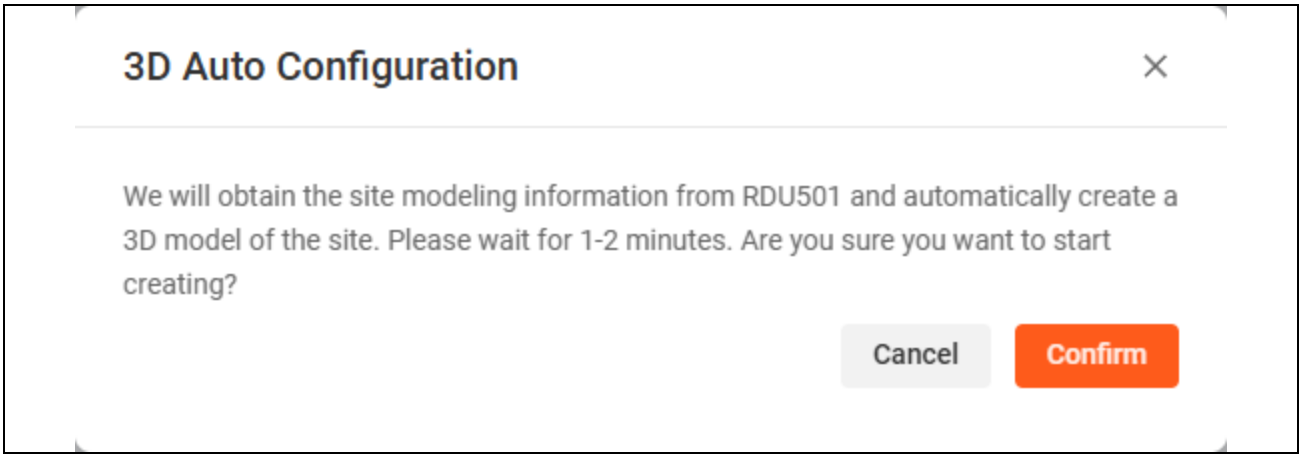


© 2026 Vertiv Group Corp. All Rights Reserved.

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 151. 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 4.3 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 58.

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:

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

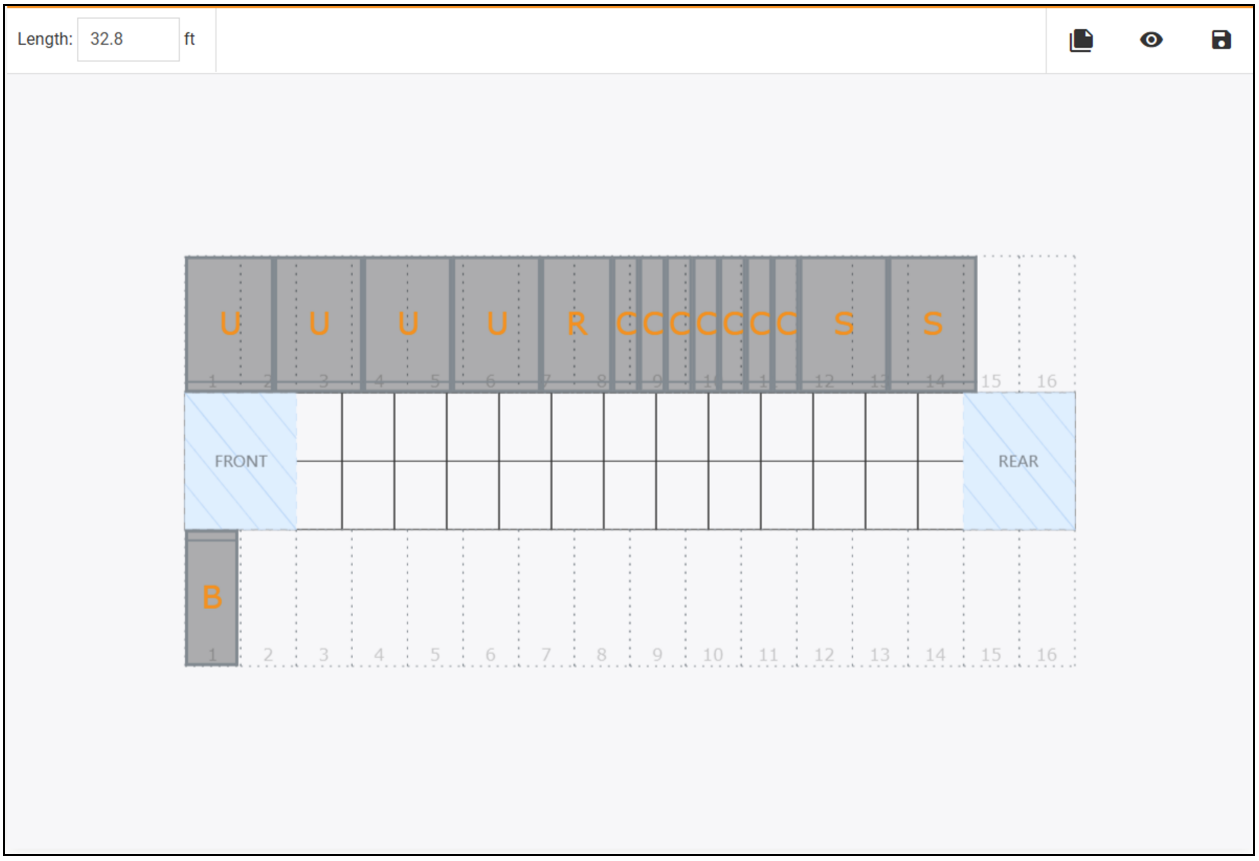
© 2026 Vertiv Group Corp. All Rights Reserved.

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

4.2.2 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 4.4 below .

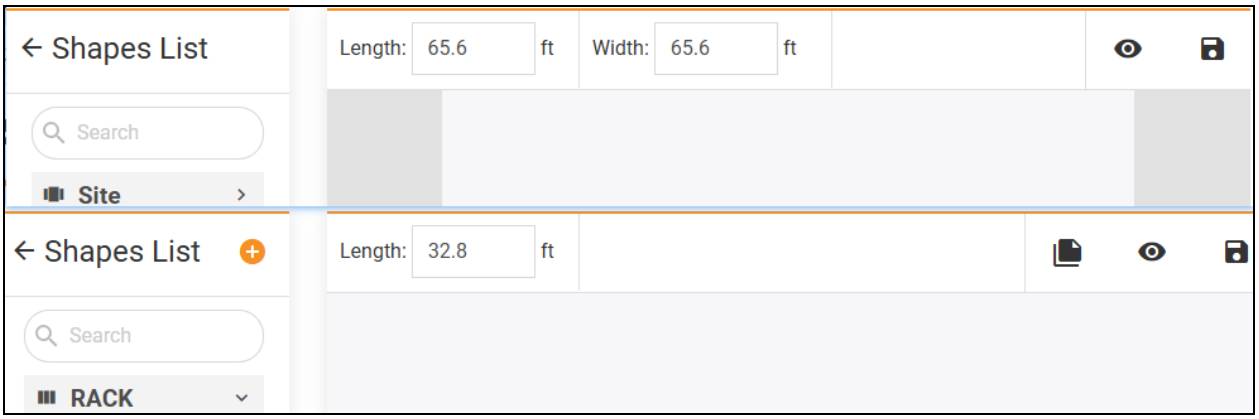
Figure 4.4 Drag and Drop the Device to the Canvas



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 4.4 above .

© 2026 Vertiv Group Corp. All Rights Reserved.

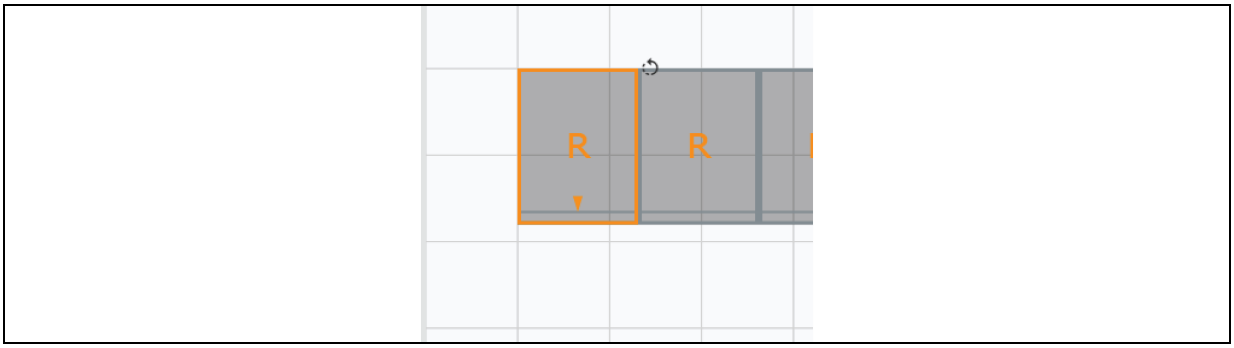
Figure 4.5 Modify the Size of the Canvas for a Location/Site



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 4.6 below .

Figure 4.6 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 4.7 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.7 Rotation Device in SmartAisle2

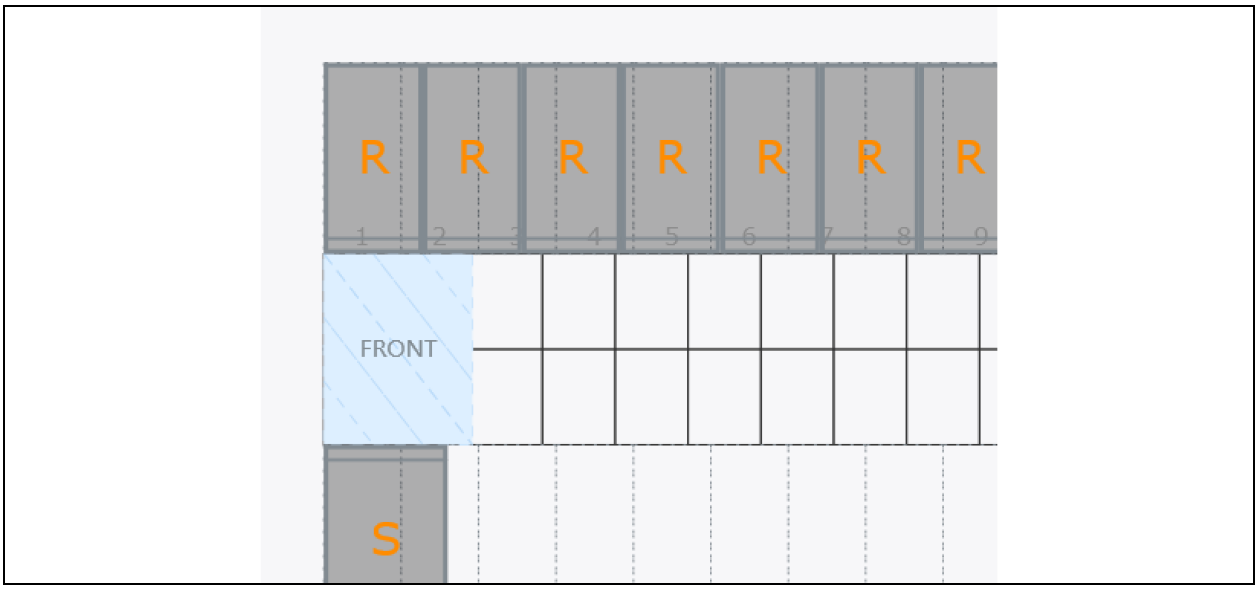
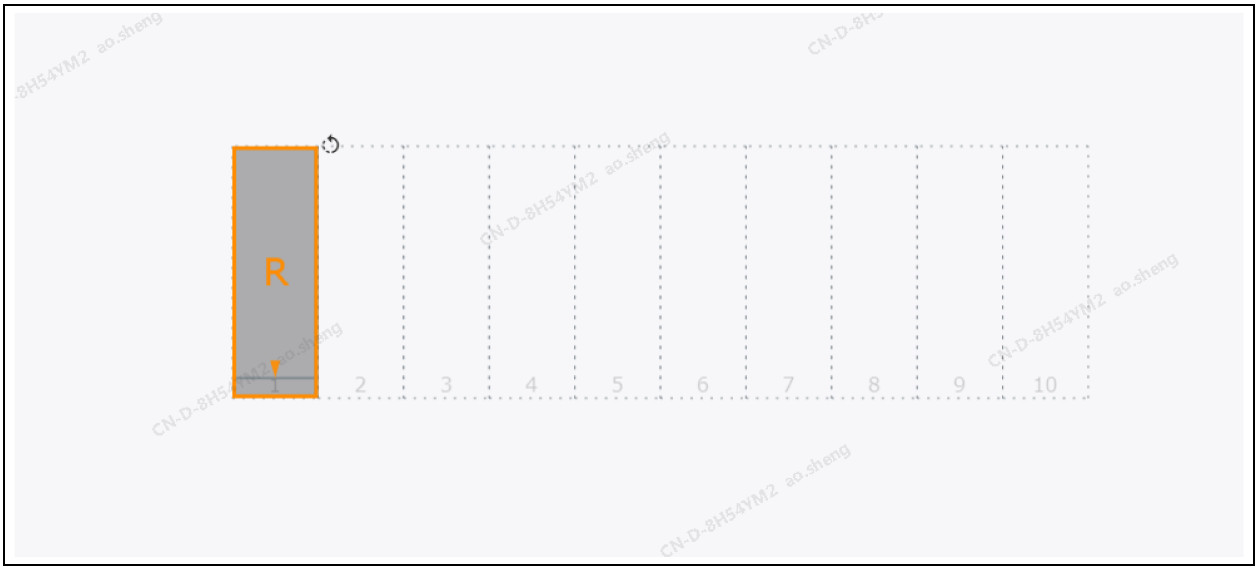


Figure 4.8 Rotation Device in the SmartRow 2 site



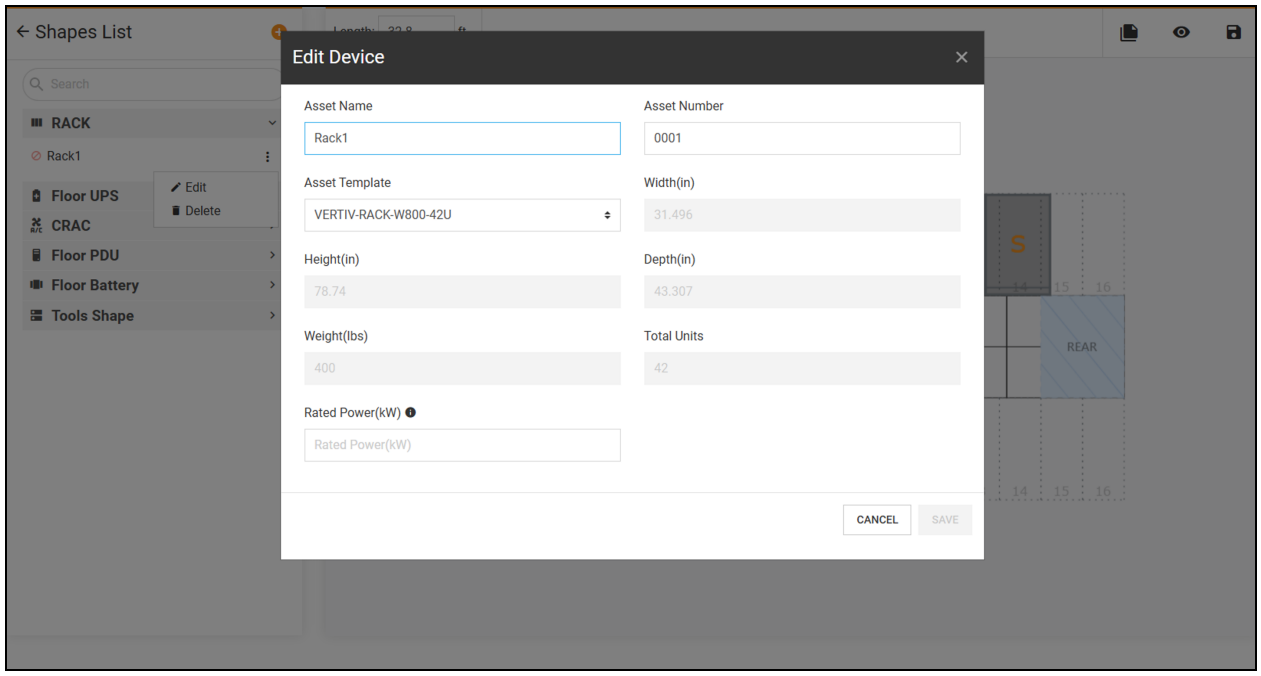
4.2.3 Editing or Adding the Devices

Editing the Device

After entering the 3D configuration page of the site, users can click the ellipses (⋮) on 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 4.9 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.9 Edit Device



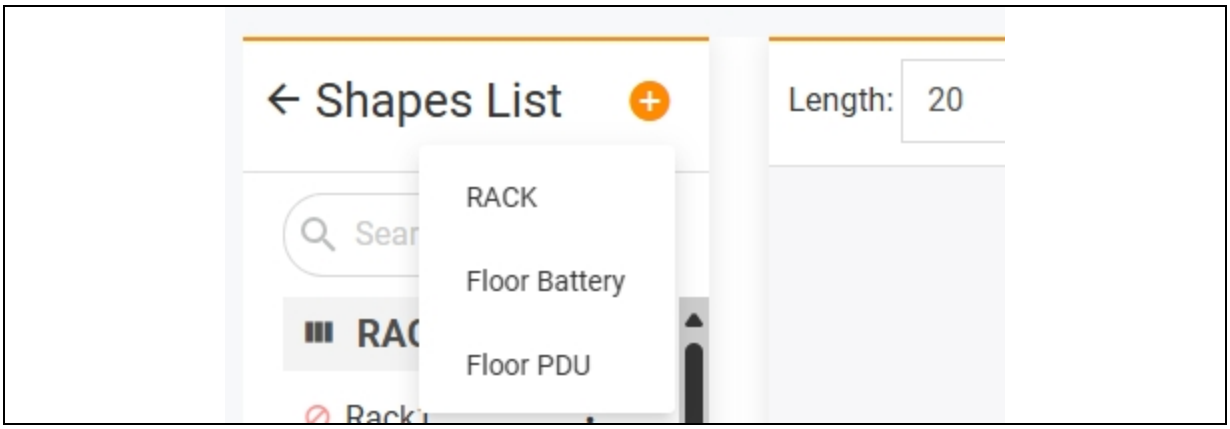
© 2026 Vertiv Group Corp. All Rights Reserved.

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 4.10 Add Device in 3D Configuration



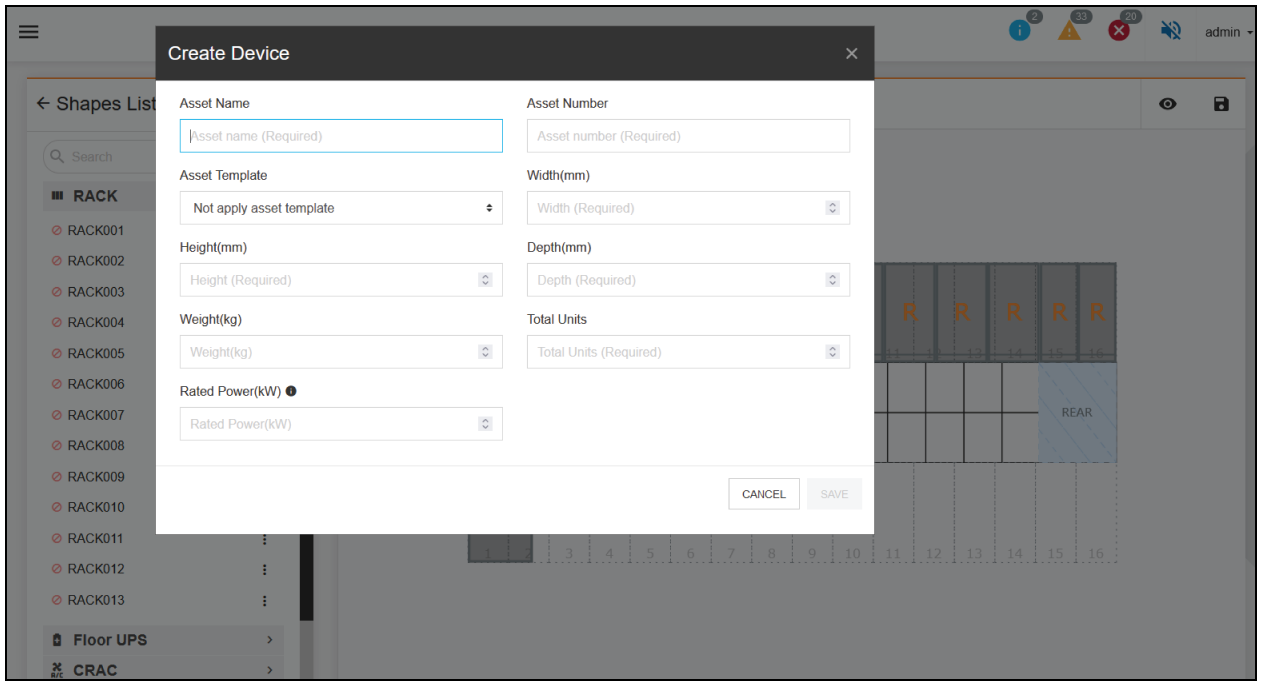
1. Adding Rack and Floor Battery

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 73 and Lead-Acid Battery 3D Configuration on page 74.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.11 Add Device Popup Window

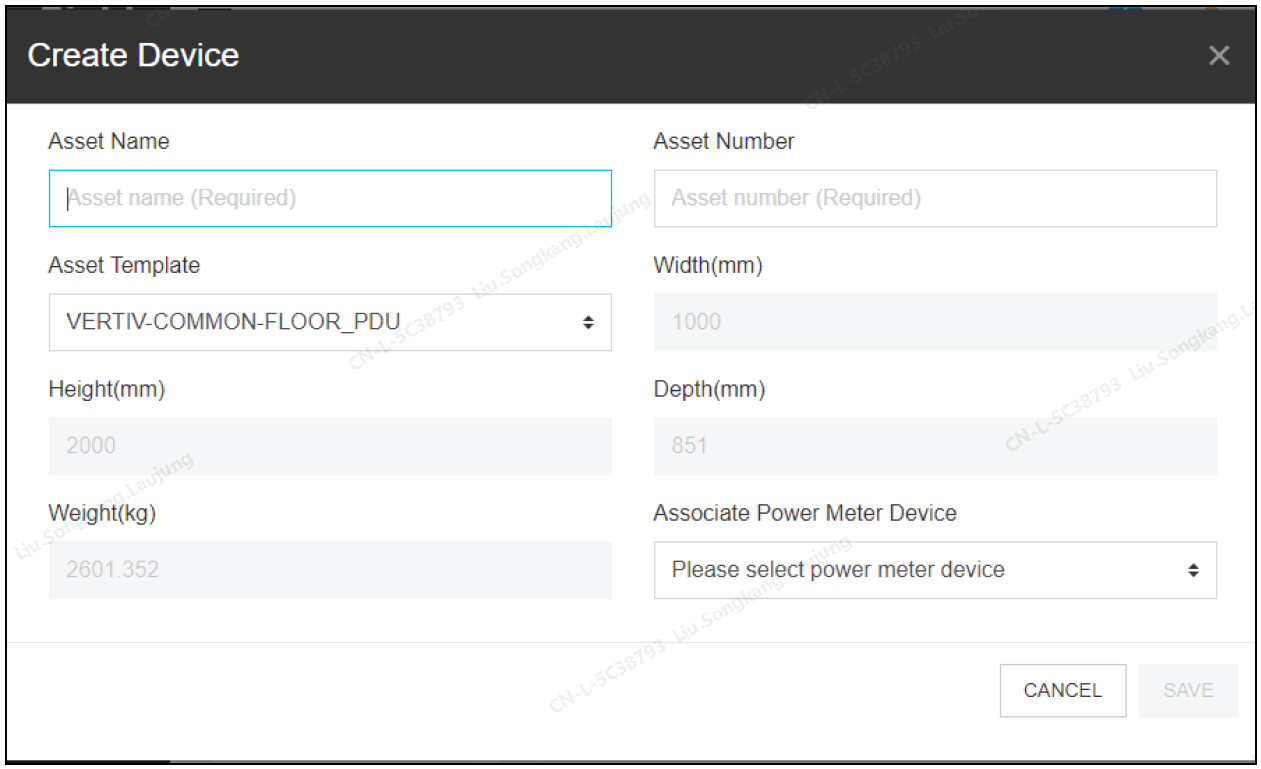


2. Adding a Floor PDU

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.12 Adding a Floor PDU

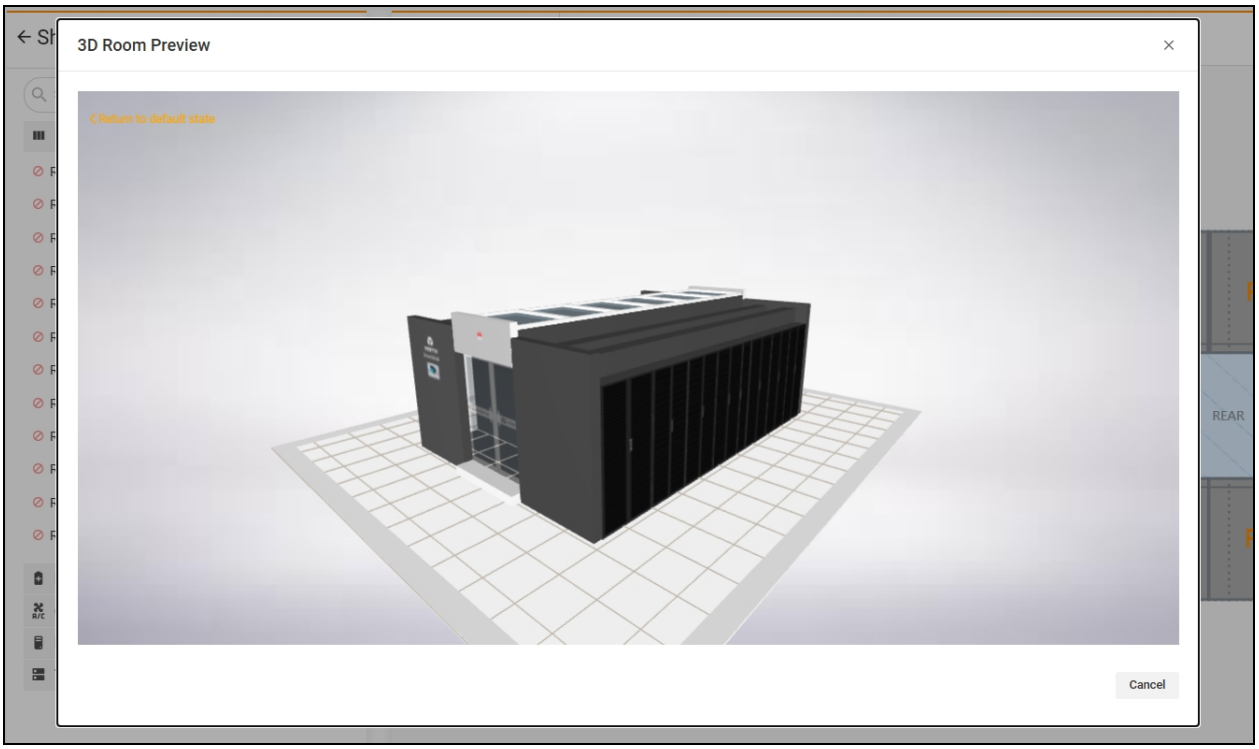


4.2.4 Preview or Save 3D Configuration

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. As shown in Figure 4.13 on the facing page .

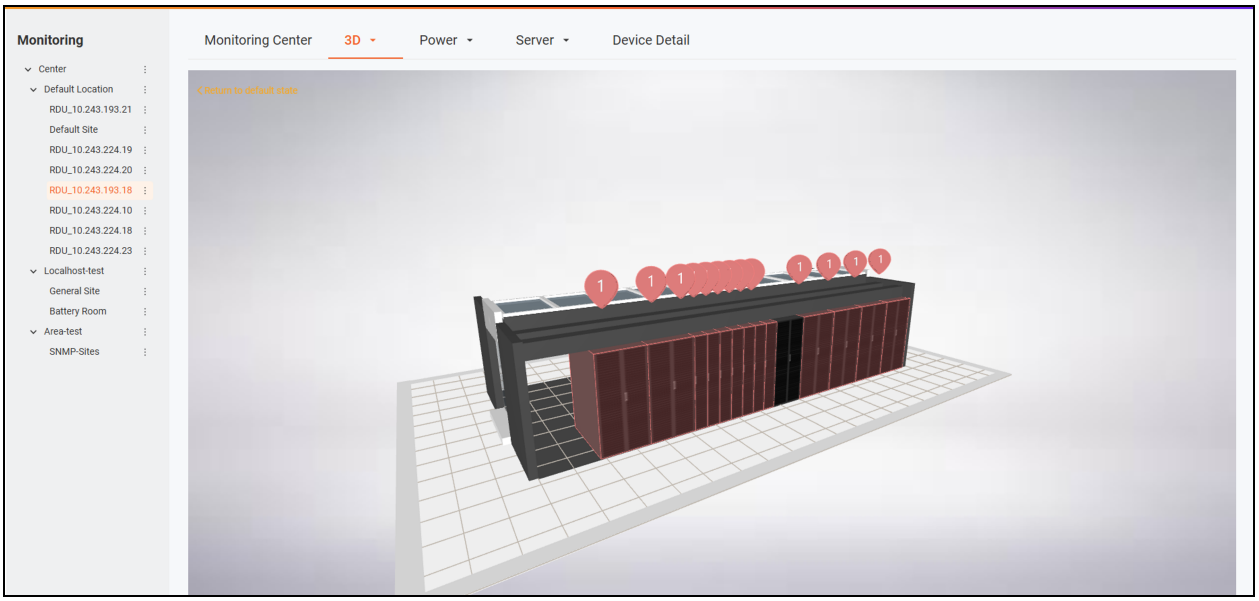
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.13 Preview of 3D View



Once you have verified that all the information is correct, click the *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 4.14** below .

Figure 4.14 3D Room Monitoring

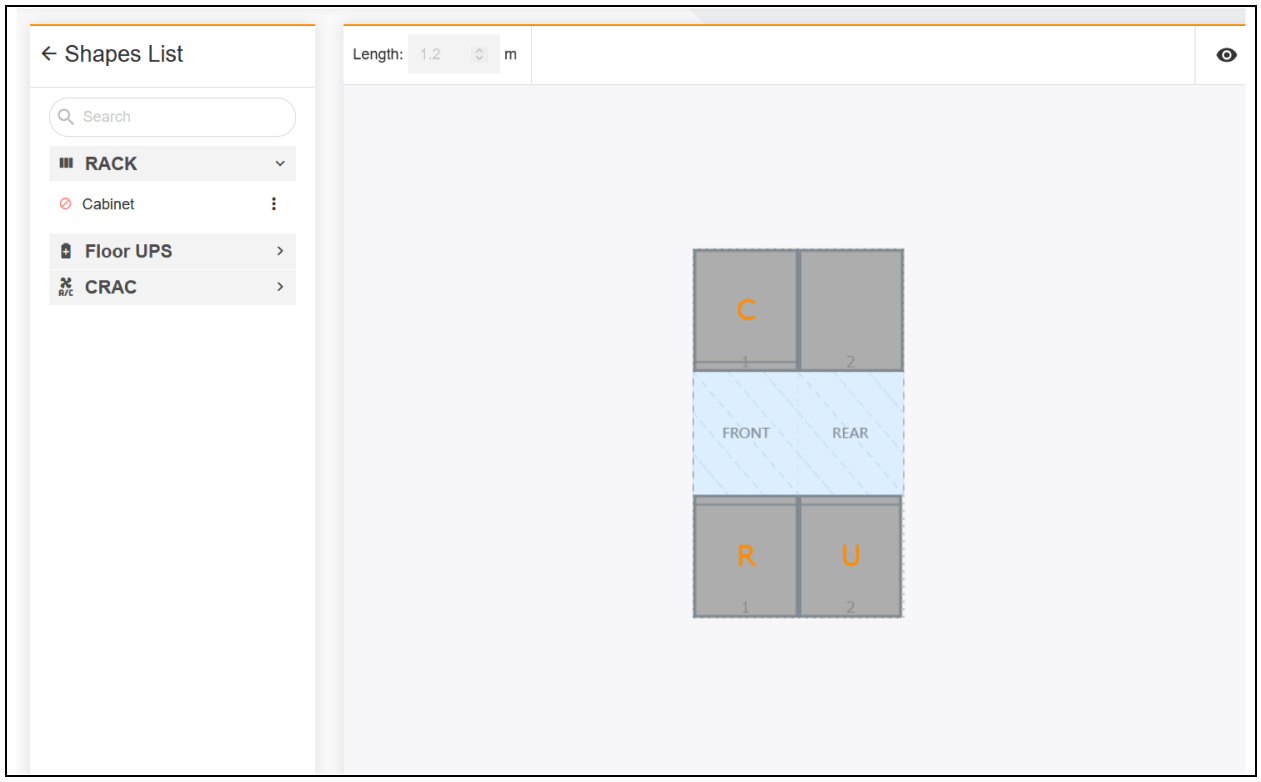


© 2026 Vertiv Group Corp. All Rights Reserved.

4.2.5 Configuring the Rack

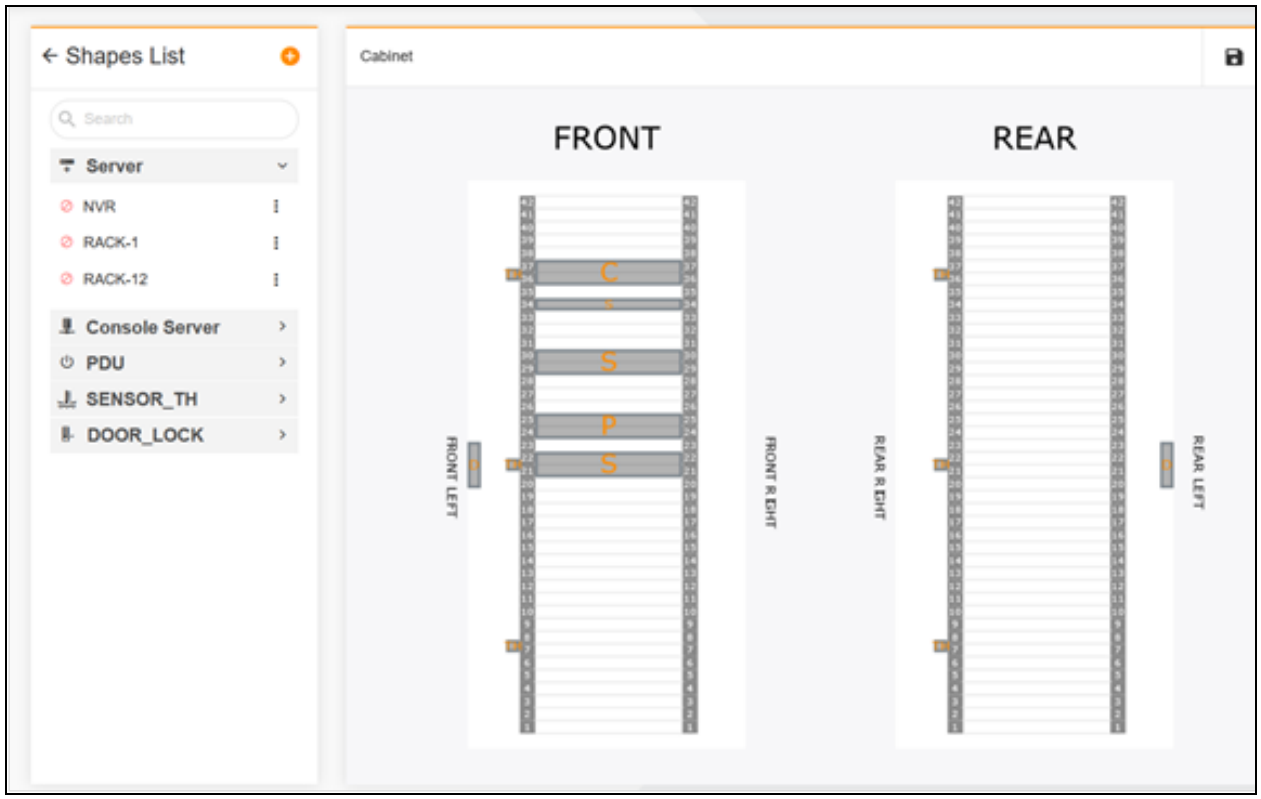
After entering the 3D configuration page of the site, you can double-click any rack on the graph to enter the 3D configuration of the current rack. As shown in Figure 4.15 below .

Figure 4.15 3D Configuration of the Smart Aisle 3 Site



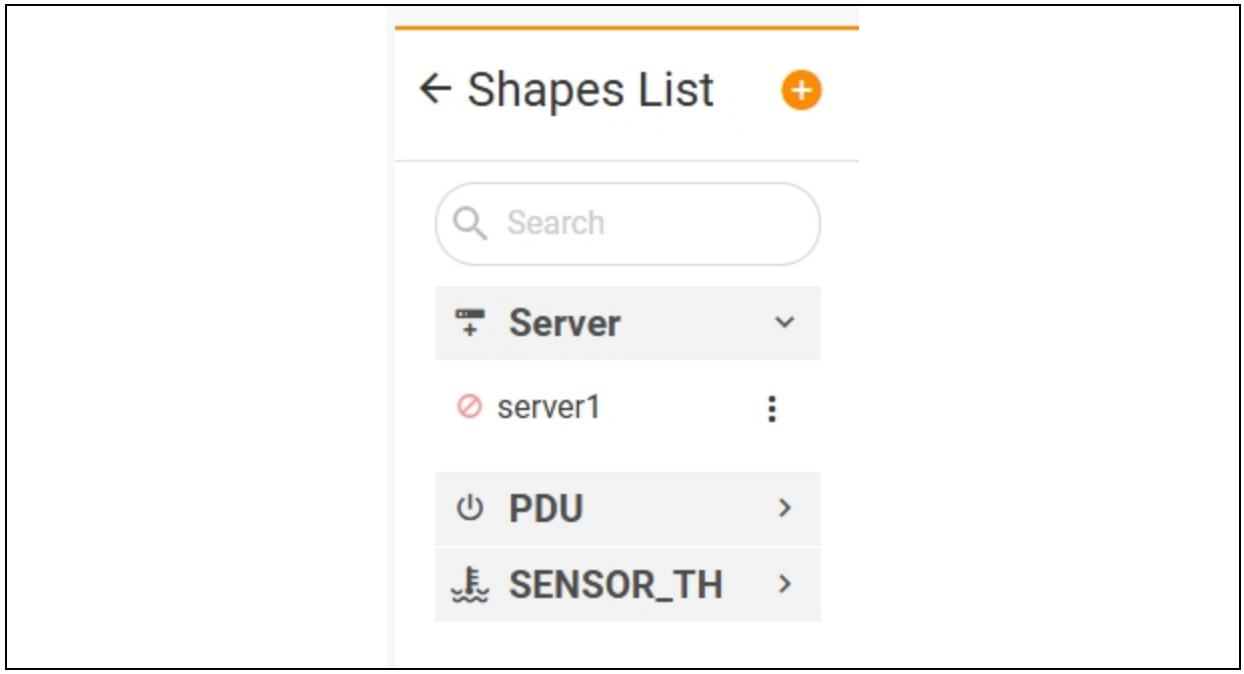
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.16 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 4.17** below .

Figure 4.17 Shapes List of Rack



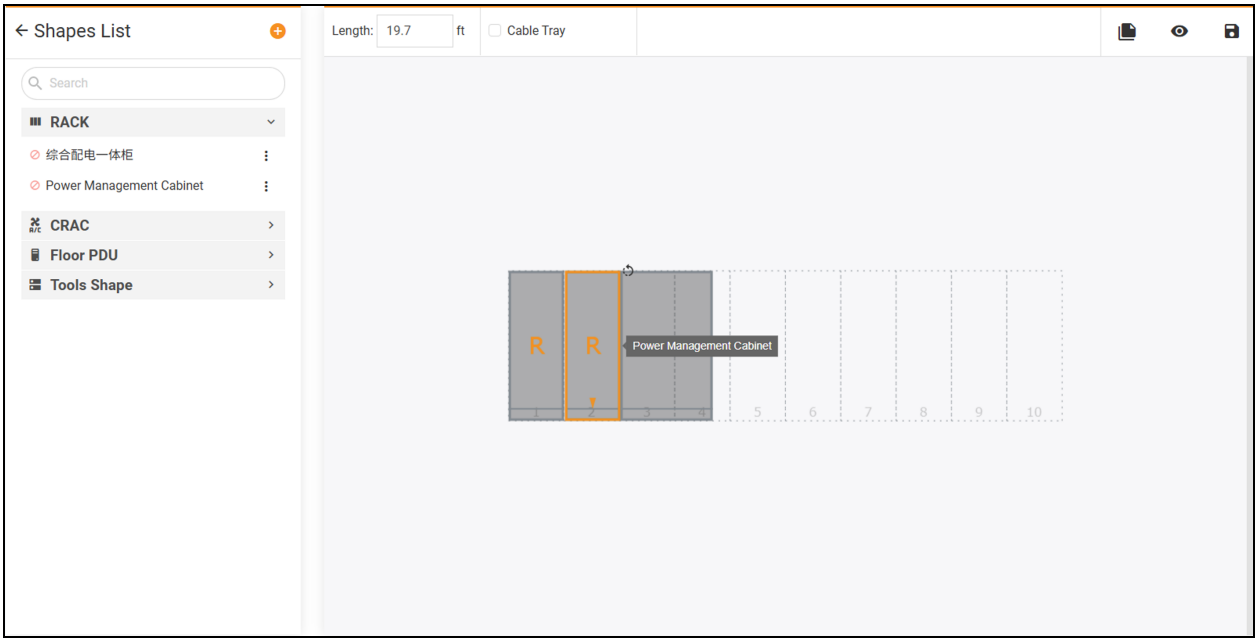
© 2026 Vertiv Group Corp. All Rights Reserved.

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 4.18 below .

Figure 4.18 3D Configuration of the SmartRow2 Site



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.19 PMC Cabinet 3D Configuration

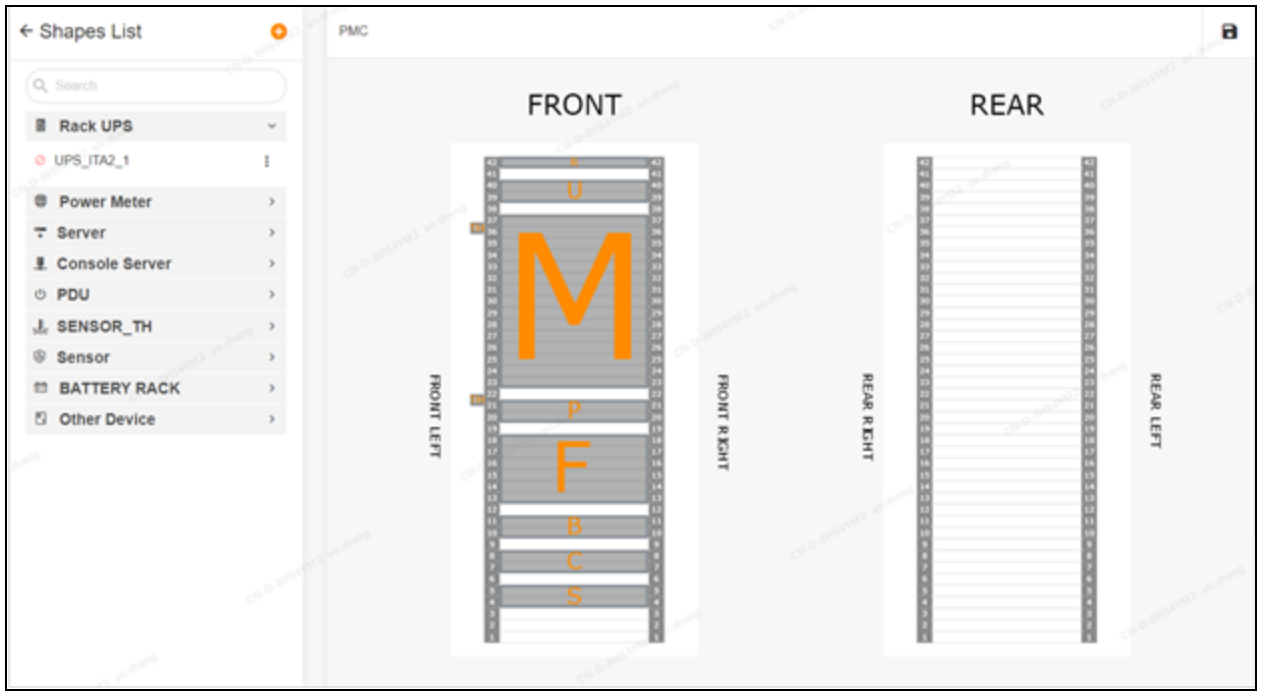
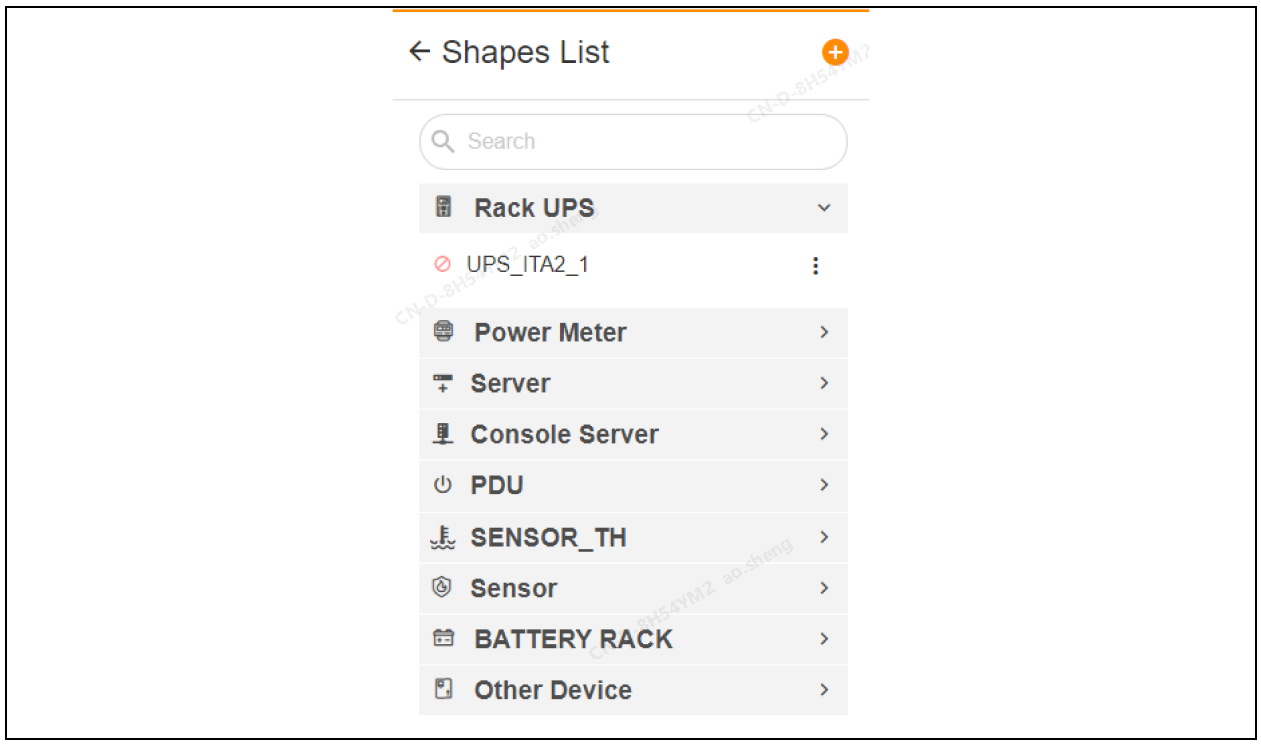


Figure 4.20 Shapes List of PMC Cabinets



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

© 2026 Vertiv Group Corp. All Rights Reserved.

- **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.
- **Power 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.
- **Temperature and humidity sensor**: 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.

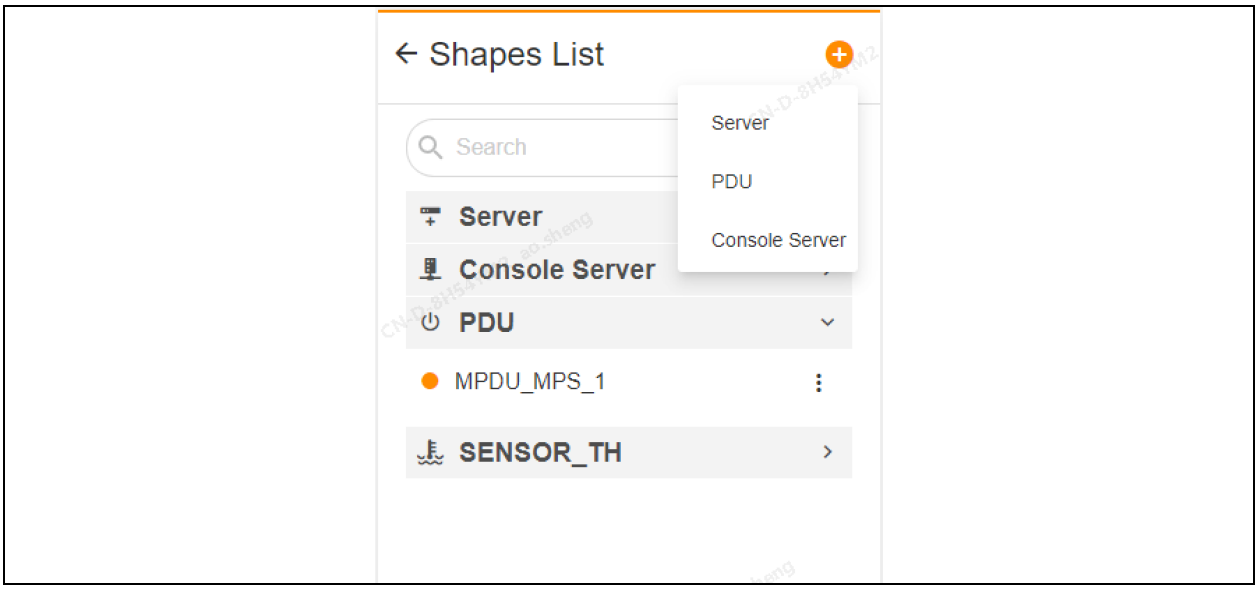
To remove a device from the canvas of 3D configuration, select it and press the Delete key on keyboard.

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 4.21** on the facing page .

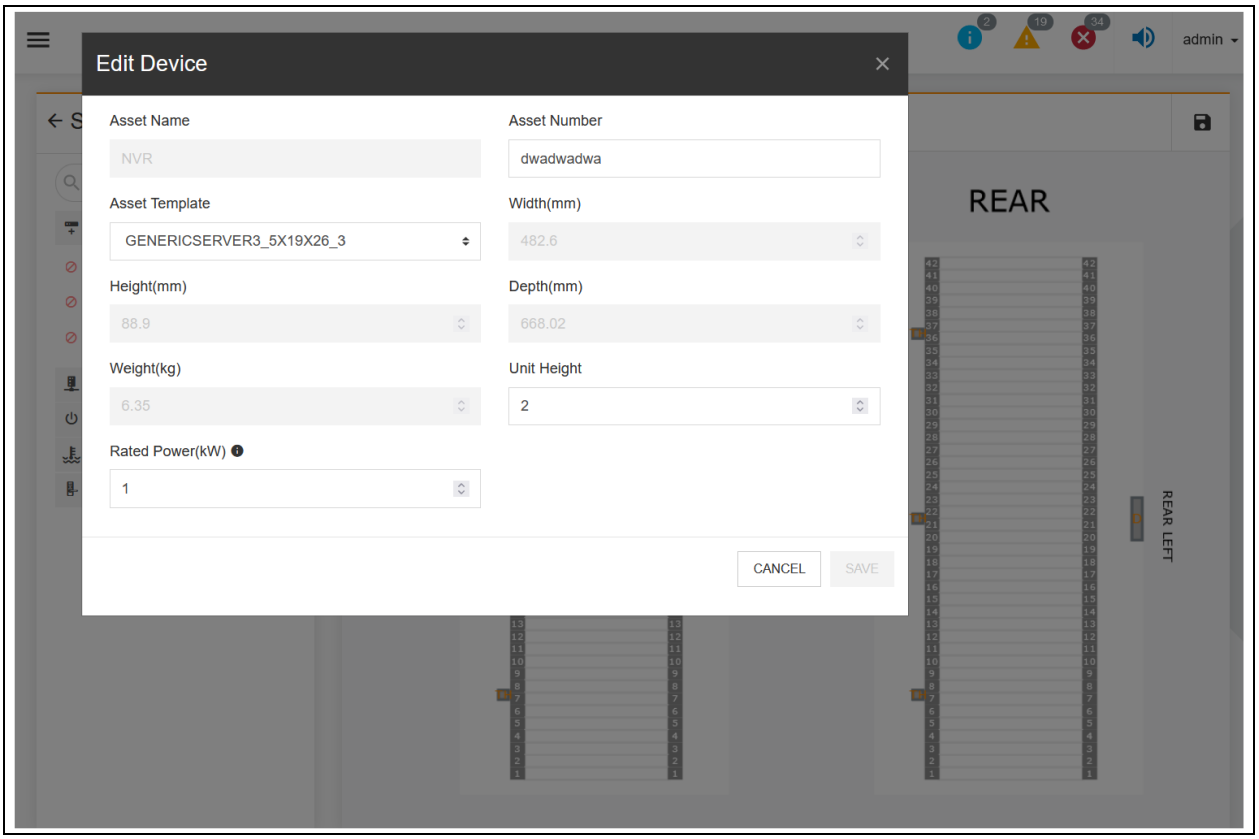
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.21 3D Configuration of a Common Cabinet—Adding Devices



After adding the server device, the user can edit the device information. As shown in Figure 4.22 below .

Figure 4.22 The Server Configuration window



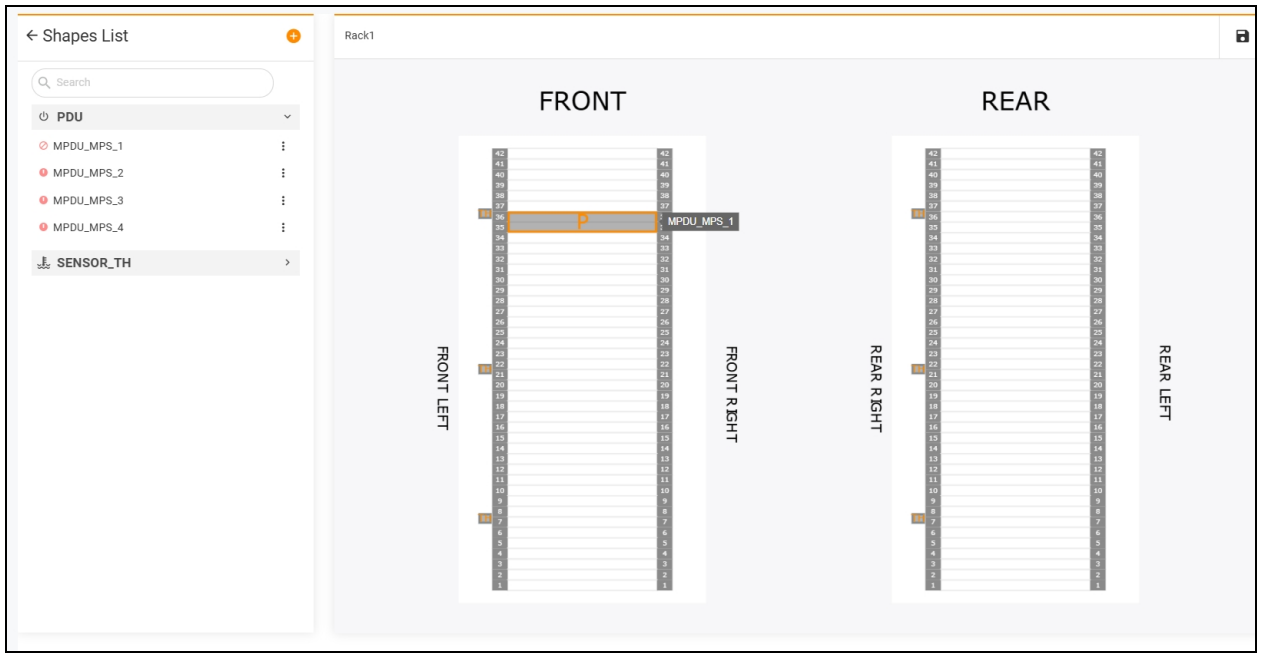
The information that can be changed for the server device includes:

© 2026 Vertiv Group Corp. All Rights Reserved.

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 152 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 4.23** below .

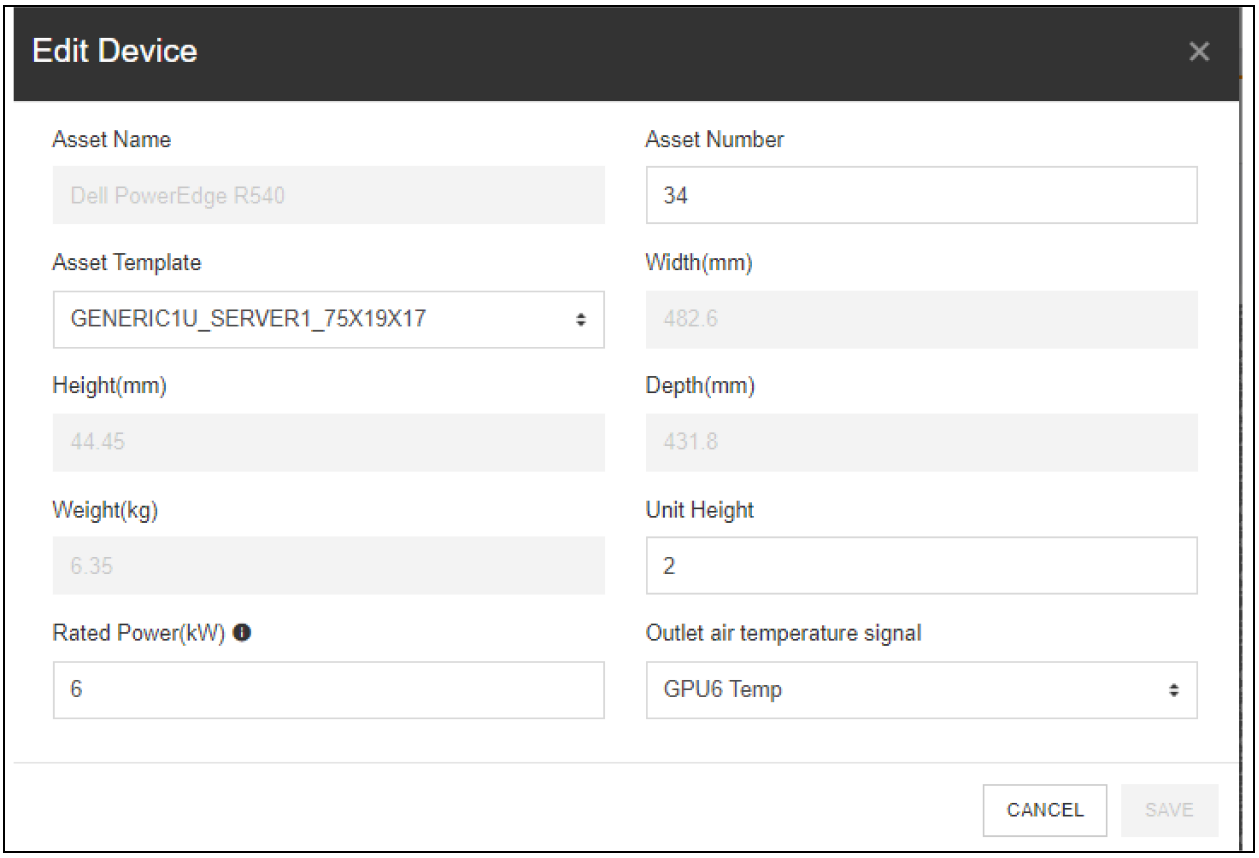
Figure 4.23 3D Configuration—Dragging the Device



After adding a PDU device, you can edit the PDU device information. As shown in **Figure 4.24** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.24 PDU Configuration Window



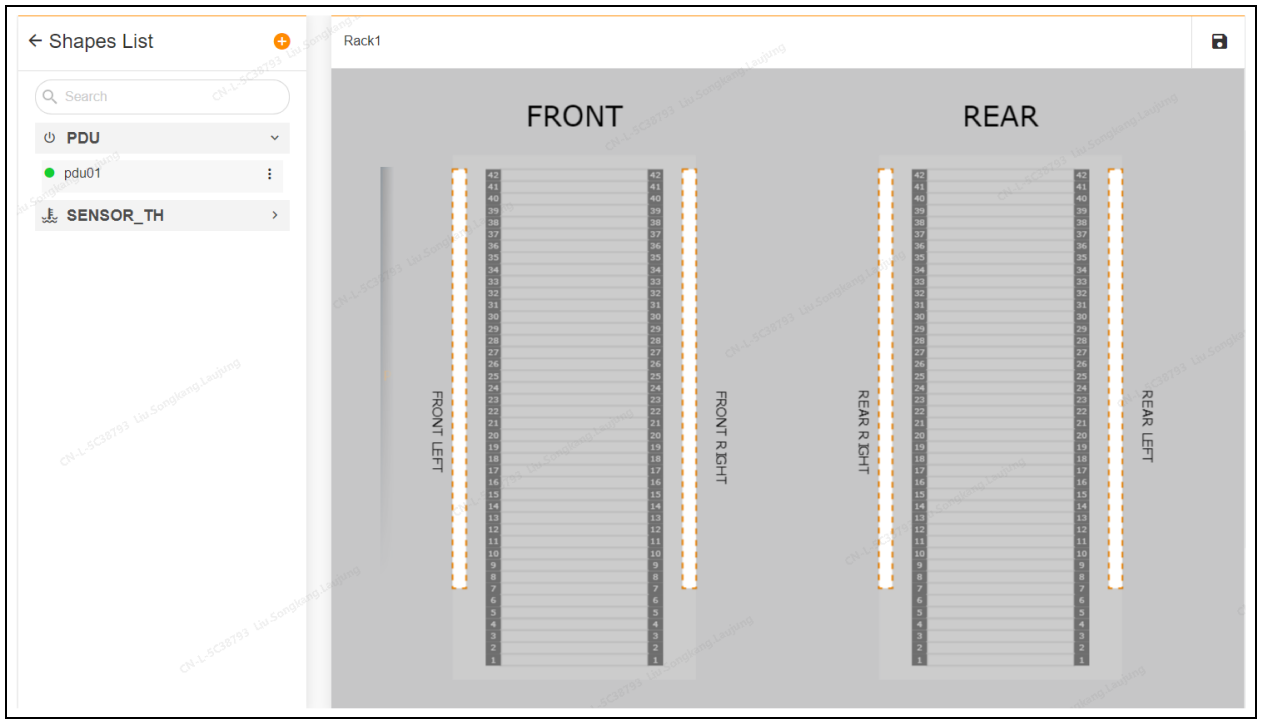
The PDU device information that can be changed includes:

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.25 A ZERO U PDU can be Configured in Four Positions at the Front and Rear Doors

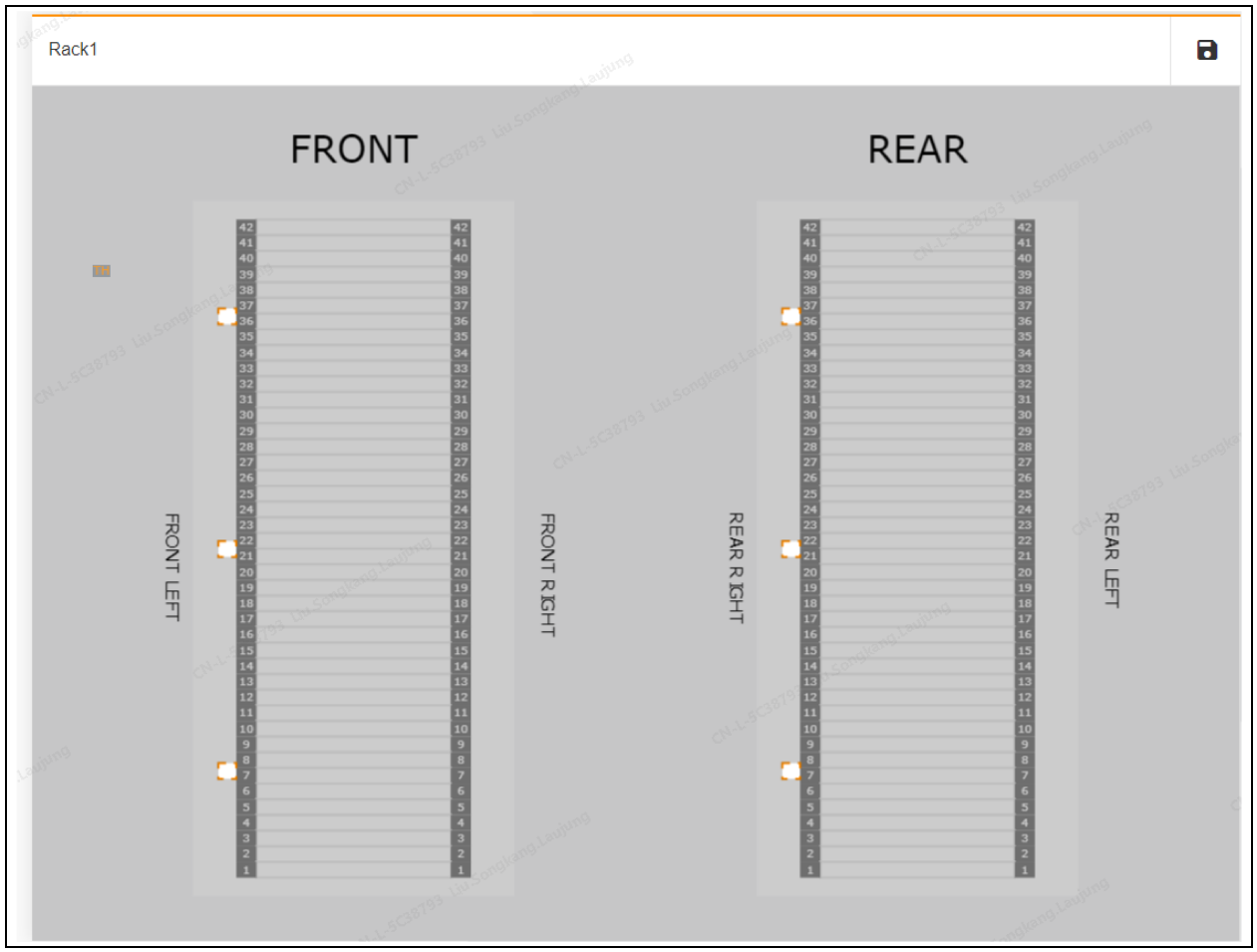


3. U Height: When it is 0, it does not occupy the U position of the cabinet, when it is not 0, dragging the PDU into the cabinet will occupy the U position of the cabinet.

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

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.26 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.

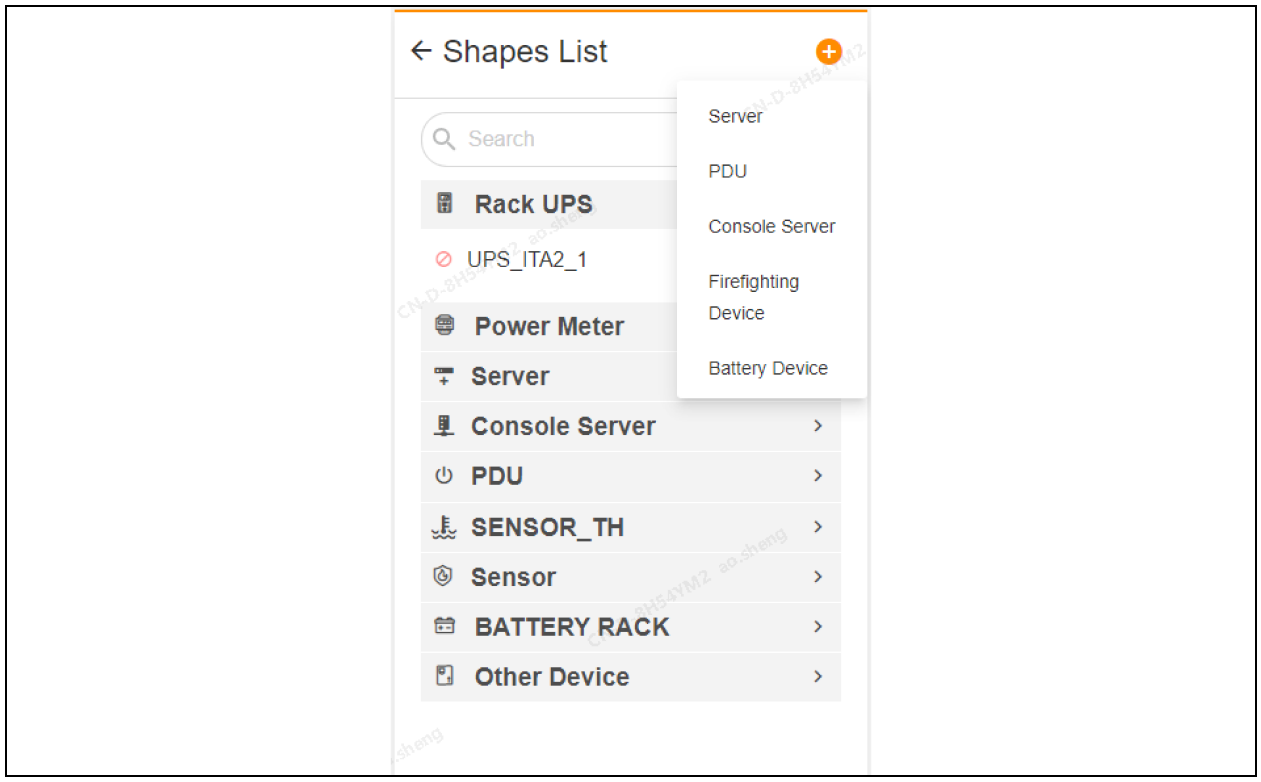
NOTE: Under the SmartAisle3 site, the temperature and humidity sensors, door locks, and other devices in the cabinet cannot be edited, configured, or deleted. Door locks, POD BUST, POD DIDO, POD POWER devices are also not displayed in the shapes list.

PMC Cabinet Configuration

Click *Add* to the shapes list to add servers, PDUs, switches, firefighting equipment, and battery equipment, as shown in **Figure 4.27** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

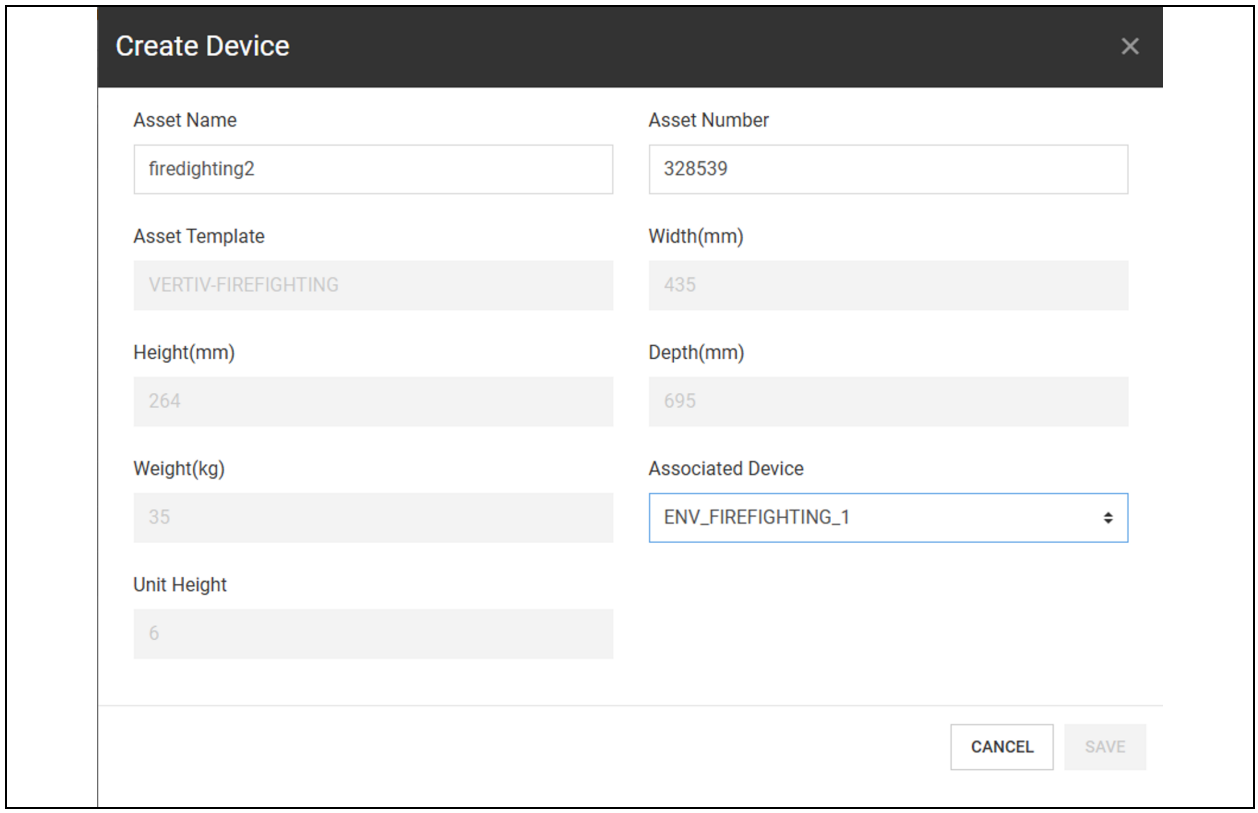
Figure 4.27 PMC Cabinet 3D Configuration—Add Equipment



When adding fire-fighting equipment, you can associate it with the monitorable fire-fighting device as shown in Figure 4.28 on the facing page , and the alarm information of the device can be displayed in the 3D visualization after association.

© 2026 Vertiv Group Corp. All Rights Reserved.

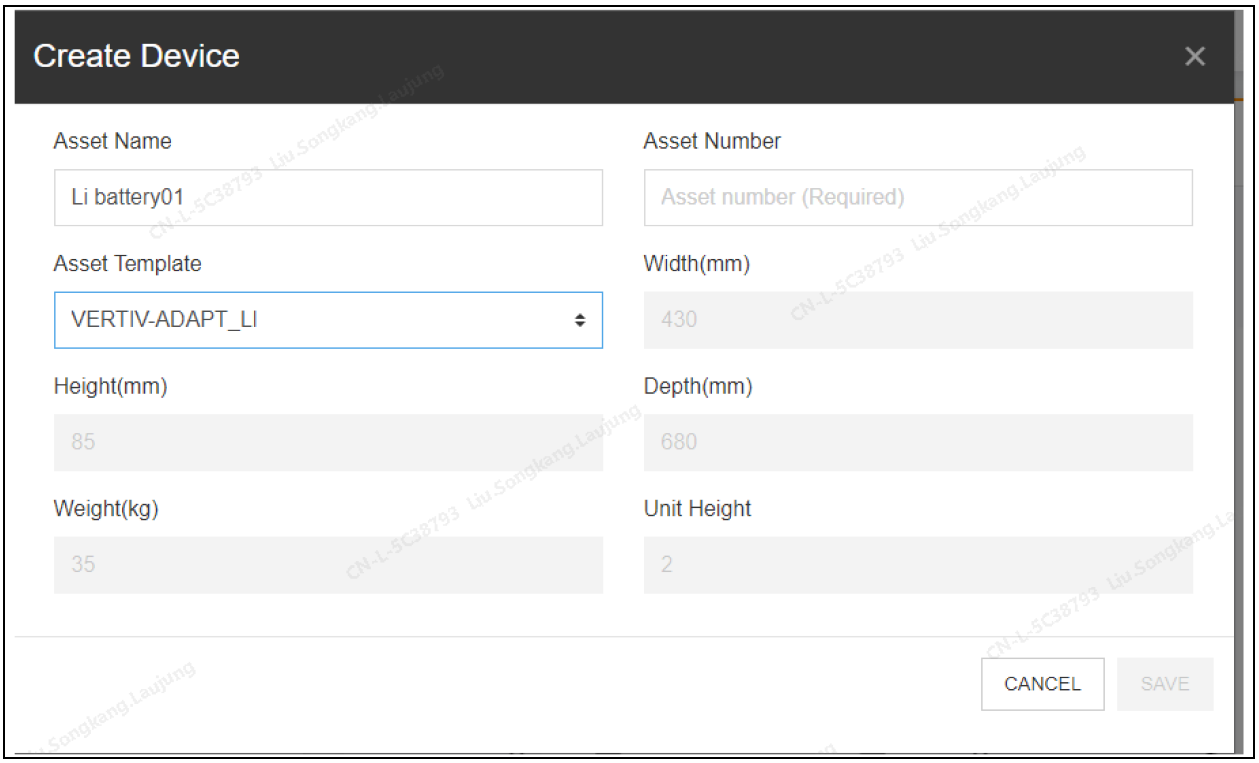
Figure 4.28 Firefighting Equipment Configuration Popup Window



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 4.29 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.29 Adding a Rack-Mounted Battery Device



4.2.6 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:

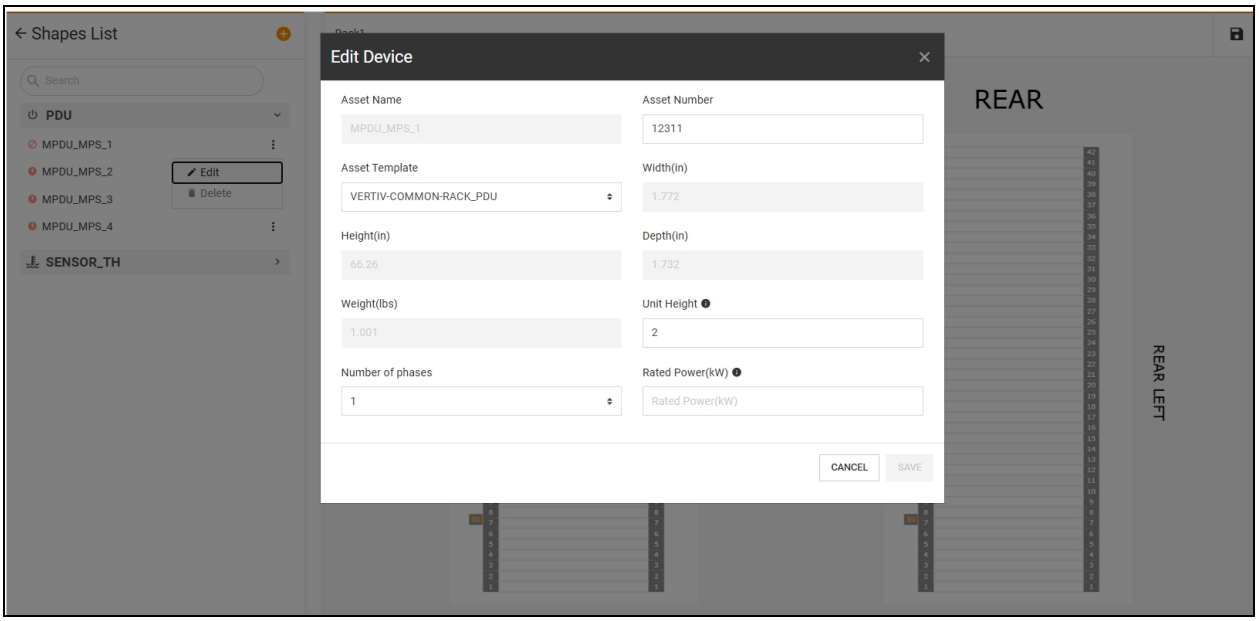
- Incomplete information: Devices with incomplete information cannot be dragged. Users must edit the device's basic information first
- Available for placement: Devices available for placement can be dragged into the current cabinet without additional information.
- Already placed in another cabinet: 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 4.30 on the facing page .

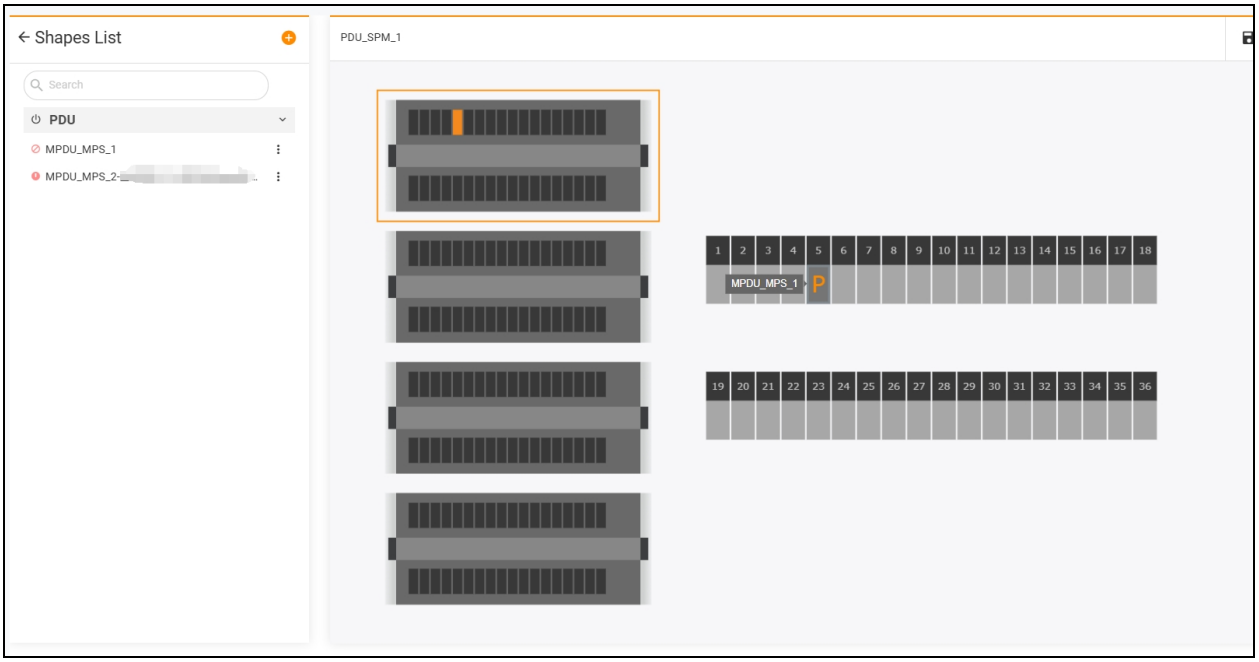
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.30 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 4.31 below .

Figure 4.31 Dragging and Adjusting the Position of the Device in the PDU



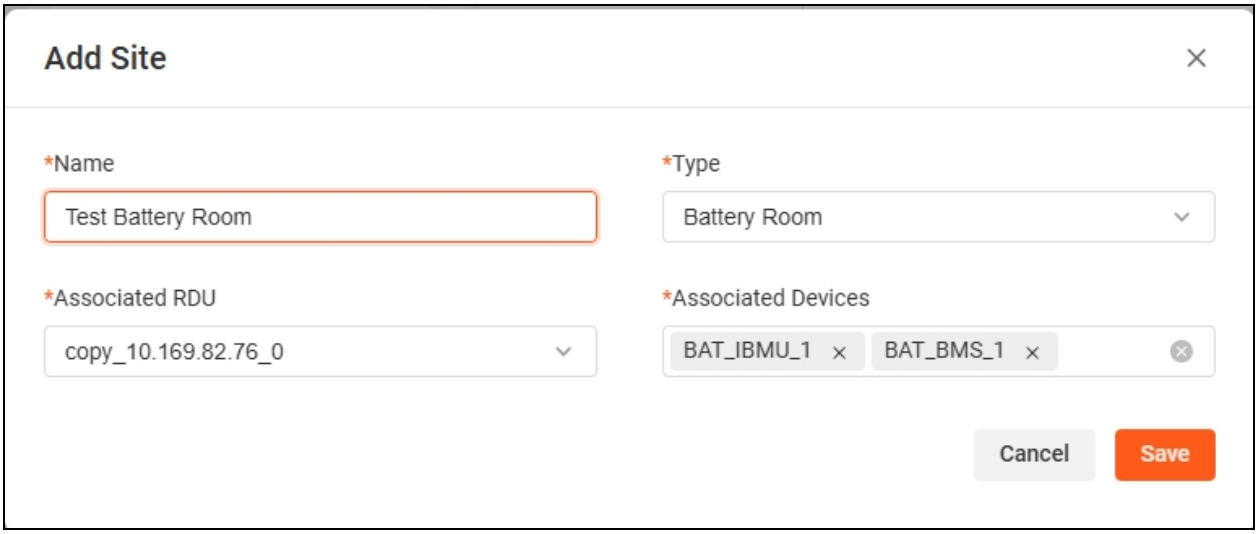
Click the *save* icon to complete Configuration.

© 2026 Vertiv Group Corp. All Rights Reserved.

4.2.7 3D Configuration of the Battery Room

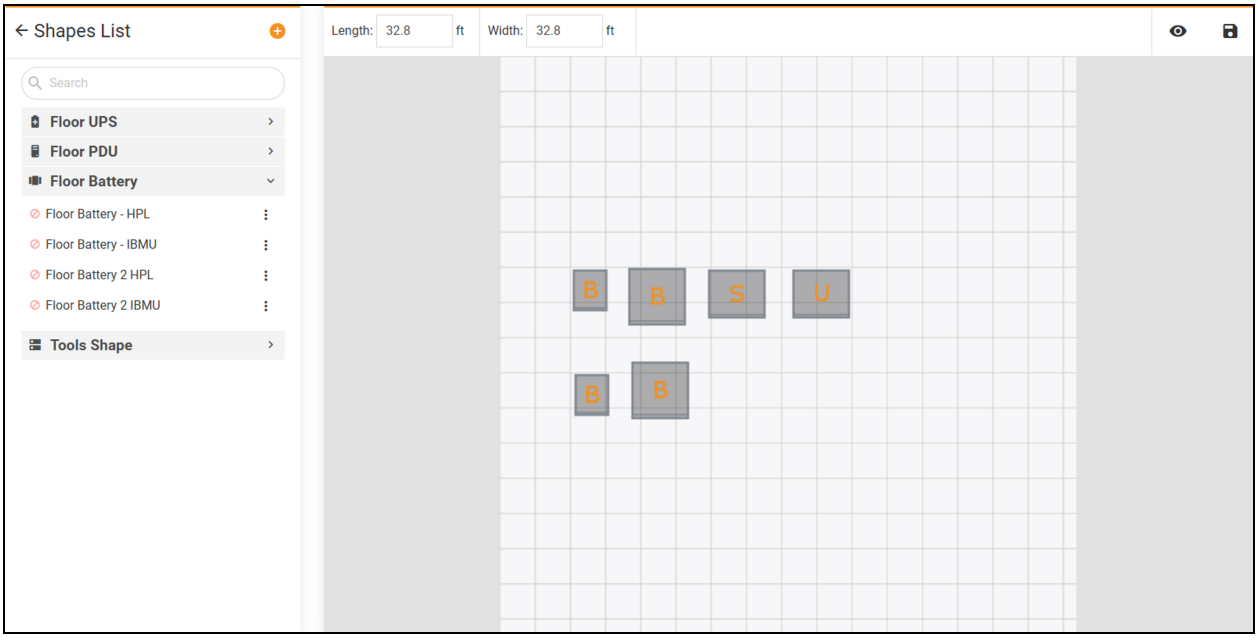
In the monitoring tree, click the ellipses (⋮) next to the location level and select Add Site. In the pop-up window, select Type as Battery Room, select the RDU where the devices come from and select UPS, Lead-acid Battery, Lithium Battery, Power Meter devices that you want to place into the battery room. Click *Save* to create this new battery room site. As shown in Figure 4.32 below .

Figure 4.32 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 4.33 below .

Figure 4.33 Placing Devices in Battery Room 3D Configuration

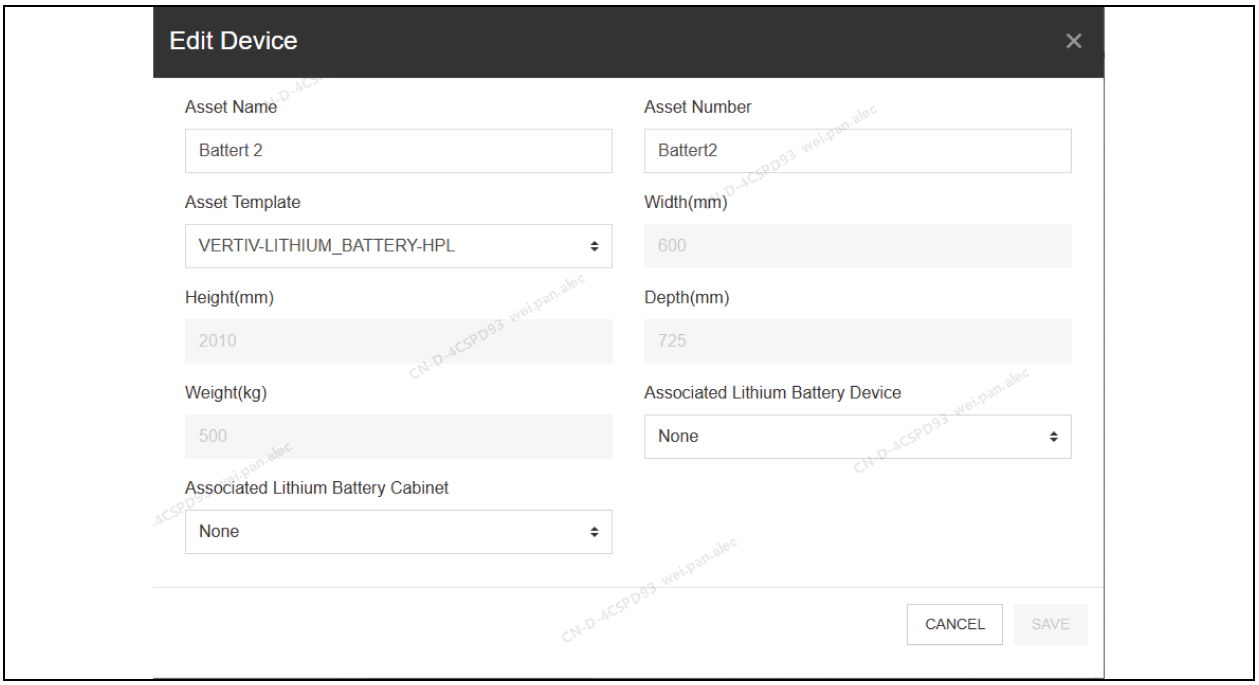


© 2026 Vertiv Group Corp. All Rights Reserved.

4.2.8 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 4.34 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 4.35 below .

Figure 4.35 Battery Configuration



© 2026 Vertiv Group Corp. All Rights Reserved.

4.2.9 Lead-Acid Battery 3D Configuration

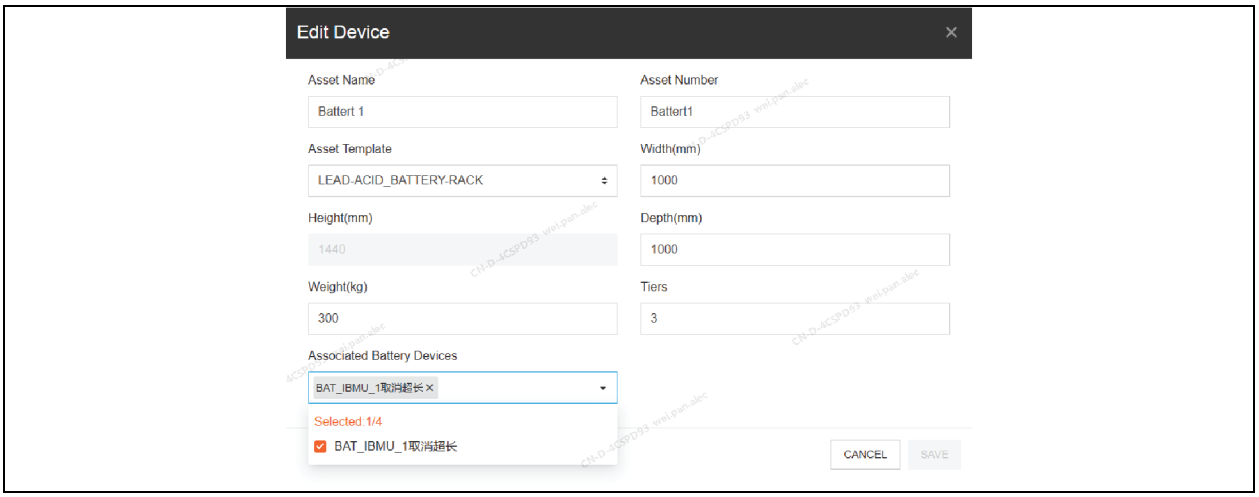
To display lead-acid batteries in 3D, you need to create a 3D model of the lead-acid battery first, the size of the model can be adjusted according to the size of the real device, and then you need to correlate the model with the real lead-acid battery device, so that you can display the signals and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

Click 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.

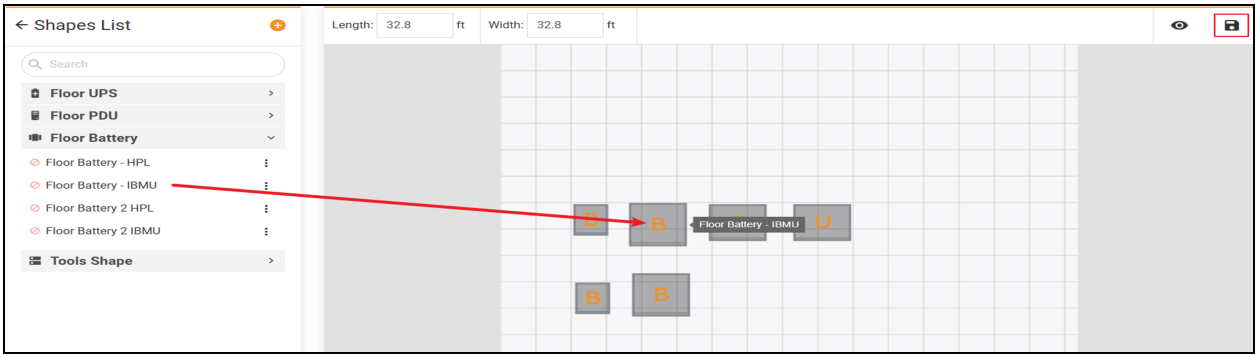
Select the template **lead-acid battery rack**, fill in the relevant information, and save it. In the configurable fields, the Height of the lead-acid battery model is determined by tiers, the more tiers the higher the battery model. And you can associate battery devices with the battery model so that when displaying the 3D of lead-acid battery, the signals and alarms of the selected battery devices can be shown in the Figure 4.36 below .

Figure 4.36 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 4.37 below .

Figure 4.37 Battery Configuration



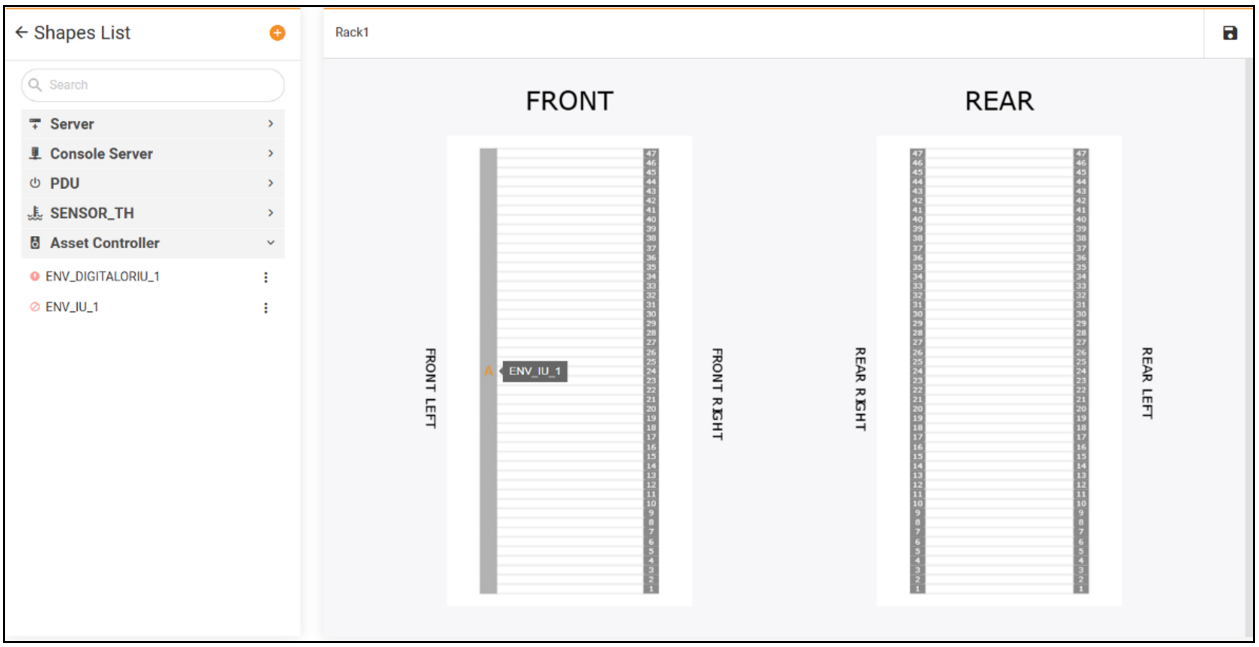
© 2026 Vertiv Group Corp. All Rights Reserved.

4.2.10 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. Suppose Smart Infrasight has already monitored the U-position asset manager through RDU501. In that case, 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 4.38 below .

Figure 4.38 U-Position Asset Manager



NOTE:

1. 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. When a rack already has a U-position Asset Manager in place, dragging another U-position Asset Manager into the same rack does not override the existing one and does not take effect.

3. For users upgrading from earlier SI versions (SI v3.0 and later) in which a U-position Asset Manager has already been connected, after upgrading to an SI version that includes the U-position Asset Manager feature, you can enable Monitoring and all related functions by going to SI > Configuration Tool > Device Management > Device Configuration > RDU Management and clicking Synchronize Configuration for the corresponding RDU.

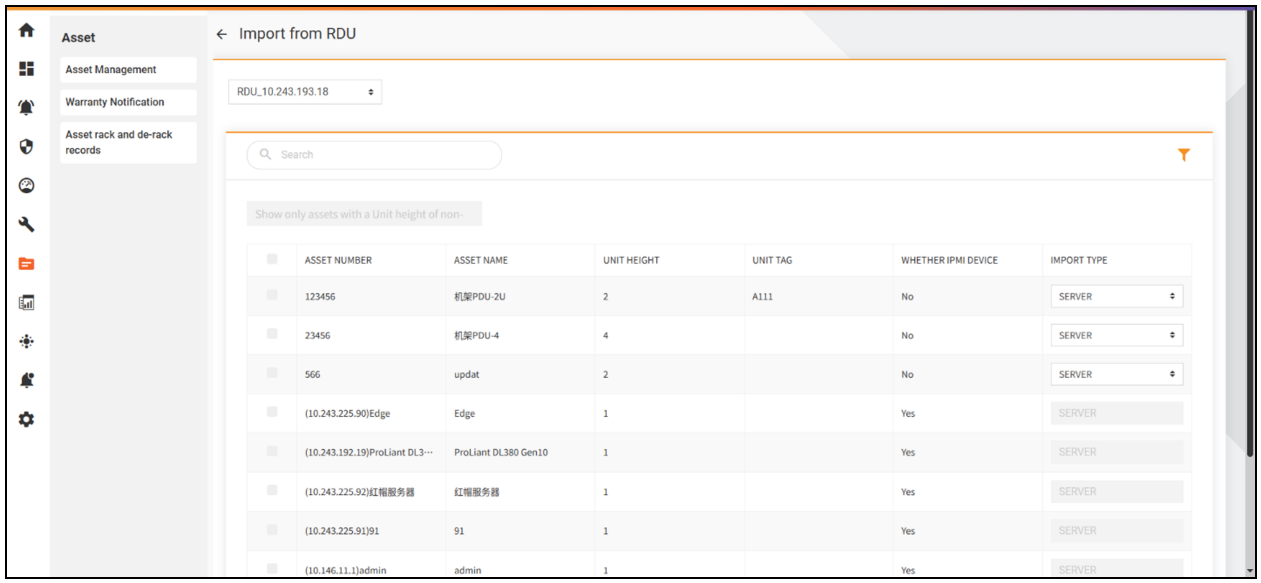
4. In 3D Configuration and 3D View, if devices appear overlapped, verify that the U height configuration of the devices is correct.

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

© 2026 Vertiv Group Corp. All Rights Reserved.

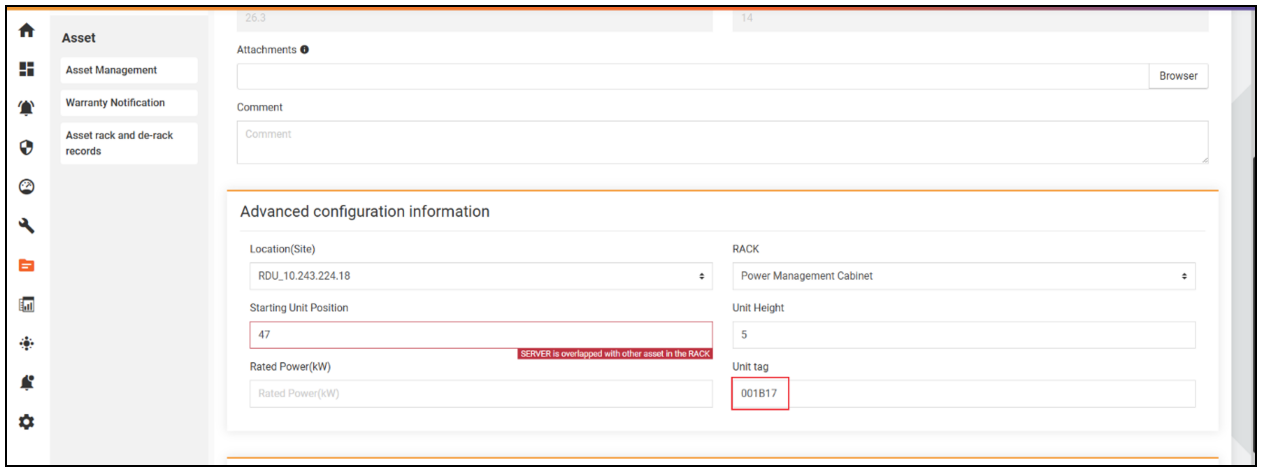
a) Use the Asset Import function in Smart Infrasight to import the managed assets from RDU501. Using RDU501 APP, you can easily scan and enter U-position tags (Unit tag in Smart Infrasight) into RDU501, and then you can import the managed assets in RDU501 together with their U-position tags into Smart Infrasight through Smart Infrasight's Asset Import function, as shown in Figure 4.39 below , which can be used to import assets from RDU501 to Smart Infrasight.

Figure 4.39 Asset Import 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 Figure 4.40 below .

Figure 4.40 Asset Information - Unit Tag

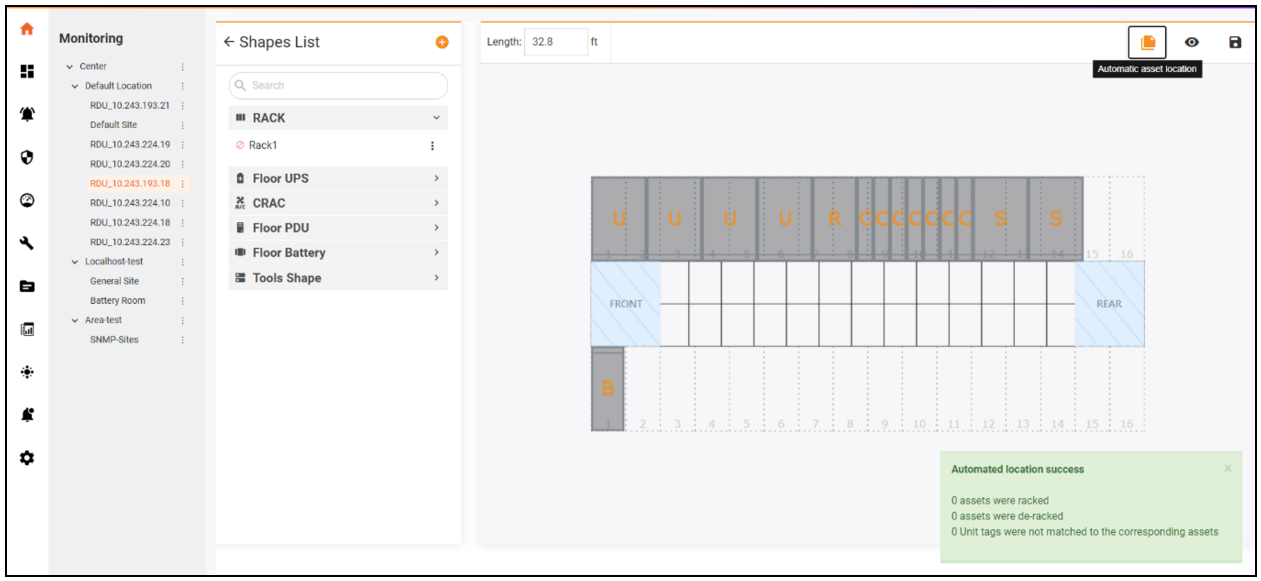


After completing the configuration of U-position Asset Manager, Smart Infrasight can automatically synchronize the asset location information and move the asset from the original cabinet to the new cabinet when the asset location is moved at the data center field.

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 4.41 Battery Configuration



© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

5 Power Train

5.1 General

5.1.1 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.

5.1.2 Functional Modules

- Creating a Power Train Diagram
- Asset List and Operations
- Canvas and Operations
- Power Configuration
- Circuit Configuration

5.2 Detailed Functions

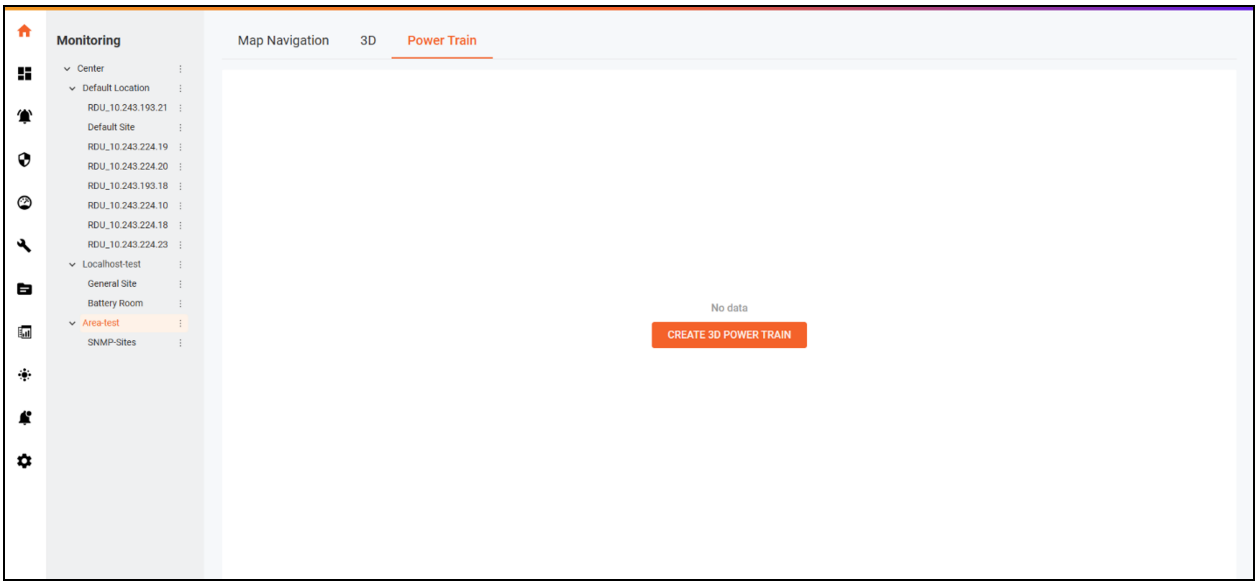
5.2.1 Creating a Power Train Diagram

After logging in to the SI system, the user 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 5.1 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 5.1 Creating a Power Distribution Link Diagram



5.2.2 Asset List and Operations

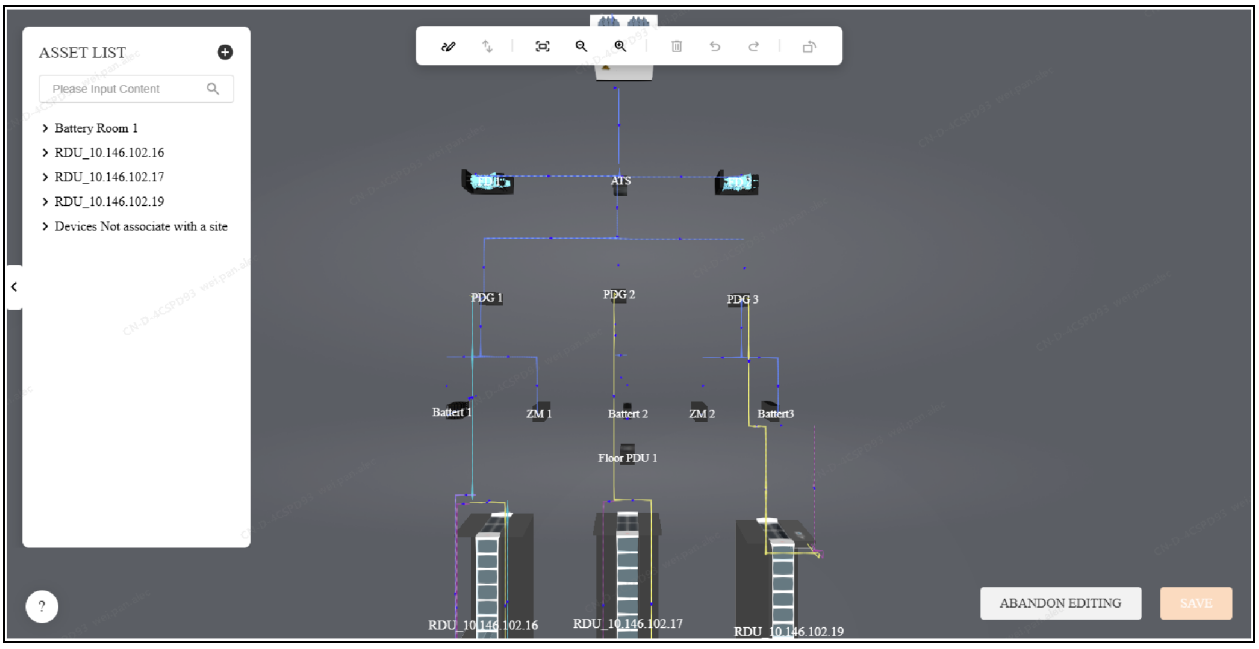
Asset List

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 5.2** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 5.2 3D Configuration



NOTE:

1. If an asset is first dragged onto the Power Train canvas and then placed into a Micro Module, after entering Power Train, the asset and all its connections (including upstream and downstream connections) are removed from the canvas.

2. If an asset is placed onto the Power Train canvas together with a Micro Module and is subsequently removed from the Micro Module, after entering Power Train, the asset appears in the asset list and can be dragged onto the canvas.

3. After a Micro Module is dragged onto the canvas, asset entries such as Smart Aisle2, Smart Aisle3, or Smart Row2 can no longer be dragged onto the canvas.

4. Asset entries can be dragged onto the canvas. Asset entries that already exist on the canvas cannot be dragged onto the canvas repeatedly.

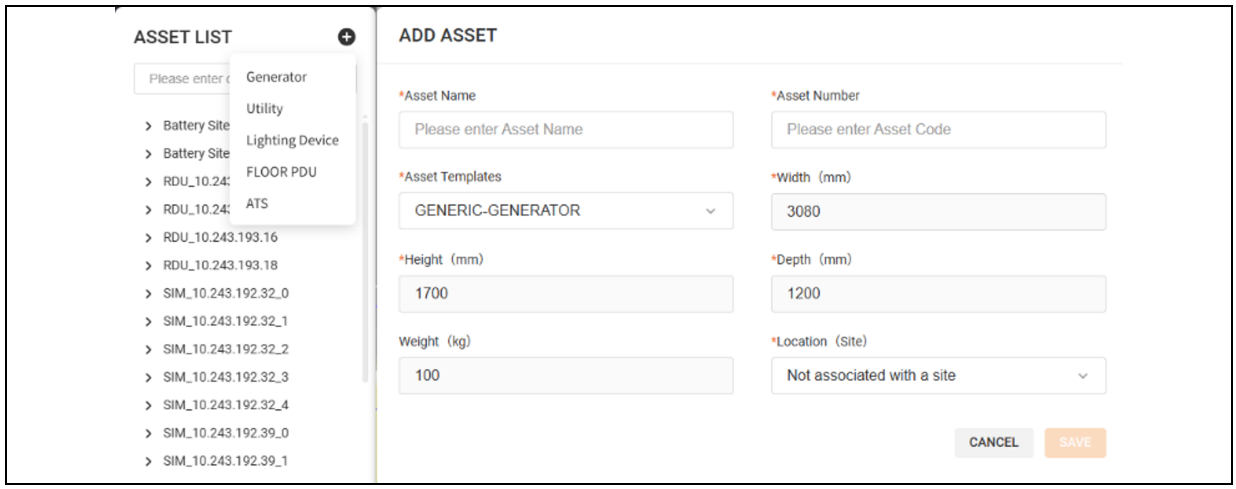
5. If the asset collides with other assets on the canvas when dragged into the canvas, the dragging action fails.

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 5.3 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 5.3 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 5.4** below .

Figure 5.4 Deleting the Asset

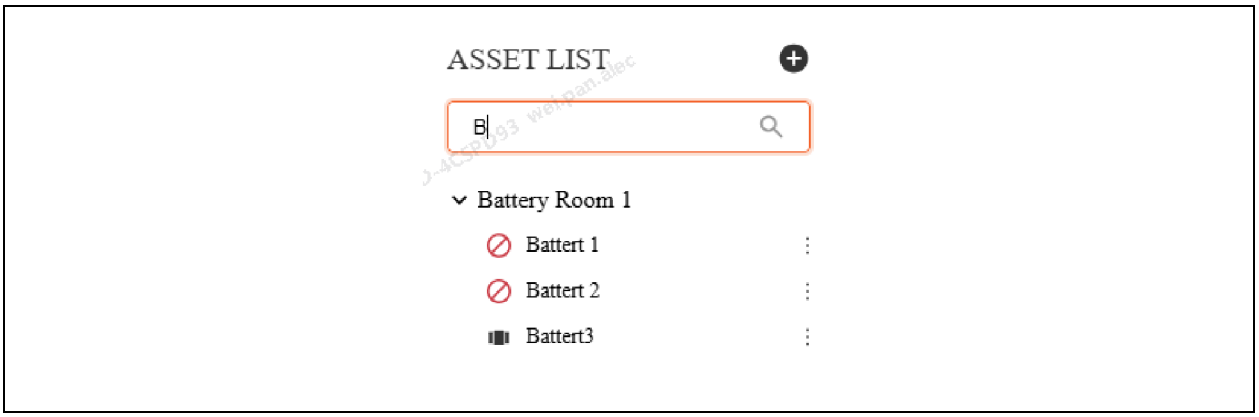


4. Searching the Asset

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 5.5** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 5.5 Searching the Asset



Interactions :

When an asset is placed onto the canvas, the corresponding 3D model is displayed based on the asset's width, depth, and height. The asset name is displayed on the model.

- Press Ctrl and left-click the mouse to select multiple assets.
- Left-click to select an asset or a connection. Press and hold the left mouse button to adjust the 3D view perspective.
- Press and hold the right mouse button to pan the view.
- Scroll the mouse wheel to zoom the view.
- Press and hold the mouse wheel and drag the mouse to rotate the 3D view.
- When an asset is selected, press and hold the left mouse button to drag and adjust the asset's position on the canvas. During movement, the asset's connections move together with the asset. If a collision occurs at the target position after the asset is moved, the move operation fails. When an asset is selected, clockwise rotation by 90 degrees is supported. Collision detection is performed during rotation. If the rotated position collides with another asset, the rotation fails.
- When a single asset is clicked, the Power Configuration panel is displayed. For details, see Power Configuration on page 85.

NOTE:

1. If an asset size is changed and the change causes assets to overlap in the Power Train topology, the overlapping visual layout is retained.

2. If an asset is placed onto the Power Train canvas together with a Micro Module and is subsequently removed from the Micro Module, after entering Power Train, the asset appears in the asset list and can be dragged onto the canvas.

3. When a Micro Module is displayed as an integrated object on the canvas, the maximum display height is 2200 mm. If the actual height exceeds this value, the Micro Module is displayed at a height of 2200 mm.

© 2026 Vertiv Group Corp. All Rights Reserved.

5.2.3 Canvas and Operations

Canvas

The canvas is a container for placing power assets and circuit connections. By default, it displays a top-down view, with the center of the canvas shown in the middle of the screen. The default canvas size is 100 m × 100 m.

- Zoom canvas: Scroll the mouse wheel up to zoom in and scroll down to zoom out. The view zooms in or out with the mouse cursor as the center.
- Adjust 3D view: Press and hold the mouse wheel and move the mouse to drag and adjust the 3D view.
- Select asset or connection: Click the left mouse button to select an asset or a connection.
- Adjust 3D view when nothing is selected: When no asset or connection is selected, press and hold the left mouse button to drag and adjust the 3D view.
- Pan canvas: Press and hold the right mouse button to pan the canvas.

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Rotate

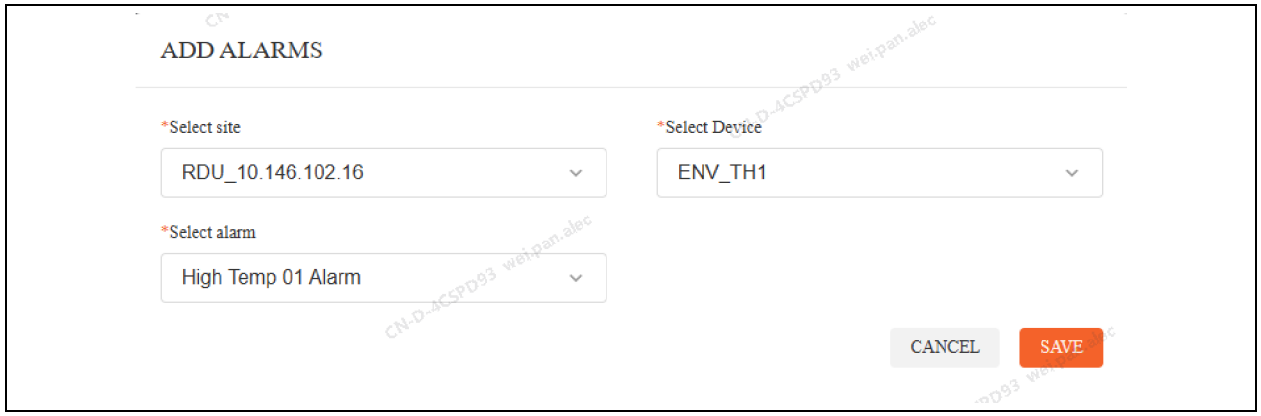
By default, this button is grayed out. It becomes highlighted when you select an asset and, when clicked, rotates the asset model 90 degrees clockwise.

5.2.4 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:

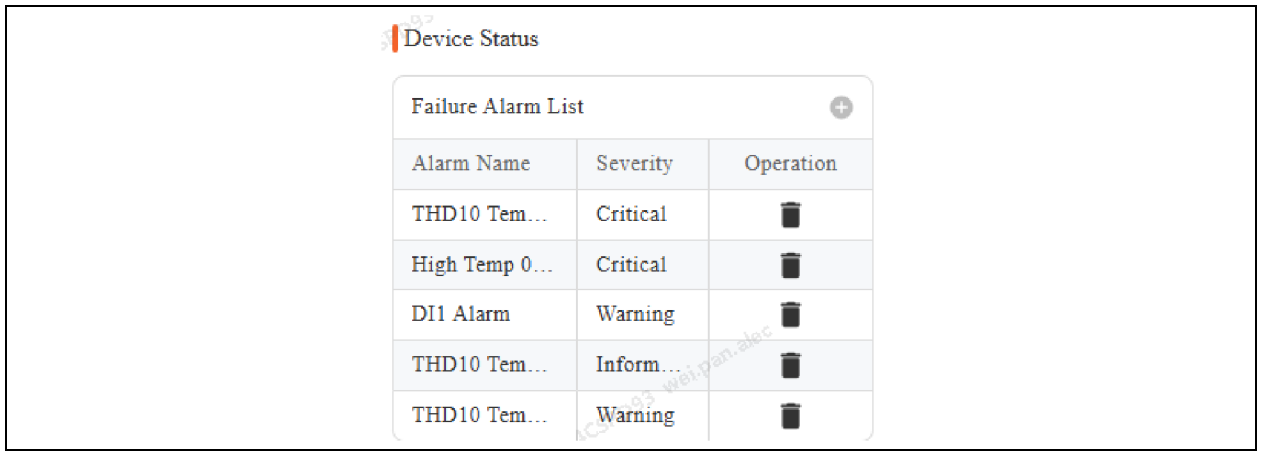
Device Failure Alarms

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 5.6 below .

Figure 5.6 Failure Alarm List



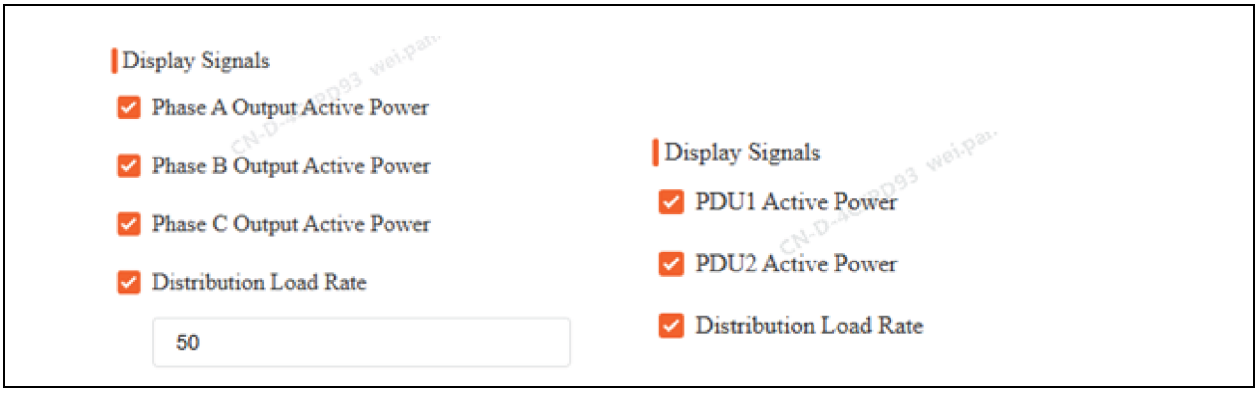
If you need to change the monitored alarm, you need to delete the alarm first and then add the alarm, click the *Delete* button on the right side of a single alarm to delete the alarm.

© 2026 Vertiv Group Corp. All Rights Reserved.

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 5.7 below .

Figure 5.7 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:

Figure 5.8 The Percentage Indicator Of The Load Factor



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

© 2026 Vertiv Group Corp. All Rights Reserved.

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.

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

3. When data is displayed on a percentage indicator and the denominator is 0, (--) is displayed. When the mouse pointer hovers over the indicator, a tooltip displays The rated power is 0. Calculation is not supported.

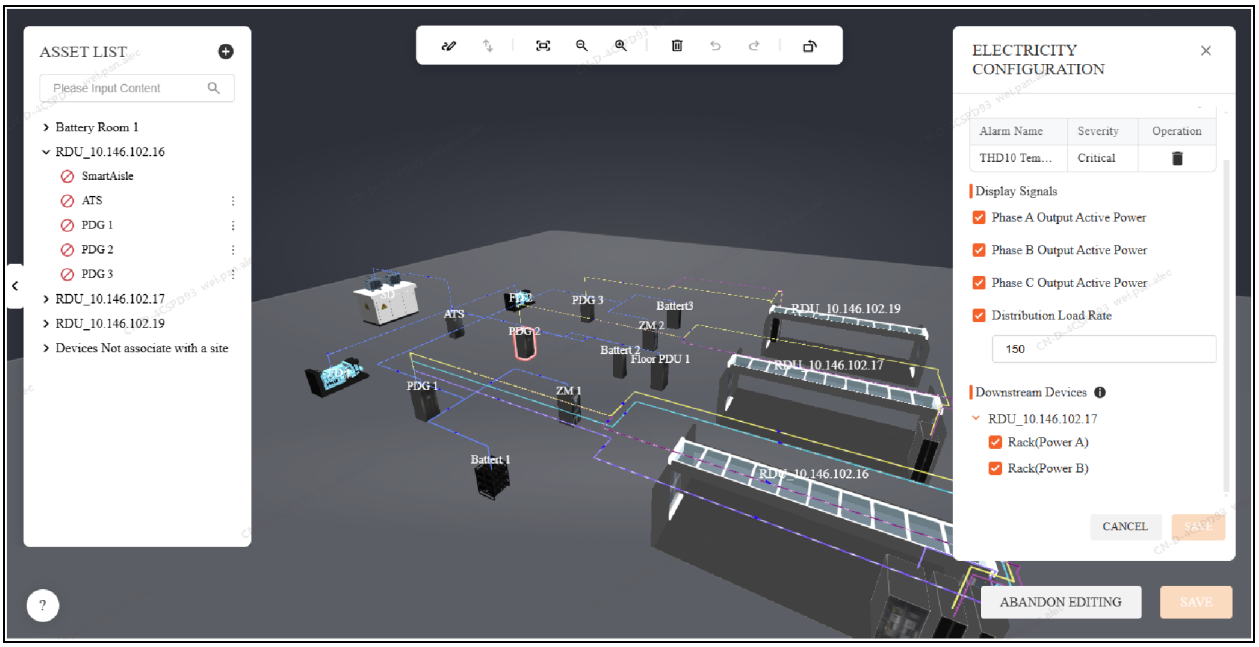
4. When data is displayed on a percentage indicator and the signal used as the numerator is empty, (--) is displayed. When the mouse pointer hovers over the indicator, a tooltip displays The load power signal is not selected. Calculation is not supported.

5. If the remaining capacity signal value fails to be retrieved, (--) is displayed. When the mouse pointer hovers over the indicator, a tooltip displays Failed to retrieve the signal.

Downstream Devices

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.

Figure 5.9 Power Train Topology – Display Page



© 2026 Vertiv Group Corp. All Rights Reserved.

NOTE:

1. SR2 PMC Cabinet: Also referred to as the Integrated Power Distribution Cabinet, this is a special rack deployed and installed together with Smart Row2. Each SR2 site is equipped with one PMC cabinet. Depending on the configuration selected by the customer, the PMC cabinet may contain a UPS and power distribution modules to serve as the power distribution equipment for SR2, or it may contain no power distribution equipment and function only as a standard rack.

2. Micro Module: Includes Smart Aisle3 (SA3), Smart Aisle2 (SA2), and Smart Row2 (SR2).

3. For air conditioners and rack circuits connected to a Micro Module, if the device configuration within the Micro Module is later changed and no longer includes air conditioners or racks, the circuits and configurations that connect the devices to the fixed connection points of the Micro Module are retained.

5.2.5 Circuit Configuration

Circuit connections dynamically display the direction of power flow. Based on the Alarm configuration of each connection, the display priority of the connection status is Abnormal > Normal. For connections from external devices of a Micro Module to air conditioners or racks inside the Micro Module, the Alarm status of the main line and branch lines is displayed independently and does not affect each other.

Click a *circuit connection* to display the Circuit Connection panel. When the connection is in an abnormal state, the panel displays the status and the corresponding Alarm, as well as the custom attribute name, signal value, and signal unit. The refresh interval is 30 seconds.

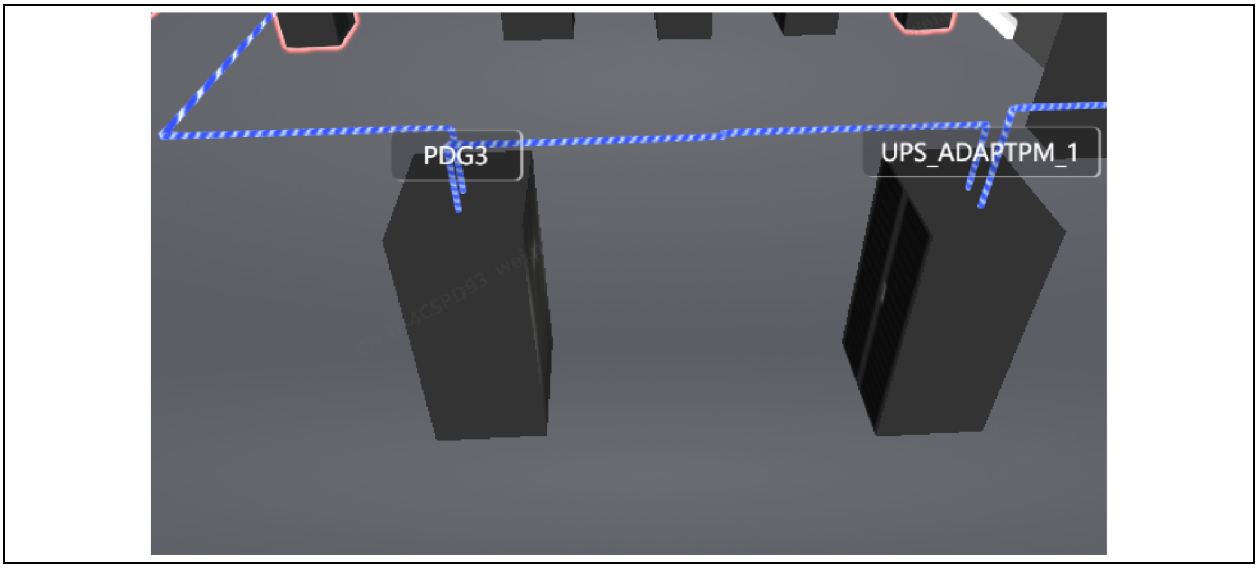
Click a *connection* to change its direction. The position of the middle segment of the connection can be adjusted. Press *Ctrl* and click the mouse to select multiple connections, which can then be deleted in batches or have their directions changed.

© 2026 Vertiv Group Corp. All Rights Reserved.

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.

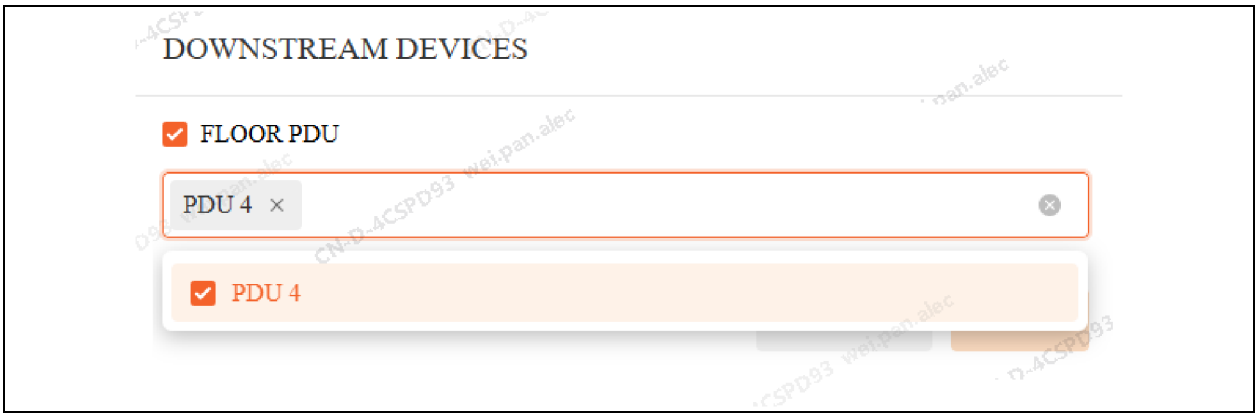
Figure 5.10 Connections Between External Devices



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.

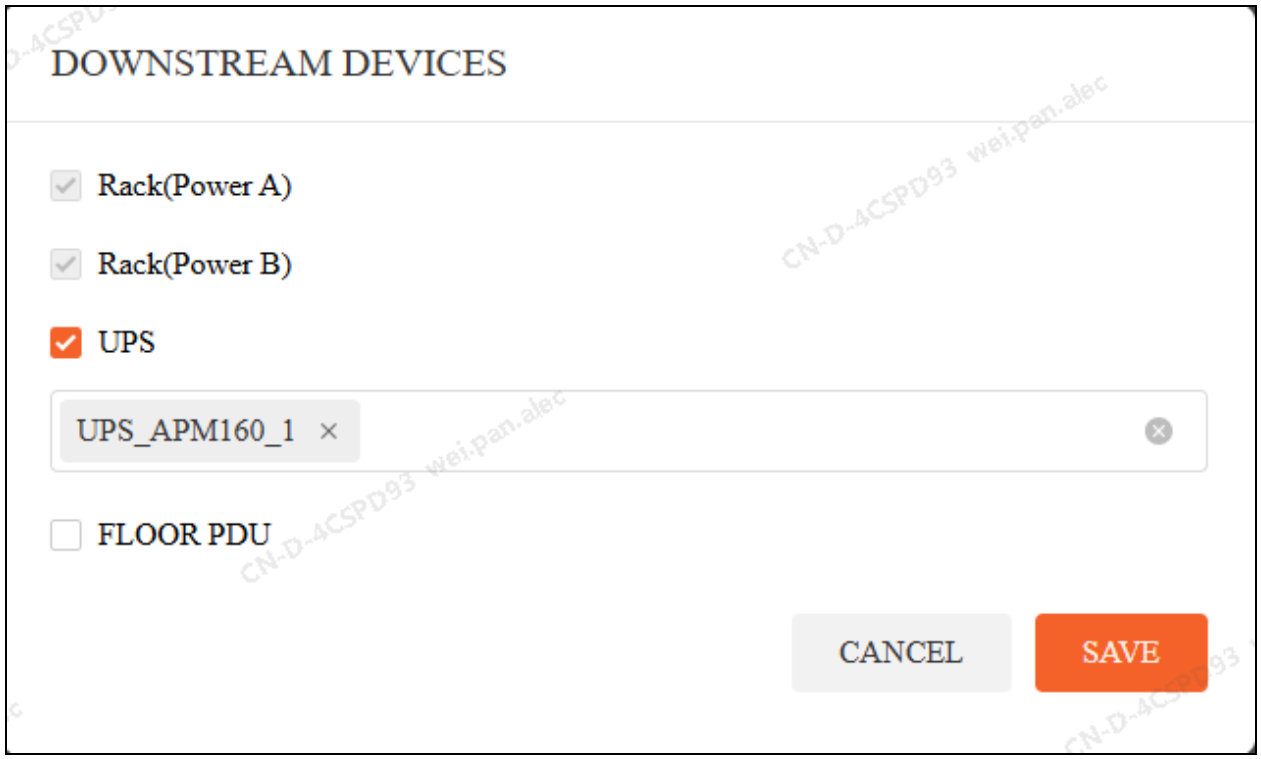
Figure 5.11 Power Distribution Cabinet Device Multi-Select Checkbox



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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 5.12 UPS Device Multi-Select Checkbox



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.

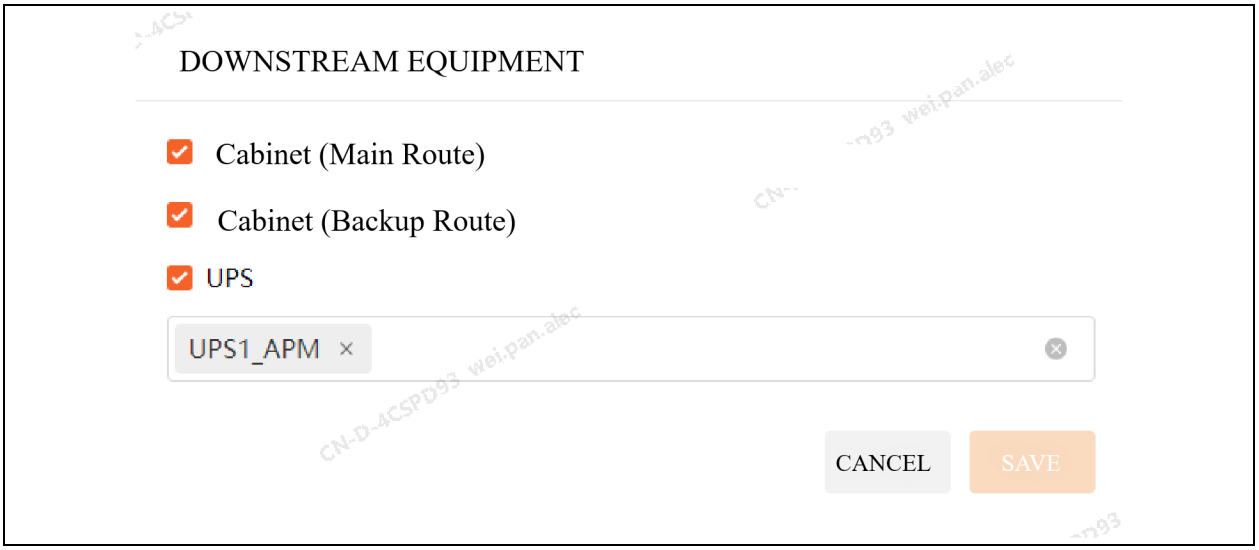
Rack Power B: Similarly, circuit connections from the power distribution cabinet to each rack in the Smart Solution will be established and the power distribution cabinet will be seen as power source B of all racks in the Smart Solution.

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

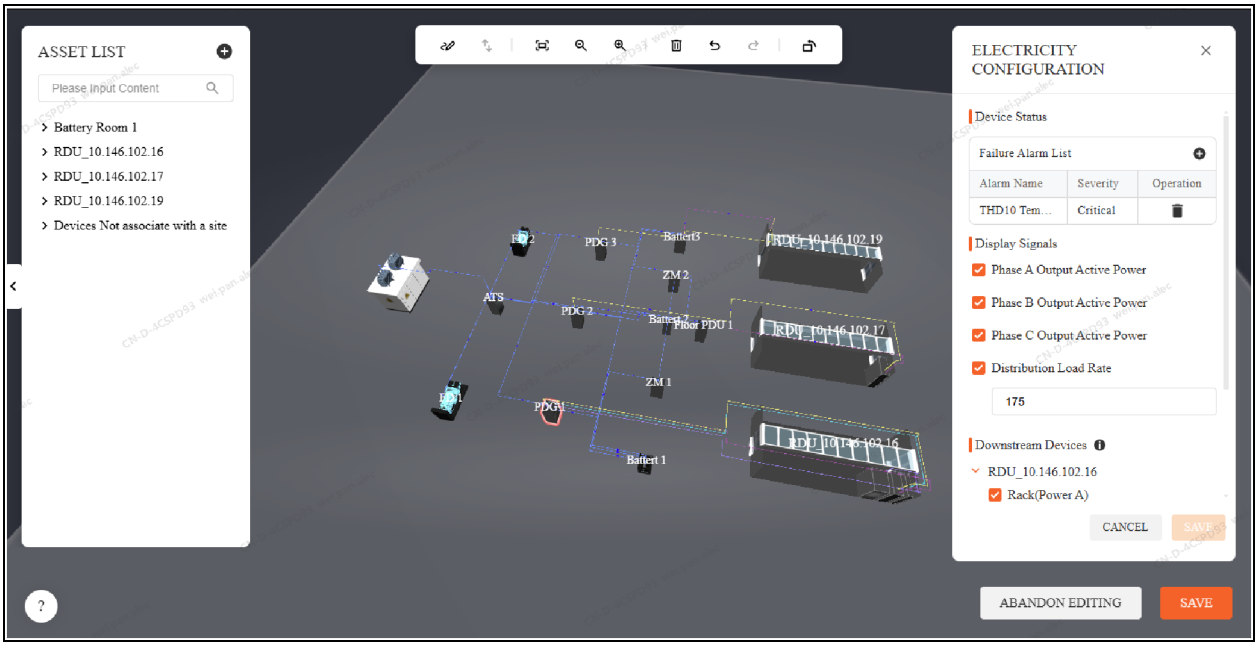


Editing the Circuit Connections (between Assets and Smart Solution)

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.

Figure 5.13 Power Configuration Panel

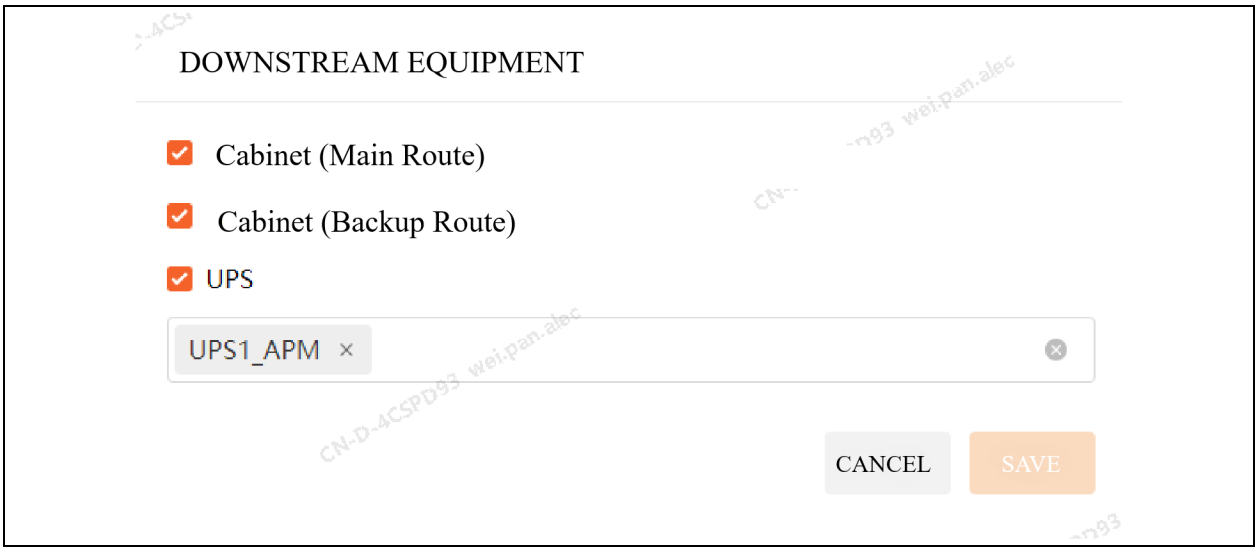


Connection Restriction

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

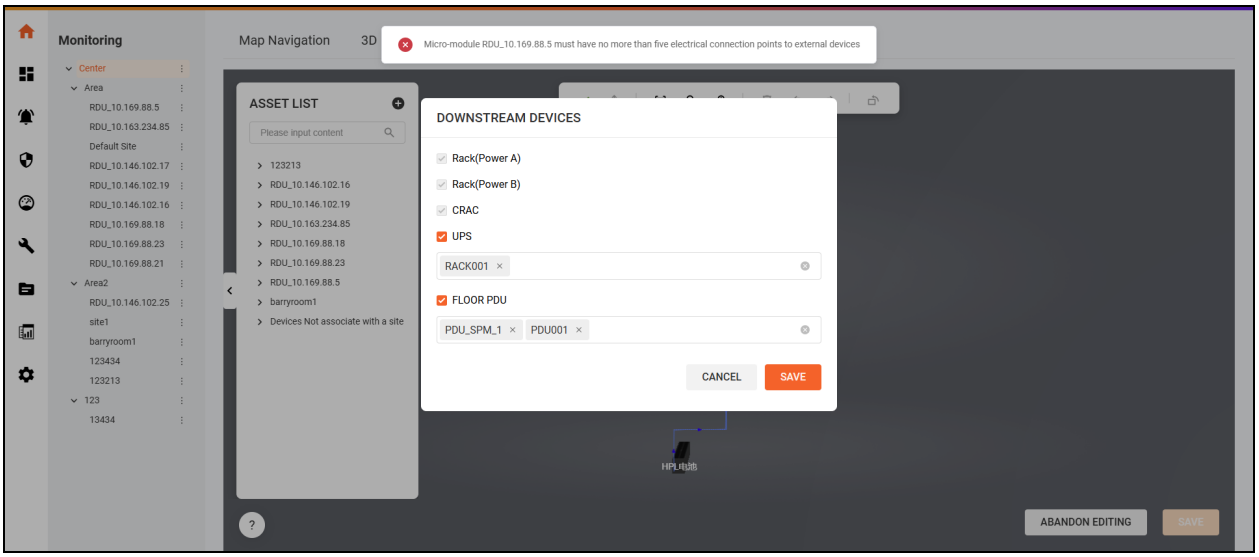
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 5.14 Downstream Device Configuration Information



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

Figure 5.15 Too Many Connections Error Messages



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.

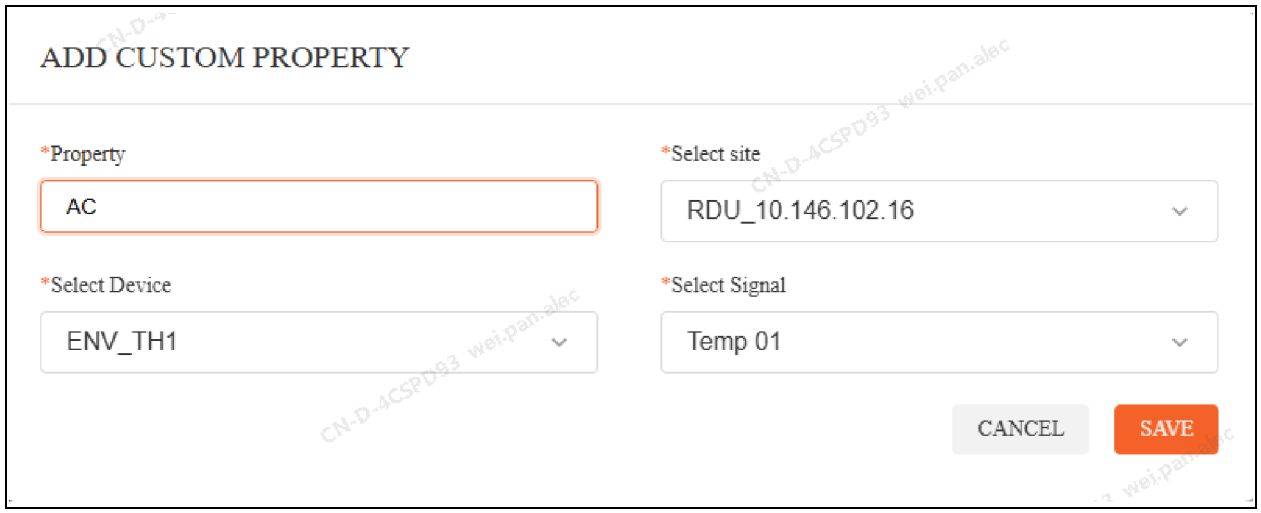
Circuit Line Configuration

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

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 5.16 below .

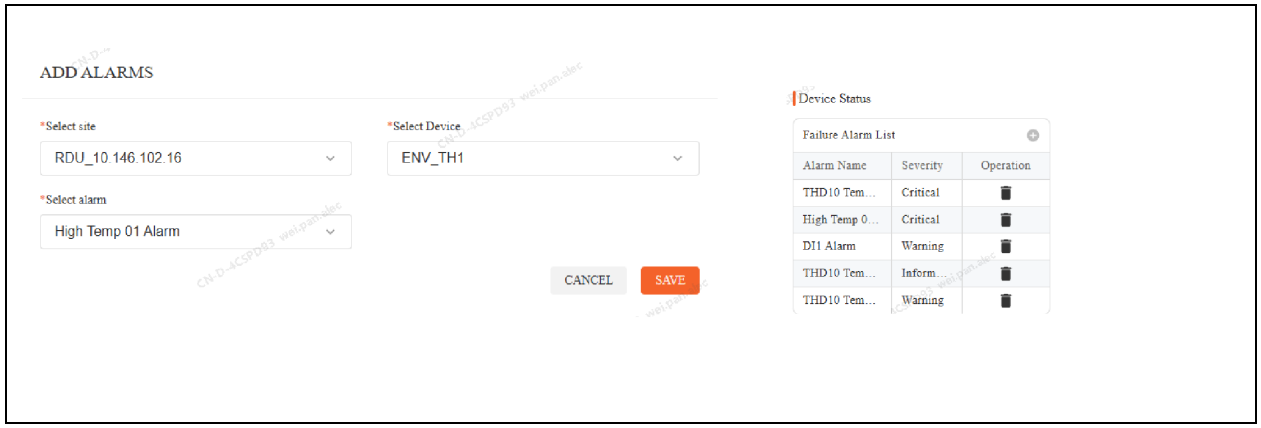
Figure 5.16 Adding the Custom Properties



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 circuit line flashes continuously to indicate the abnormal condition. Click the *Add* button to add an abnormal alarm that can imply the connection is abnormal, click *Save* to add the abnormal alarm to be monitored in Exception.

In the alarm list, the following Figure 5.17 below shows the alarms.

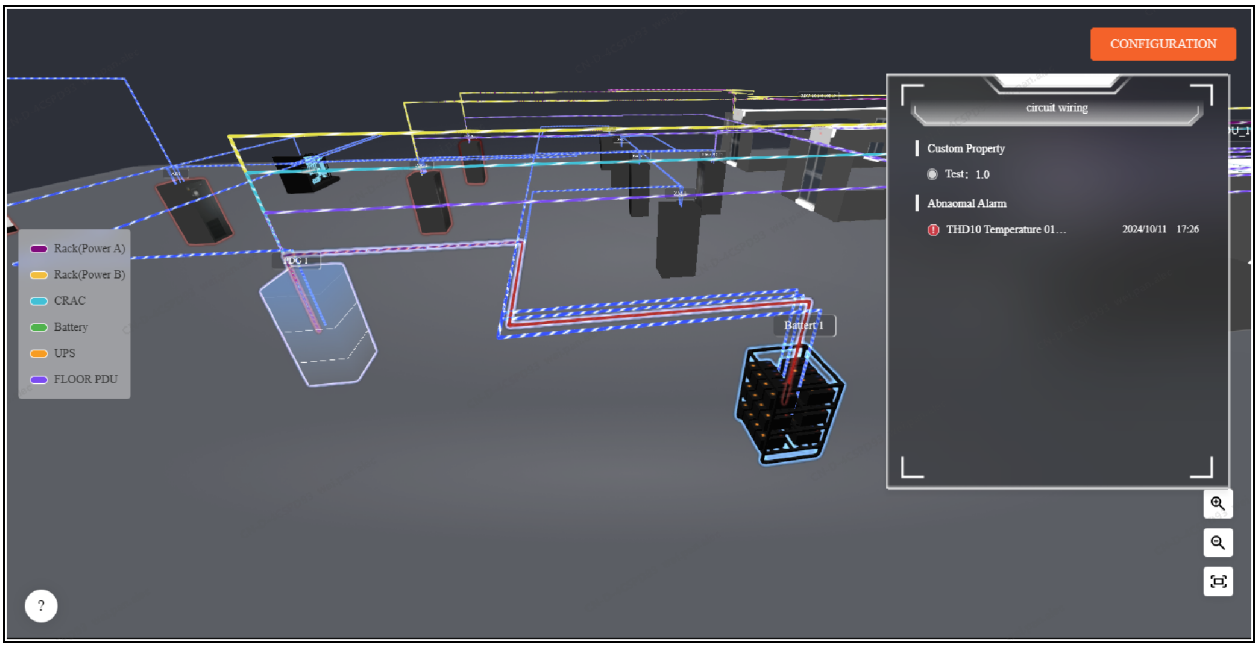
Figure 5.17 Adding Alarms



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 5.18 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 5.18 Viewing the Completed Configuration



© 2026 Vertiv Group Corp. All Rights Reserved.

6 3D Visualization

6.1 General

6.1.1 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.

6.1.2 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 active alarms from different devices.

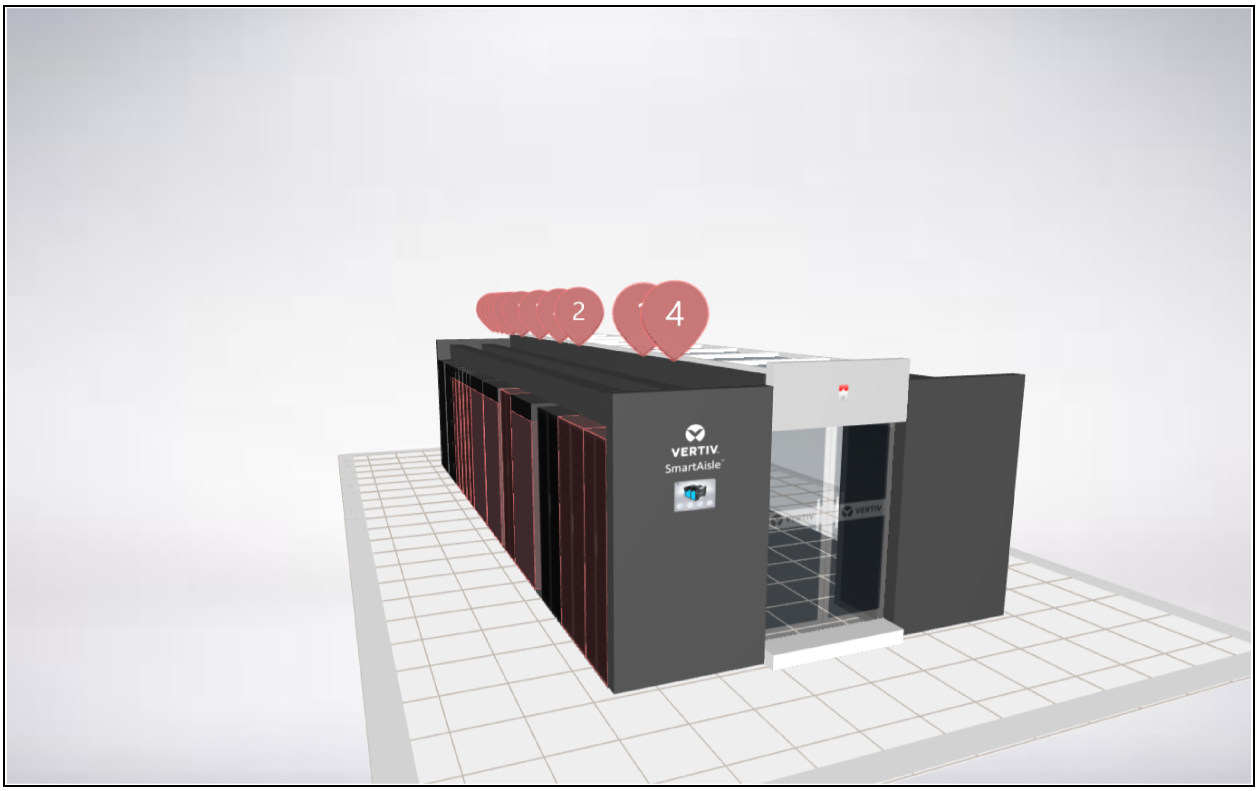
Users can interact with the 3D view as follows:

- 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 .

© 2026 Vertiv Group Corp. All Rights Reserved.

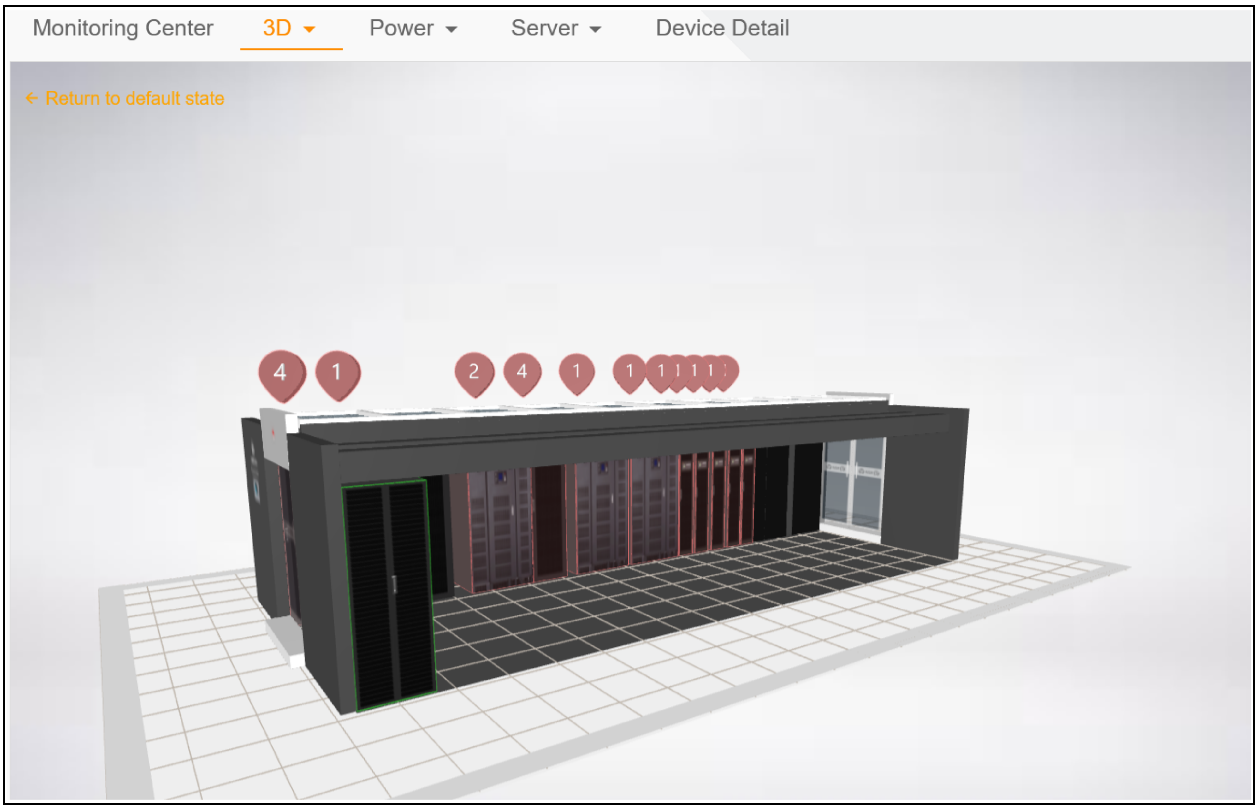
Figure 6.1 The Default 3D View of Smart Aisle2



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 .

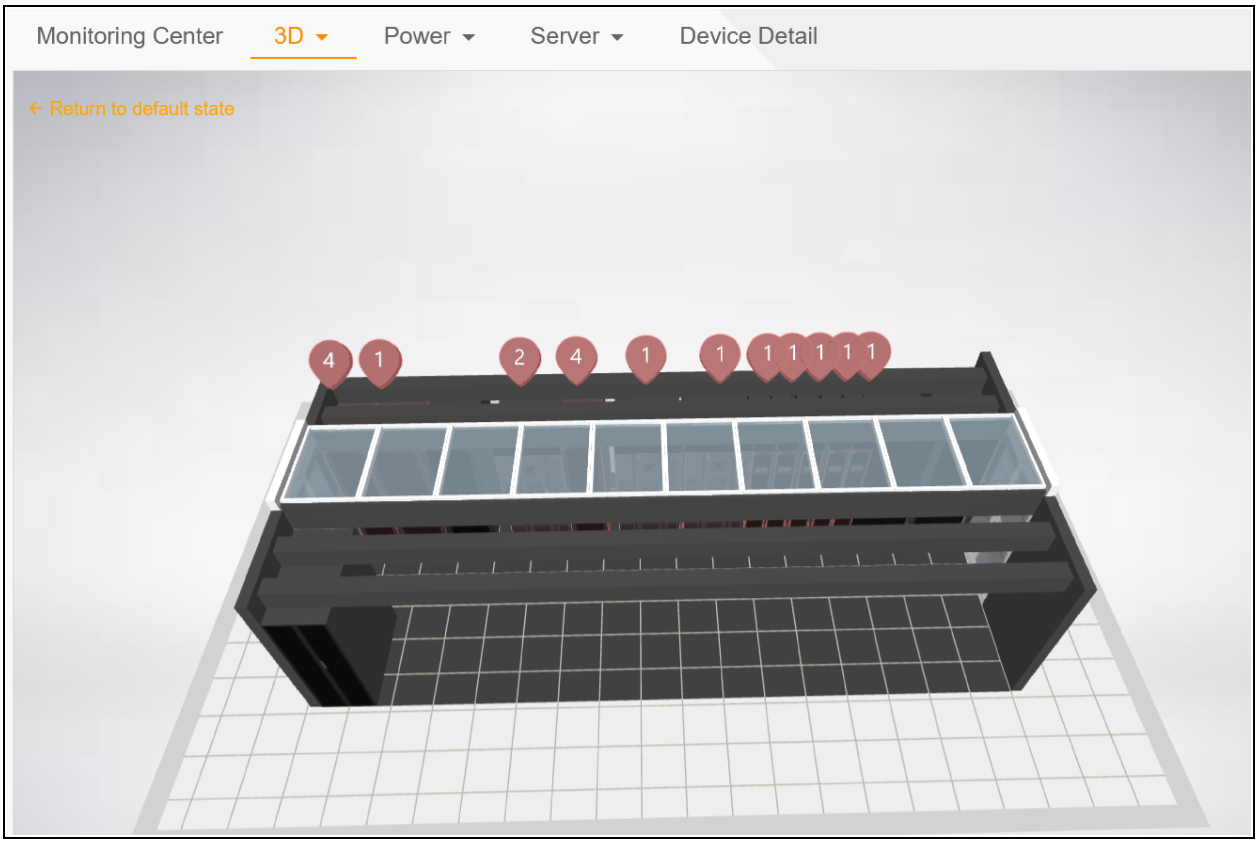
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.2 Rotated 3D View of the Smart Aisle2 Site



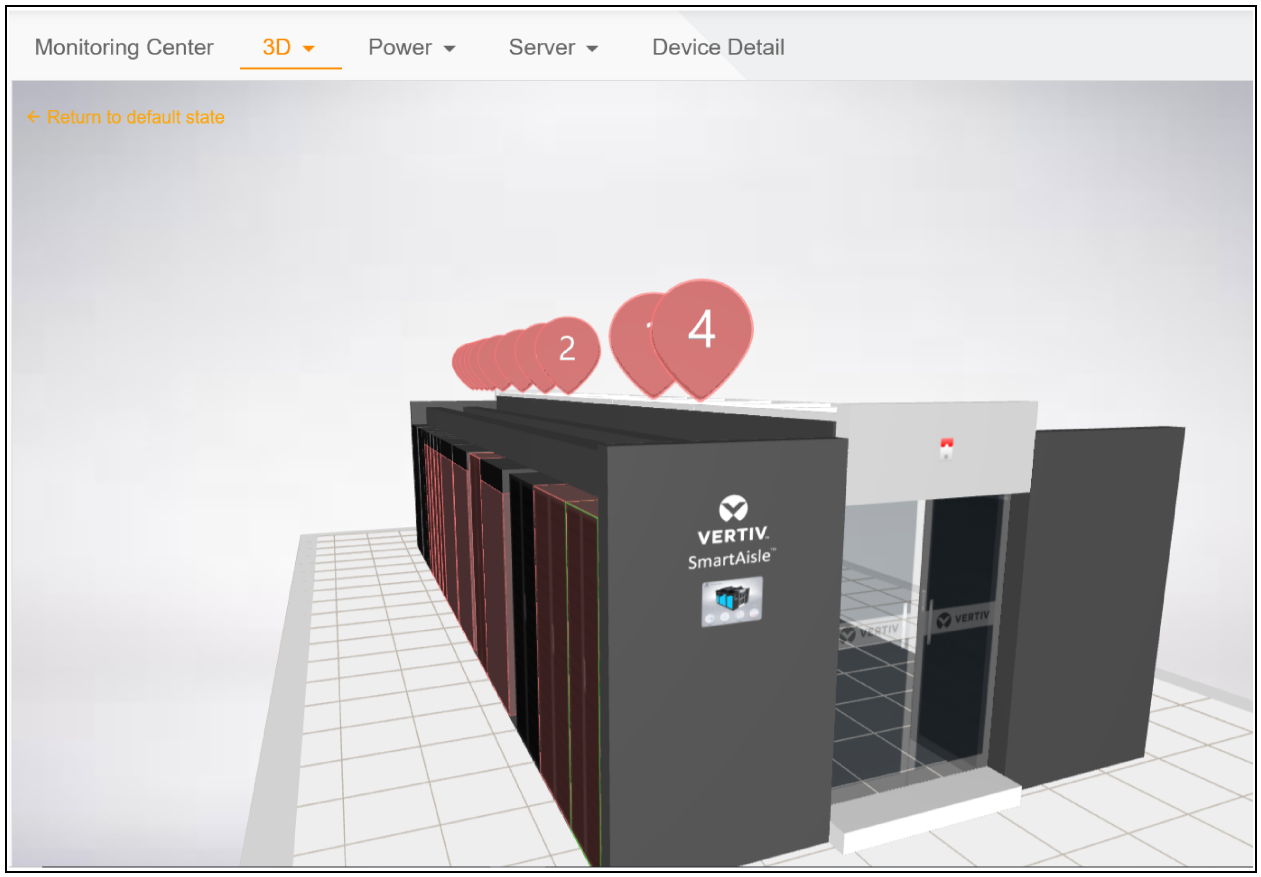
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.3 Top View of Smart Aisle2



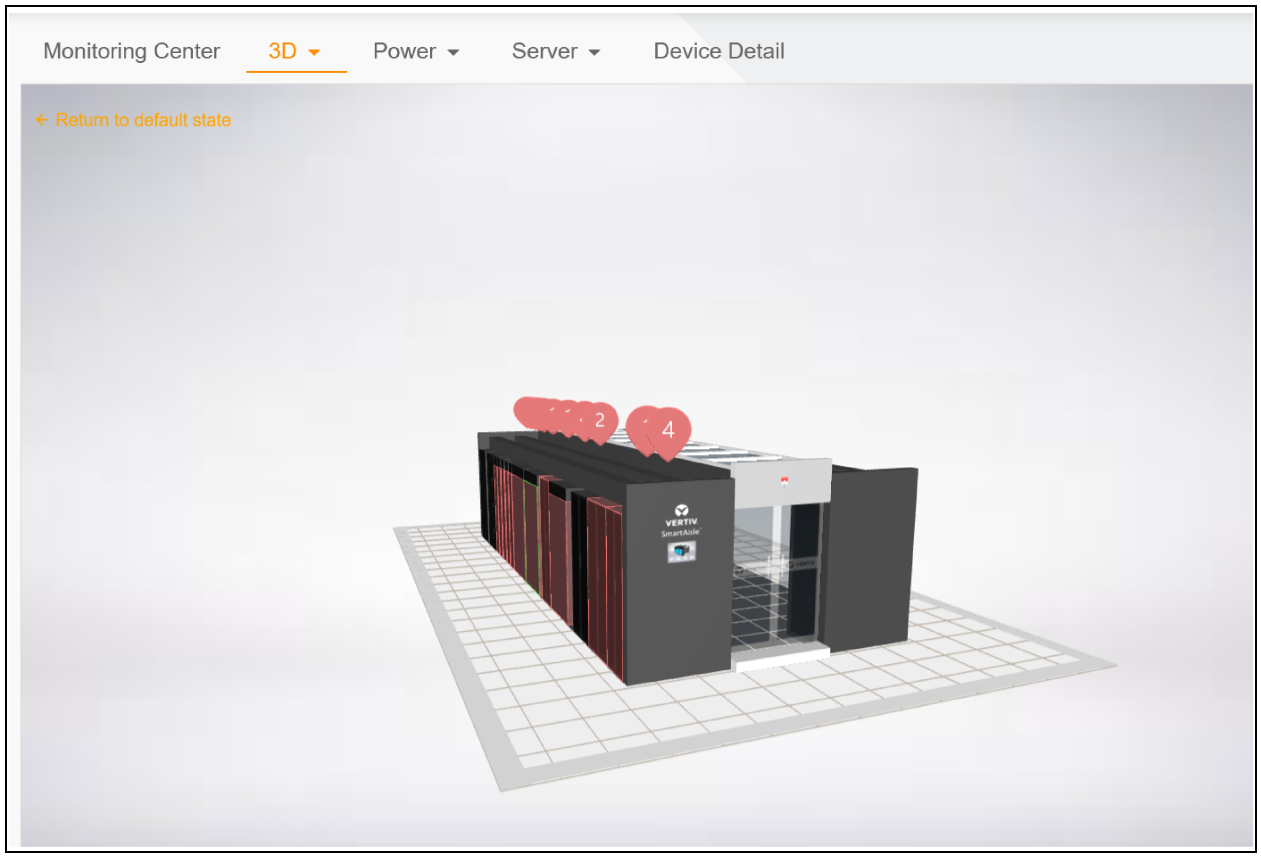
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.4 Zoom-in View of Smart Aisle2



© 2026 Vertiv Group Corp. All Rights Reserved.

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

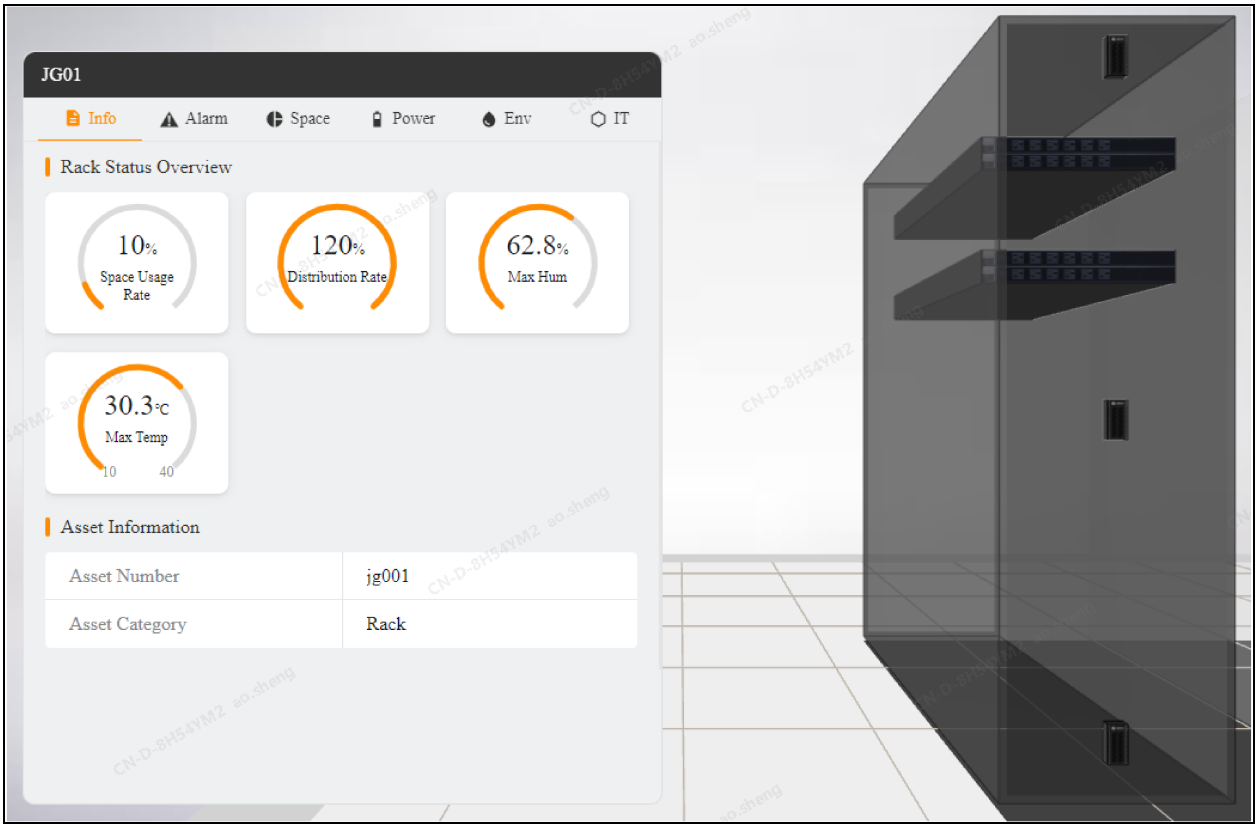


© 2026 Vertiv Group Corp. All Rights Reserved.

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.

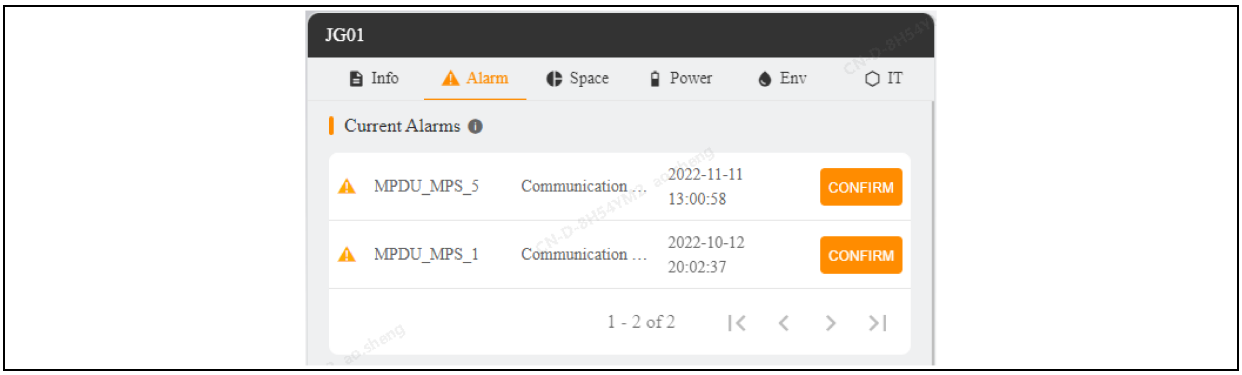
Selecting the IT category displays servers, switches, and other IT equipment.

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 103 .

Figure 6.8 Alarm Window



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.9 Alarm Trends

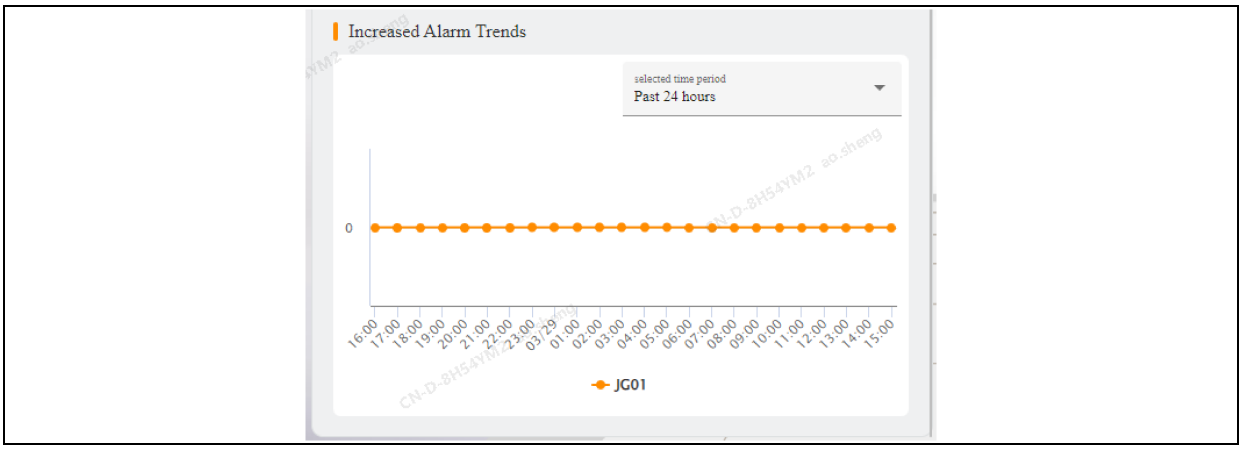
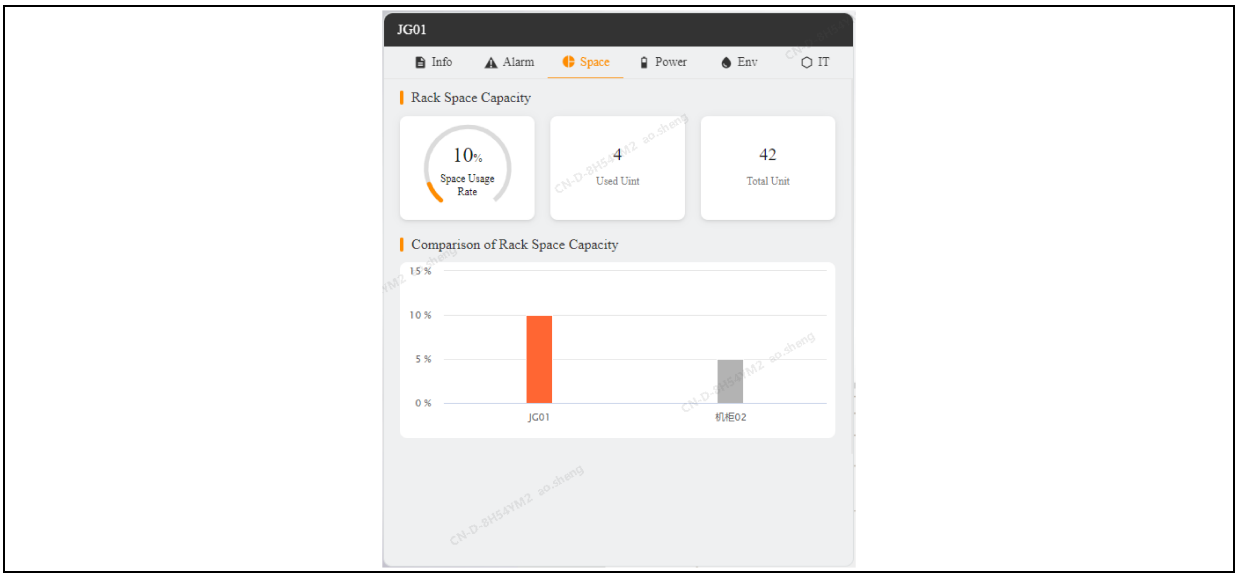


Figure 6.10 Space Card



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.11 Power Distribution Card

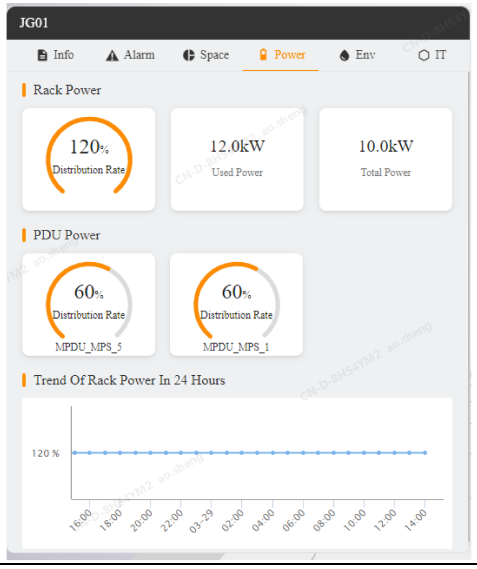


Figure 6.12 Environment Card

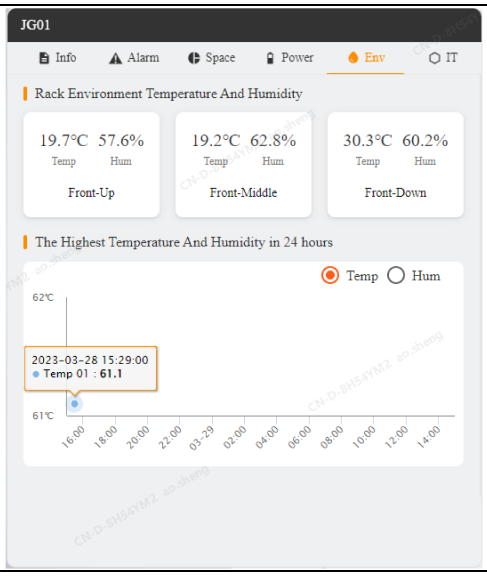
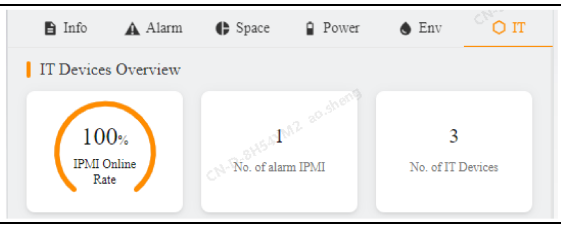


Figure 6.13 IT Card



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).

© 2026 Vertiv Group Corp. All Rights Reserved.

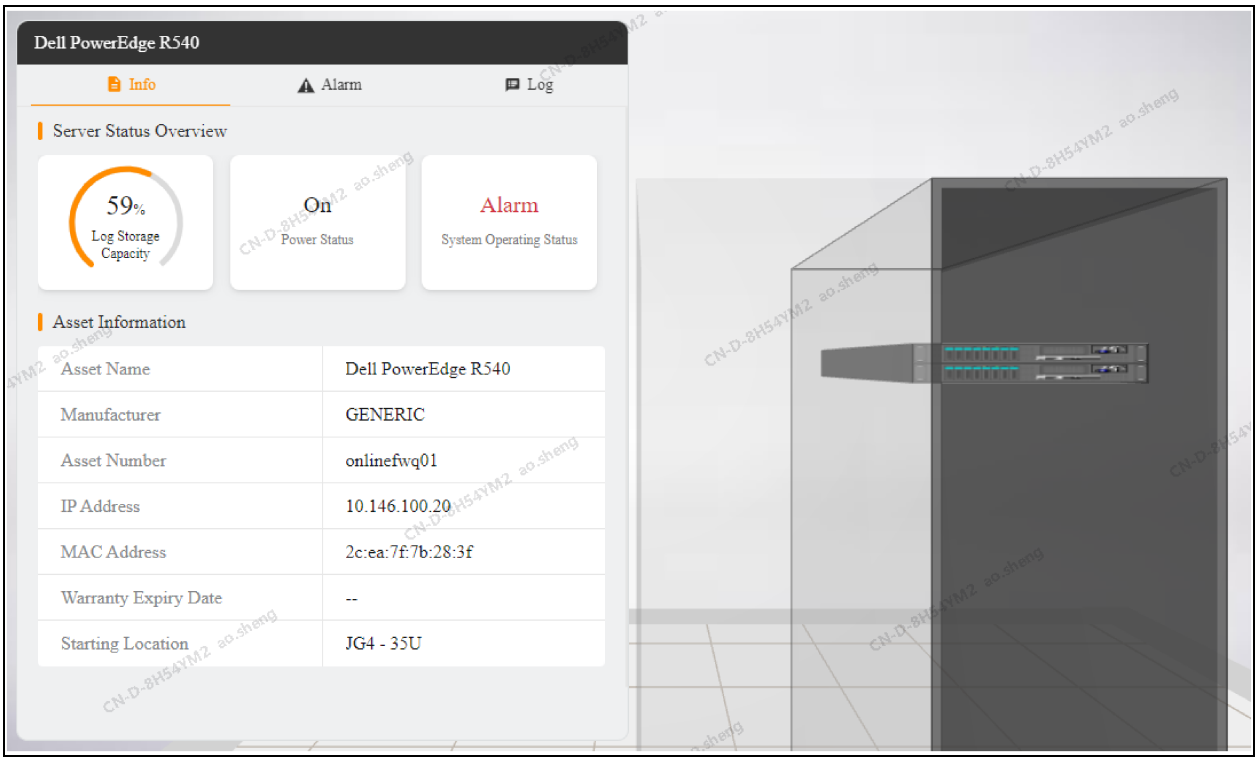
Figure 6.14 3D single-cabinet view of Smart Aisle2 site - IT



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

© 2026 Vertiv Group Corp. All Rights Reserved.

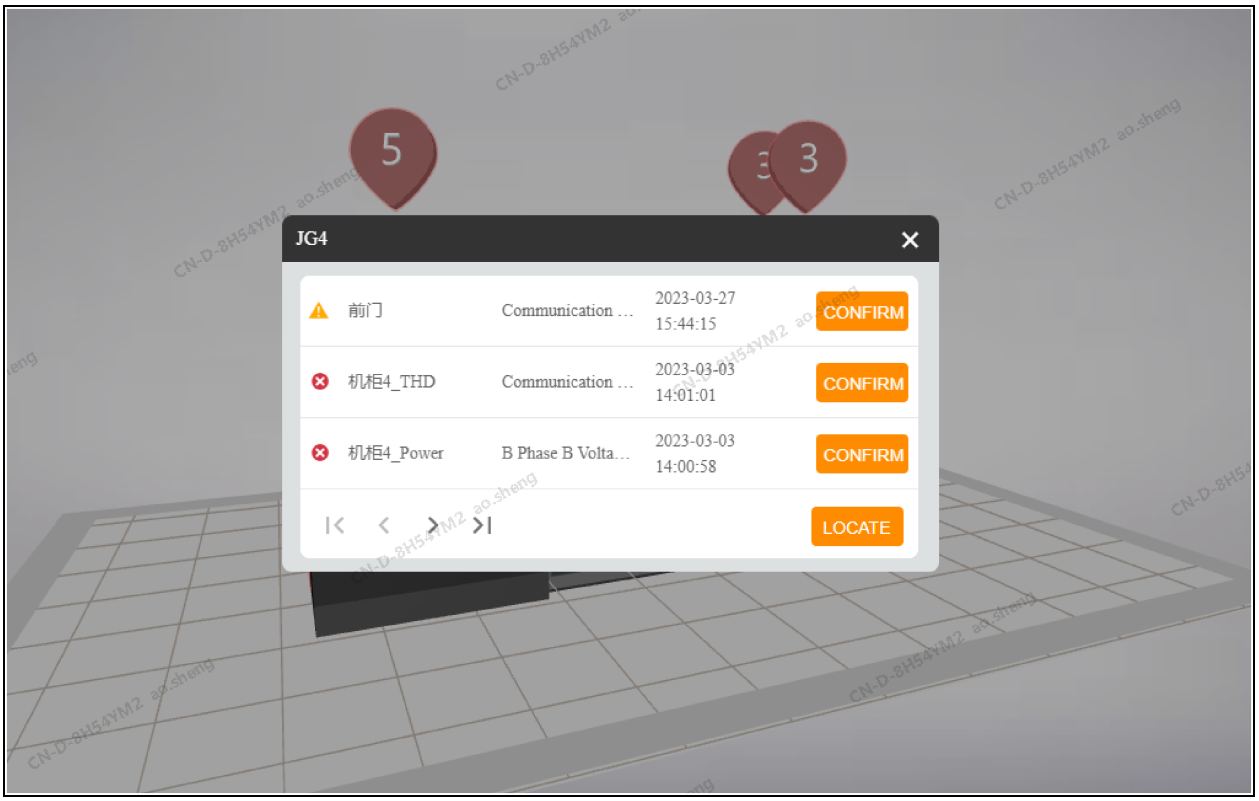
Figure 6.15 Smart Aisle2 Site Server View



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.

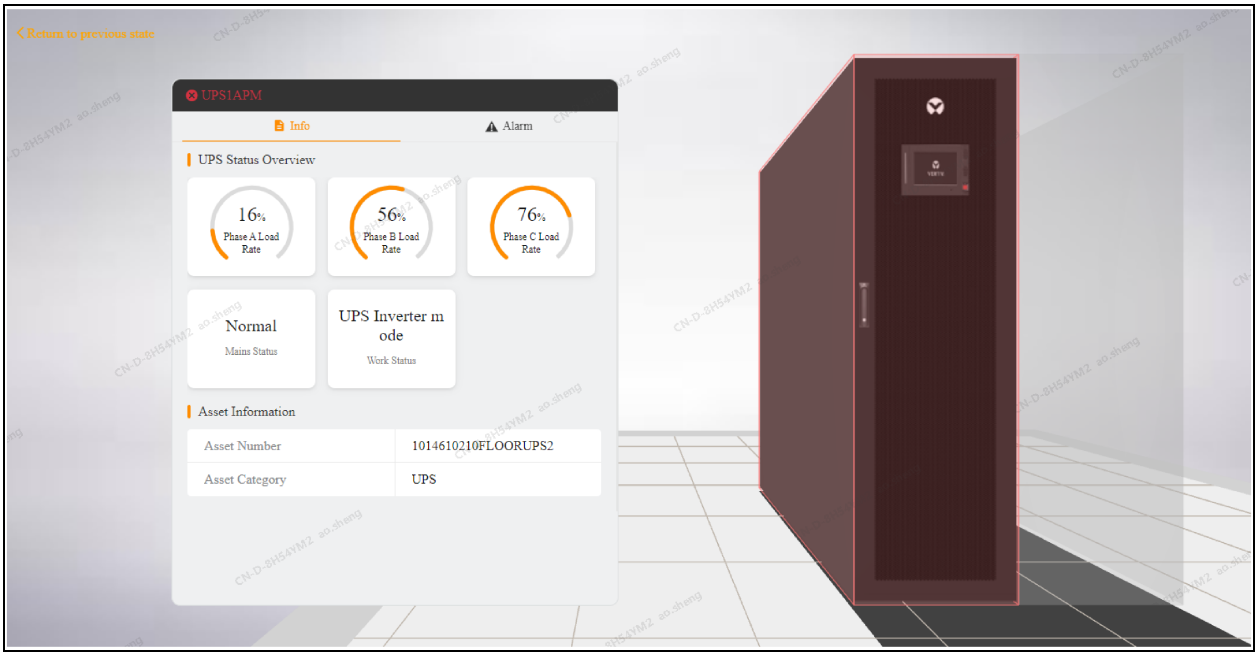
© 2026 Vertiv Group Corp. All Rights Reserved.

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.

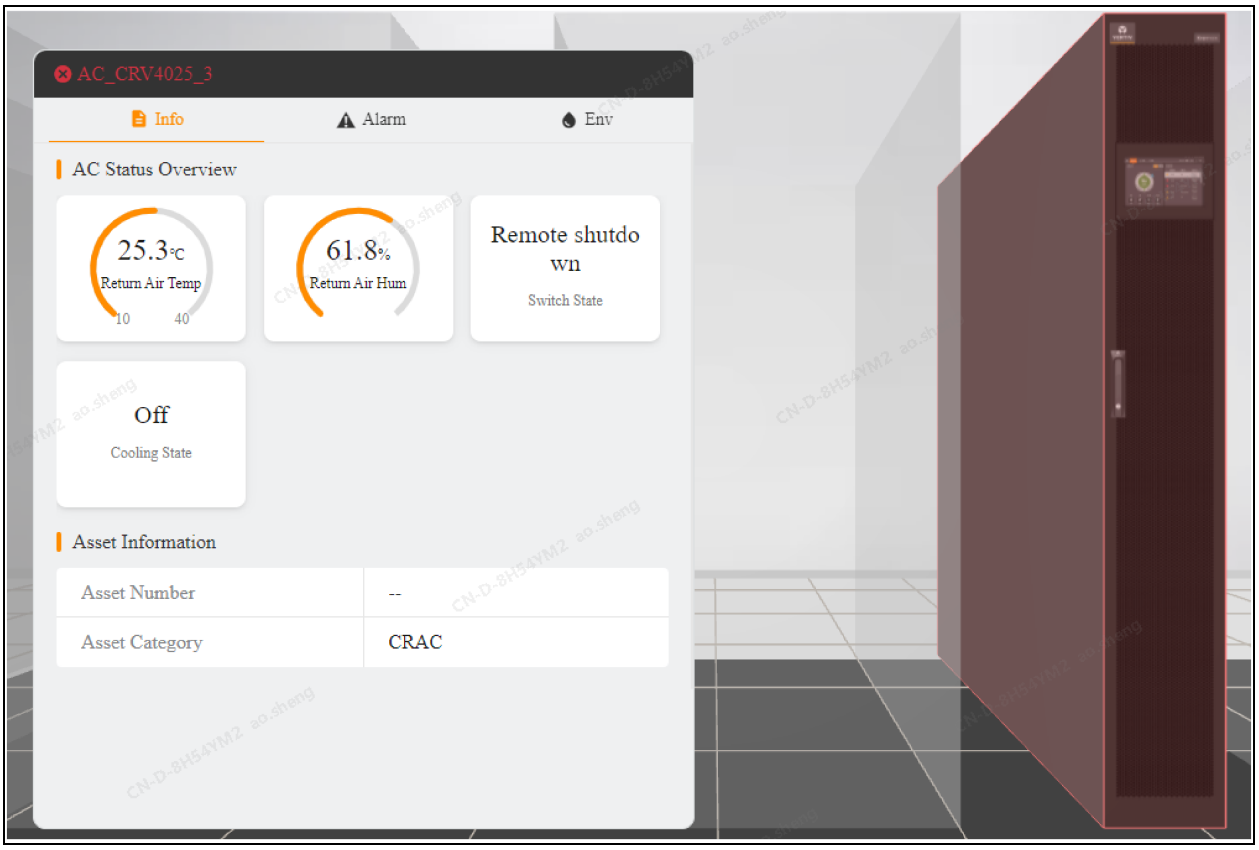
Figure 6.17 Basic Information Card of the UPS



© 2026 Vertiv Group Corp. All Rights Reserved.

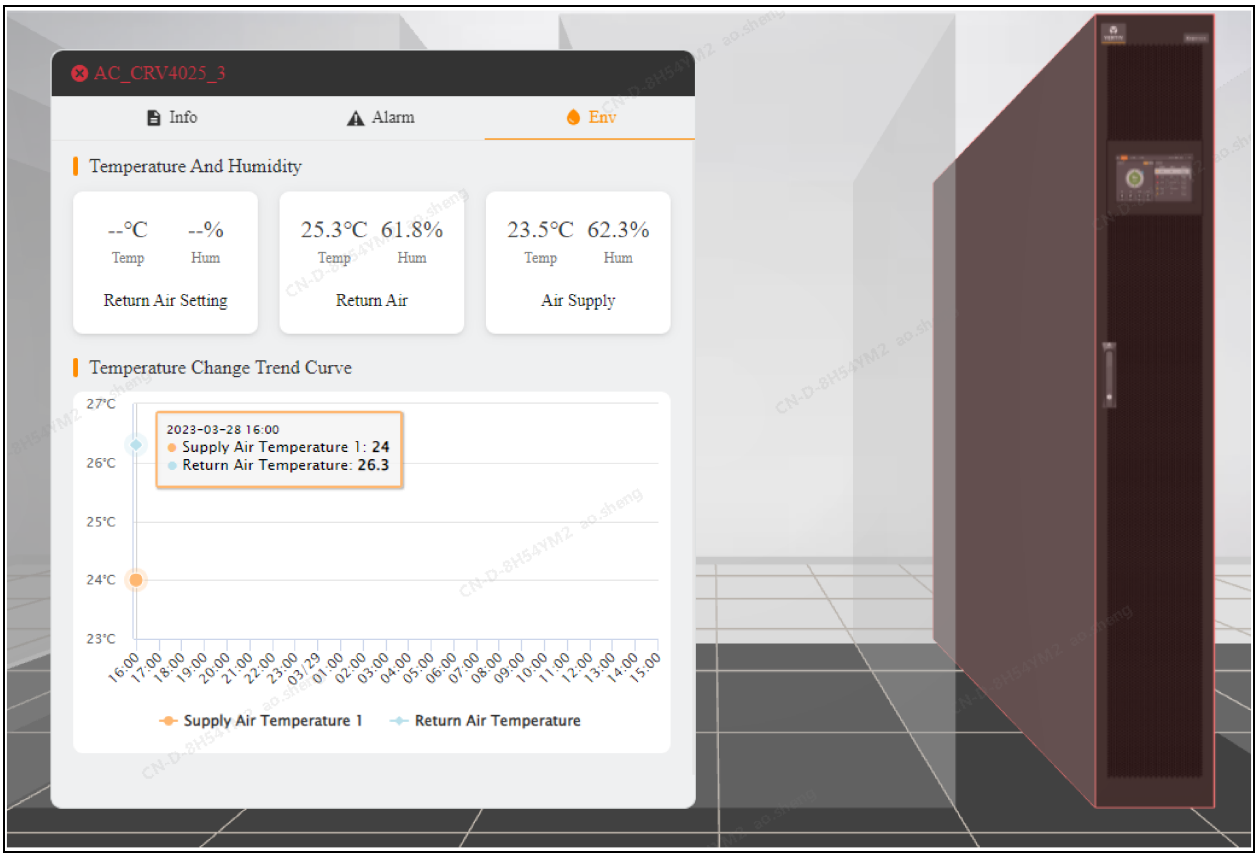
As shown in **Figure 6.18** below , the air conditioner's single cabinet houses three cards: basic status, alarm, and environment. The basic status card provides an overview of the air conditioner's status and asset information. The alarm card, similar to those for UPS and cabinet systems, displays current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

Figure 6.18 Air-conditioner Information



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.19 Air-condition Environment Card



The power distribution cabinet primarily contains three cards: basic information, alarm, and status. The basic information card primarily includes an overview of the SPM's status and the asset information for the added SPM. Alarm cards are similar to cabinets and UPS. The status card is a real-time power state diagram, that depicts the status of the branch and the TOP20. As shown in Basic Information Card of the SPM Cabinet .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.20 Basic Information Card of the SPM Cabinet

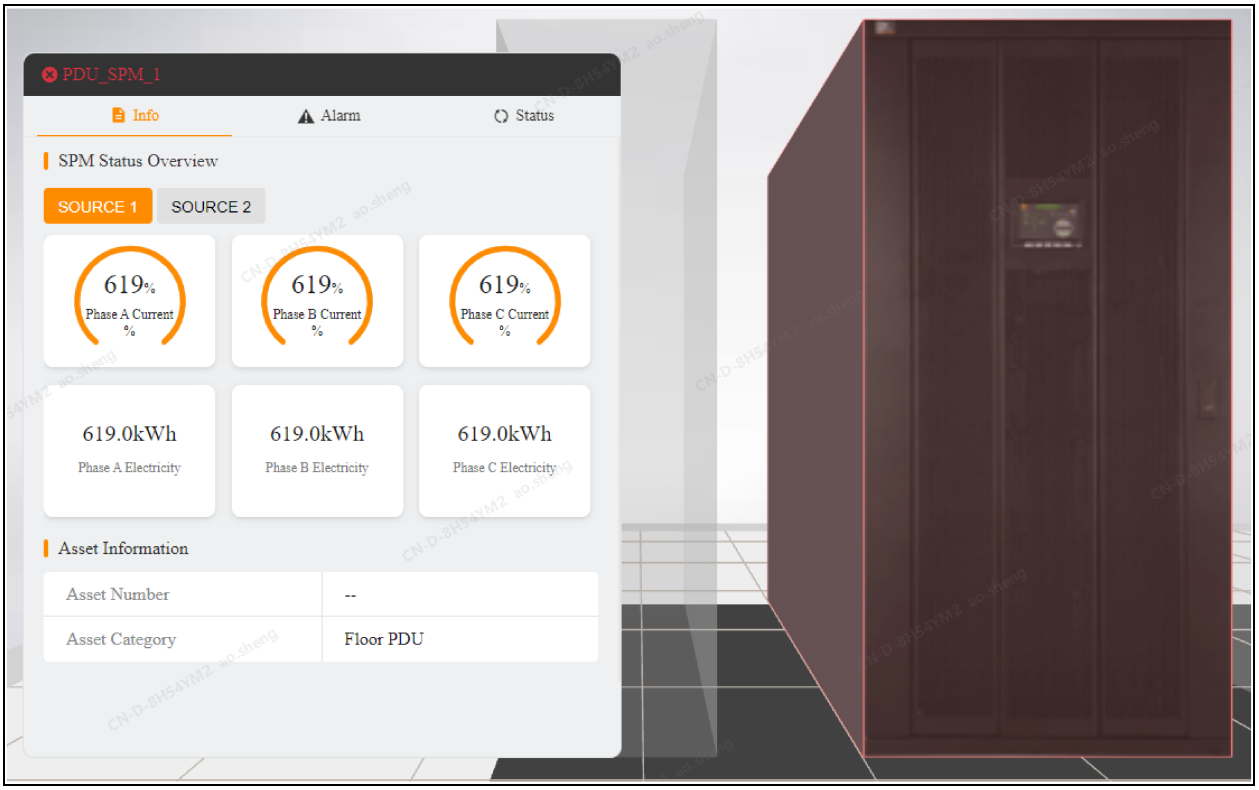


Figure 6.21 SPM Cabinet Status Card



© 2026 Vertiv Group Corp. All Rights Reserved.

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

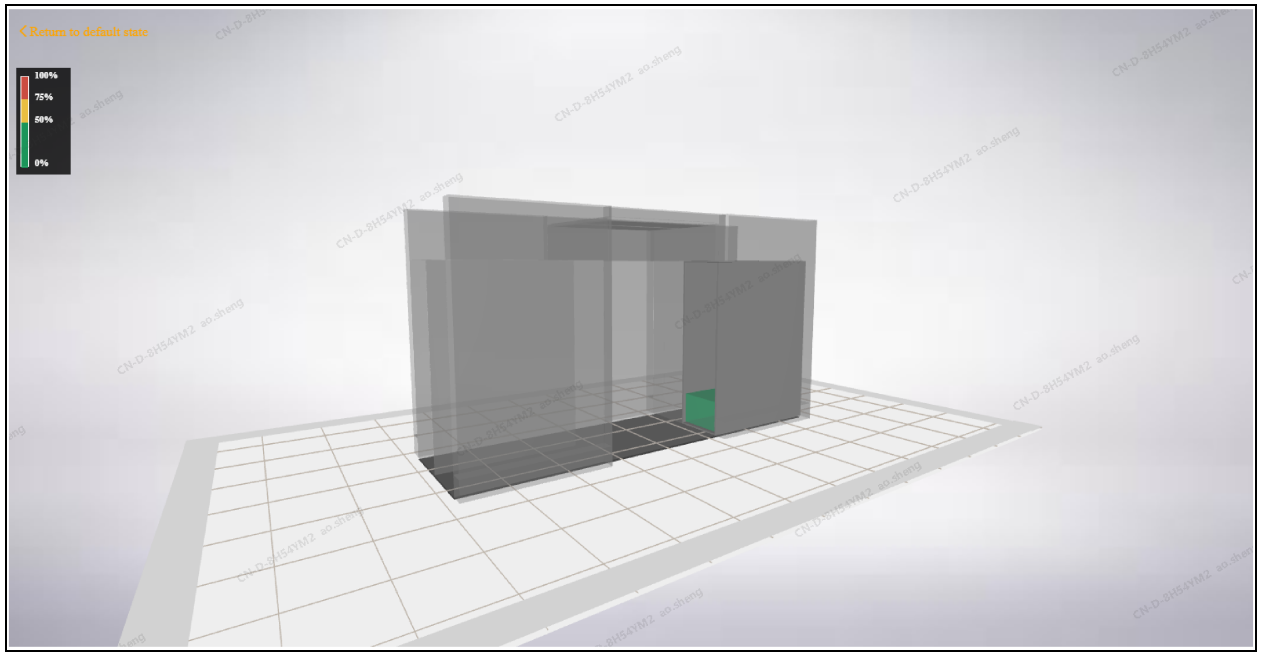
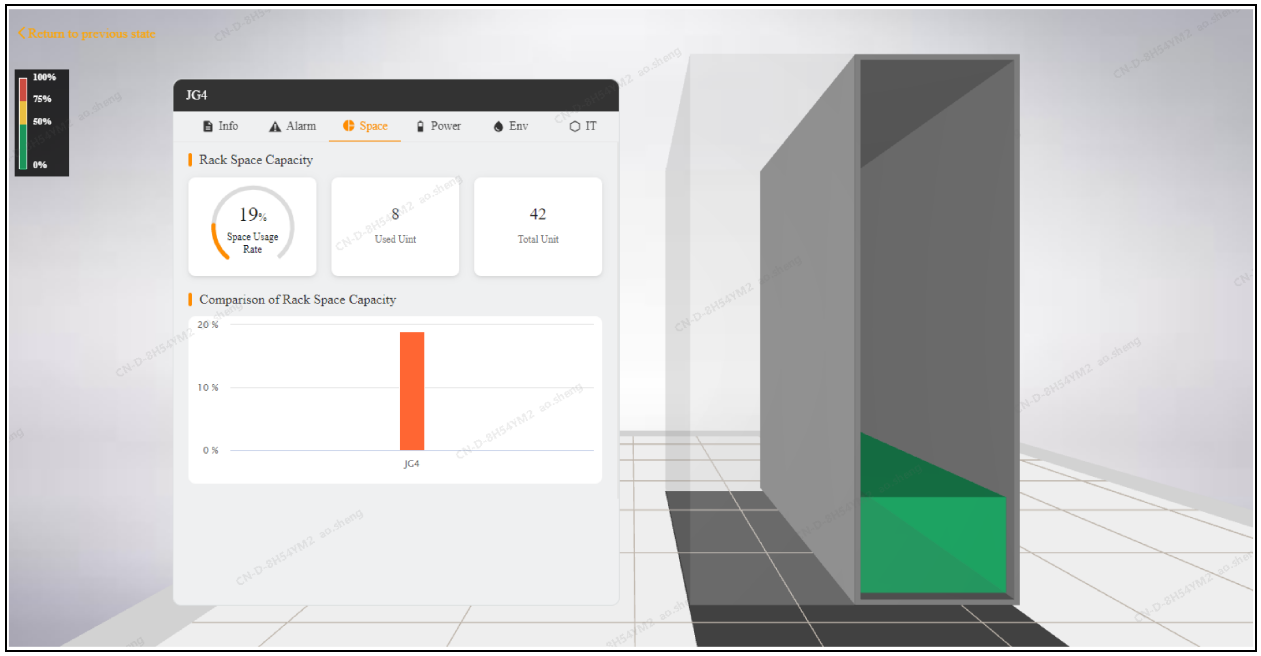


Figure 6.23 Cabinet Space Capacity



© 2026 Vertiv Group Corp. All Rights Reserved.

Power Capacity 3D Visualization

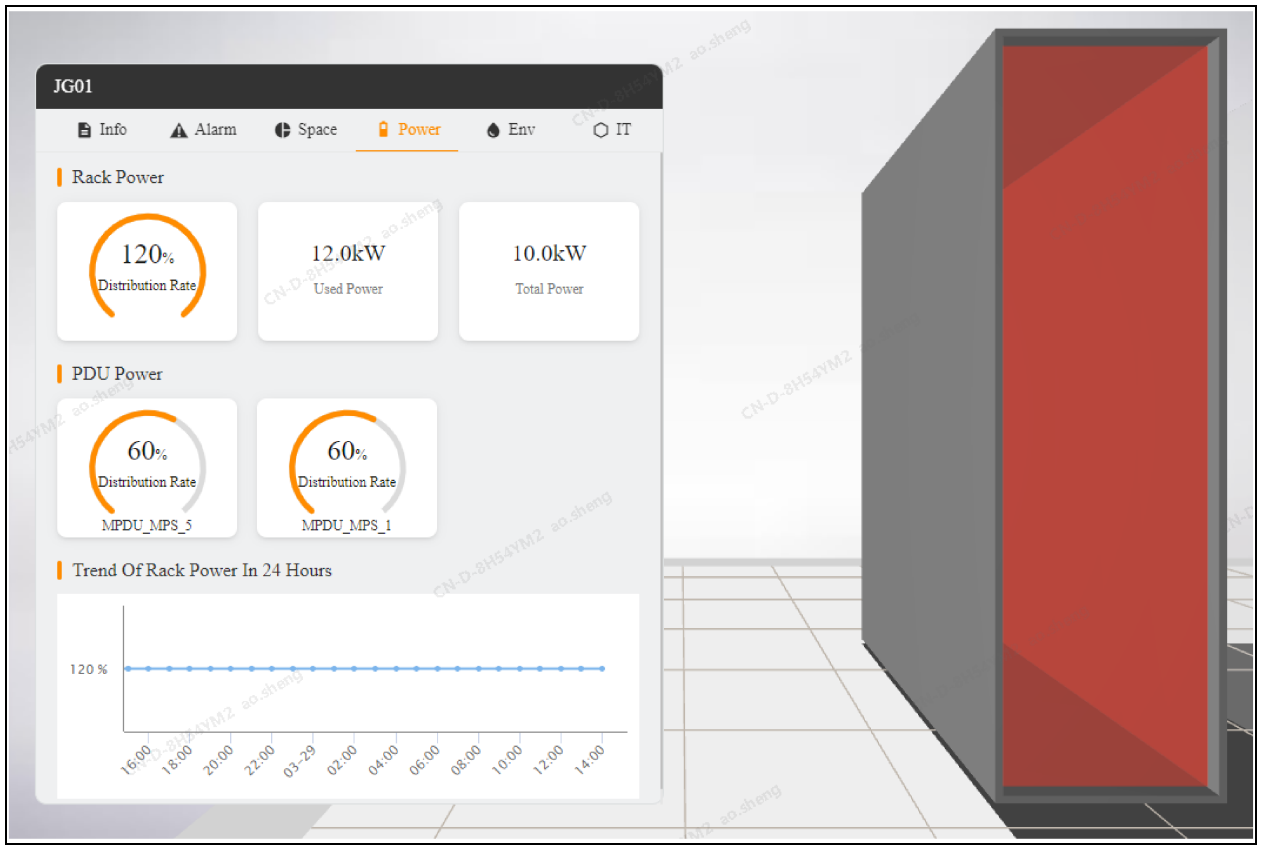
Navigate to the Power Capacity tab to access the 3D view, as shown in **Figure 6.24** below ,This view displays power distribution usage for each cabinet at the current site using color-coded 3D blocks. You can rotate, zoom, and pan the view. Click on a *cabinet* to focus on it (similar to Smart Aisle2.0's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

Figure 6.24 Smart Aisle2 Power Capacity View



© 2026 Vertiv Group Corp. All Rights Reserved.

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.26 Temperature Labels of Smart Aisle2

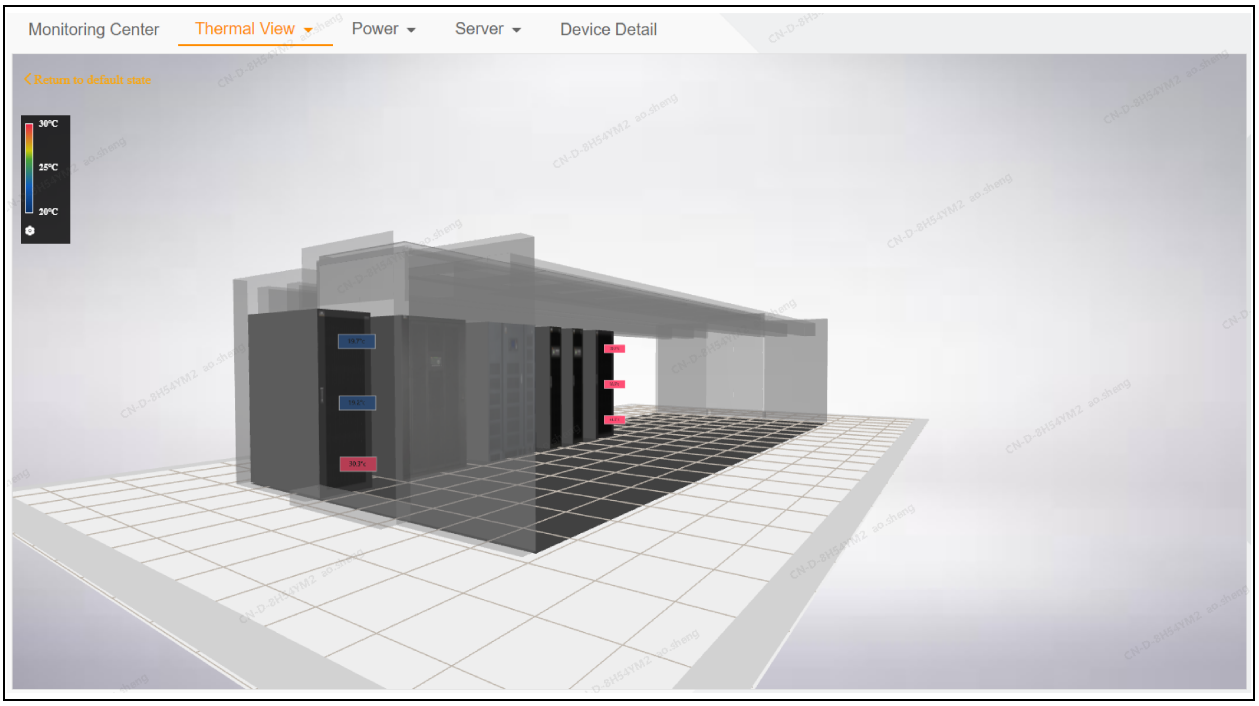
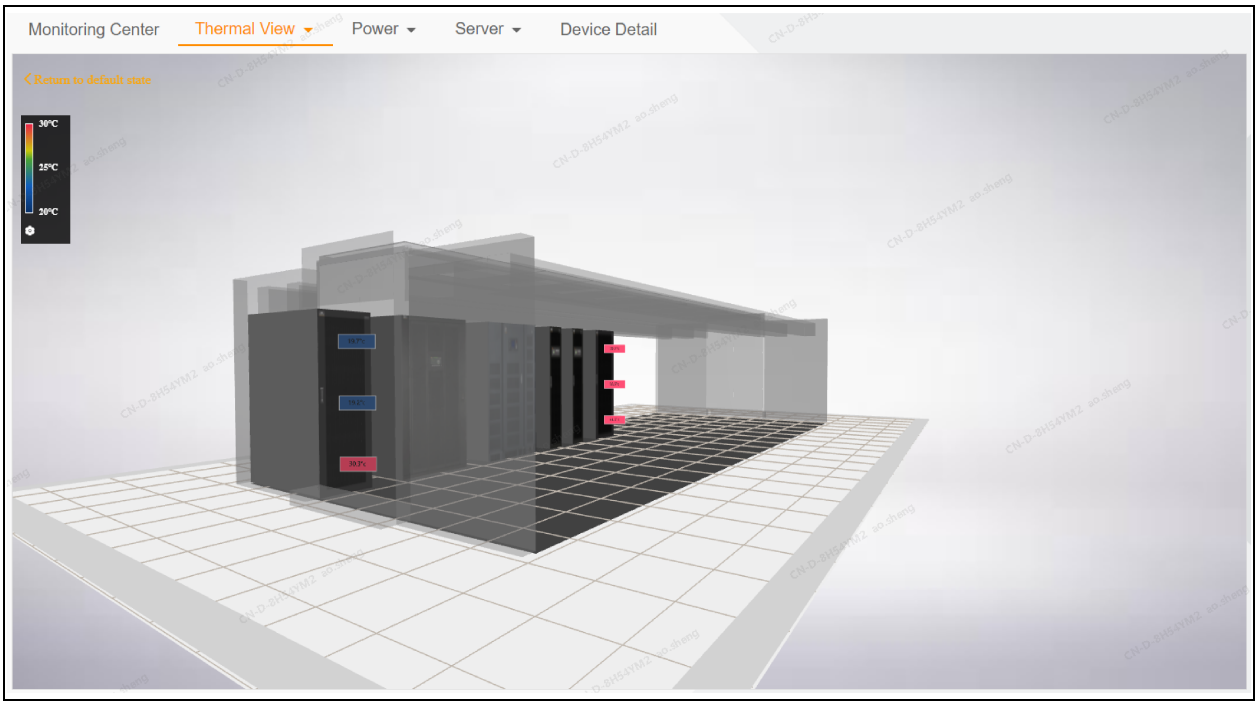


Figure 6.27 Temperature Label Detail



© 2026 Vertiv Group Corp. All Rights Reserved.

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

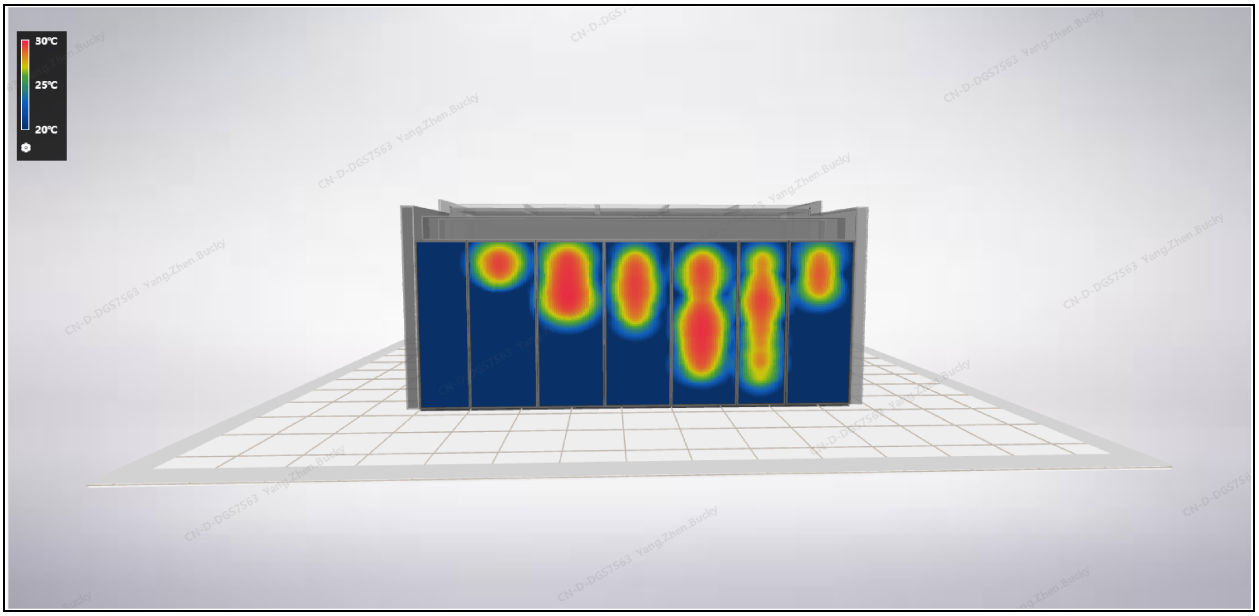


© 2026 Vertiv Group Corp. All Rights Reserved.

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 click on a device.

Figure 6.29 Smart Aisle2 Site Heat Map



6.2.2 Smart Aisle3 Site 3D Visualization

View 3D scenes of Smart Aisle3 sites, including space capacity, power capacity, temperature labels, and heat maps. To access the 3D model, click on a Smart Aisle3 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 View

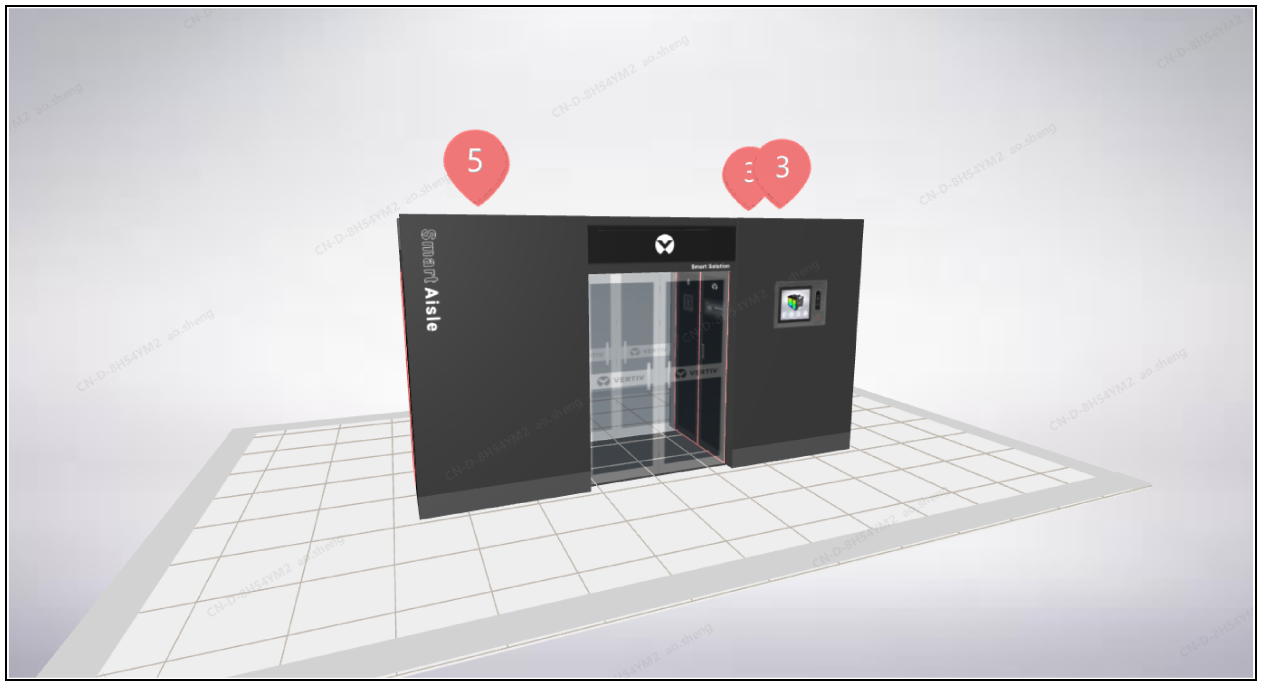
As shown in **Figure 6.30** on the next page , the 3D view of the Smart Aisle3 site, showing assets inside Smart Aisle3 and alarms. Users can navigate the 3D environment as follows:

- 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

The default view is illustrated in **Figure 6.30** on the next page .

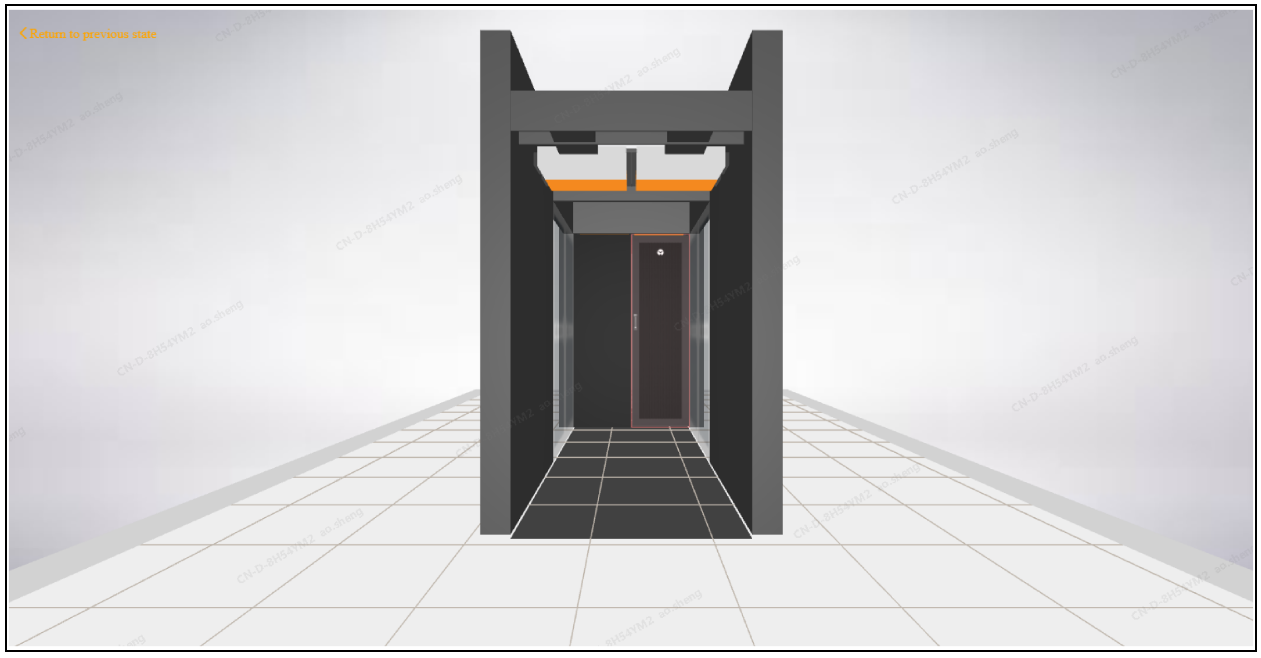
© 2026 Vertiv Group Corp. All Rights Reserved.

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



© 2026 Vertiv Group Corp. All Rights Reserved.

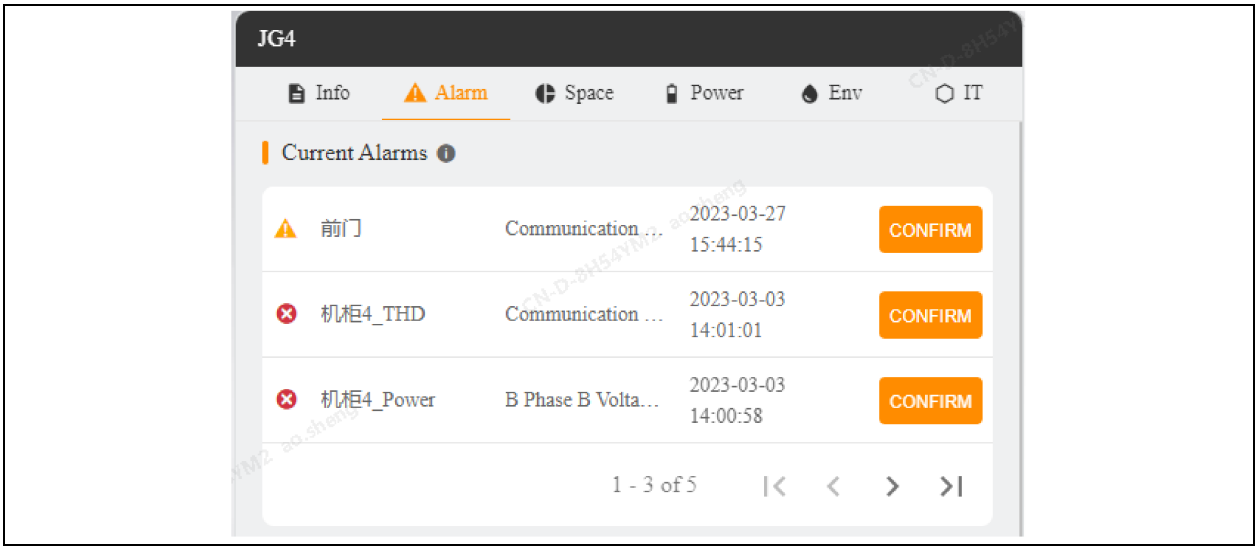
In the single-row view, click on *any cabinet* to access the single-cabinet view, as shown in the Figure 6.32 below . The left panel displays different perspectives about the cabinet, including basic details, alarms, space, power, environment, and IT categories. The basic information provides an overview 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 120 .

Figure 6.33 Alarm Card Content



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.34 Alarm Trend

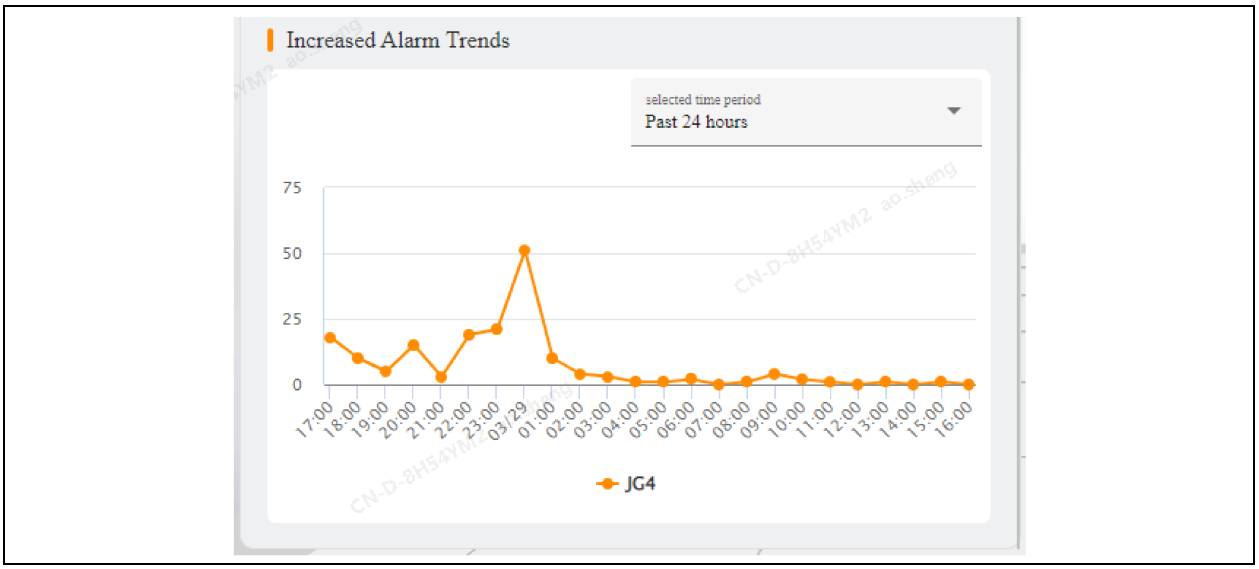
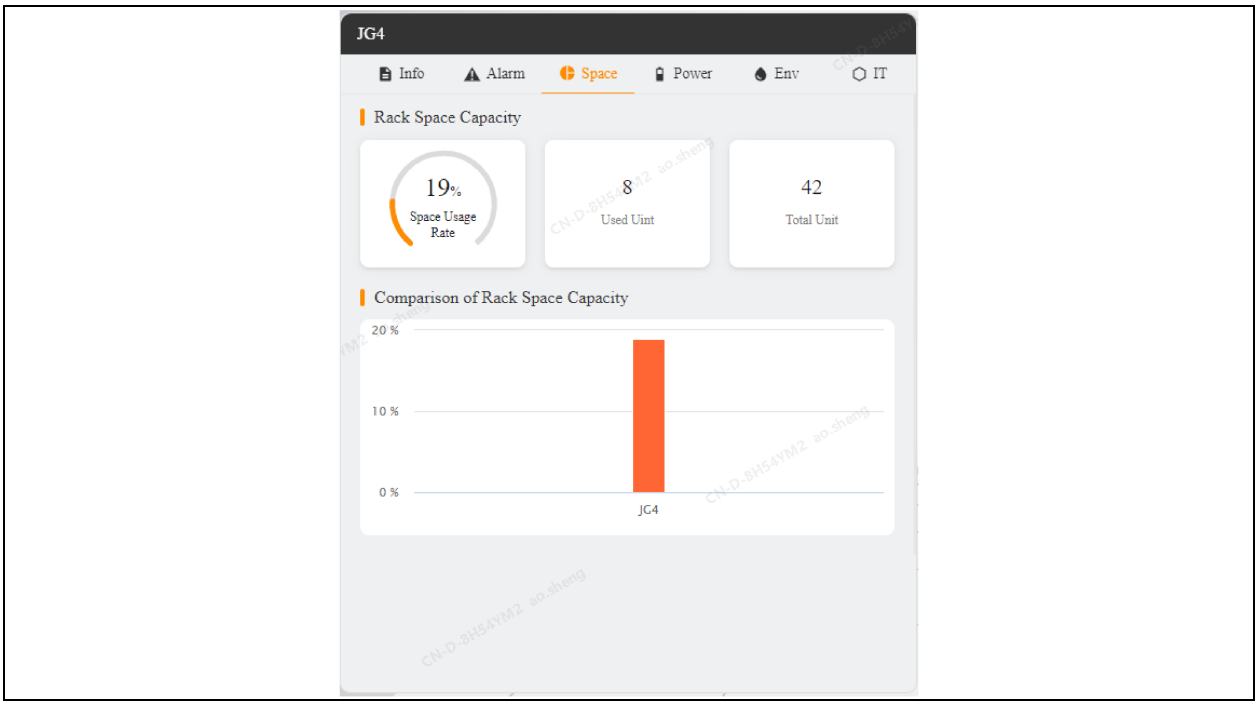


Figure 6.35 Space Usage

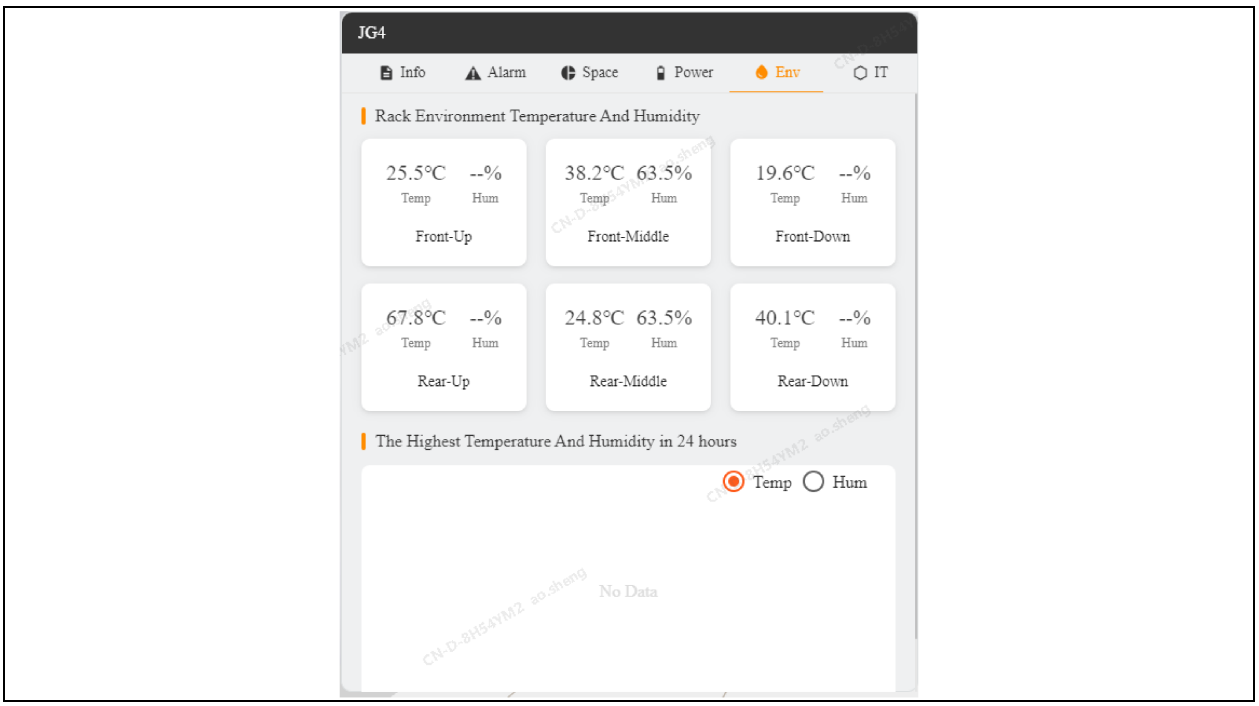


© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.36 Power Usage

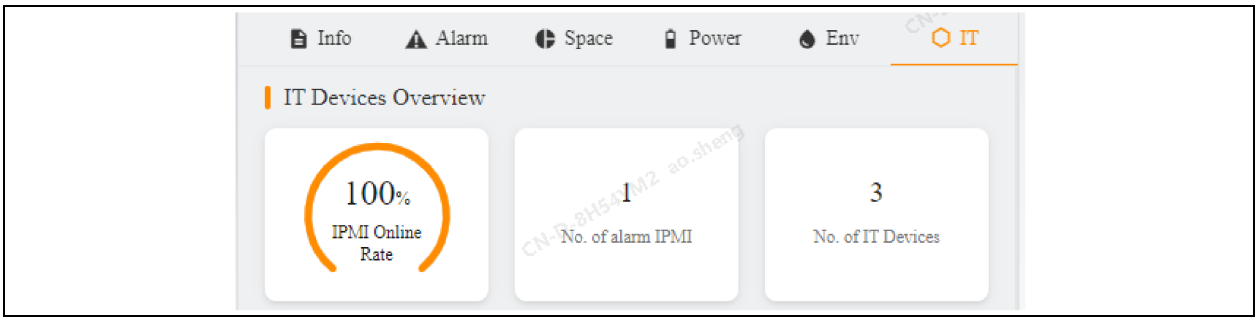


Figure 6.37 Environment Information



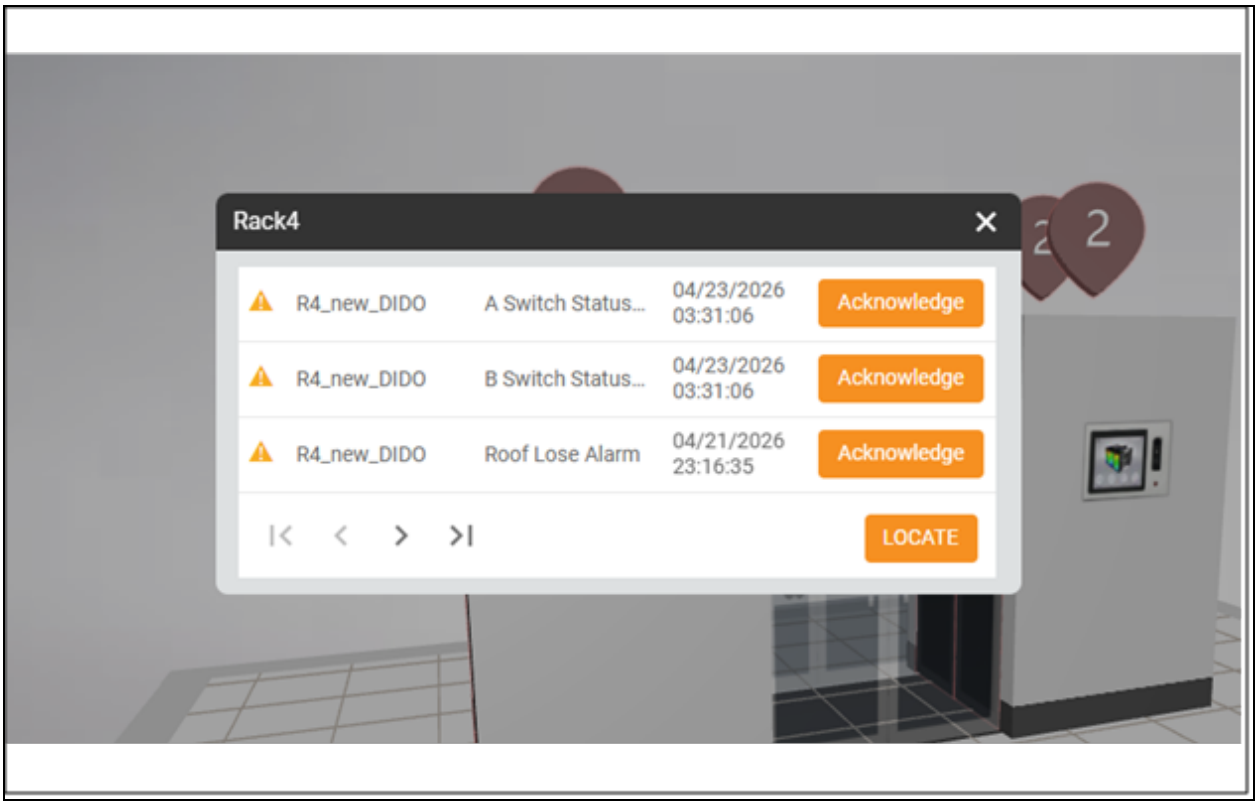
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.38 IT Devices Overview



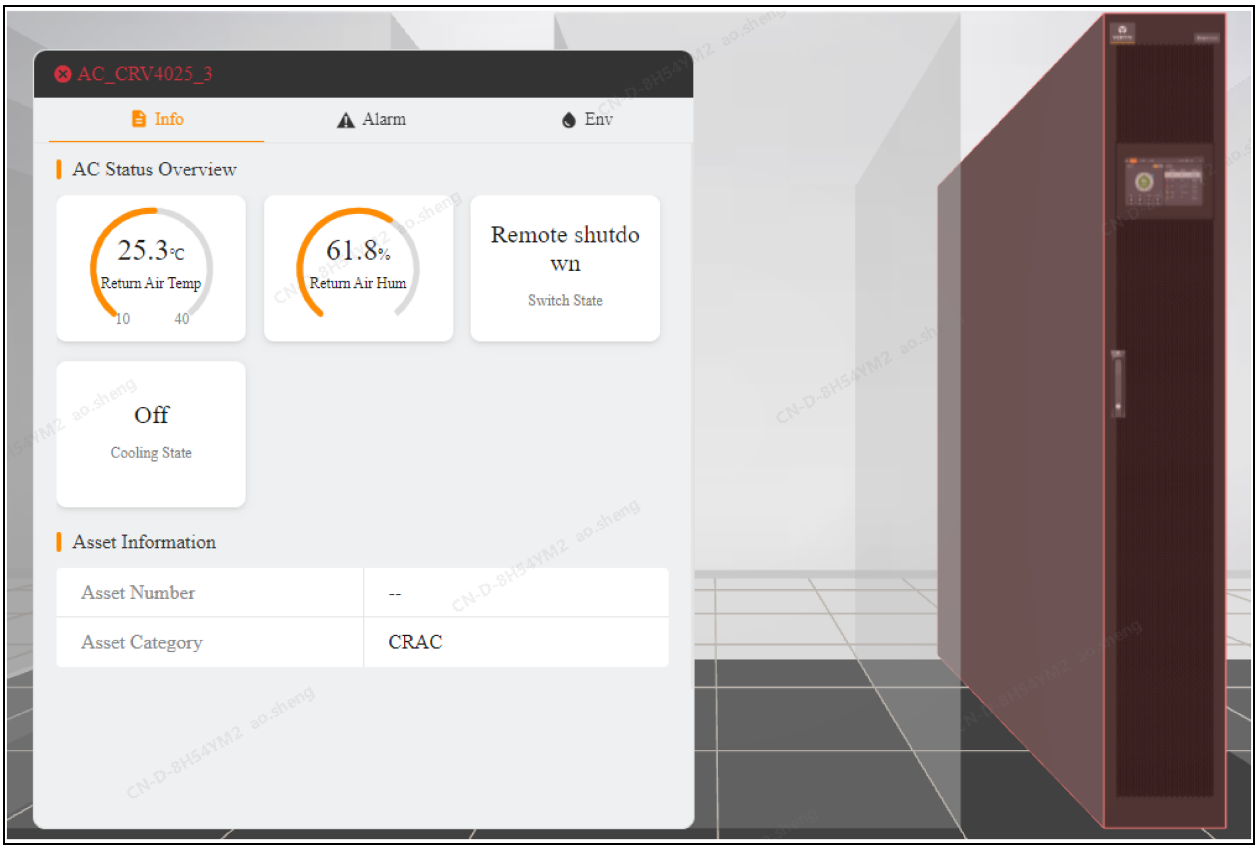
When an alarm exists on a device, it flashes red and there is an alarm bubble floating on the top, and you can click the *bubble* to know the alarm content and other information of the device. As shown in Figure 6.39 below .

Figure 6.39 Smart Aisle3 Site— Alarm Popup Window



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.40 Basic content of an Air Conditioner



The content of the Space Capacity, Power Capacity, Thermal View, and Heat Map modules is similar to that described in the Smart Row2 Site 3D Visualization below section.

6.2.3 Smart Row2 Site 3D Visualization

View 3D scenes of Smart Row2 sites, including space capacity, power capacity, temperature labels, and heat maps. To access the 3D model, click on an Smart Row2 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

As shown in **Figure 6.41** on the next page , the 3D view of the Smart Row2 site displays assets within Smart Row2 and associated 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

The default view is illustrated in **Figure 6.41** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.41 The Default 3D View of Smart Row Site

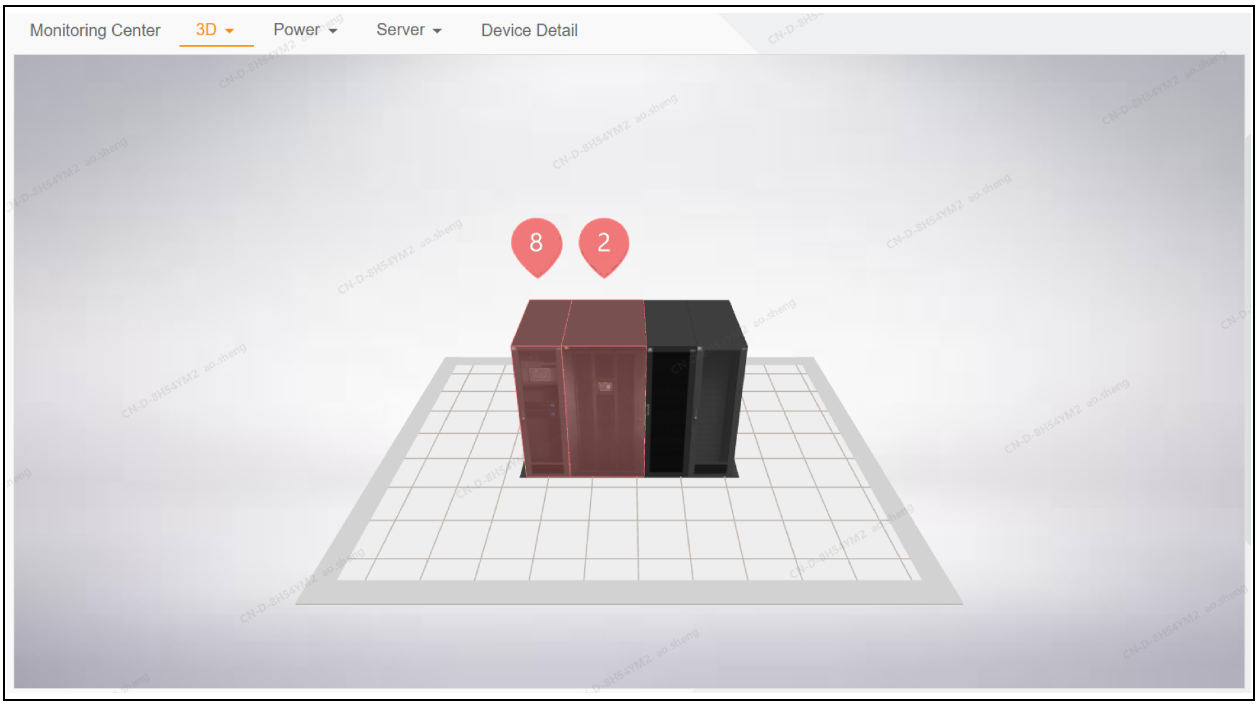
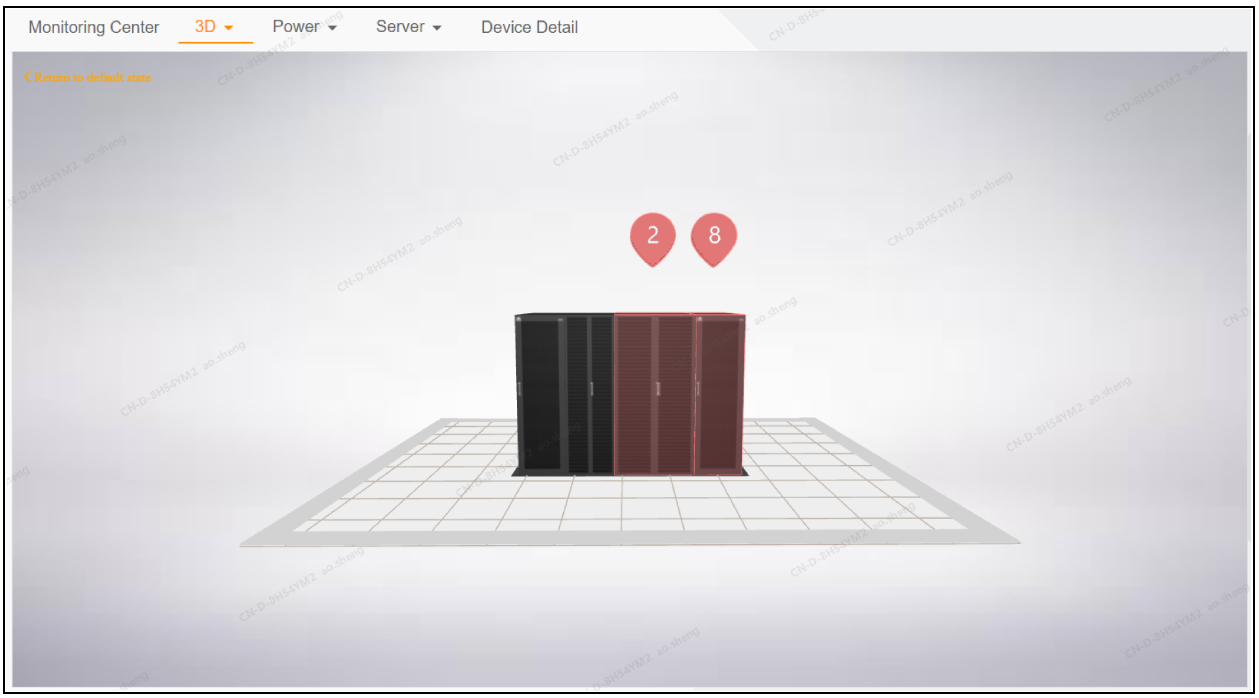


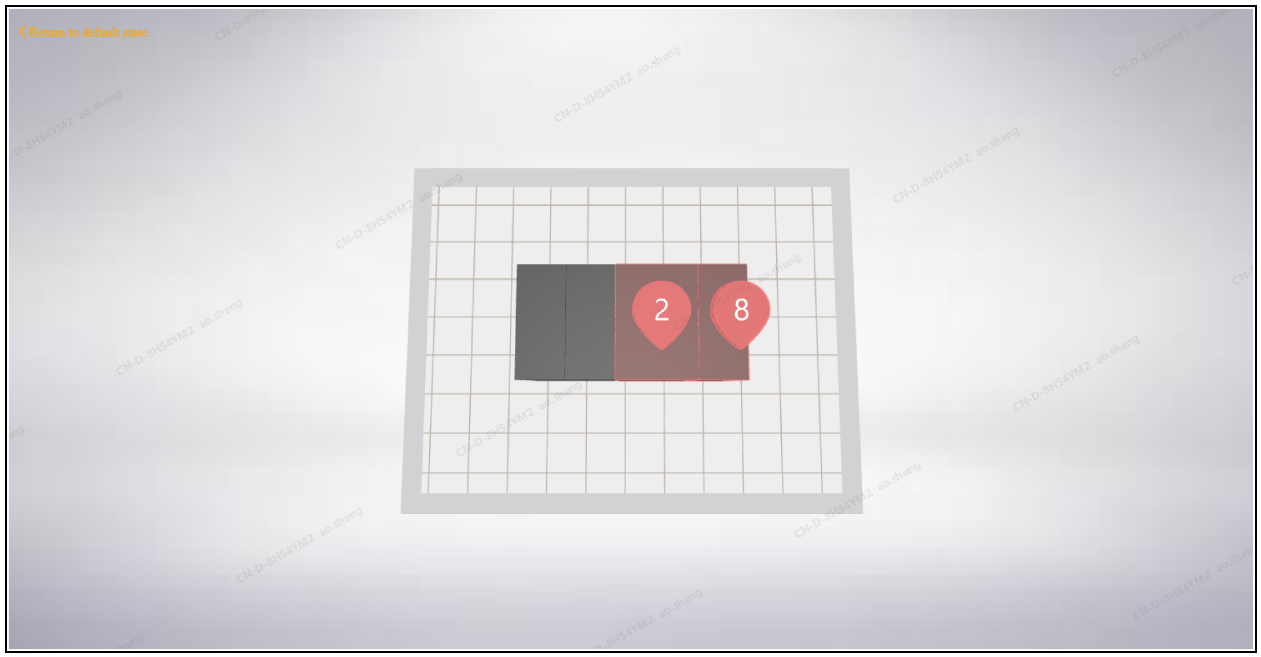
Figure 6.42 3D Back View of the Smart Row Site



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

© 2026 Vertiv Group Corp. All Rights Reserved.

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

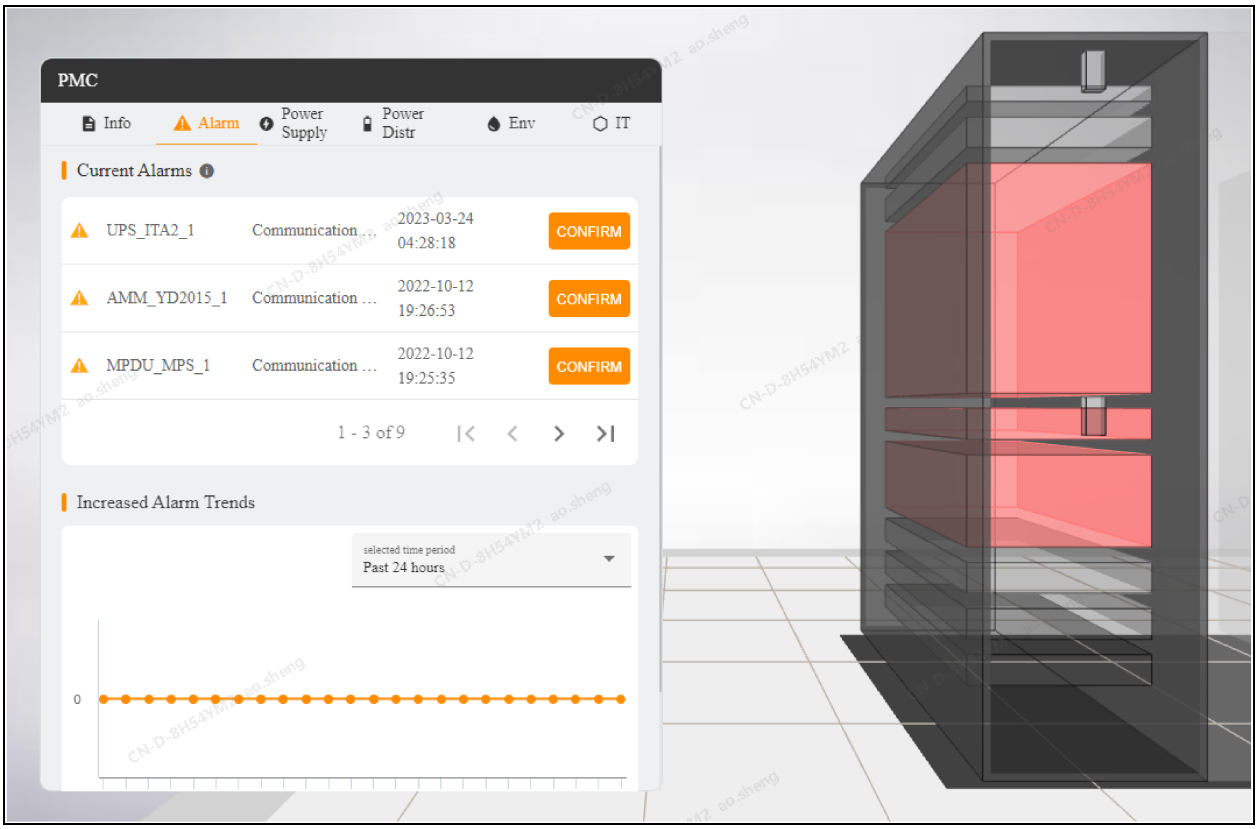
Figure 6.44 Single-Cabinet View of the PMC Cabinet at the Smart Row Site



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 129 .

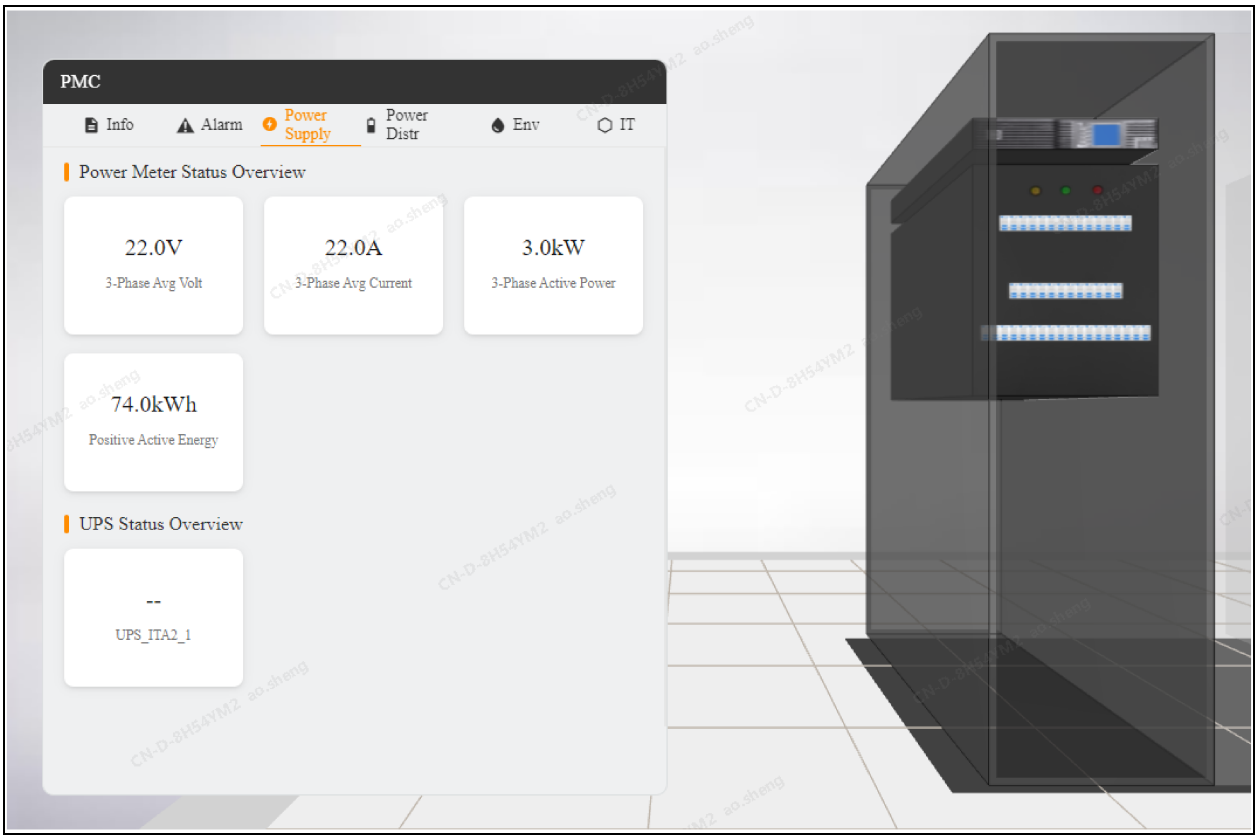
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.45 Alarm Card of the PMC Cabinet



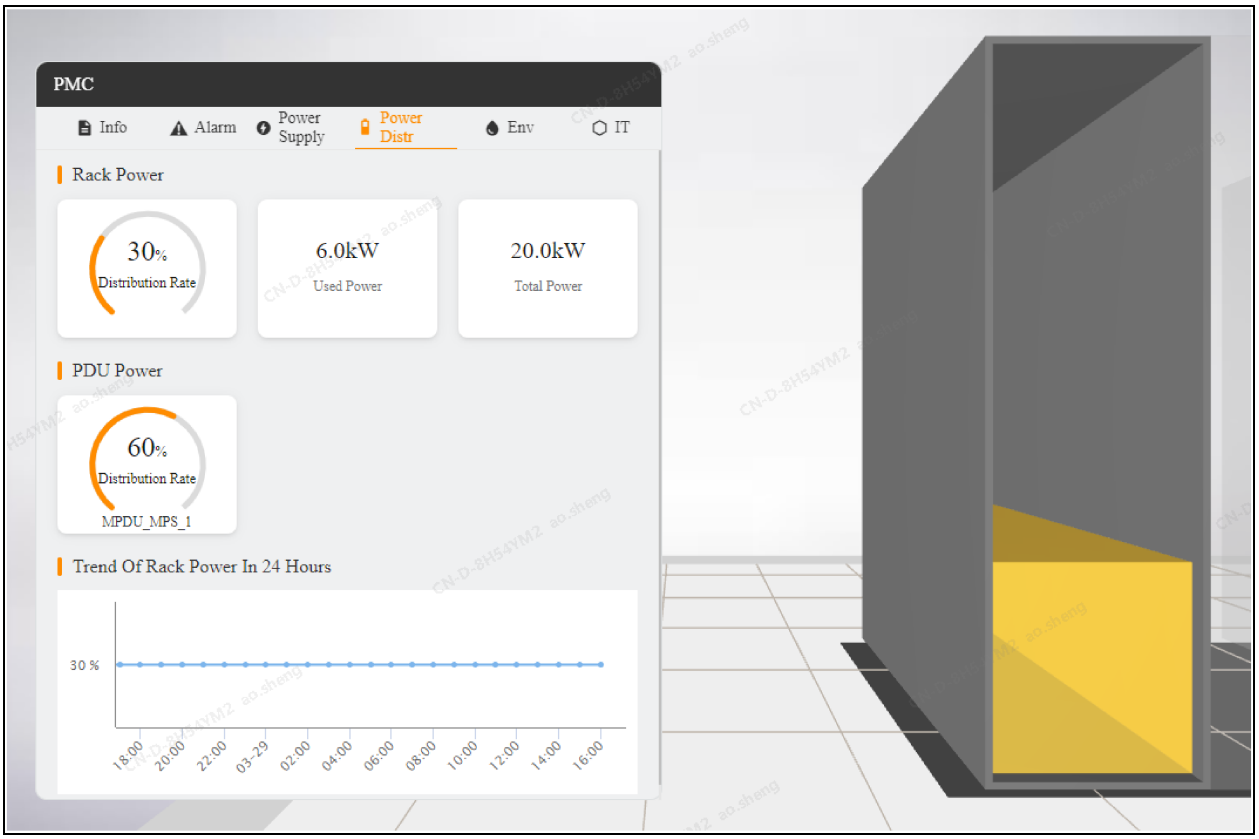
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.46 Power Supply Card of the PMC Cabinet is Displayed



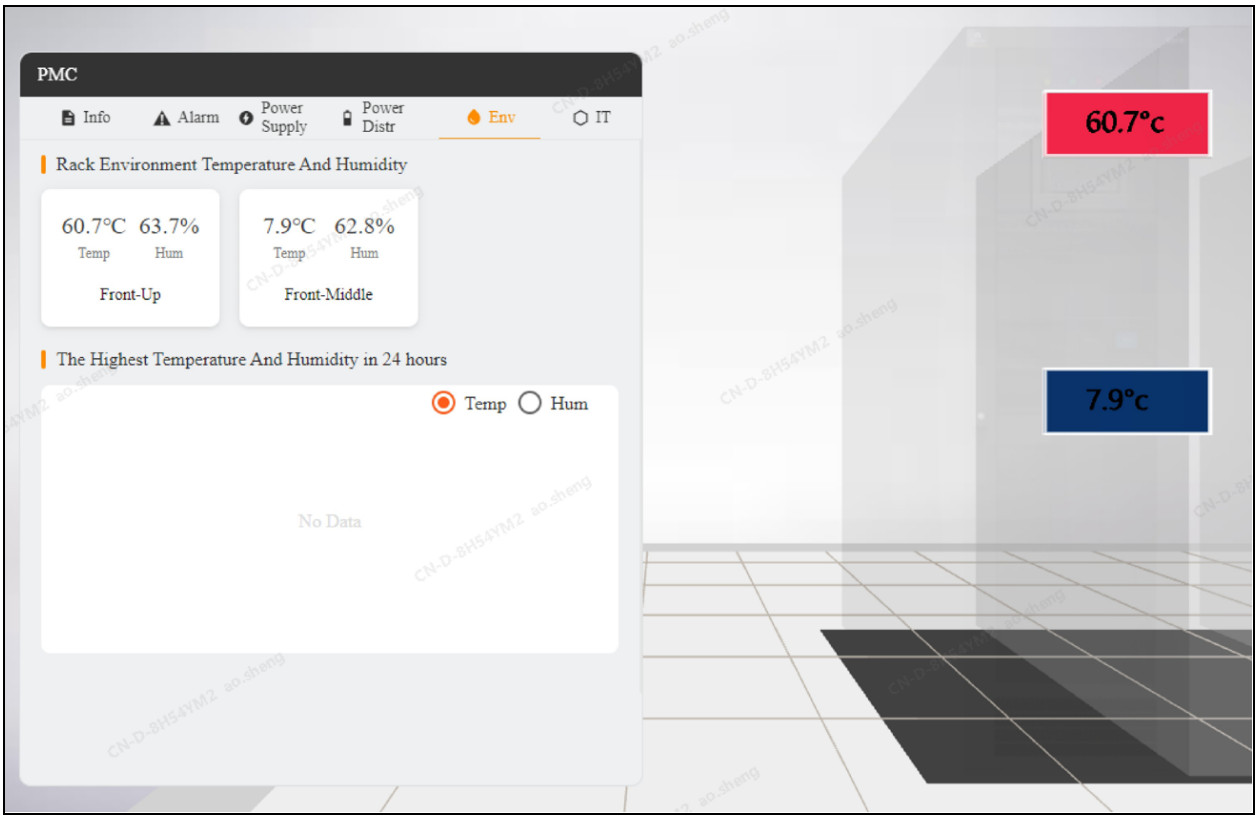
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.47 Power Distribution Card of the PMC Cabinet



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.48 PMC Cabinet Environment Card



© 2026 Vertiv Group Corp. All Rights Reserved.

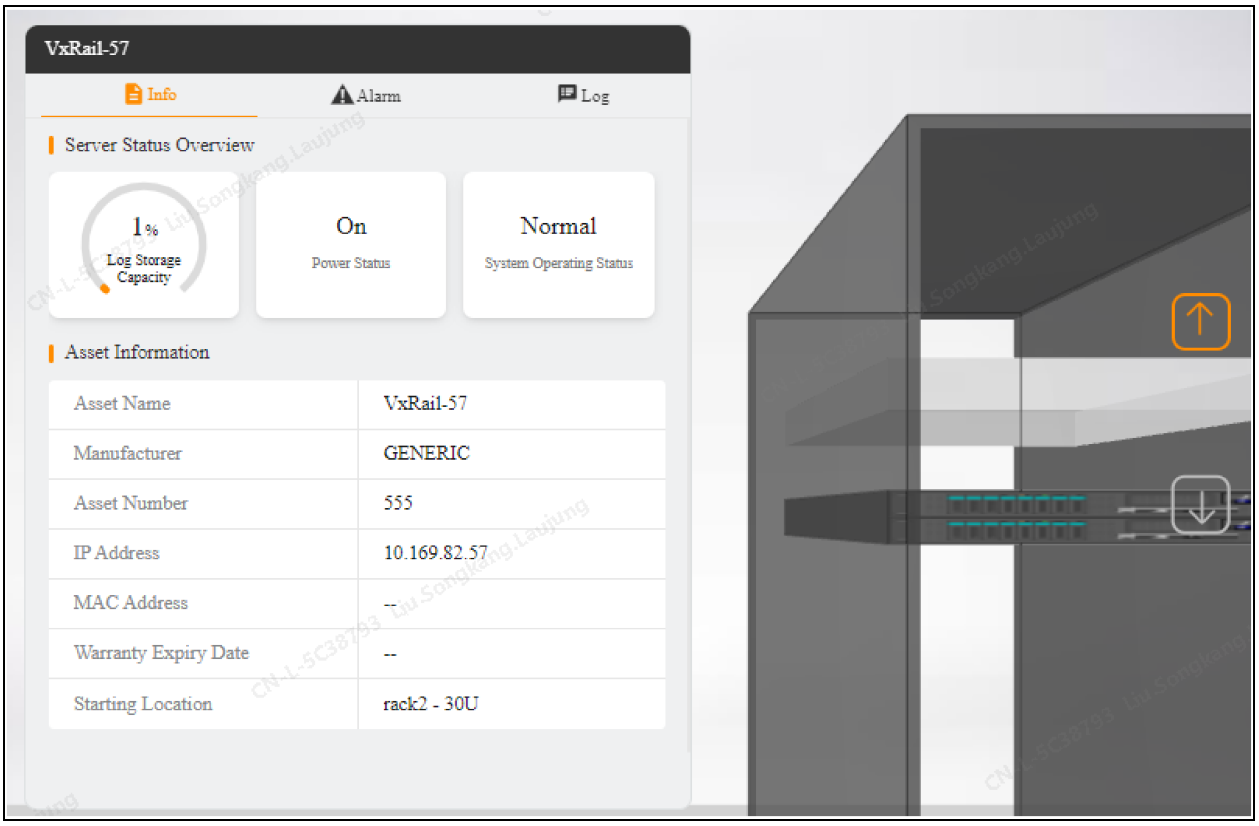
Figure 6.49 IT Card of the PMC Cabinet



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

© 2026 Vertiv Group Corp. All Rights Reserved.

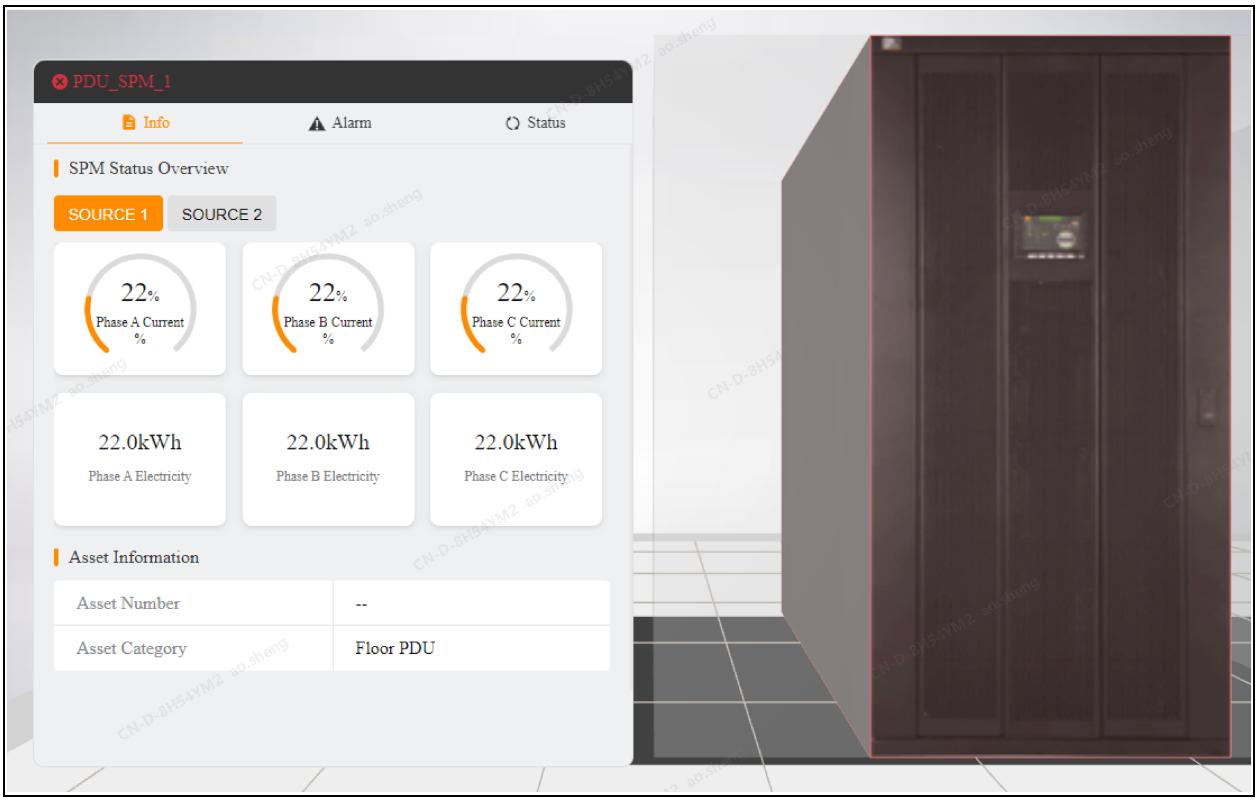
Figure 6.50 View of the Smart Row Site Server



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.

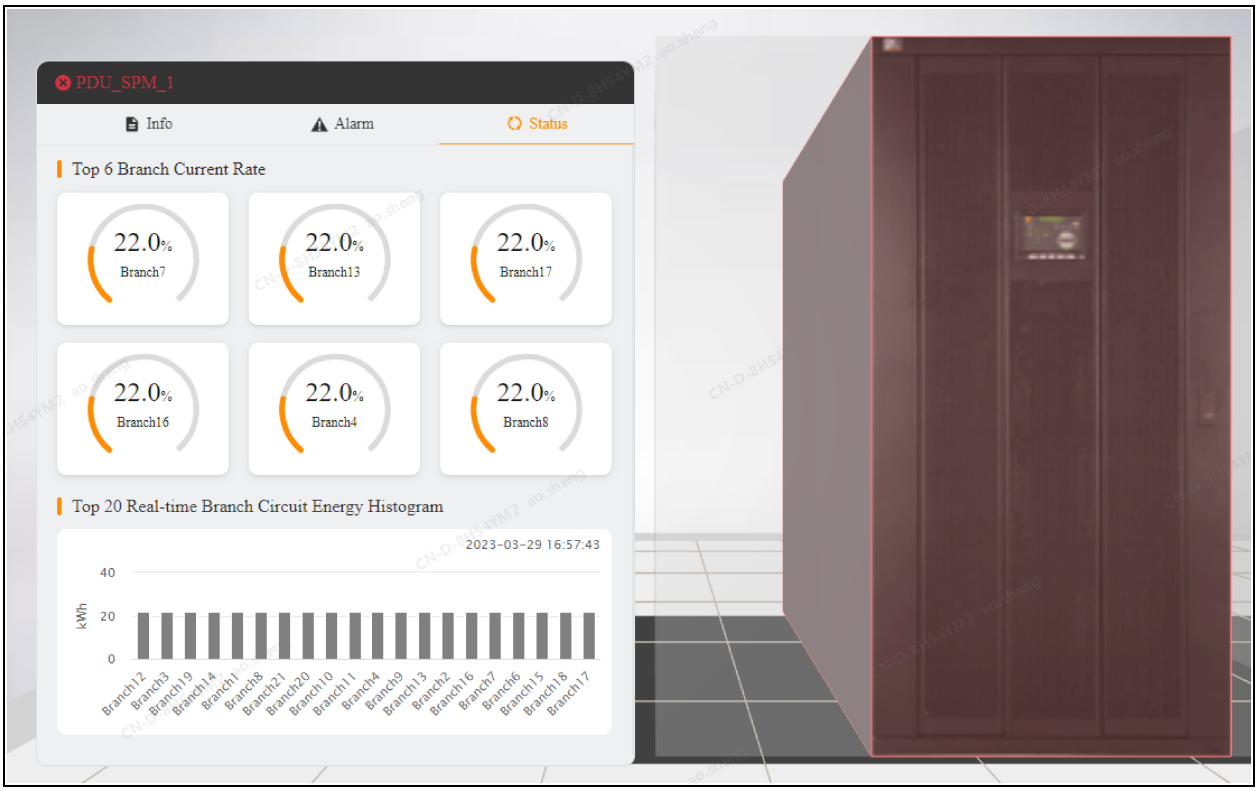
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.51 Basic Information and Cards of the SPM Cabinet



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.52 SPM Cabinet Status Card

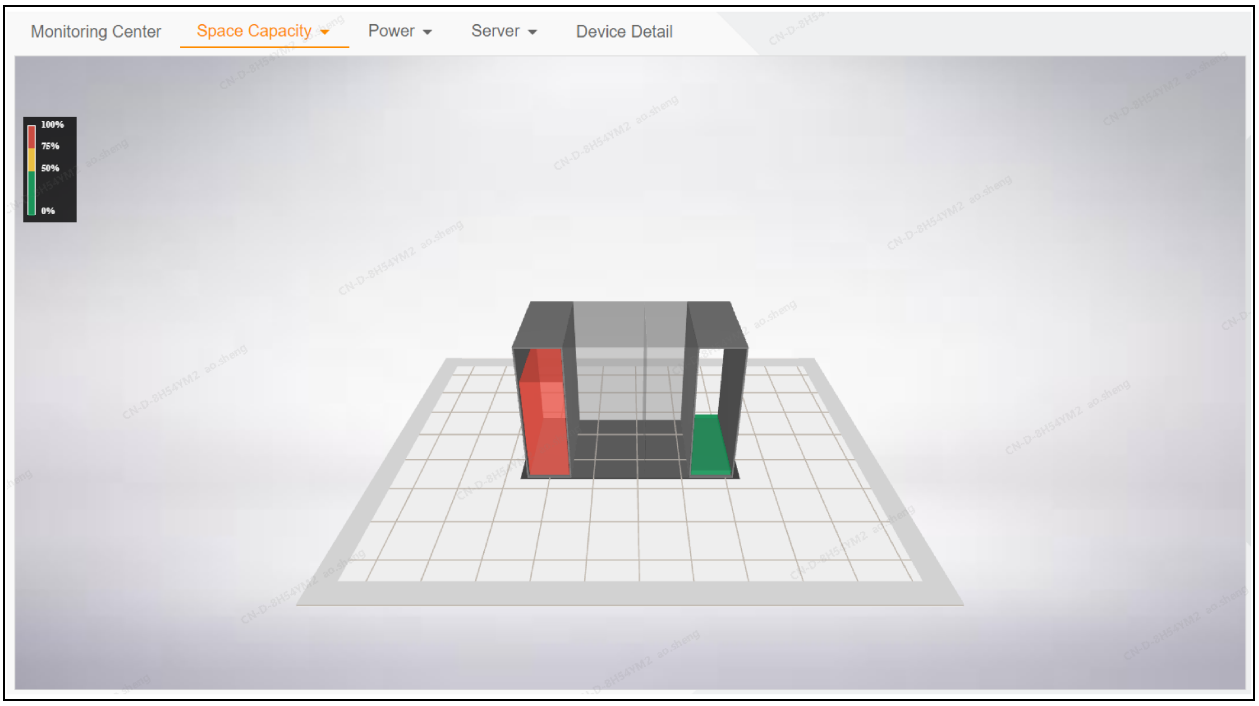


Space 3D View

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.54 Power Capacity 3D View of Smart Row Site

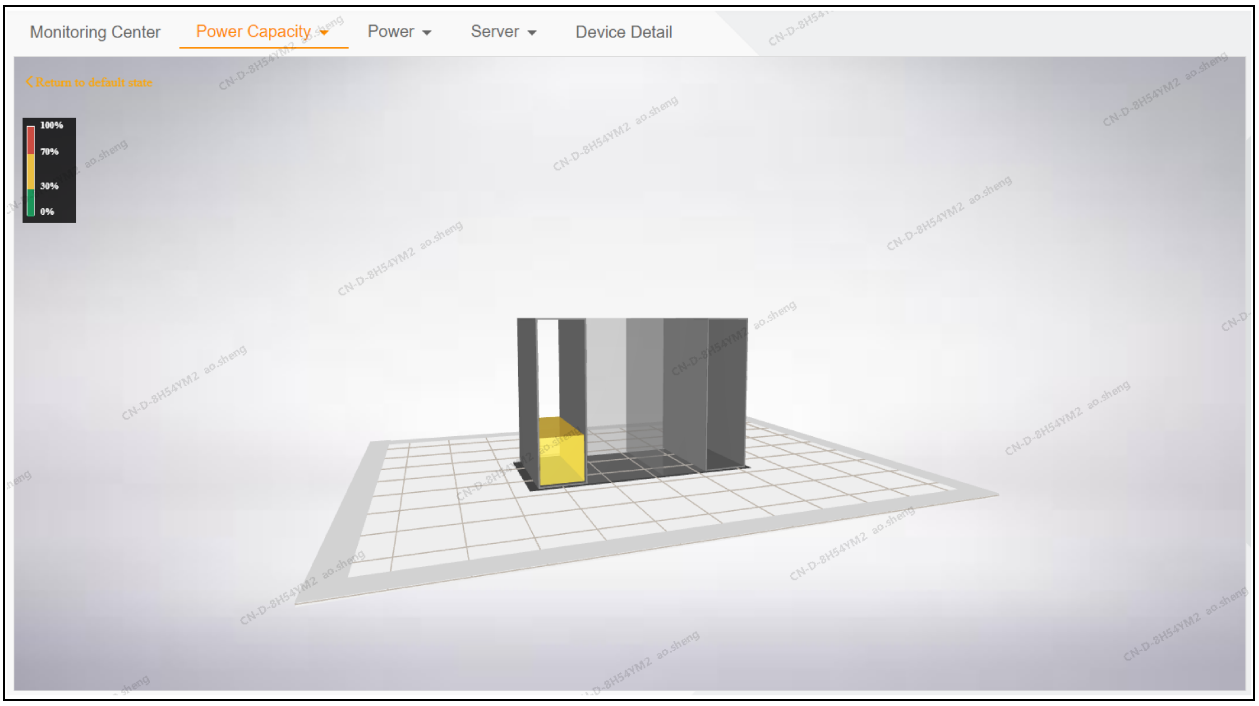
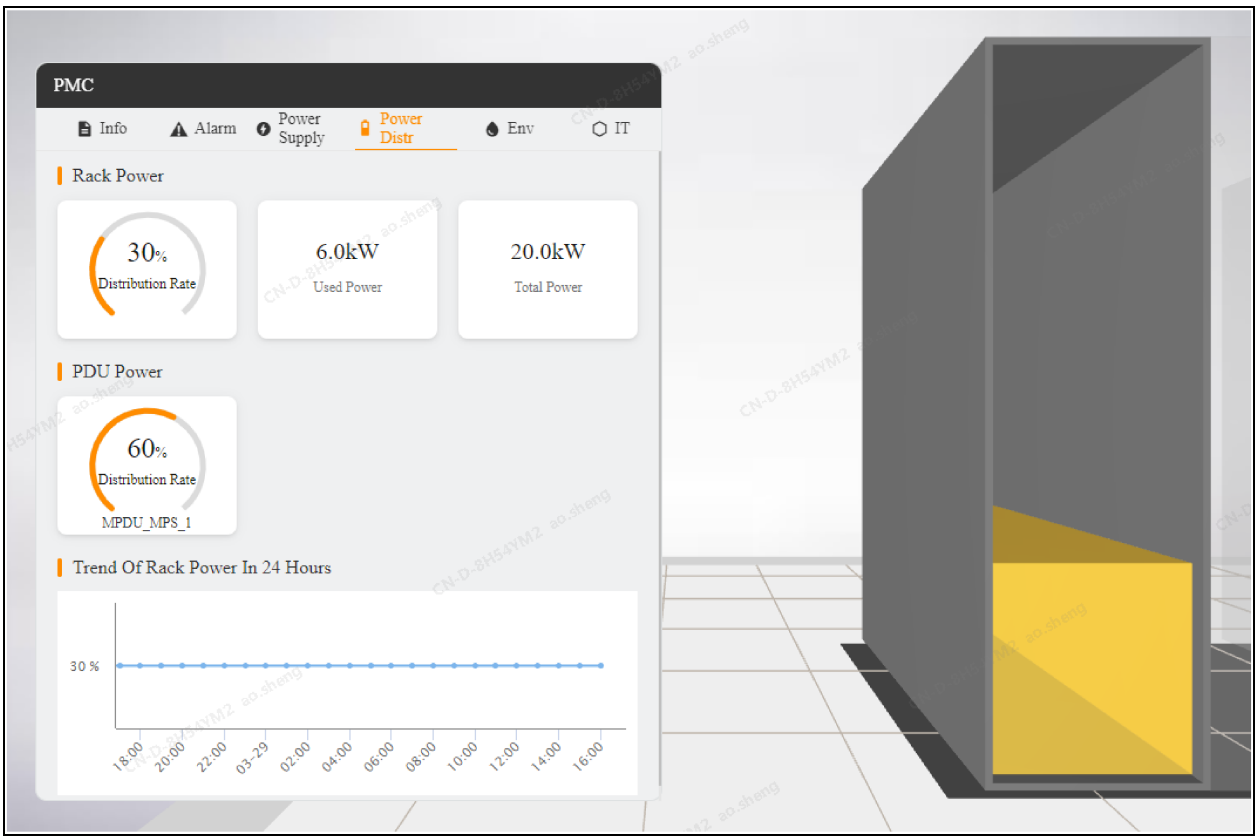


Figure 6.55 Power Capacity of a PMC Cabinet

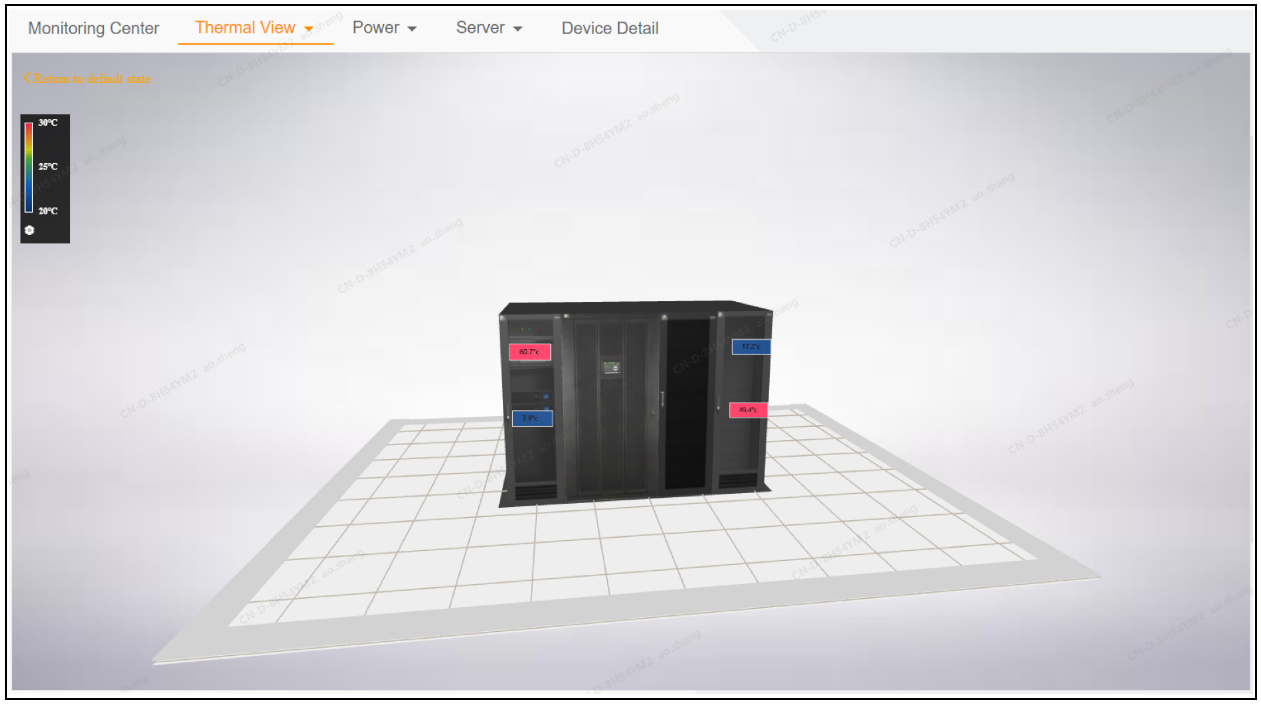


© 2026 Vertiv Group Corp. All Rights Reserved.

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



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.57 Temperature Label and Environmental Information of a PMC Cabinet

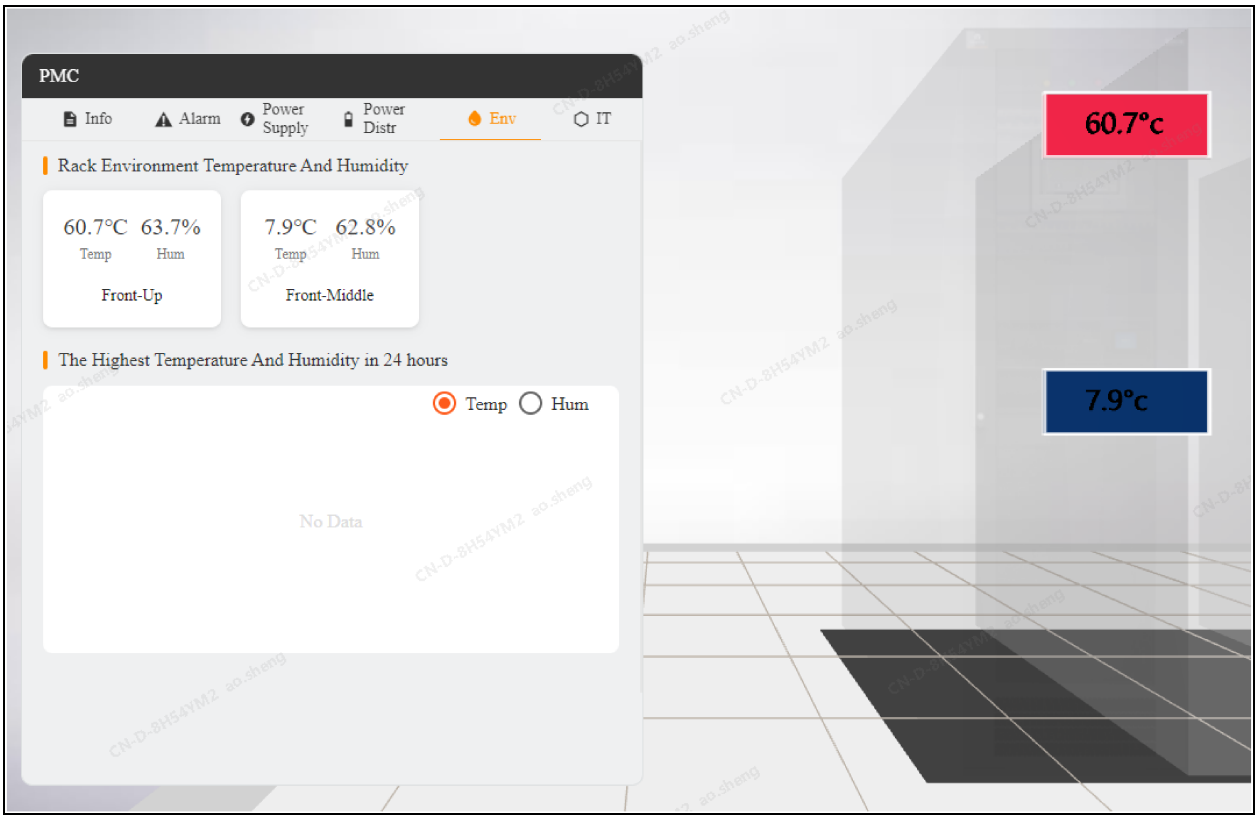


Figure 6.58 The color of the Label Changes after Adjusting the Temperature Range

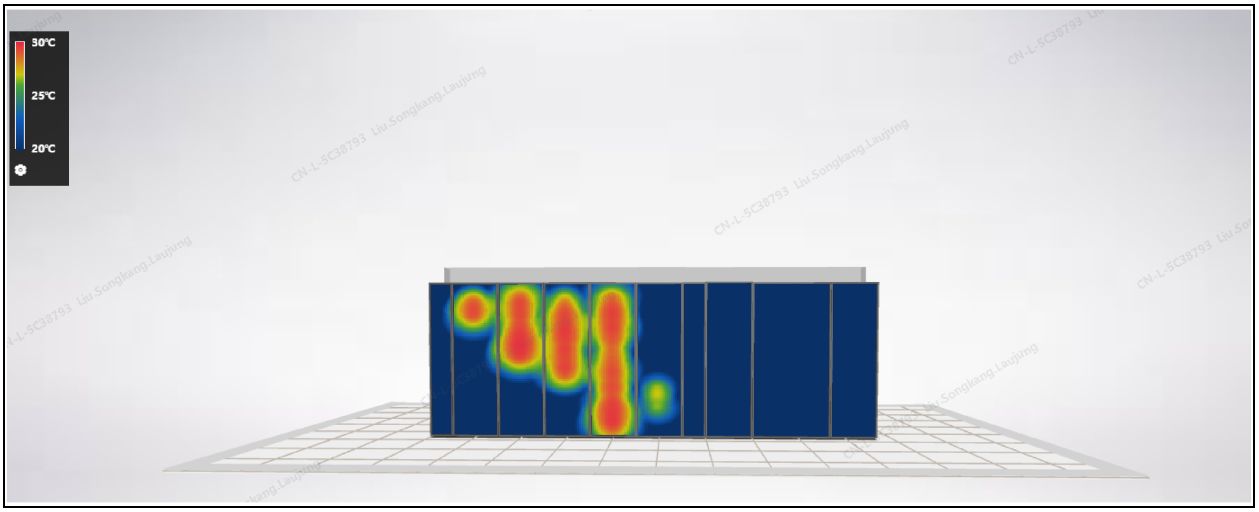


© 2026 Vertiv Group Corp. All Rights Reserved.

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.

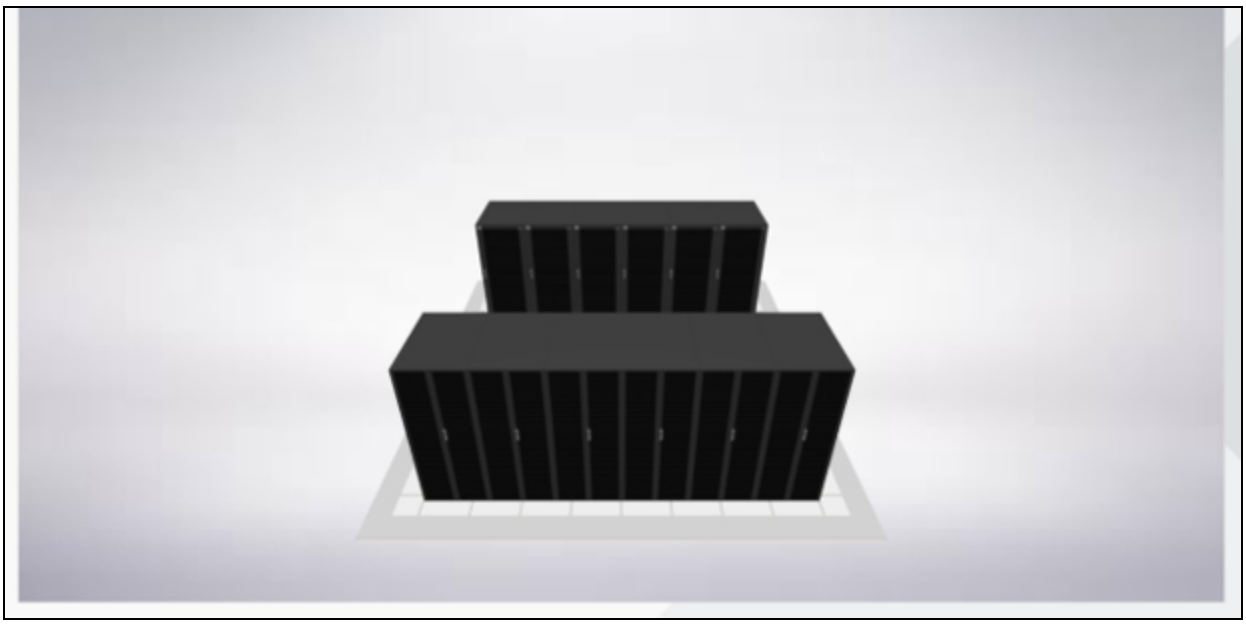
Figure 6.59 Heat Map 3D View of Smart Row Site



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

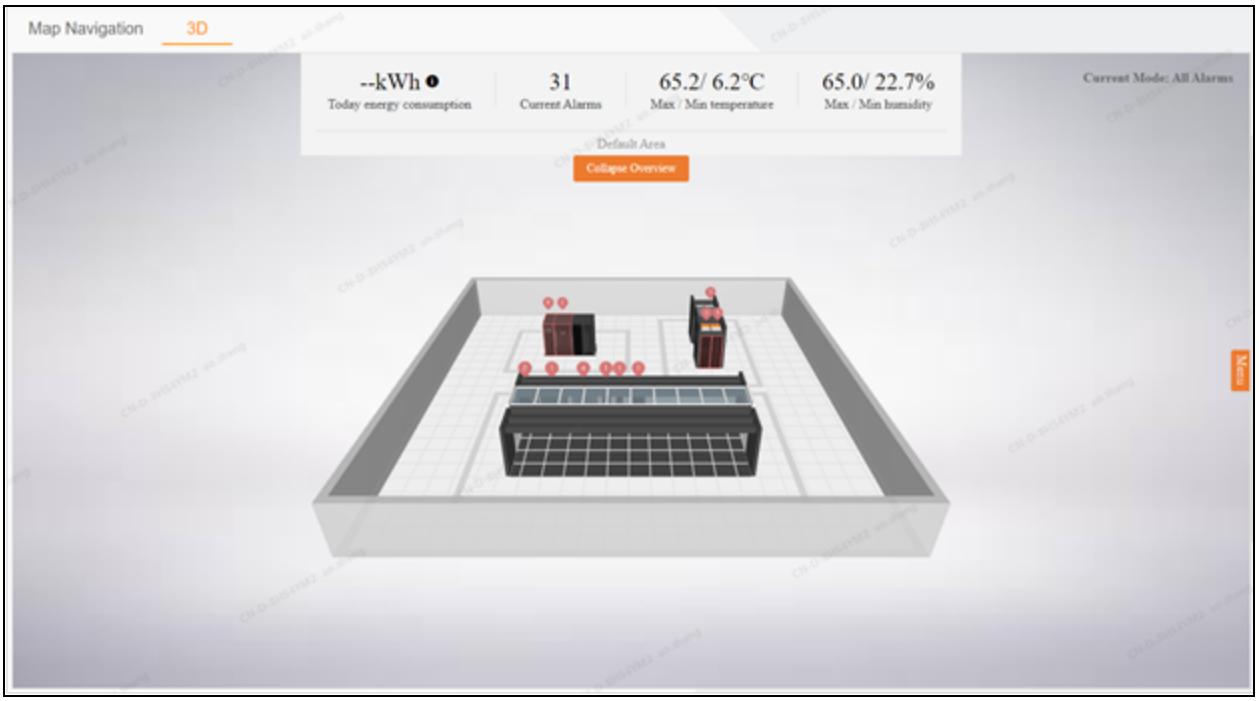


© 2026 Vertiv Group Corp. All Rights Reserved.

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.

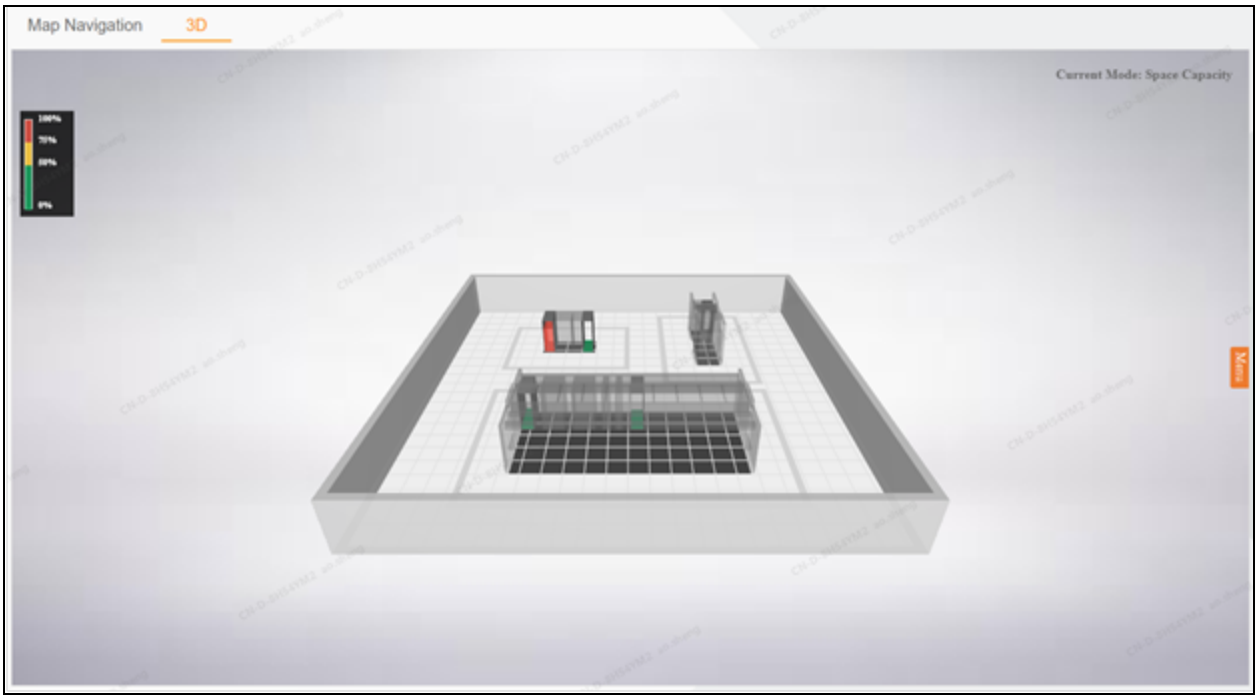
© 2026 Vertiv Group Corp. All Rights Reserved.

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

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

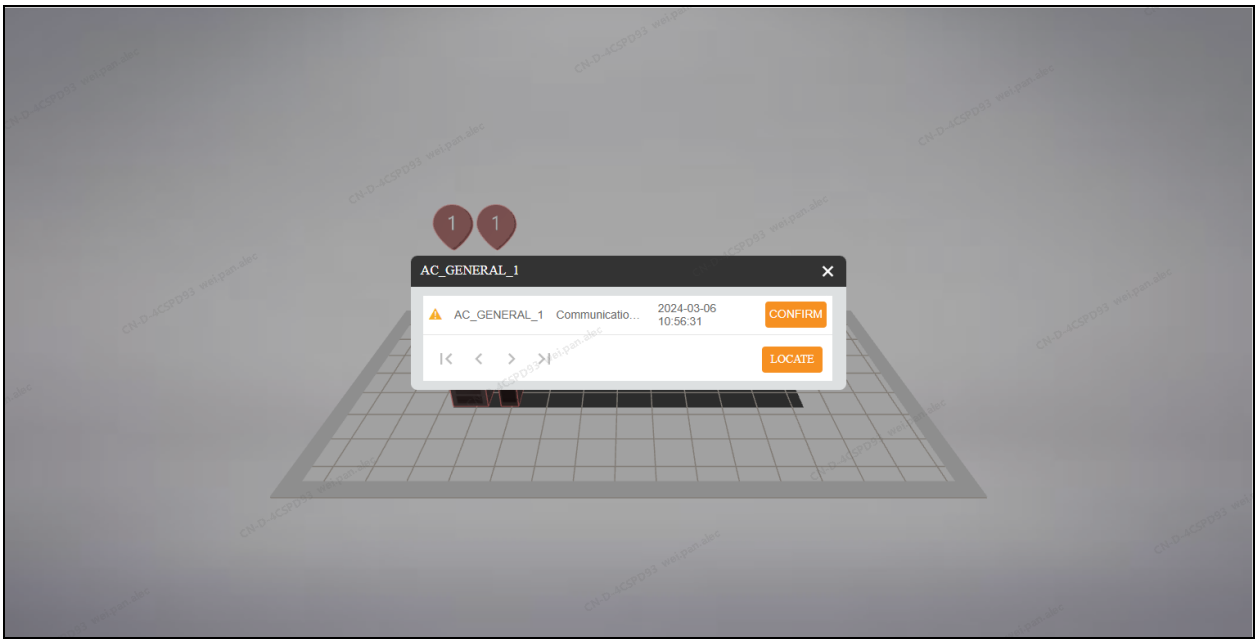


In the 3D view of the battery room site, all assets include the floor UPS, lead-acid battery racks, lithium battery cabinets, etc will be displayed. You can click on each device to open the device detail panel. The running status points and alarms status can be seen from the panel.

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

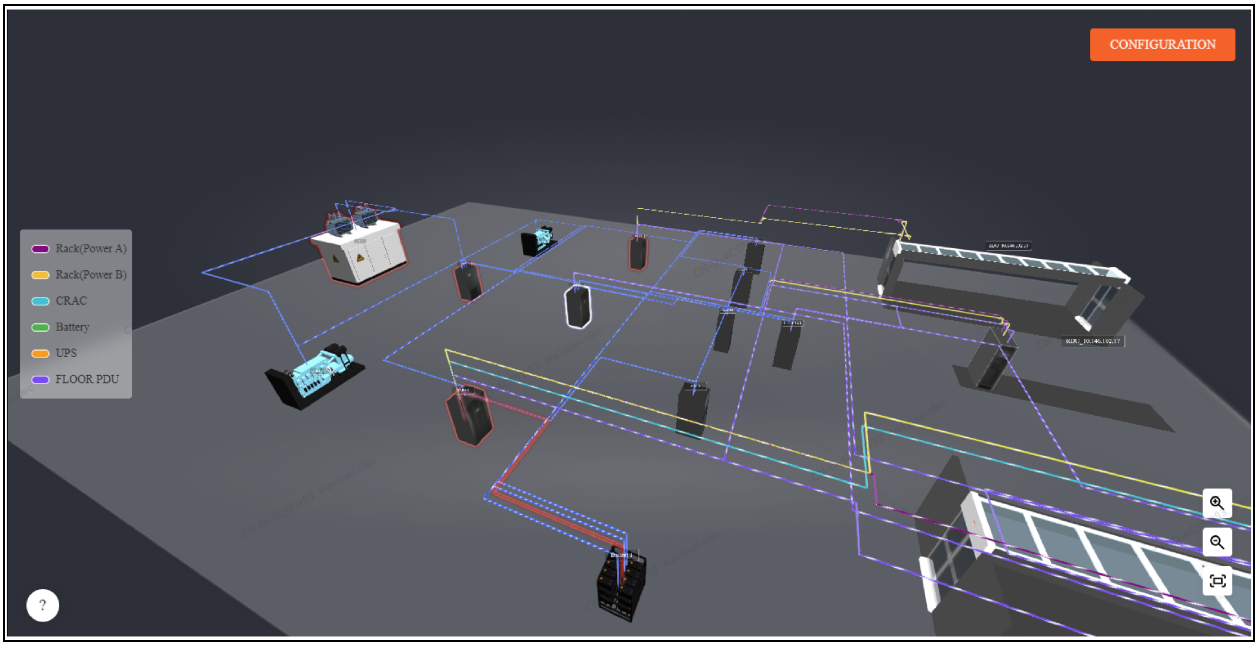
Figure 6.65 Region-Level 3D Module—Alarm Popup



6.2.7 Power Train Diagram 3D Visualization

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

Figure 6.66 Power Train-3D Visualization



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.

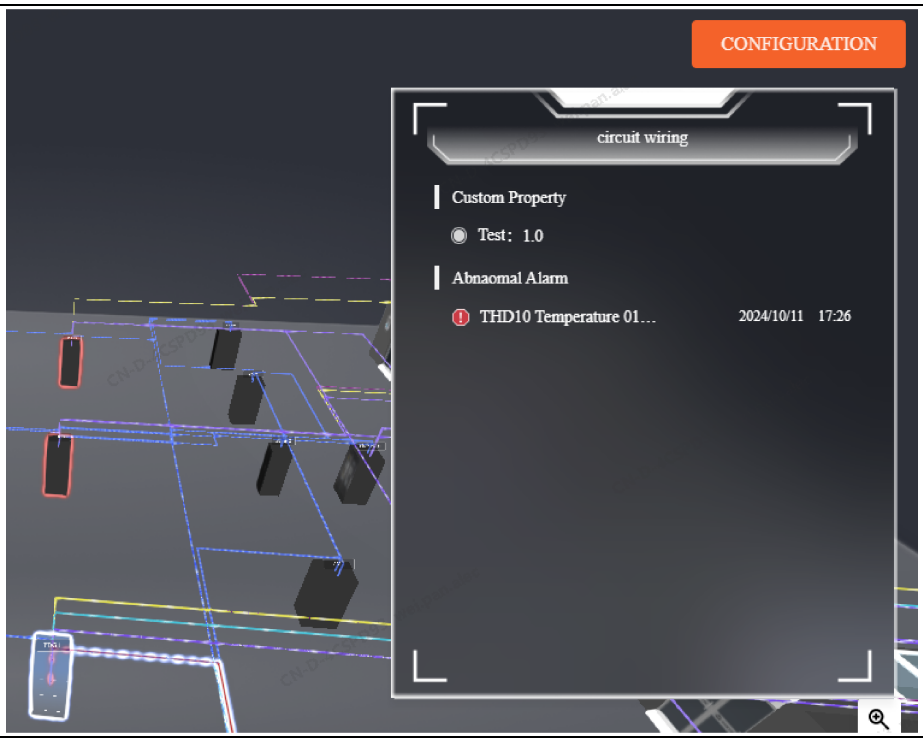
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 6.67 Device Information



Click on the *circuit connection* to see the alarms and attributes of the circuit connections between devices, as shown in Figure 6.68 below .

Figure 6.68 Alarm Attributes



© 2026 Vertiv Group Corp. All Rights Reserved.

7 Single-Site Power Distribution and Thermal Management

7.1 General

7.1.1 Overview

On the Power and Thermal Management tab page of the monitoring home page, users can view power distribution and cooling-related professional information for 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 Detailed Features

7.2.1 Power Distribution Professional Interface

The Power Distribution page includes four functional modules: Three-Phase Unbalance, Maximum Power Trend Per Hour, Power Consumption, and UPS Topology.

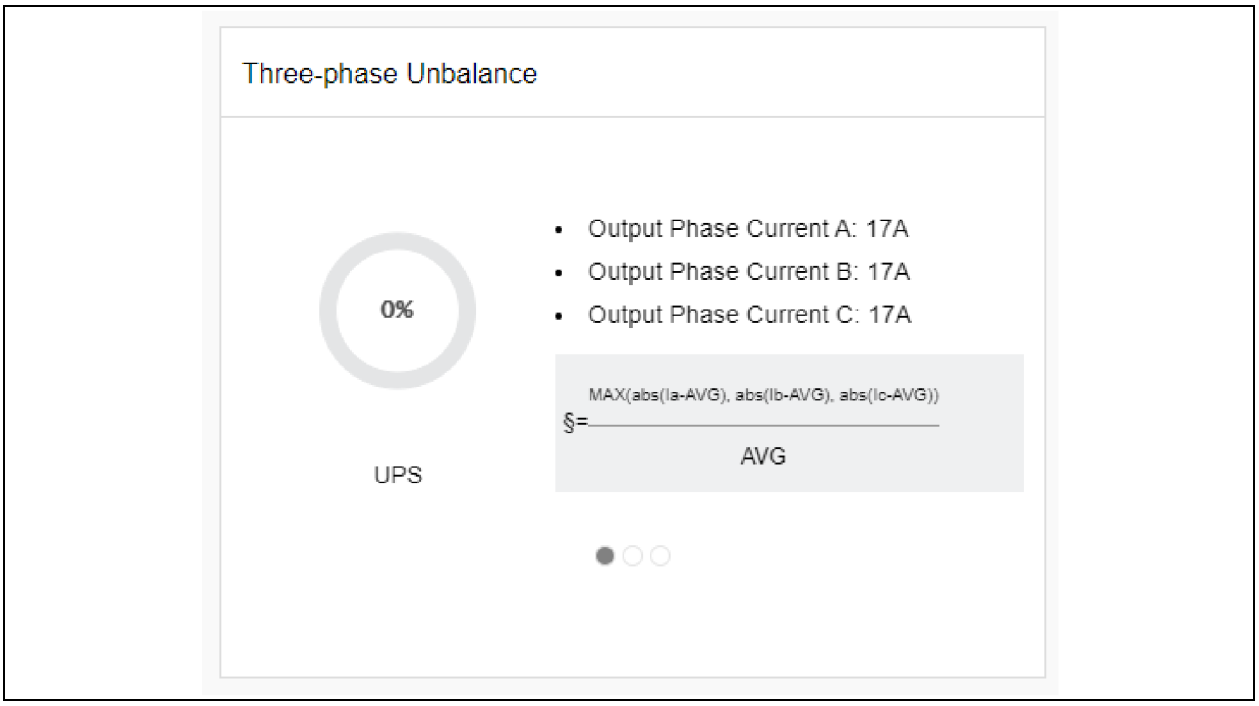
The Three-Phase Unbalance module displays the current three-phase imbalance of each UPS under the current site. Each card centers a donut chart that shows the three-phase imbalance percentage of the current device. On the right side of the card, three items of Real-time Data collected are listed: Output Phase Current A, Output Phase Current B, and Output Phase Current C.

The lower-right corner of each card displays the calculation formula for three-phase imbalance. The calculation logic is as follows: take the maximum absolute value of the difference between each phase current and the three-phase average current, then divide it by the three-phase average current (AVG). The result is the three-phase imbalance of the device. The bottom of the card displays the corresponding device name.

When multiple UPS devices exist under the site, pagination indicators appear at the bottom of the module. Click the indicators to switch and view the three-phase imbalance cards of other devices, as shown in Figure 7.1 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 7.1 Three-Phase Unbalance



The Maximum Power Trend Per Hour module displays the peak power trend of all UPS devices under the current site over the past 24 hours.

Click Configuration in the upper-right corner of this module to open the configuration dialog box, where you can set the safety line threshold. The dialog box contains the following fields:

- **Total Power (kW)**: Enter the rated total power of the device or circuit. This field is required. Unit: kW.
- **Safety Line Ratio (%)**: Enter the percentage of the safety line relative to the total power. Unit: %. Manually setting this value automatically calculates the safety power.
- **Safety Power (kW)**: Enter the safety power of the device or circuit. Unit: kW. Manually setting this value automatically calculates the safety line ratio.

After completing the fields, click *Save* to apply the configuration. Click *Cancel* or (X) in the upper-right corner to close the dialog box and discard the changes.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 7.2 Hourly Maximum Power Trend

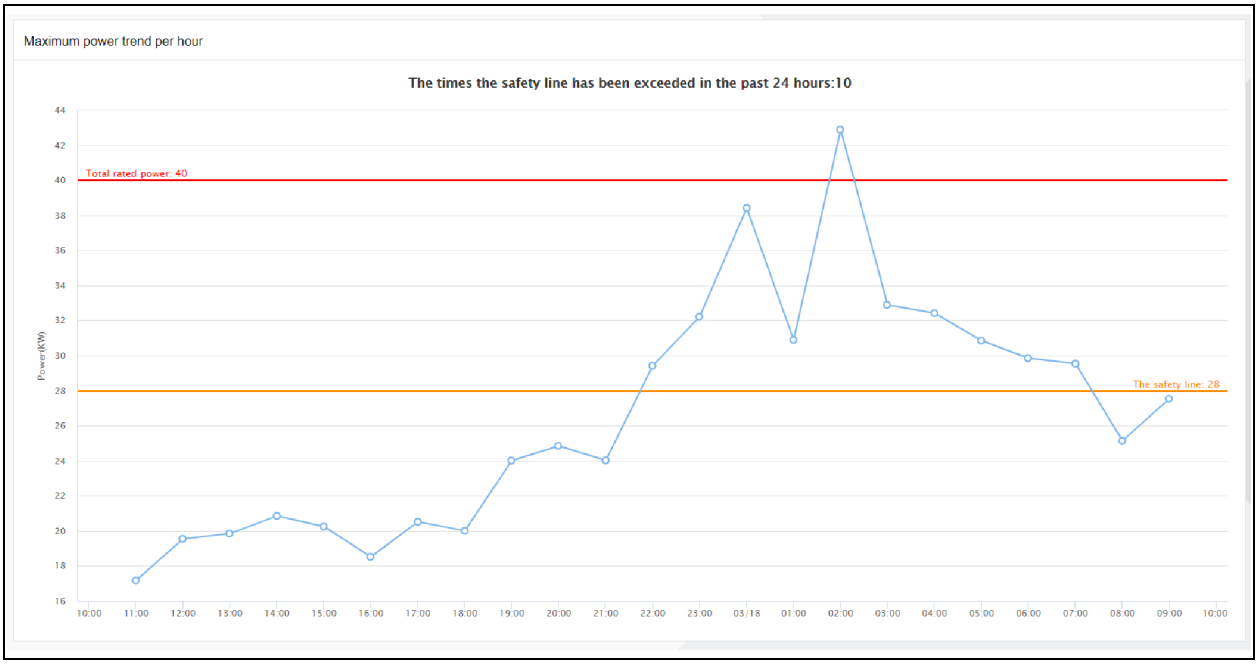
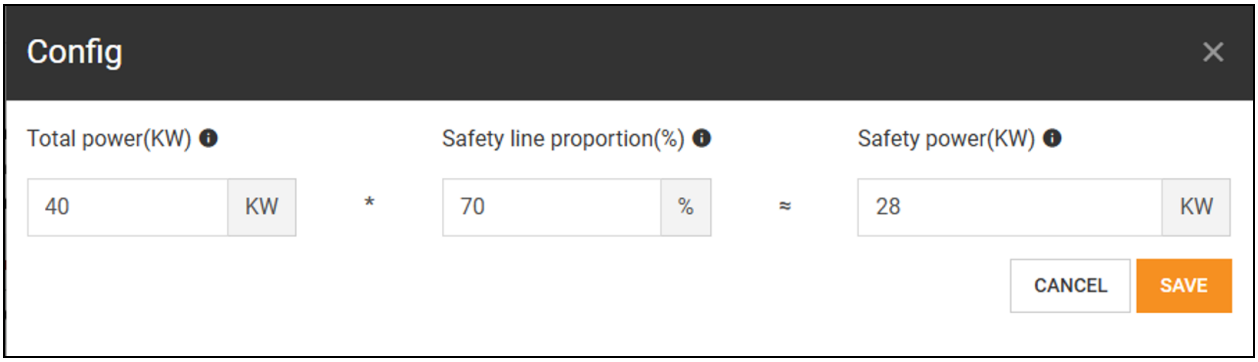


Figure 7.3 Safety line Config



The Energy Consumption Bar Chart module displays the energy consumption trend of the current site within a specified time range in the form of a bar chart. The vertical axis is measured in kilowatt-hours (kWh), and the horizontal axis represents the time scale.

The upper-left corner of the module displays Today's Total Energy Consumption and its real-time value, along with the timestamp of the most recent data update.

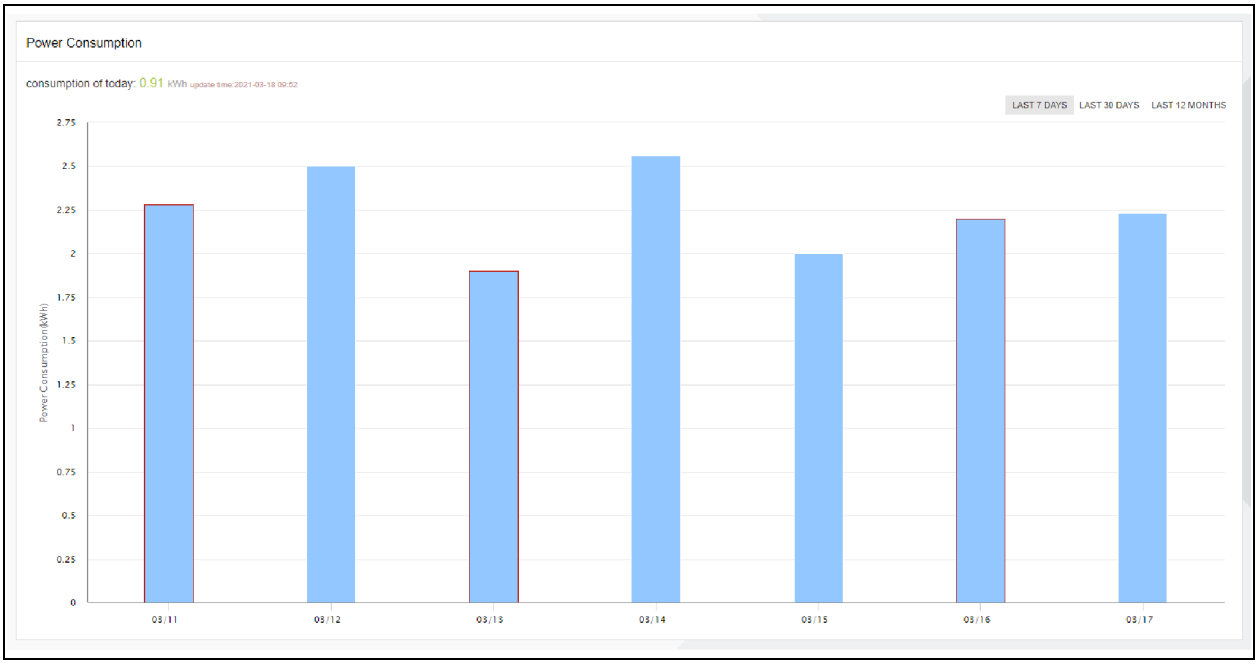
Click the *time range selector* in the upper-right corner to choose one of the following statistical periods:

- Past 7 Days: Displays daily energy consumption for the last 7 days, by day.
- Past 30 Days: Displays daily energy consumption for the last 30 days, by day.
- Past 12 Months: Displays monthly energy consumption for the last 12 months, by month.

After switching the statistical period, the chart automatically refreshes to display the energy consumption data for the selected time range.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 7.4 Bar Chart of Energy Consumption



The UPS Topology module displays the power supply path status and Real-time Data of each UPS device under the current site in the form of a flowchart.

The top of the topology displays the current device name and the Power Supply Mode. The flowchart uses line colors to distinguish the current power supply status: solid lines indicate that the path is connected, and dashed lines indicate that the path is disconnected.

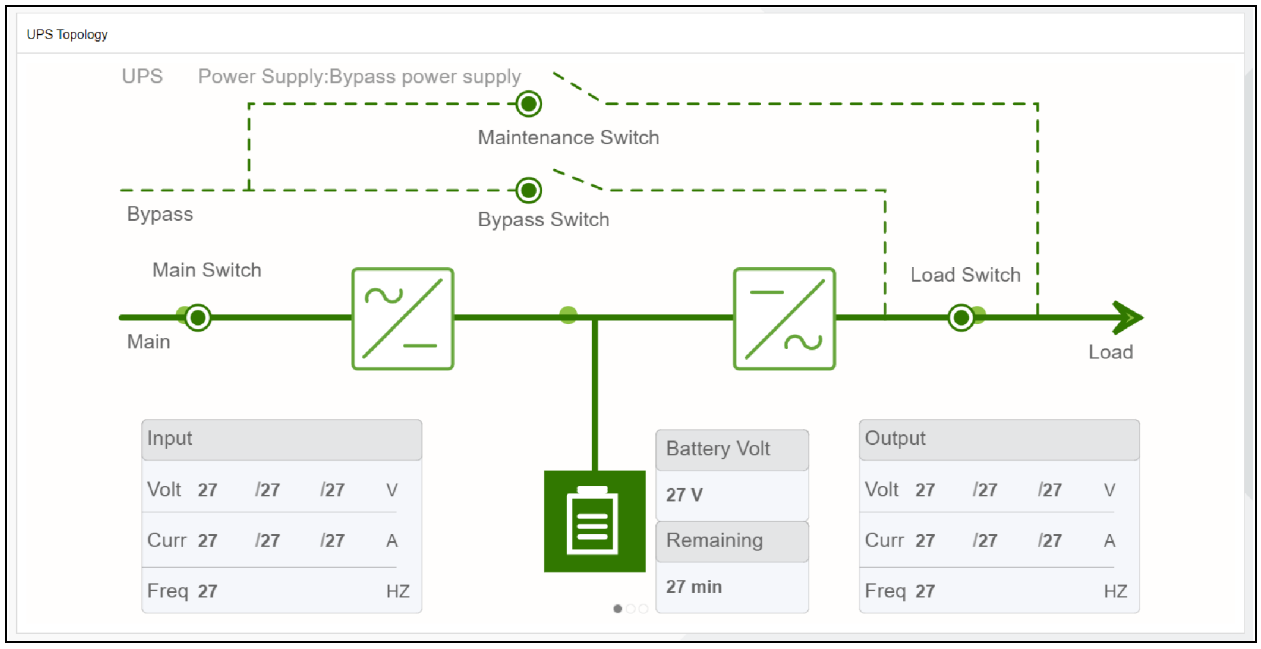
Below the topology, Real-time Data collected for the device is displayed in three columns:

- Input: Displays three-phase input Voltage, three-phase input Current, and input Frequency.
- Battery: Displays the current Battery Voltage and Backup Time.
- Output: Displays three-phase output Voltage, three-phase output Current, and output Frequency.

When multiple UPS devices exist under the site, pagination indicators appear at the bottom of the module. Click the *indicators* to switch and view the topology information of other devices.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 7.5 UPS Topology



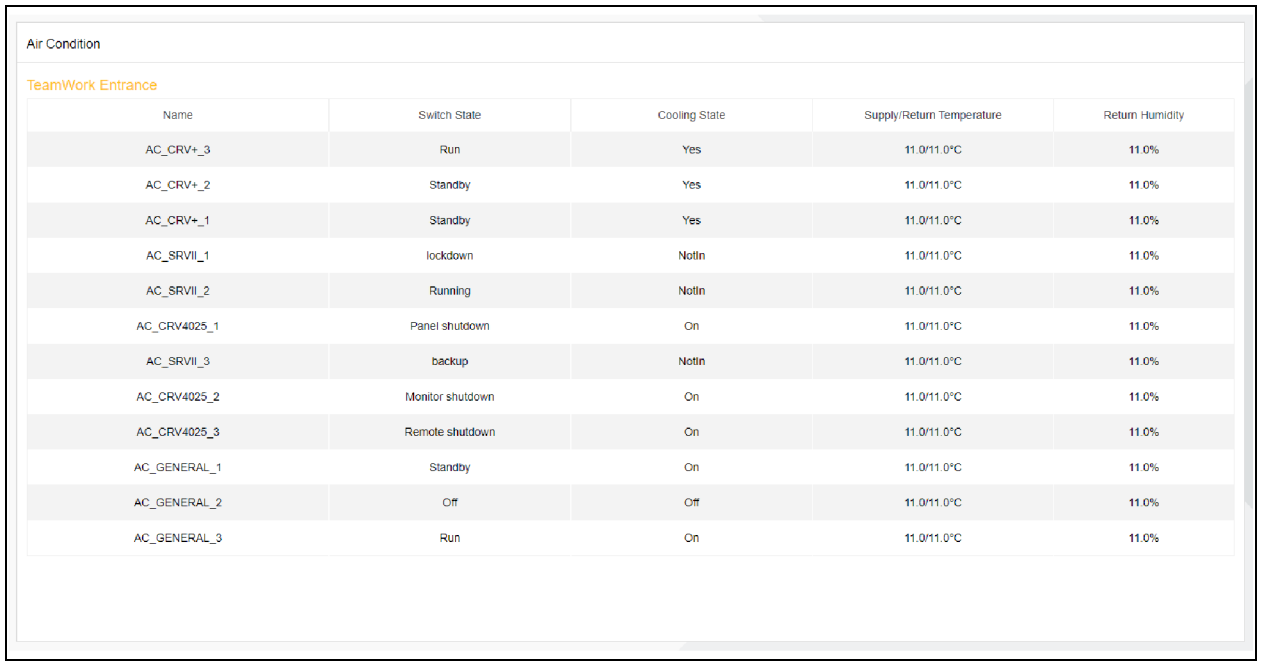
7.2.2 Thermal Management Professional Interface

The Thermal Management page contains four functional modules: Thermal Device Status, Thermal Mgmt Alarms, Comparison of Supply And Return Temperature, and Comparison of Hot And Cold Aisle Temperatures.

The Thermal Device Status module displays the real-time operating status of all CRAC devices under the current site in a table format. At the top of the table, Group Control Entry is displayed. Click it to go to the CRAC group control management page.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 7.6 Air Conditioning Status



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%

The CRAC-Related Alarms module displays the Alarm information of each CRAC device under the current site.

Figure 7.7 Air Conditioner Alarms

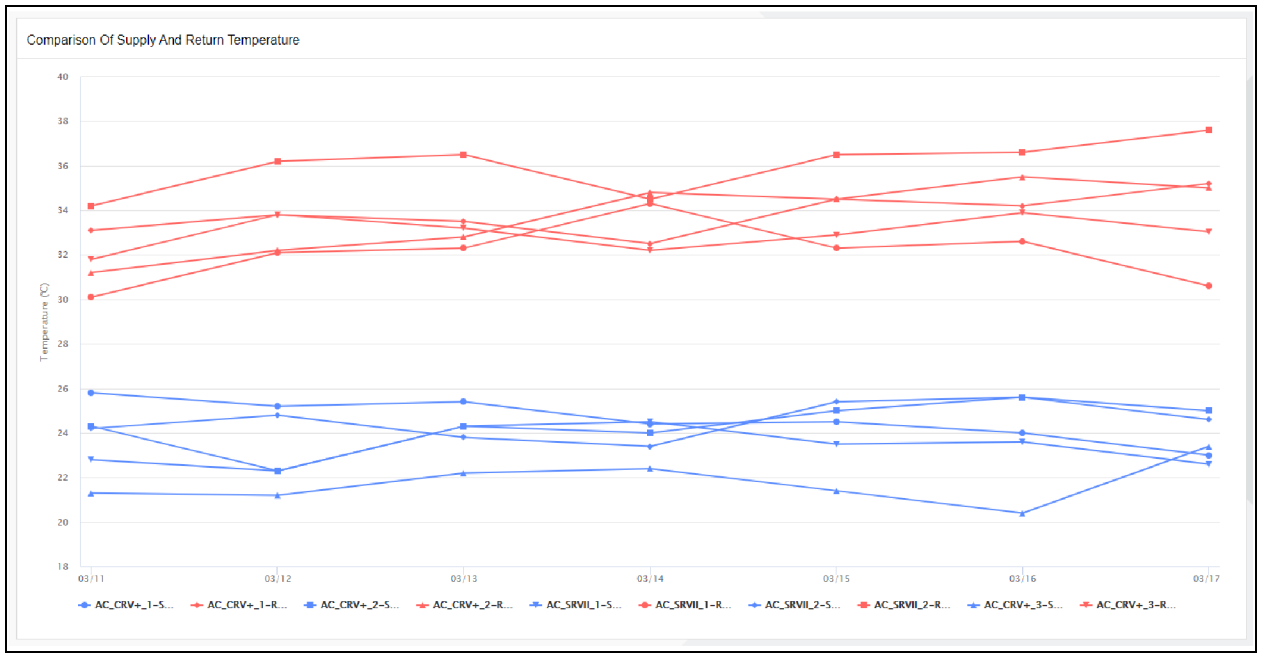


The Multi-CRAC Supply Air Temperature and Return Air Temperature Comparison module displays line charts of the supply air temperature and return air temperature for the selected CRAC devices under the current site.

Click *Configuration* in the upper-right corner of this module to open the configuration dialog box, where you can select the CRAC devices that participate in the comparison.

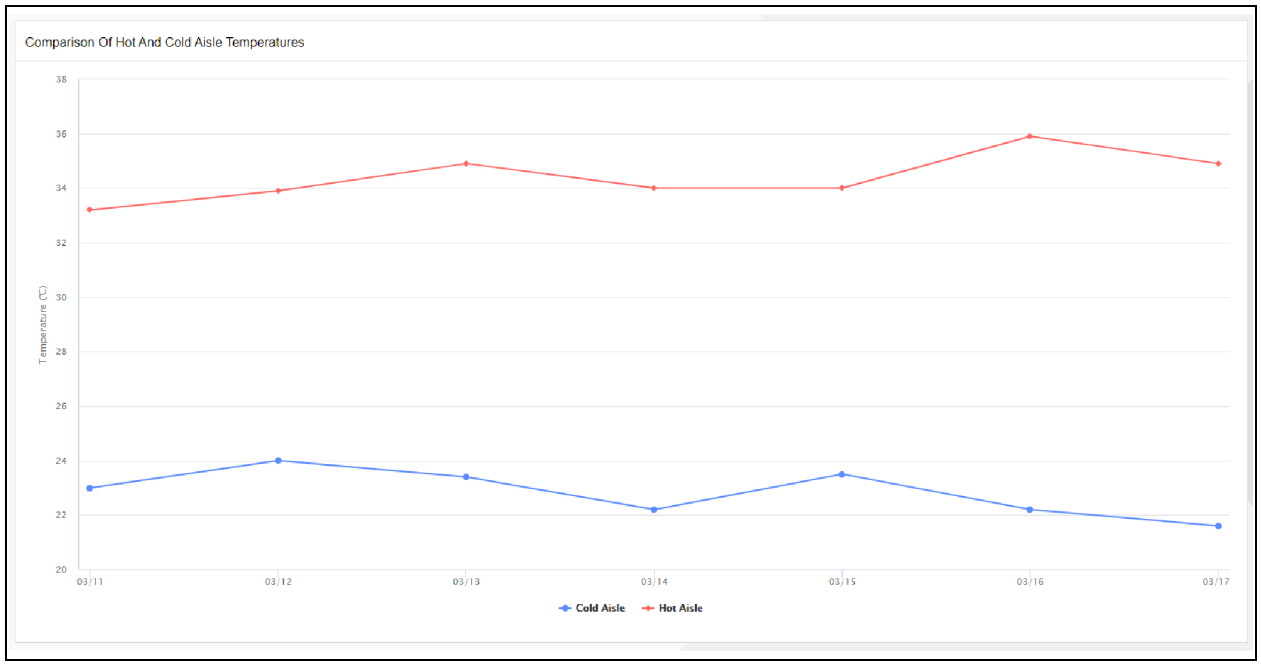
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 7.8 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 7.9 Comparison of Hot and Cold Aisle Temperatures of Single Air Conditioner



© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

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 Detailed Configuration

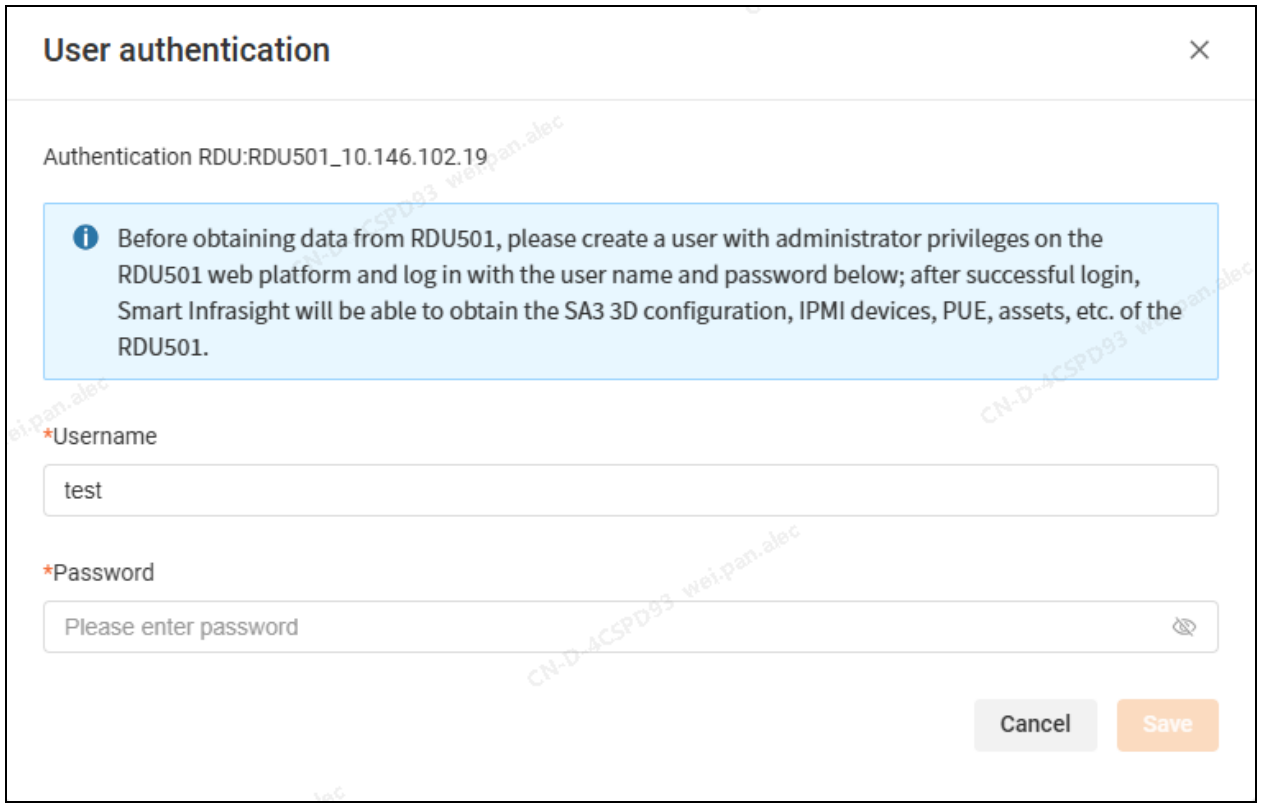
8.2.1 User Authentication Configuration

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 ellipses (⋮) next to the site and select User Authentication.
3. Enter the username and password of the newly created RDU501 account and click *Save*.

© 2026 Vertiv Group Corp. All Rights Reserved.

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 username 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.

8.2.2 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.

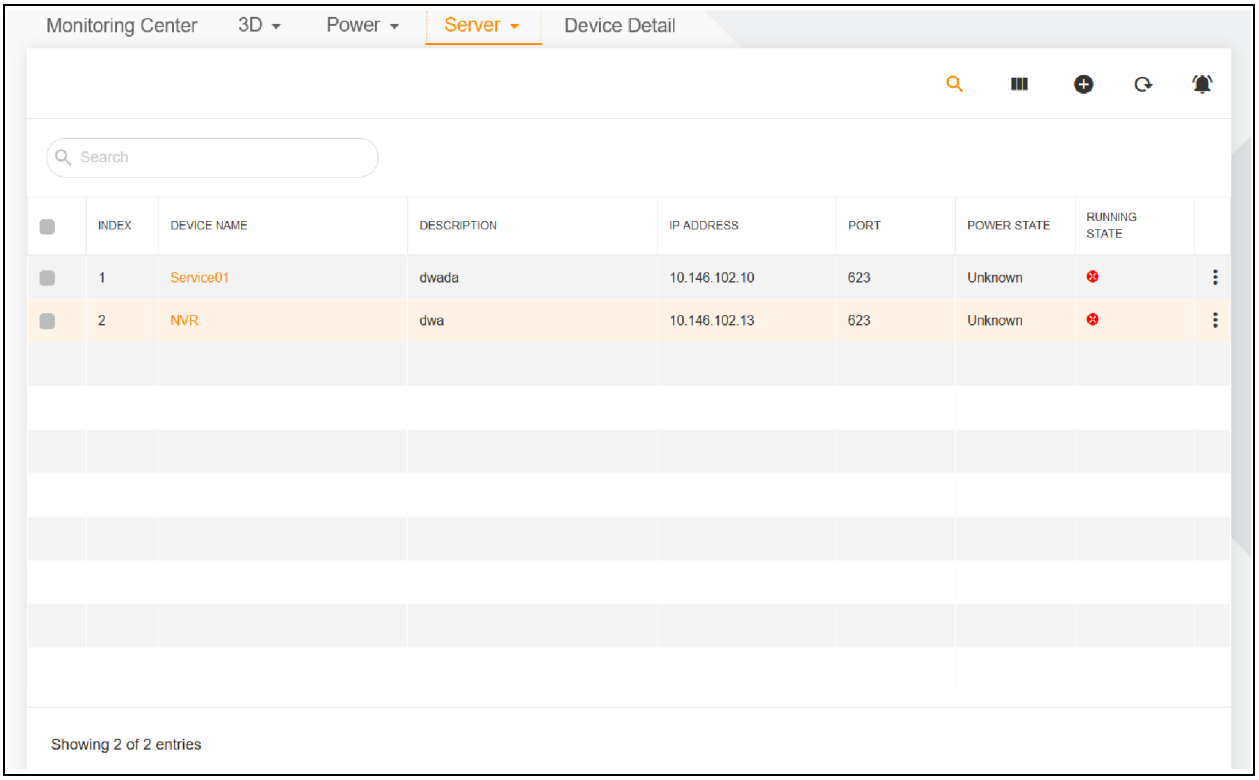
IPMI Device Management

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.

© 2026 Vertiv Group Corp. All Rights Reserved.

- 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.

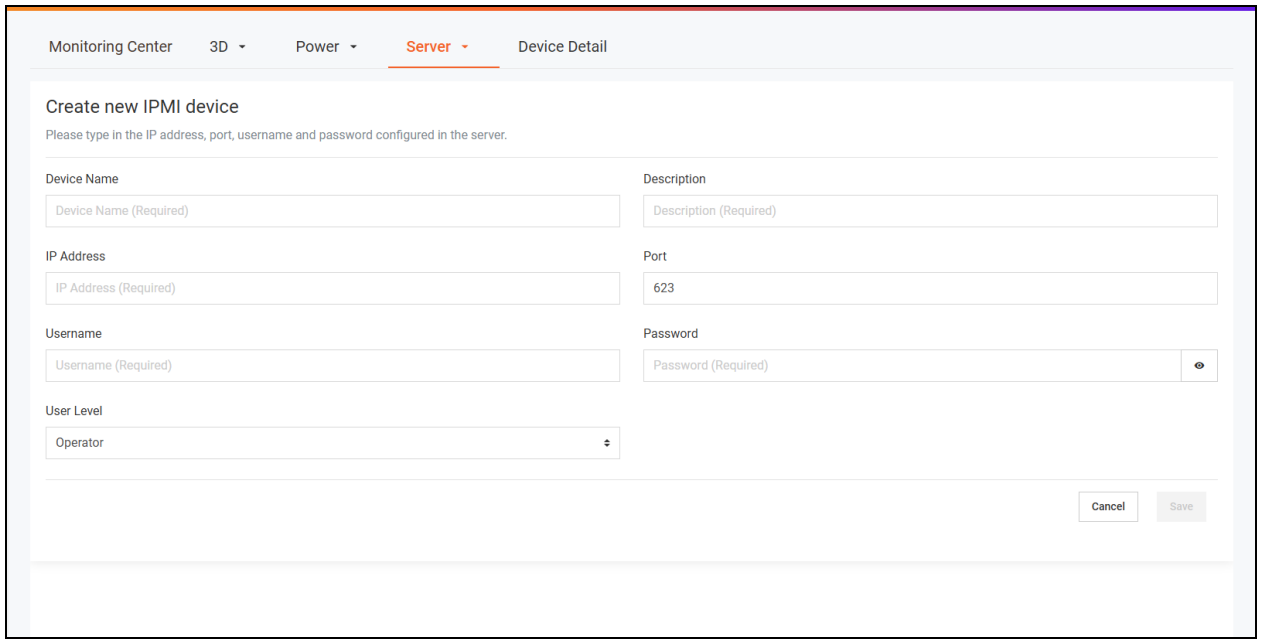
Figure 8.2 IPMI Device List



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.

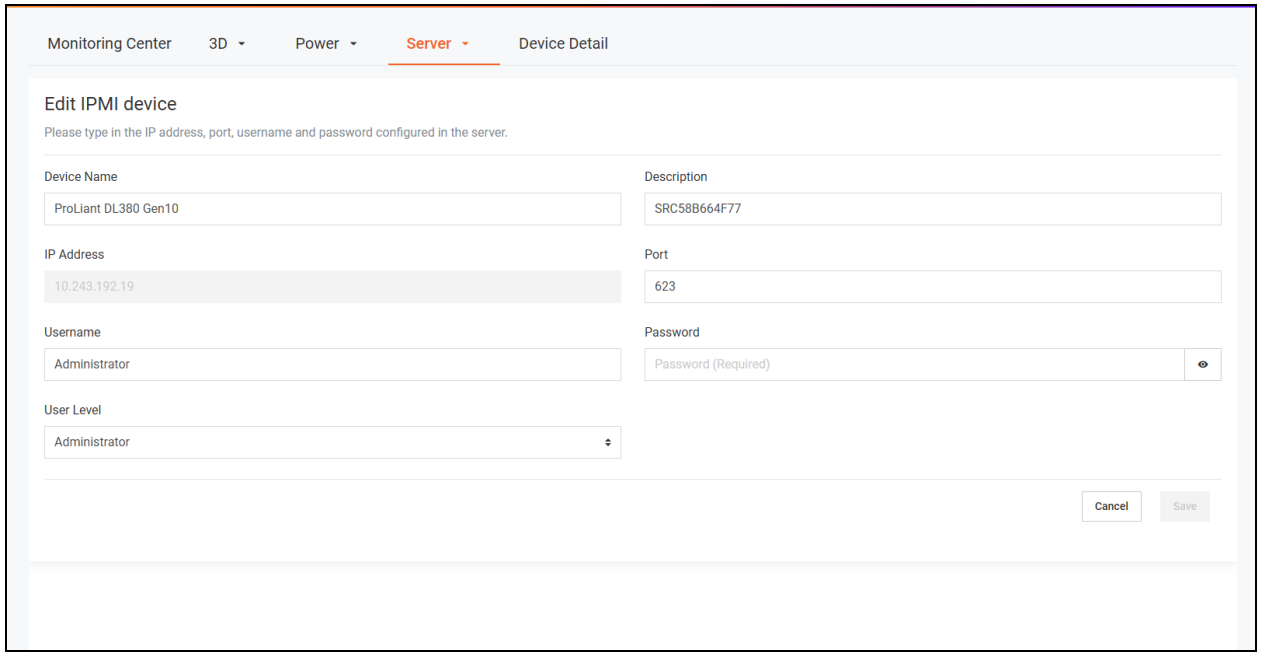
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 8.3 Adding an IPMI Device



Click on the ellipses (⋮) on the right of 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

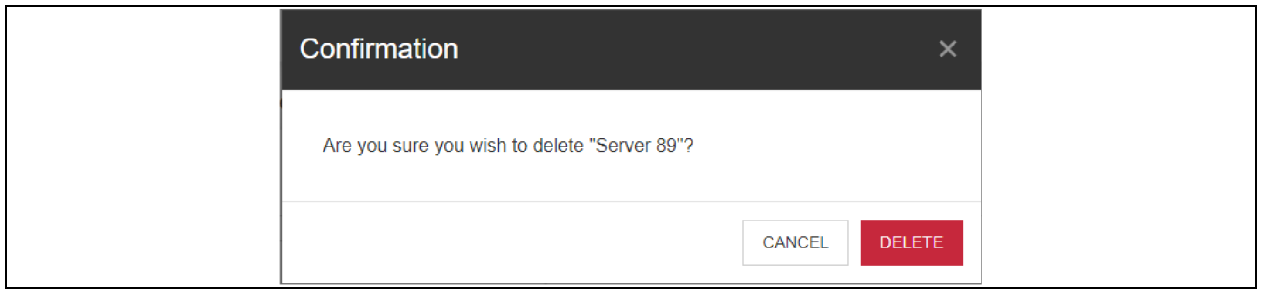


Click the ellipses (⋮) on the right of an IPMI device in the IPMI device list, select the *Delete* button, and a confirmation and deletion window will pop up to delete the IPMI device. As shown in Figure 8.5 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

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



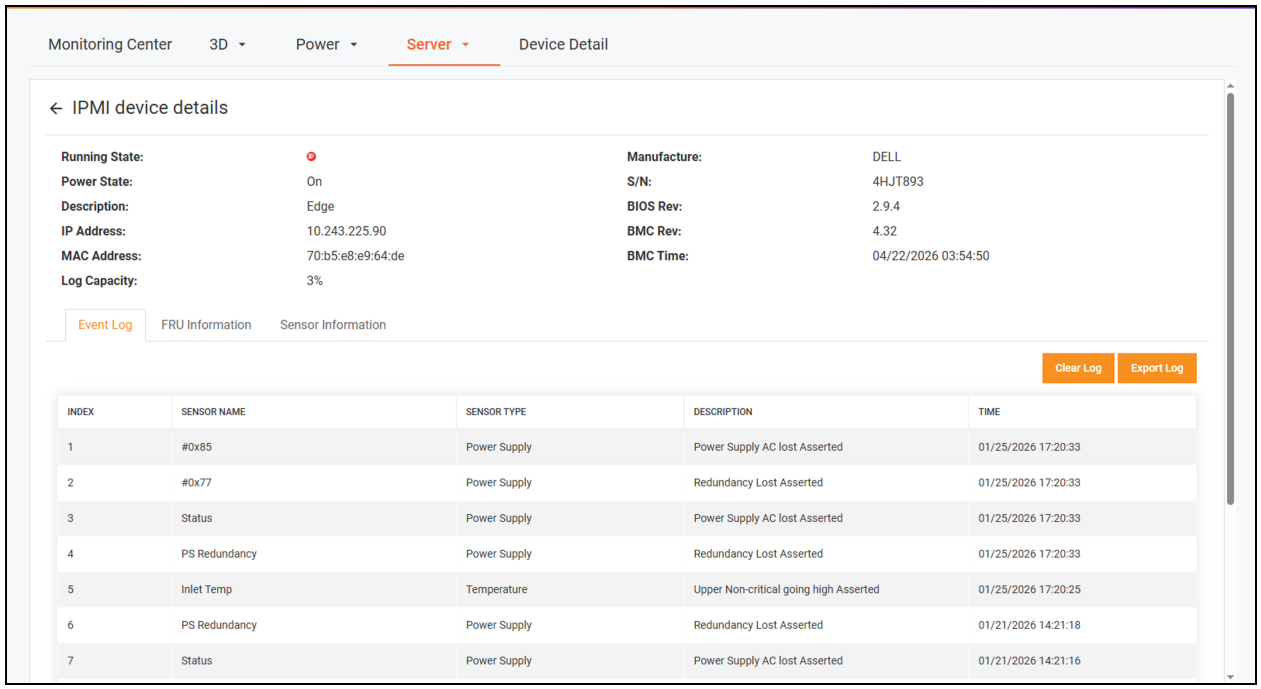
View IPMI Device Details

Click the ellipses (⋮) on the right of 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



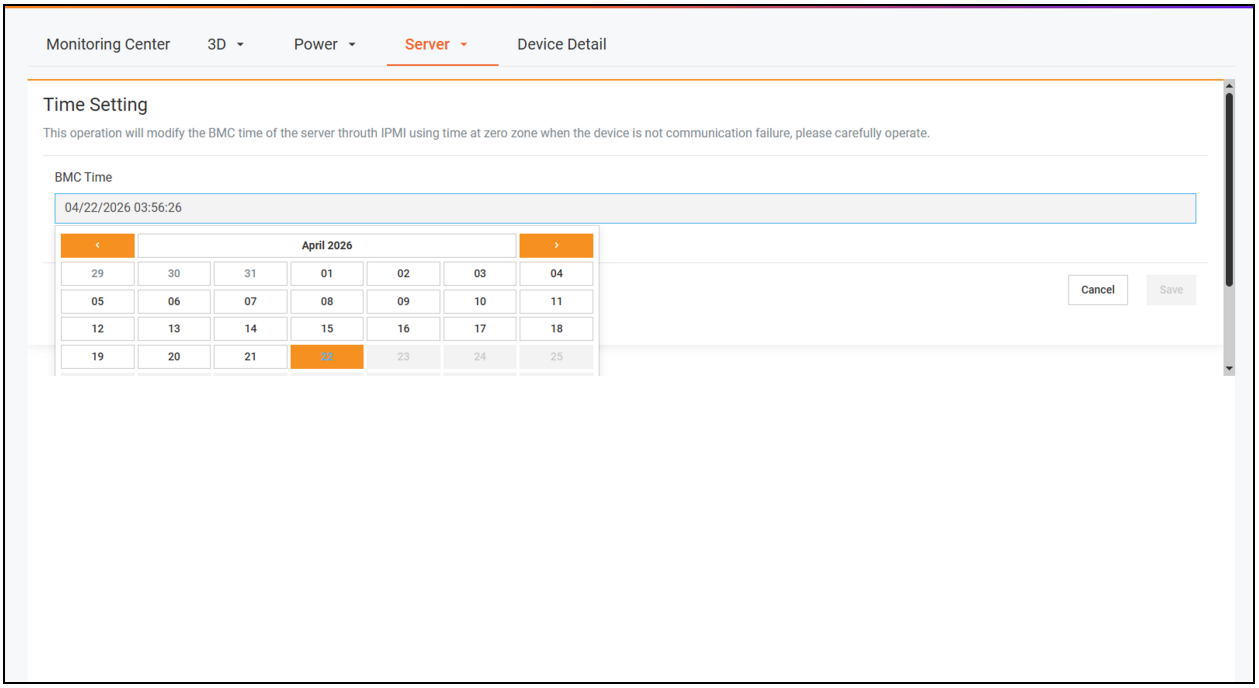
© 2026 Vertiv Group Corp. All Rights Reserved.

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 the ellipses (⋮) on the right of 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

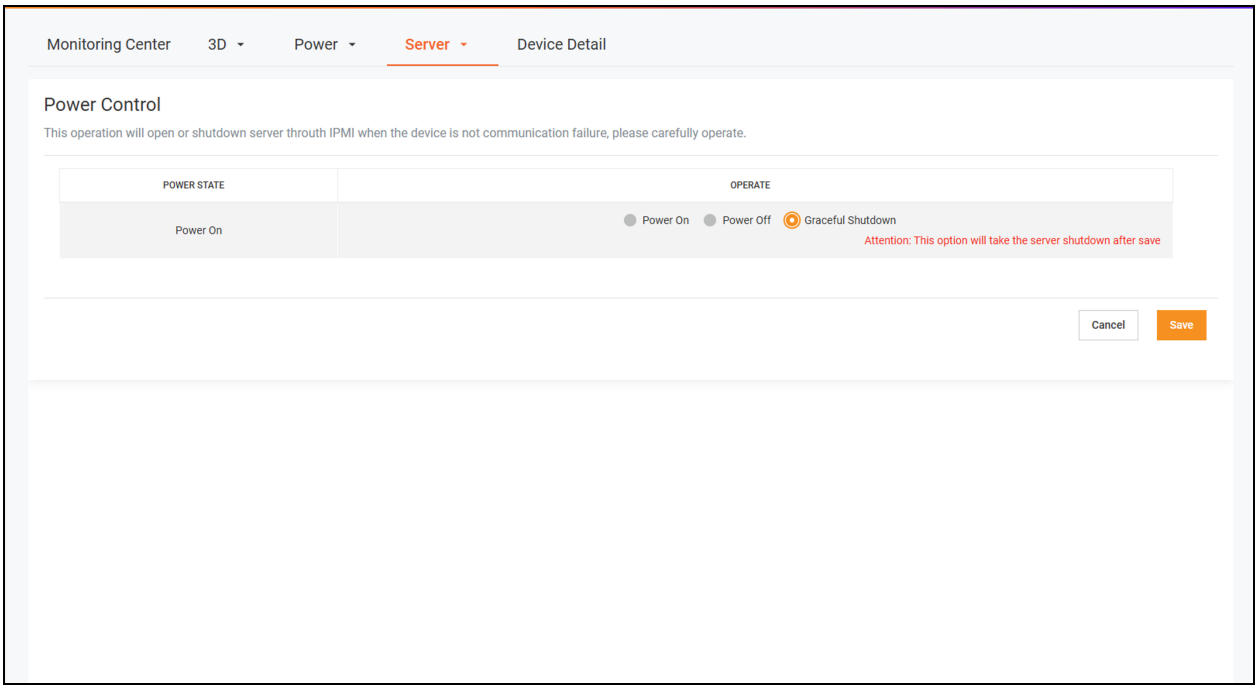


IPMI Device ON/OFF Control

Click the ellipses (⋮) on the right of 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 8.8 IPMI Device Power ON/OFF Control



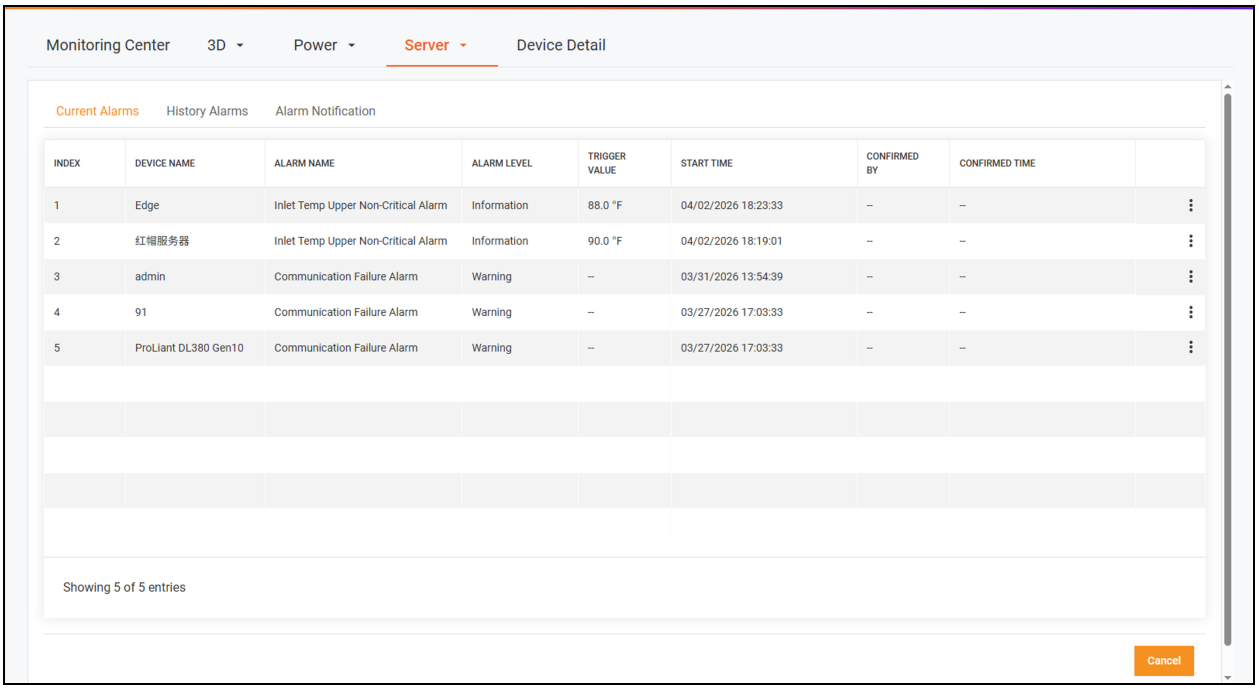
IPMI Device Alarm Management

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 on the next page .

There are three tabs for Alarms and Notifications, and the current Alarms tab is displayed by default, as shown in Figure 8.9 on the next page . Click on the *Confirm* button in the ellipses (⋮) on the right of the current alarm record. After the alarm is confirmed, no alarm notifications will be sent.

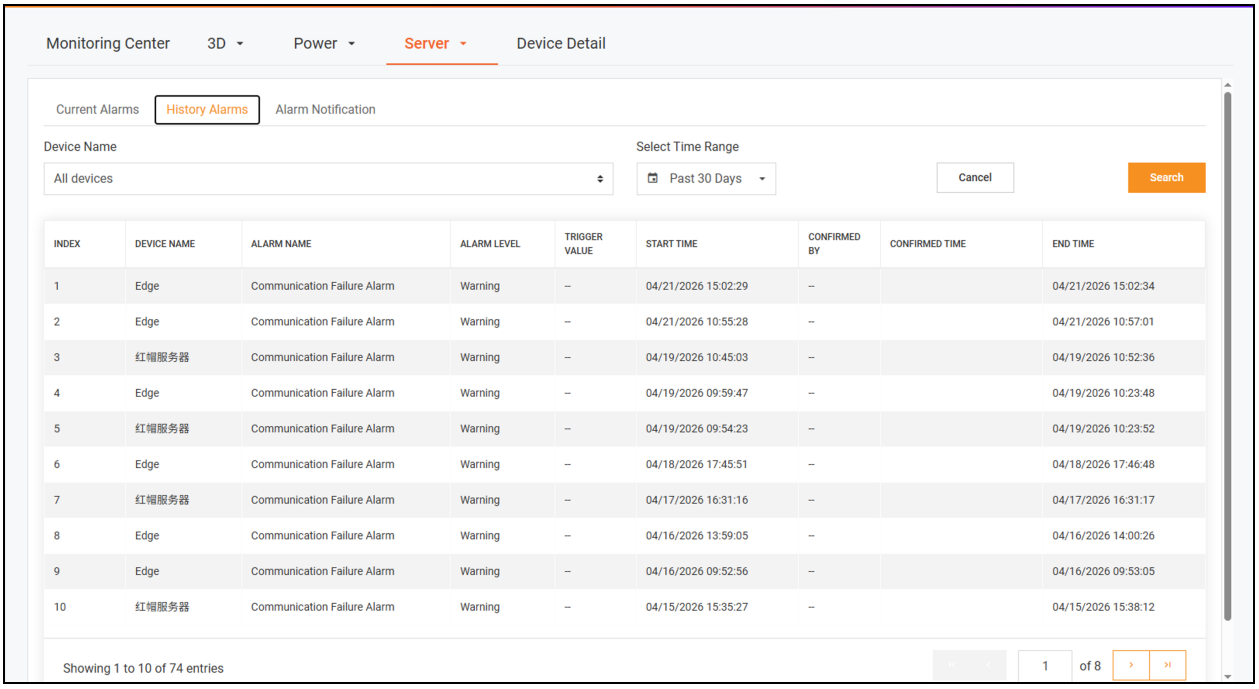
© 2026 Vertiv Group Corp. All Rights Reserved.

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.

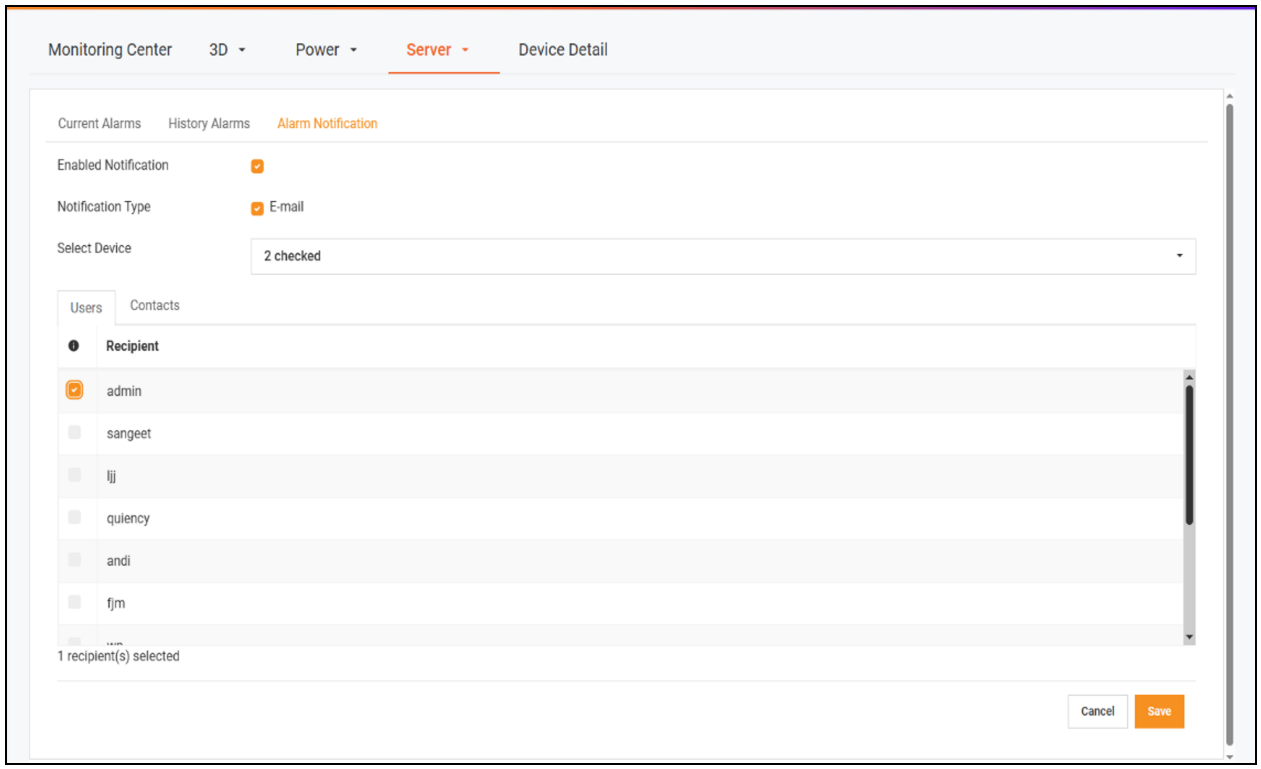
Figure 8.10 IPMI Device Alarm History



© 2026 Vertiv Group Corp. All Rights Reserved.

In Alarm Notification, after you select **Enable Notification** 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



8.2.3 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.

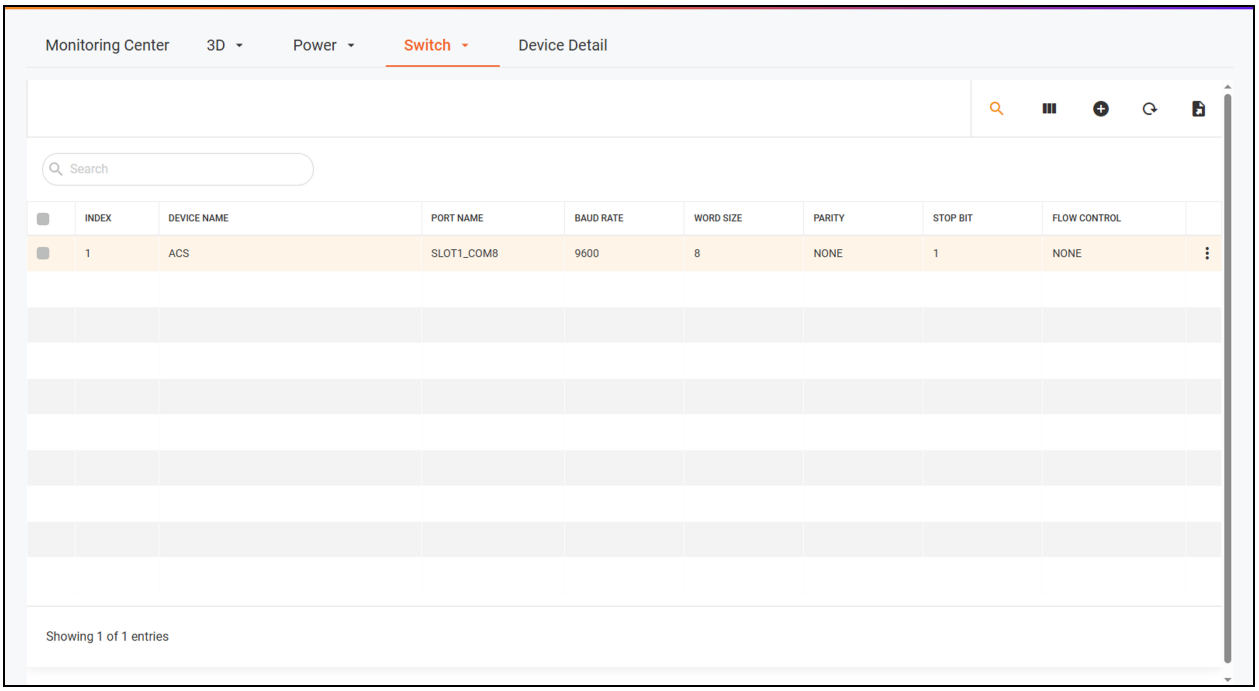
Click the *Switch* tab to enter the console device management page, as shown in **Figure 8.12** on the next page .

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.

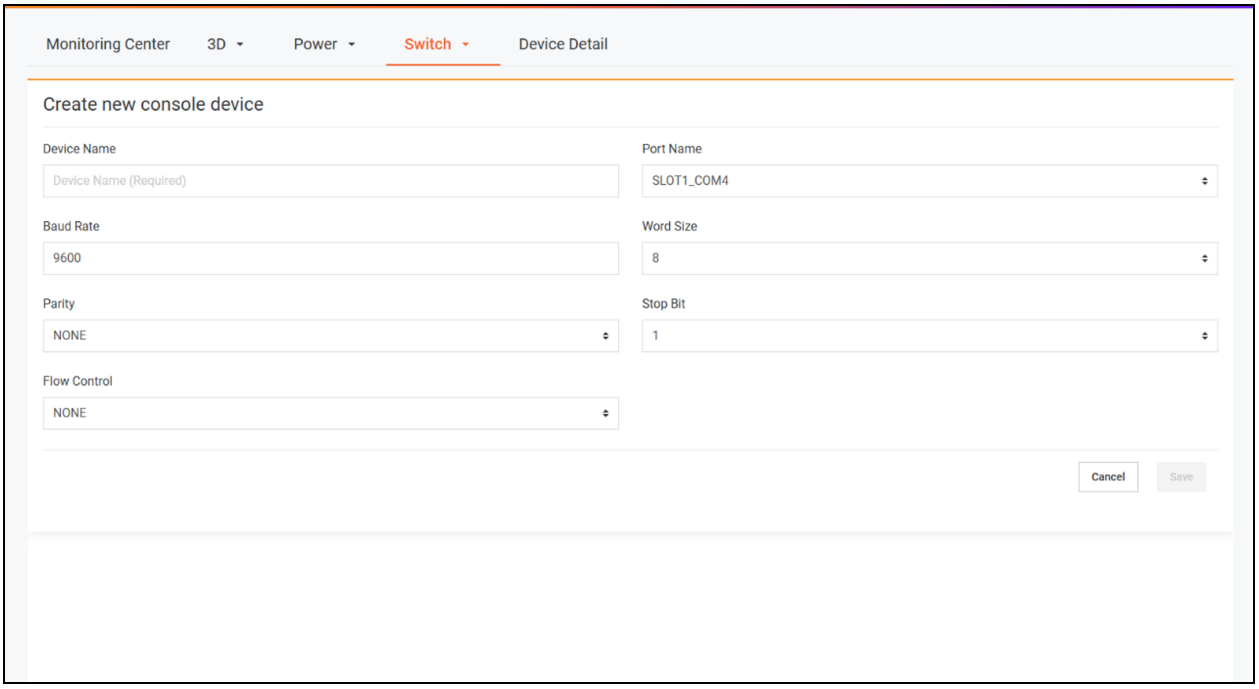
© 2026 Vertiv Group Corp. All Rights Reserved.

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** below . Newly added console devices are added in RDU501 synchronously.

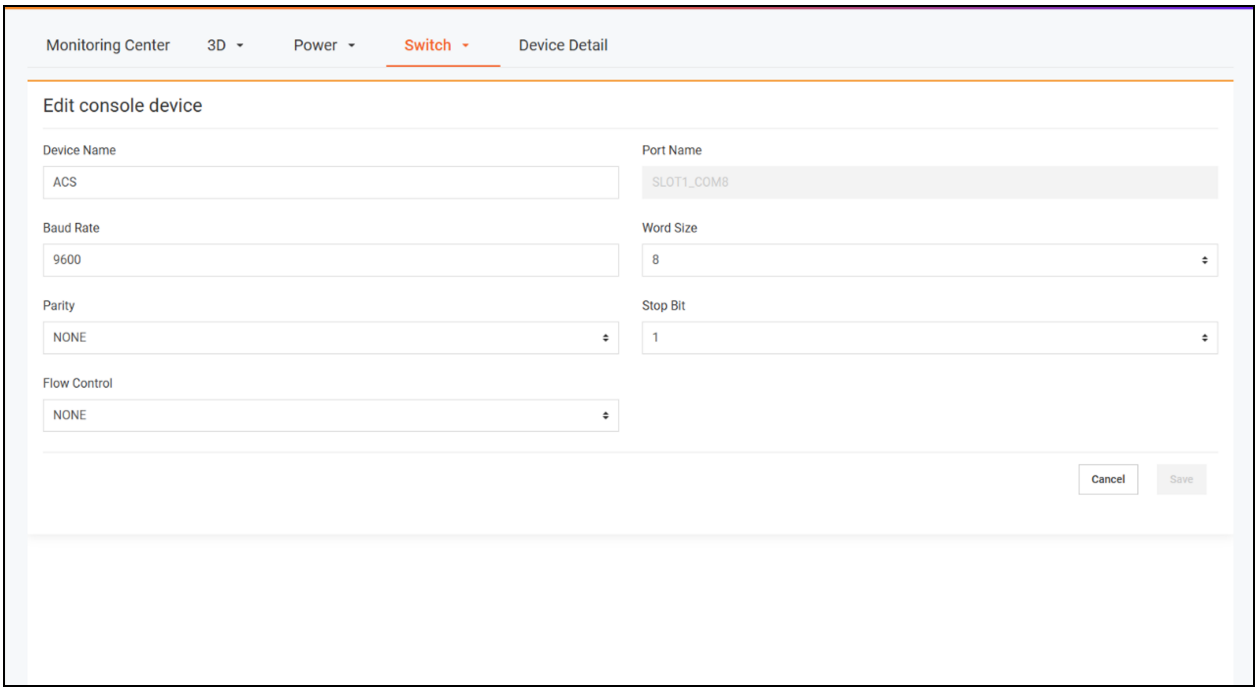
Figure 8.13 Adding a Console Device



© 2026 Vertiv Group Corp. All Rights Reserved.

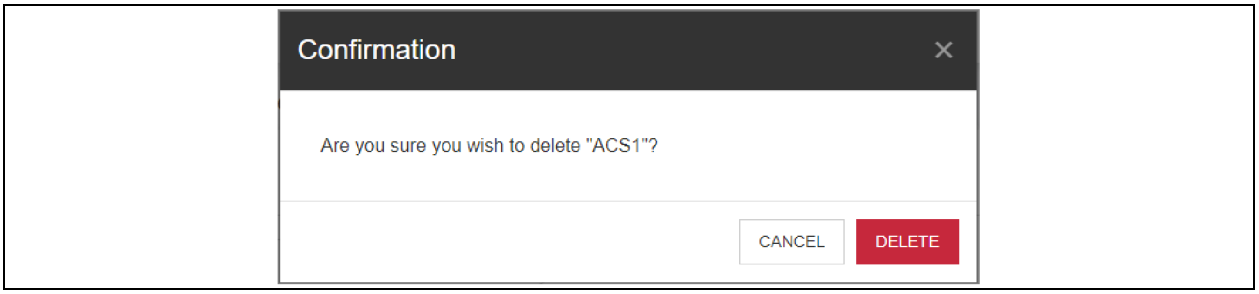
Click the ellipses (⋮) on the right of a console device in the console device list and select Edit to open the Edit Console Device page, as shown in Figure 8.14 below . Enter the new information of the console device (the port information is not allowed to be modified, the baud rate, data bits, check 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 (⋮) on the right of 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 below . 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

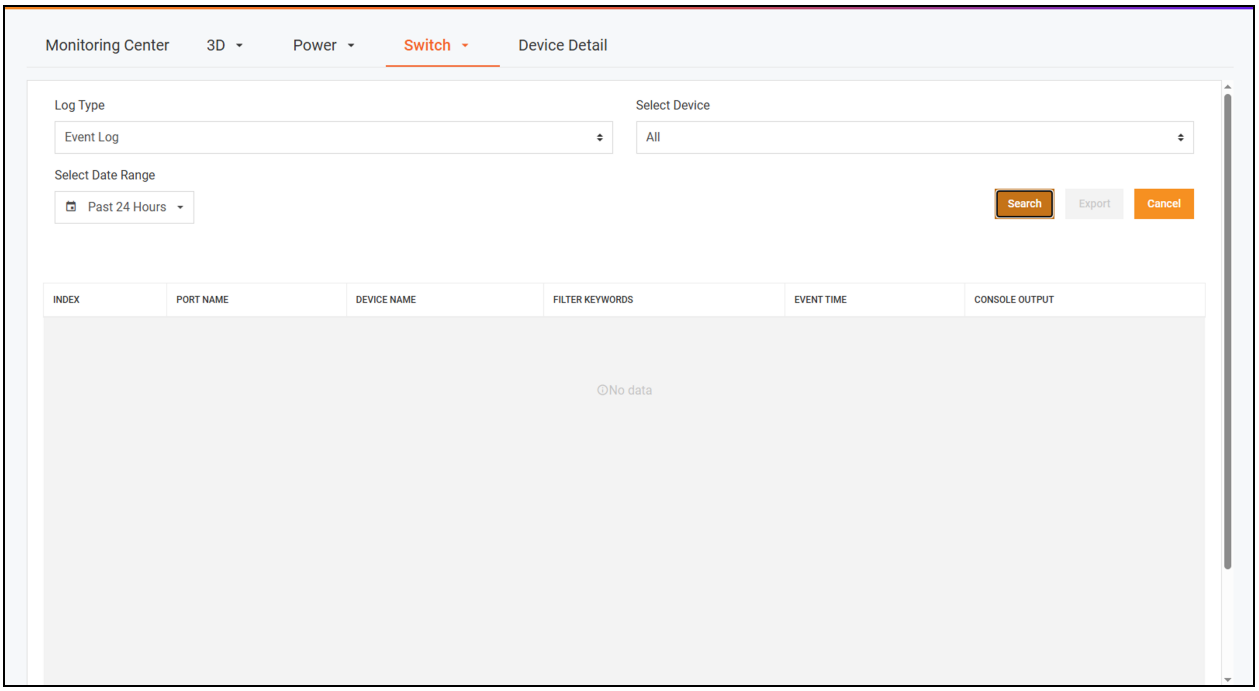


Console Logs

Use the Console History Log button at the top right of the IPMI device list page to open the Console Device Logs page. The Console Device Log contains event logs and history logs, and the event logs are displayed by default, as shown in Figure 8.16 on the next page . 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 8.16 Console Device Event Log



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

© 2026 Vertiv Group Corp. All Rights Reserved.

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 Vertiv™ Smart InfraSight™ dashboard includes the following functional modules:

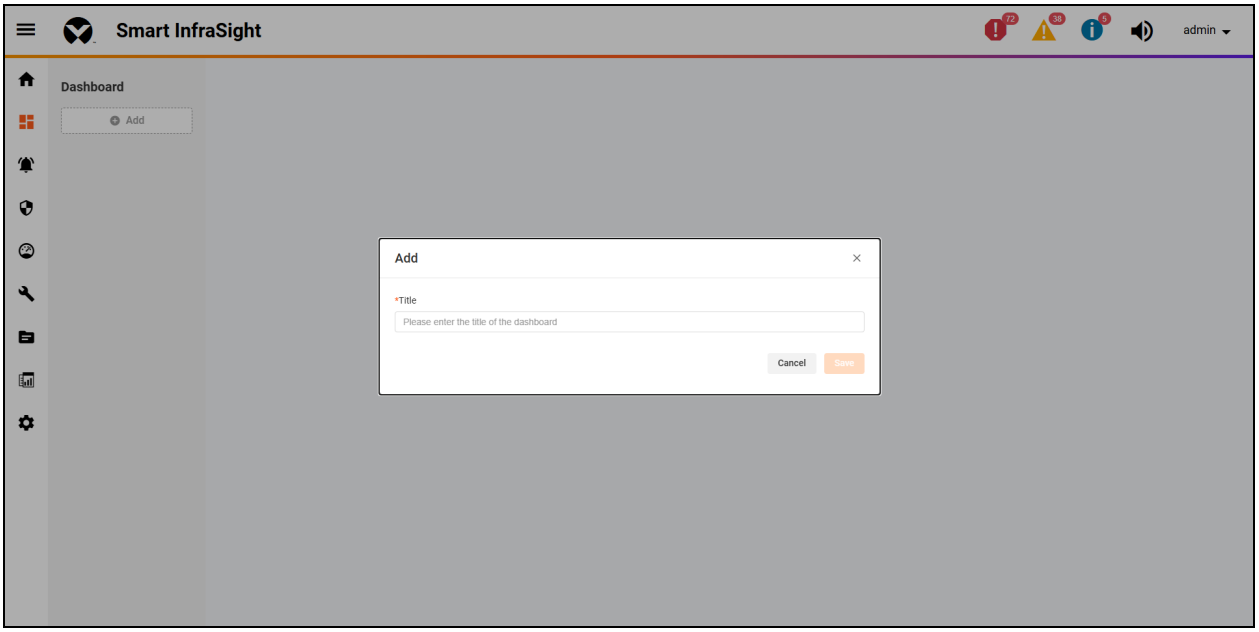
1. Adding a Dashboard
2. Adding and deleting visualizations
3. Editing a Dashboard
4. Pop out a Dashboard
5. Deleting a Dashboard

9.2 Detailed Features

9.2.1 Dashboard

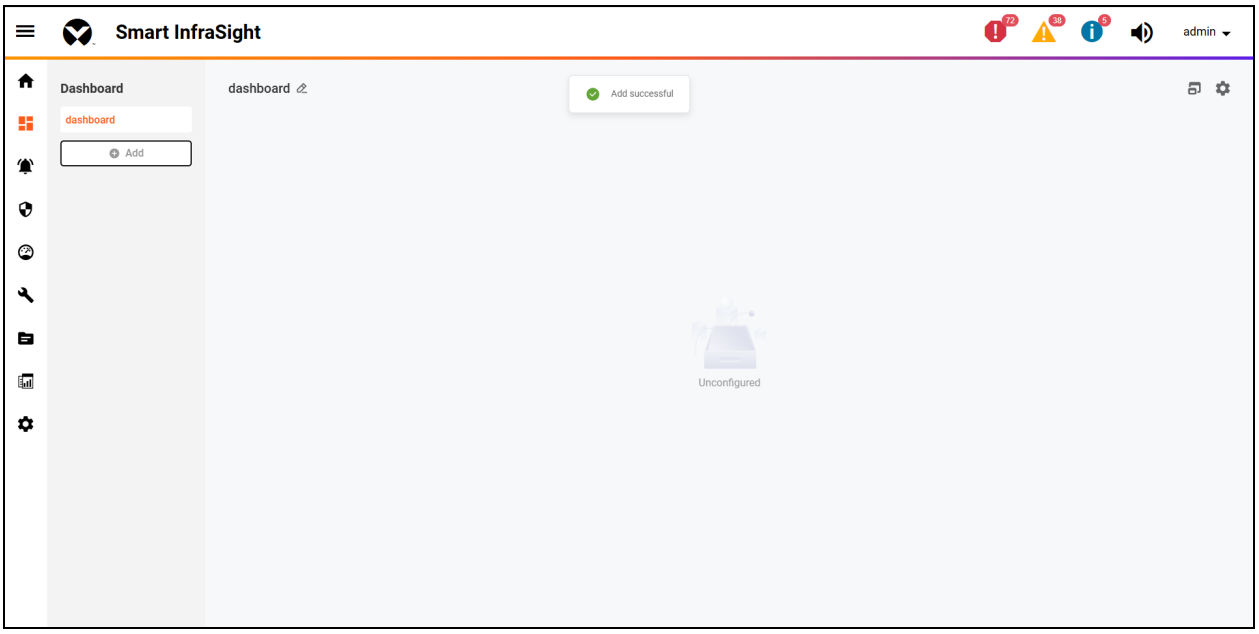
In the dashboard list, click the *Add* button and enter a dashboard name in the Add pop-up box, and click *Save* to enter the dashboard interface.

Figure 9.1 Adding a Dashboard



© 2026 Vertiv Group Corp. All Rights Reserved.

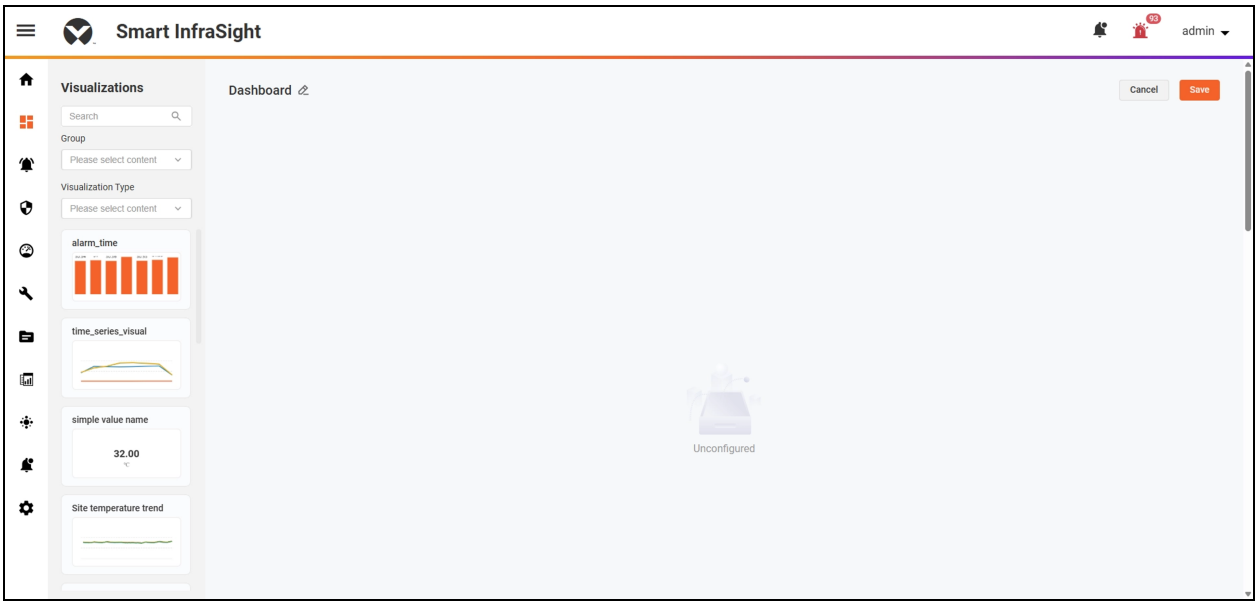
Figure 9.2 The Added Dashboard



9.2.2 Adding a Visualization

Click the *edit* icon in the upper-right corner to enter edit mode. The dashboard list is hidden, and the Visualizations panel appears on the left side. In the Visualizations panel, you can search for a visualization by name, or filter by Group or Visualization Type. Visualizations that have not been assigned to a group appear under the Ungrouped option in the Group drop-down list.

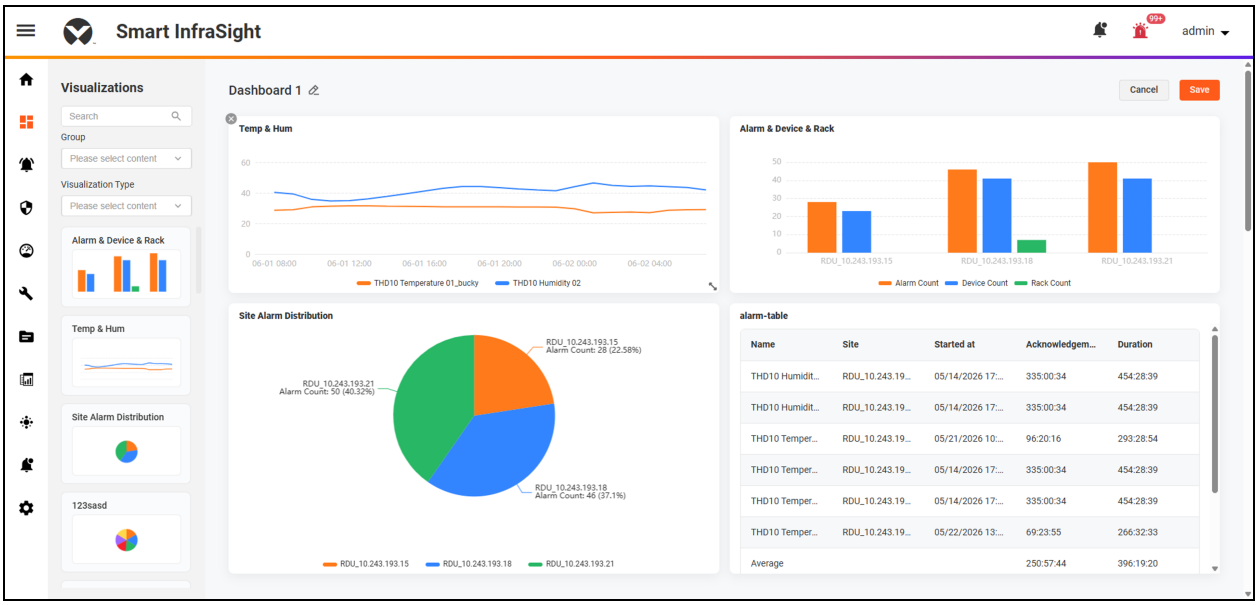
Figure 9.3 Adding a Visualization



© 2026 Vertiv Group Corp. All Rights Reserved.

Select a visualization from the Visualizations panel and drag it into the dashboard content area by holding down the mouse button. During the drag operation, a shaded area indicates the target position of the visualization. Release the mouse button to place the visualization at the shaded position. You can drag the same visualization or other visualizations into the dashboard multiple times.

Figure 9.4 Adding a Visualization

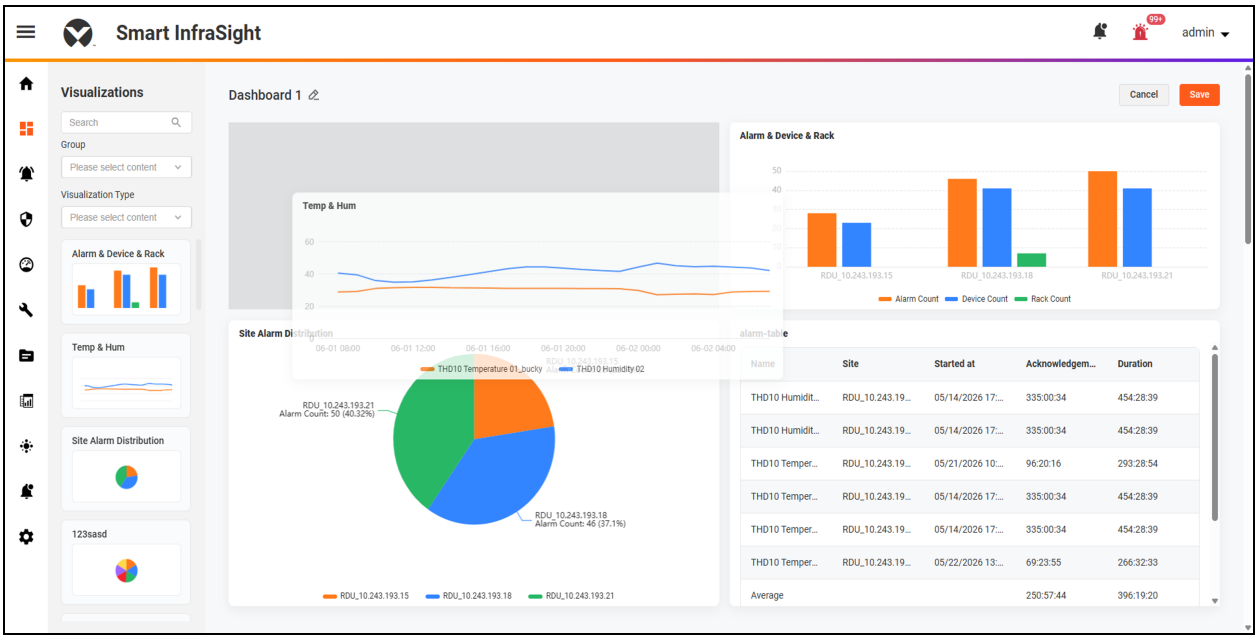


9.2.3 Move, Resize, and Delete a Visualization

To move a visualization, hover over it, then click and hold to drag it to a new position. The platform applies collision detection logic to determine valid placement positions. The shaded area indicates the final position of the visualization. Release the mouse button to complete the move.

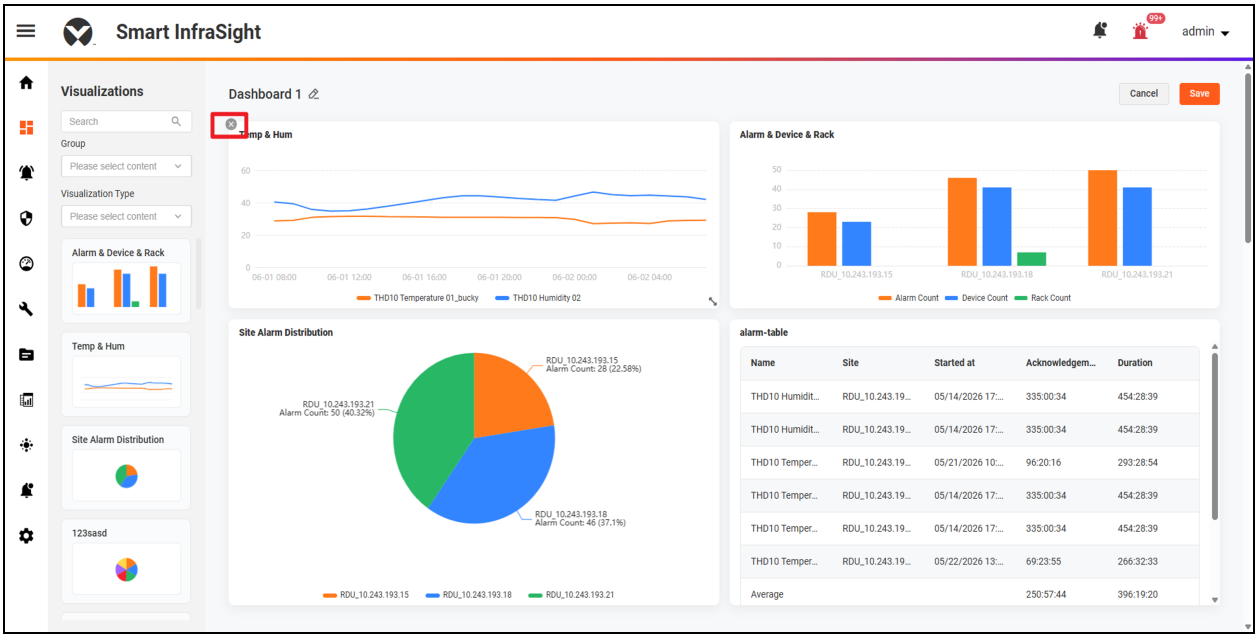
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 9.5 Dragging a Visualization



In edit mode, hover over a widget and click the delete icon in the upper-left corner to remove it.

Figure 9.6 Deleting a Visualization



All operations described above must be performed in edit mode. After completing your edits, click *Save* in the upper-right corner to retain all visualization configurations.

© 2026 Vertiv Group Corp. All Rights Reserved.

9.2.4 Deleting a Dashboard

After configuring a dashboard, all dashboards are visible in the Dashboard list. Hover over a dashboard in the list to reveal the delete icon. Click the *delete* icon, and the platform prompts you to confirm the deletion. Click *Confirm* to proceed. The Dashboard list refreshes automatically, navigates to the first dashboard, and displays a deletion success message.

NOTE: All dashboards are visible and editable to any user with Dashboard permission. Proceed with caution when performing delete operations.

© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

10 Alarm

10.1 General

10.1.1 Overview

The Alarm module is a core feature of the Smart InfraSight Platform used to monitor equipment status, retrieve fault information, and execute automatic responses. You can use this module to monitor Active Alarms in real time, trace historical alarms, and export alarm reports. The platform also supports controlling equipment at sites through alarm linkage. Additionally, you can configure alarm suppression rules for specific time periods to reduce unnecessary interference.

10.1.2 Functional Modules

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

- Active Alarms: View the list of real-time triggered alarms that have not ended.
- Alarm History : Search for historical alarms that have ended or were triggered in the past.
- Automations: Configure the devices at the site for linkage control triggered by alarms.
- Alarm Suppression: Configure rules to mask alarms during specific time periods or under specific conditions.

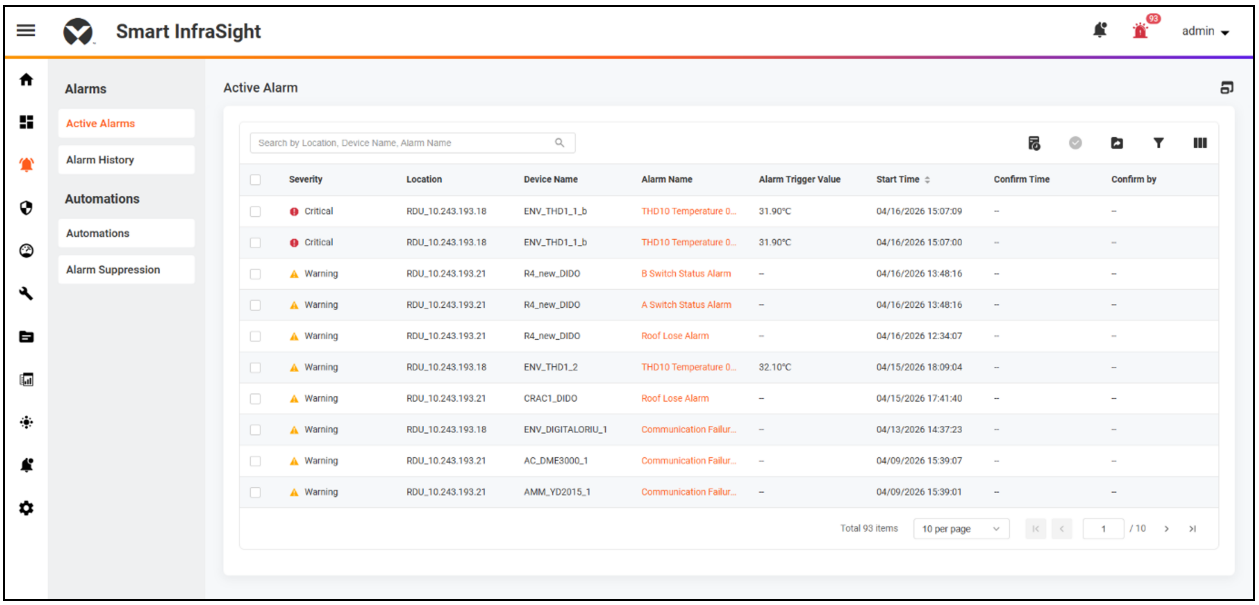
10.2 Detailed Functions

10.2.1 Active Alarms

Select the Active Alarm icon in the primary menu to open the Active Alarms page by default. The alarm list displays the alarm severity icon, location, equipment name, alarm name, trigger value, start time, and confirm time. The Amount of Notes column and receive time column are hidden by default. Click the *column management* icon in the upper right corner of the table to control column visibility, as shown in Figure 10.1 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.1 Active Alarms

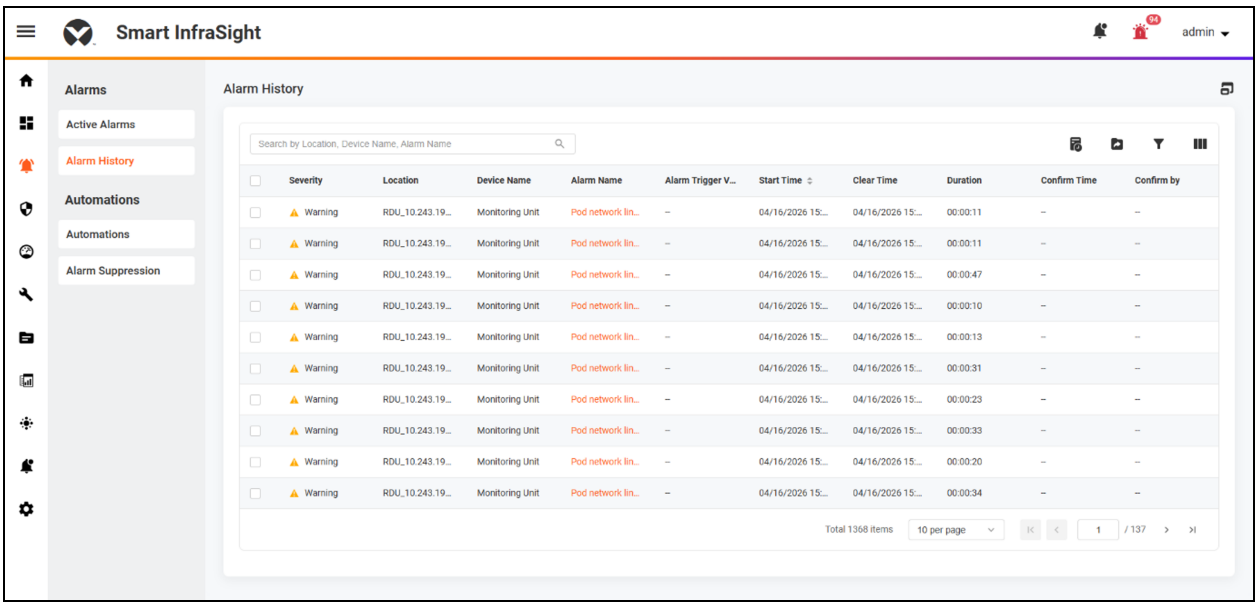


NOTE: If no alarms are found, the list displays **No Data.**

10.2.2 Alarm History

Select the Alarm History in the primary menu to display the list of historical alarms that have occurred in the platform. The list displays the alarm severity icon, location, equipment name, alarm name, trigger value, start time, clear time, duration, confirm time, and acknowledger. The Amount of Notes column and receive time column are hidden by default. Click the column management icon in the upper right corner of the table to control column visibility.

Figure 10.2 Alarm History



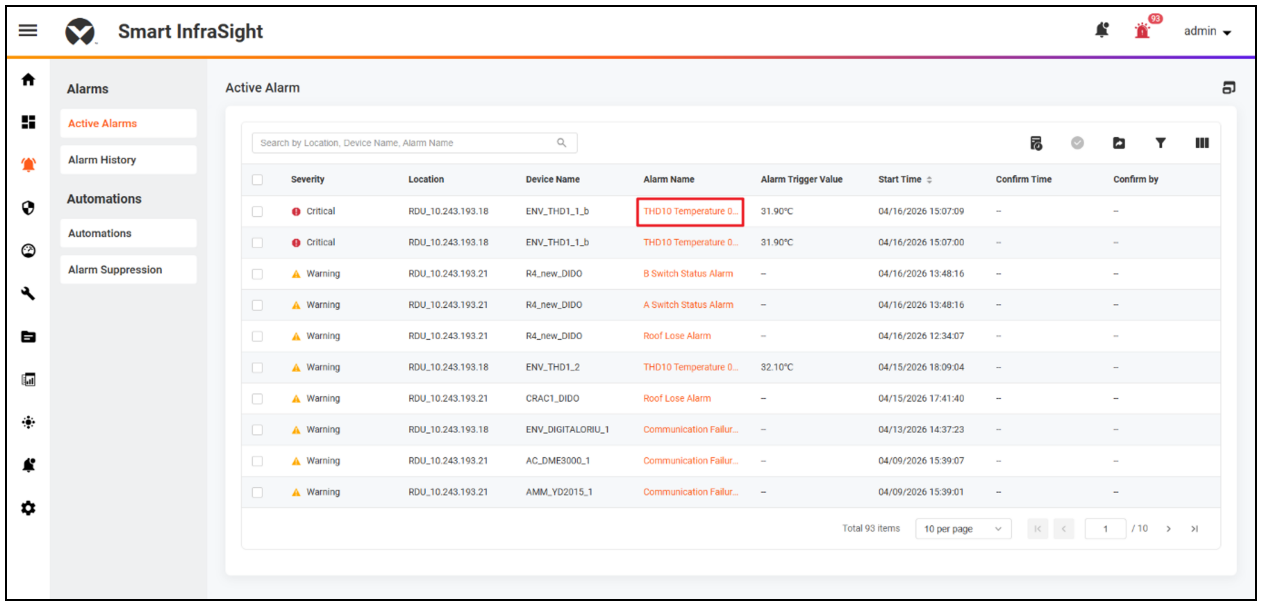
NOTE: If no alarms are found, the list displays **No Data.**

© 2026 Vertiv Group Corp. All Rights Reserved.

10.2.3 View Alarm Details

On the Active Alarms or Alarm History page, click an *alarm* name to view the alarm details.

Figure 10.3 Viewing Alarm Details



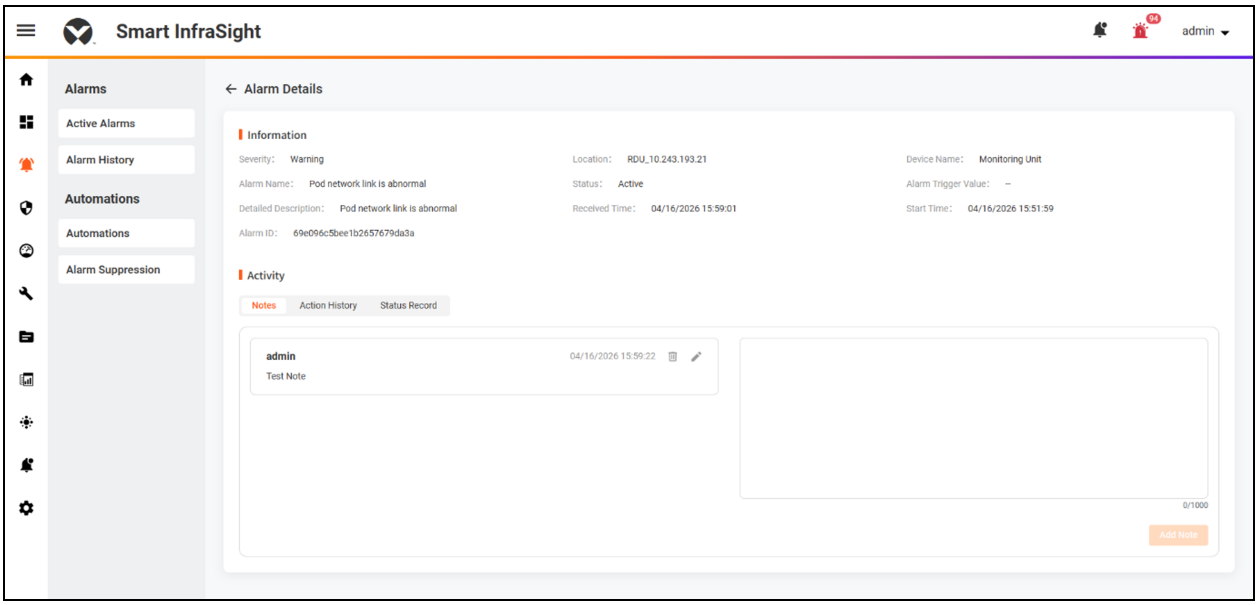
In addition to the attributes displayed in the alarm list, the alarm details page provides features to add alarm notes, view action history, and view status records.

10.2.4 Alarm Notes

On the alarm details page, click the *Notes* tab at the bottom, enter relevant notes in the text box, and click Add Note. Successfully added notes appear in the note list below, Click on the *edit* icon to edit a note or click on the *delete* icon to delete a note.

© 2026 Vertiv Group Corp. All Rights Reserved.

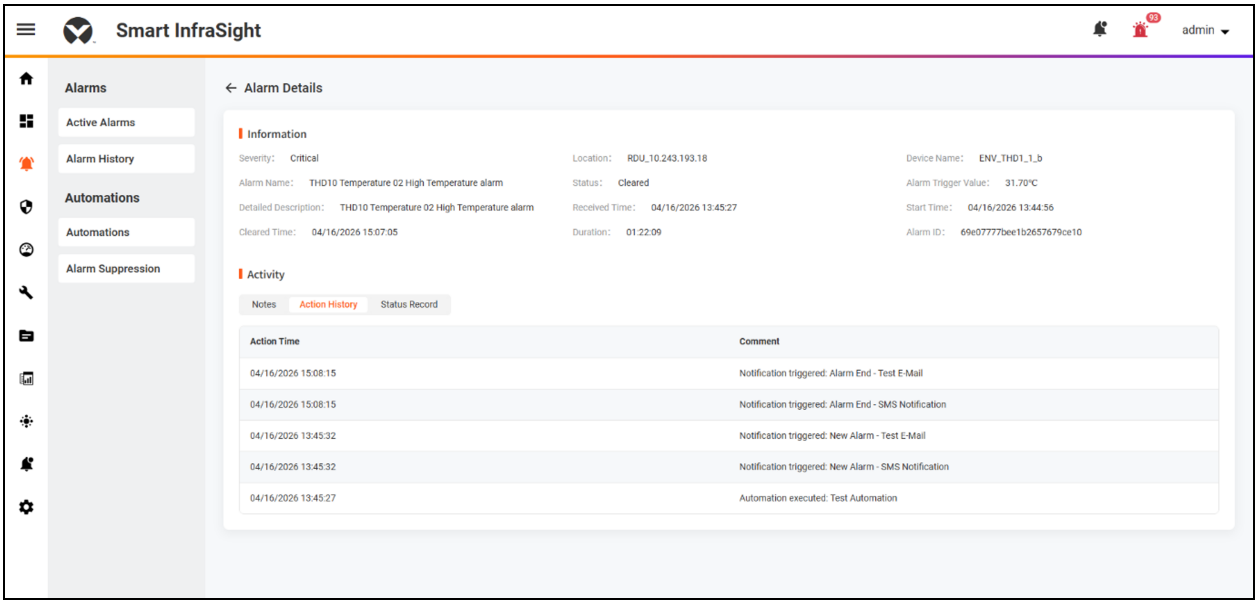
Figure 10.4 Adding Alarm Notes



10.2.5 Action History

On the alarm details page, click the *Action History* tab at the bottom to view the configured alarm notification records for this alarm.

Figure 10.5 Viewing the Action History

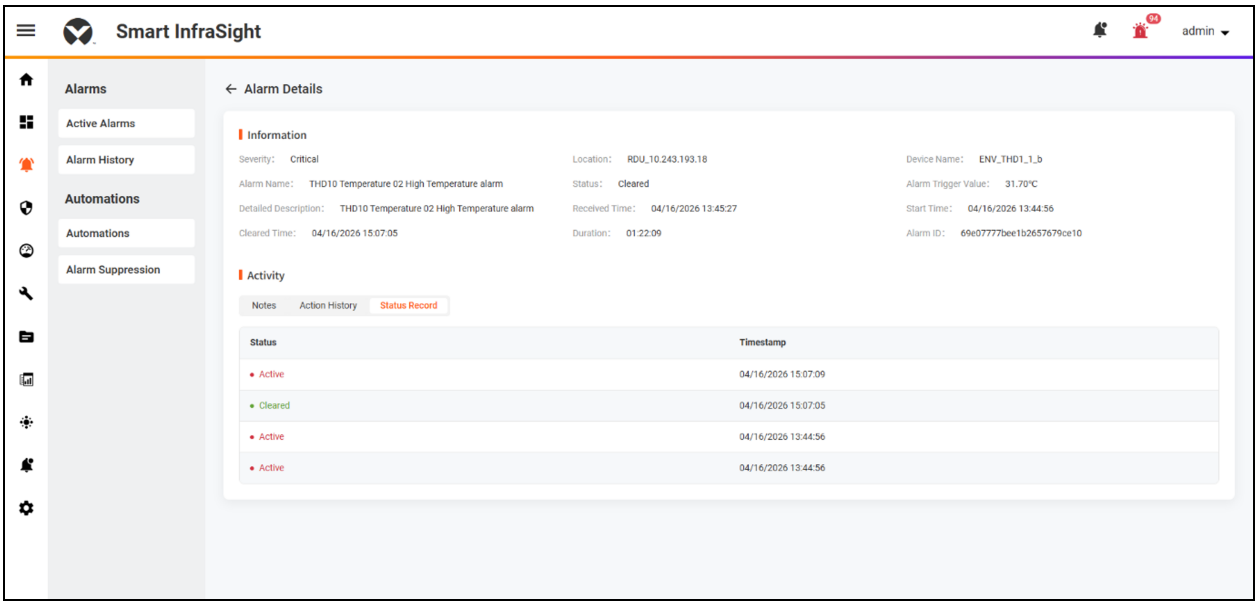


10.2.6 Alarm Status Records

On the *Alarm Details* page, click the *Status Records* tab at the bottom to display the status record of the alarms as shown in Figure 10.6 on the facing page , such as alarm start time and end time).

© 2026 Vertiv Group Corp. All Rights Reserved.

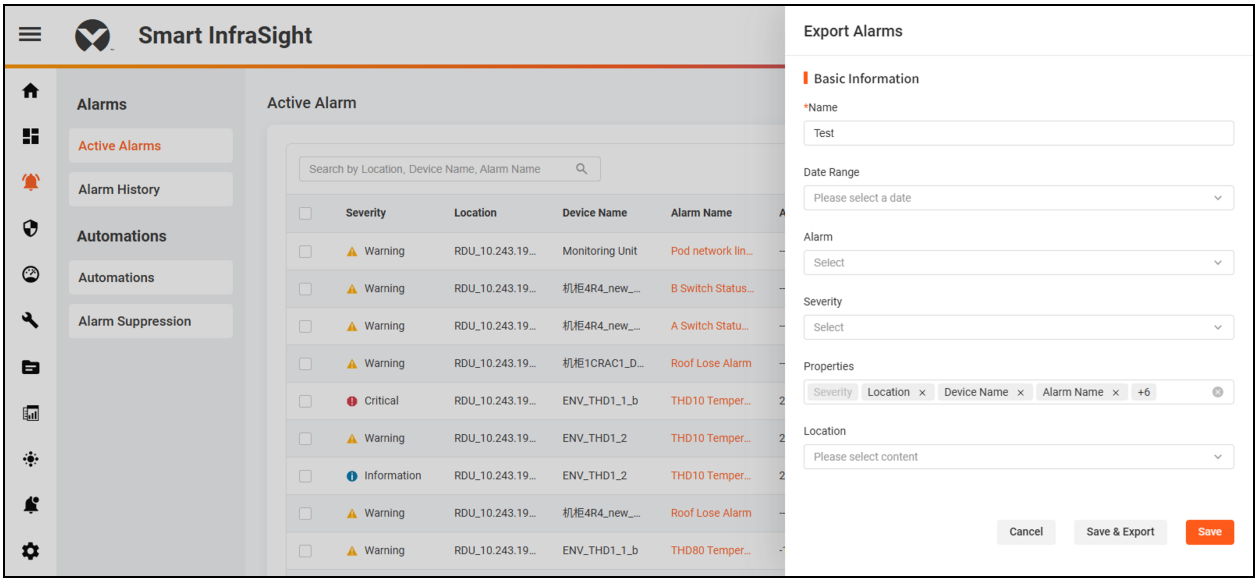
Figure 10.6 Viewing the Alarm Status Record



10.2.7 Export Alarms

On the alarm list page, click *Export* in the upper right corner, as shown in **Figure 10.7** below In the right panel that appears, enter the export file name, and select the alarm type, date, alarm severity, and specific fields to export. Click *save*.

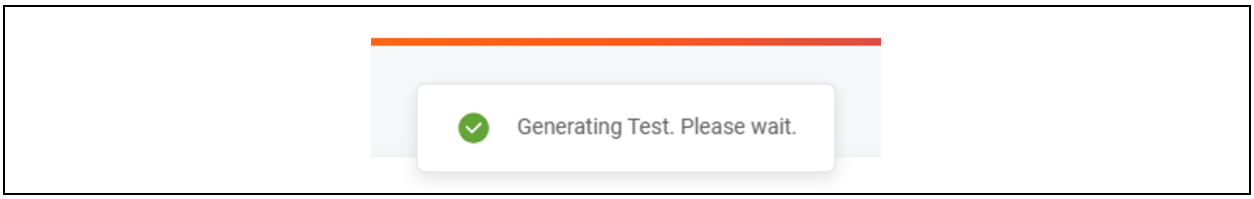
Figure 10.7 Export Alarms



After you click *save*, a prompt indicates that the file is generating, as shown in **Figure 10.8** on the next page .

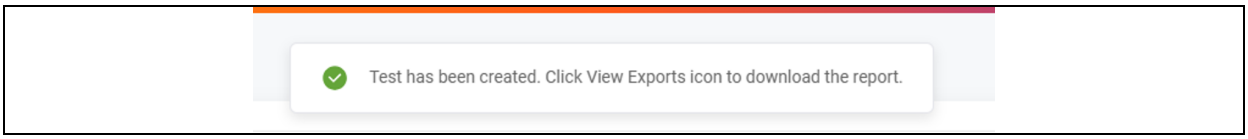
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.8 Generating Export Alarms Prompt



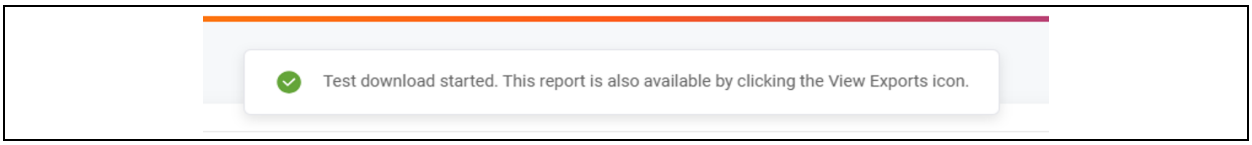
Upon successful export, a success prompt appears, as shown in Figure 10.9 below .

Figure 10.9 Export Success Prompt



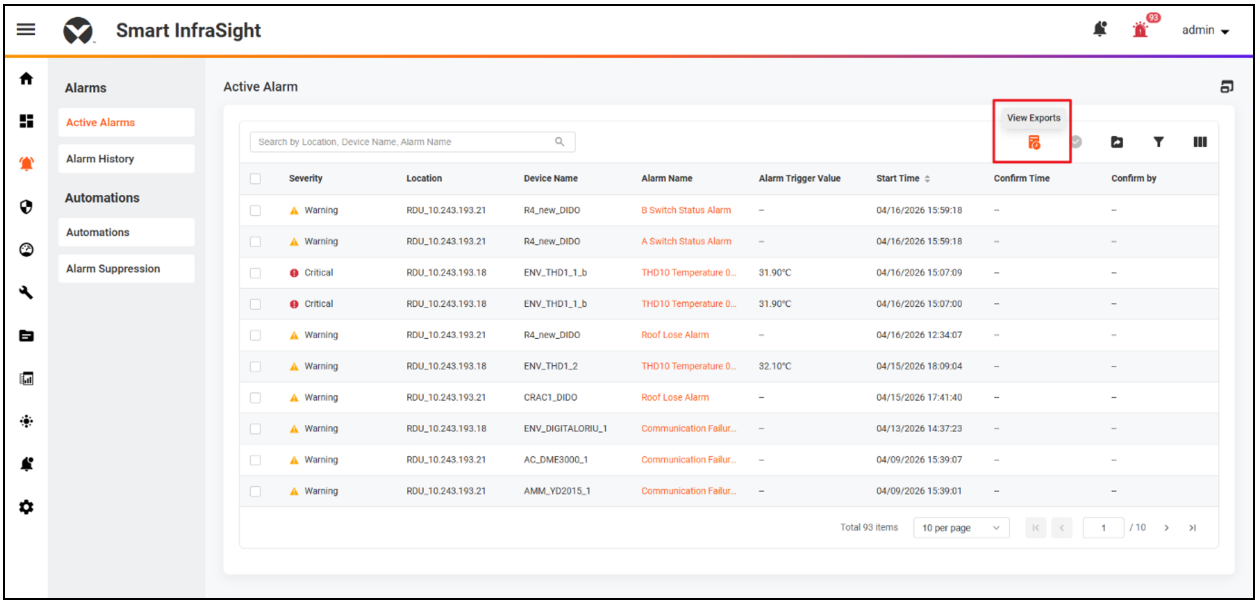
After clicking the *Save* button, you will be prompted that the export file has been generated successfully.

Figure 10.10 View Exports



Click the *Save and Export* button, and the exported file will be automatically downloaded after it is successfully generated, as shown in Figure 10.12 on the facing page .

Figure 10.11 View Exports

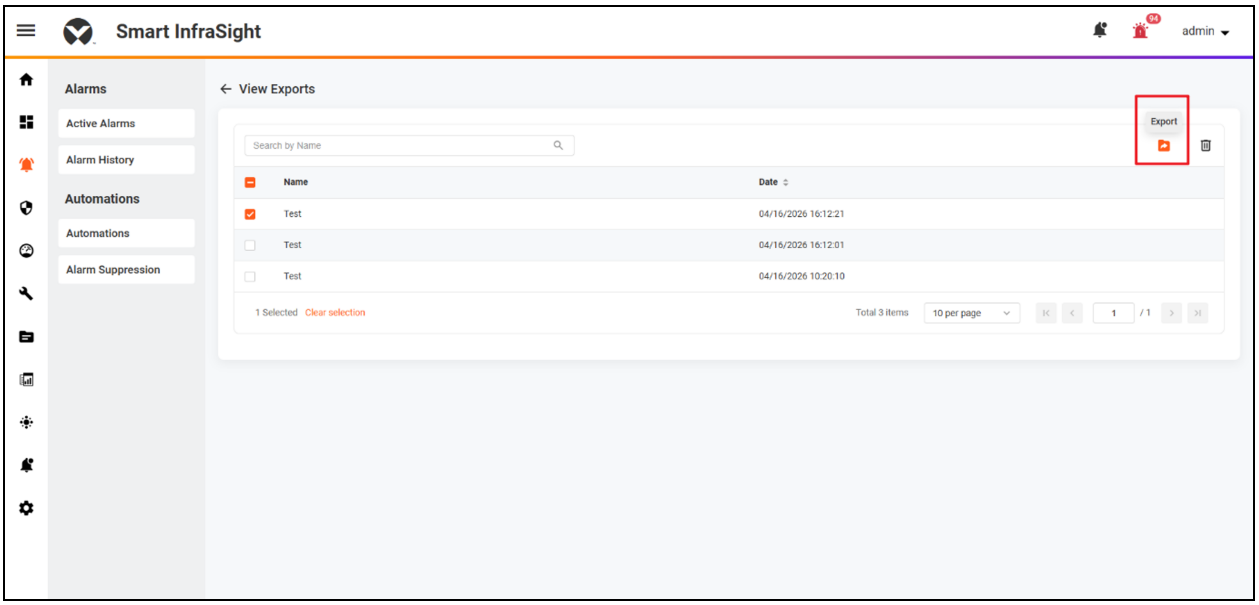


On the alarm export records page, you can download the table.

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

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.12 Downloading and Exporting the Report to Excel



10.2.8 Automations

Automations List

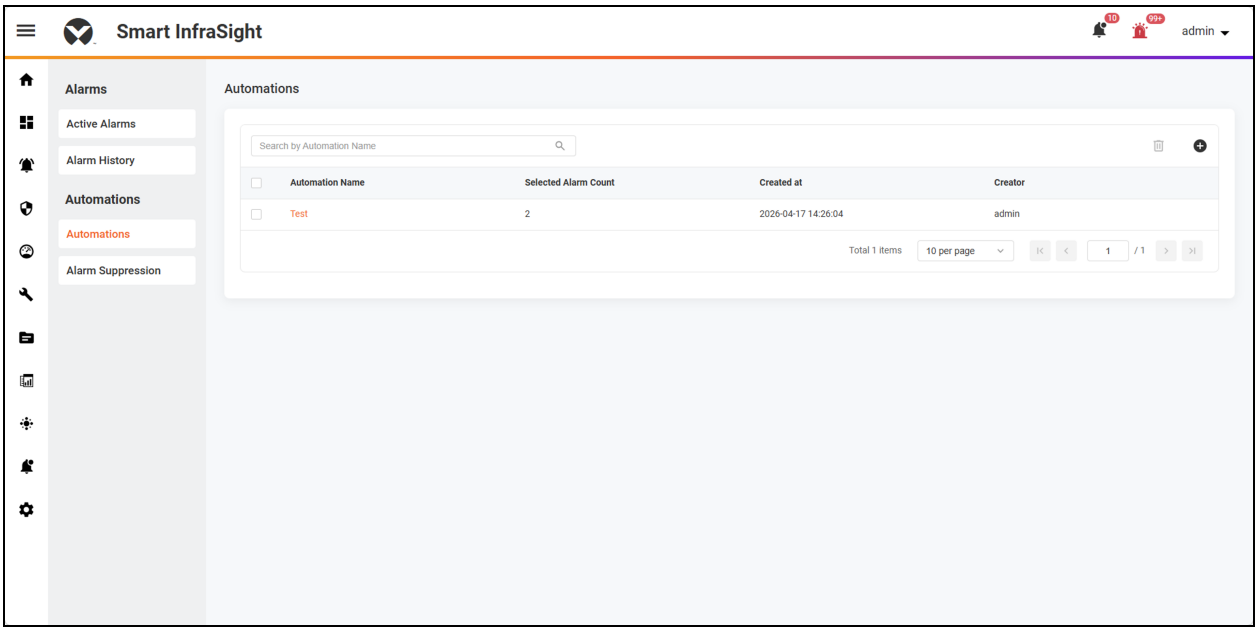
The Automations page displays all created Automations entries in a list format. The list contains the following columns: Automation Name, Number of Selected Alarms, Created Time, and Created By.

Enter a Automation name keyword in the search bar to quickly filter target entries. The list supports paginated display. You can adjust the number of entries per page or navigate to a specific page number in the bottom-right corner.

1. Select one or more Automations and click the Delete icon in the top-right corner to batch delete the selected entries.
2. Click a *Automations* name to enter the edit page for that Automation.
3. Click the (+) icon in the top-right corner to enter the Add Automation page. As shown in Figure 10.13 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.13 Automations List



Adding Automation

The process of adding an Automation consists of three steps: Select Alarms → Configure Actions → Preview and Confirm.

Step 1: Select Alarms

Enter a name in the Automations Name field. The name must be 1–32 characters long and does not support special characters. If unsupported characters are entered, the page displays the following message: "Contains unsupported characters: ~\ ` !@$%^&*=[]{}|:;'",<>?".

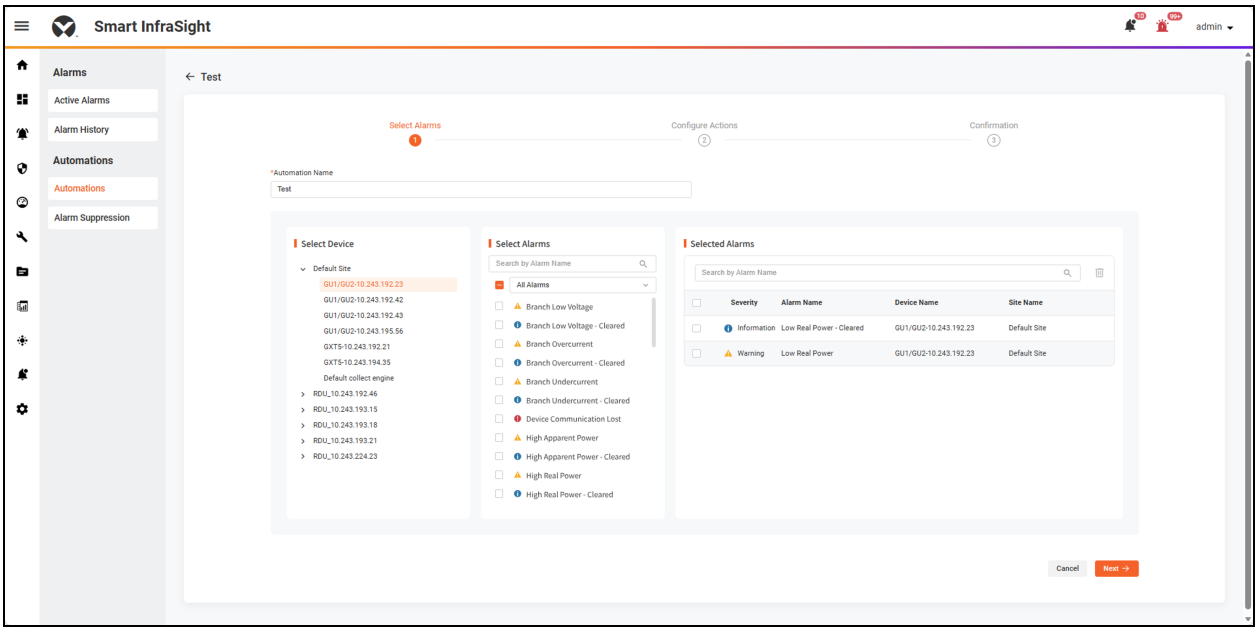
The alarm selection area is displayed in three side-by-side columns:

- **Select Device**: Expand the device tree by site hierarchy and click to select the target device.
- **Select Alarms**: Displays all available alarms under the selected device. Supports searching by alarm name. Select individual alarms or use All Alarms to select all entries in bulk. Alarm entries use icons to indicate severity: a red circle icon for critical alarms, a yellow triangle icon for major alarms, and a blue circle icon for minor alarms.
- **Selected Alarms**: Displays all currently selected alarm entries in real time. The list contains four columns: Severity, Alarm Name, Device Name, and Site Name. Supports searching by alarm name and removing selected entries.

At least one alarm must be selected before you can click *Next* to proceed to Step 2: Configure Actions on the facing page. As shown in **Figure 10.14** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.14 Selecting an Alarm



Step 2: Configure Actions

The top of the **Figure 10.15** on the next page provides the following global parameter configuration options:

Action Execution Order: Drop-down list. Required. Select either Execute Simultaneously or Execute Sequentially.

Automations Delay: Input field (minutes + seconds). Required. Default value is 0 minutes 5 seconds. This defines the delay between when a selected alarm is triggered and when the Automations actions are initiated.

Action Execution Interval: Input field (minutes + seconds). Required when Action Execution Order is set to Execute Sequentially. Default value is 0 minutes 0 seconds. This defines the time interval between each action during sequential execution.

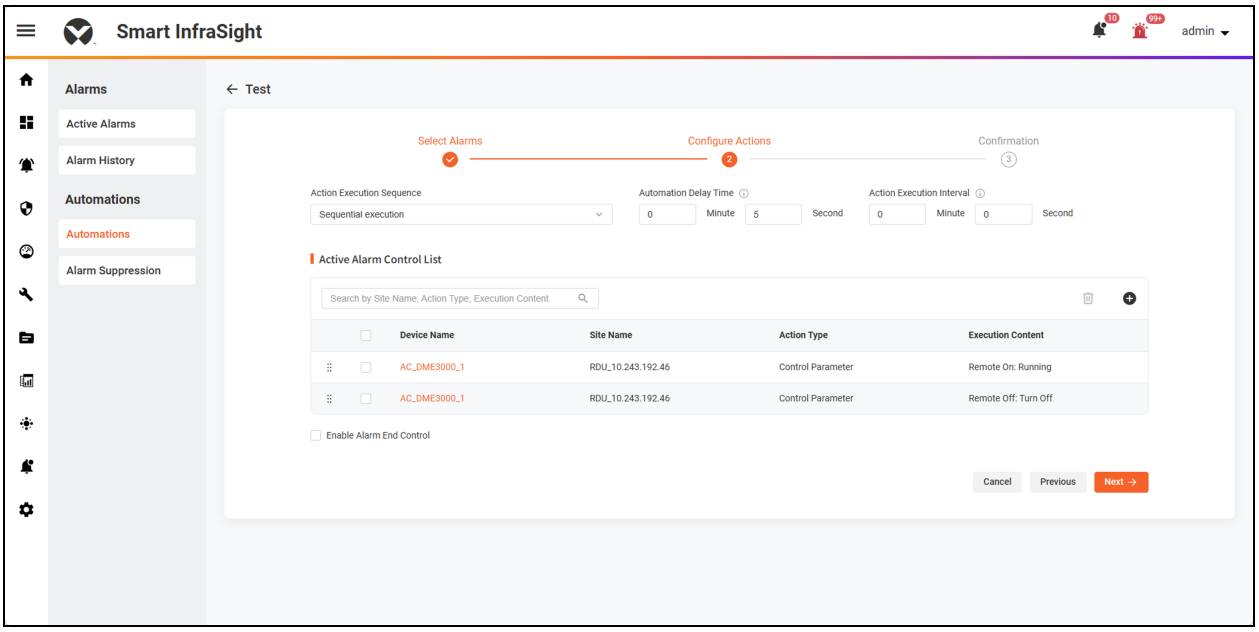
The Active Alarm Control List at the bottom of the Figure below displays all added Automations actions. The list contains five columns: **Order, Device Name, Site Name, Action Type**, and **Execution Content**. Supports searching by site name, action type, and execution content. Select entries and click the Delete icon to remove them. Click (+) in the top-right corner of the list to add a new Automations action. The platform displays the Add Automations Action dialog box.

After enabling Alarm Clearance Control at the bottom of the **Figure 10.15** on the next page , a Cleared Alarm Control List appears below the active alarm control list. Use this list to configure Automations actions that are triggered when an alarm is cleared.

After completing the action configuration, click *Next* to proceed to Step 3: Preview and Confirm on page 179.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.15 Configuring the Actions



Add Automations Action Dialog Box as shown in **Figure 10.16** on the facing page .

The fields in the dialog box are as follows:

Action Type: Remote Control

Select Site: Drop-down list. Select the site to which the target device belongs.

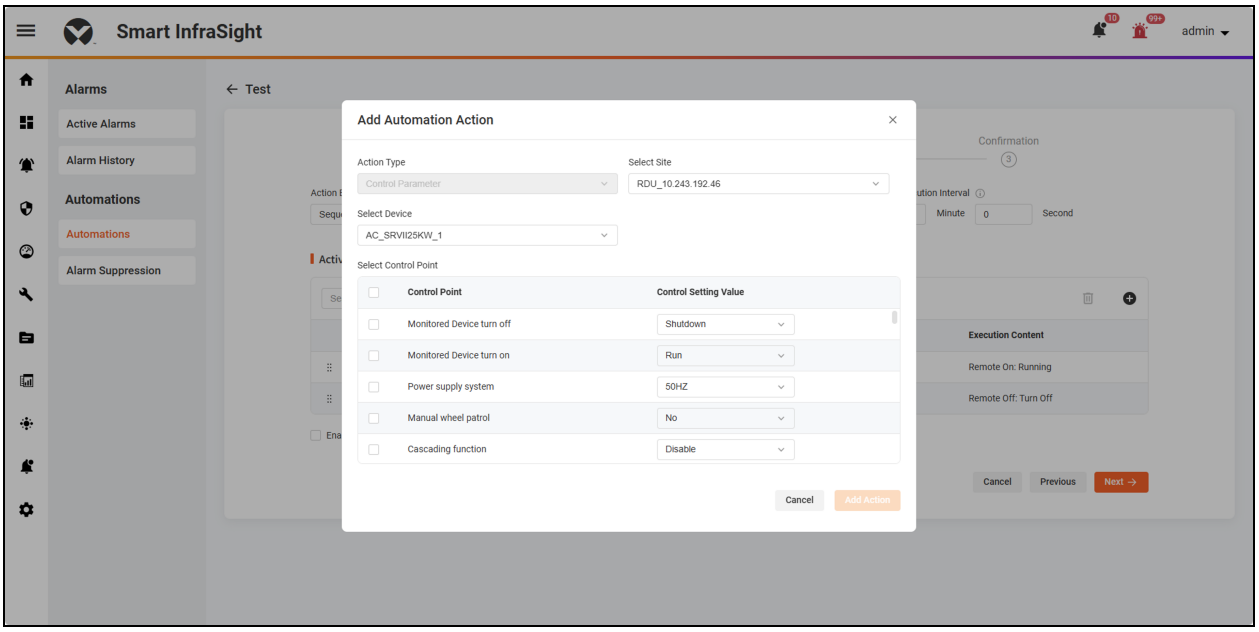
Select Device: Drop-down list. Select the target device on which the Automations action is to be executed.

Select Control Signal: Displays all control signals supported by the selected device in a list format. Each control signal has a corresponding Control Signal Set Value drop-down list for specifying the execution value of that signal. Select the checkbox at the top to select all control signals in bulk, or select individual entries as needed.

After completing the configuration, click *Add Action* to add the action to the Active Alarm Control List. Click *Cancel* to close the dialog box without saving.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.16 Adding an Automation Action



Step 3: Preview and Confirm

The **Figure 10.17** on the next page displays a read-only summary of all configuration details for the current Automations, organized into the following three sections:

Basic Information: Displays the Automations name.

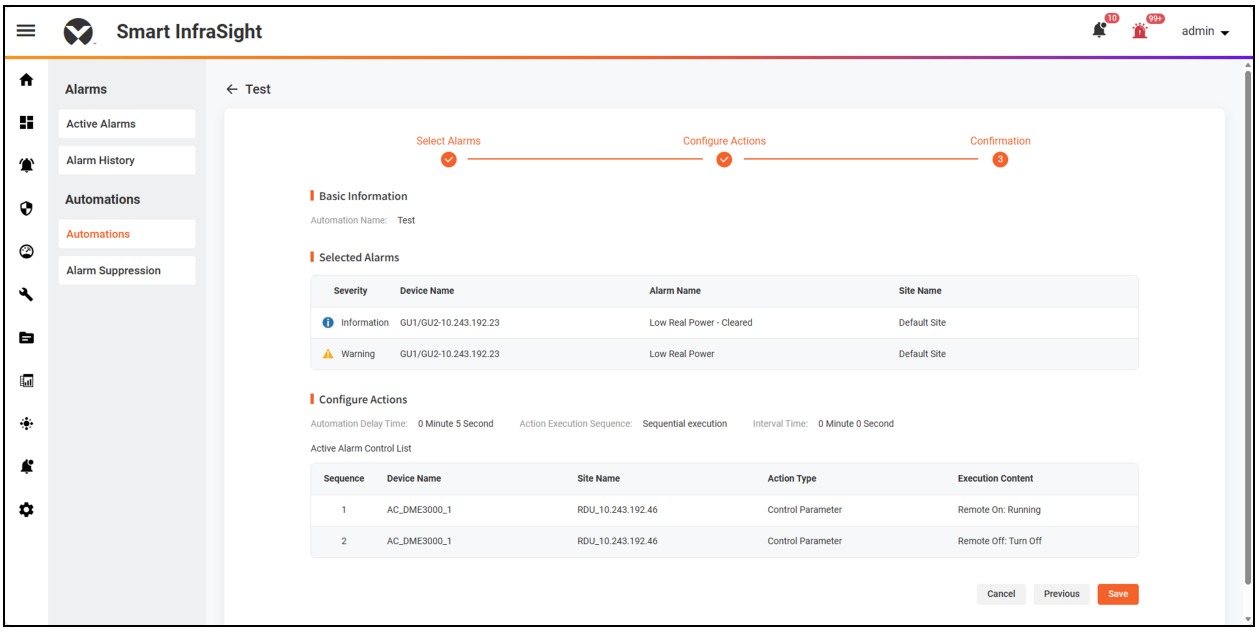
Selected Alarms: Lists all selected alarms in a table format with four columns: Severity, Device Name, Alarm Name, and Site Name.

Configured Actions: Displays global parameters including Automations delay, action execution order, and execution interval, as well as the Order, Device Name, Site Name, Action Type, and Execution Content for each action in the Active Alarm Control List.

After confirming that the configuration is correct, click *Save* to complete the addition. To make changes, click *Previous* to return to the previous step. Click *Cancel* to discard the current addition and return to the Automations list.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.17 Confirmation Window



Edit Automation

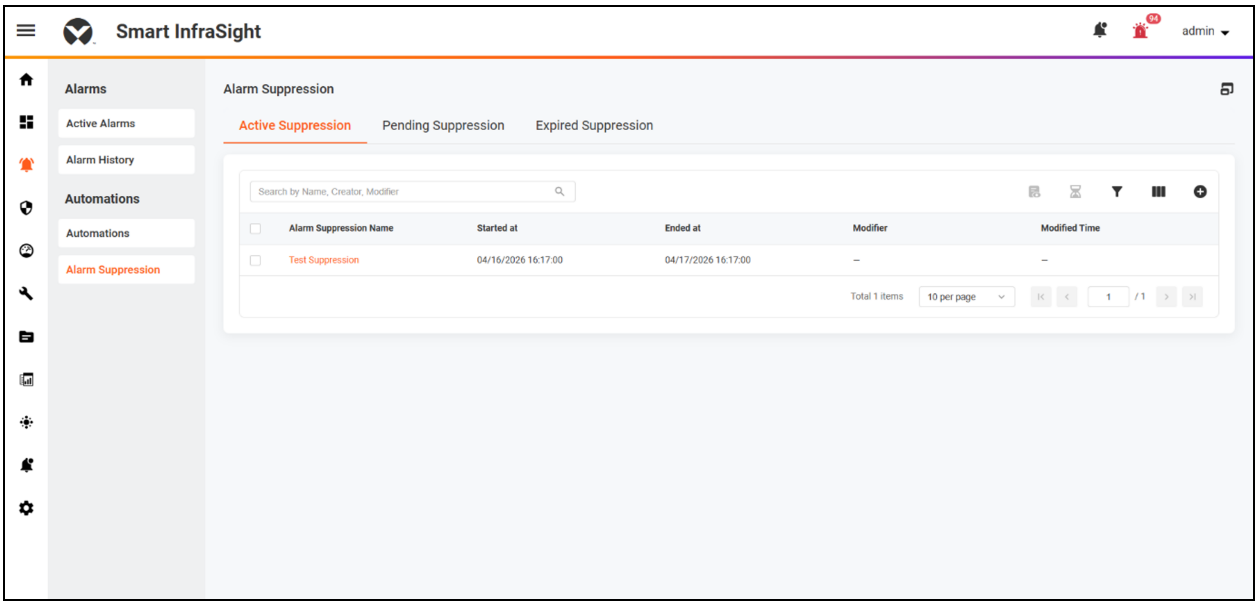
Refer to Add Automations Setting Adding Automation on page 176.

10.2.9 Alarm Suppression

When alarm binding relationships are configured, but you need to temporarily ignore alarm notifications for specific sites, equipment, or signals (for example, during equipment maintenance), you can create an alarm suppression rule. This prevents alarms generated by the selected sites or equipment from triggering alarm notifications during a specific time period. On the Alarm Suppression page, click the *Add* button to navigate to the new alarm suppression rule page, as shown in the **Figure 10.18** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.18 Alarm Suppression

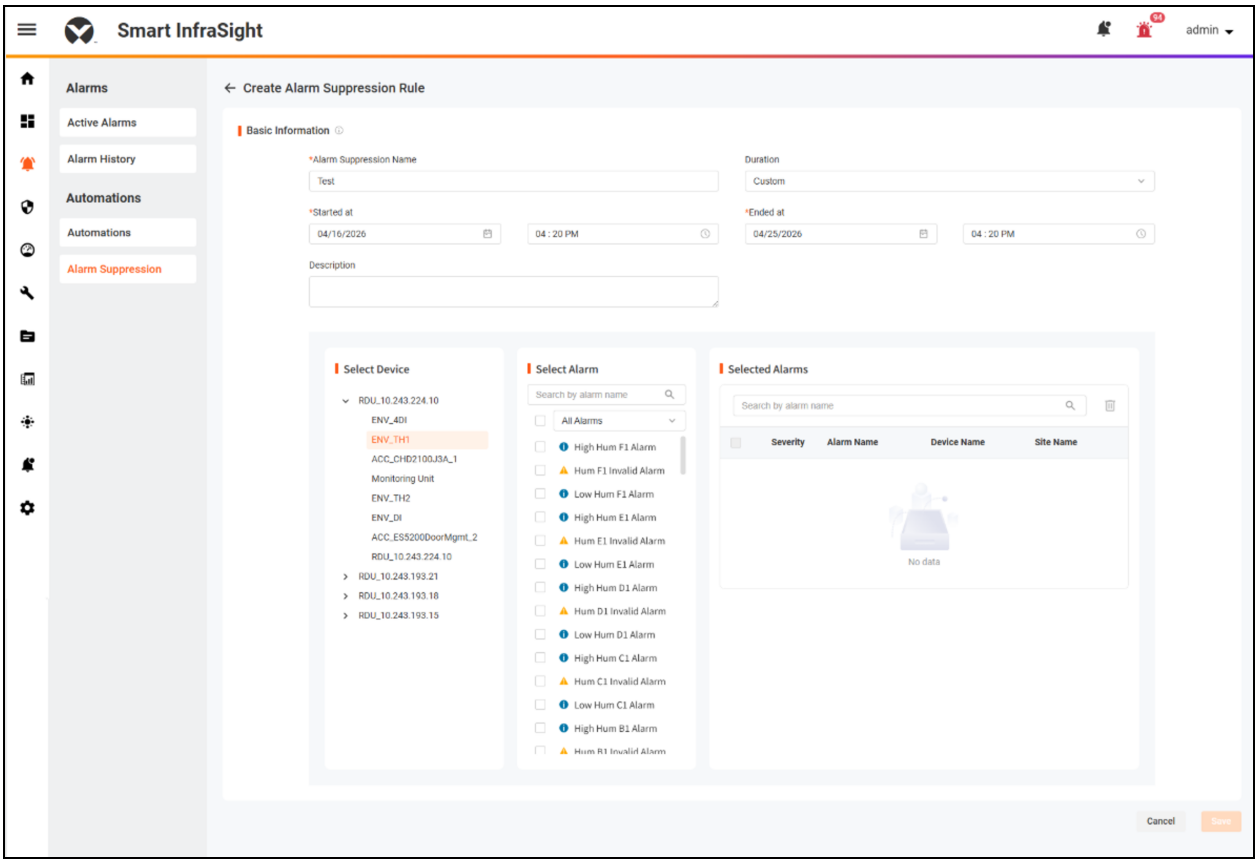


Adding an Alarm Suppression Rule

Go to the Add Alarm Suppression Rule page. Select the alarms to suppress. Once an alarm is masked, it no longer sends any alarm notifications or triggers automations. You can query the alarm information in Active Alarms or Alarm History. Select the suppression duration, including the start and end times. Notifications resume after the end time, or you can choose to keep the alarm suppressed indefinitely. Enter an alarm rule name and Description (optional), and click *Save* to save the alarm suppression rule. As shown in Figure 10.19 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.19 Adding Alarm Suppression Rule

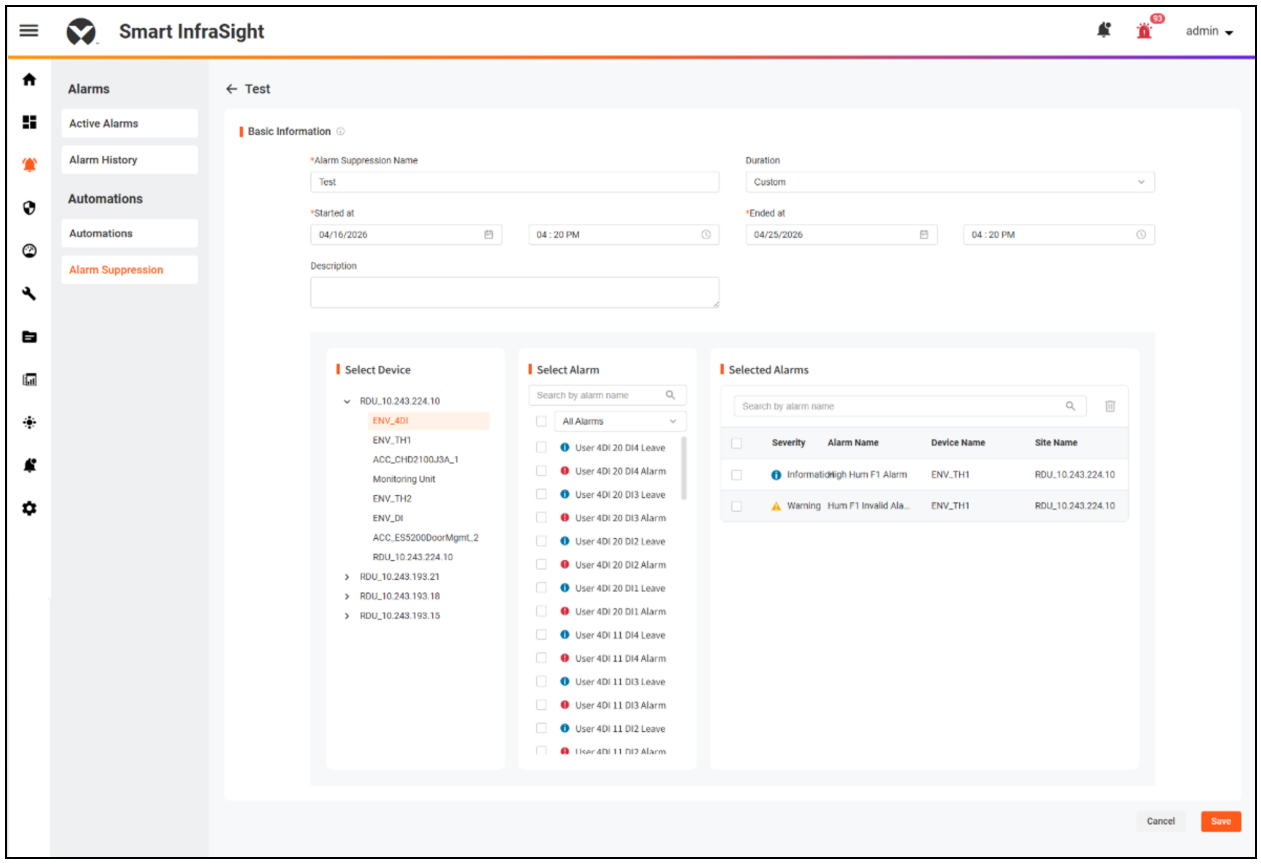


Editing an Alarm Suppression Rule

On the Alarm Suppression Rules list page, click a *rule* name to enter the edit page for that rule. As shown in **Figure 10.20** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.20 Editing an Alarm Suppression Rule



Viewing the Suppressed Alarms

On the Alarm Suppression Rules list page, after selecting a rule, click *Preview* Alarms in the upper right corner of the table to query alarms whose notifications are masked by this rule. As shown in **Figure 10.21** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 10.21 Viewing the Suppressed Alarms

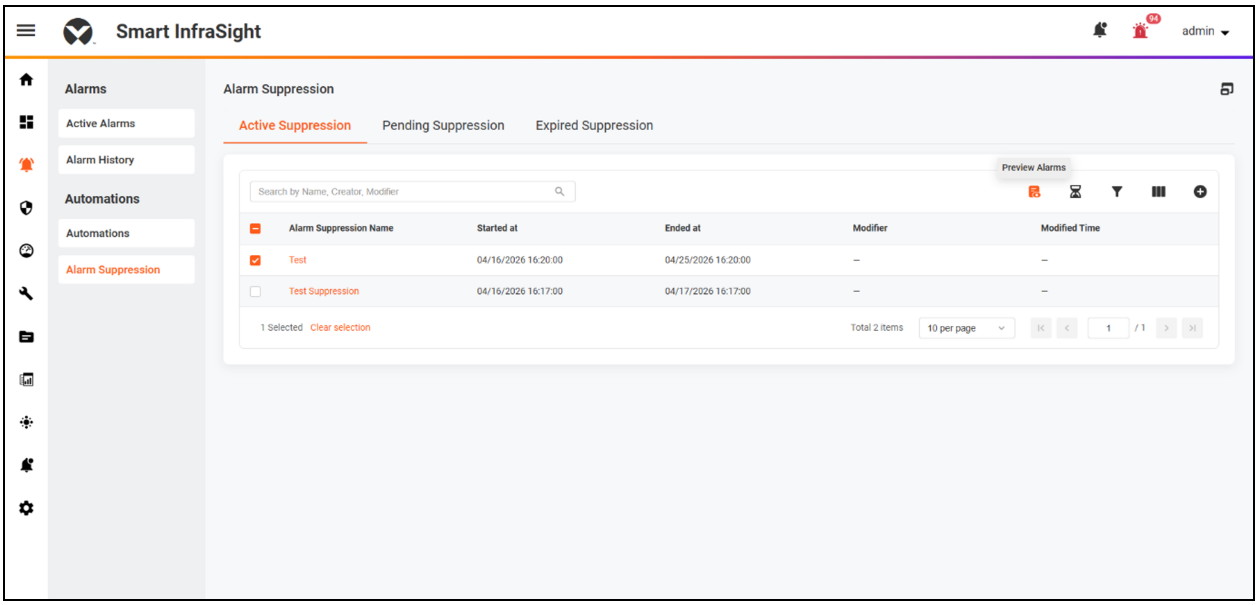
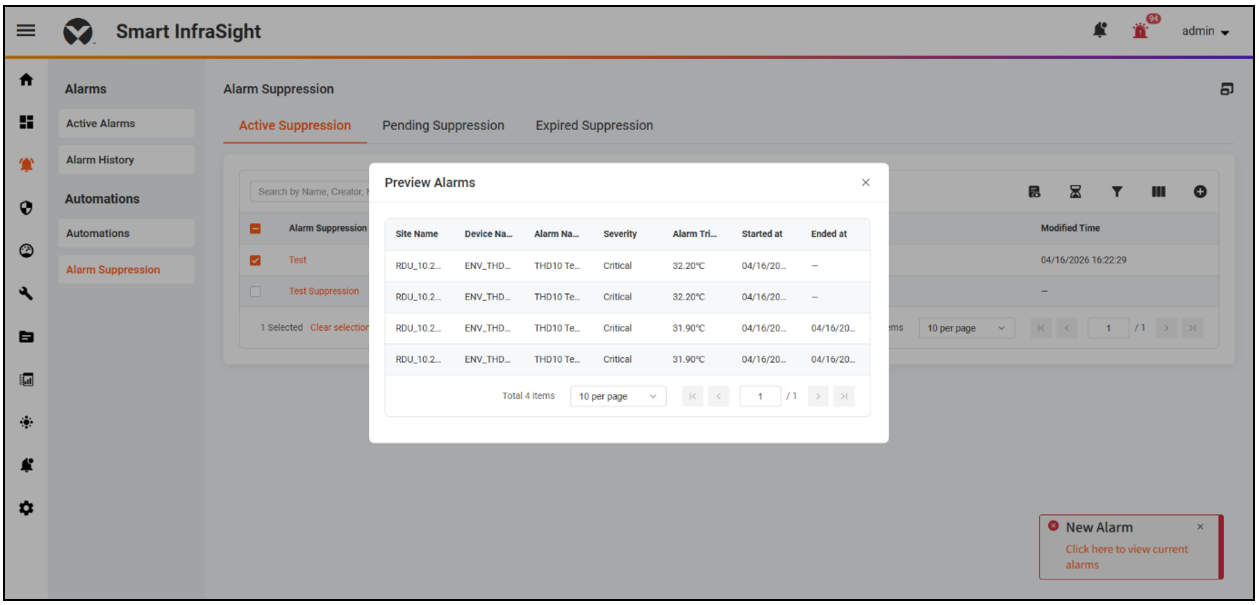


Figure 10.22 Viewing the Suppressed Alarms - Alarm Table



Manually Expire Alarm Suppression Rules

On the Alarm Suppression Rules list page, after selecting a rule, click the *Expire* icon in the upper right corner of the table to manually expire it. Once expired, the rule automatically becomes invalid and can be viewed in the Expired Suppression Rules list.

© 2026 Vertiv Group Corp. All Rights Reserved.

Copy Expired Alarm Suppression Rules

On the Expired Alarm Suppression Rules list page, click a rule name to view the settings of the expired rule. After selecting an expired rule, click the *copy* icon in the upper right corner of the table to navigate to the Add Alarm Suppression Rule page. The platform automatically imports the configuration information from the original rule. Reconfigure the suppression duration, enter a new suppression rule name, and save to create a new alarm suppression rule.

© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

11 Security

11.1 General

11.1.1 Overview

The Security module provides centralized management of site access control and video surveillance. You can use this module to configure doors, access cards, permission groups, and access schedules, while also tracking door status, access events, and related alarms. In addition, you can view live and recorded videos, query events and access logs, and manage NVR and IPC devices, helping you monitor and control physical security activities from a single platform.

11.1.2 Functional Modules

The Vertiv™ Smart InfraSight™ Security includes the following functional modules. For detailed descriptions of each module, see Detailed Features below.

- Door Access Monitoring: Add and manage IP access controllers and doors, configure door unlock permissions, synchronize data to devices, and view real-time signals, alarms, control commands, and configuration signals.
- Card Management: Add, edit, delete, and search access cards. Configure cardholder information, fingerprint data, and authorize door unlock permissions for access control devices.
- Time Setting: Configure time ranges and assign them to permission groups to define when access cards are allowed to unlock doors.
- Log Query: View and search access logs and door event logs, with support for filtering and sorting.
- Real Time Video: Preview live video feeds from IPC devices, with support for image capture, video recording, electronic zoom, and split-screen display.
- History Video: Search, play, and download recorded videos by date and device, with support for playback control and batch downloading.
- Device Management: Add, edit, and delete NVR devices, and manage IPC devices within NVR channels.

11.2 Detailed Features

11.2.1 Door Access Monitoring

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

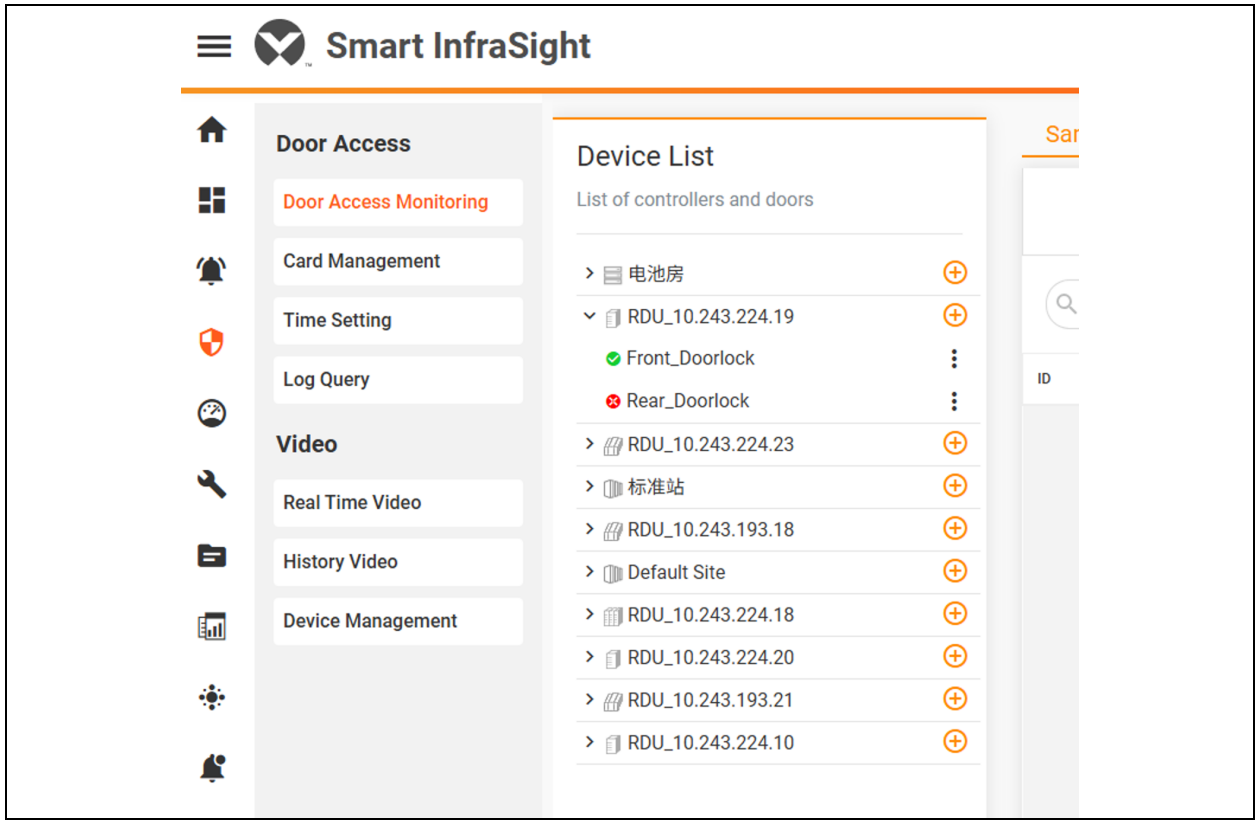
- Adding, removing and modifying the IP access controller.
- Adding, removing and modifying the door that connected to the IP access controller.
- Synchronizing the data to IP access controllers.
- Configuring the door access permissions for the access control cards through the IP-based controller.
- Configuring the door access permissions for the access control cards through the serial-based controller.
- Viewing the real-time signals, active alarms, control commands, and setup signals for access controllers.

© 2026 Vertiv Group Corp. All Rights Reserved.

Access Control Device List

In the top-level menu, select *Security*. The **Access Control Monitoring** page opens by default. On this page, you can add IP access controllers and their doors. Serial access control devices connected through the RDU collector are displayed here automatically. The icon preceding the controller name indicates its communication status: a green icon indicates normal communication, and a red icon indicates a communication failure, as shown in **Figure 11.1** below .

Figure 11.1 Access Control Device List



NOTE:

1. If no access control controllers have been added to the platform, the Access Control Device list displays site information only.

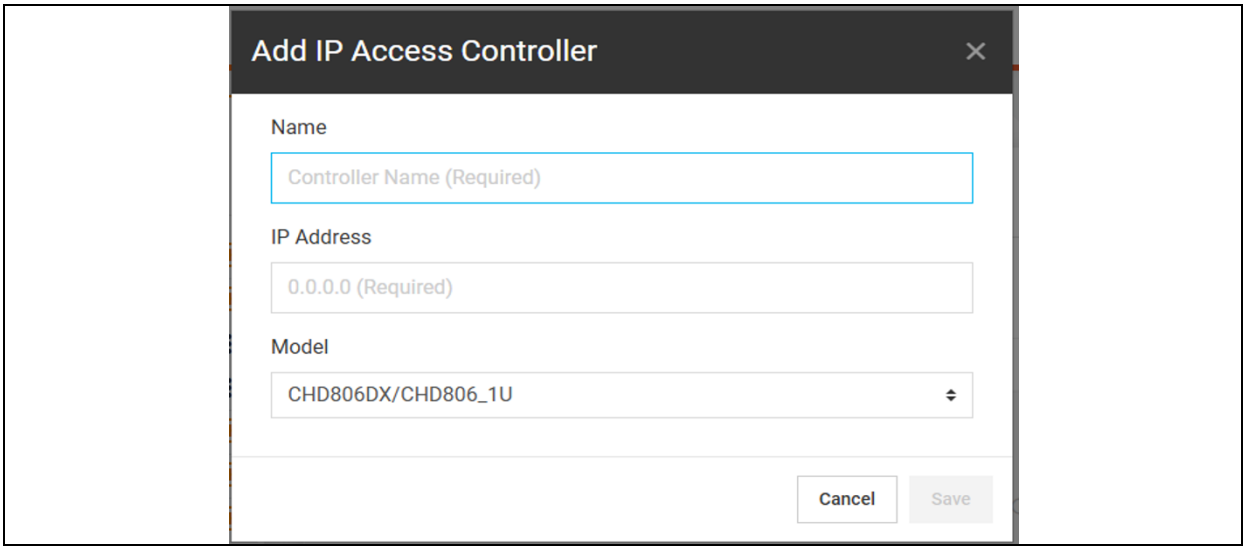
2. The Device list interface differs between administrator group users and standard users. Standard users cannot perform operations such as adding IP controllers, adding doors, or granting permissions.

© 2026 Vertiv Group Corp. All Rights Reserved.

Adding an Access Controller

1. Click *Add IP Access Controller* button. The dialog box is as shown in **Figure 11.2** below .
2. Enter the name and IP address of the IP access controller, select the model of the access controller, and click *Save* button.

Figure 11.2 Adding IP Access Controller



NOTE:

1. This function is available to administrator group users only.

2. The access control controller name must be 3–64 characters and must be unique.

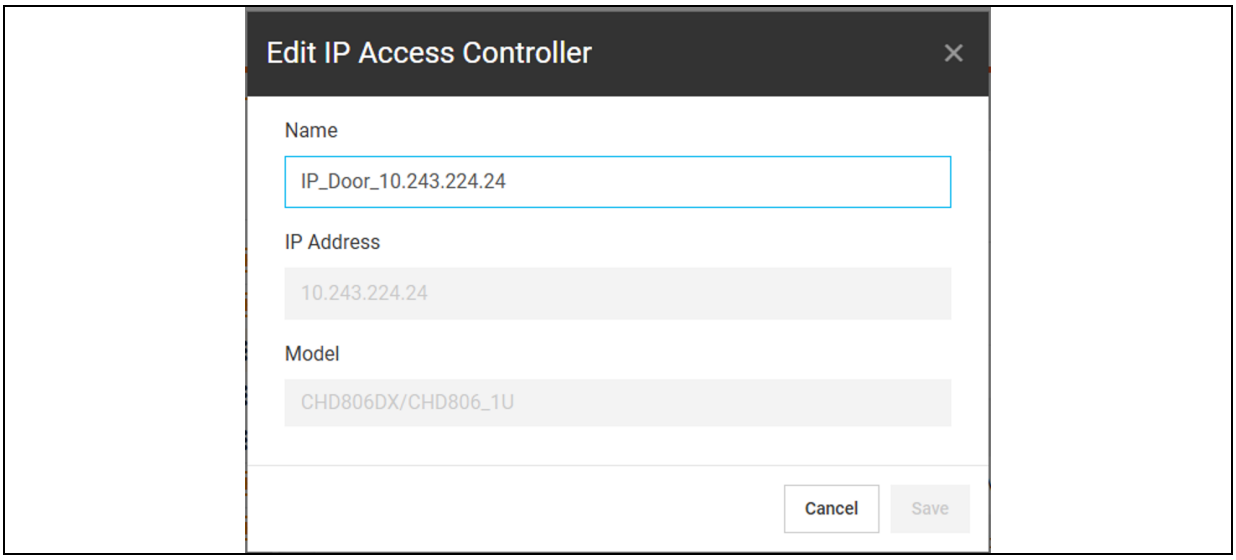
3. The name and IP address are required fields. The Save button is only enabled after all required fields are completed and validated successfully.

Editing the Access Controller

Click the *button* to the right of the IP access control controller name, select **Edit IP Access Control Controller** from the drop-down list. The Edit IP Access Control Controller dialog box appears. Modify the controller name and click *Save*, as shown in **Figure 11.3** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.3 Editing the Access Controller



NOTE:

1. This function is available to administrator group users only.

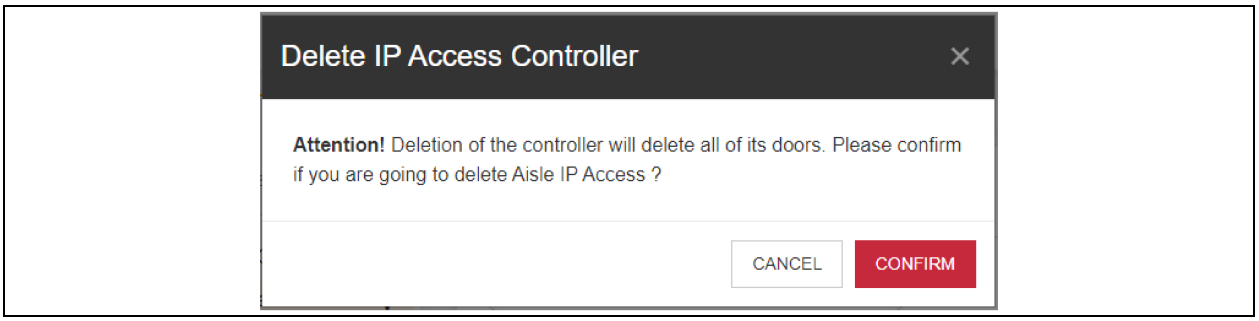
2. The IP address and model of the access controller cannot be modified. To change these, delete the controller and add it again.

3. The name and IP address are both required fields. The Save button can only be clicked after all required information has been entered and validated successfully.

Deleting 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 11.4** below .

Figure 11.4 Deleting the IP Access Controller



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

NOTE:

1. This function is available to administrator group users only.

2. The IP address and model of the access controller cannot be modified. To change these, delete the controller and add it again.

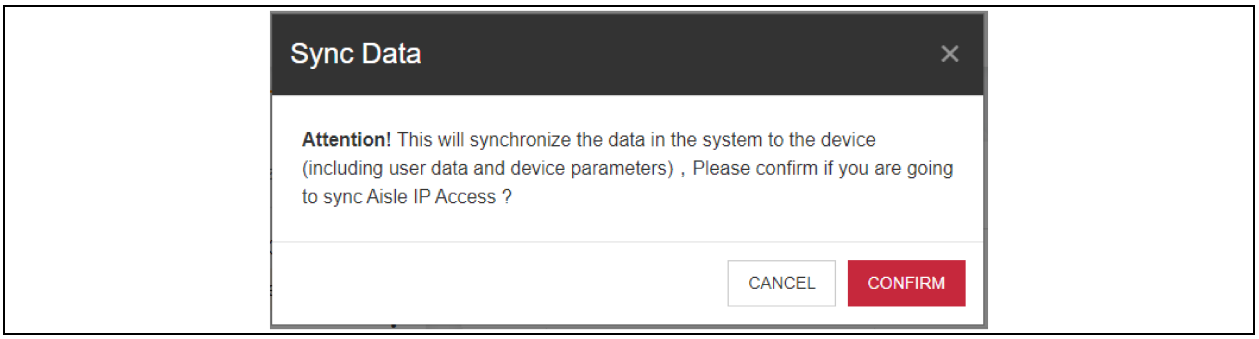
© 2026 Vertiv Group Corp. All Rights Reserved.

3. In the Edit dialog box, the Save button is only enabled after changes have been made.

Sync data

1. Click the ellipses (⋮) on the right side 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 11.5 below .

Figure 11.5 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:

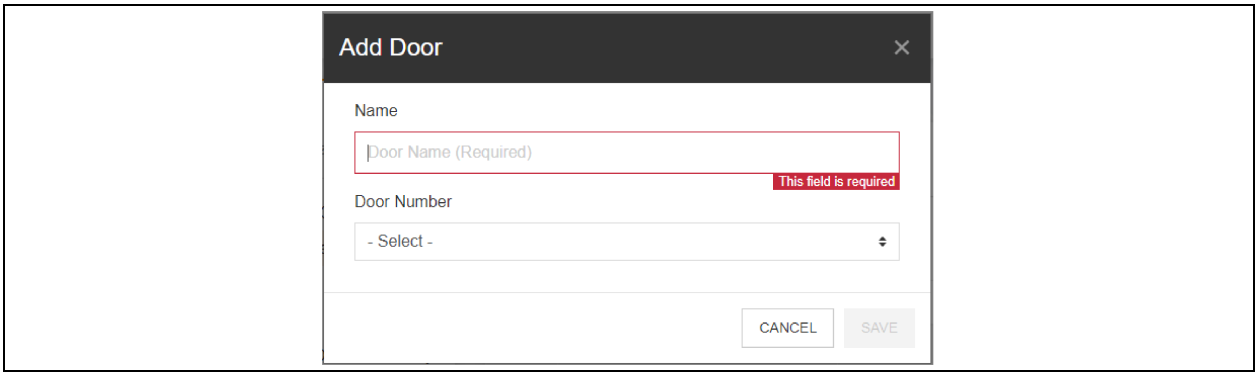
1. This function is available to administrator group users only.

2. The primary use case for the Sync Data function is to replace an IP access control controller and sync the existing data from the platform to the new access control device.

Adding a Door

1. Click 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 11.6 below .

Figure 11.6 Adding a Door



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

NOTE:

1. This function is available to administrator group users only.

© 2026 Vertiv Group Corp. All Rights Reserved.

2. The door name must be 3–64 characters long, and duplicate door names are not allowed within the same site.

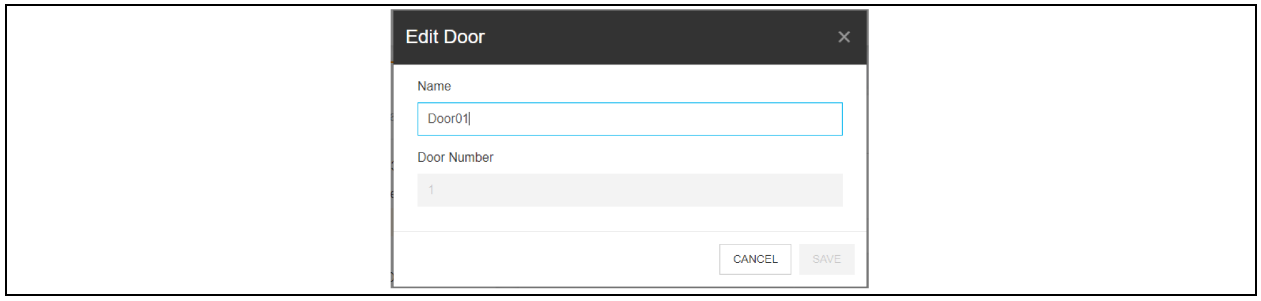
3. Within the same IP access control controller, each door number can only be used once. Door numbers that are already in use cannot be selected.

4. Both the door name and door number are required fields. The Save button is only enabled after all information has been entered and validated successfully.

Editing a Door

Click on the ellipses (⋮) on the right side 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 11.7 below .

Figure 11.7 Editing a Door



NOTE:

1. This function is available to administrator group users only.

2. The door name must be 3–64 characters long, and duplicate door names are not allowed under the same access control controller.

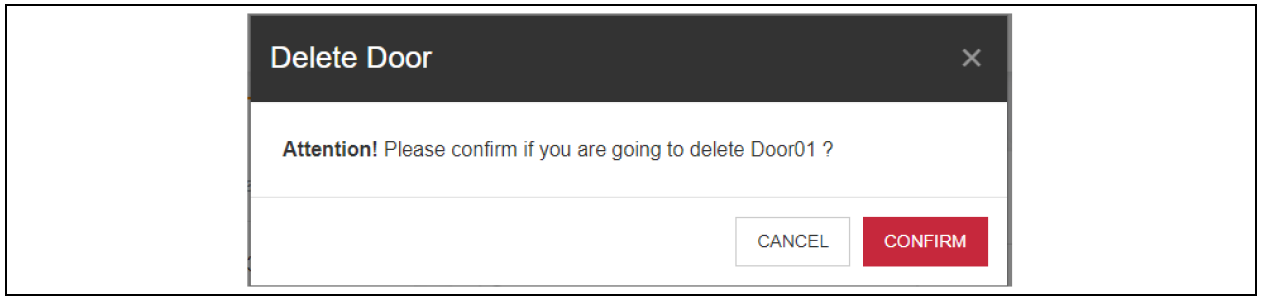
3. The door number cannot be edited. To change the door number, delete the door and add it again.

4. In the Edit dialog box, the Save button is only enabled after changes have been made.

Deleting the Door

1. Click 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 11.8 below .

Figure 11.8 Deleting the Door Popup



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

© 2026 Vertiv Group Corp. All Rights Reserved.

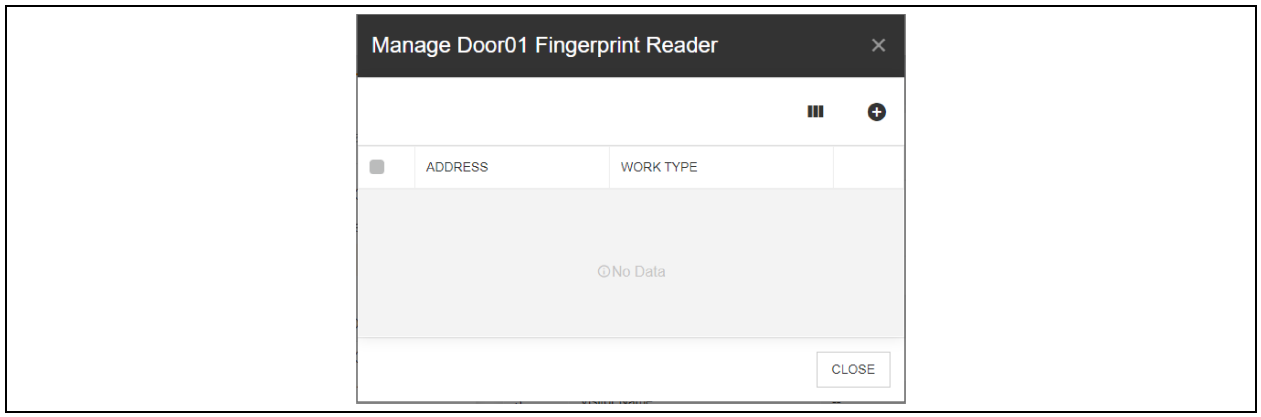
NOTE: This function is available to administrator group users only.

Managing Fingerprint Readers

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

1. Click on the ellipses (⋮) next to each door name in the IP access controller. and Select **Manage Fingerprint Reader** from the drop-down menu. The fingerprint reader management interface Readers dialog box appears, as shown in **Figure 11.9** below .
2. Click the *Add* button in the upper-right corner of the dialog box to add a new row in the fingerprint card reader table. After selecting the working mode of the fingerprint card reader, a green indicator appears to the right of the working mode, indicating that the fingerprint card reader has been added successfully. An address will be automatically assigned to it.
3. For fingerprint card readers that have already been configured, the working mode can be modified, but the address cannot be changed.
4. Click the ellipses (⋮) button next to a fingerprint card reader record, and select *Delete* from the drop-down list to remove the configured fingerprint card reader. Multiple configured fingerprint card reader records can also be selected for batch deletion.
5. Once all fingerprint card reader management operations are complete in the dialog box, click the *Close* button to exit.

Figure 11.9 Managing Fingerprint Readers



NOTE:

1. This function is available to administrator group users only.

2. The baud rate of the access controller and the fingerprint card reader must be consistent for them to communicate with each other. If the access control controller and the fingerprint card reader cannot communicate, a service technician must use the manufacturer's debugging tool to configure the baud rate. After confirming that communication is functioning normally, the fingerprint card reader can be added or modified.

3. Each door under an IP access controller allows a maximum of 2 fingerprint card readers.

4. 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

5. If a fingerprint card reader that is currently in use needs to be moved to another door, delete the fingerprint card reader on the Manage Fingerprint Card Readers page first, then physically relocate the fingerprint card reader hardware, and re-add and authorize the fingerprint card reader on the page.

Access Control Device Authorization

1. Click on the ellipses (⋮) to the right of an IP access controller door name, or click the ellipses (⋮) button to the right of a serial access control device name, and select Permission from the drop-down list. The dialog box shown in **Figure 11.10** below . The dialog box displays all access cards currently in the system along with the door access permissions for each card. The card ID, cardholder, and department are the basic information of each access card. The Permission Group column displays the door access permission of each access card for the selected door (including No Permission, Privilege, Group 1, Group 2, Group 3, and Group 4). The Door Method column displays the door method of each access card for the selected door (--, Card /Fingerprint 1/Fingerprint 2, Card /Card + PIN).

Figure 11.10 Permission

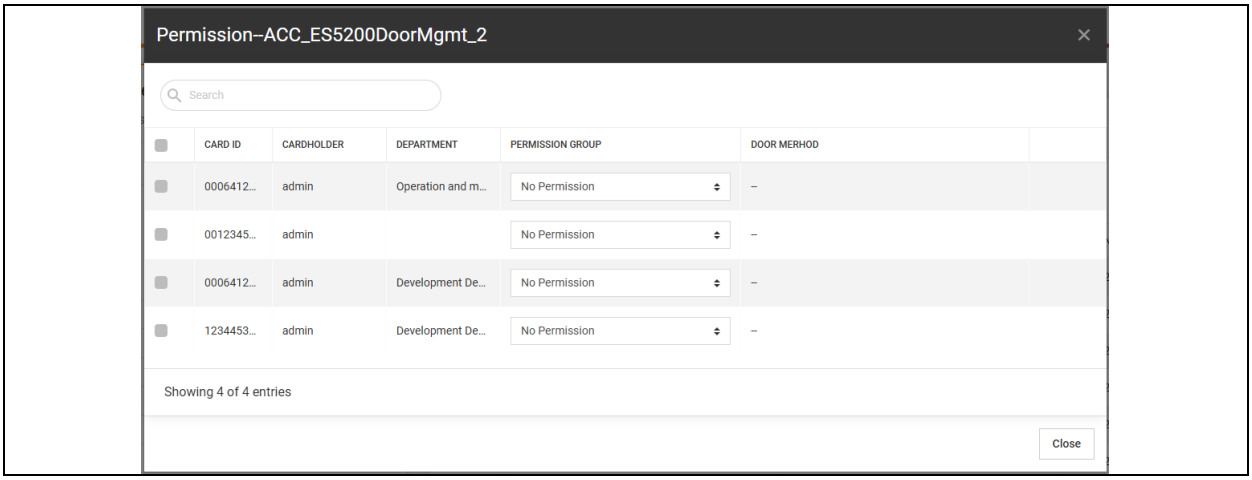
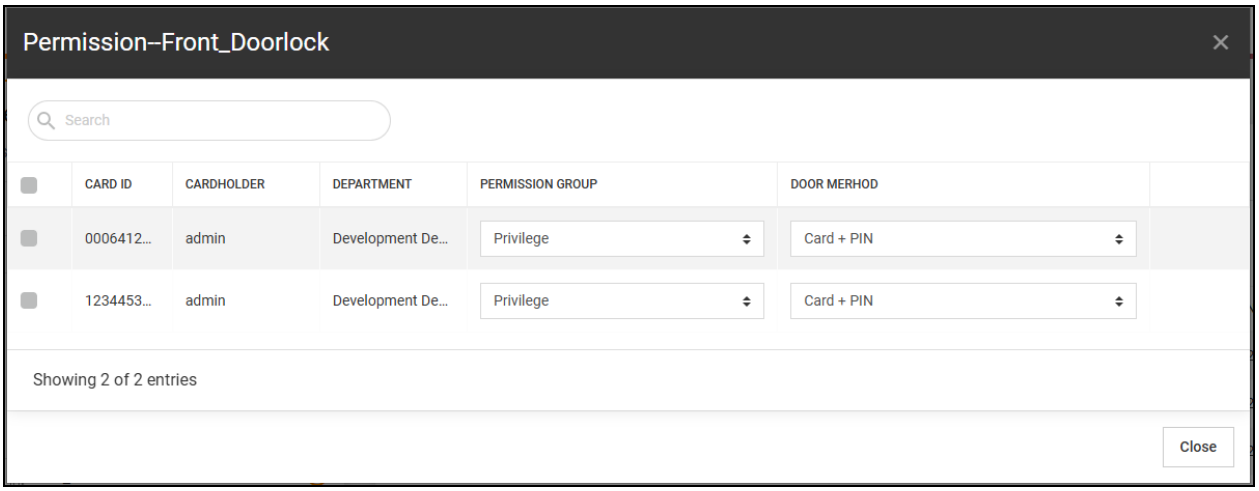


Figure 11.11 SCID Permission



© 2026 Vertiv Group Corp. All Rights Reserved.

NOTE:

1. The VRA7002 lock supports authorization by Card, Fingerprint 1, and Fingerprint 2, and the three methods can exist independently.

2. After clearing the authorization of a VRA7002 lock, all data (user/card/fingerprint 1/fingerprint 2) stored in the device will be deleted. If fingerprint unlocking is required, the fingerprints must be re-enrolled and re-authorized.

3. The VRA7003 lock supports authorization by Card or Card + PIN, and only one method can exist at a time.

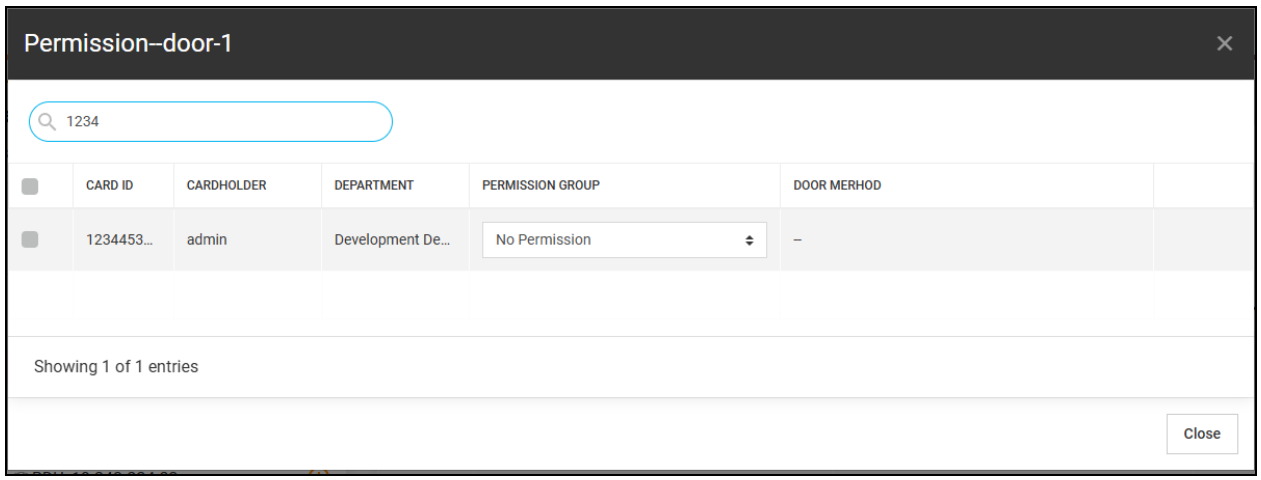
4. The VRA7003 lock supports a 4–6 digit PIN (i.e., password; however, due to SI limitations, only 4 digits are allowed). Each digit of the PIN must be within the range of 1–4 (digits outside this range cannot be used to open the door due to hardware limitations, as there are no corresponding buttons).

5. This function is available to administrator group users only.

6. For functions related to access card management, refer to Section Access Card Management on page 200.

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 11.12 below .

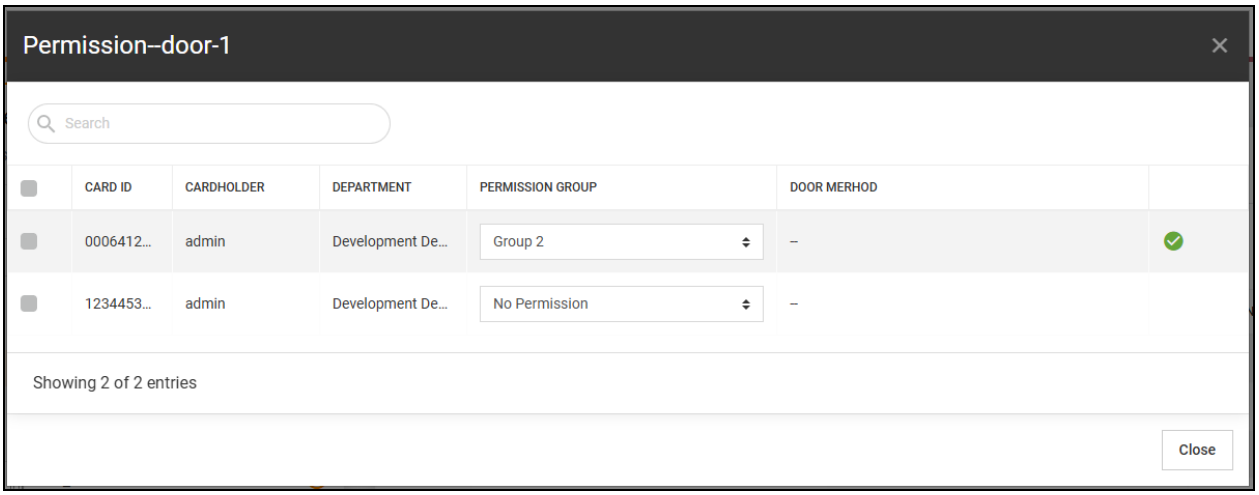
Figure 11.12 Searching the Access Card



3. After selecting an option from the PERMISSION GROUP dropdown, 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. Door Authorization—Group Modification shows an example of the page after successful authorization for Group 1.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.13 Door Authorization—Changing the Permission Group of the Access Card



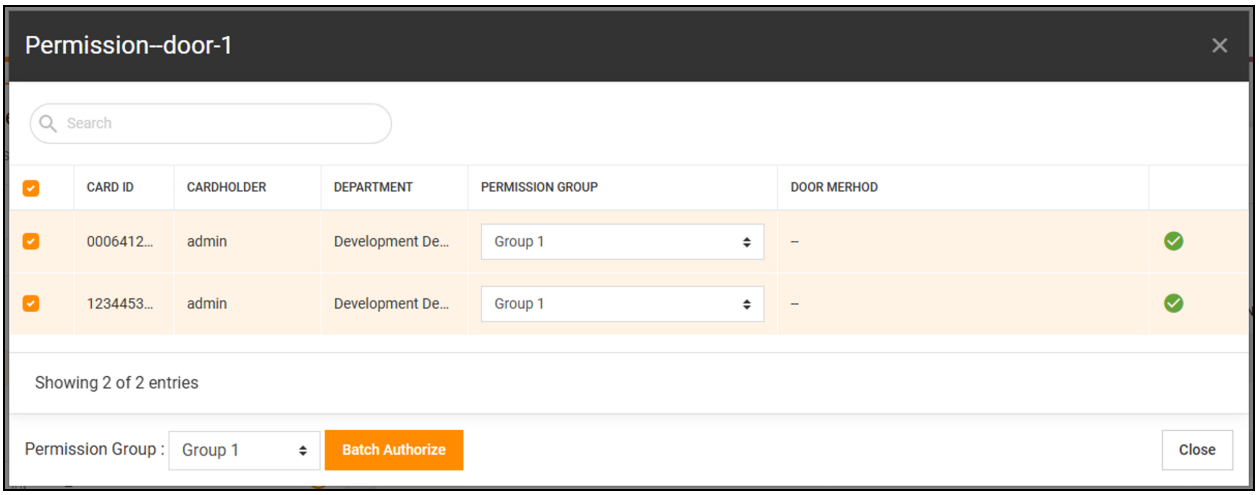
NOTE:

1. When the 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.

2. For functions related to time period settings, refer to Section Time Settings on page 208.

4. Click 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 1 and click *Batch Authorize* Button. Upon successful batch authorization, the page will appear as shown in Figure 11.14 below .

Figure 11.14 Door Authorization—Group Modification



© 2026 Vertiv Group Corp. All Rights Reserved.

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.

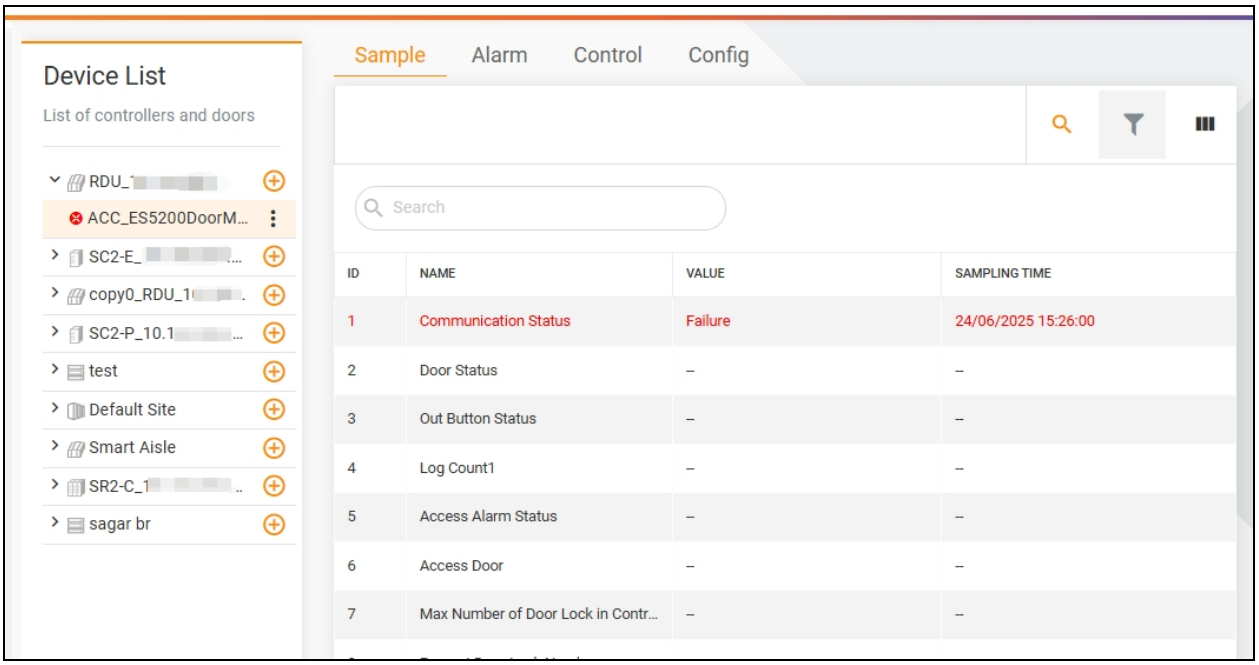
2. For serial access control, when modifying permissions in batches, a maximum of 4 access cards can be authorized at a time.

3. For SCID, when modifying permissions in batches, a maximum of 4 access cards can be authorized at a time. When more than 4 access cards are selected, the Batch Authorization button will be disabled. When the batch permission is set to Privileged User, the door opening method of the selected access cards will be set to Card.

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 11.15** below .

Figure 11.15 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 6 seconds.

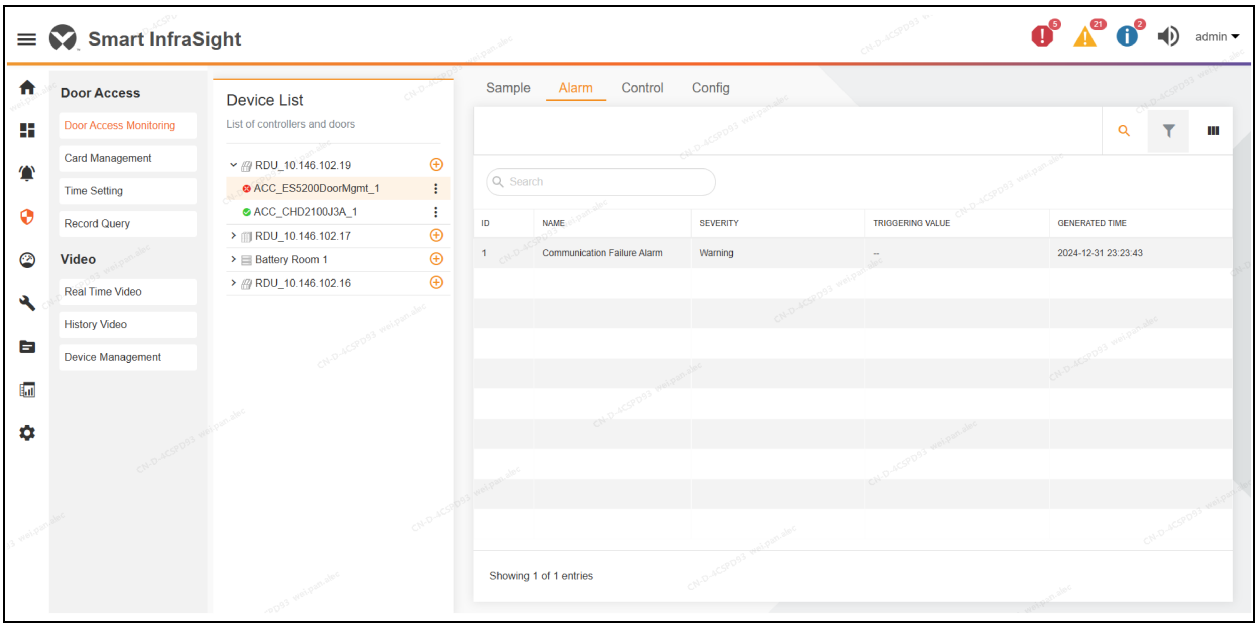
2. When the real-time signal is unavailable, both the value and acquisition time are displayed as (--).

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 11.16** on the next page . When a new alarm appears, the alarm list is automatically refreshed.

© 2026 Vertiv Group Corp. All Rights Reserved.

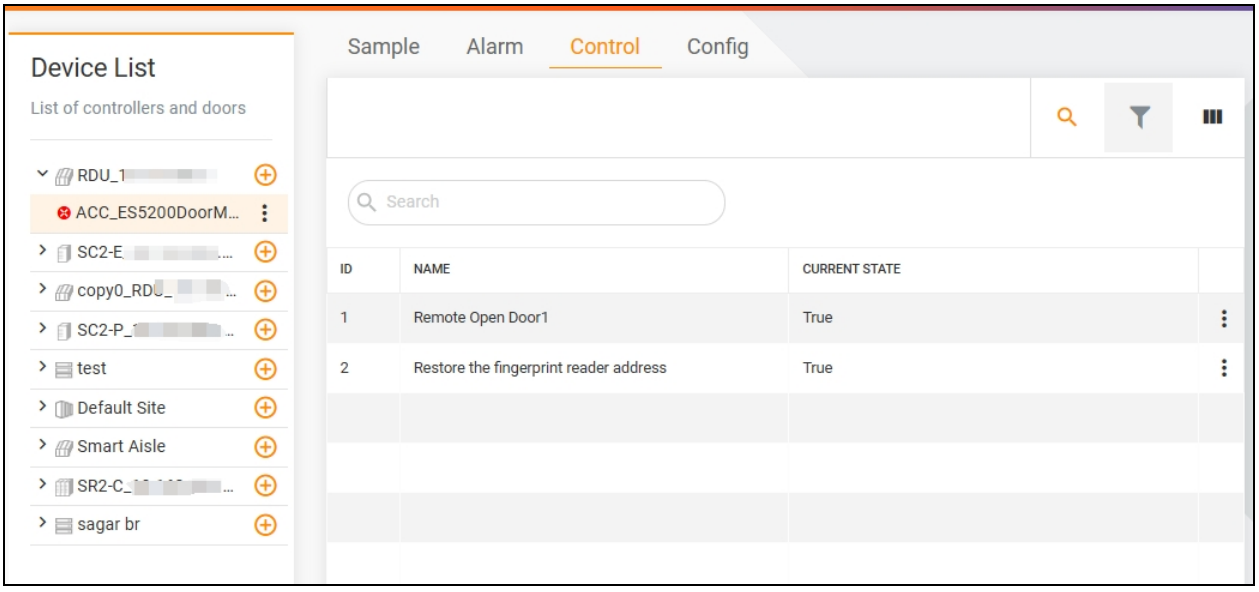
Figure 11.16 Current Alarms



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 11.17** below .

Figure 11.17 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 6 seconds.

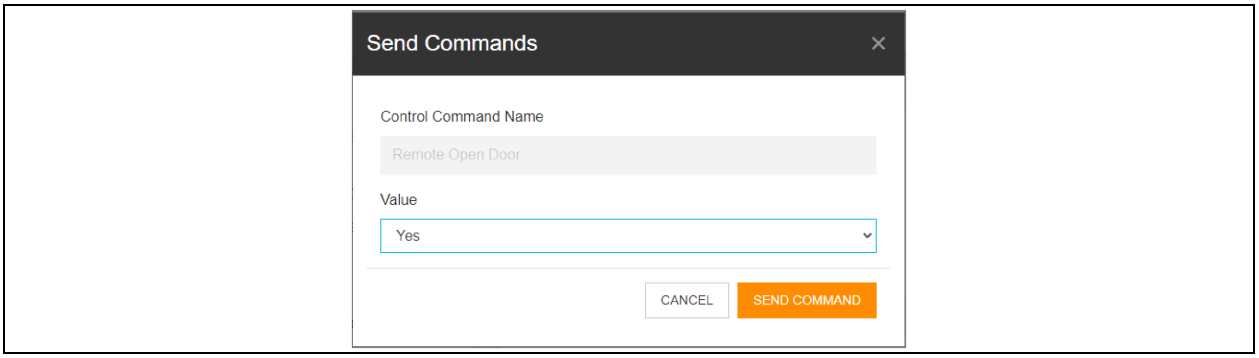
© 2026 Vertiv Group Corp. All Rights Reserved.

3. The control command Delete All Users is available to administrator group users only. This command will not be displayed when a regular user logs in.

2. Click the ellipses (⋮) next to the control command and select **Send Commands** from the drop-down menu. The Send Commands popup will appear, as shown in **Figure 11.18** below . Choose the desired control command from the drop-down list and click *Send Command*. This will transmit the command to the device.

When a control command is sent successfully, the dialog box closes and an **Operation Success** message appears in the lower-right corner of the screen. When a control command fails to be sent, an **Operation Failed** message appears in the lower-right corner of the screen.

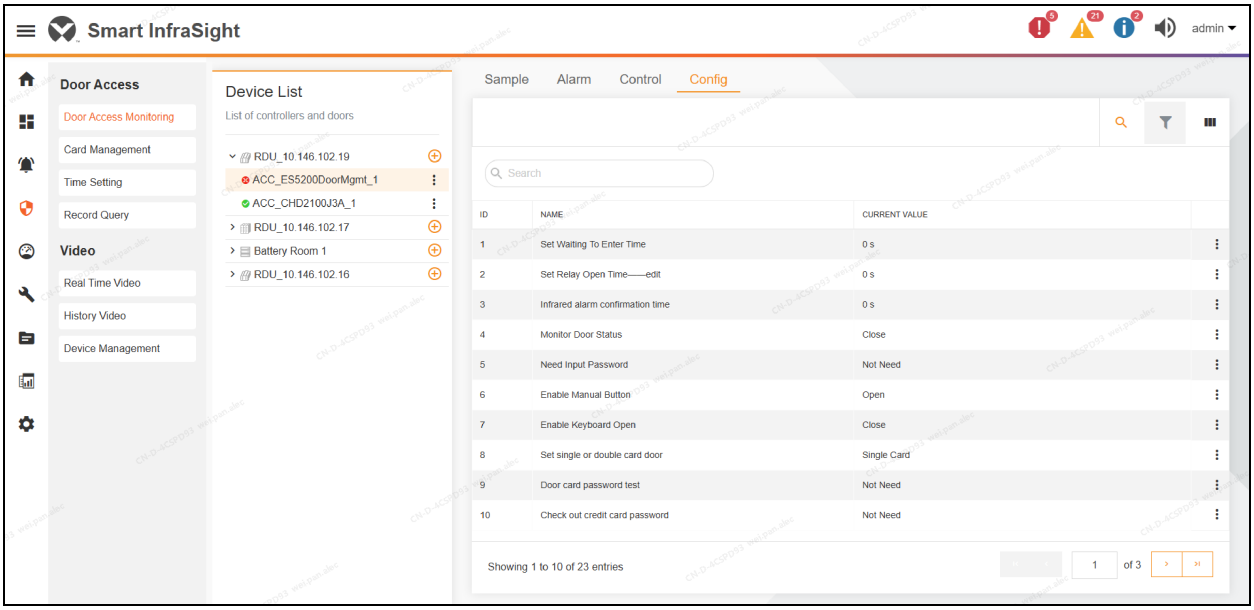
Figure 11.18 Sending Commands



Config Signal

1. On the *Access Monitoring* page, as shown in **Figure 11.19** 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 11.19 Config Signal - Access controller



2. Enter the search content in the search box above the setting signal list. The system will perform a fuzzy search on the names of the setting signals based on the entered content.

© 2026 Vertiv Group Corp. All Rights Reserved.

NOTE:

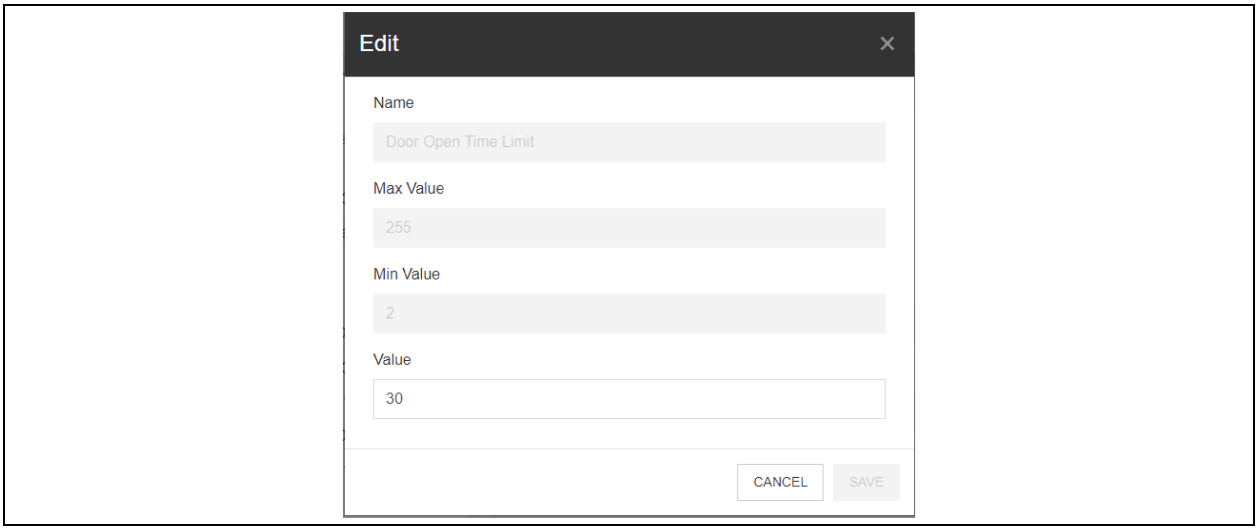
1. This function is available to administrator group users only. The Settings tab will not be displayed when a regular user logs in.

2. When no setting signals are found, No Data is displayed in the list. When the value of a setting signal cannot be retrieved, -- is displayed.

3. The setting signal data is refreshed periodically, with a refresh interval of 6 seconds.

3. Click the ellipses (⋮) on the right of the controller setting signal, and select *Edit* button from the drop-down list. The Edit Controller Setting Signal dialog box appears. Enter or select the value to be modified in the value input field or drop-down list, then click the *Save* button as shown in Figure 11.20 below . If the controller setting signal is edited successfully, the dialog box closes and an Operation Successful message appears in the lower-right corner of the screen. If the controller setting signal fails to be edited, a Setting Failed message appears in the lower-right corner of the screen.

Figure 11.20 Editing the Setting Signal



11.2.2 Access Card Management

This module introduces the management functions for access cards, including adding, deleting, editing, and querying access cards, as well as configuring door unlock permissions based on access card dimensions.

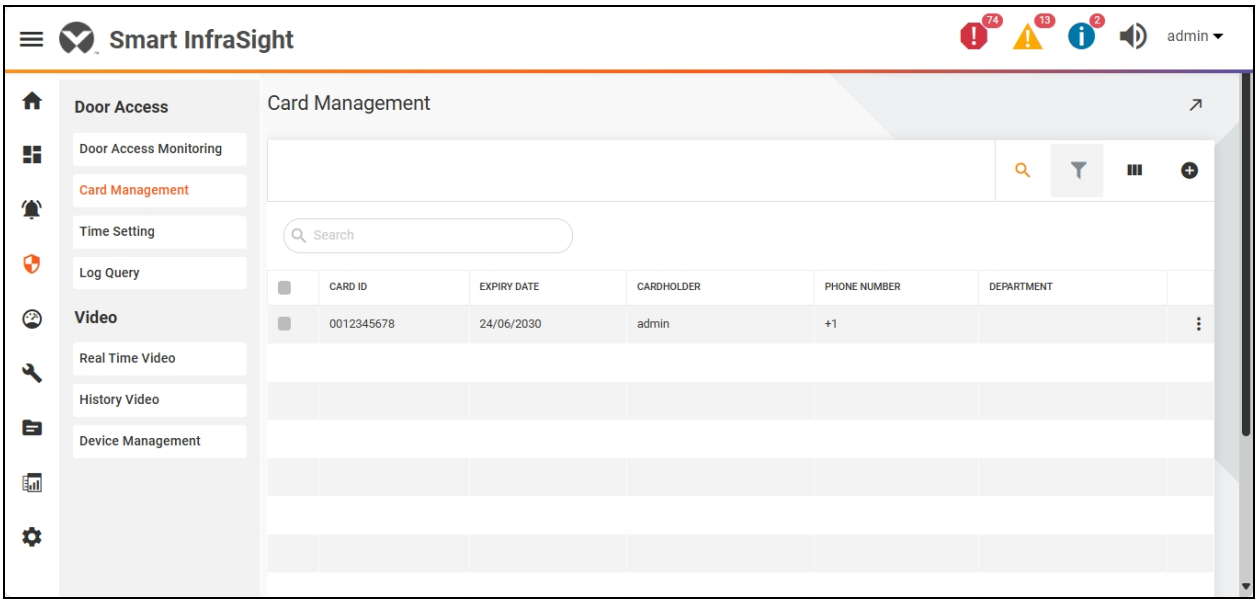
Permission: This feature is available only to administrator users.

Access Card List

1. Select Security from the first-level menu, then select Access Card Management from the second-level menu. After entering the Access Card Management page, the system displays all access card information in list format, with 10 records displayed per page by default. The list contains the following fields: Card Number, Validity Period, Cardholder, Phone Number, and Department. As shown in Figure 11.21 on the facing page .

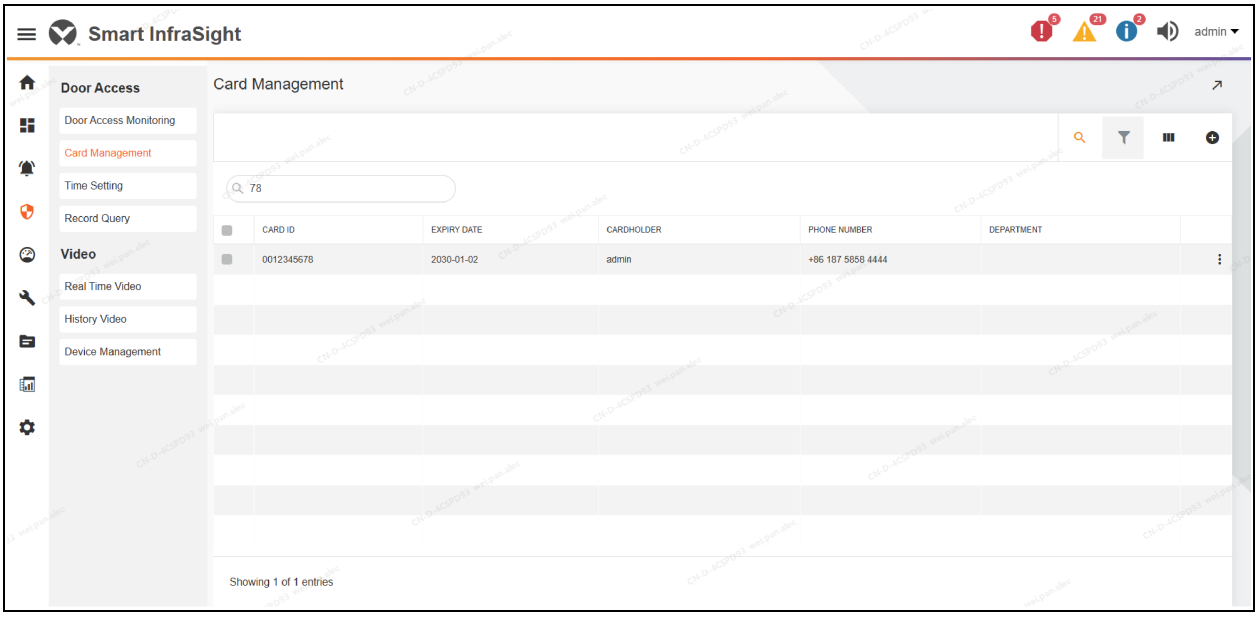
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.21 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 78 and search results are shown in Figure 11.22 below .

Figure 11.22 Access Card List - Search

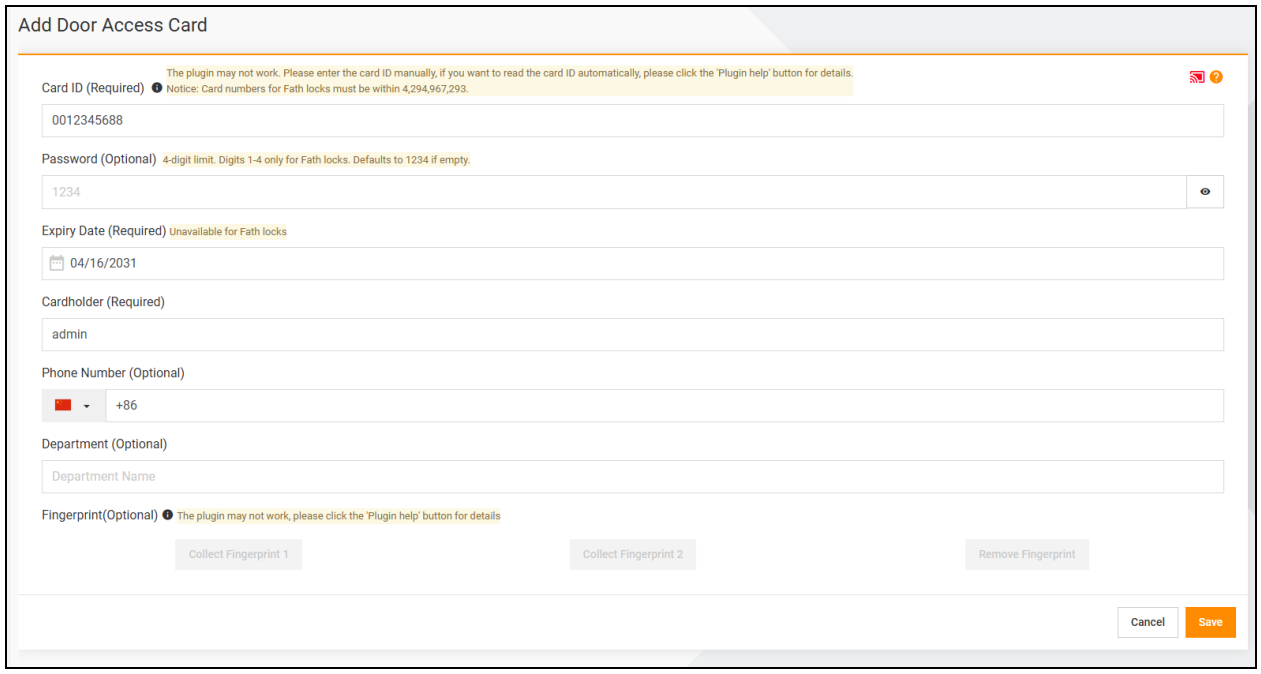


Adding an Access Card

1. Click the *Add Access Card* button in the upper-right corner to navigate to the Add Access Card page, as shown in Figure 11.23 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.23 Adding Access Cards



2. Enter the following information as required:
   - Card Number (Required)
   - Password (Optional)
   - Cardholder (Required): Select from the contact list
   - Phone Number (Optional)
   - Department (Optional)
   - Validity Period (Required): Set the valid time range for the access card
   - Fingerprint Information (Optional): You can collect Fingerprint 1, Fingerprint 2, or both.
3. To collect fingerprint information, connect the fingerprint scanner to your computer, install the fingerprint scanner driver and the Card Reader and Fingerprint Scanner Plugin, then collect Fingerprint 1 and Fingerprint 2 in sequence. You can also collect only one fingerprint. For details, refer to Plugin Help in the upper-right corner of the page. Collected fingerprint information can be deleted using the Clear Fingerprint button.
4. Click *Save* to complete the operation.

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. The cardholder must be selected from the user names in the contact list.

3. When entering a phone number, China is selected by default. To select another country, click to switch to the corresponding country.

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

5. If collecting fingerprints for an access card, at least one fingerprint must be collected. Either Fingerprint 1 or Fingerprint 2 can be used.

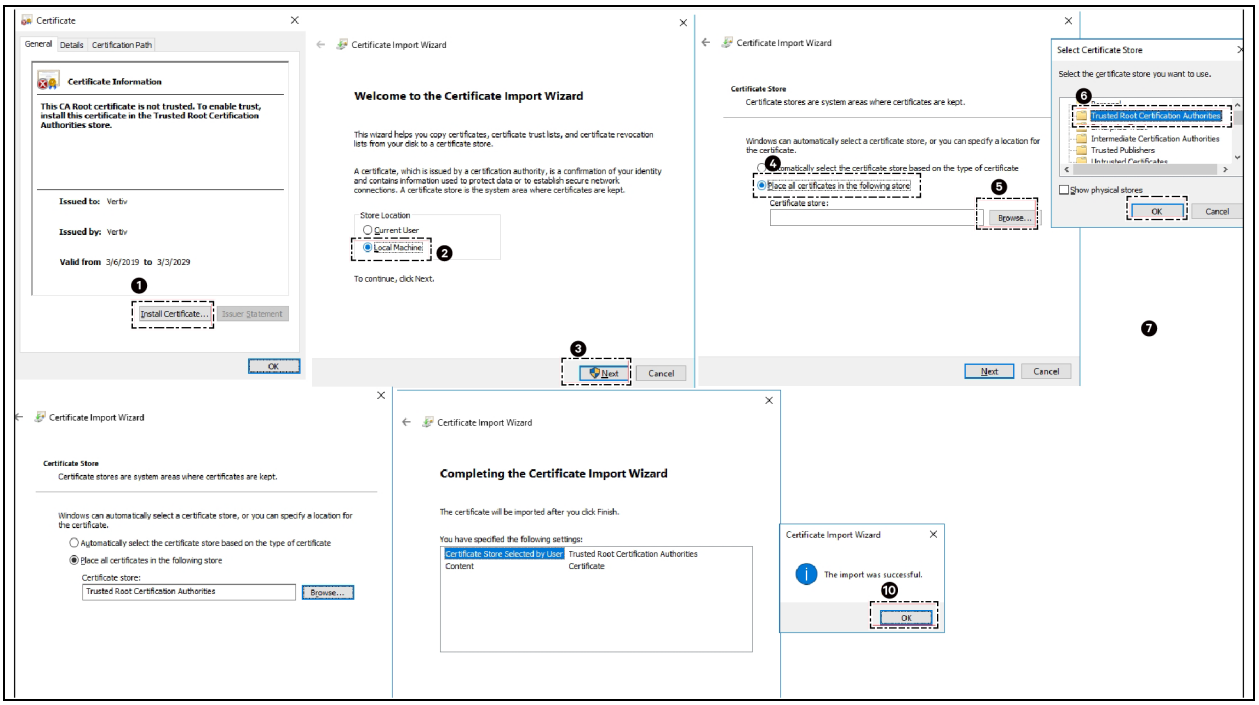
© 2026 Vertiv Group Corp. All Rights Reserved.

6. Card Number and Cardholder are required fields. The Save button can only be clicked after all required information is entered and validated.

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 as shown in **Figure 11.24** below .

Figure 11.24 Importing the Certificate



NOTE:

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

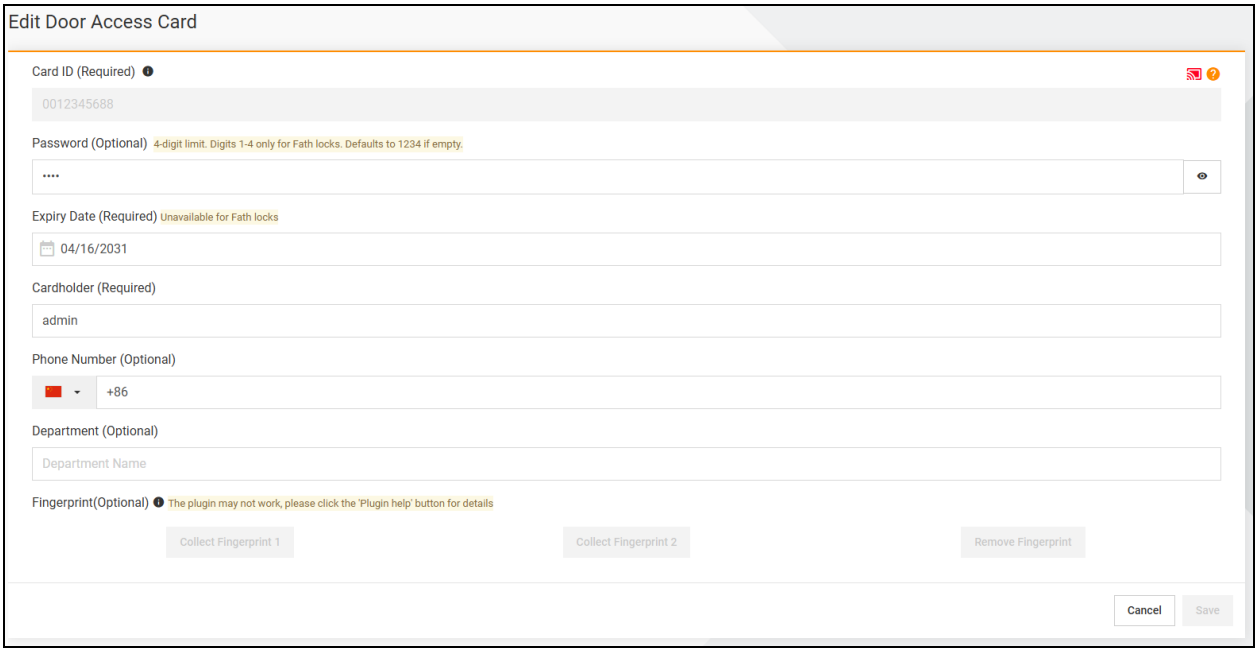
2. It can connect 1 card reader and 1 fingerprint machine to the computer at the same time.

© 2026 Vertiv Group Corp. All Rights Reserved.

Editing the Access Card

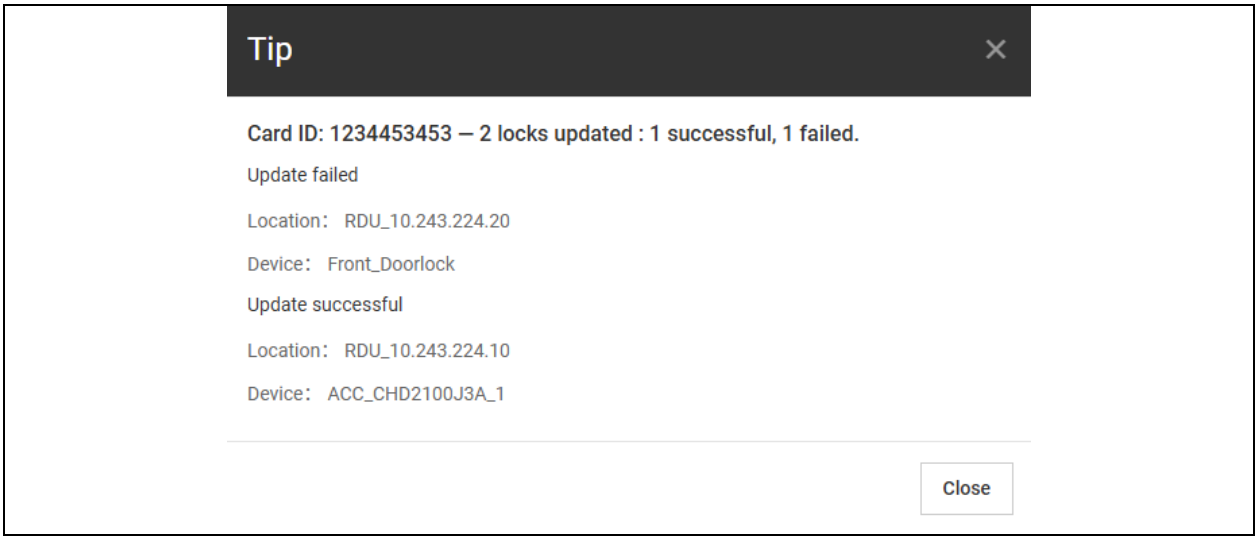
1. Click on the *ellipses* on the right side of the access card, and select *Edit* in the pop-up drop-down menu as shown in Figure 11.25 below . After changing the password, expiration date, cardholder, phone number or department information of the access control card, click *Save*.

Figure 11.25 Editing the Access Card



2. After modifying the access card password, if offline devices exist among the associated access control controllers, the system displays a prompt window listing the access control controllers with successful and failed password updates, including their locations and device names. The interface is shown in Figure 11.26 below .

Figure 11.26 Modify Access Card Password Prompt



© 2026 Vertiv Group Corp. All Rights Reserved.

NOTE:

1. The card number cannot be modified. To change the card number, delete the card and add a new one.

2. Collected Fingerprint 1 and Fingerprint 2 can be deleted using the Clear Fingerprint button.

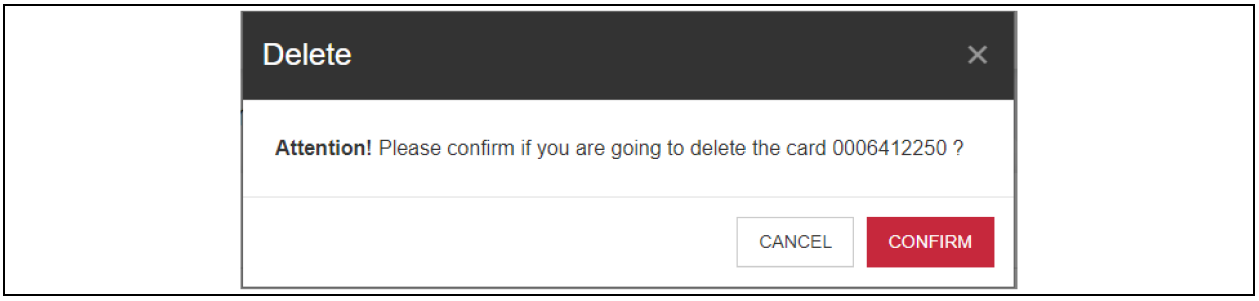
3.In the edit window, the Save button is only enabled after changes have been made.

4. If the card password is used for the VRA7003 and the door-opening method is Card + PIN, note that each digit of the new password must be within the range of 1–4. Otherwise, the operation may partially succeed and partially fail.

Deleting the Access Card

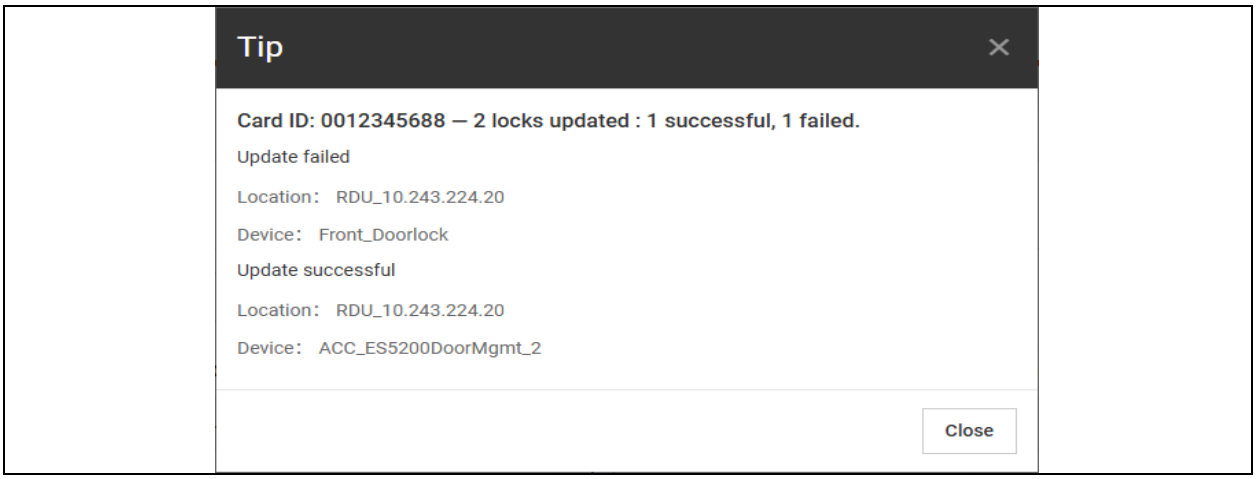
Click the ellipses (⋮) on the right side of the access card and select *Delete* in the pop-up drop-down menu to popup as shown in Figure 11.27 below . Click the *Confirm* to delete the access card.

Figure 11.27 Deleting the Access Card Prompt



The deletion result is displayed in a dialog box, listing the access control controllers with successful and failed updates, including their locations and device names. The prompt interface is shown in Door Authorization—Group Modification on page 208.

Figure 11.28 Deleting access card result prompt

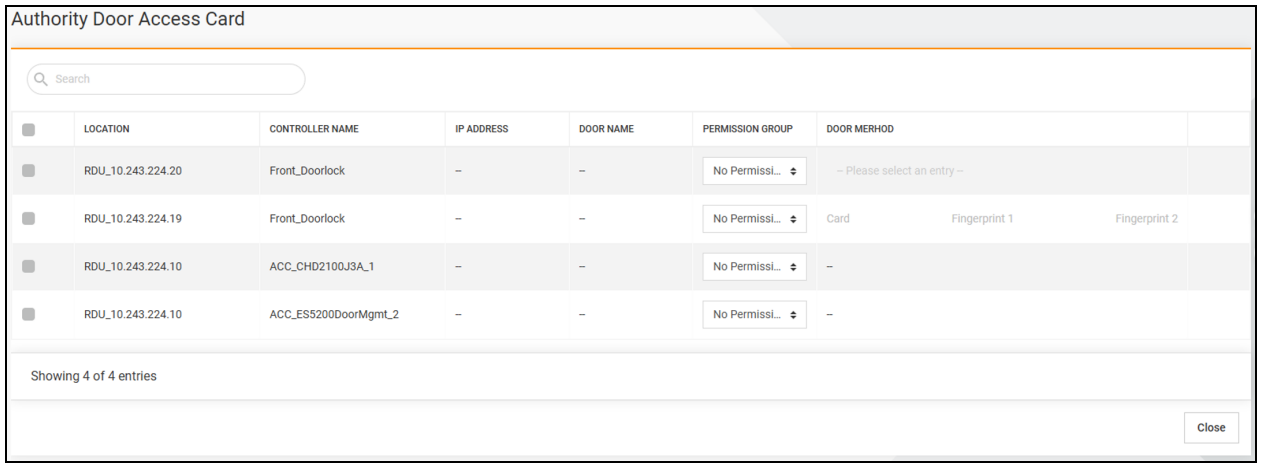


© 2026 Vertiv Group Corp. All Rights Reserved.

Access Card Authorization

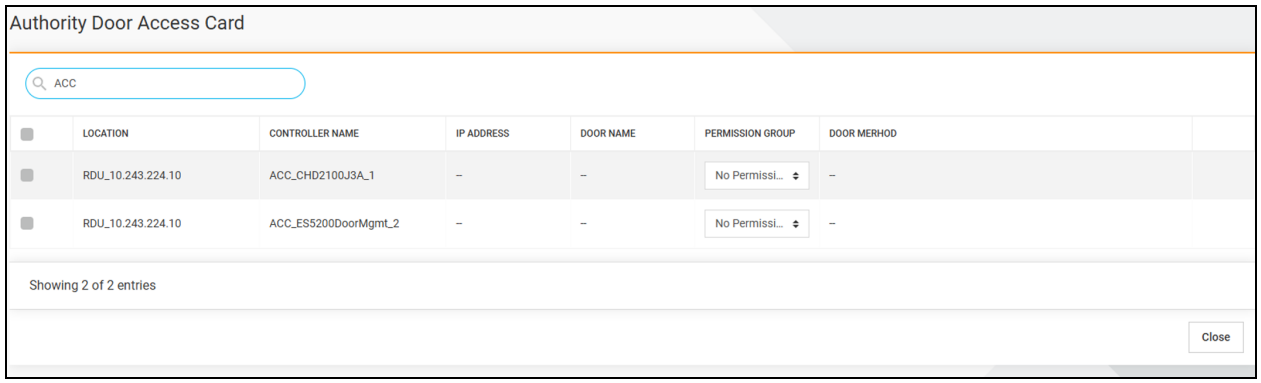
1. Click the ellipses (⋮) on the right side of an access card, then select Authorize from the drop-down menu. The interface is shown Figure 11.29 below . The page displays all access control devices and door unlock permissions in the current system. The Permission Group column shows the door unlock permissions for the access card (including No Permission, Privileged User, Permission Group 1, Permission Group 2, Permission Group 3, and Permission Group 4).The Door-Opening Method column displays the door-opening method configured for the access card on the selected door (--, Card Number / Fingerprint 1 / Fingerprint 2, Card Number / Card Number + PIN).

Figure 11.29 Access Card Authorization



2. Enter search criteria in the search box above the list. The system searches access control devices based on the entered content. This search function supports fuzzy matching for Access Control Controller Name and IP Address. Enter ACC and the search results are as shown in Figure 11.30 below .

Figure 11.30 Access Authorization - Change Permission Groups



NOTE:

1. The card number cannot be modified. To change the card number, delete the card and add a new one.

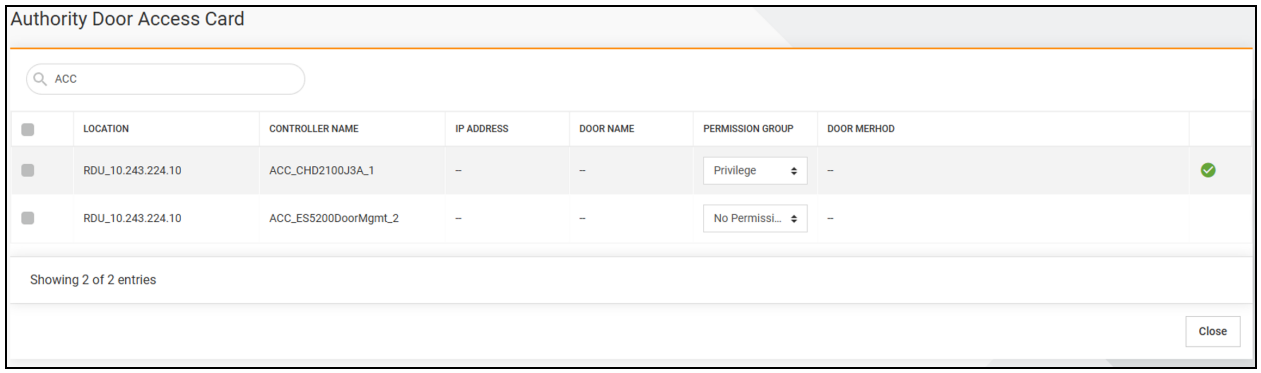
2. Collected Fingerprint 1 and Fingerprint 2 can be deleted using the Clear Fingerprint button.

3. In the edit window, the Save button is only enabled after changes have been made.

© 2026 Vertiv Group Corp. All Rights Reserved.

3. After selecting permission from the Permission Group drop-down list, a rotating icon appears in the last column, indicating that authorization is in progress. A green icon appears when authorization succeeds. A red icon appears when authorization fails, and the permission group reverts to the previous option. Select Privileged User from the permission group. When authorization succeeds, Figure 11.31 below .

Figure 11.31 Door Authorization—Group Modification



NOTE:

1. The VRA7002 lock supports authorization via Card Number, Fingerprint 1, and Fingerprint 2. These three methods can exist independently.

2 .Clearing authorization on the VRA7002 deletes all data stored on the device (users, card numbers, Fingerprint 1, and Fingerprint 2). To use fingerprint unlocking again, re-enroll and re-authorize the fingerprints.

3. The VRA7003 lock supports authorization via Card Number or Card Number + PIN. Only one method can be active at a time.

4. The VRA7003 lock supports a 4–6 digit PIN (password); however, due to SI limitations, only 4-digit PINs are allowed. Each digit of the PIN must be within the range of 1–4. Values outside this range will prevent the door from opening due to hardware button constraints.

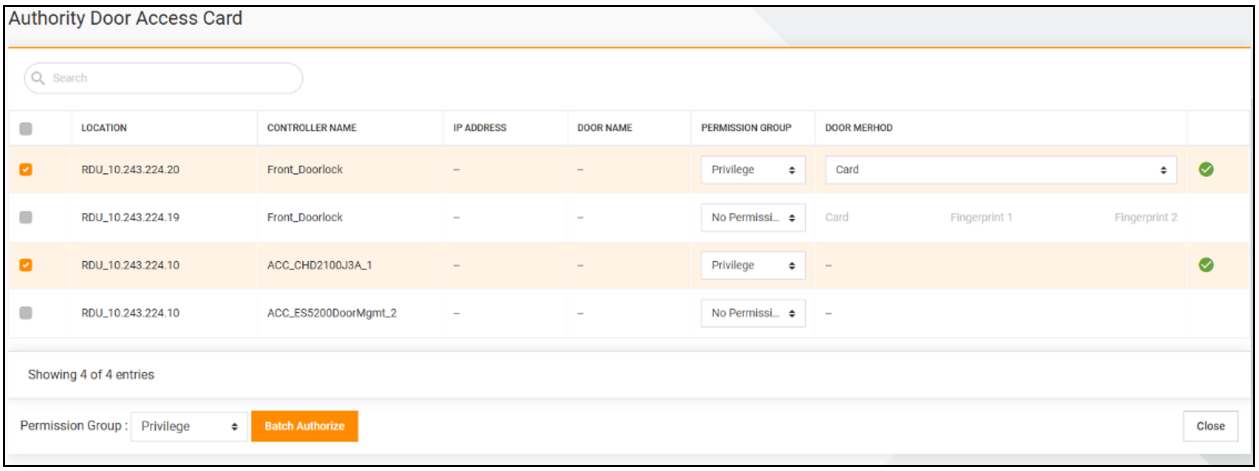
5. When No Permission is selected, the access card has no door unlock permission. When Privileged User is selected, the access card can unlock doors at any time. When Permission Group 1 through Permission Group 4 is selected, the access card can only unlock doors during the corresponding time periods.

6. For information about setting time periods, see 11.2.3 Time Period Settings.

4. Click the *check box* in the header of the first column to select all data. When two or more records are selected, a Batch Edit button appears in the lower-right corner of the interface. Select a permission group and click the *batch edit* button to modify permissions for the selected access control devices in bulk. The last column displays the authorization result. A green icon appears when authorization succeeds. A red icon appears when authorization fails, and the permission group reverts to the previous option. Select some access control controllers, choose Privileged User from the permission group, and click the *batch edit* button. When batch authorization succeeds, the result is as shown in Figure 11.32 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.32 Door Authorization—Group Modification



NOTE:

1 .For IP-based access control controllers: When batch editing permissions, a maximum of 100 access control devices are supported per operation. When more than 100 access control devices are selected, the batch edit button is disabled. A message prompts: 'Batch edit quantity cannot exceed 100'.

2. For serial-based access control controllers: When batch editing permissions, a maximum of 4 access cards are supported per operation. When more than 4 access cards are selected, the batch authorization button is disabled.

3. For SCID, batch permission modification supports a maximum of 4 access cards per operation. When more than 4 access cards are selected, the Batch Authorization button is disabled. When the batch permission is set to privileged user, the door-opening method for all selected access cards will be set to Card.

11.2.3 Time Settings

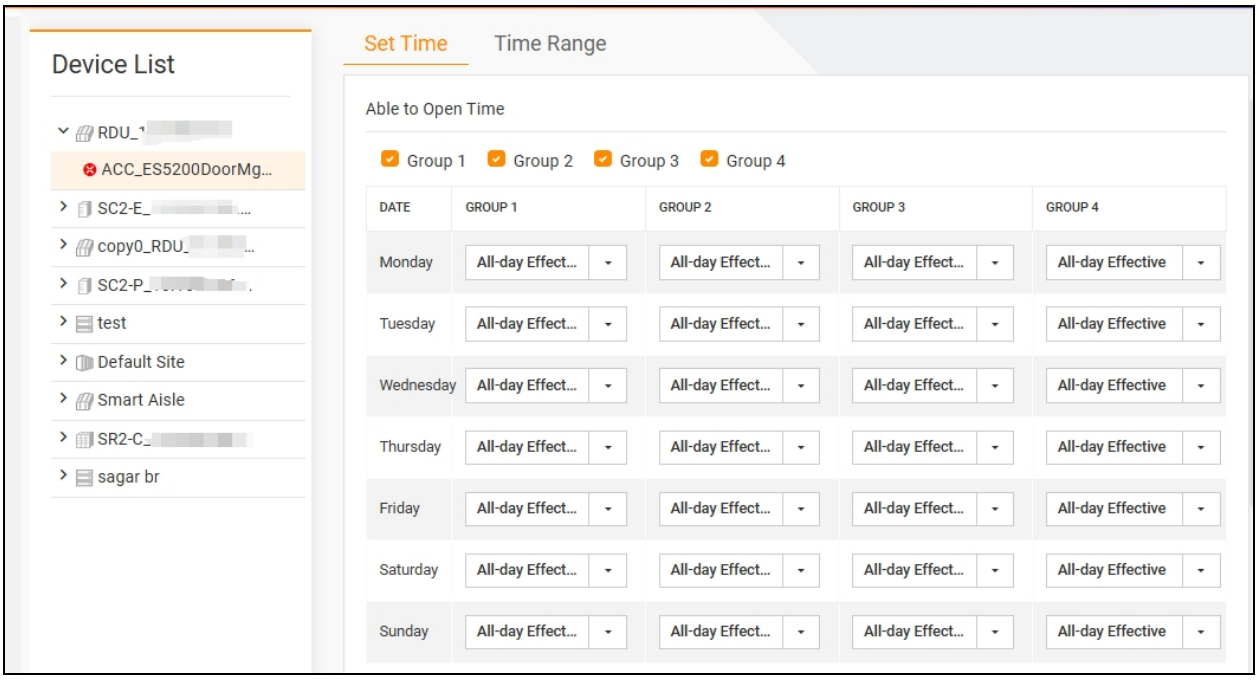
This module is used to configure time periods for access control controllers. When authorizing an access card, the bound permission group determines the time periods during which the card can be used to unlock doors.

Setting the Time Period

1. Navigate to Security, then click on *Time Setting*. The Set Time page appears, The Time Period Settings page opens. The left side displays the access control controller list, with the first access control controller selected by default. The right side displays the Configure Time Period tab by default. The icon in front of the access control controller name indicates its communication status. A green icon indicates normal communication, and a red icon indicates communication failure, as shown in **Figure 11.33** on the facing page . Hover over a time period name to view its specific time range.
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.

© 2026 Vertiv Group Corp. All Rights Reserved.

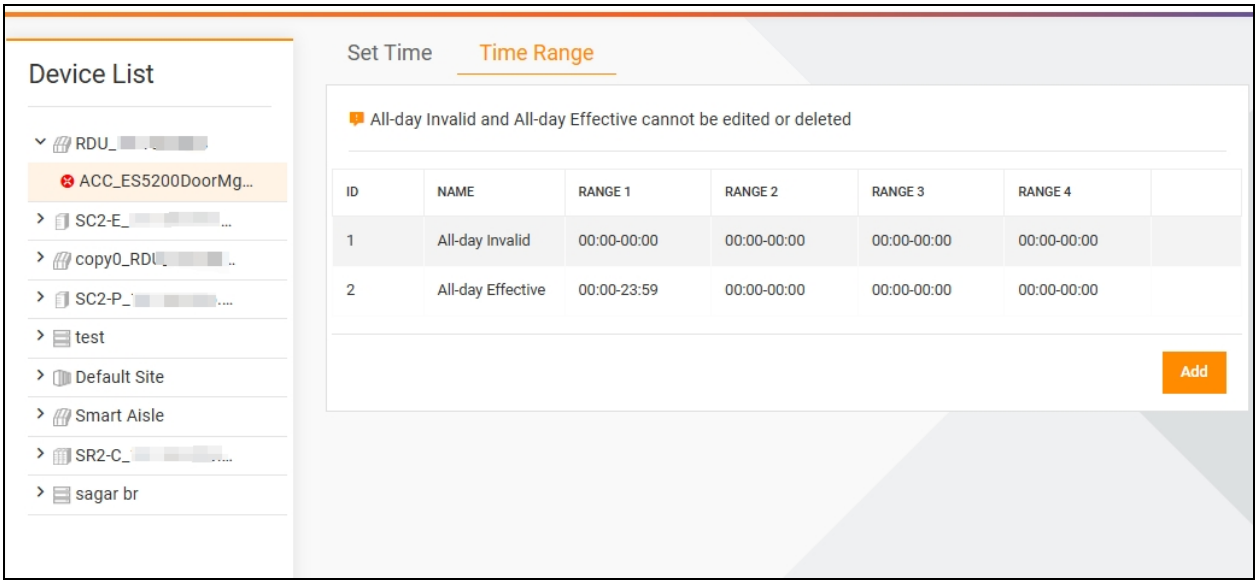
Figure 11.33 Hour List



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 door unlock time range for a permission group, simply select the appropriate time period for that permission group. For example, set the Monday door unlock permission for Permission Group 1 to All-Day Invalid. After completing the settings, click *Save*, as shown in Figure 11.34 below .

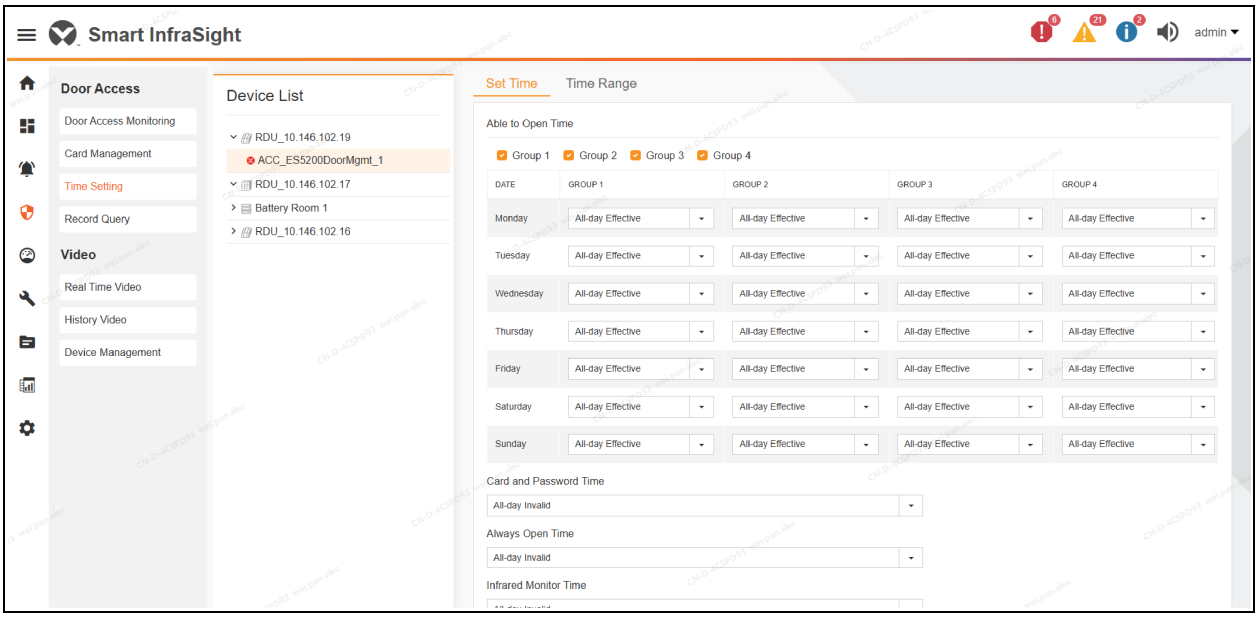
Figure 11.34 Modifying the Time Period



© 2026 Vertiv Group Corp. All Rights Reserved.

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 11.35 Modifying the Time Period



NOTE:

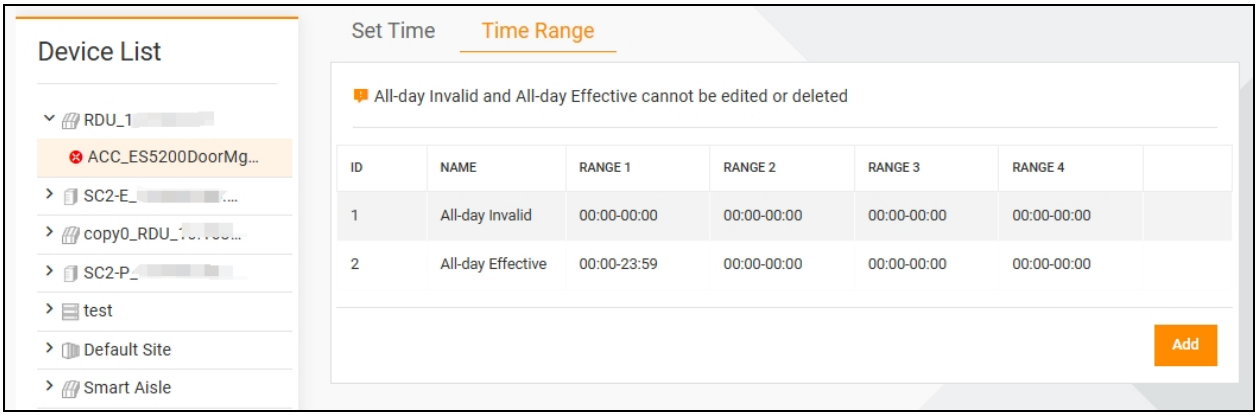
1. Select an access controller, when the Swipe the card with password column of the controller is Invalid all day, the check box of Swipe the card with password will be unchecked automatically.

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.

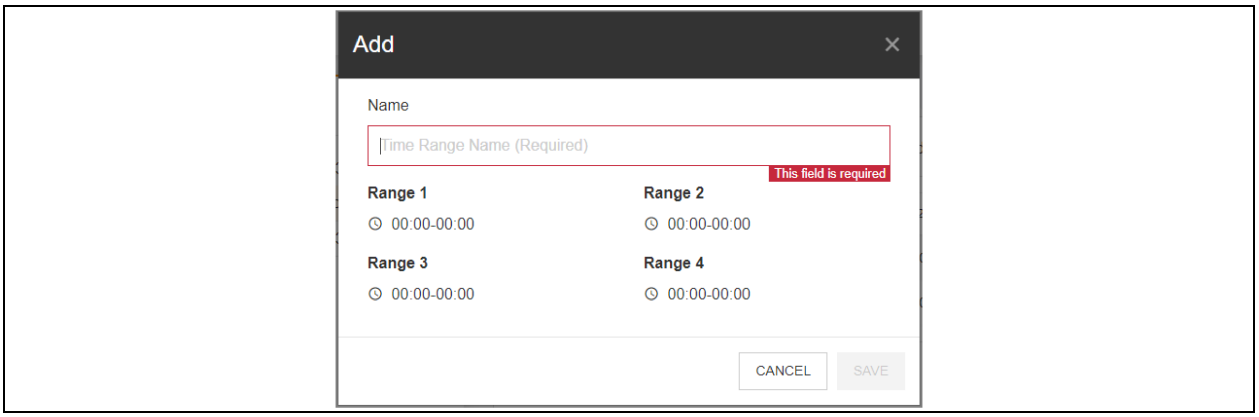
Figure 11.36 Default Time Range



© 2026 Vertiv Group Corp. All Rights Reserved.

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 11.37 below .

Figure 11.37 Adding/Selecting the Time



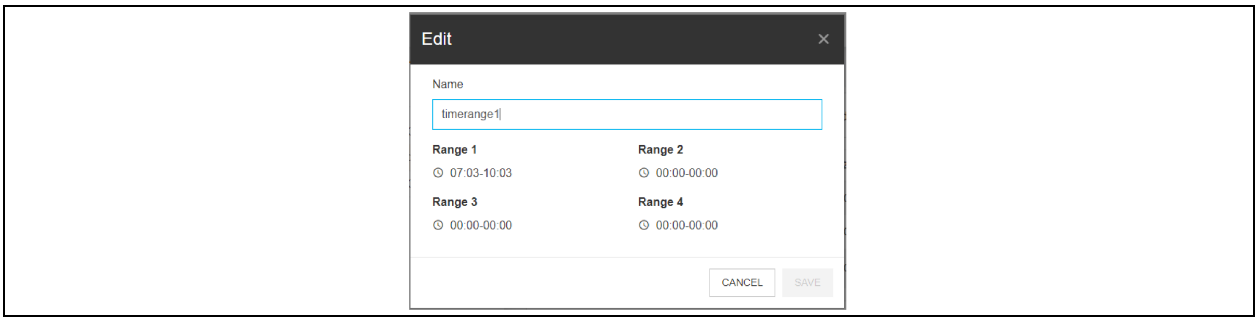
3. After adding a new time range, you can select it when setting permissions for a group.
4. Click the *Edit* button and you can modify the details of the time range, as shown in Figure 11.38 below .

NOTE:

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

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

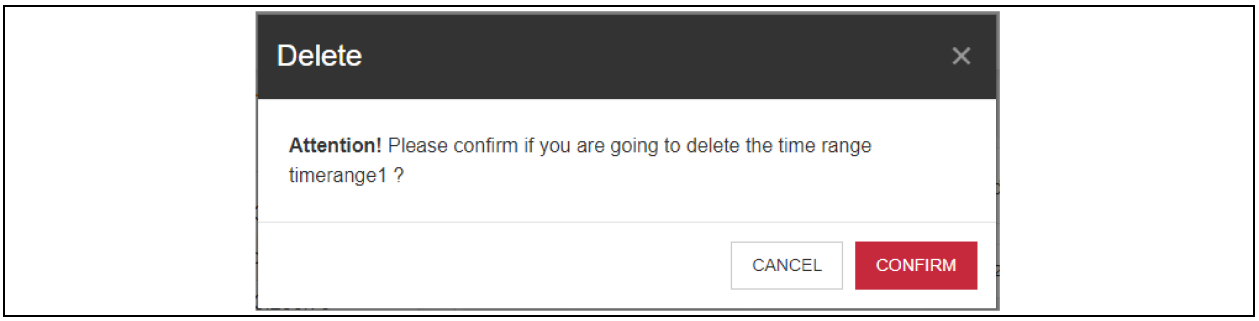
Figure 11.38 Editing the Time Range



5. When deleting the period data, click the *Delete* button on the right side of the period data as shown in Figure 11.39 on the next page . Click the *Confirm* button and the data will be deleted.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.39 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.

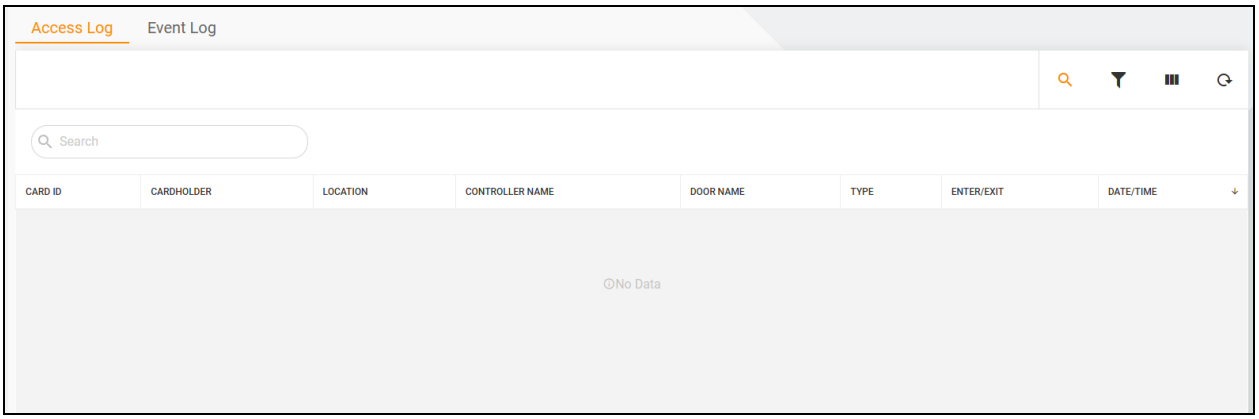
11.2.4 Log Query

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 swipe card log is sorted in reverse order of time, as shown in Figure 11.40 below .

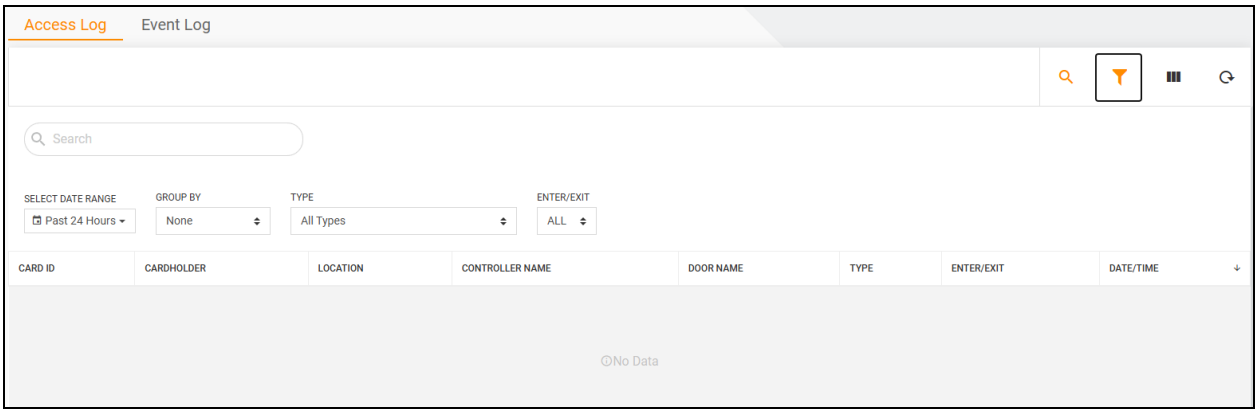
Figure 11.40 Access Log



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 11.41 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.41 Access Log - Filtering



Event Log

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 11.42** below .

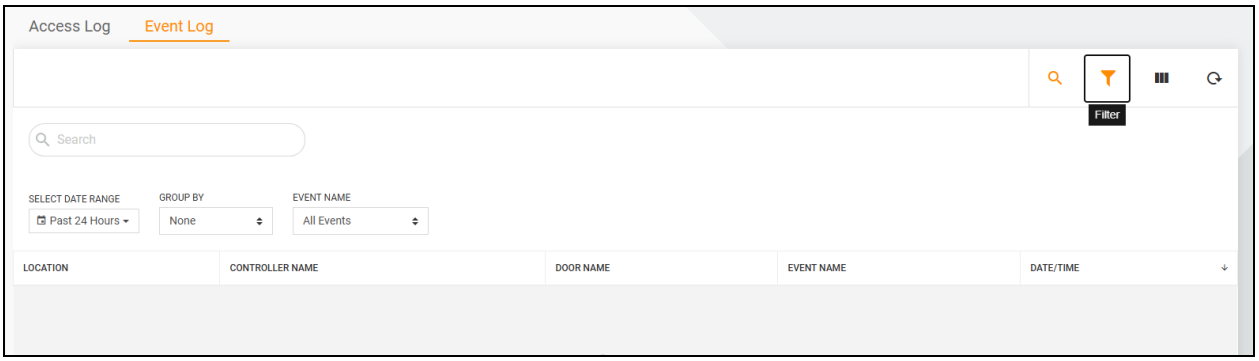
Figure 11.42 Event Log



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 11.43** below .

Figure 11.43 Filtering the Event Log



© 2026 Vertiv Group Corp. All Rights Reserved.

11.2.5 Real Time Video

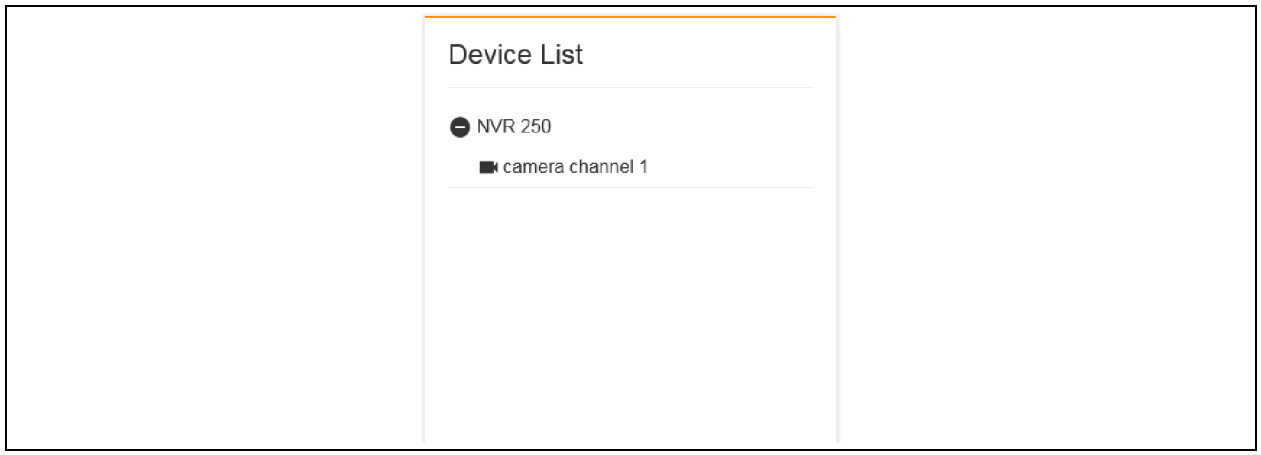
This module introduces the functions of previewing live video.

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 11.44** below .

Figure 11.44 Device List

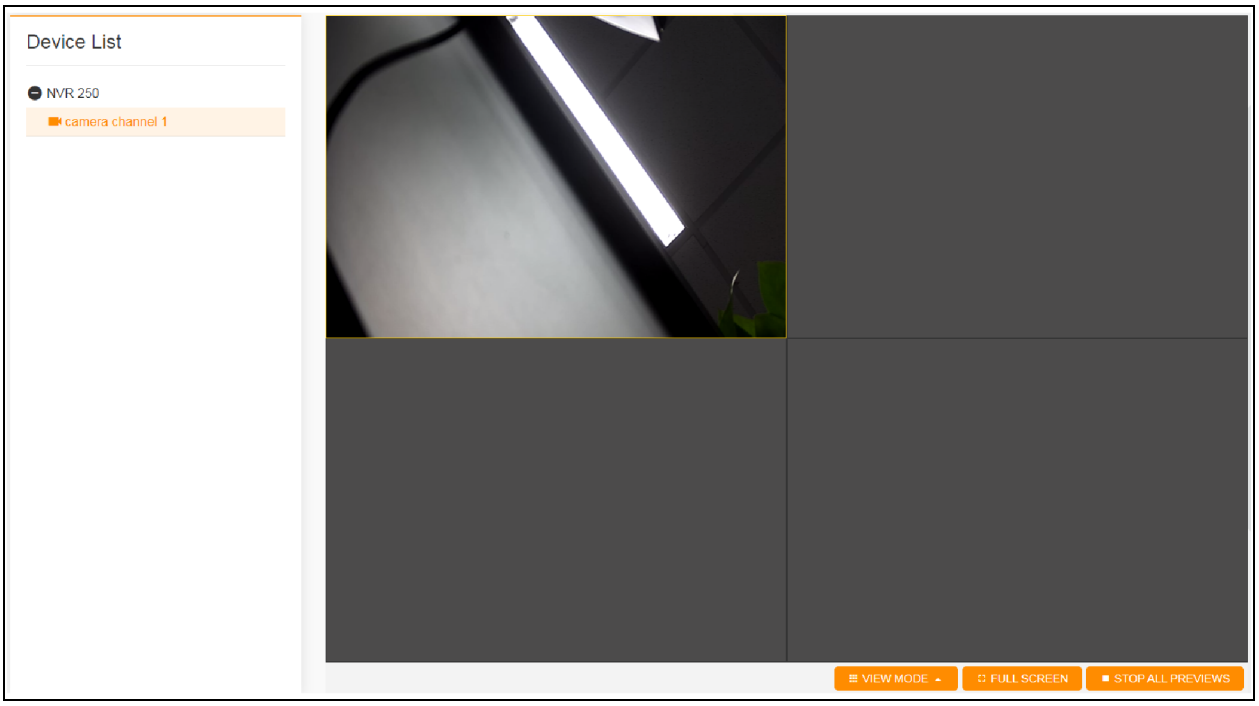


Previewing the Video

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 11.45** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

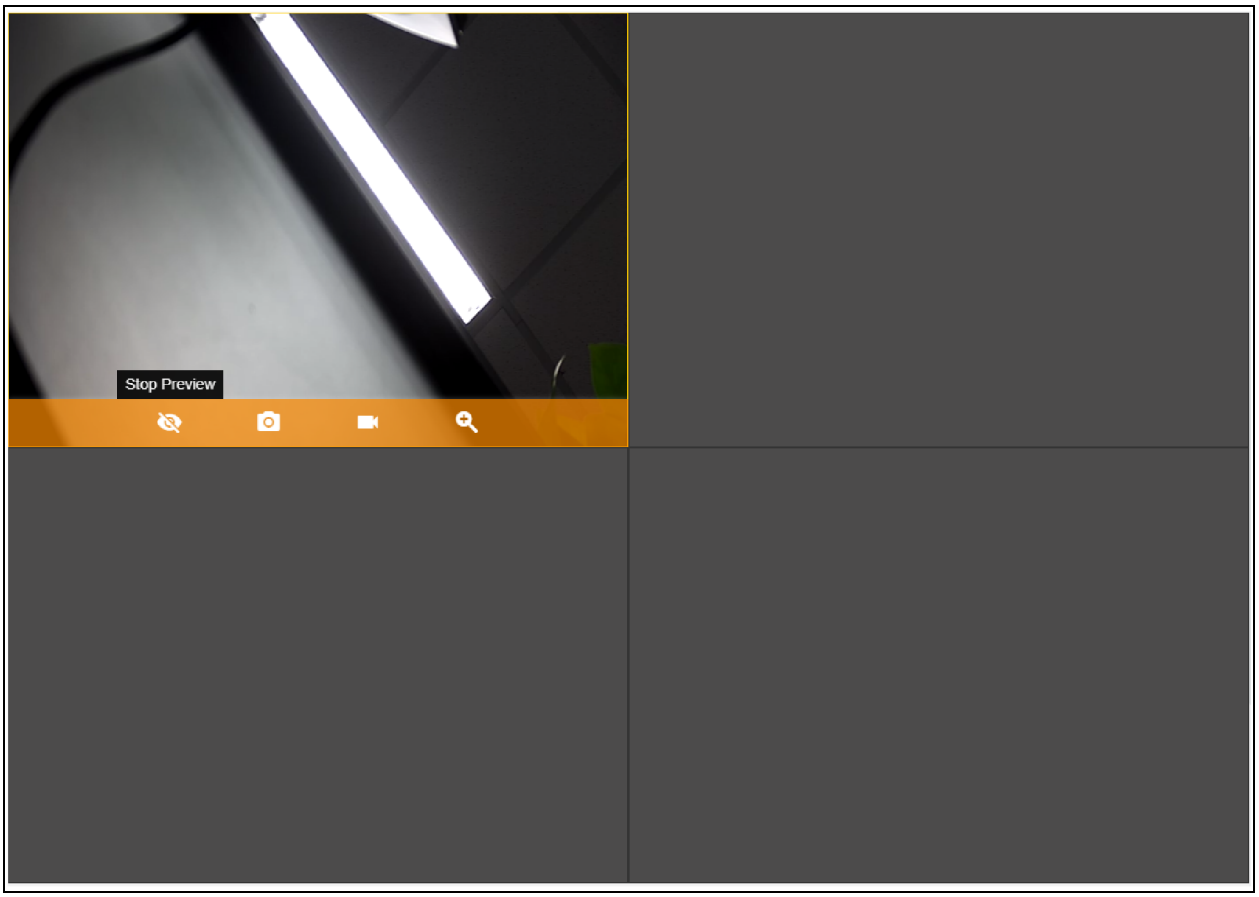
Figure 11.45 Previewing the Video



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 11.46** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.46 Stopping the Preview



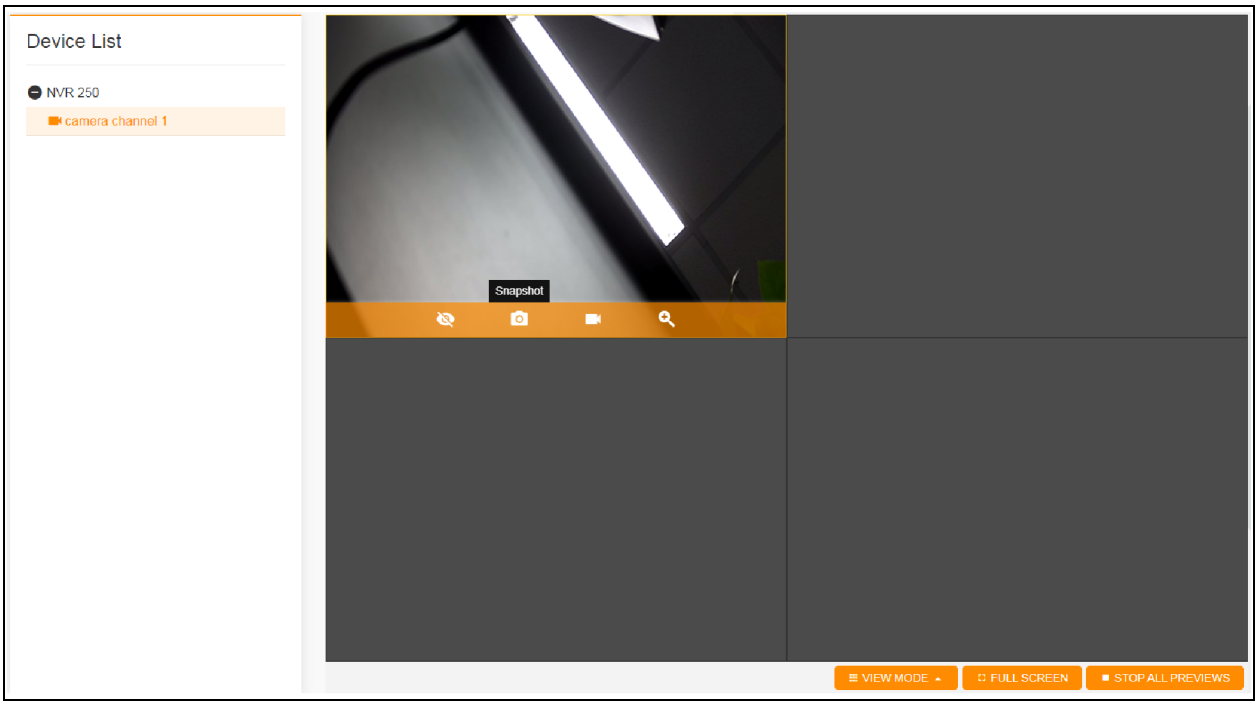
NOTE: The video preview feature is currently supported on Chrome 73+, Firefox 66+, and Edge 87+. It is not available on other browsers.

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 11.47** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.47 Capturing the Image



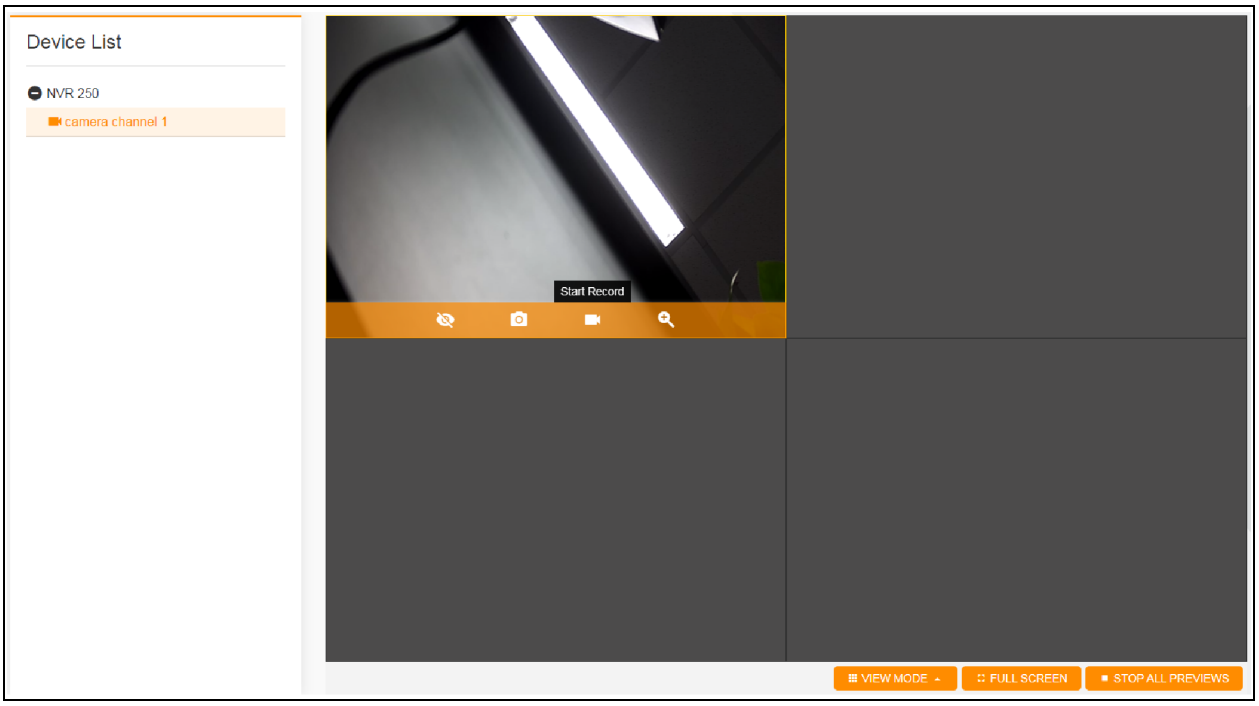
2. After clicking the snapshot button, the currently playing frame will be automatically captured.

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 11.48** on the next page .

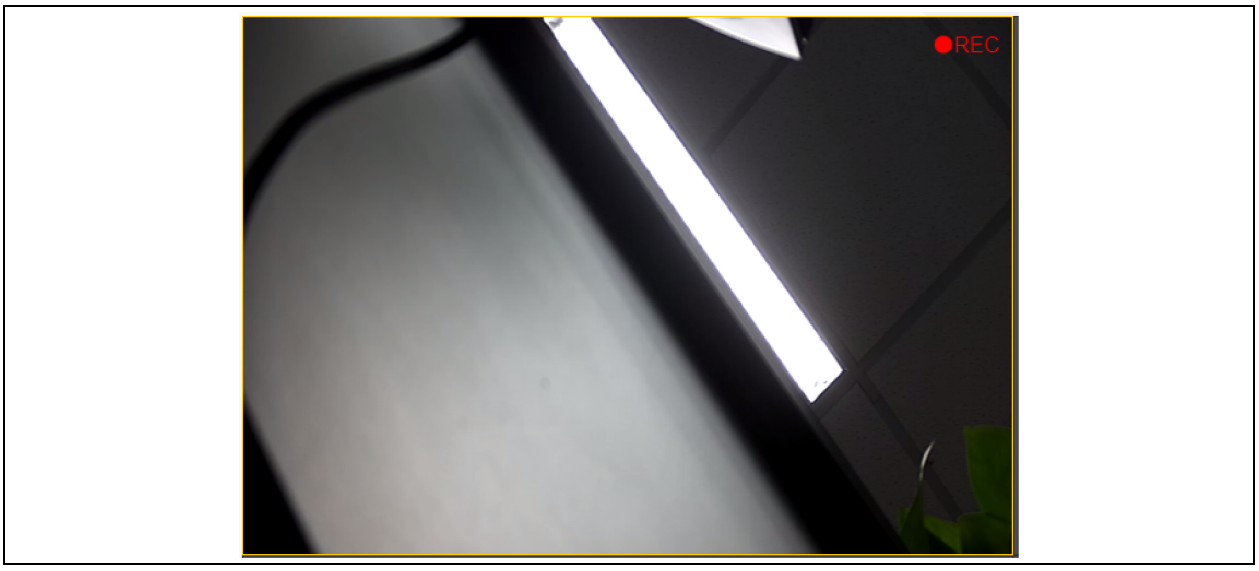
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.48 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 11.49 below .

Figure 11.49 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

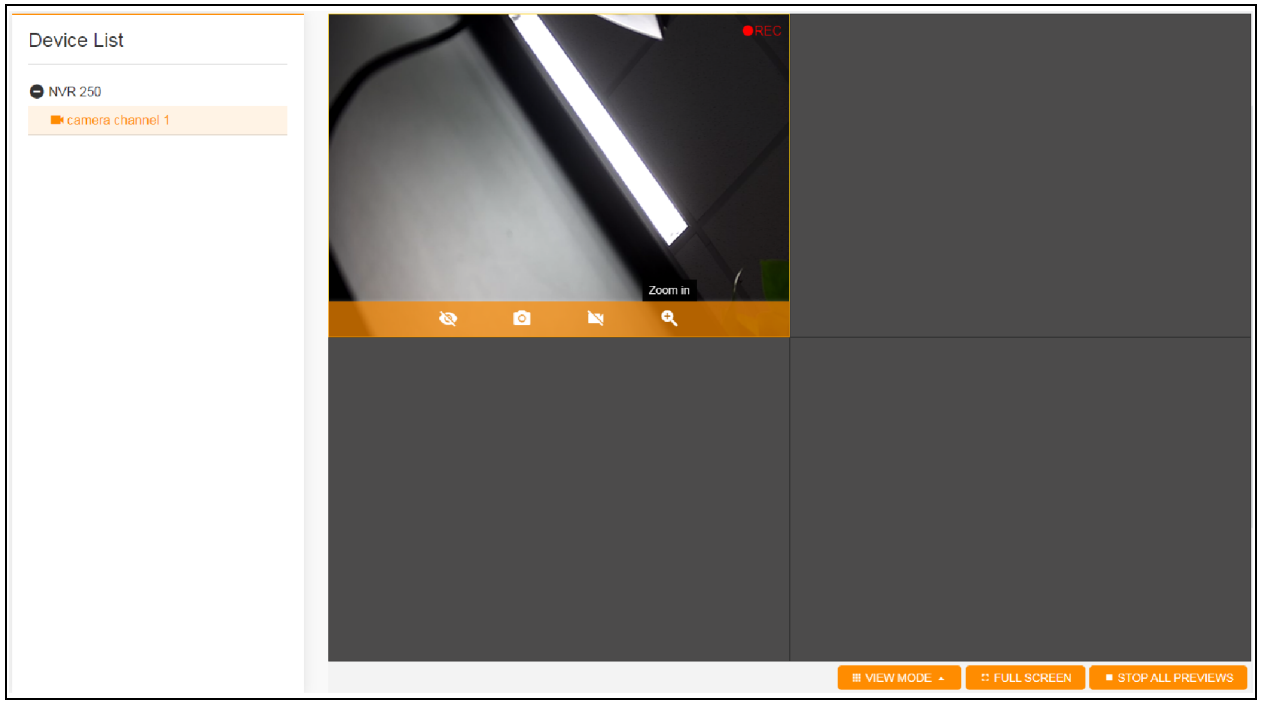
2. Multiple videos can be recorded at the same time.

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 11.50 below .

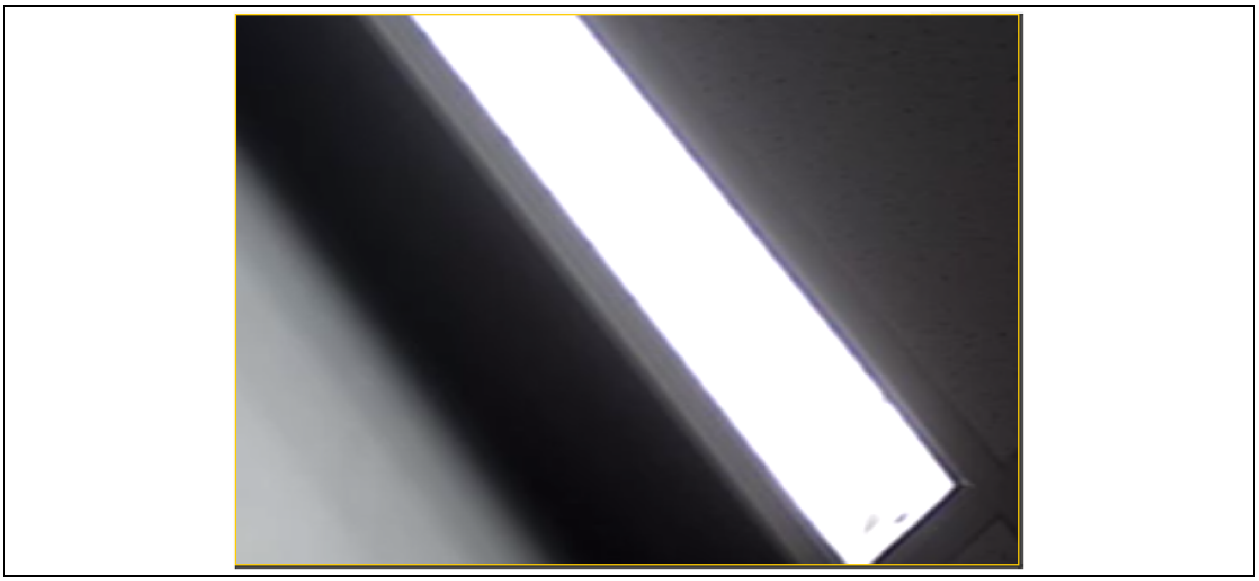
Figure 11.50 Zoom-in



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 11.51 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.51 Zoom-in View



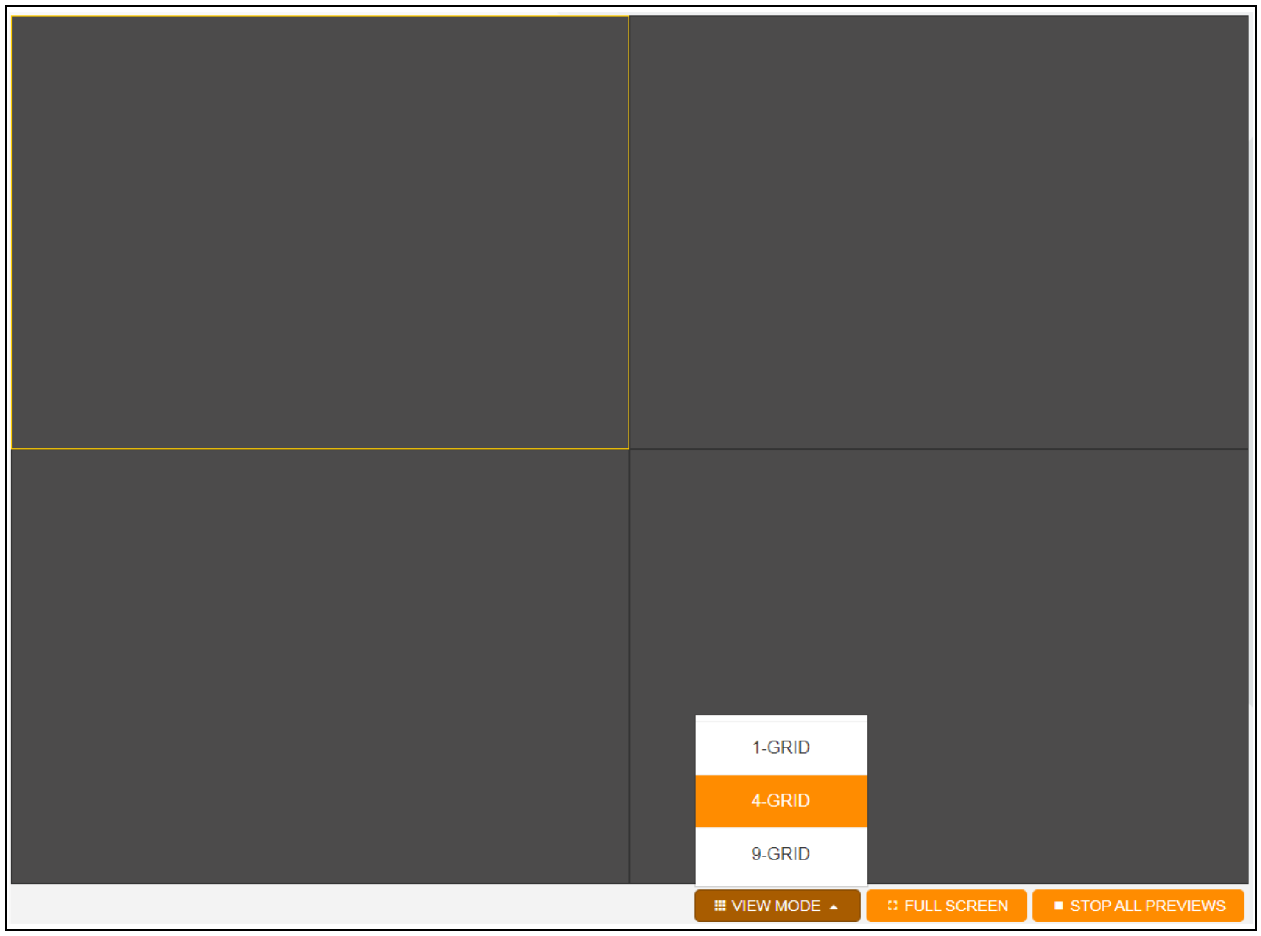
3. To restore a window, hover your mouse over its bottom edge and click the *restore* button.

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 11.52 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

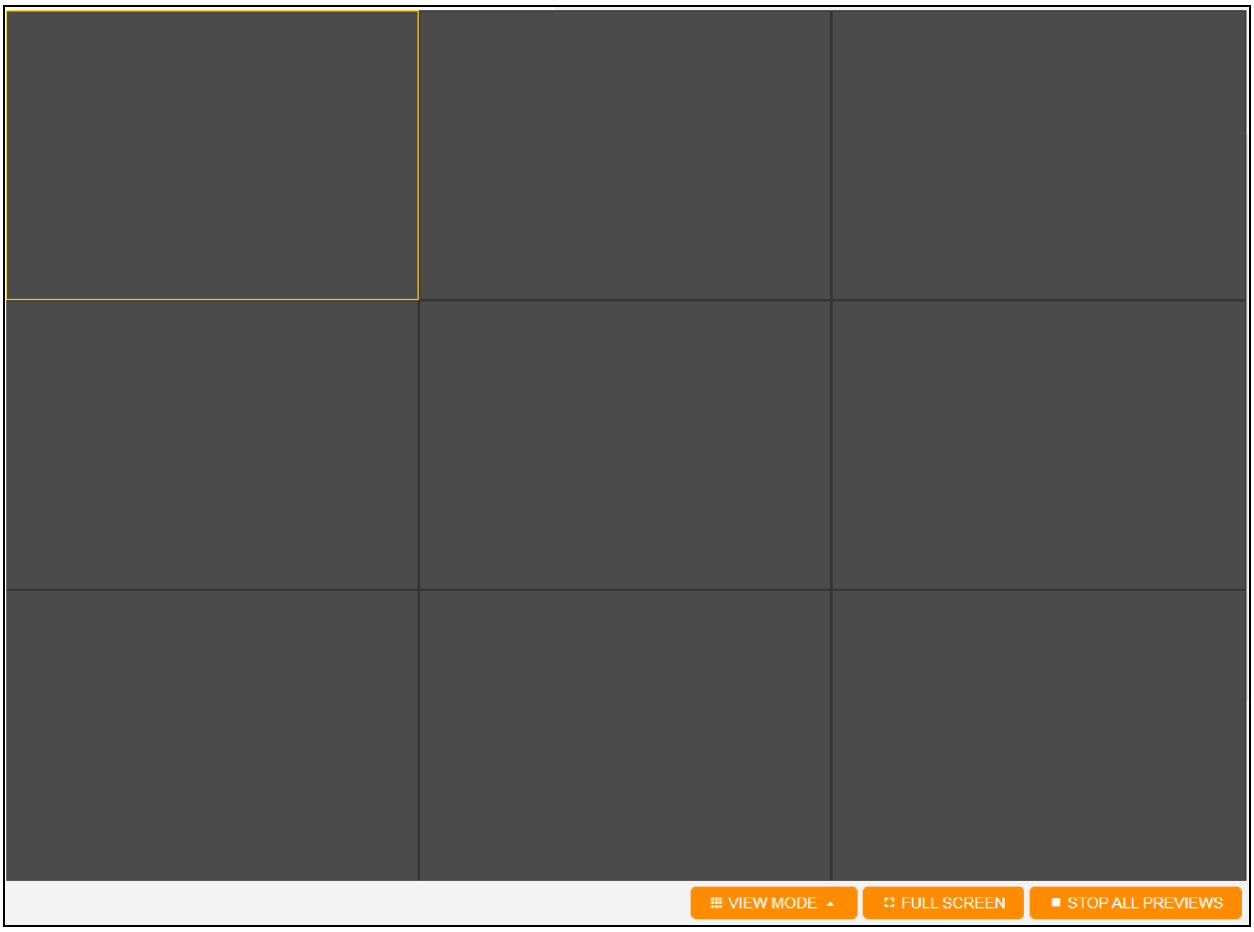
Figure 11.52 Split-Screen Mode



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 11.53** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.53 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.

11.2.6 Stored Videos

This module covers the functions for managing Stored 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 Stored Videos

Navigate to Security, then select Stored 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 11.54** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.54 Stored 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 Stored video for the chosen date. The orange bar at the bottom of the playback screen indicates available video segments, as shown in **Figure 11.55** below .

Figure 11.55 Searching the Stored Videos

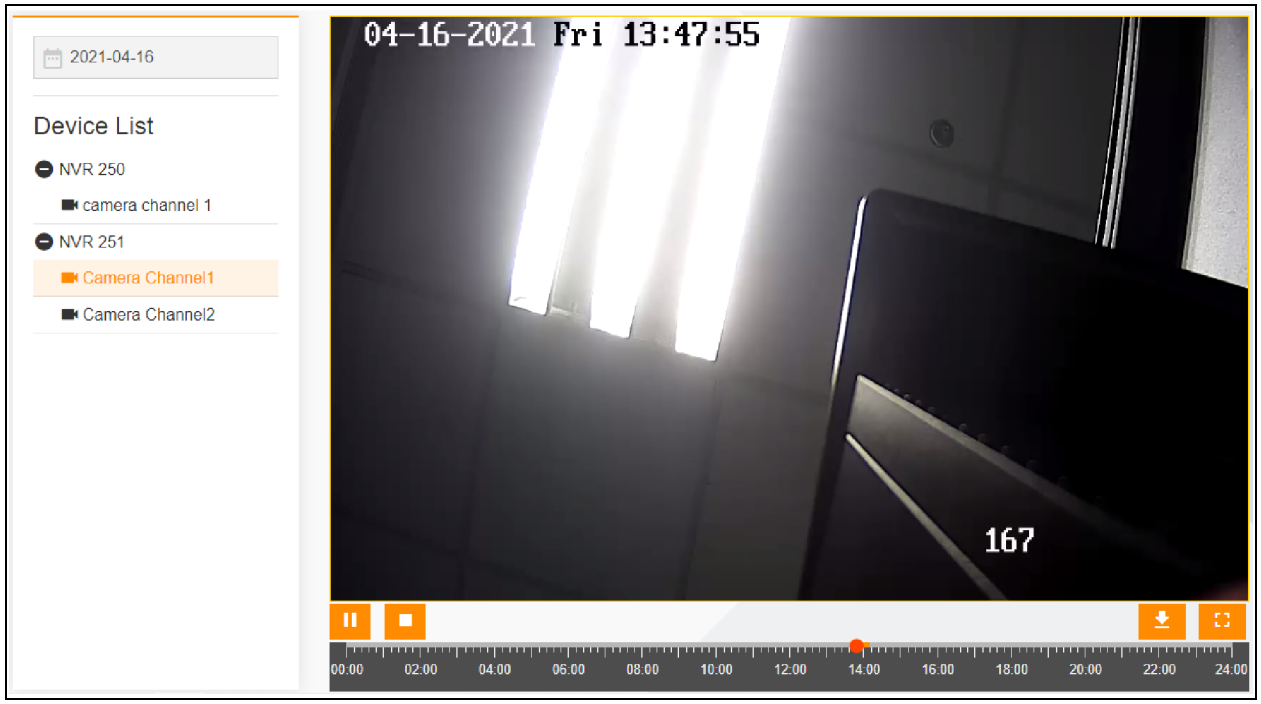


© 2026 Vertiv Group Corp. All Rights Reserved.

Playing a Stored 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 Stored video, as shown in Figure 11.56 below .

Figure 11.56 Playing a Stored Video



NOTE: Currently, Stored 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 11.57 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.57 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 11.58** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.58 Stored Video—Full Screen



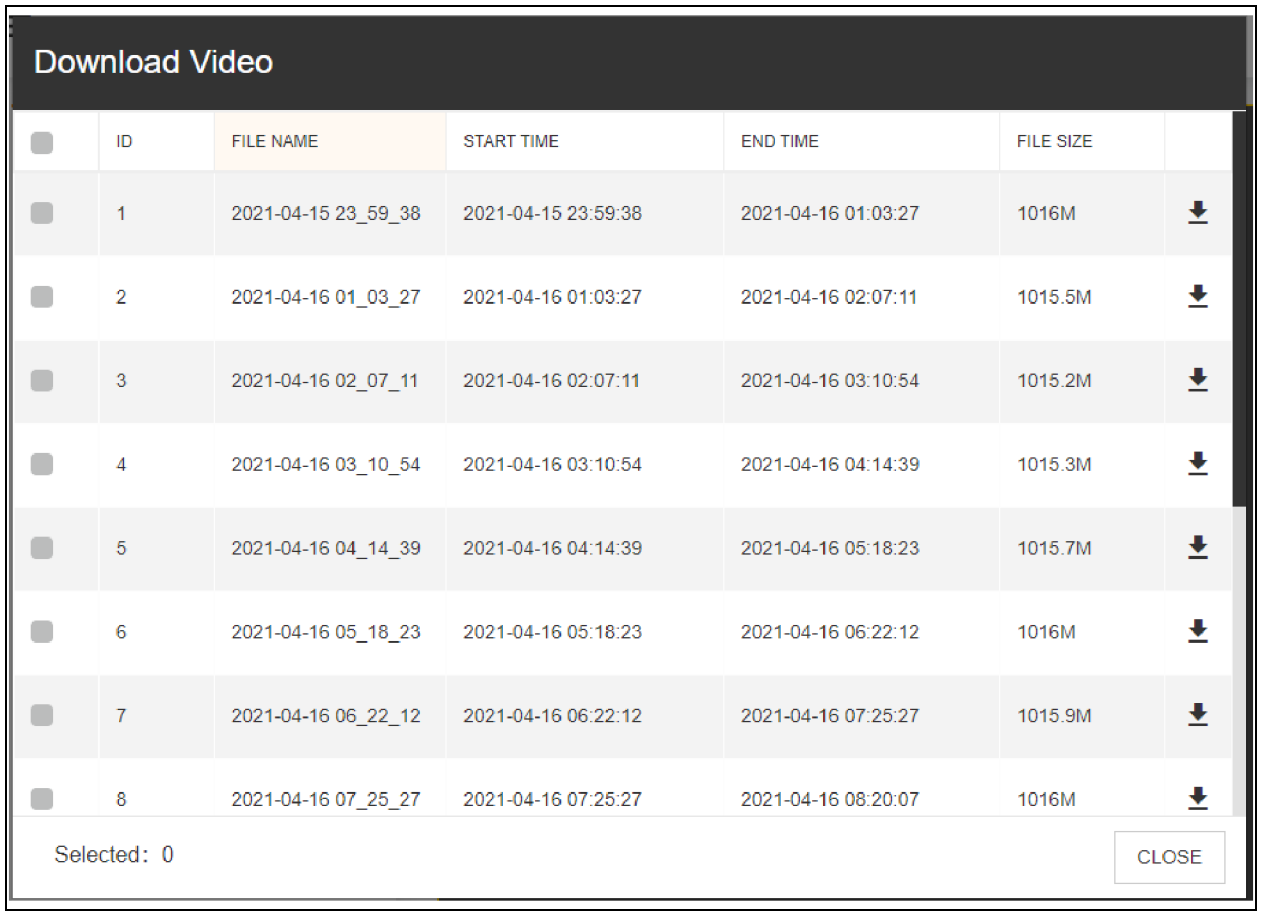
2. After the full screen display, press the *Esc* key to exit the full screen mode.

Downloading the Stored 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 Stored videos download page, as shown Figure 11.59 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

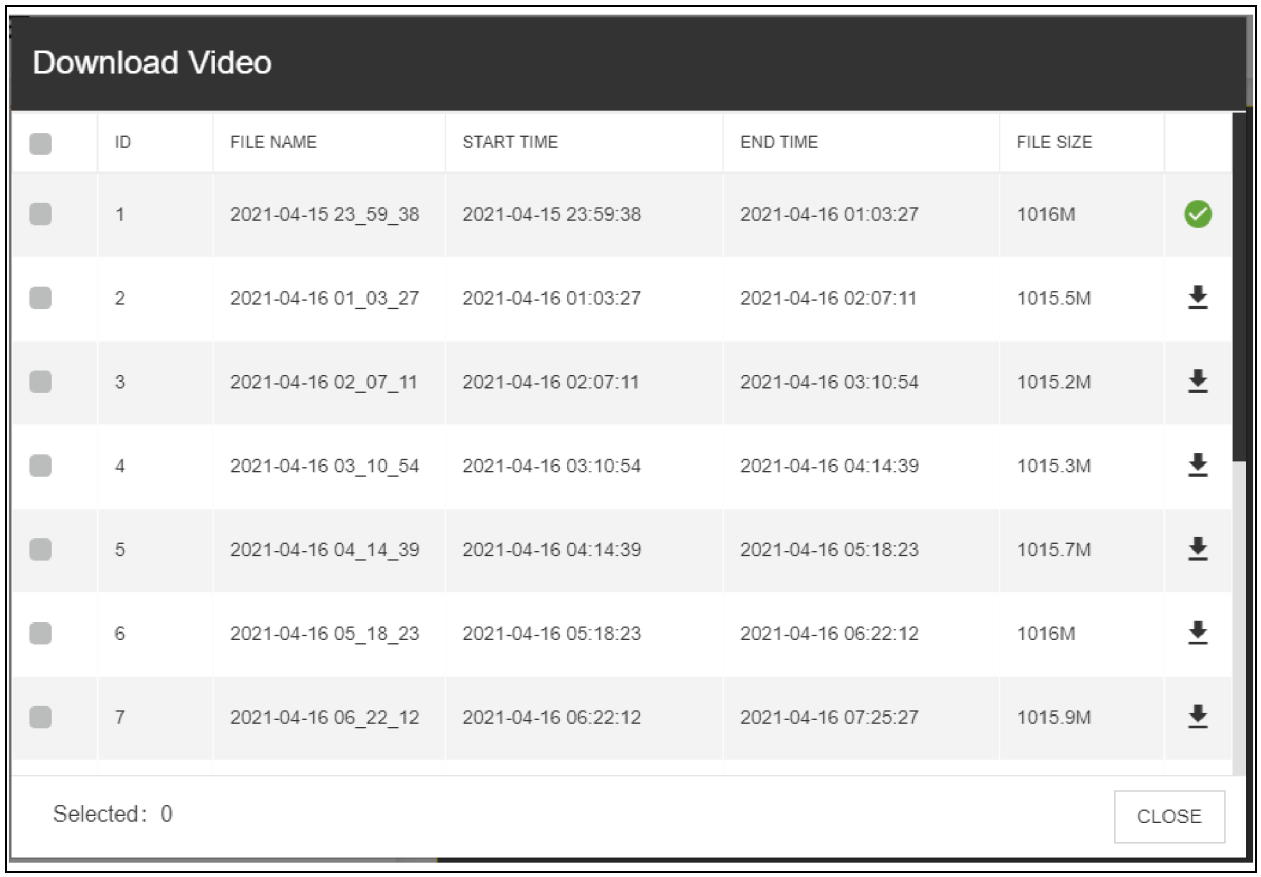
Figure 11.59 Download Video Popup Window



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 11.60 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

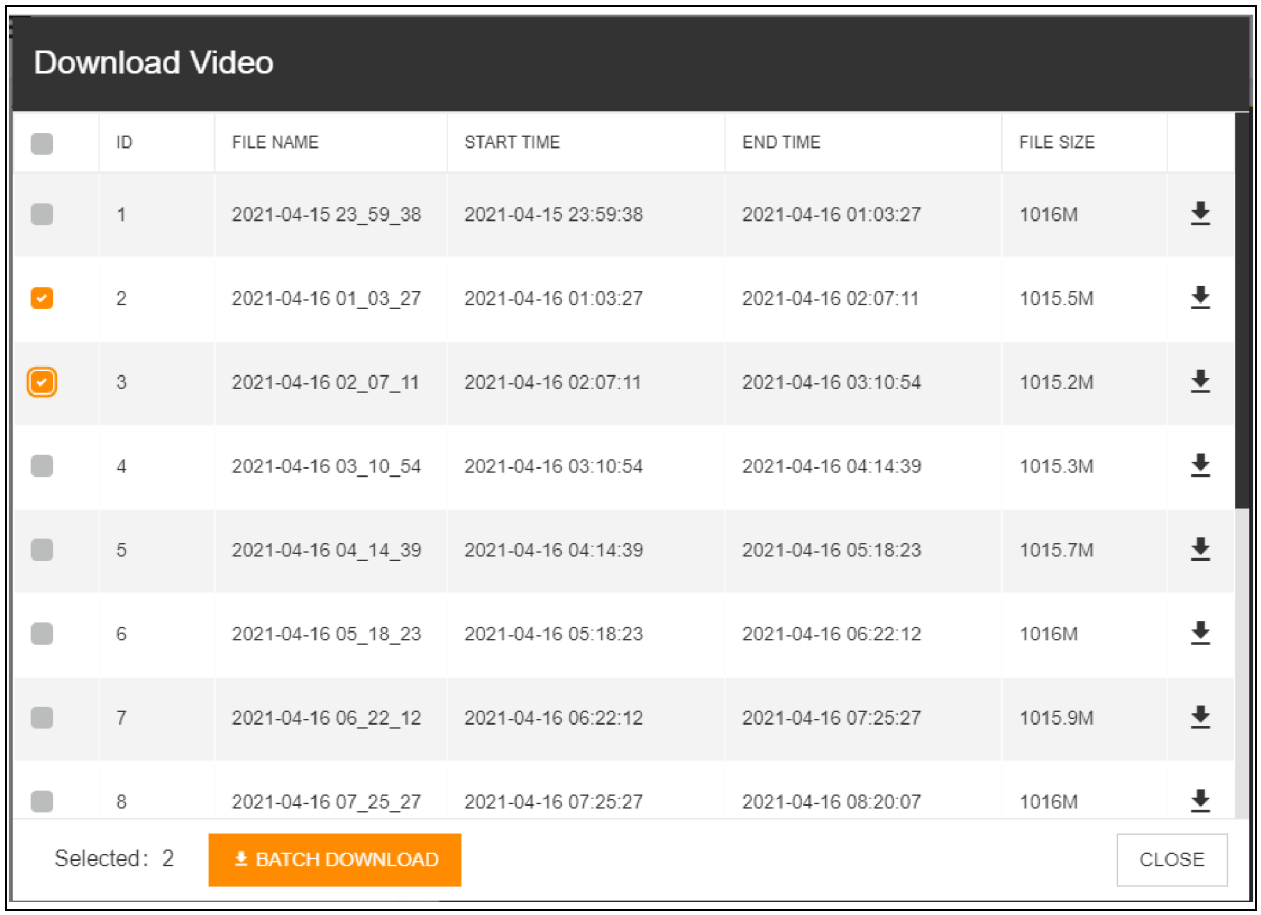
Figure 11.60 Downloading Stored Video



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 11.61 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

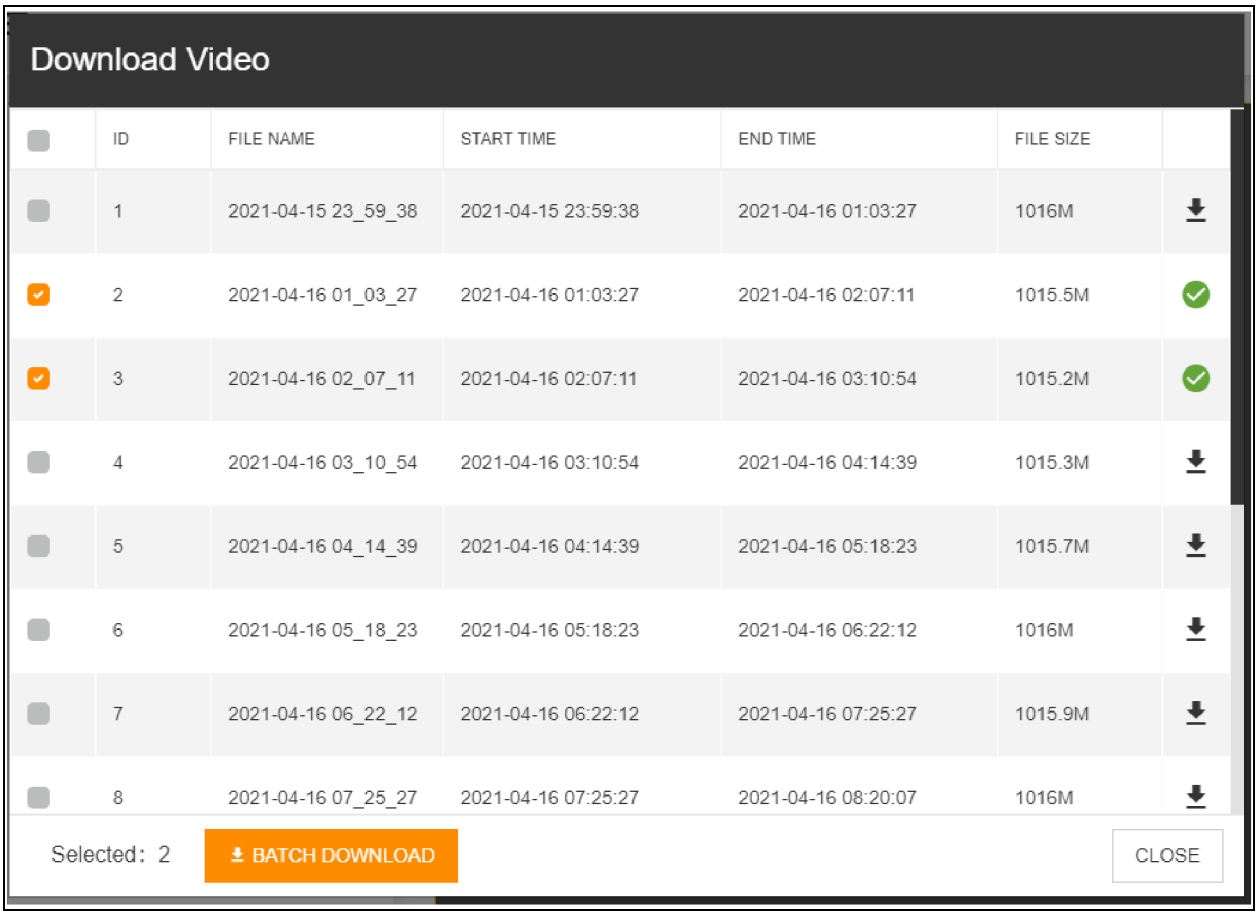
Figure 11.61 Download Stored Video Popup Window



6. When you click the *batch download* button. The browser will automatically download these video files in turn, as shown in Figure 11.62 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.62 Downloading the Stored Video in Batches



NOTE:

1. Downloading Stored 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.

11.2.7 Device Management

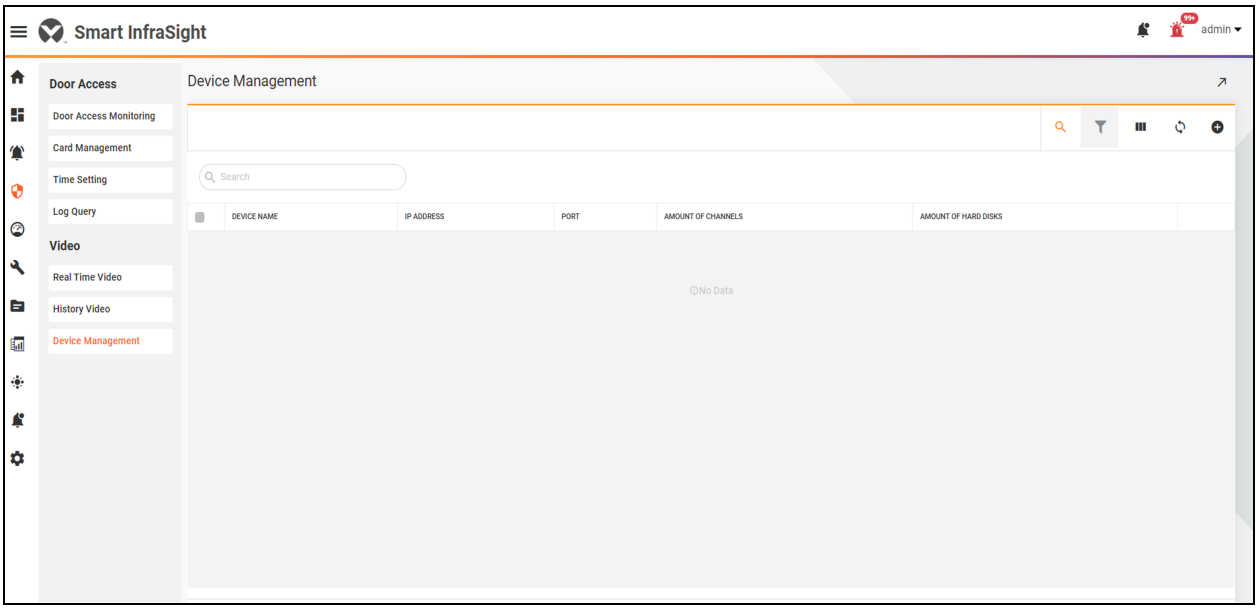
This module describes the management functions of video devices, including adding, deleting, and modifying NVR devices, and adding, deleting, and modifying IPC devices in the channel list.

Device List

Go to Security, then click on *Device Management* to open the Device Management page. Device data is paginated with 10 entries per page. The device List includes five columns: **Device Name**, **IP Address**, **Port**, **Channel Quantity**, and **Hard Disk Quantity**, as shown in **Figure 11.63** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.63 Video Device List

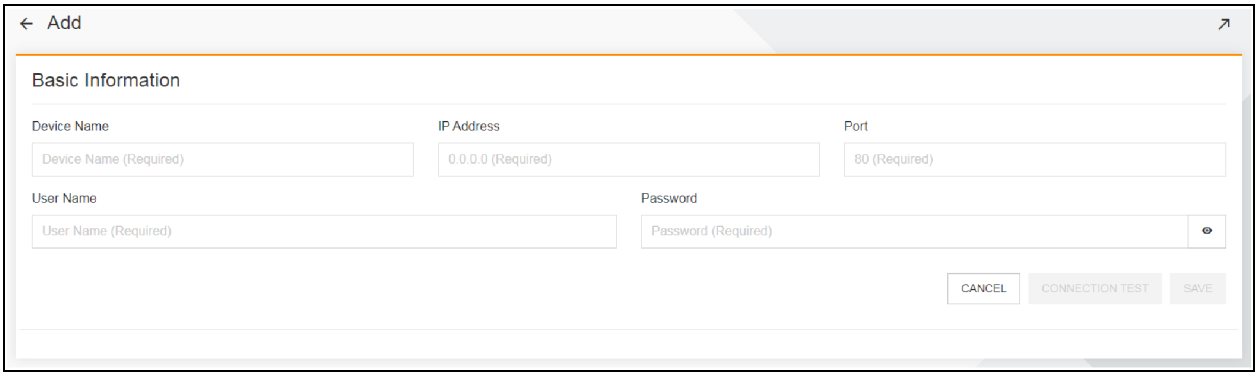


NOTE: If no video devices have been added to the Platform, the device List displays No Data.

Adding a Device

1. Click the *Add* button. to open the add device page, as shown in Figure 11.64 below .

Figure 11.64 Adding NVR Device



2. Enter the device Name, IP Address, Port, device username and password.
3. To verify the entered credentials and network settings, click Connection Test. If the information is incorrect, the Platform displays a corresponding prompt..
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 between 3 and 64 characters and must be unique.

2. The IP Address must be unique.

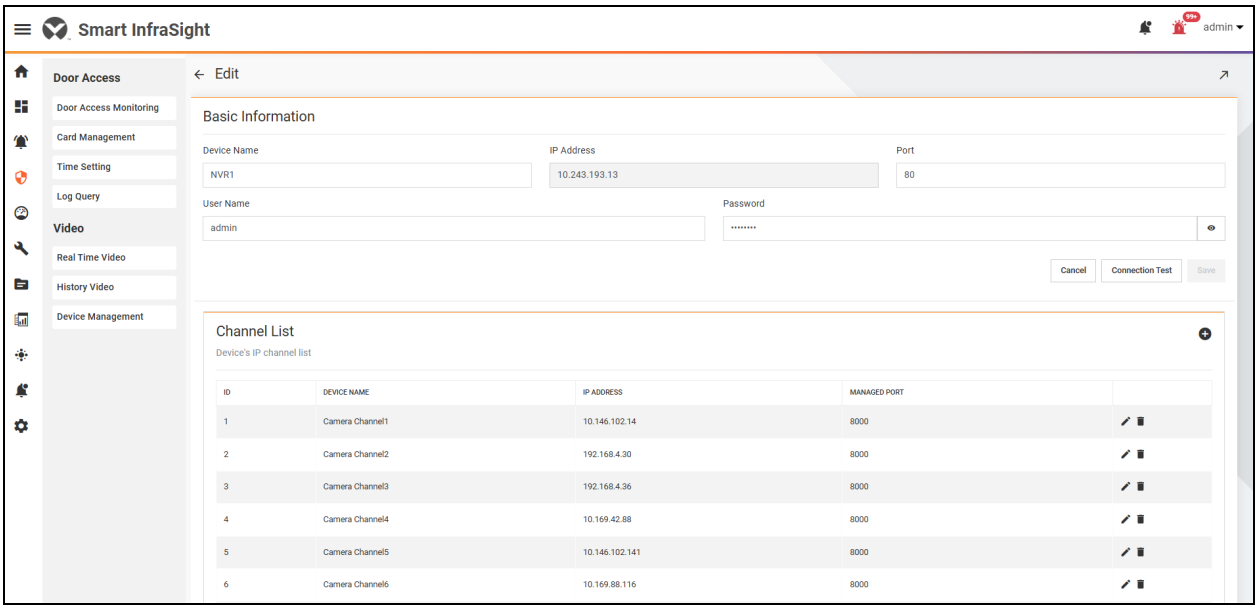
© 2026 Vertiv Group Corp. All Rights Reserved.

3. The Connection Test and Save buttons are only enabled after all required fields are correctly completed and validated.

Editing the Device

1. Click 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 11.65** below .

Figure 11.65 Editing NVR Device



2. Modify the Device Name, username, or password, and click *save*.

NOTE:

1. You cannot modify the IP Address or Port of a video device. To change these, delete the device and add it again.

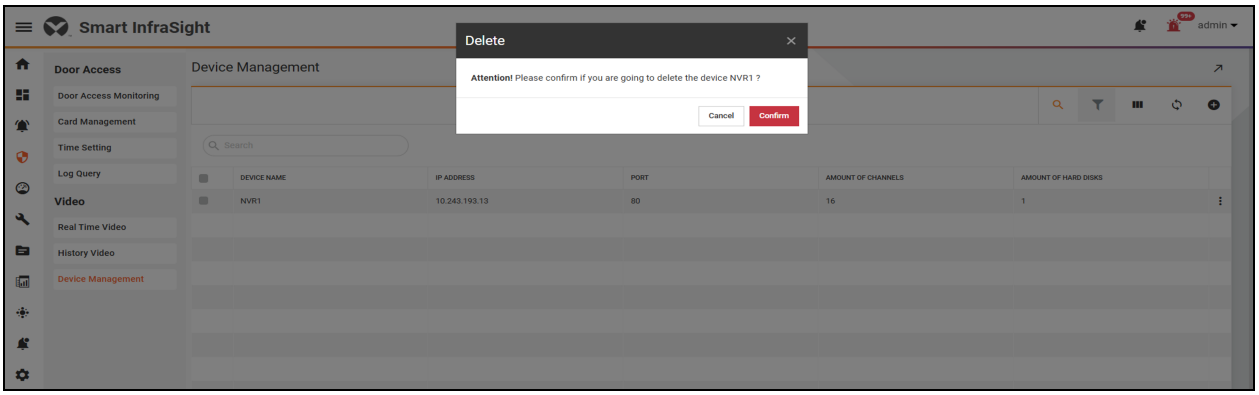
2. In the Edit page, the Save button is only enabled after information has been modified.

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 11.66** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 11.66 Deleting the Device



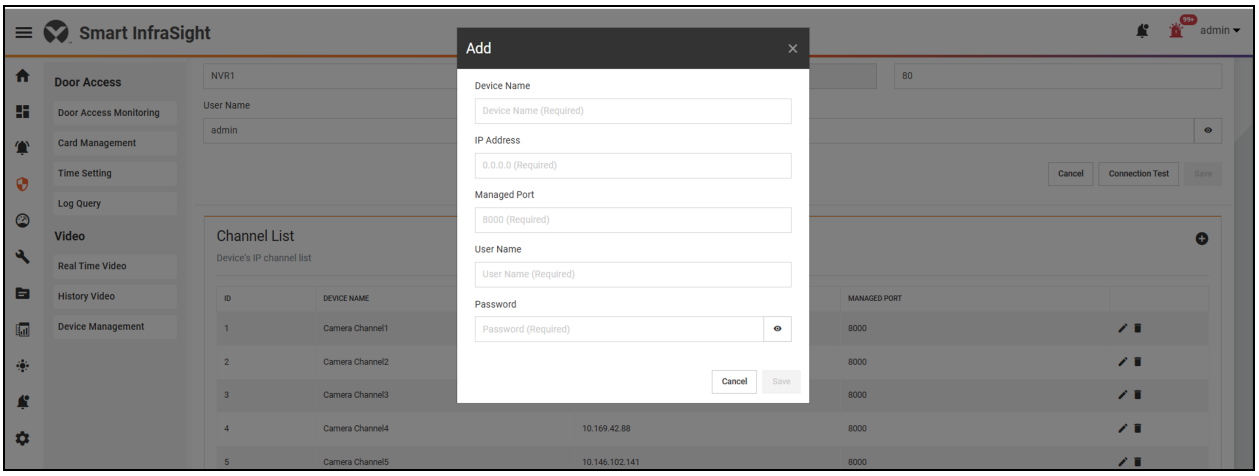
2. Click on *Confirm* and the device will be deleted.

NOTE: When a device is deleted, all IPC device data within its channels will also be deleted.

Adding an IPC Device to the Channel

1. 1. Go to **Security > Device Management**. Click 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 at the bottom of the page. The following interface appears as shown in **Figure 11.67** below .

Figure 11.67 Adding an IPC Device



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

NOTE:

1. The IPC Device Name must be between 3 and 64 characters and must be unique within the same NVR channel.

2. The IP Address of the IPC device must be unique within the same NVR channel.

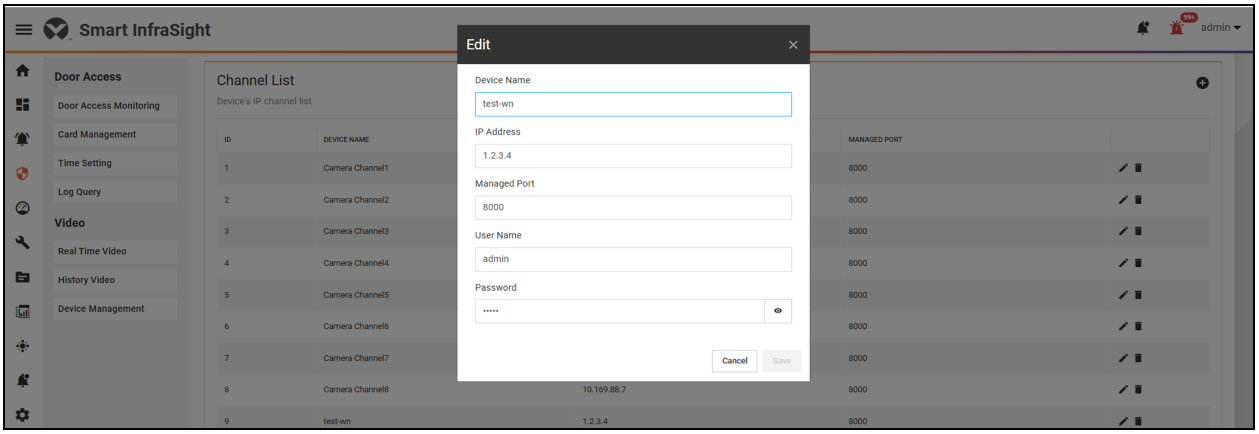
3. The Save button is only enabled after all required fields are correctly completed and validated.

© 2026 Vertiv Group Corp. All Rights Reserved.

Editing the IPC Device in the Channel

1. In the channel list, click *edit* on the right side of the IPC device entry. The following interface appears as shown in Figure 11.68 below .

Figure 11.68 Editing the IPC Device



2. Modify the IPC Device Name, IP Address, Management Port (default is 8000), or the IPC username/password. Click *Save*.

NOTE:

1. The IPC Device Name must be between 3 and 64 characters and must be unique within the same NVR channel.

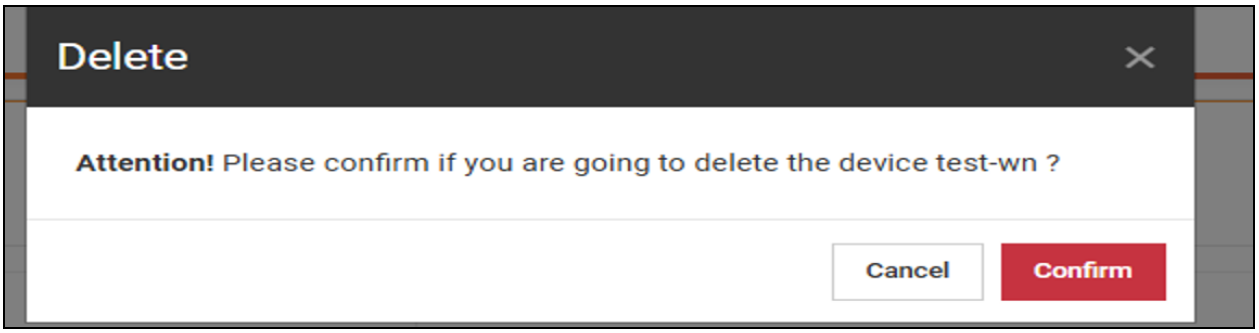
2. The IP Address of the IPC device must be unique within the same NVR channel.

3. In the Edit window, the Save button is only enabled after information has been modified.

Deleting the IPC Device in the Channel

1. In the channel list, click *delete* on the right side of the IPC device information, and the prompt interface will pop up as shown in Figure 11.69 below .

Figure 11.69 Deleting the IPC Device



2. Click *Confirm* to remove the IPC device from the Channel List.

NOTE: Deleting a device only removes the device data from the current Platform.

© 2026 Vertiv Group Corp. All Rights Reserved.

12 Energy Management

12.1 General

12.1.1 Overview

The Energy Consumption module includes Energy Consumption Configuration and PUE Configuration.

Energy Consumption Configuration allows you to calculate the energy consumption under a specific combination by adding device signals — for example, calculating the energy consumption of a particular site.

PUE is typically defined as the total energy consumption of the data center divided by the energy consumption of IT equipment. The total data center energy consumption includes IT equipment energy consumption as well as the energy consumption of systems such as cooling and power distribution. The PUE value is always greater than 1; the closer it is to 1, the less energy non-IT equipment consumes, indicating a higher energy efficiency level of the data center. PUE Configuration supports calculation in the following modes: electric energy mode, power mode, and data retrieval from RDU mode.

12.1.2 Functional Modules

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

- Energy Consumption Configuration
- PUE

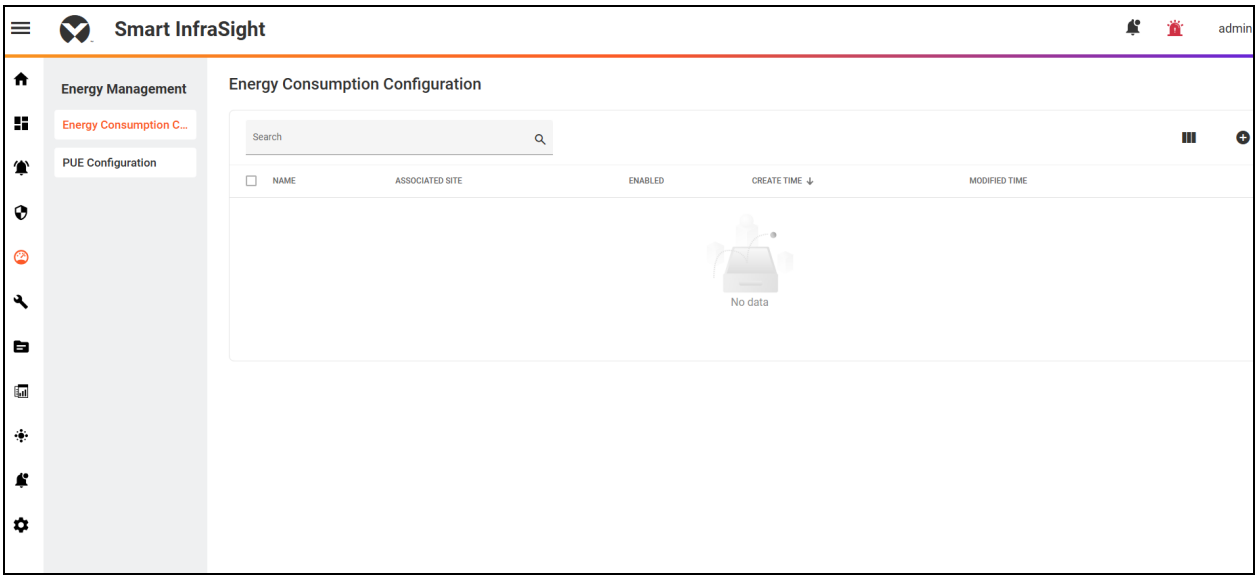
12.2 Detailed Features

12.2.1 Energy Consumption Configuration

In the Vertiv™ Smart InfraSight™ home page, click the *corresponding menu* item to go to the Energy Consumption Configuration page, as shown in Figure 12.1 on the next page .

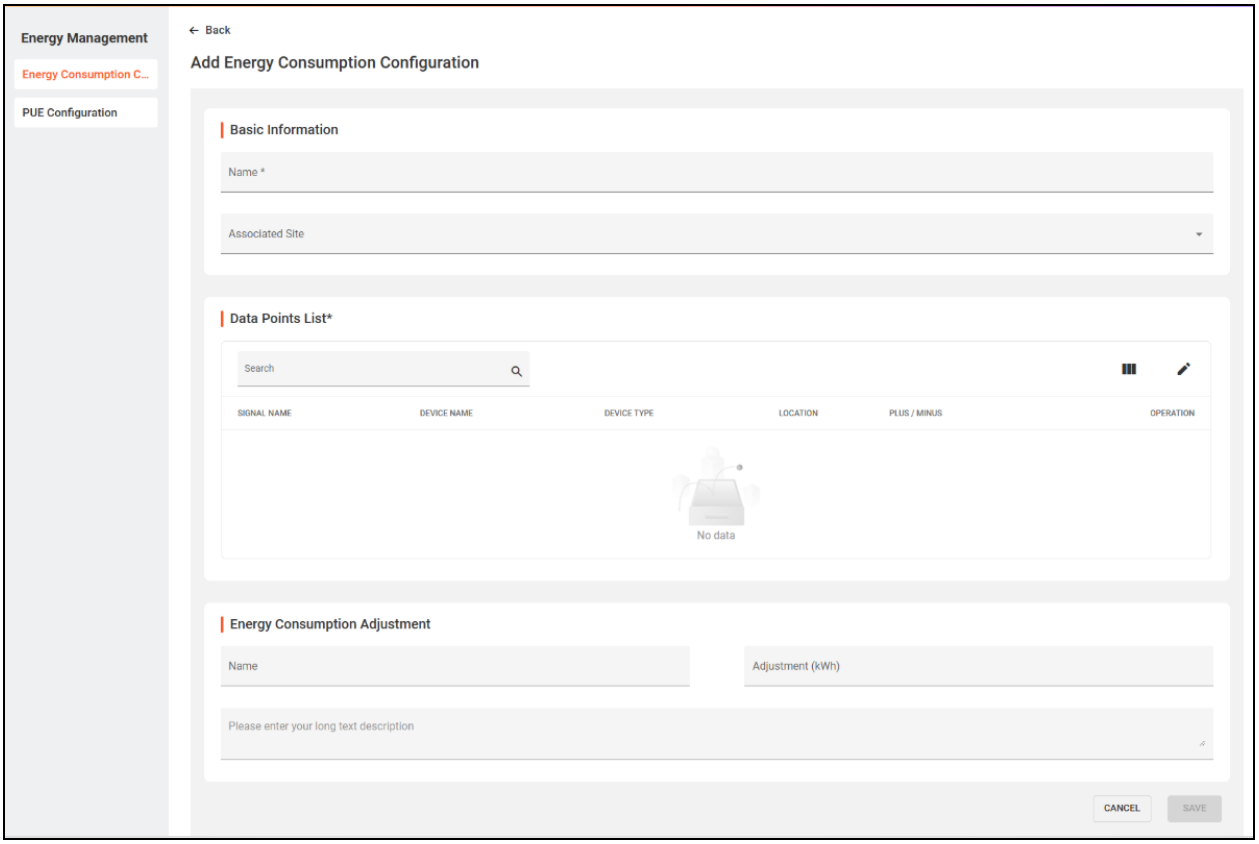
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 12.1 Energy Consumption Configuration



Then click the (+) icon in the upper-right corner to go to the Add Energy Consumption Configuration page. On this page, enter a name, select an associated site, and configure the adjustment value.

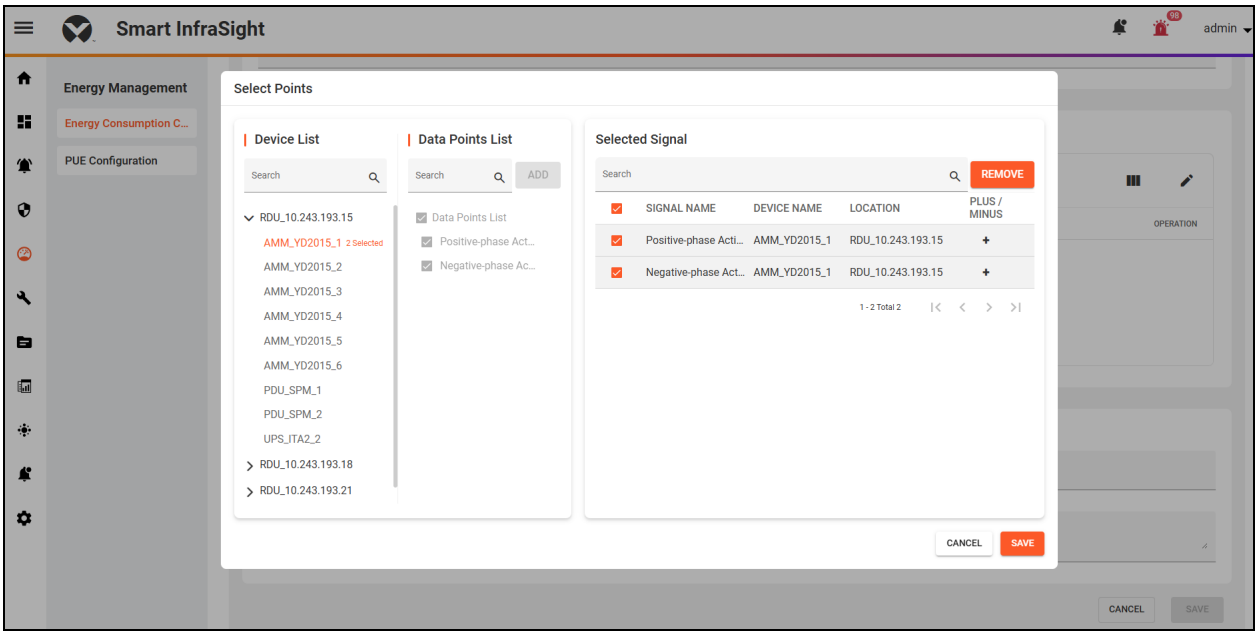
Figure 12.2 Adding the Energy Consumption Configuration



Click the *Edit* icon in the signal list to add device signals:

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 12.3 Adding Device Signals



The energy consumption calculation formula is:

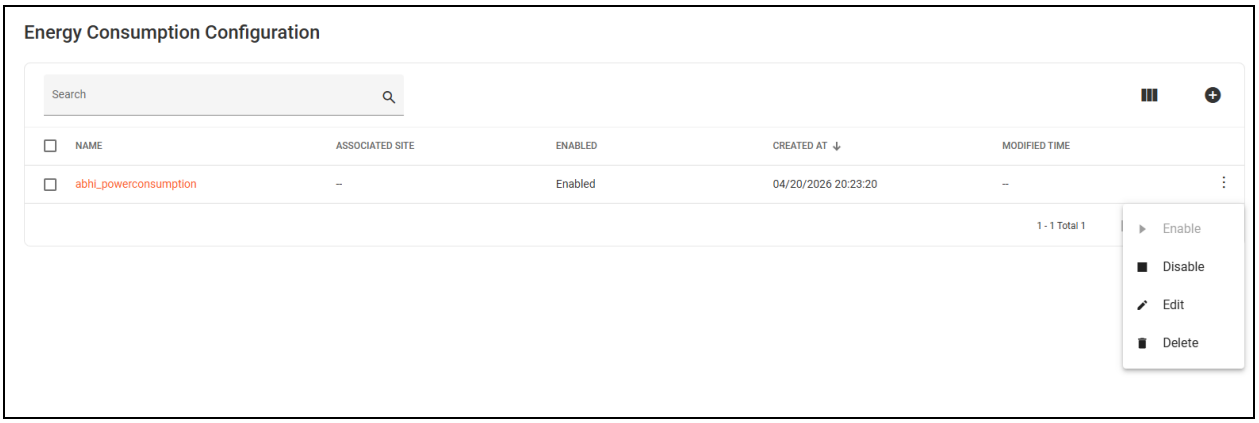
Energy Consumption = Signals marked (+) − Signals marked (−) + Energy Consumption Adjustment Value (configurable based on actual requirements).

Click *Save* to complete the energy consumption configuration.

Enable Energy Consumption Configuration

Click the ellipses (⋮) in the Energy Consumption Configuration list, then click the *Edit* icon, as shown below:

Figure 12.4 Enabling/disabling the Energy Consumption Configuration



Editing the Energy Consumption Configuration

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

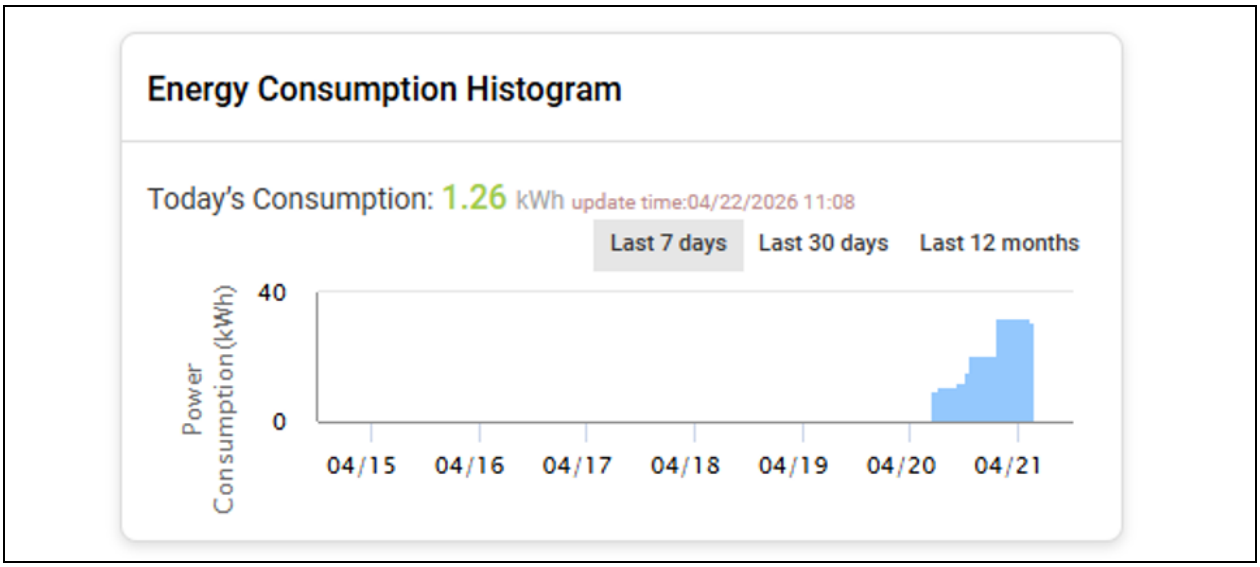
Deleting the Energy Consumption Configuration

Click the ellipses (⋮) icon in the Energy Consumption Configuration list, then click the icon, as shown in **Figure 12.5** below :

© 2026 Vertiv Group Corp. All Rights Reserved.

After the energy consumption configuration is complete, you can select an associated site. Once associated, the calculation results of the energy consumption configuration are used to represent the energy consumption changes of the site. For example, the energy consumption bar chart widget automatically retrieves the calculation results of the energy consumption configuration associated with the site.

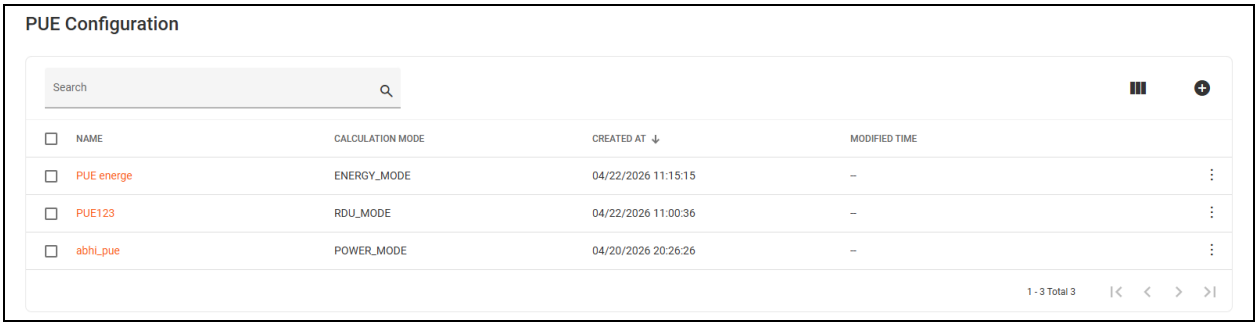
Figure 12.5 Energy Consumption Histogram



12.2.2 PUE Configuration

PUE Configuration List

Figure 12.6 PUE Configuration List



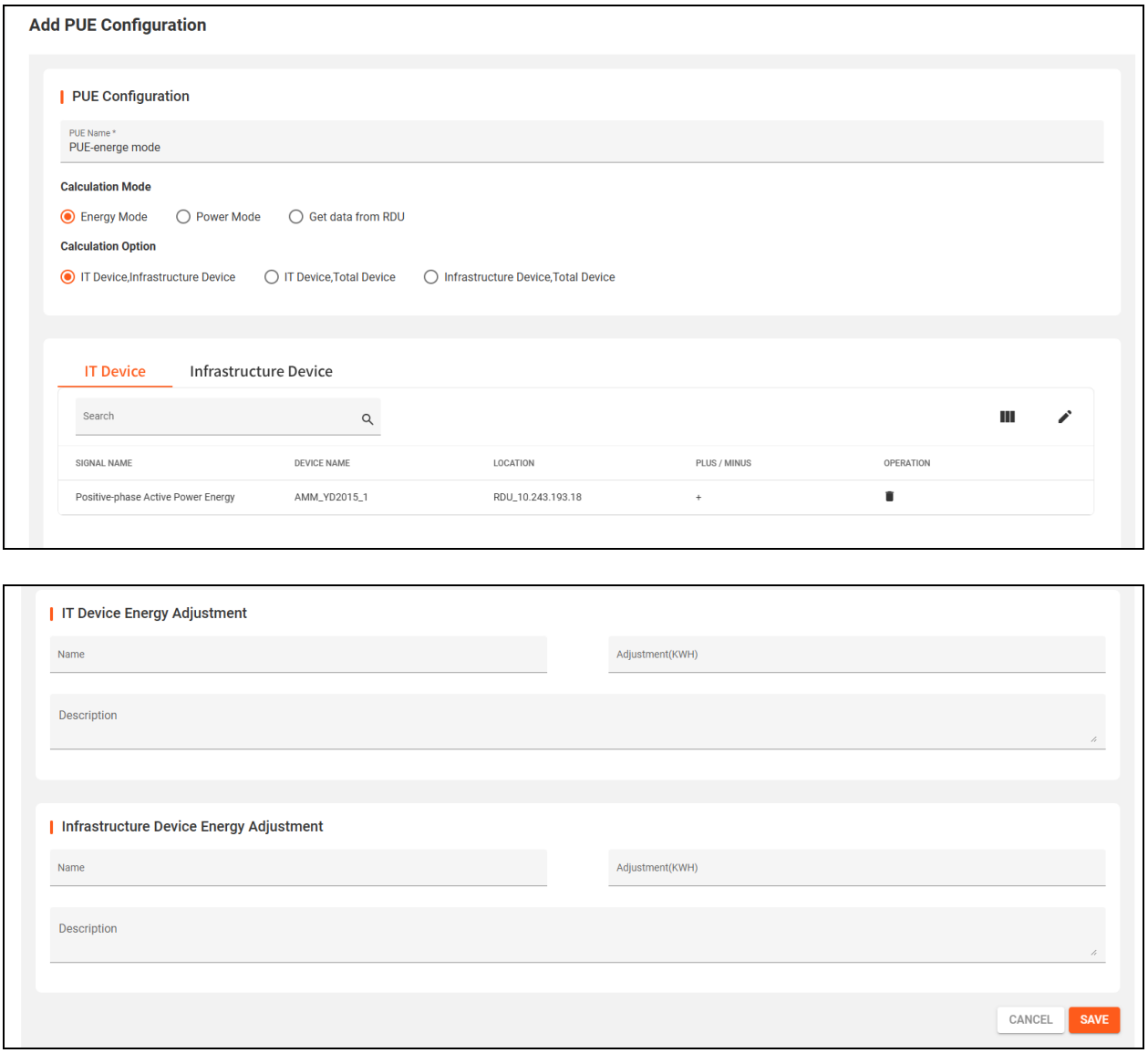
The Columns button on the right side allows you to show or hide columns (Calculation Mode, Created Time, and Modified Date).

Add PUE Configuration

On the Smart InfraSight home page, click the *PUE Configuration* icon, select PUE Configuration, and click the (+) plus sign in the upper-right corner to go to the Add PUE Configuration page, as shown in **Figure 12.7** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 12.7 Adding PUE Configuration



Three PUE calculation modes are available:

1. Energy Mode: Calculates the PUE value based on the previous day's device energy consumption (kWh). In this mode, the platform calculates the energy consumption PUE value at 01:00 every day based on the selected signals. After saving the Energy Mode PUE Configuration, the previous day's energy consumption PUE value is calculated immediately. The calculation method is as follows (using IT devices and infrastructure devices as an example):

If the current day's IT device energy consumption is 20 kWh, the previous day's IT device energy consumption is 10 kWh, the current day's total device energy consumption is 50 kWh, and the previous day's total device energy consumption is 30 kWh, then PUE = (50 - 30) / (20 - 10) = 2.0.

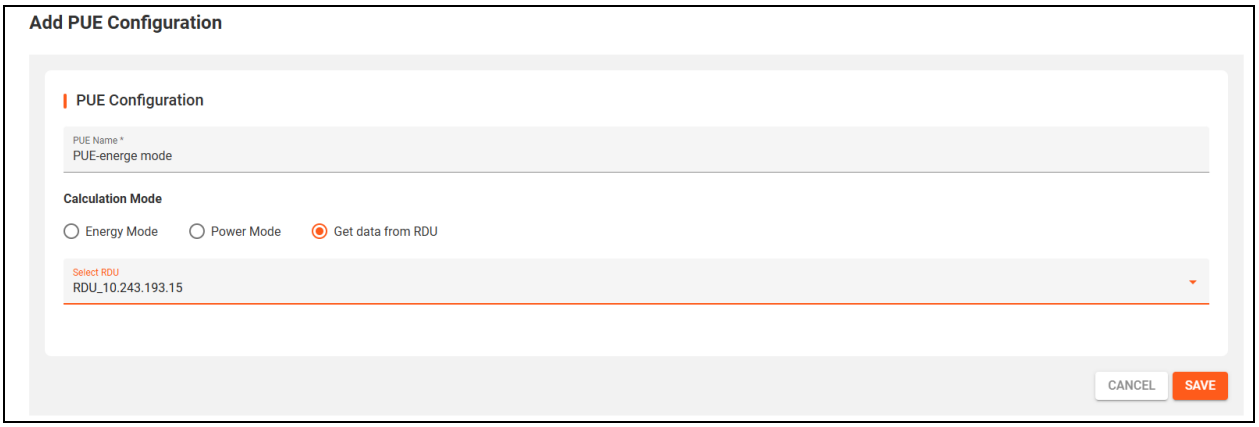
2. Power Mode: Calculates the PUE value based on real-time device power (kW). The PUE value is calculated every 30 seconds based on the selected signals and saved to the current time point. The calculated PUE value is stored at every full hour. After saving the Power Mode PUE Configuration, the current power PUE value is calculated immediately. The calculation method is as follows (using IT devices and infrastructure devices as an example):

© 2026 Vertiv Group Corp. All Rights Reserved.

For example, if the current total power consumption of the IT devices is 20 kW and the current total power consumption of all devices is 50 kW, then the PUE is calculated as follows: PUE = 50 / 20 = 2.5.

3. Getting Data from RDU: If the selected RDU has a PUE configuration, the platform can directly get the RDU's PUE mode and calculated PUE value. The data storage policy and widget display style are determined by the RDU's PUE calculation mode. If the RDU's PUE calculation mode is Power Mode, the platform saves data every 30 seconds, and the PUE widget display style is the same as the platform's Power Mode. If the RDU's PUE calculation mode is Energy Mode, the PUE value is saved once per hour, the PUE widget display style is the same as the platform's Power Mode, and the mode displays **Energy Consumption Mode**. After saving, the platform immediately retrieves and saves the PUE value from the selected RDU, as shown in **Figure 12.8** below .

Figure 12.8 Getting Data from RDU



NOTE: To use the Retrieve Data from RDU feature, you must first complete RDU user authentication under Monitoring > Site Monitoring Tree > Site Menu > User Authentication before the platform can retrieve PUE calculation data from the RDU.

After selecting the calculation mode:

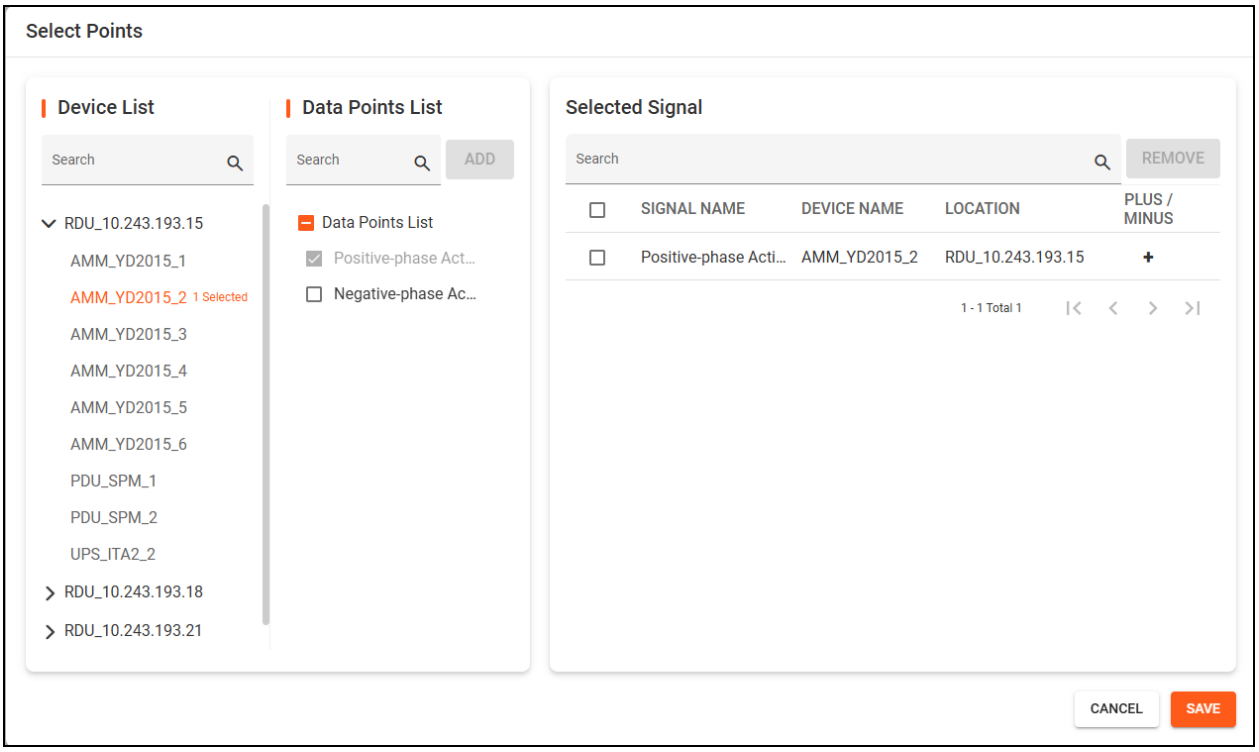
If Energy Mode is selected, select the device energy consumption signals to participate in the PUE calculation.

If Power Mode is selected, select the device power signals to participate in the PUE calculation.

Click the *edit* icon upper-right corner of IT Device / Infrastructure Device / Total Device to go to the signal Configuration page for the corresponding device type, and select the signals that make up the corresponding device.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 12.9 Configuring the Device Signals

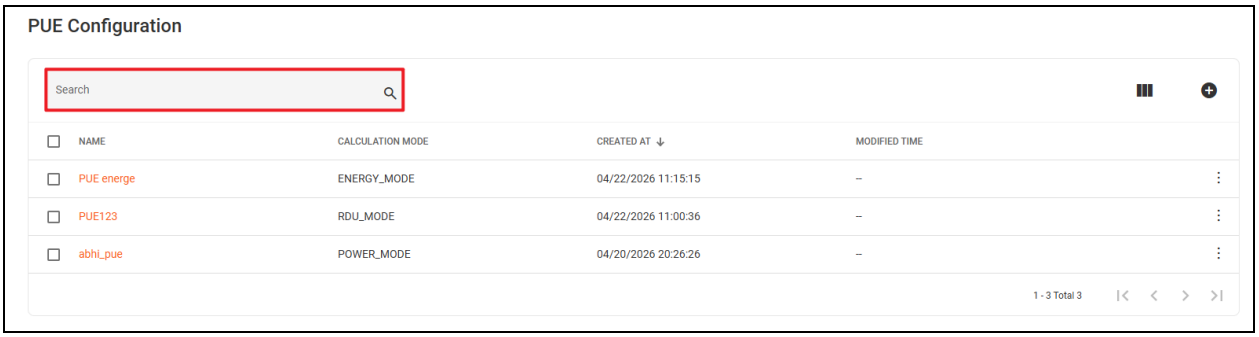


If Energy Mode is selected, you can optionally enter IT Device Energy Adjustment, Infrastructure Device Energy Adjustment and Total Device Energy Adjustment.

Searching PUE Configuration

Enter a keyword in the search box to search for a PUE Configuration by name, as shown in **Figure 12.10** below .

Figure 12.10 Searching for the PUE configuration



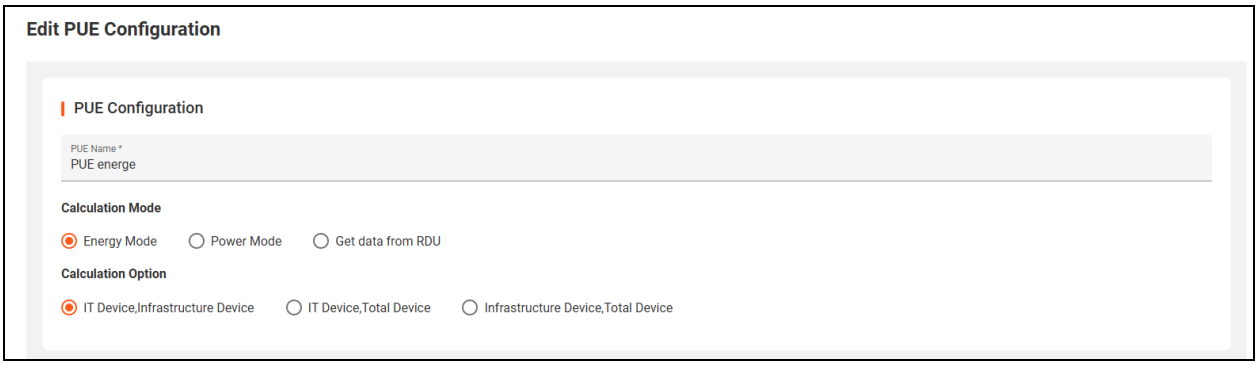
Editing the PUE Configuration

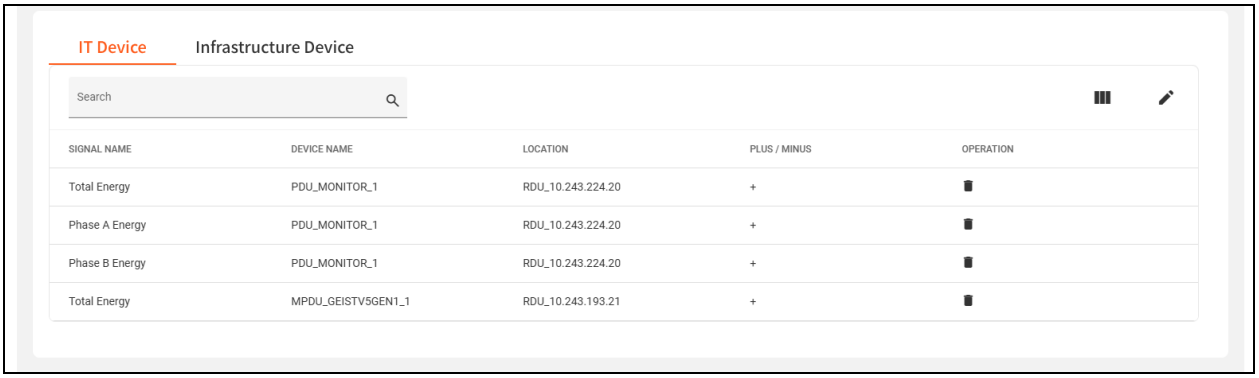
Click on the ellipses (⋮) in the PUE Configuration List, then click the *edit* icon to go to the Edit PUE Configuration page.

1. In Energy Mode and Power Mode, you can change the Calculation Mode, Calculation Option, and the signals used for PUE calculation.
2. In Get Data from RDU mode, you can change the Calculation Mode only.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 12.11 Editing the PUE Configuration

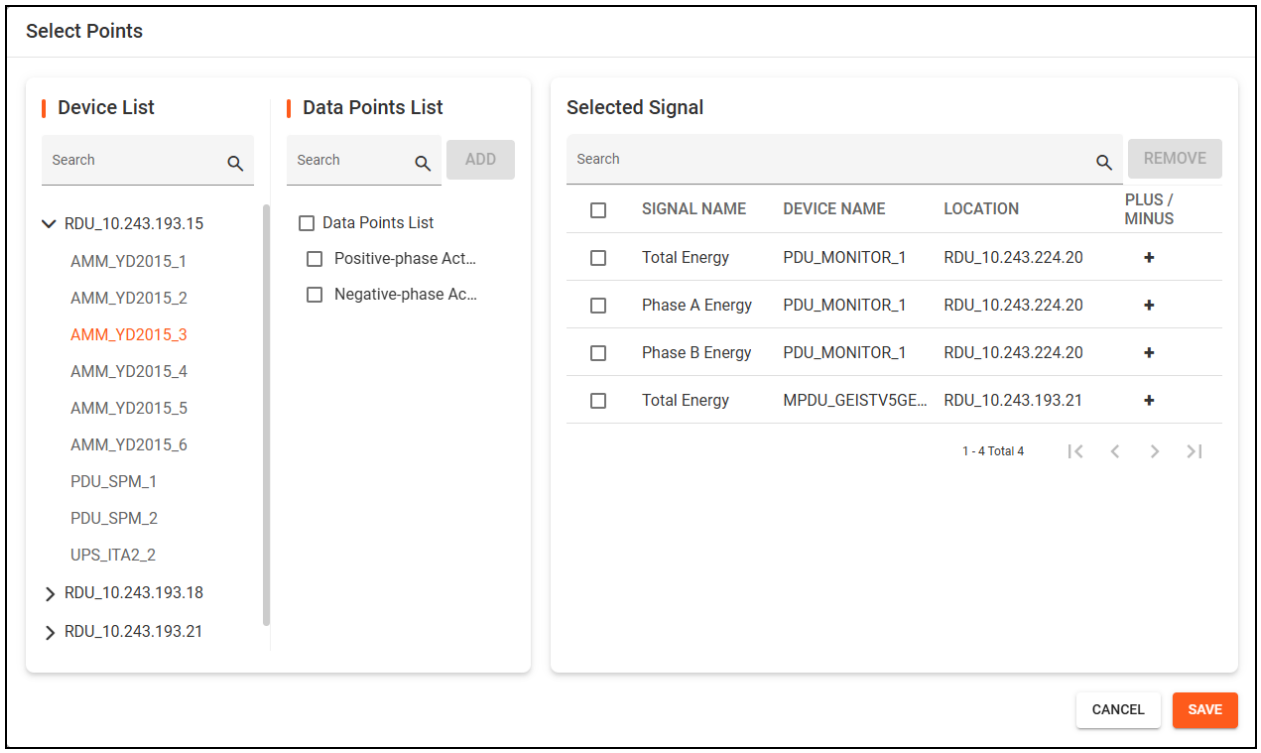




Click on the *edit* icon on the upper right corner of the IT Device / Infrastructure Device / All Devices to go to the signal Configuration page for the corresponding device type, and select the signals that make up the corresponding device, as shown in **Figure 12.12** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

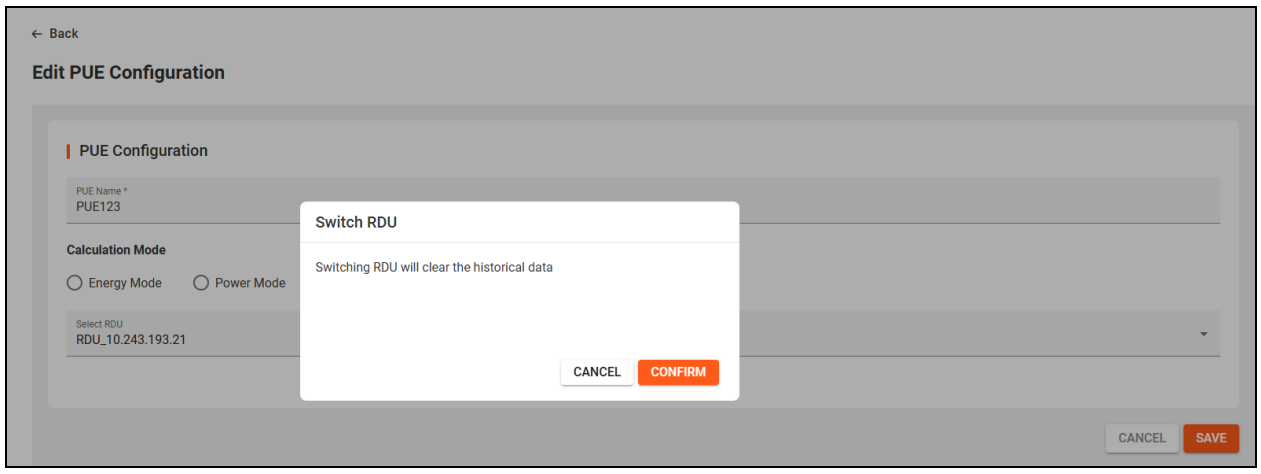
Figure 12.12 Configuring the Device Signals



Depending on the Calculation Option selected, you must select the signals that make up the IT devices, infrastructure devices, and all devices before the PUE value can be calculated.

If you are editing a configuration in Get Data from RDU mode and switch to a different RDU, the platform displays a Switch RDU dialog. As shown in **Figure 12.13** below .

Figure 12.13 Switch RDU



© 2026 Vertiv Group Corp. All Rights Reserved.

Deleting the PUE Configuration

1. Deleting PUE configurations in bulk:

Select the *checkboxes* of the PUE configuration list to delete the list, then click the *Delete* icon, as shown in **Figure 12.14** below .

Figure 12.14 Batch Delete PUE Configurations

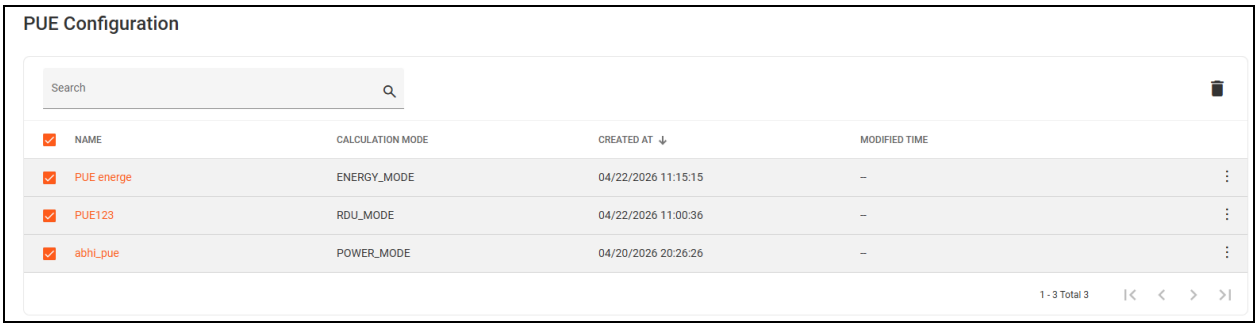
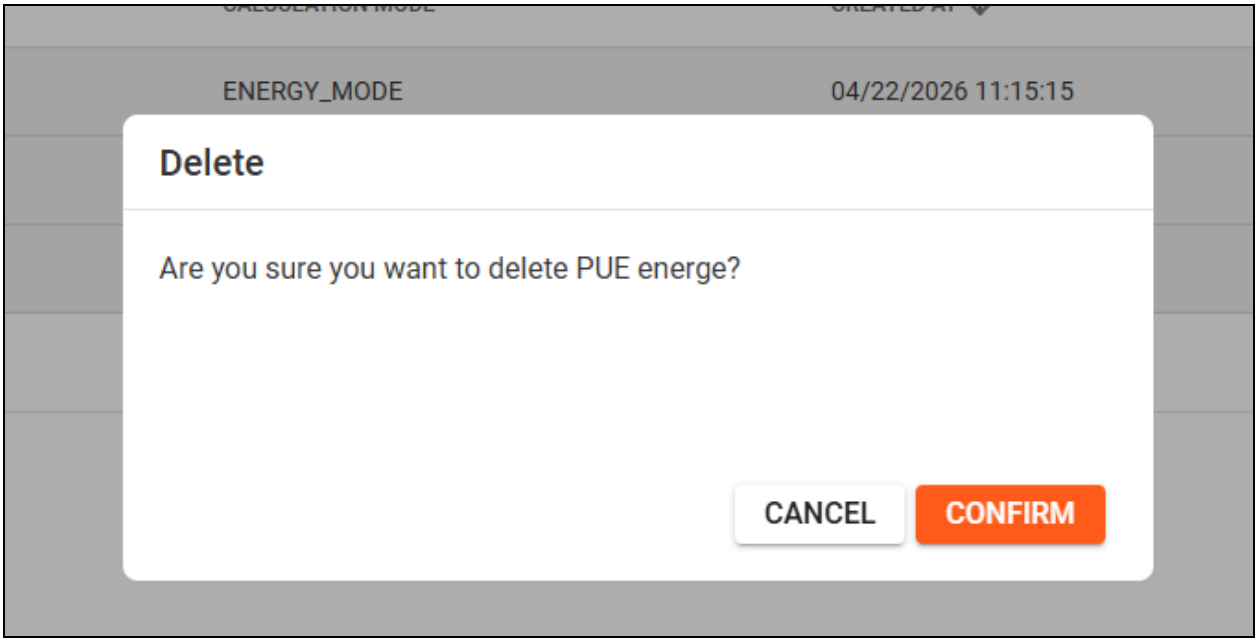


Figure 12.15 Deleting the PUE Configurations

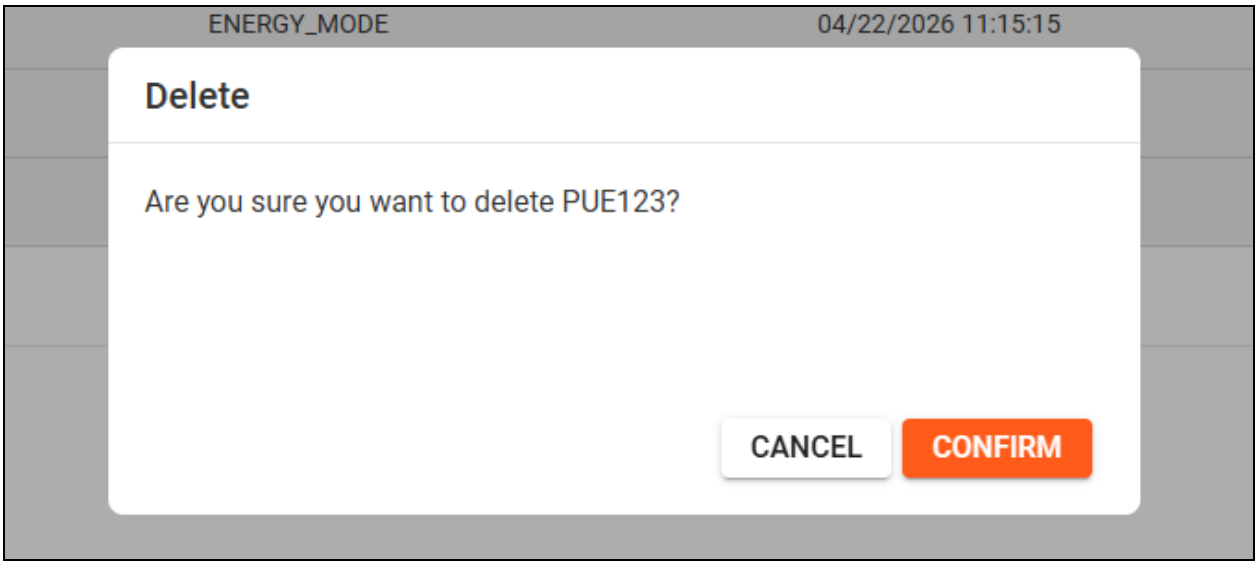


2. Deleting a single PUE configuration:

Click on the ellipses (⋮) in the PUE Configuration List, then click on the *delete* icon to delete the PUE configuration. As shown in **Figure 12.16** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 12.16 Deleting a single PUE configuration



© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

13 Configuration Tool

13.1 General

13.1.1 Overview

The Configuration Tool serves as the core entry point for O&M administrators to centrally manage basic O&M tasks, including device onboarding, communication parameters, data collection templates, and firmware upgrades. After entering the Configuration Tool, the left navigation bar contains the following four functional modules.

13.1.2 Functional Modules

- Device Management: Centrally manages SNMP and RDU devices connected to the platform. You can view the online status, IP address, device type, model, data collection template, and site information. This module also provides capabilities for adding, deleting, filtering, and performing bulk operations on devices.
- Communication Configuration: Configures communication parameters between the platform and devices, including SNMP protocol versions, community strings, ports, and other connection parameters to ensure the platform can successfully communicate with target devices.
- Data Collection Template Management: Manages built-in and custom data collection templates. A data collection template defines which data points the platform retrieves from a device and the associated collection rules. Devices must be associated with a corresponding template during onboarding.
- Firmware Management: Manages firmware versions and performs upgrade operations for devices that support remote upgrades to ensure device firmware remains under control.

13.2 Detailed Features

13.2.1 Device Management

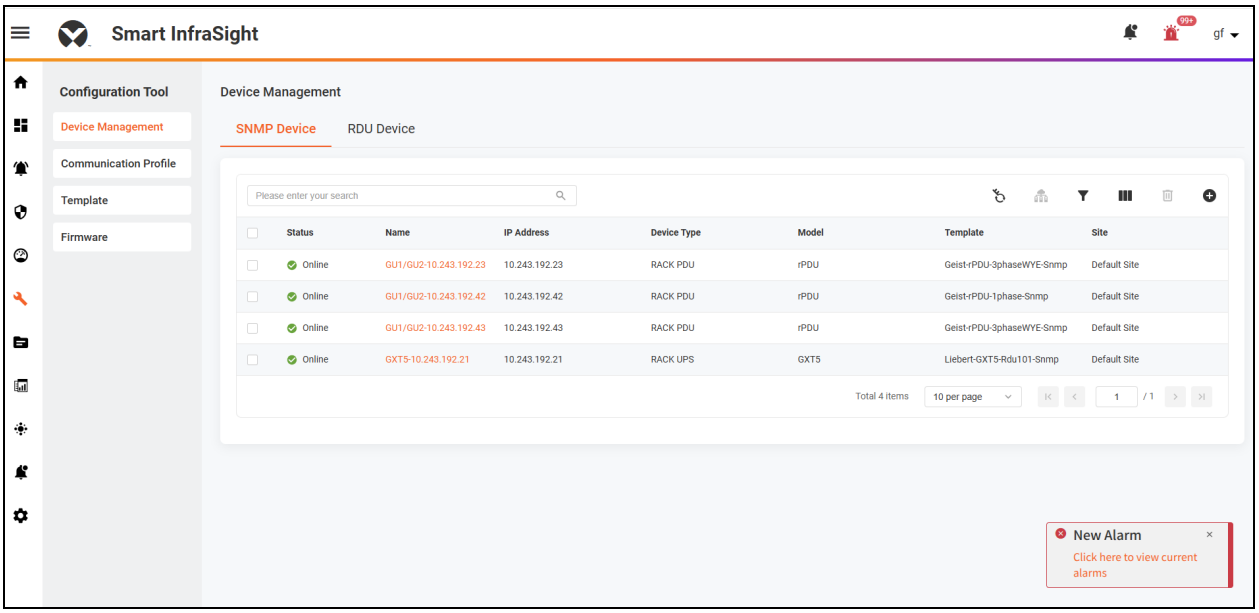
SNMP Device

Adding SNMP Device

Navigate to the SNMP Device List, as shown in Figure 13.1 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

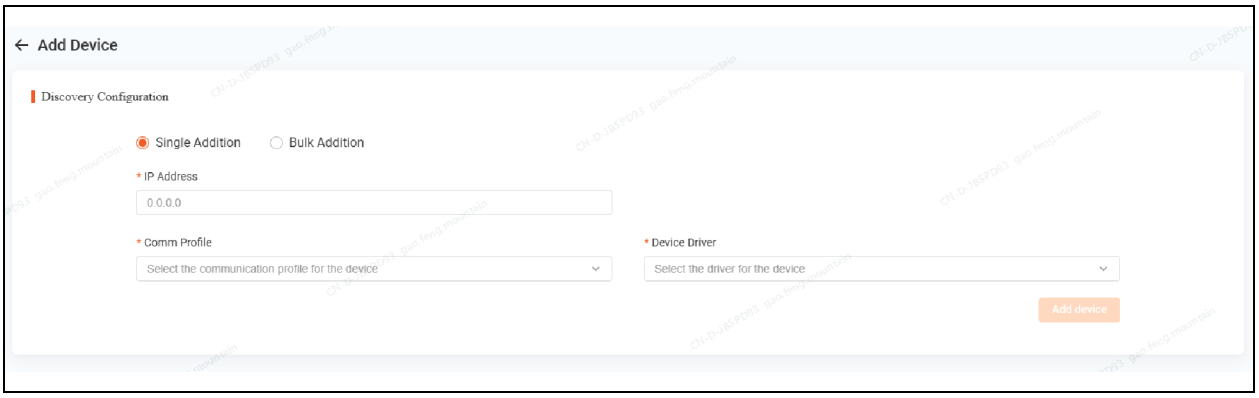
Figure 13.1 SNMP Device List



Before adding a device, you must first configure a communication configuration and a collection template. For details, refer to the Detailed Features) and Template on page 284.

Click the (+) icon 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 13.2** below .

Figure 13.2 Add Device – Single Addition



Single Addition

- Enter the IP address. The IP address must not duplicate an existing one.
- Select a communication configuration.
- Select a device driver.

Click *Add Device* to complete the addition. Upon success, the platform returns to the SNMP Device List.

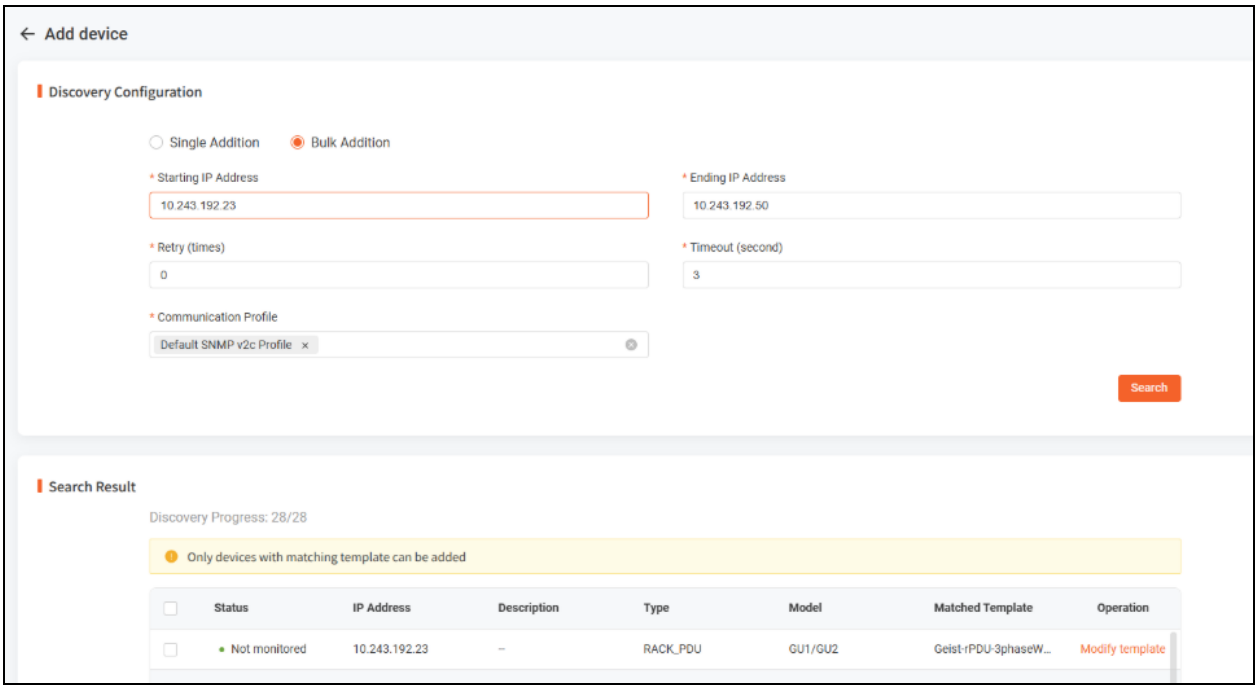
© 2026 Vertiv Group Corp. All Rights Reserved.

Batch Addition

- Enter the start IPv4 address and end IPv4 address. The start IP must be less than the end IP.
- Enter the number of retries. The default value is 0.
- Enter the timeout duration. The default value is 3 seconds.
- Select a communication configuration. If the Use as default for device discovery checkbox was selected when adding or editing a communication configuration Detailed Features the platform automatically pre-selects that communication configuration's protocol during discovery.

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 13.3** below .

Figure 13.3 Add Device – Bulk Addition



The search results are shown in as shown in **Figure 13.3** above . After the search completes, each discovered device is assigned one of the following statuses:

- **Not Respond / Already Monitored** — The entry is disabled and no operations can be performed.
- **Missing Driver** — Click *Select Driver* in the Actions column. The status changes to Not Monitored, after which the device can be selected and added to monitoring.
- **Not Monitored** — The device can be directly selected and added to monitoring. Alternatively, click *Change Driver* in the Actions column to change the assigned driver..

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.4 Device Search Result

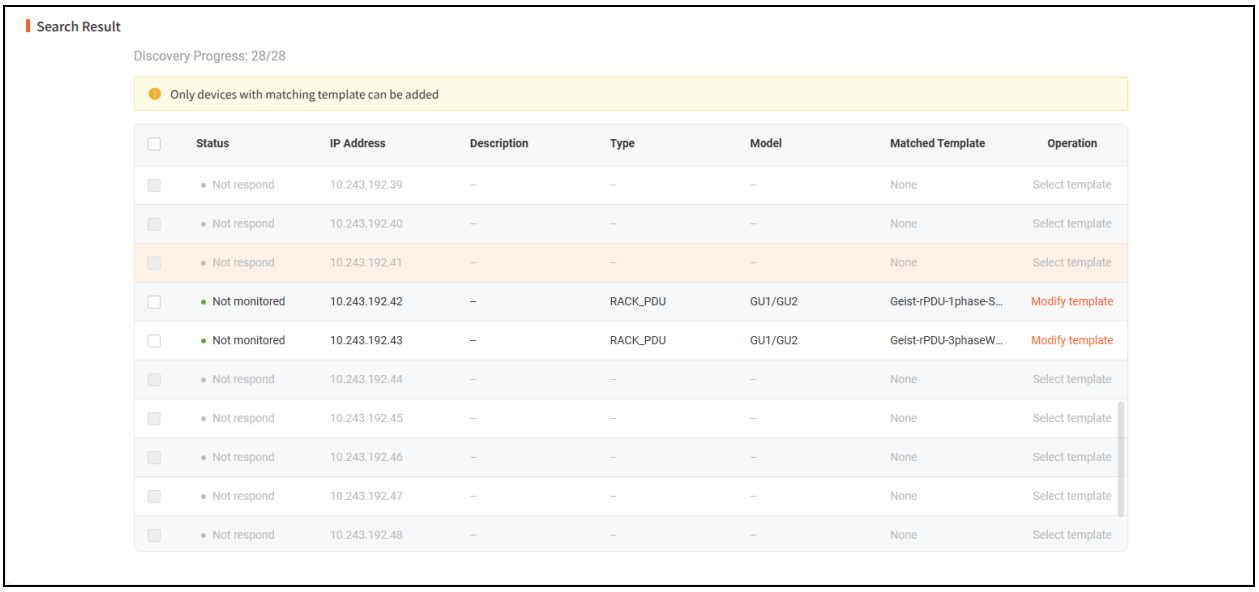
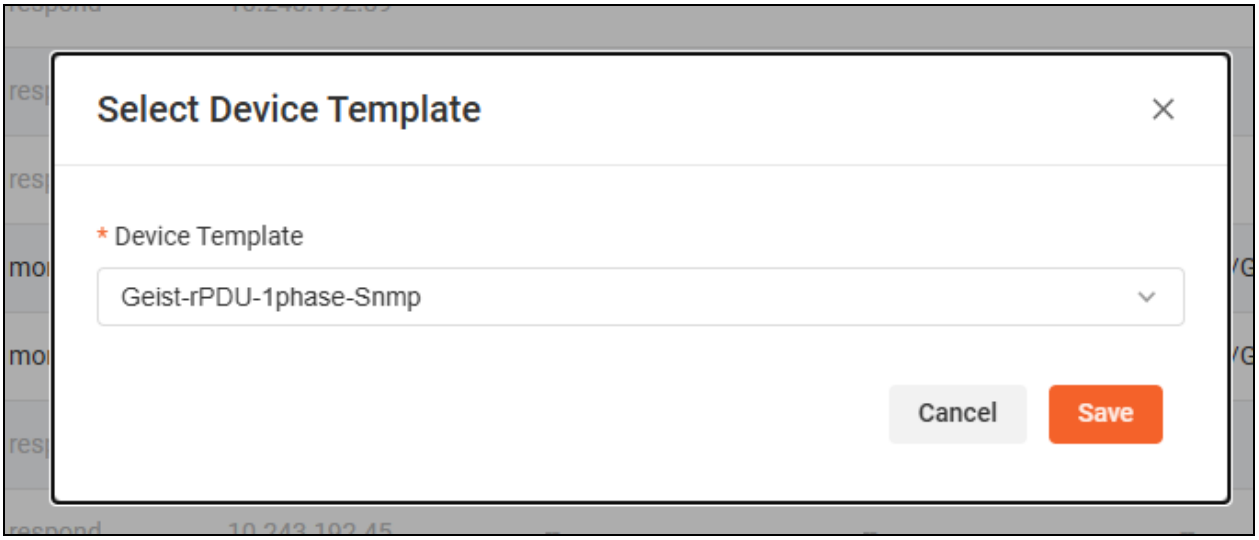


Figure 13.5 Selecting the Device Driver

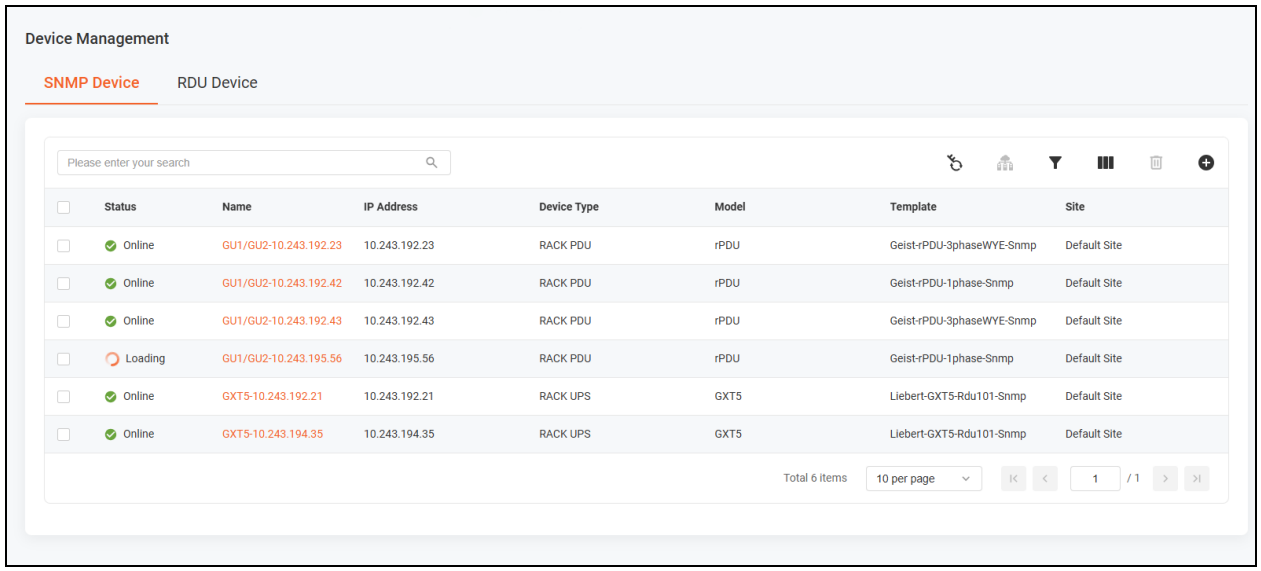


After the search completes, select one or more devices with a **Not Monitored** status using the checkboxes, then click *Add Device* to add them. Upon success, the platform redirects to the SNMP Device List page, as shown in **Figure 13.6** on the facing page .

Newly added devices display a status of **Communicating**, and are assigned to **Default Site** by default **Figure 13.7** on the facing page . The device status updates only after refreshing the page or navigating away and returning.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.6 Newly Added SNMP Devices

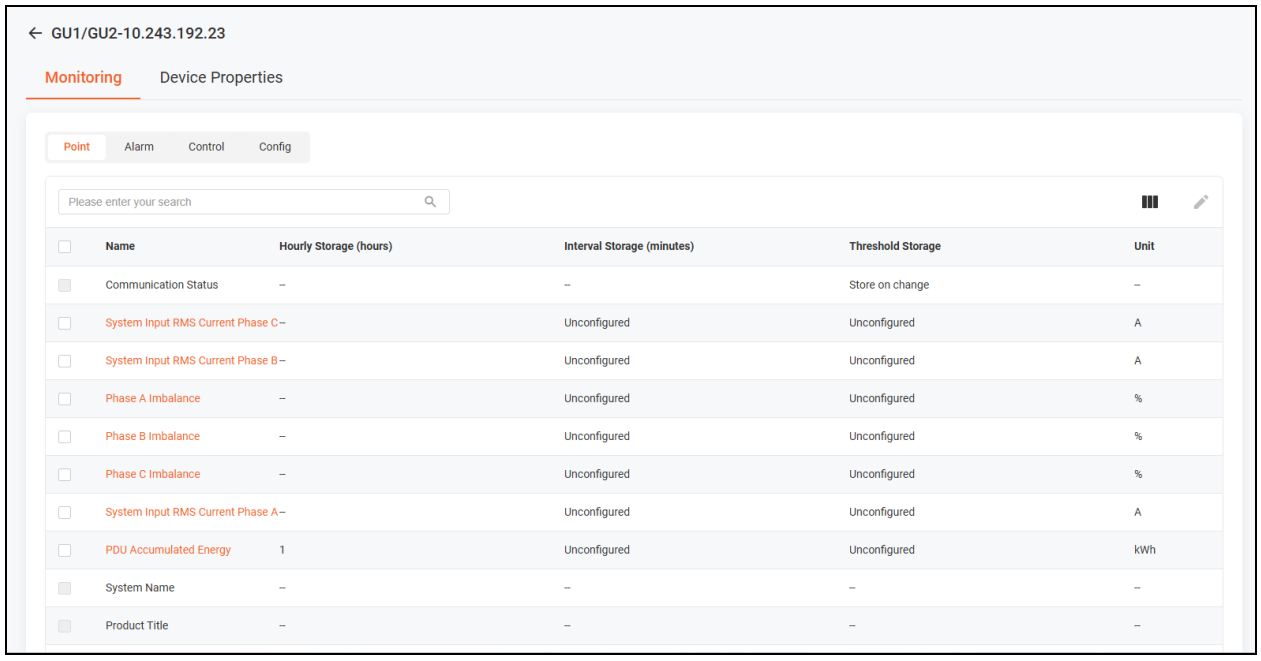


SNMP Device Configuration

Click an *SNMP device name* to go to the device configuration page, see **Figure 13.7** below .

- The **Monitoring** tab is used to modify device configuration.
- The **Device Properties** tab displays the device's basic information and communication configuration.

Figure 13.7 SNMP Device Configuration

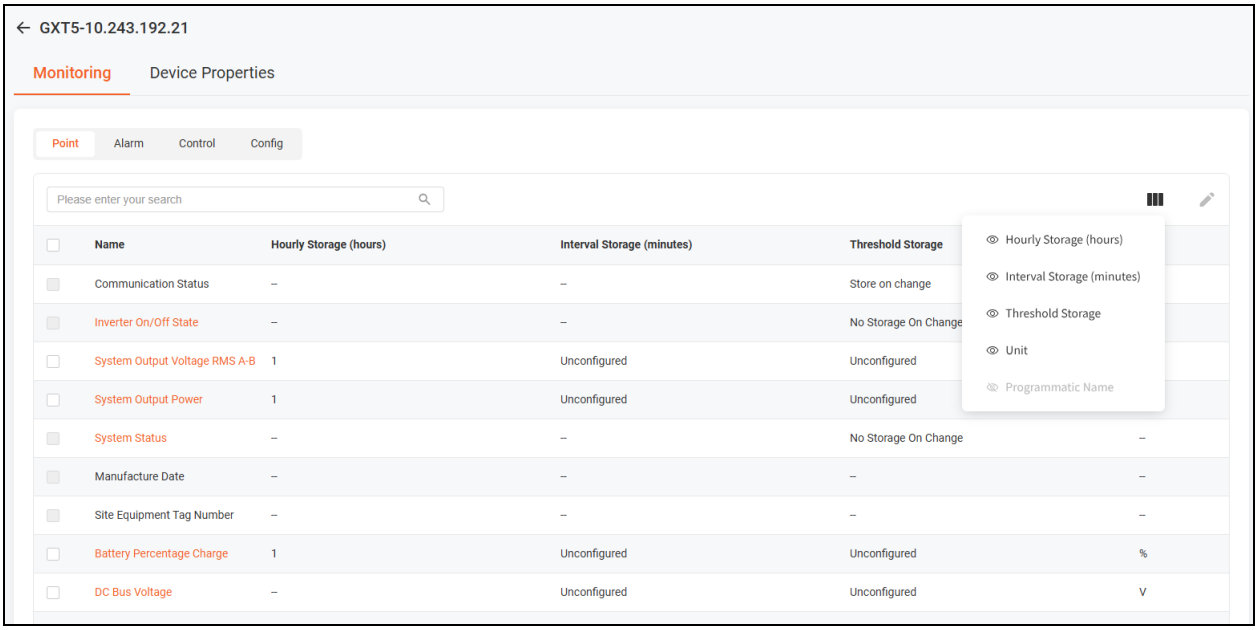


© 2026 Vertiv Group Corp. All Rights Reserved.

Point

Click the *column visibility* icon to expand the drop-down list and control which table columns are displayed, as shown in Figure 13.8 below . Grayed-out items in the drop-down list indicate columns that are currently hidden.

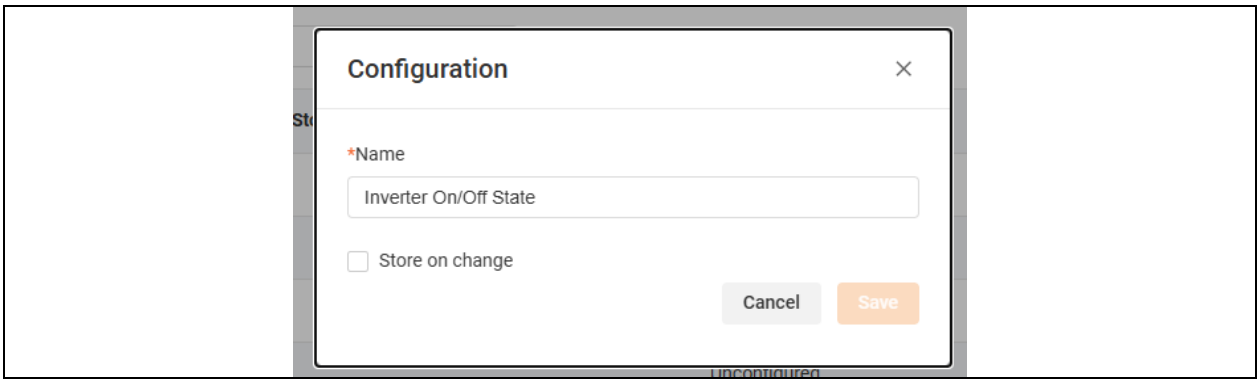
Figure 13.8 Configure Column Visibility for Monitoring



Data Point Types:

- Digital Data Points — Click *Edit* to open the edit dialog box. (see Figure 13.9 below)
    - Store on Change (checked): Stores data whenever a change occurs.
    - Store on Change (unchecked): Does not store data when a change occurs.

Figure 13.9 Editing the Digital Data Point Configuration

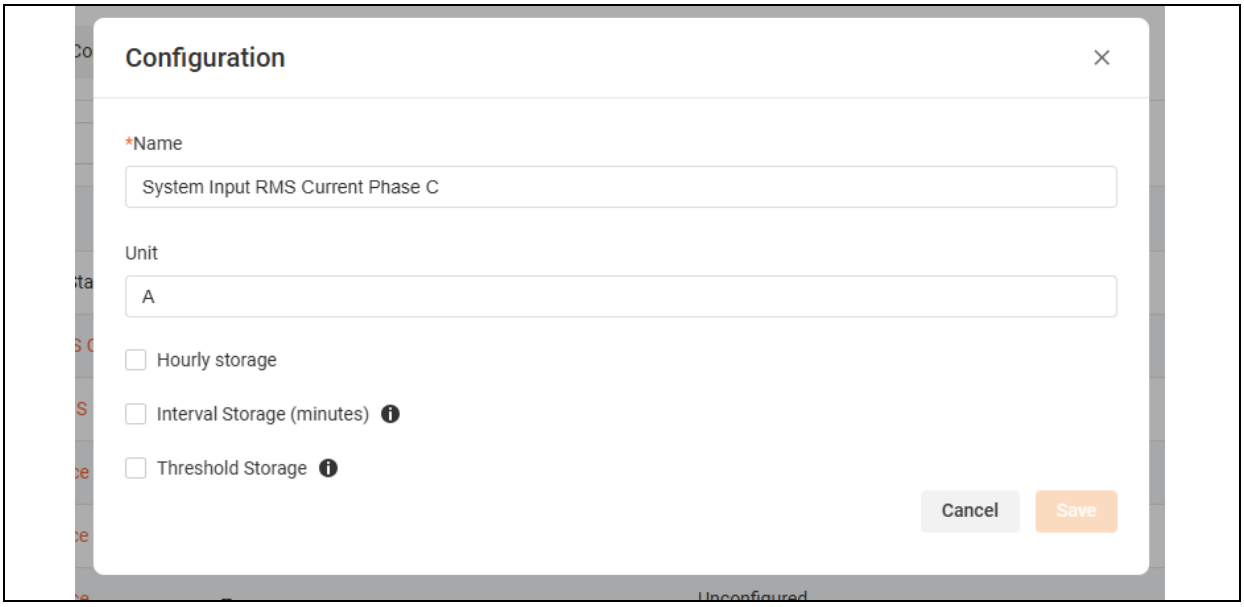


- Analog Data Points: Click the entry in the Name column to open the edit dialog box , see Figure 13.10 on the facing page .
- Hourly Storage: When enabled, data is stored at 1-hour intervals by default.

© 2026 Vertiv Group Corp. All Rights Reserved.

- **Interval Storage:** Disabled by default. When enabled, the default interval is 3 minutes. Available intervals are 10 minutes and 30 minutes. Data is stored at the selected interval.
- **Threshold Storage:** Disabled by default. When enabled, the default threshold value is 10. The signal value is stored when its change exceeds the configured threshold.

Figure 13.10 Editing the Analog Data Point Configuration



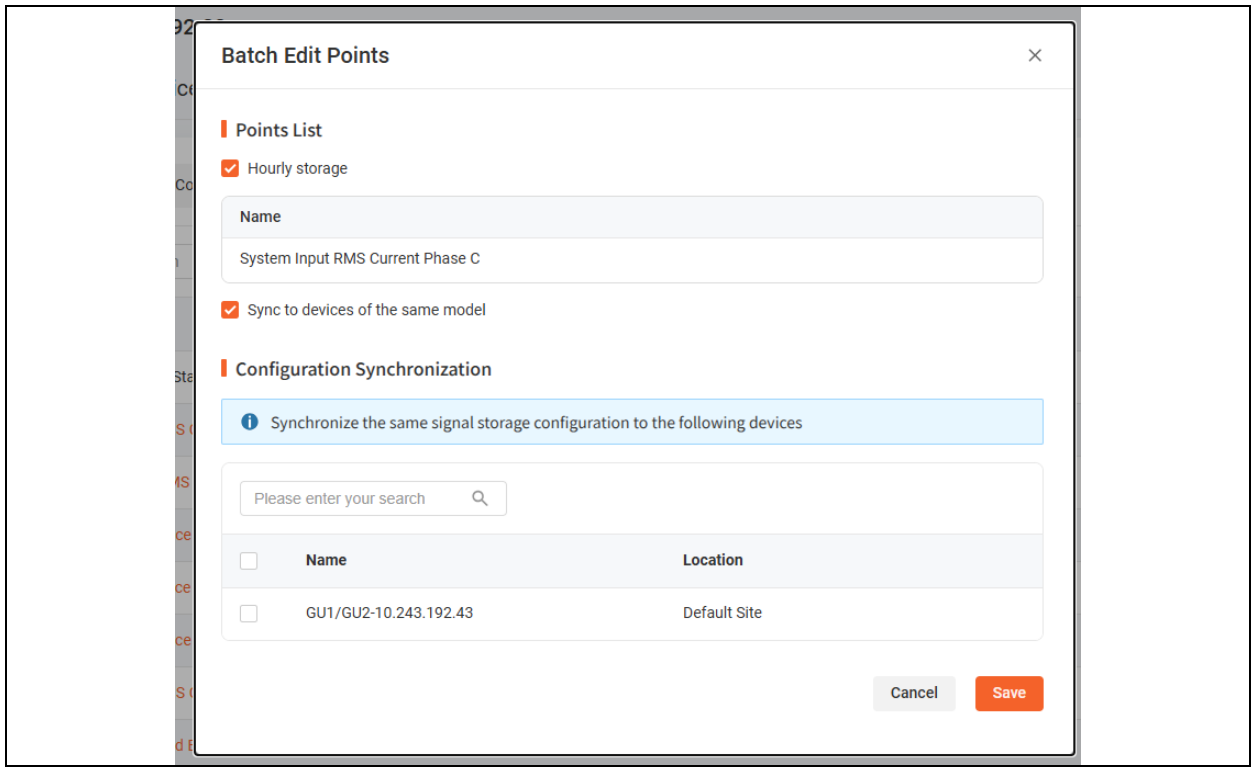
- **Read-only Data Points** — Non-editable data points, such as communication status.

Sync Configuration

Click the *Batch Edit* icon in the upper-right corner of the table to open the dialog box. This allows you to batch-sync the selected data point configurations to other devices of the same model (see **Figure 13.11** on the next page).

© 2026 Vertiv Group Corp. All Rights Reserved.

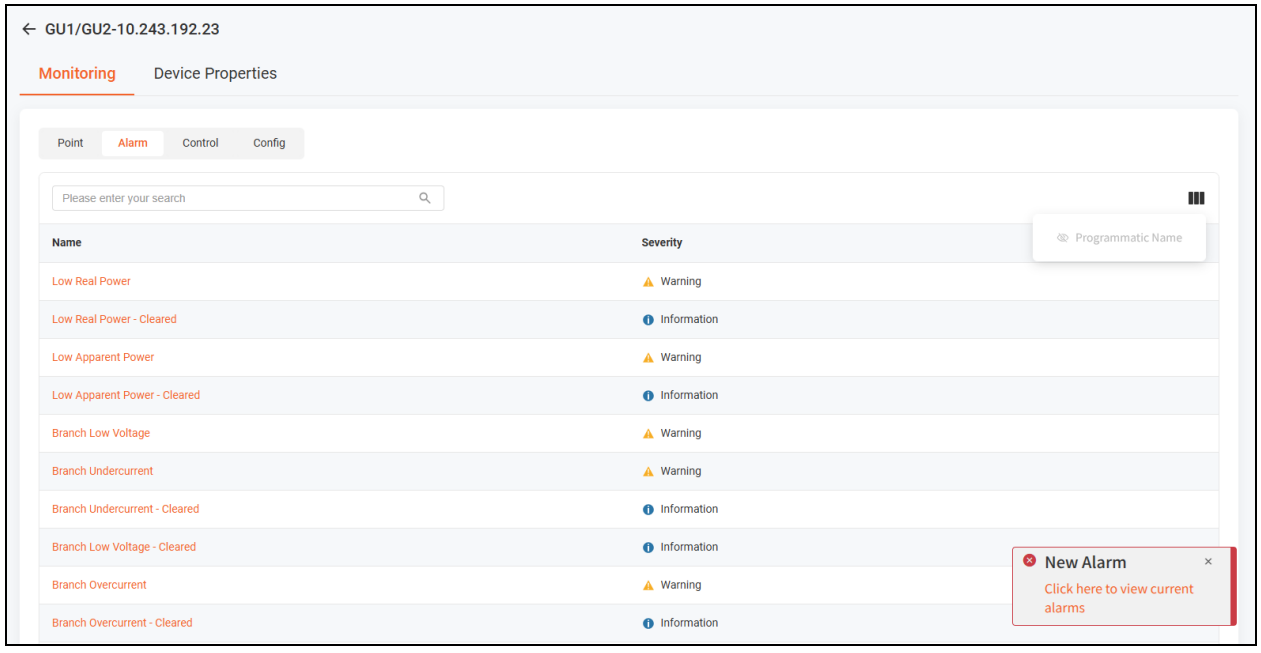
Figure 13.11 Batch Edit Data Points / Sync Configuration



Alarm

Click the *column visibility* icon to expand the drop-down list and control which table columns are displayed. Grayed-out items in the drop-down list indicate columns that are currently hidden (see **Figure 13.12** below).

Figure 13.12 Device Alarm List



© 2026 Vertiv Group Corp. All Rights Reserved.

Click an *entry* in the **Name** column to open the edit dialog box (see **Figure 13.13** below).

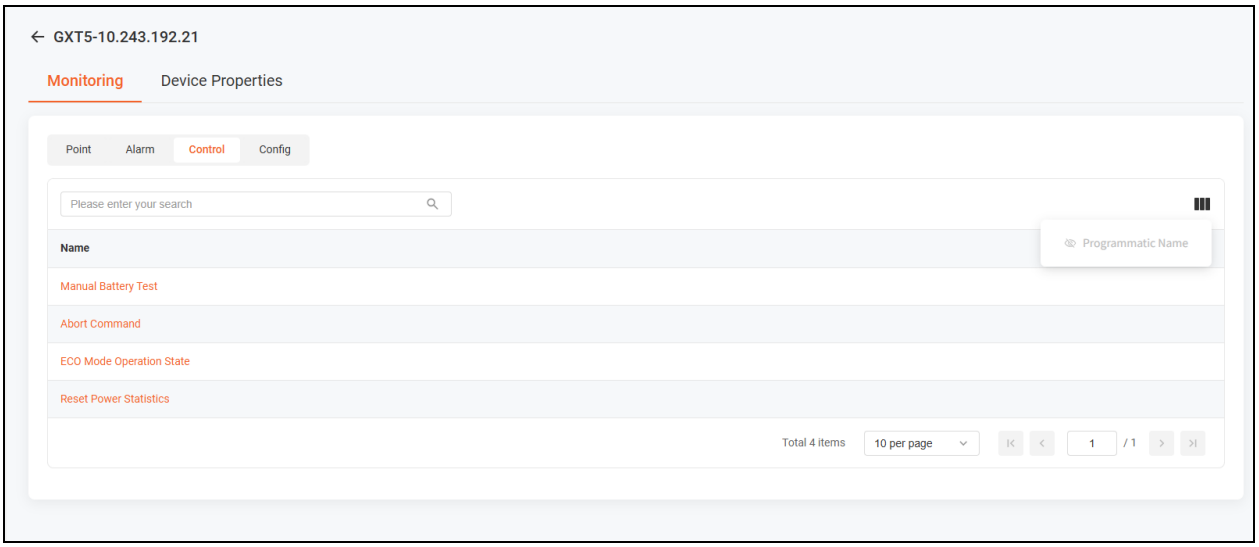
Figure 13.13 Editing an Alarm



Control

The **Control** tab primarily displays digital signal data points. Click the *column visibility* icon to expand the drop-down list and control which table columns are displayed. Grayed-out items in the drop-down list indicate columns that are currently hidden (see **Figure 13.14** below).

Figure 13.14 Control Tab



Click an *entry* in the **Name** column to open the edit dialog box and modify the control name (see **Figure 13.15** on the next page).

© 2026 Vertiv Group Corp. All Rights Reserved.

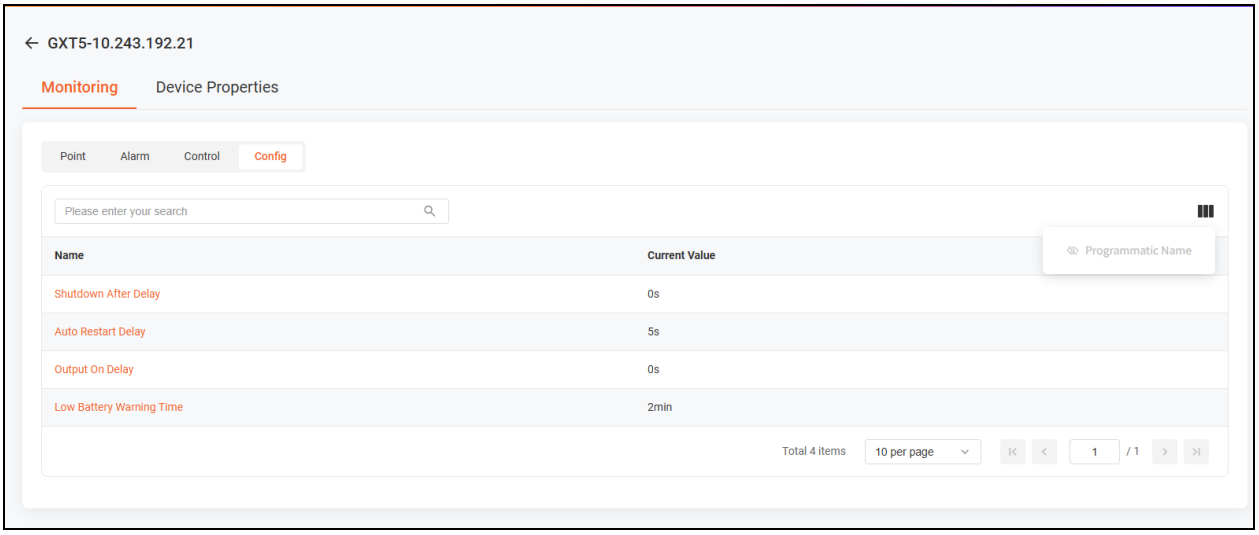
Figure 13.15 Editing the Control Configuration



Config

The **Config** tab primarily displays analog signal data points and is used to configure and send commands. Click the *column visibility* icon to expand the drop-down list and control which table columns are displayed. Grayed-out items in the drop-down list indicate columns that are currently hidden (see **Figure 13.16** below).

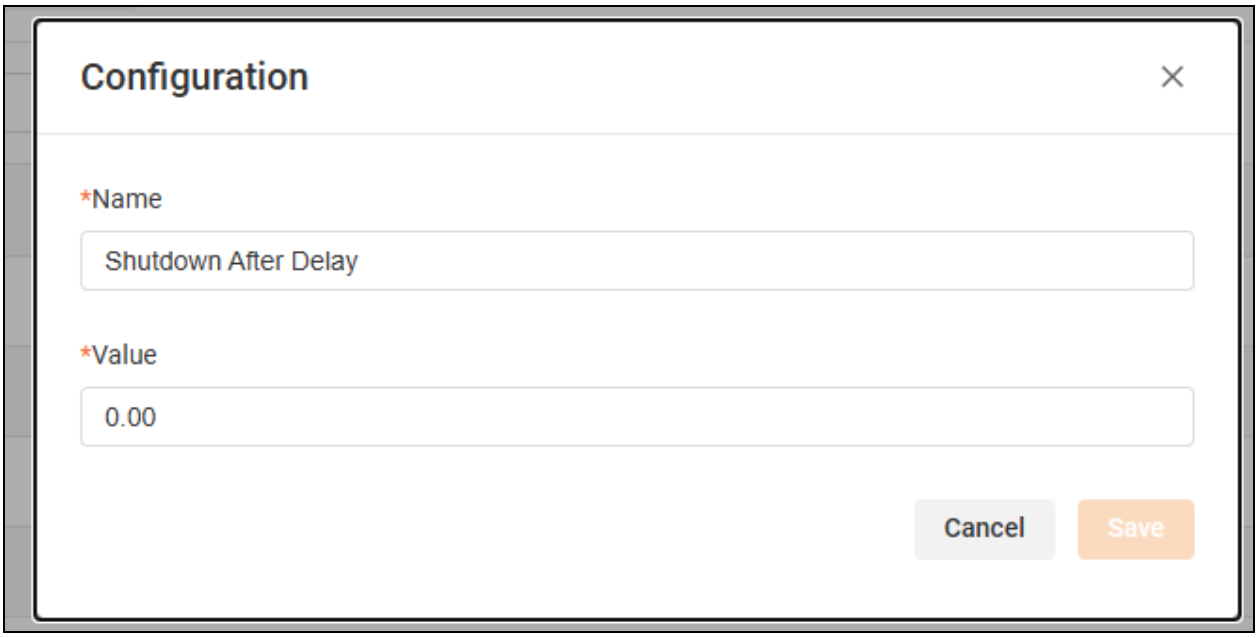
Figure 13.16 Config Tab



Click an *entry* in the **Name** column to open the edit dialog box (see **Figure 13.17** on the facing page).

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.17 Editing the Config Signal Configuration



Device Properties

The Device Properties page contains the following sections: Basic Information, Communication Configuration, Communication Card Access Settings, and Hardware & Firmware Information.

Communication Configuration:

After modifying and saving the communication configuration, the device reconnects using the new protocol.

Communication Card Access Settings:

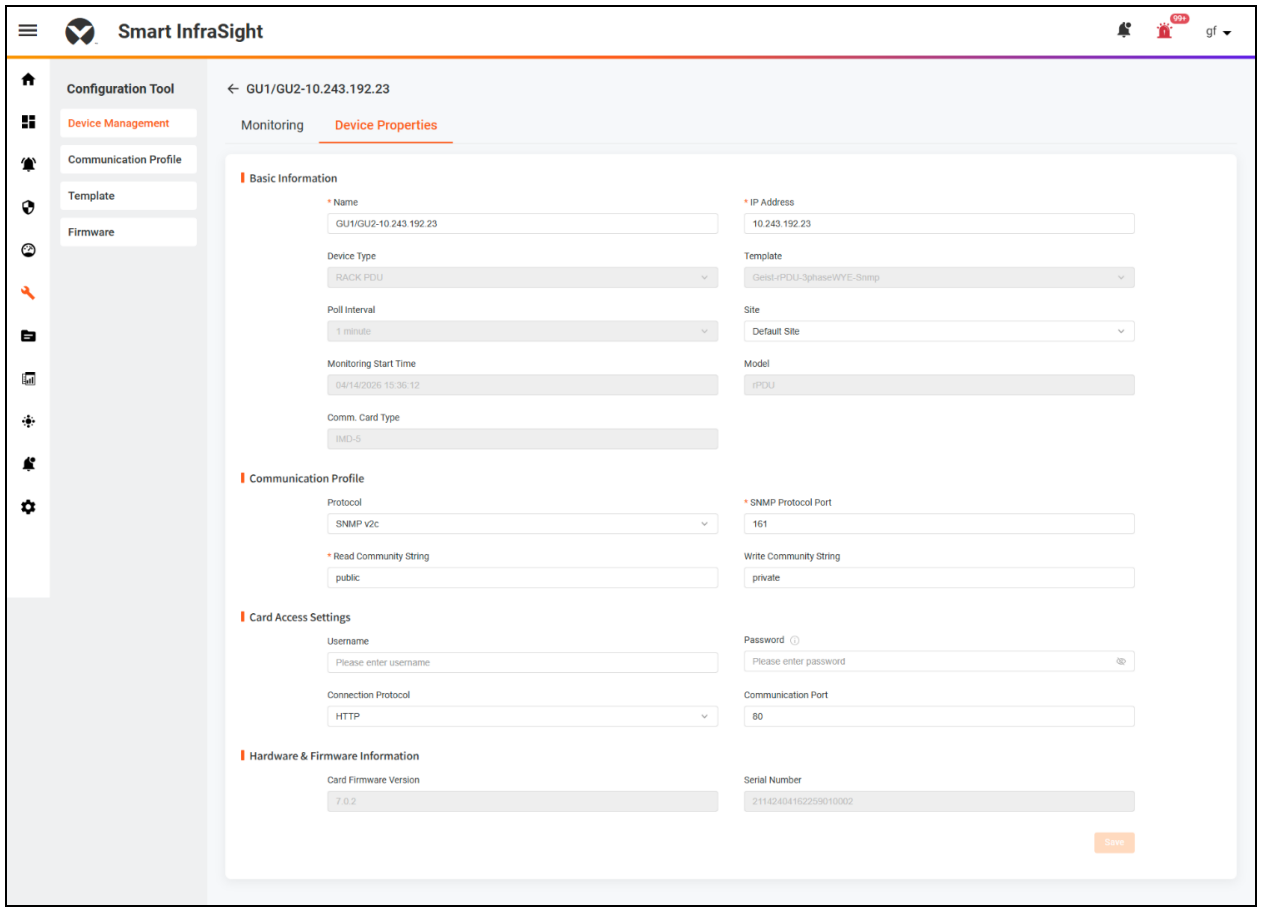
This section is displayed only when the device has a communication card. It is primarily used for firmware upgrades of the device or the communication card.

Hardware & Firmware Information:

The firmware version of the device or communication card, and the device serial number. This information serves as a reference when upgrading the firmware of the device or communication card. As shown in **Figure 13.18** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.18 Device Properties Configuration



Firmware Upgrade

Fleet Management Overview

Fleet Management is used for **batch management** of Vertiv devices and communication cards. It allows users to perform operations such as firmware upgrades on multiple devices or cards simultaneously, avoiding the inefficiency and version inconsistency caused by handling devices one at a time.

1. Use Cases

a. Data centers or equipment rooms with a large number of similar Vertiv devices that require unified firmware versions.

b. Centralized upgrade or configuration of multiple communication cards.

c. Reducing manual one-by-one operations to improve maintenance efficiency and minimize human error.

2. Key Features

a. Batch firmware upgrade: Upgrade firmware on multiple devices or communication cards at once.

b. Centralized management: Manage device groups through a unified entry, reducing repetitive logins and configurations.

c. Task tracking: View the execution progress and results of batch tasks.

© 2026 Vertiv Group Corp. All Rights Reserved.

3. Supported Devices and Communication Cards

Fleet Management is applicable only to Vertiv devices equipped with the following communication / monitoring cards:

a. Vertiv devices with **UNITY** , **RDU101** or **RDU120** communication cards, for example: GXT5 SU, Petc.

b. Vertiv GEIST rPDUs with **IMD-3** or **IMD-5** monitoring cards.

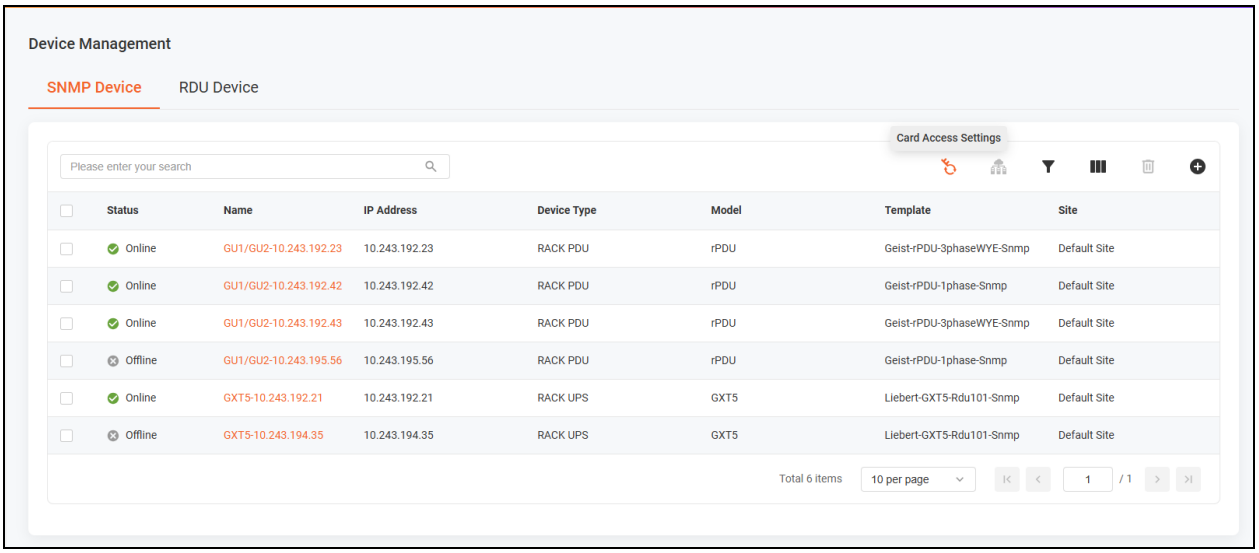
NOTE: Refer to the latest compatibility list for the specific supported device models.

Fleet Management Upgrade Steps:

1. Refer to Section Firmware on page 308 to add device firmware. Ensure the correct model is selected when adding firmware.
2. Configure the correct communication information for the device or communication card to be upgraded.

Method 1: Go to the SNMP Device List, select devices in bulk or click the *Card Access Settings* icon in the upper-right corner of the table directly (see **Figure 13.19** below).

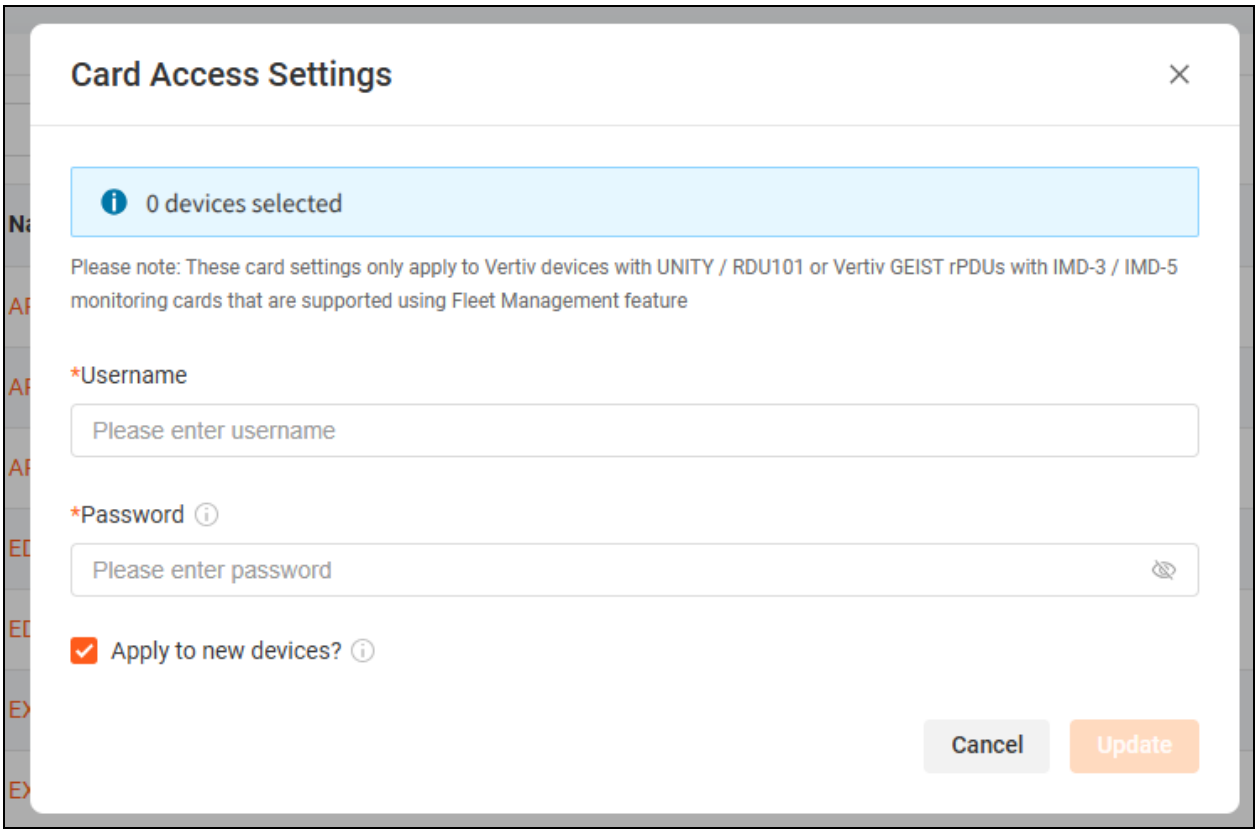
Figure 13.19 Card Access Settings Window



Click to open the dialog box (see **Figure 13.20** on the next page).

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.20 Card Access Settings

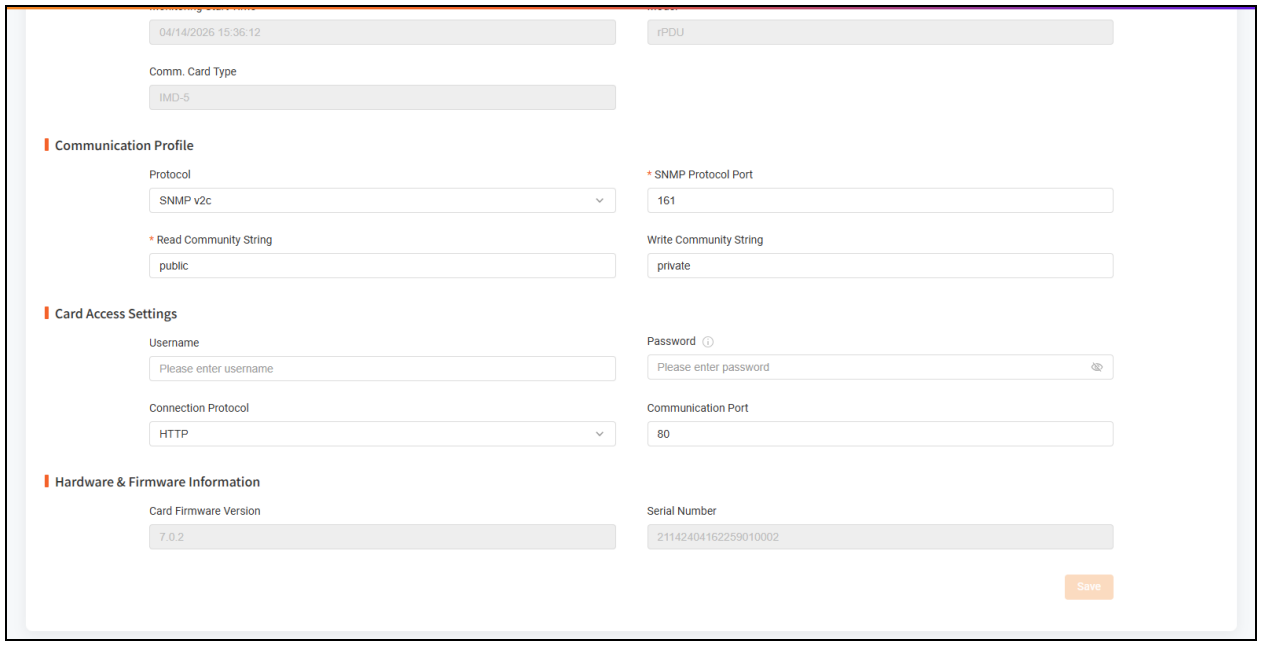


Select **Apply to new devices** to use the configured username and password as the default credentials for all subsequently added devices.

Method 2: Go to a device's details page, open the Device Properties tab, locate the **Card Access Settings** section, and set the username and password (see **Figure 13.21** on the facing page).

© 2026 Vertiv Group Corp. All Rights Reserved.

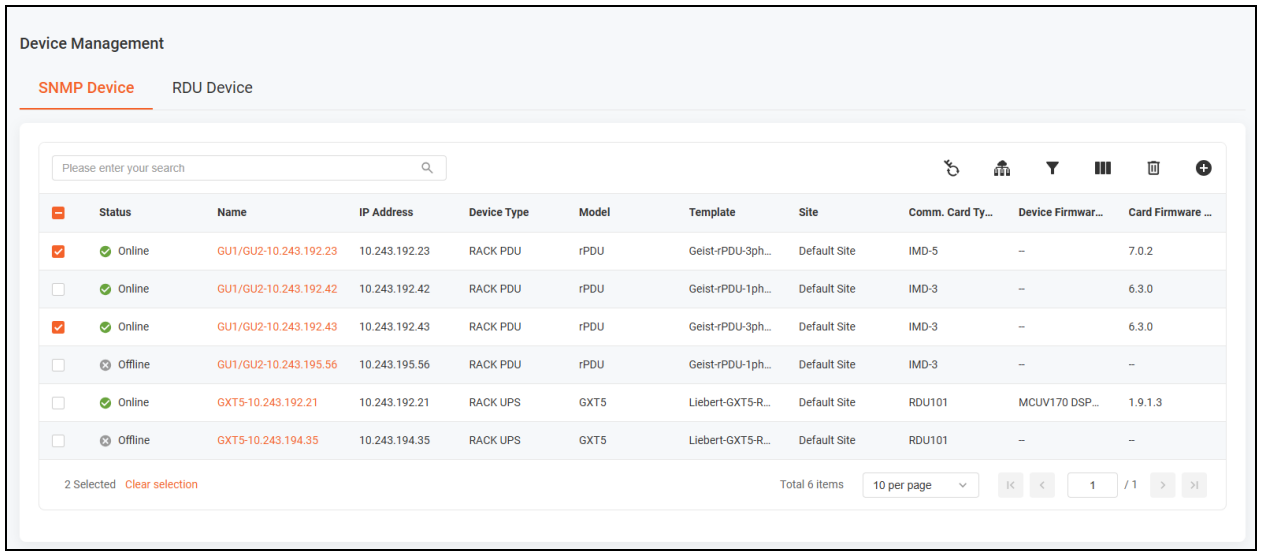
Figure 13.21 Card Access Settings in Device Properties



As shown in the **Figure 13.21** above , configure the correct communication protocol and communication card port in the **Card Access Settings** section.

3. Select the devices to be upgraded. All selected devices must be online. Click the *Fleet Management* icon in the upper-right corner of the device list table (see **Figure 13.22** below).

Figure 13.22 Fleet Management Window

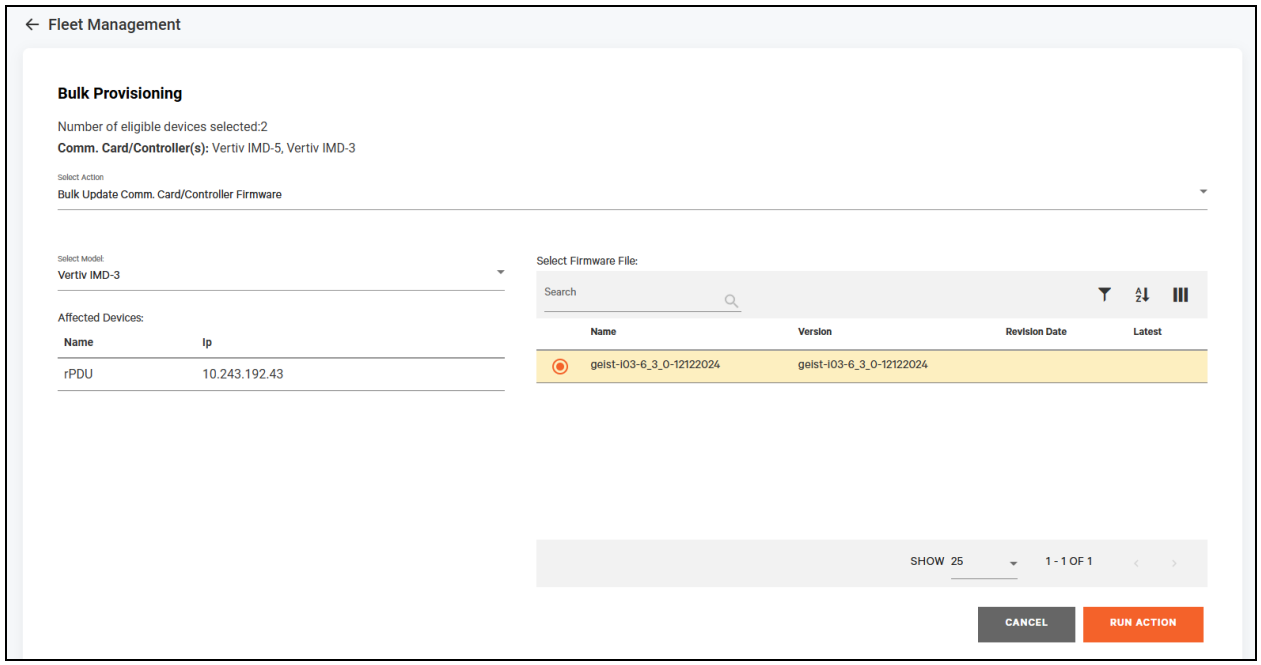


4. Go to the Firmware Upgrade page (see **Figure 13.23** on the next page). Configure the following options:

- **Select Operation:** Choose Batch Update Communication Card or Batch Update Device Firmware.
- **Select Model:** Select the correct model to filter the available firmware files for that model.

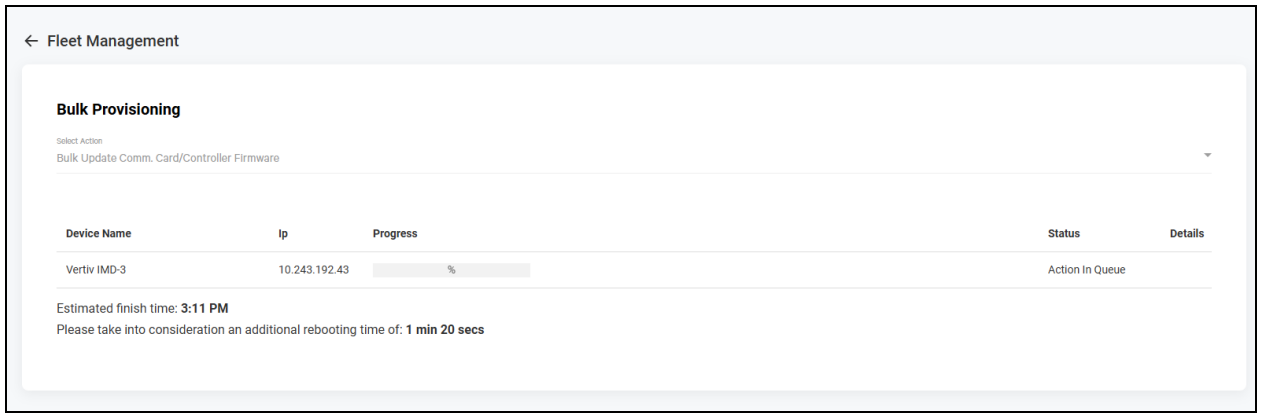
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.23 Batch Firmware Upgrade Configuration



5. Execute the operation. A confirmation dialog box appears asking whether to proceed. After confirming, the platform navigates to the upgrade progress page (see **Figure 13.24** below).

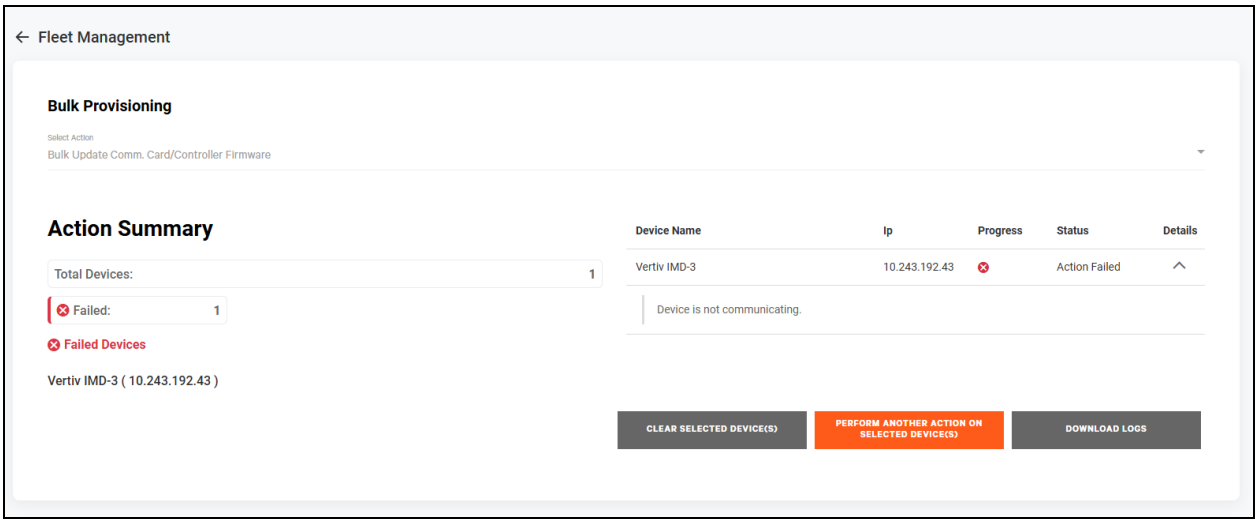
Figure 13.24 Batch Firmware Upgrade Progress



Upgrade failed (see **Figure 13.25** on the facing page).

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.25 Batch Firmware Upgrade Failed

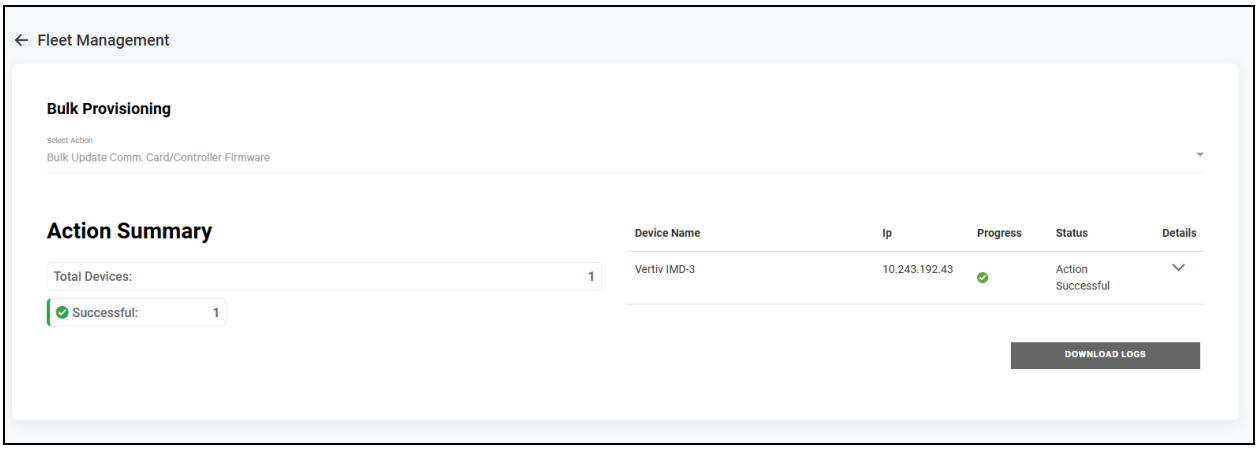


Clear Selected Devices: Clears all devices selected for the current upgrade operation.

Perform Another Operation on Selected Devices: Continues to perform another operation on the devices selected in the current operation.

Upgrade successful (see Figure 13.26 below)

Figure 13.26 Batch Firmware Upgrade Successful



NOTE:

Only one firmware upgrade operation can be performed across the entire platform at a time.

An IP address change on the SI server will cause the firmware upgrade feature to become unavailable. Please refer to section 19.16 SI IP Change Causes Firmware Upgrade Unavailability for resolution.

© 2026 Vertiv Group Corp. All Rights Reserved.

RDU Device

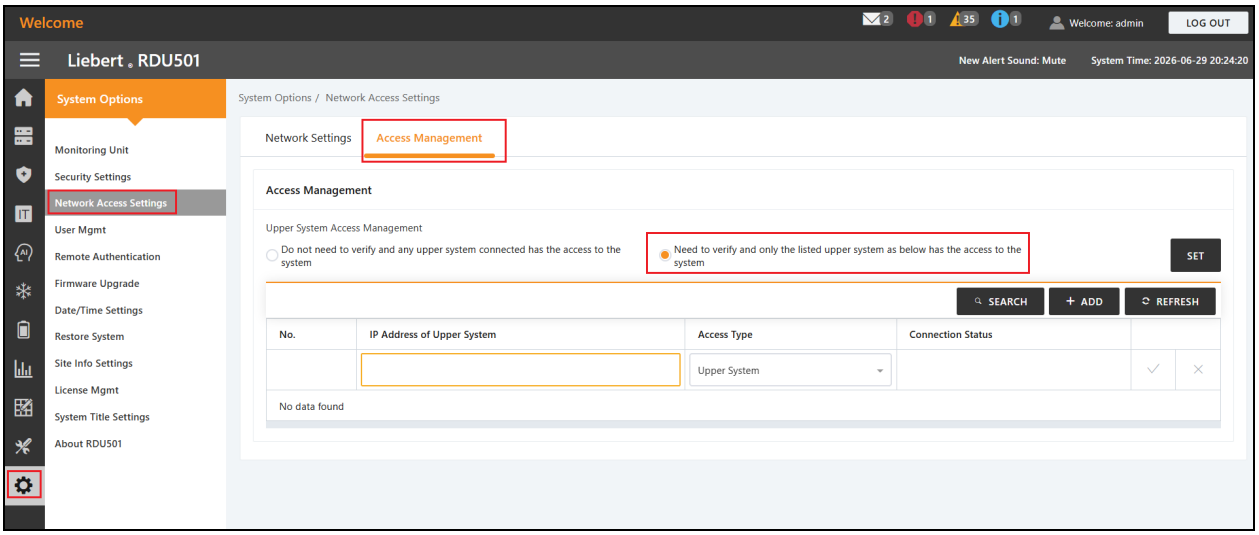
Adding an RDU

RDU501

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:

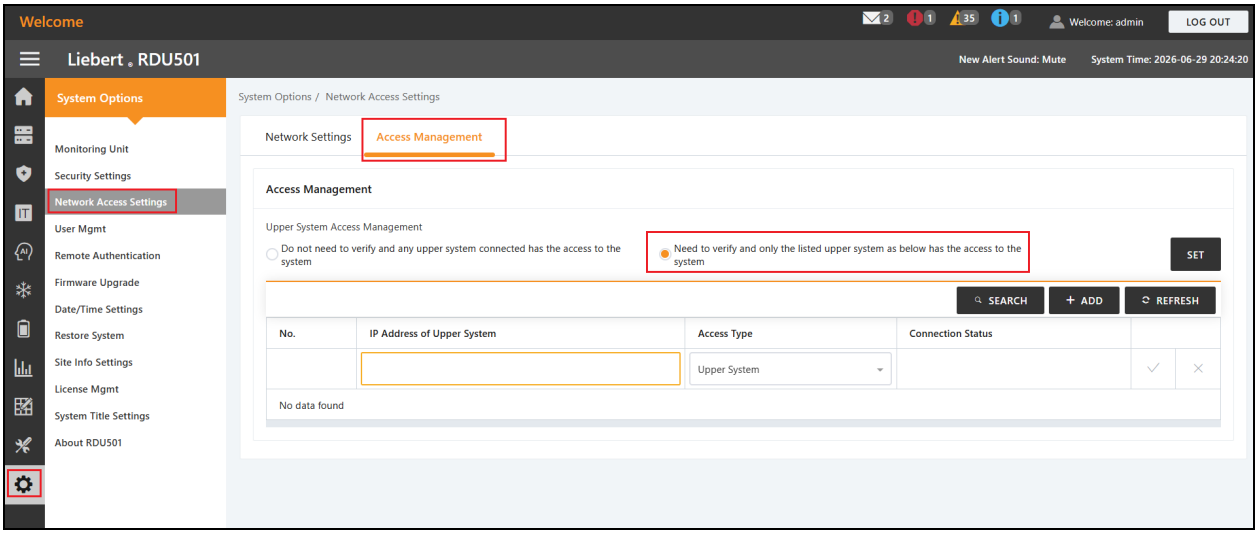
Configuration 1: Allow any Smart InfraSight™ to access the current RDU501, as shown in**Figure 13.27** below .

Figure 13.27 Access to the Current RDU 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 13.28** below .

Figure 13.28 Allowing Visitors' IP Address



NOTE: If the pre-search configuration has been confirmed but the RDU is still not found in Smart InfraSight, the RDU network may be interrupted. Check whether the RDU's network connection is normal.

© 2026 Vertiv Group Corp. All Rights Reserved.

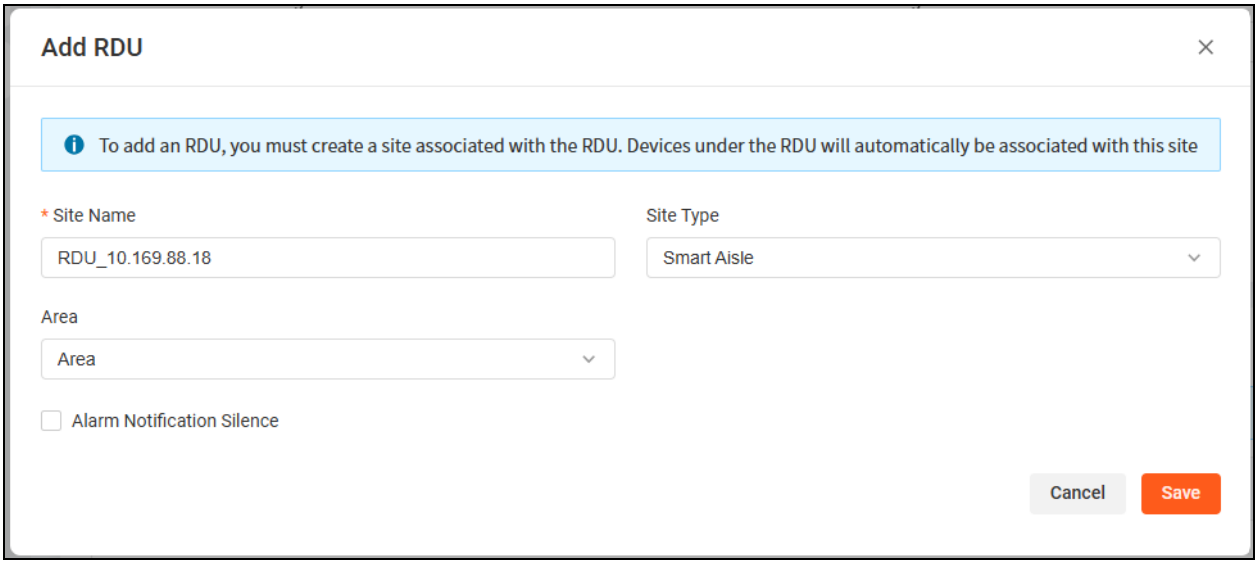
RDU Searching and on-boarding Monitoring:

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. 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 Management 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, as shown in **Figure 13.29** below .

Figure 13.29 Editing the Area



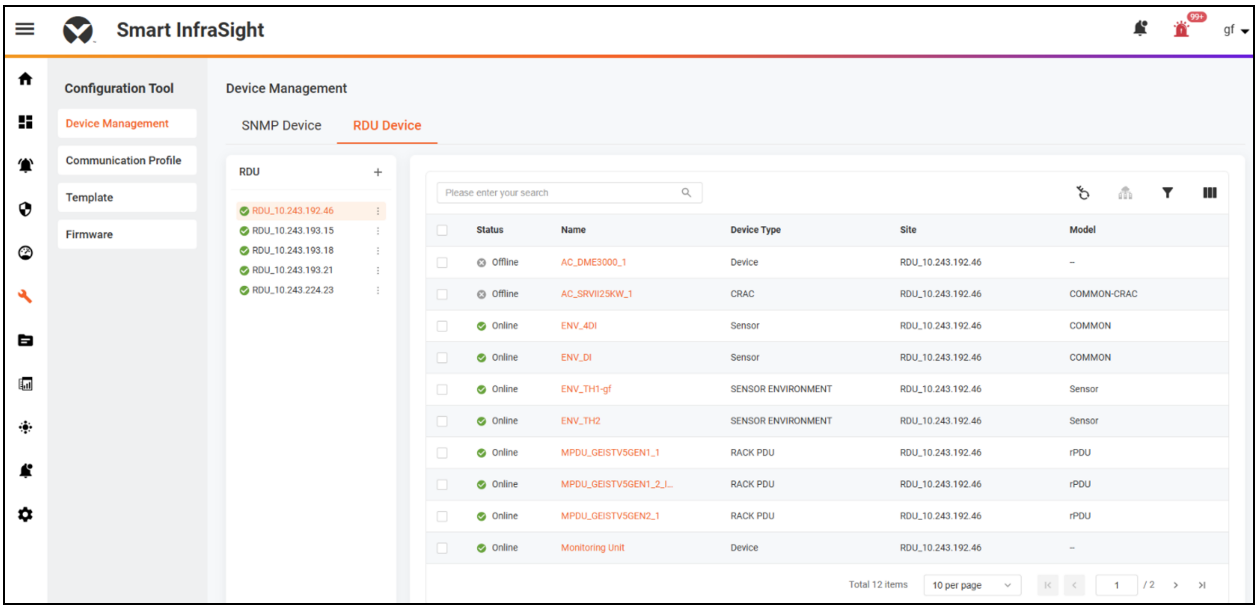
Device Configuration (Optional)

Suppose the initial settings of the device do not meet the actual requirements. In that case, 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. Please refer to the upcoming RDU Device Configuration section.

After adding, the **Figure 13.30** on the next page is displayed.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.30 Added RDU Device List

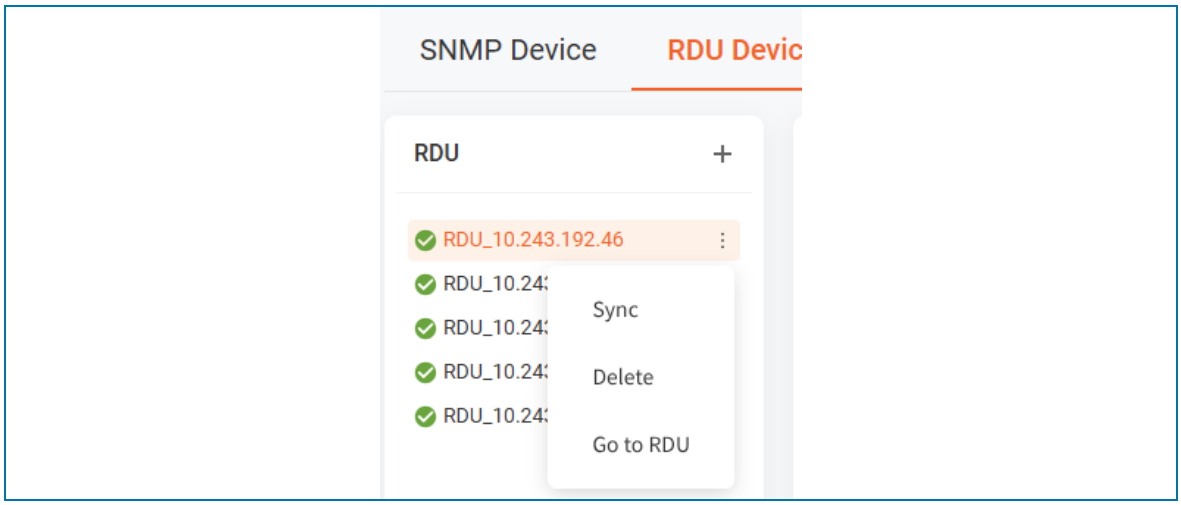


RDU Management

1. Sync RDU Configuration

a. In the RDU list, select an RDU and click the ellipses (⋮) on the right of the RDU name. A configuration drop-down list for the selected RDU appears, as shown in the Figure 13.31 below .

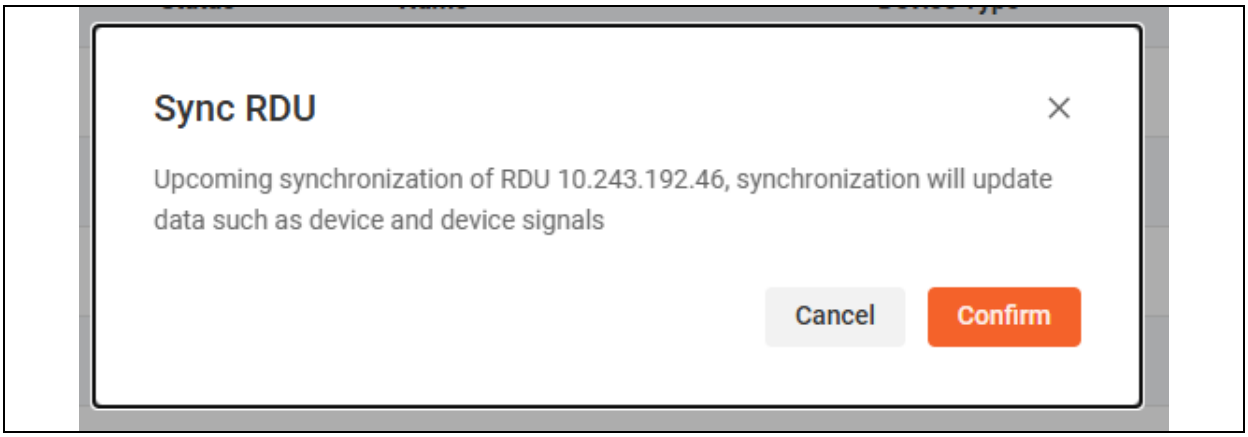
Figure 13.31 RDU Configuration Drop-down List



b. Since the selected RDU may already have configuration associations in the 3D configuration or widgets, a confirmation dialog box appears after clicking the Sync button. The user can choose to confirm or cancel based on the actual situation. If Cancel is selected, the configuration will not be synced. If OK is selected, the RDU configuration sync process begins, as shown in the Figure 13.32 on the facing page .

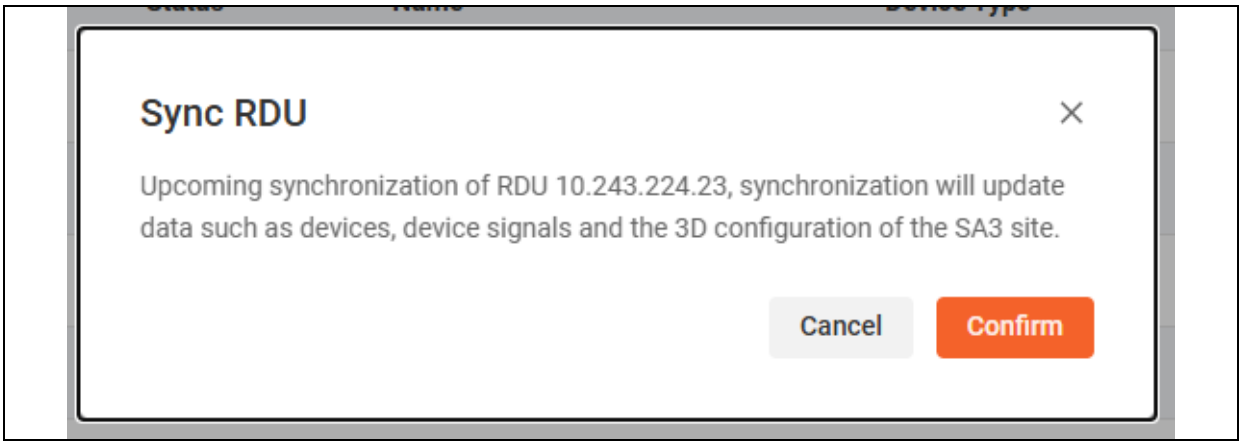
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.32 Sync RDU Configuration Progress



If the site is of SA3 type, the following prompt will be displayed.

Figure 13.33 SA3 Site Sync Prompt



2. Delete RDU

a. In the RDU list, select an RDU and click the *configuration* icon, then click the *Delete* button, as shown in the Figure 13.34 below .

Figure 13.34 RDU Deletion Prompt

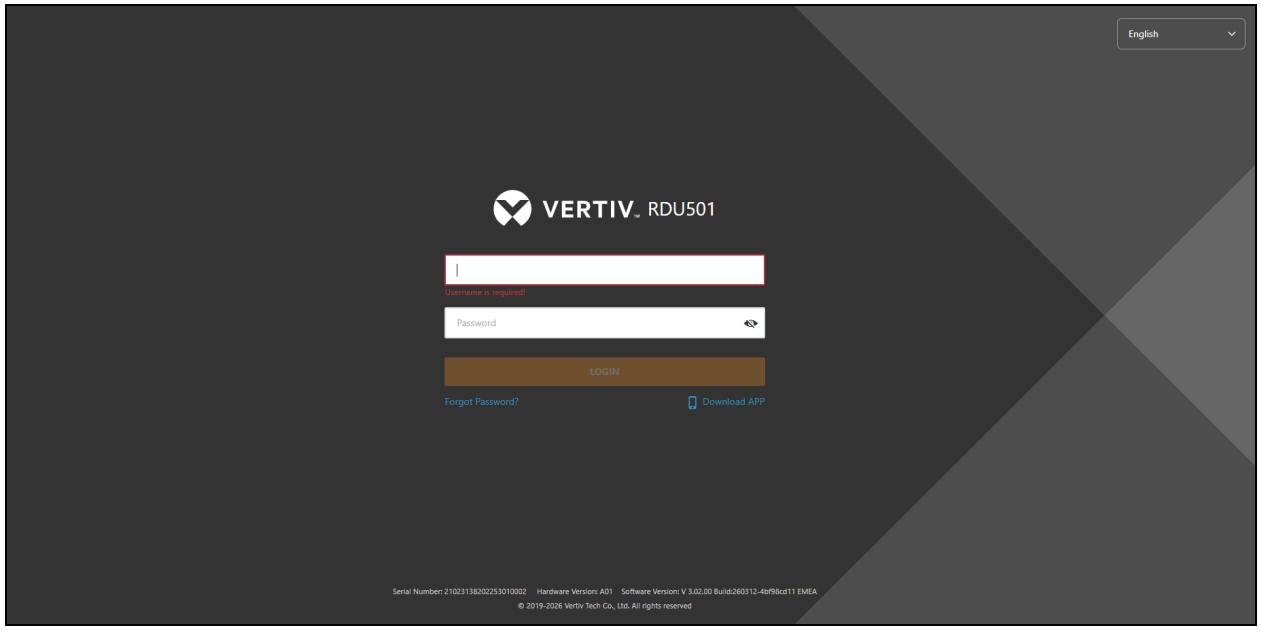


© 2026 Vertiv Group Corp. All Rights Reserved.

3. Navigate to RDU

a. In the RDU list, select an RDU and click the *configuration* icon, then click the *Go to RDU* button, as shown in the **Figure 13.35** below .

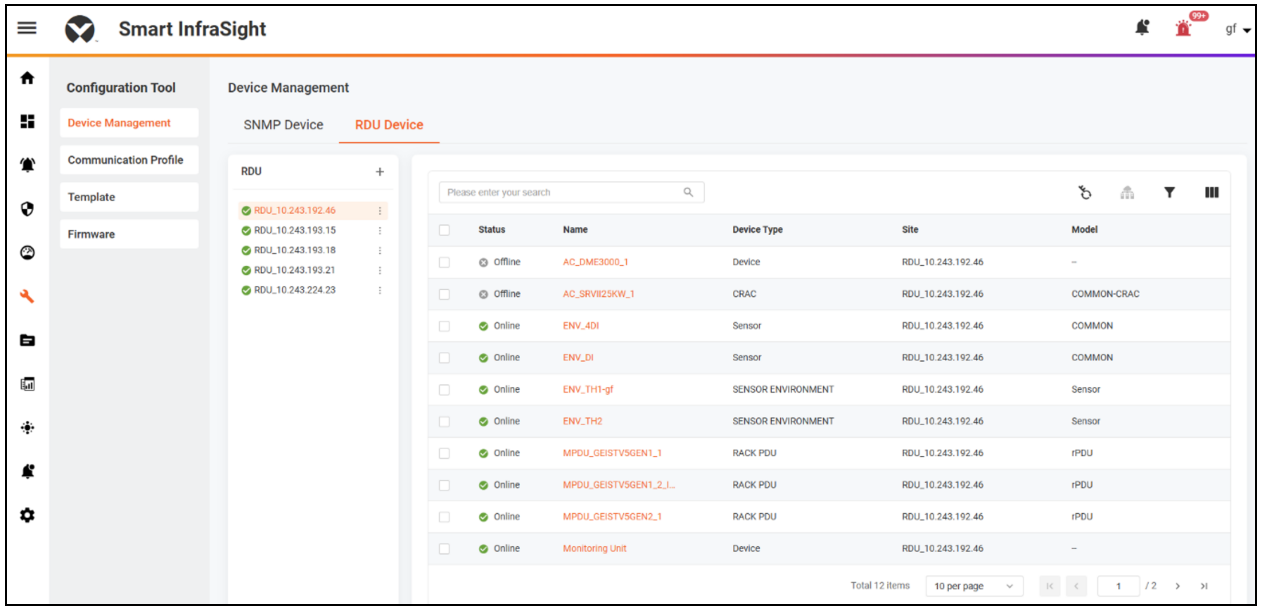
Figure 13.35 RDU Configuration



4. View Devices Associated with an RDU

a. To view devices associated with an RDU, click the *RDU site name* on the left. All associated devices will be displayed in the table on the right, as shown in the **Figure 13.36** below .

Figure 13.36 Devices Associated with RDU



© 2026 Vertiv Group Corp. All Rights Reserved.

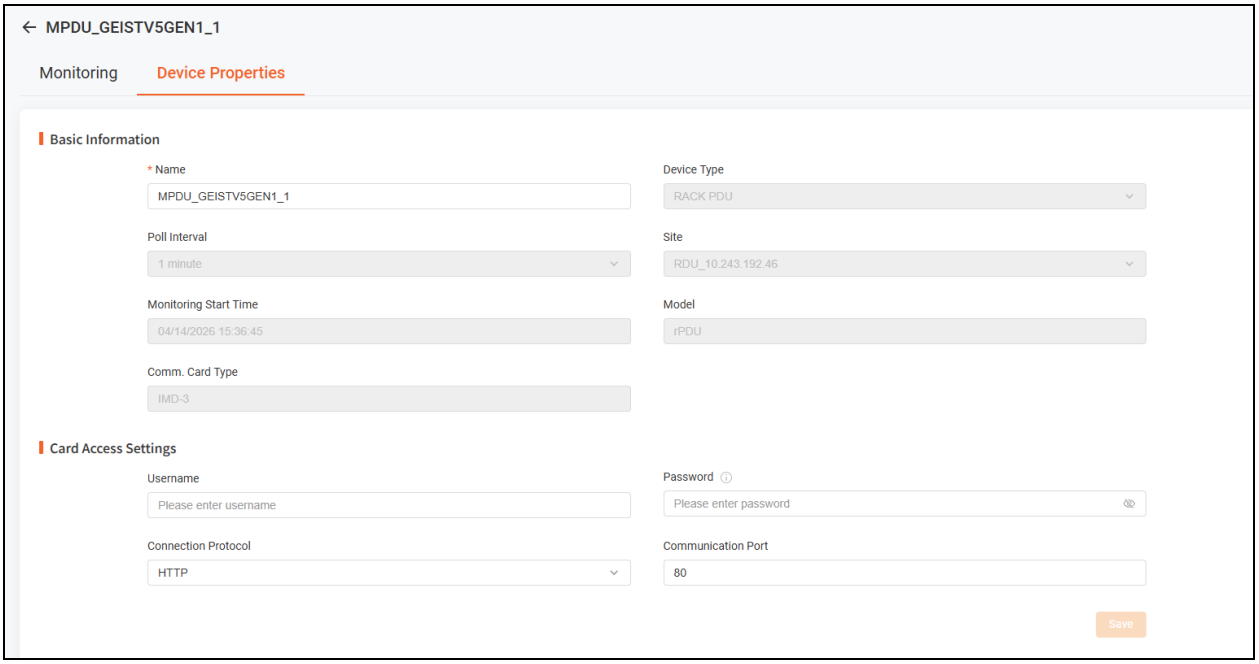
5. Device Configuration

a. Click the *name* in the table's name column to navigate to the corresponding device configuration page.

b. The device configuration page consists of two main tabs: **Monitoring** and **Device Properties**.

c. Click the **Device Properties** tab to view the basic information of the device details. If the device has a communication card, the communication settings for the card can be configured here for firmware upgrade purposes. If no changes have been made, the *Save* button remains disabled, as shown in **Figure 13.37** below .

Figure 13.37 Device Properties



RDU Device Configuration

Signal Standardization

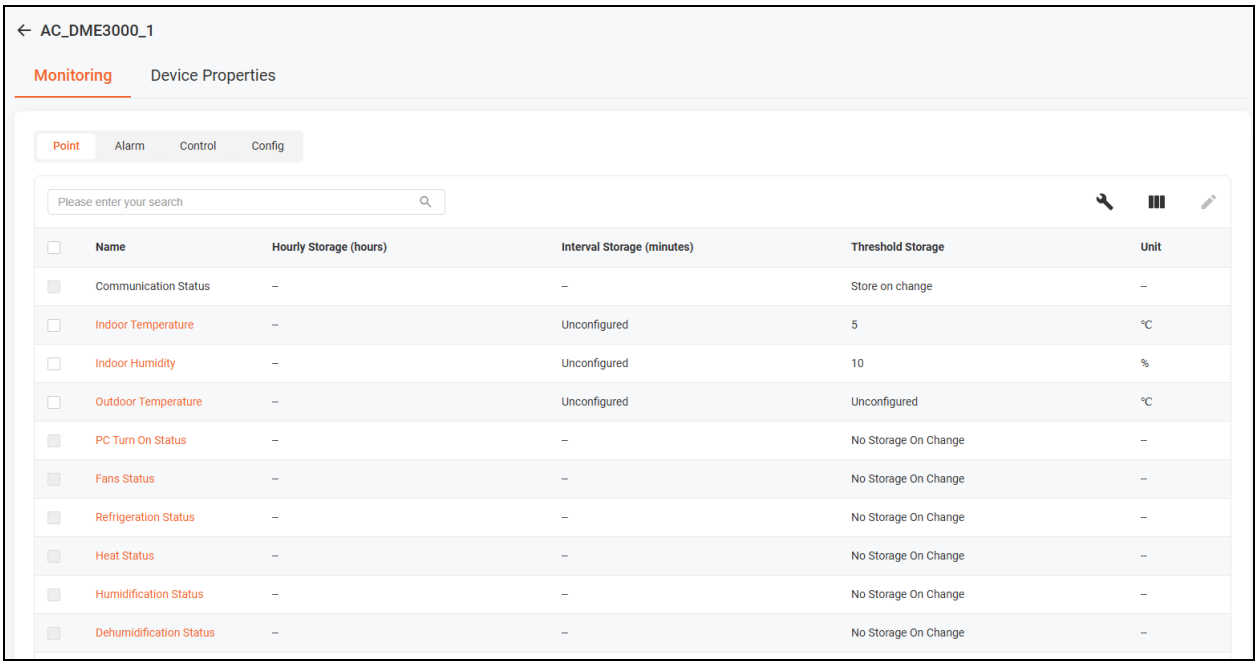
If the devices monitored by the RDU are non-standard devices, or if the device signals have not been standardized, the Signal Normalization feature can be used to associate non-standard device signals with standardized signals through manual configuration. Once normalized, the signals can be displayed in 3D views and dashboards. (It is recommended that non-professionals consult on-site configuration personnel before performing signal normalization.)

Configure Signal Normalization

a. In the Configuration Tool, click on *Device Management* page, under the Monitoring - Data Points tab, click the *Signal Normalization* button to open the Signal Normalization page, as shown in the **Figure 13.38** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.38 Signal Normalization Page



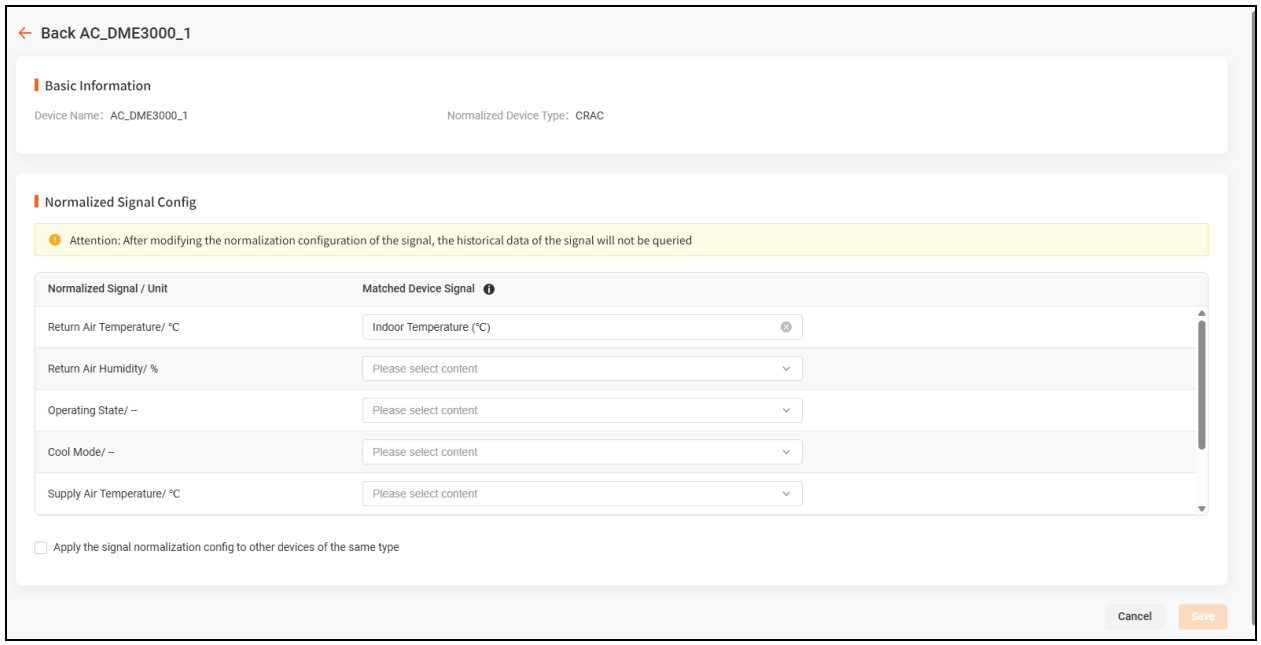
b. In the Signal Normalization page, the device type will be automatically set to the standardized device type (only UPS, air conditioning, and power meter devices are supported).

NOTE:If no signal normalization is configured and Save is clicked directly, the non-standard device type (default type is Other) will also be updated to the corresponding device type.

c. Based on the standardized signal names listed on the left, select the corresponding actual device signals on the right to match them one by one, completing the signal normalization configuration. For example, if the standardized signal name on the left is Phase A Input Voltage, select the actual signal corresponding to Phase A Input Voltage for the current device from the drop-down list on the right (if no corresponding signal exists for the device, the field can be left blank). If the device has already completed standardization and synchronization, the matched device signals will be pre-selected by default and cannot be modified, as shown in the Figure 13.39 on the facing page .

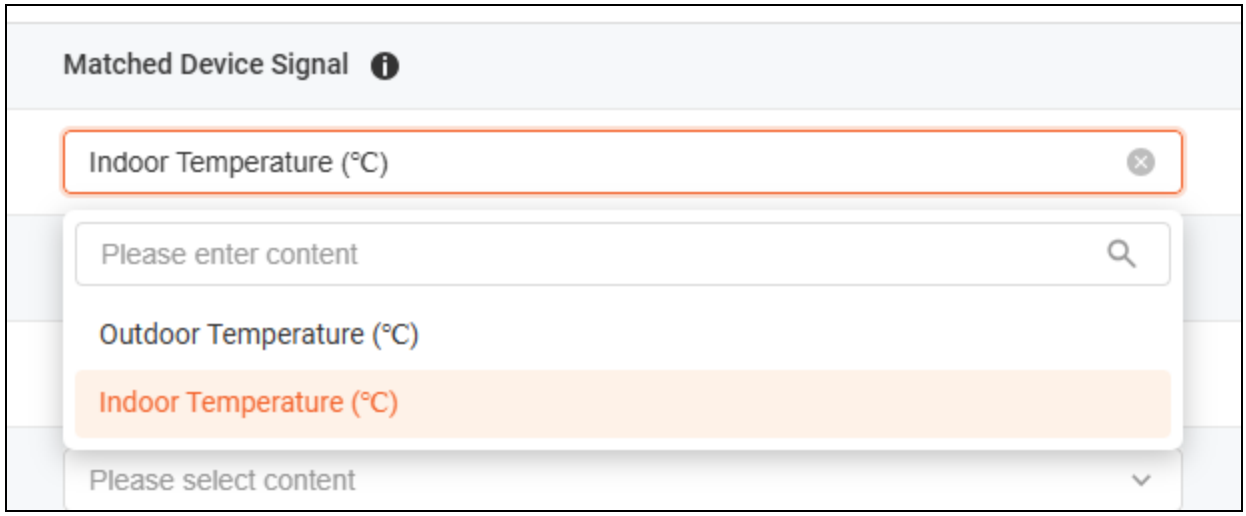
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.39 Configuring Signal Normalization Matching



d. When selecting matching device signals, click to open the device signal drop-down list to search for signal names. Only device signals with the same unit as the standardized signal will be filtered and displayed, as shown in the Figure 13.40 below .

Figure 13.40 Signal Normalization - Select Signal



e. After completing all or part of the signal normalization configuration, click *Save* to complete the normalization of the device type and the selected device signals.

NOTE:

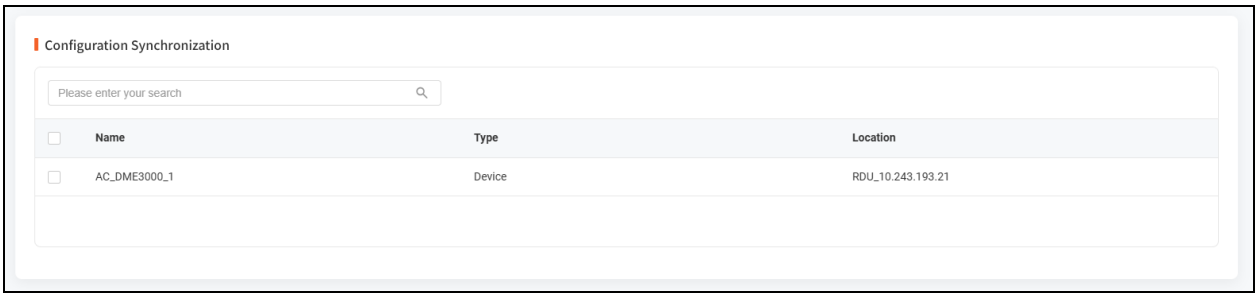
1. After modifying the signal normalization configuration, historical records prior to the modification can no longer be queried by that device signal in the historical signal report. Please proceed with caution.

© 2026 Vertiv Group Corp. All Rights Reserved.

2. If the driver of the device on the bound RDU is updated and an RDU Sync Configuration is performed in SI, the signal normalization configuration for the device will be reset. In this case, whether the signals are normalized is determined solely by the updated driver.

After completing the device signal normalization matching, users can select the checkbox below to choose other devices of the same type to apply the signal normalization configuration to (synchronization is only supported for devices in SI that have the same driver model and driver version as the current device). In the sync signal normalization configuration table, devices can be searched and filtered by entering the device name, device type, or site for a fuzzy search, After making the selection, click *Save* to apply the signal normalization configuration to the selected devices, as shown in the Figure 13.41 below .

Figure 13.41 Sync Signal Normalization Configuration

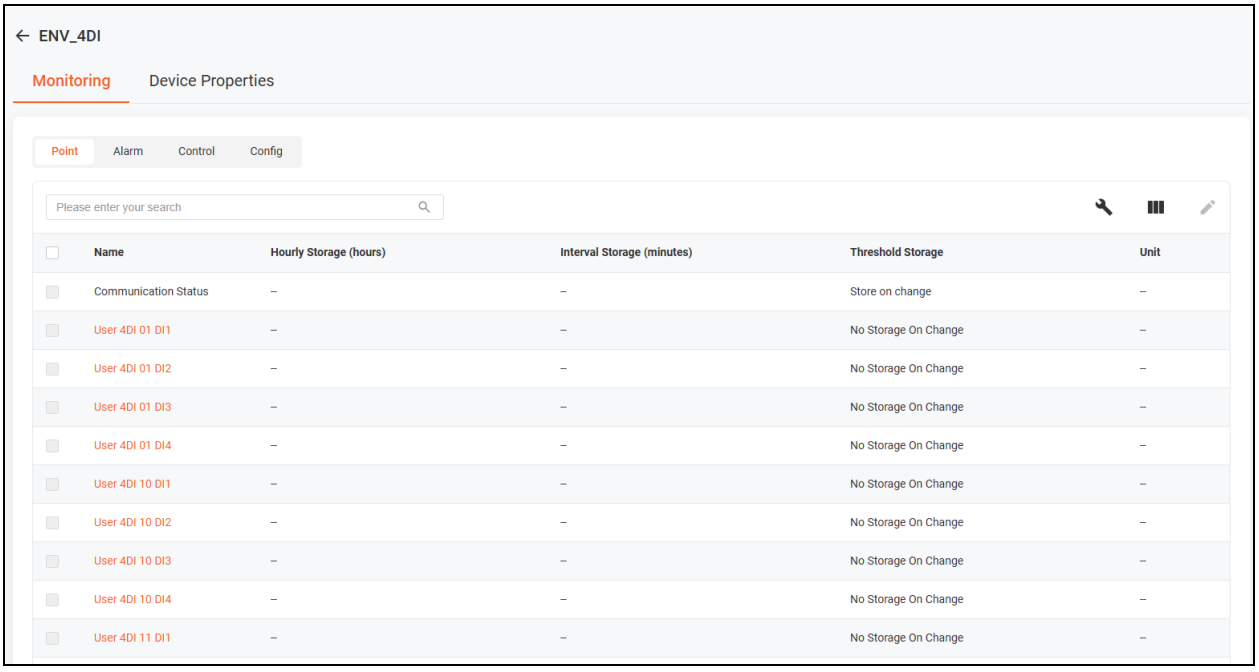


Point

1. Display Signal List

Click the *device name* in the table's name column to enter the Monitoring tab, as shown in the Figure 13.42 below .

Figure 13.42 Monitoring Tab - Data Point List



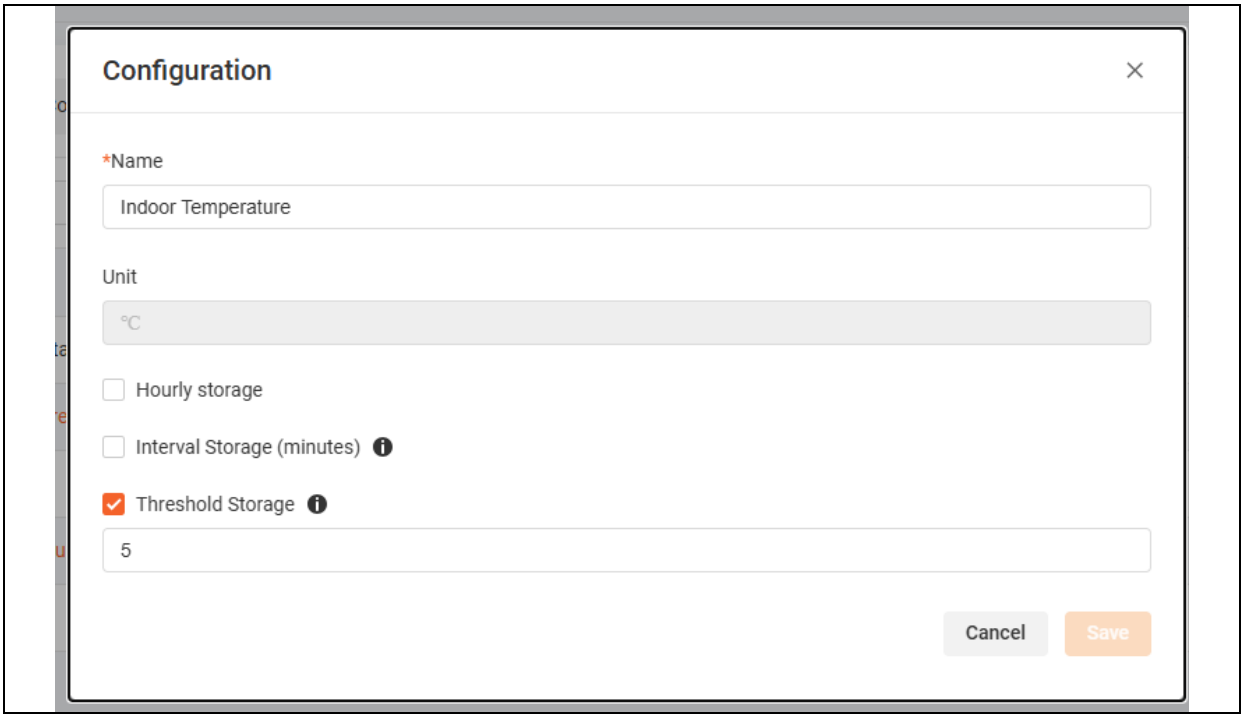
2. Use the search box to search for data points by name.

3. Signal Editing

© 2026 Vertiv Group Corp. All Rights Reserved.

a. Click the *data point* name to open the configuration dialog box.
b. The signal configuration page appears, as shown in the **Figure 13.43** below .
c. Hourly storage defaults to 1 hour. Threshold Storage: Data is stored when the value exceeds the configured threshold.

Figure 13.43 Editing the Data Point Configuration



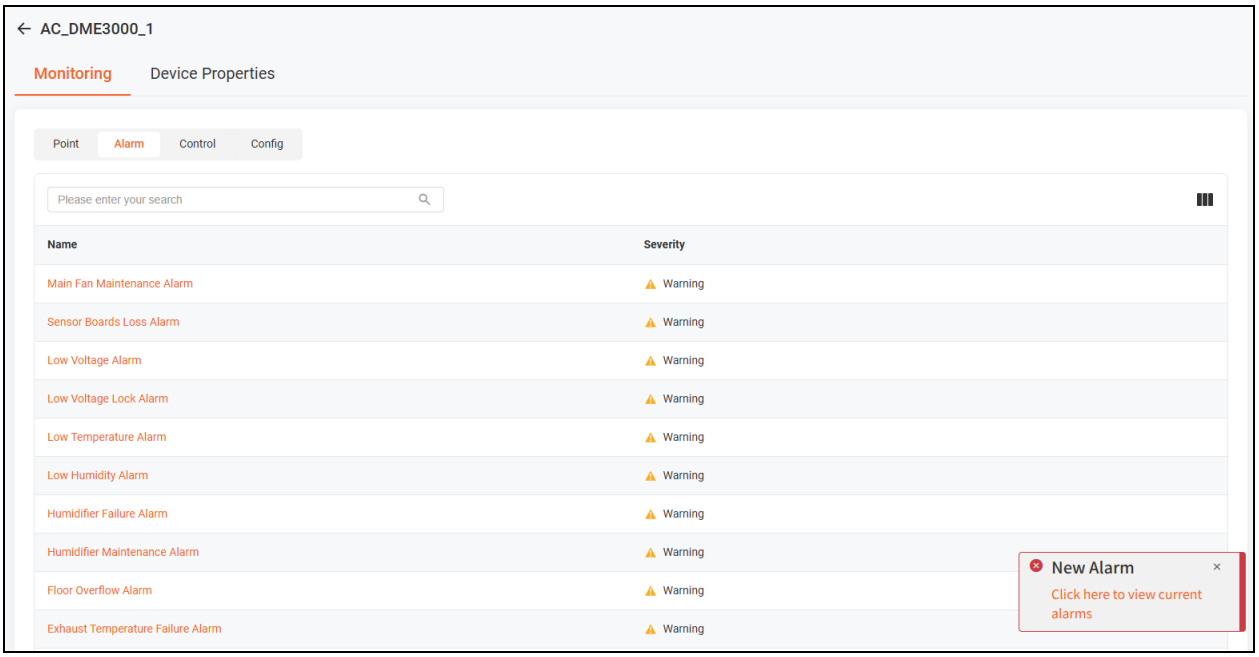
Alarm

1. Display Alarm List

a. Click the *Alarms* tab to switch to the Alarms tab, which dynamically displays the alarm list for the corresponding device, as shown in the **Figure 13.44** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.44 Monitoring Tab - Alarm List

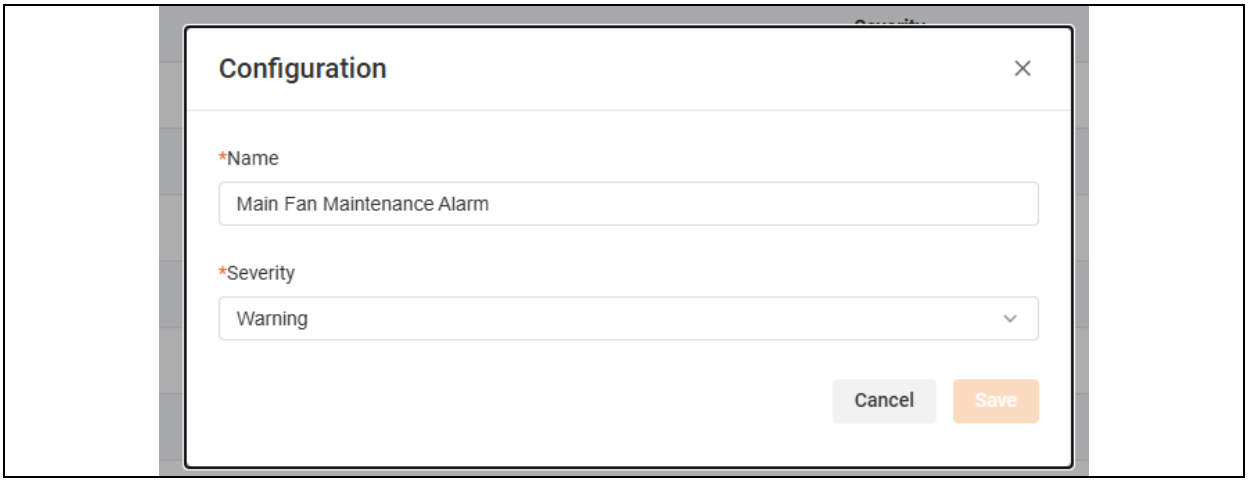


2. Use the search box to search for alarms by name.

3. Alarm Editing

a. Click the *alarm* name in the table's name column to open the name dialog box. The alarm configuration page appears, as shown in the Figure 13.45 below .

Figure 13.45 Editing the Alarm Configuration



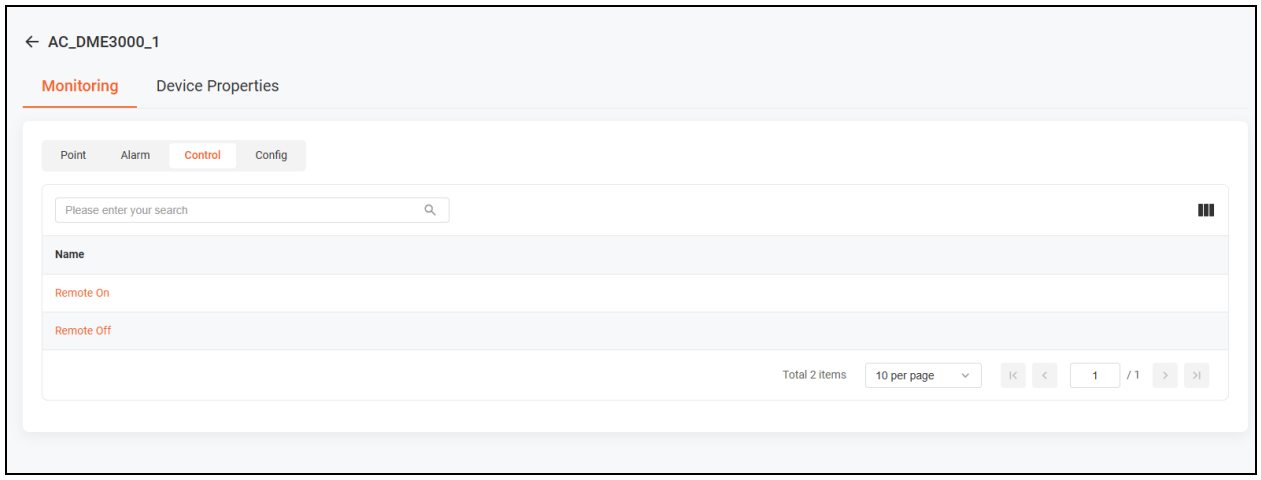
Control

1. Display Control List

Click the *Control* tab to switch to the Control tab, which displays the control list for the corresponding device, as shown in the Figure 13.46 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.46 Monitoring Tab - Control List



2. Use the search box to search for controls by name.

3. Click the *name* in the table's name column to open the editing dialog box.

The control configuration page appears, as shown in the **Figure 13.47** below .

Figure 13.47 Editing the Control Configuration



Config

1. Display Settings List

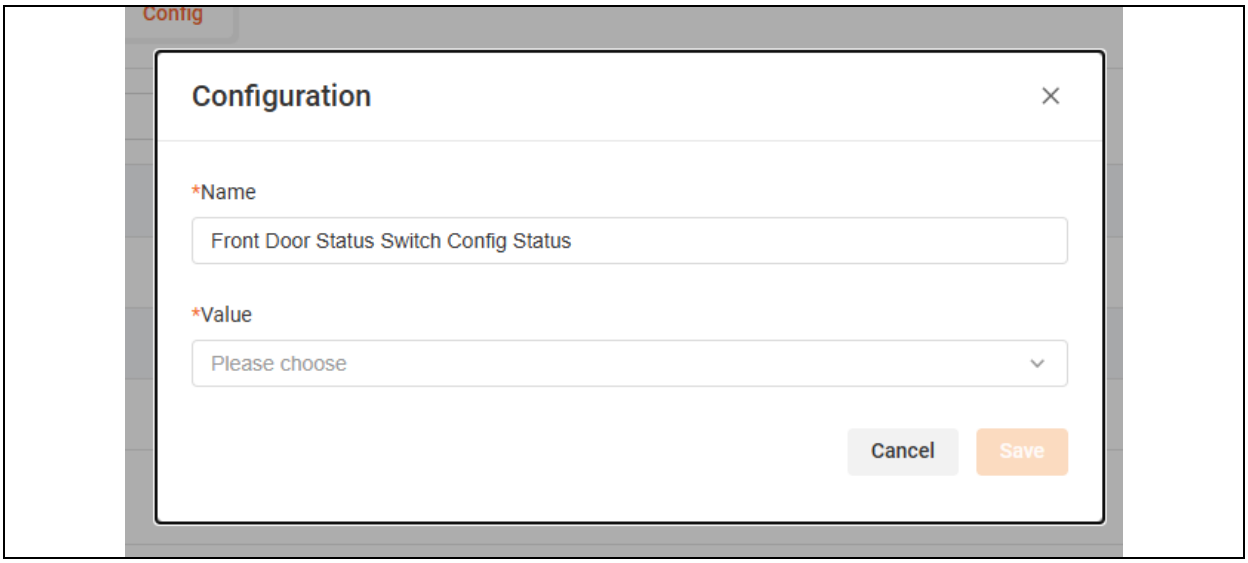
Click the *Settings* tab to switch to the Monitoring - Settings tab, which displays the settings list for the corresponding device, as shown in **Figure 13.48** on the next page .

2. Use the search box to search for settings by name.

3. When a setting name is displayed in orange, it can be clicked to open the configuration dialog box, as shown in **Figure 13.48** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.48 Editing the Settings Configuration



Device Properties

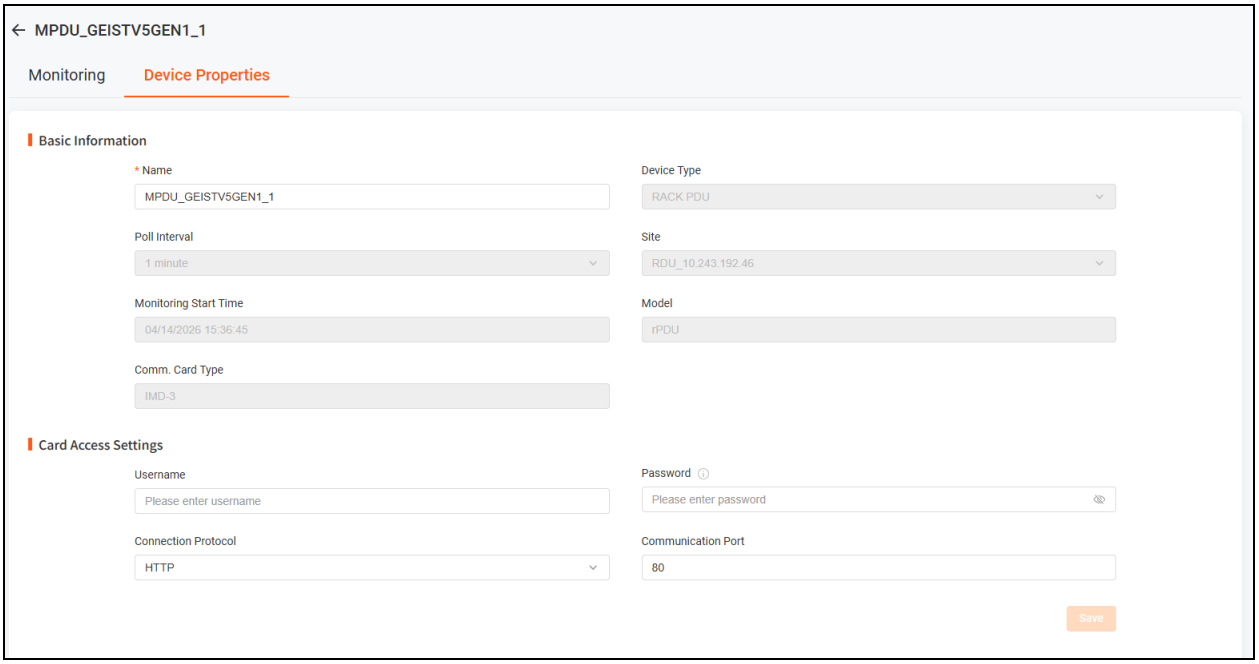
The Device Properties page contains the following sections:

Basic Information, **Card Access Settings**, (see **Figure 13.49** below).

Card Access Settings:

This section is displayed only when the device has a communication card. It is primarily used for firmware upgrades of the device or the communication card.

Figure 13.49 Device Properties Page



© 2026 Vertiv Group Corp. All Rights Reserved.

Firmware Upgrade

Fleet Management Overview

Fleet Management is used for **batch management** of Vertiv devices and communication cards. It allows users to perform operations such as firmware upgrades on multiple devices or cards simultaneously, avoiding the inefficiency and version inconsistency caused by handling devices one at a time.

4. Use Cases

a. Data centers or equipment rooms with a large number of similar Vertiv devices that require unified firmware versions.
b. Centralized upgrade or configuration of multiple communication cards.
c. Reducing manual one-by-one operations to improve maintenance efficiency and minimize human error.

5. Key Features

a. Batch firmware upgrade: Upgrade firmware on multiple devices or communication cards at once.
b. Centralized management: Manage device groups through a unified entry, reducing repetitive logins and configurations.
c. Task tracking: View the execution progress and results of batch tasks.

6. Supported Devices and Communication Cards

Fleet Management is applicable only to Vertiv devices equipped with the following communication / monitoring cards:

a. Vertiv devices with **UNITY** or **RDU101** communication cards, for example: GXT5 UPS etc.
b. Vertiv GEIST rPDUs with **IMD-3** or **IMD-5** monitoring cards.

NOTE: Refer to the latest compatibility list for the specific supported device models.

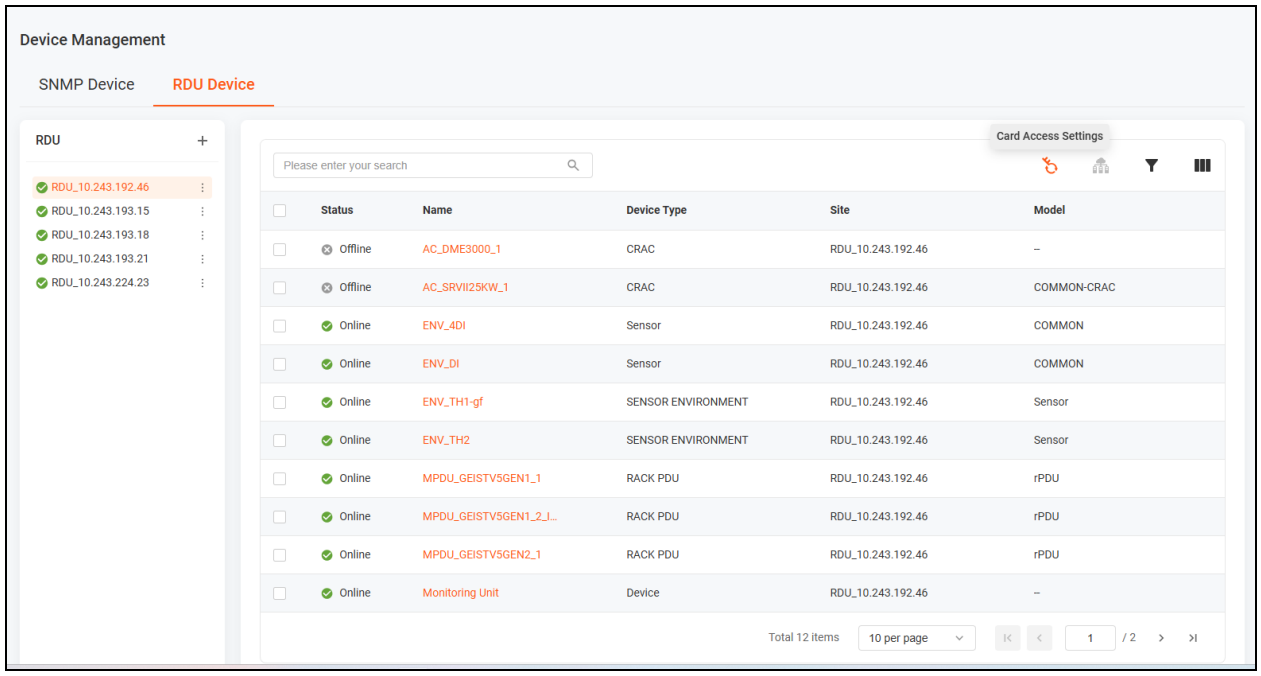
Fleet Management upgrade steps:

1. Refer to Section Firmware on page 308 to add device firmware. Ensure the correct model is selected when adding firmware.
2. Configure the correct communication information for the device or communication card to be upgraded.
   a. Set the username and password for communicating with the device's communication card:

Method 1: Go to the SNMP Device List, select devices in bulk or click the *Card Access Settings* icon in the upper-right corner of the table directly (see **Figure 13.50** on the next page).

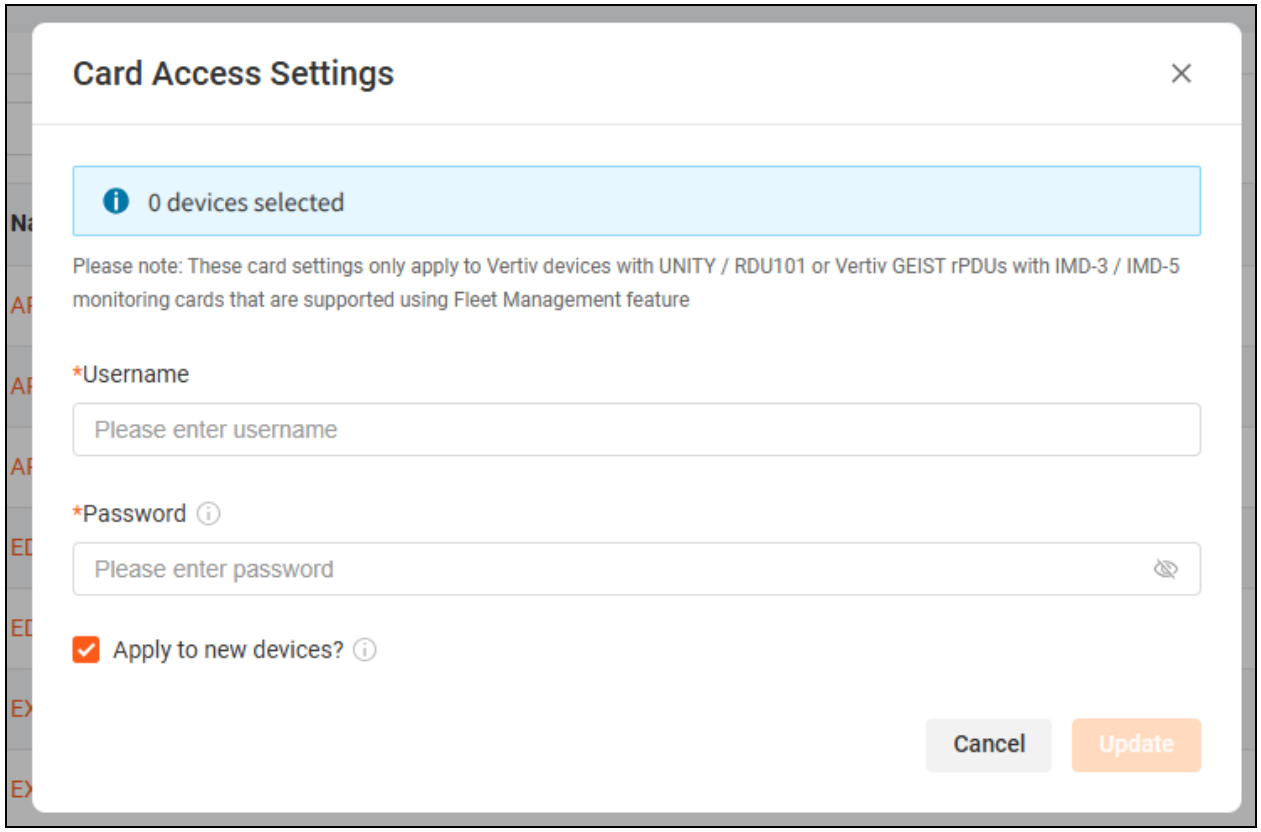
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.50 Card Access Settings Window



Click to open the dialog box (see **Figure 13.51** below).

Figure 13.51 Editing the Card Access Settings

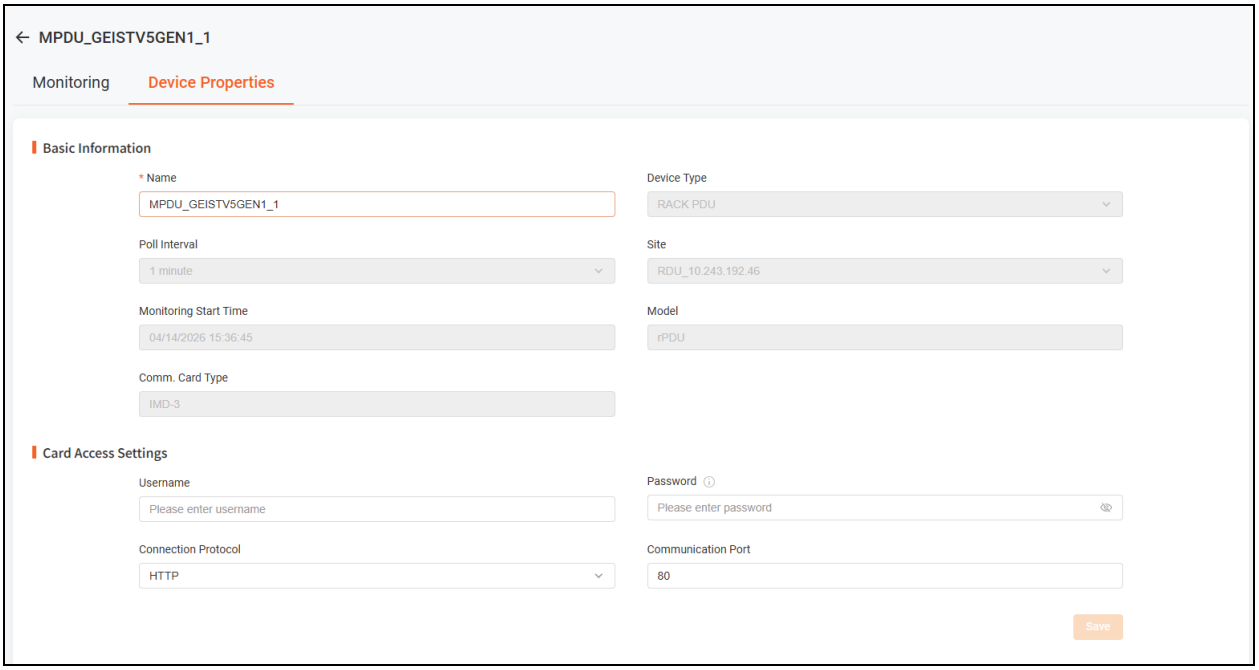


© 2026 Vertiv Group Corp. All Rights Reserved.

Select **Apply to new devices** to use the configured username and password as the default credentials for all subsequently added devices.

Method 2: Go to a device's details page, open the **Device Properties** tab, locate the **Card Access Settings** section, and set the username and password (see **Figure 13.52** below).

Figure 13.52 Card Access Settings in Device Properties



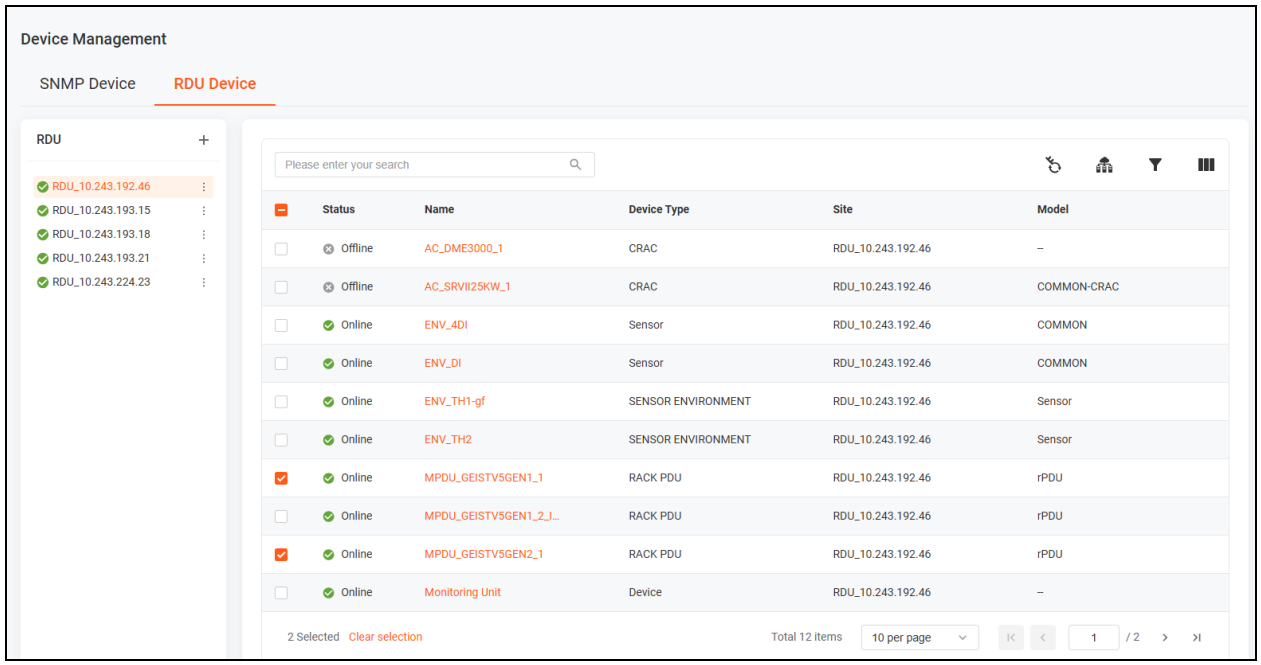
b. Set the connection protocol and communication card port:

As shown in the **Figure 13.52** above , configure the correct communication protocol and communication card port in the **Card Access Settings** section.

3. Select the devices to be upgraded. All selected devices must be online. Click the *Fleet Management* icon in the upper-right corner of the device list table (see **Figure 13.53** on the next page).

© 2026 Vertiv Group Corp. All Rights Reserved.

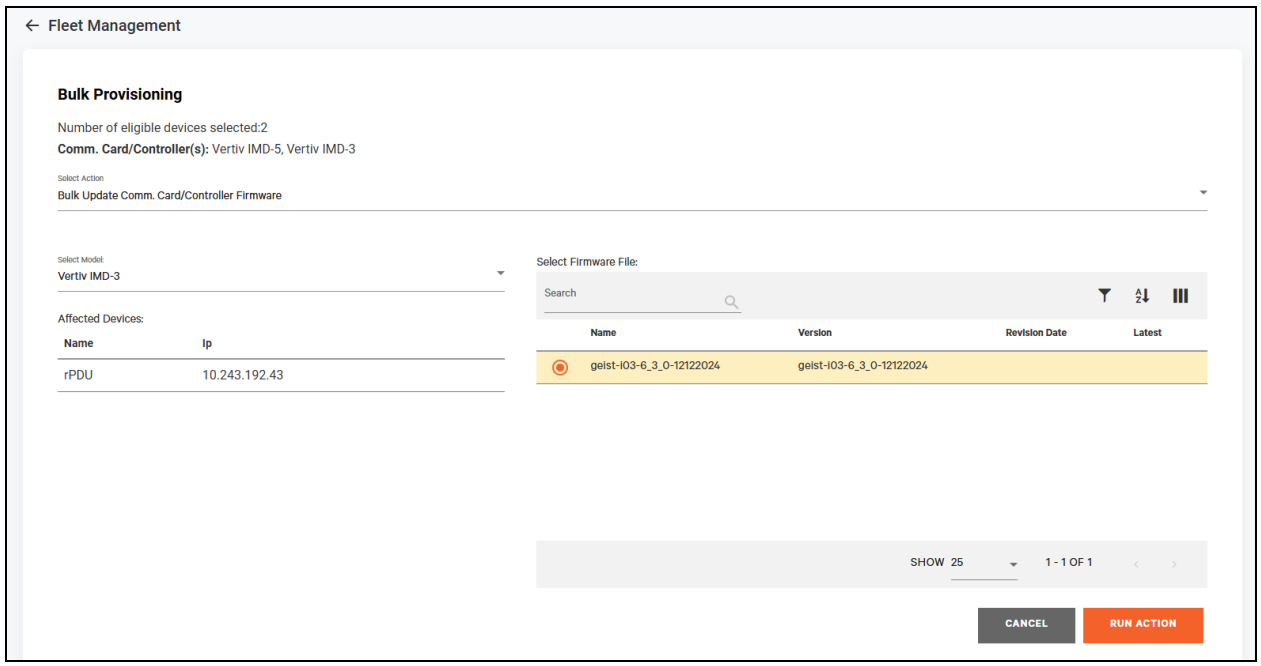
Figure 13.53 Fleet Management Icon



4. Go to the Firmware Upgrade page (see **Figure 13.54** below). Configure the following options:

- **Select Operation:** Choose **Batch Update Communication Card** or **Batch Update Device Firmware**.
- **Select Model:** Select the correct model to filter the available firmware files for that model.

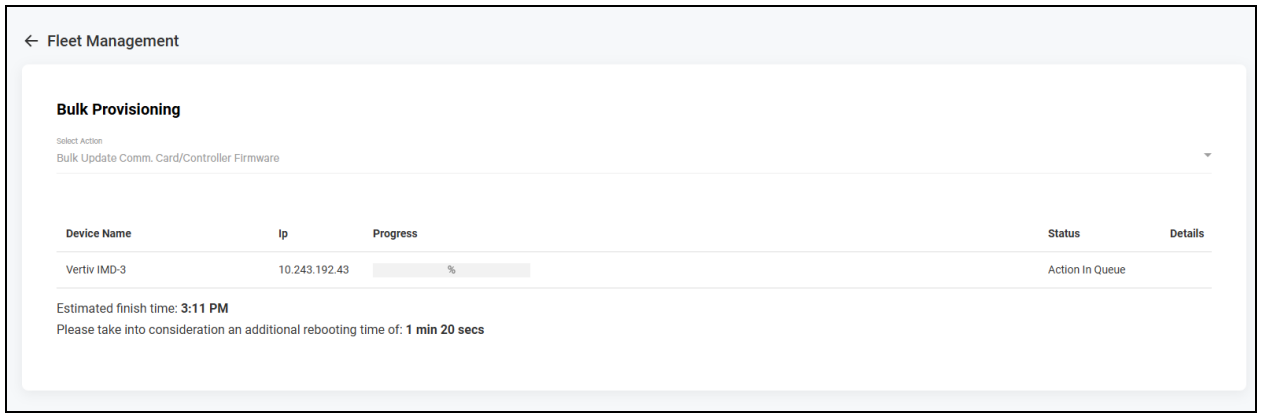
Figure 13.54 Batch Firmware Upgrade Configuration



5. Execute the operation. A confirmation dialog box appears asking whether to proceed. After confirming, the platform navigates to the upgrade progress page (see **Figure 13.55** on the facing page).

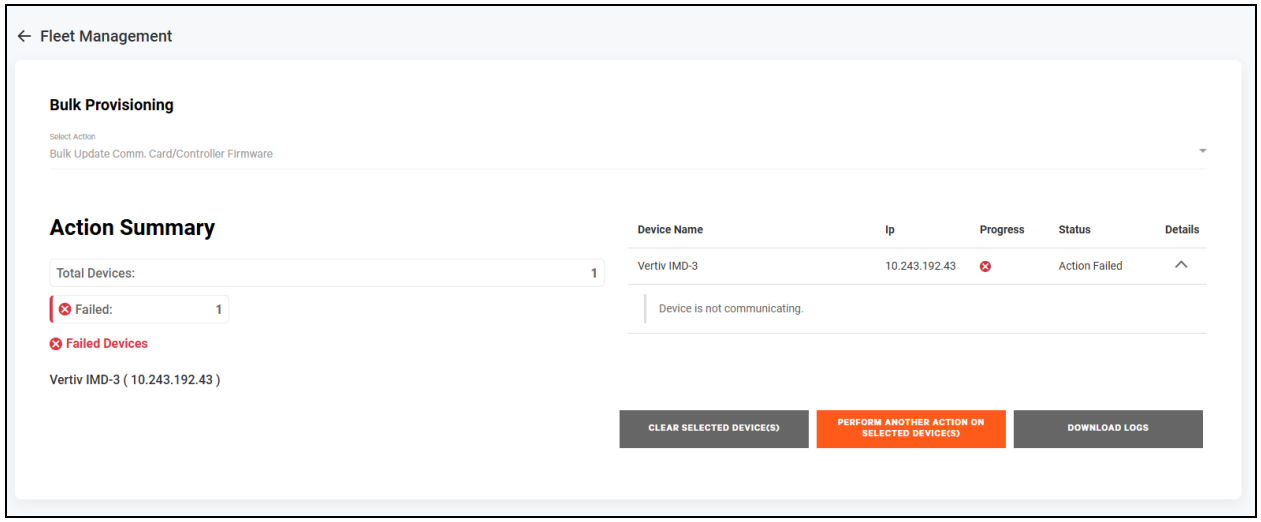
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.55 Batch Firmware Upgrade Progress



Upgrade failed (see **Figure 13.56** below).

Figure 13.56 Batch Firmware Upgrade Failed



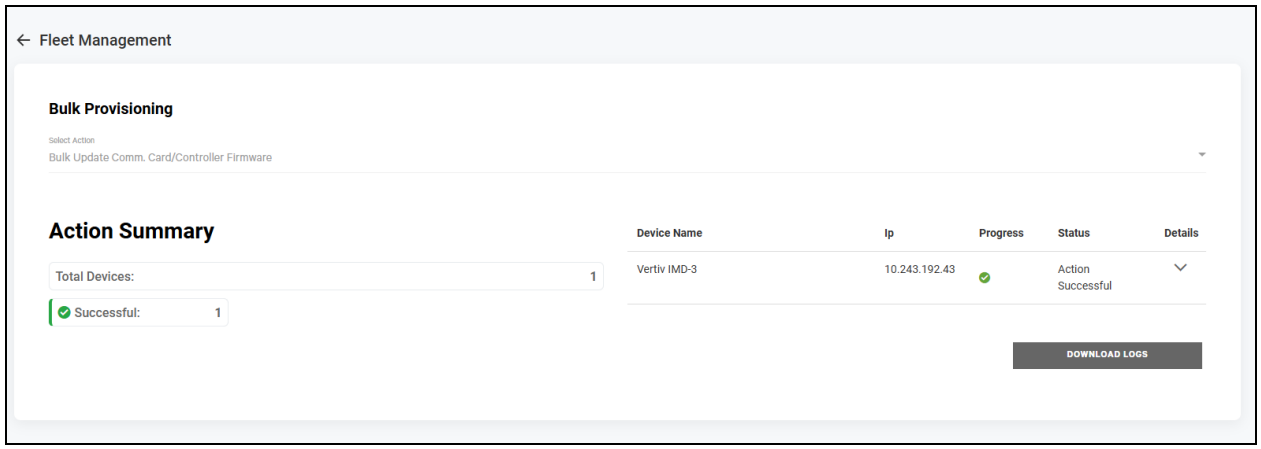
Clear Selected Devices: Clears all devices selected for the current upgrade operation.

Perform Another Operation on Selected Devices: Continues to perform another operation on the devices selected in the current operation.

Upgrade successful (see **Figure 13.57** on the next page)

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.57 Batch Firmware Upgrade Successful



NOTE: Only one firmware upgrade operation can be performed across the entire platform at a time.

An IP address change on the SI server will cause the firmware upgrade feature to become unavailable. Please refer to section 19.16 SI IP Change Causes Firmware Upgrade Unavailability for resolution.

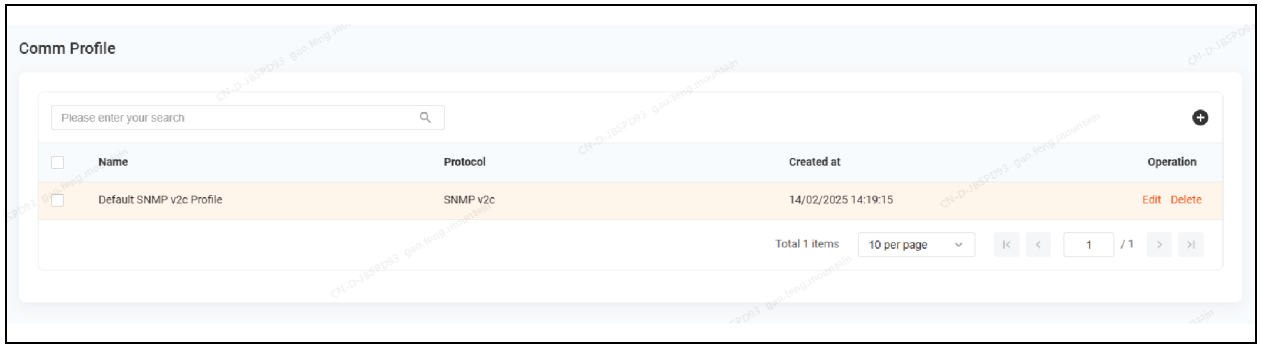
13.2.2 Communication Profile

Click *Comm Profile* under Configuration Tool to enter the communication profile list, as shown in Figure 13.58 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 13.58 Communication Profile Page



© 2026 Vertiv Group Corp. All Rights Reserved.

Adding/Editing the 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 13.59** below . If **Default for device search** is checked, this comm profile will be automatically selected when adding SNMP devices in batches in Detailed Features .

Figure 13.59 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.

If you select **SNMP v3** as the protocol, you must enter additional security settings so Smart Infrasight can communicate with the device securely.

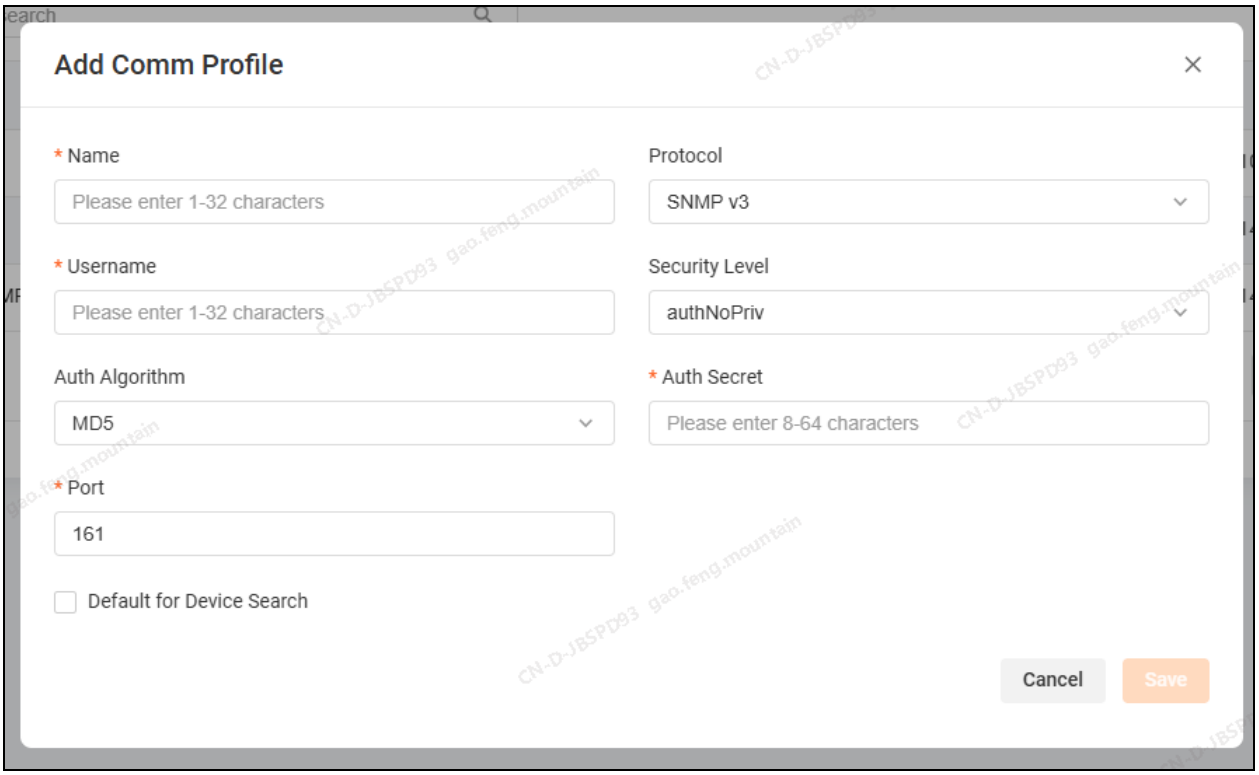
There are three security levels:

- noAuthNoPriv
- authNoPriv
- authPriv

At this security level, both the authentication secret and the privacy secret are required, as shown in **Figure 13.60** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.60 Adding the authNoPriv Comm Profile



authPriv

The authentication algorithm, authentication password, encryption algorithm, and encryption authorization password are added.

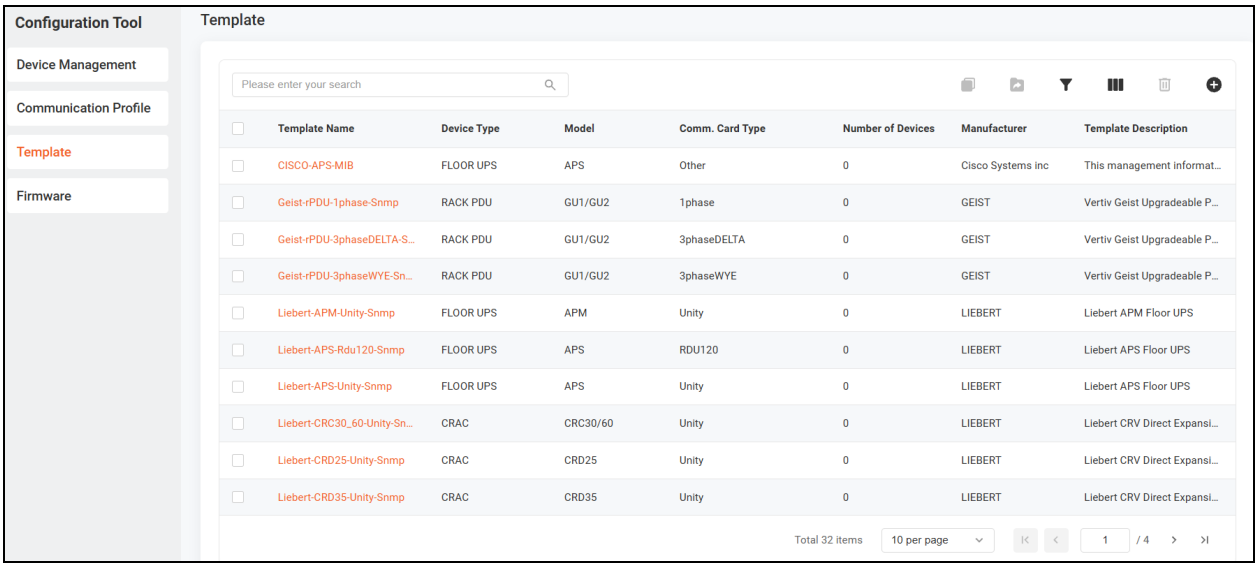
13.2.3 Template

Template list

Click *Data Collection* Template Management in the left navigation bar to enter the Data Collection Template Management list page (as shown in the Figure 13.61 on the facing page).

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.61 Template list



The page displays all configured data collection templates on the platform in a table format. By default, the list is sorted by creation time in descending order and displays 10 records per page. Each record contains the following fields:

- **Template Name:** The unique identifier for the data collection template. Click the name to enter the Edit Template page.
- **Device Type:** The category the template belongs to.
- **Protocol:** The communication protocol used by the template.
- **Manufacturer:** The name of the equipment manufacturer corresponding to the template.
- **Model:** The specific equipment model corresponding to the template.
- **Number of Associated Devices:** The number of devices currently associated with this template on the platform. Click the value to navigate to the Device List, which will be automatically filtered to show all devices using this template.
- **Version:** The current version number of the template in vX.Y.Z format (e.g., v1.0.0). Each time you duplicate or edit a template, the last digit of the version number increments automatically (e.g., from 1.0.0 to 1.0.1). The first two digits are maintained and updated only by the platform engineering team.
- **Interface Card Type:** The model of the communication card adapted for the template.
- **Template Description:** A brief description of the template.

The top of the list provides the following functions:

- **Search**: Enter keywords in the search box to perform a fuzzy search for Template Name, Device Type, Model, and
- **Manufacturer**: Search results are sorted by template name in ascending order.
- **Create**: Click *Create Template* to open the Create Template dialog box. Fill in the required information to create a template.
- **Filter**: Click the *Filter* icon to filter the list by Device Type and Model.

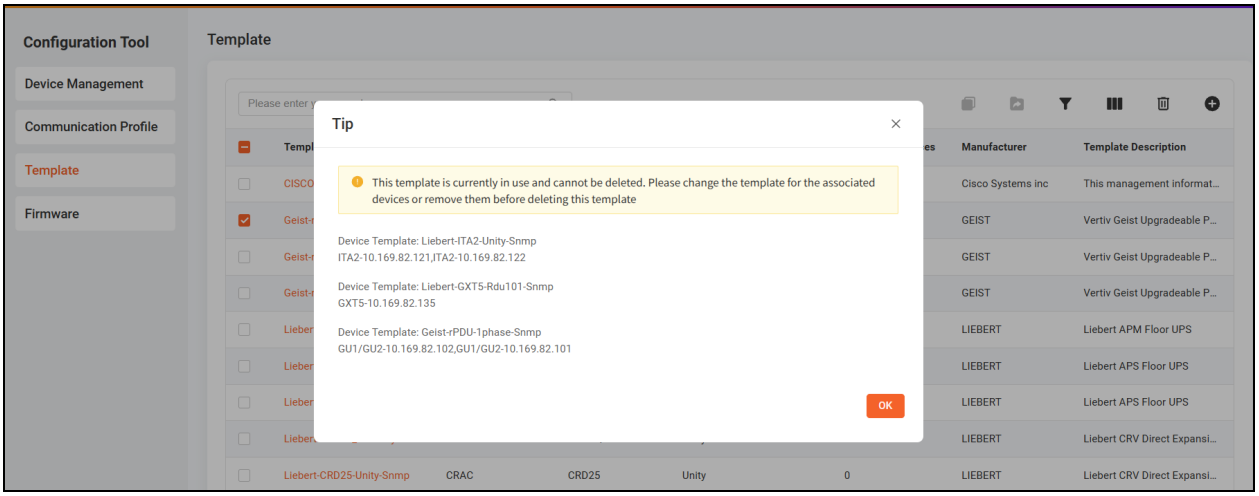
Select the checkboxes on the left side of the list to perform the following bulk operations on the selected templates:

© 2026 Vertiv Group Corp. All Rights Reserved.

- **Delete**: Click *Delete* to open a confirmation dialog box with the message **Are you sure you want to delete the selected XXX item(s)?**. Click *Confirm* to delete the templates and refresh the list. Upon completion, a **Deleted successfully** message appears.

  a. If any selected template is currently in use by a device, clicking Delete opens a notification dialog box stating "This template is currently in use and cannot be deleted. Please change the template for the associated devices or remove the devices before deleting the template." The dialog box lists the names of the occupied templates and all associated devices. (as shown in the **Figure 13.62** below).

Figure 13.62 Template In Use Cannot Be Deleted



  b. If some templates fail to delete, a notification dialog box appears stating **The following templates failed to delete**, listing the names of all templates that could not be removed.

Select a single template record to perform the following operations:

- **Export**: Click *Export* to export the template as a .template file and begin the automatic download.
- **Edit**: Click the *template name* to enter the Edit Template page.

The bottom of the list displays the total number of records. You can change the number of items displayed per page and use the pagination controls to navigate through the list.

Adding a Template

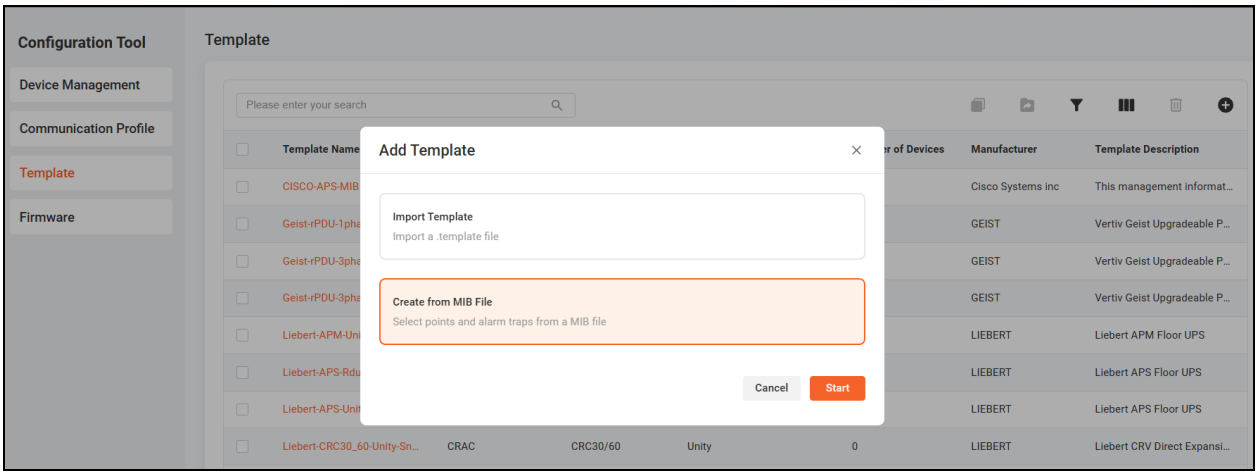
On the Data Collection Template Management list page, click (+) in the upper-right corner to open the Add Template dialog box. The dialog box provides two creation methods.

- **Import Template:** Create a template by importing a .template file.
- **Create from MIB File**: Create a template by uploading a .mib file and parsing data points and alarms from it.

Select **Create from MIB File** and click Start to enter the **Create from MIB File** page. A six-step progress indicator appears at the top of the page: **Upload MIB File, Basic Information, Select Data Points, Select Alarms, Device Mapping Rules, and Preview & Confirm.** (As shown in the **Figure 13.63** on the facing page).

© 2026 Vertiv Group Corp. All Rights Reserved.

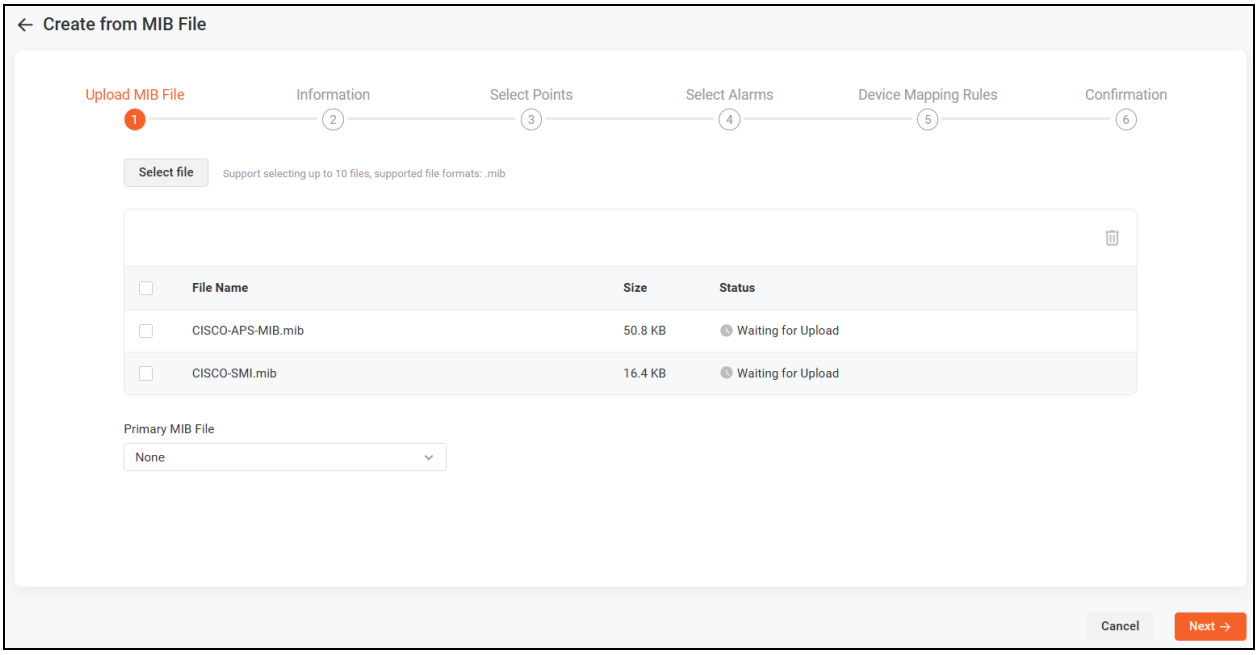
Figure 13.63 Create Template



1. Upload MIB File

Click *Select File* to choose the .mib file from your local storage. (As shown in **Figure 13.64** below).

Figure 13.64 Uploading the MIB File



The selected files are displayed in a list containing File Name, Size, and Status. The initial status is **To be uploaded.** Note the following restrictions:

- **Batch Limit:** You can select up to 10 files simultaneously. If exceeded, the platform prompts **A maximum of 10 files can be uploaded**.
- **Format Requirement**: Only .mib format is supported. Otherwise, **File format error** is displayed.

© 2026 Vertiv Group Corp. All Rights Reserved.

- **Size Limit:** Individual files must not exceed 2MB. Otherwise, **Upload file size cannot exceed XX** is displayed.
- **Duplicate Names:** If a selected file has the same name as one already in the list, the platform prompts **File with the same name already exists**, and the file is not added.

After the upload, the platform parses the files. Parsing error rules are as follows:

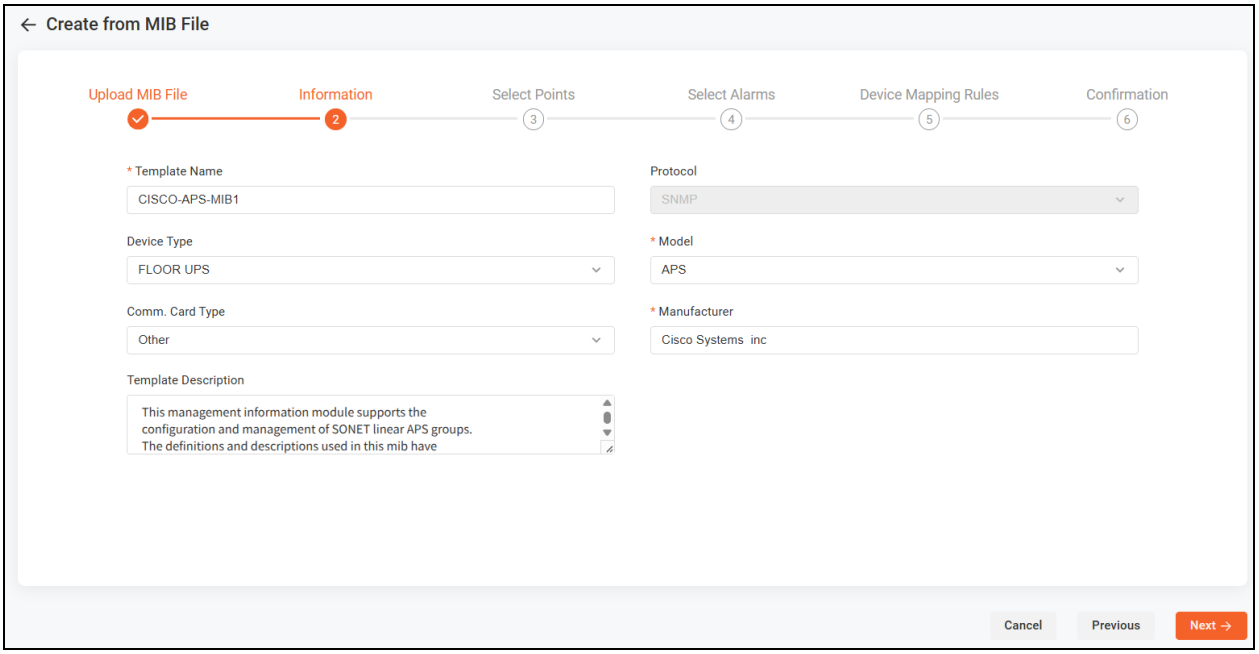
If parsing fails, the platform prompts **File cannot be parsed or an error occurred during parsing.**

If dependencies are missing, the platform prompts **Missing dependency file XXX. Please select again and ensure all dependent MIB files are chosen.**

The **Main MIB File** is an optional drop-down list (default: **None**). If multiple .mib files are uploaded, you can specify one as the main file; the platform will then parse data points and alarms only from that file. If no main file is specified, the platform parses all uploaded files. Click *Next* to proceed. If the file statuses are **To be uploaded,** the platform performs the upload before proceeding to Step 2. Click *Cancel* and confirm with **Discard current changes?** to return to the **Data Collection Template Management** list page.

2. Basic Information (As shown in the **Figure 13.65** below)

Figure 13.65 Template Basic Information Configuration



Once the upload is successful, complete the following fields:

- **Template Name:** Mandatory. 1–64 characters. If left blank, **Must be 1–64 characters** is displayed. If a duplicate name exists, the platform prompts **Value already exists**.
- **Protocol:** Drop-down list. Only SNMP is supported (read-only).
- **Device Type:** Mandatory. Default: **Floor UPS**. Options include OTHER_DEVICE, RACK UPS, CRAC, RACK PDU, and FLOOR UPS.

© 2026 Vertiv Group Corp. All Rights Reserved.

- **Model**: Mandatory. It's a dropdown list, but it also supports manual input. After clicking, enter your custom model, and the list below will display the model you entered. Once you're finished, click to save it as your custom model.. 1–64 characters.
- **Interface Card Type:** Mandatory. Default: Other. Options: Other, RDU120, RDU101, Unity, GEIST IMD, RDU-SIC, RDU-SIC G2, and SIC.
- **Manufacturer:** Mandatory. Default: VERTIV. 1–64 characters.
- **Template Description:** Optional. Multi-line text. 1–64 characters.

Click *Next* once mandatory fields are filled. If you modified Interface Card Type after returning from Step 3, a dialog box warns: **The interface card type affects alarm definitions. Modifying it may refresh the current alarm configuration.**

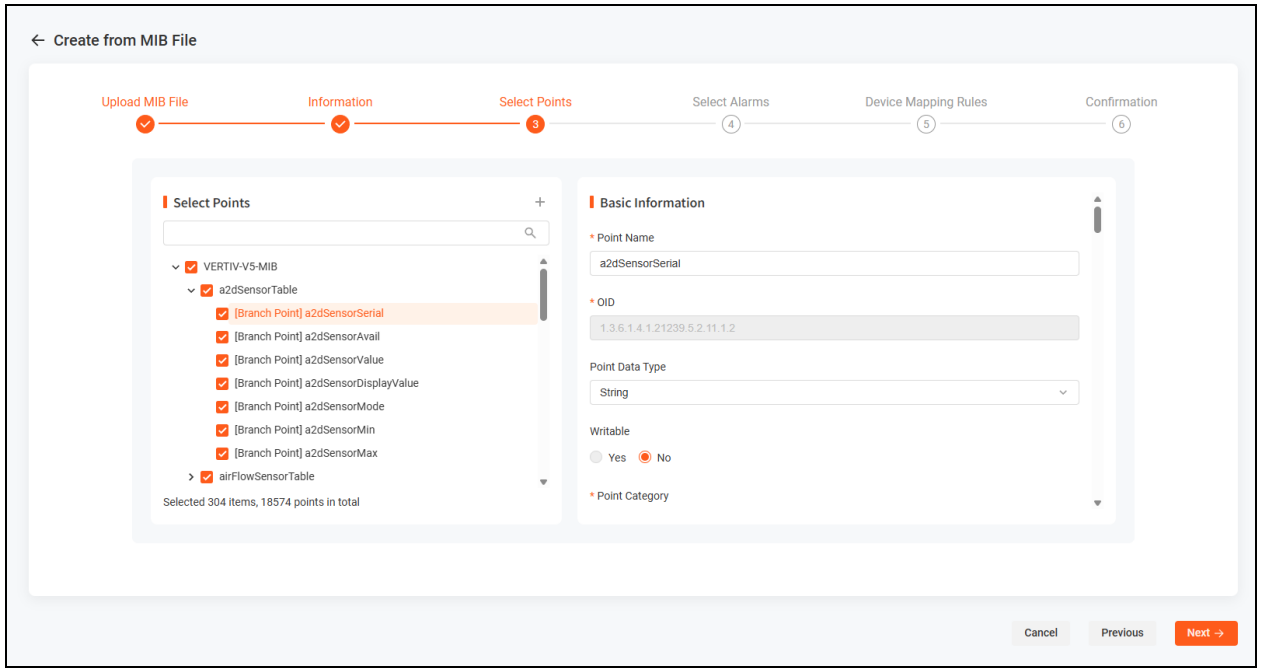
NOTE: Switching within groups (e.g., Unity/RDU101/RDU120 or Other/RDU-SIC/RDU-SIC G2/SIC) does not trigger a refresh. Cross-group switching will trigger a refresh.

Click *Back* to return to Step 1 or *Cancel* to exit the process.

3. Selecting the Data Points

The page is divided into two columns. (As shown in the **Figure 13.66** below)

Figure 13.66 Selecting the Data Points for Template



The left column displays a tree structure of all data points parsed from the .mib file, sorted by name in ascending order. All points are selected by default. The bottom displays the count as **Selected data points: XX / XX.**

- If multiple files were uploaded without a main file specified, the tree uses filenames as root nodes.
- If a main file was specified, only its results are shown.

The top search box supports fuzzy searches by data point name. Click (+) at the top of the list to open the Add Data Point drawer; manually added points are grouped under **Custom Point.**

© 2026 Vertiv Group Corp. All Rights Reserved.

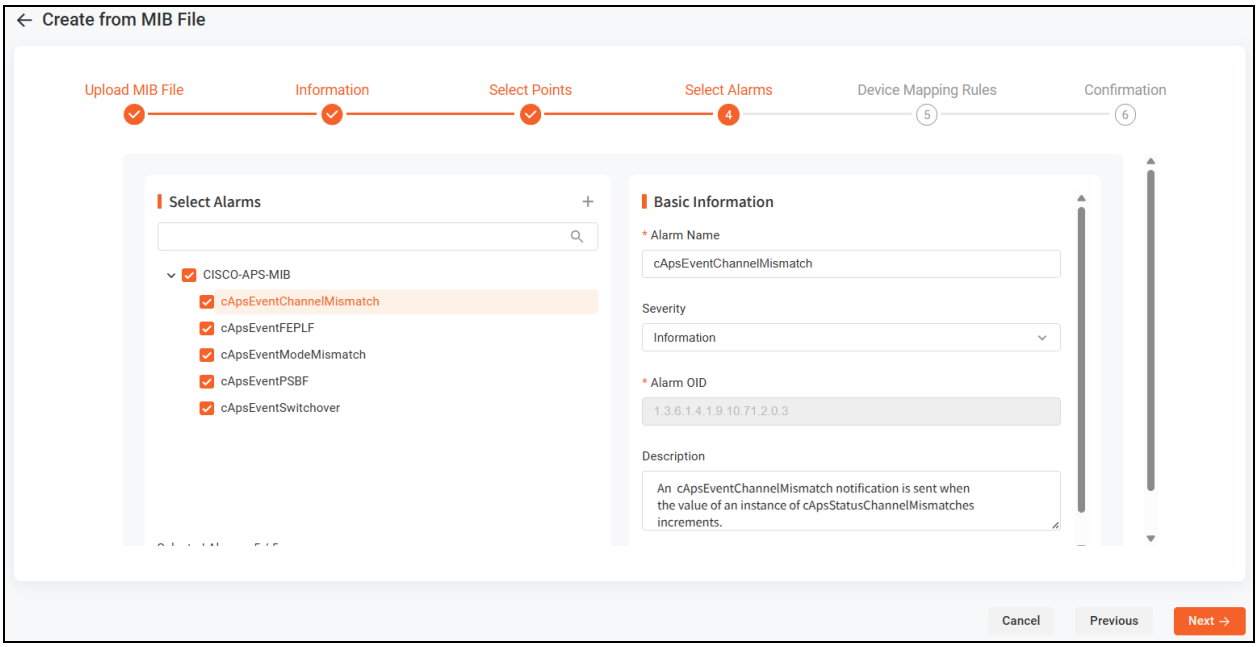
The right column is the details area. Click any point on the left to view its details (identical to the Add Data Point drawer fields). The OID field is read-only. The list focuses on the first point by default. If mandatory fields are missing, clicking Next prompts **The selected data point content is incomplete. Please provide mandatory information**. Incomplete points display a warning icon until fixed. Click *Next* to proceed to Step 4. Click *Back* to return to Step 2 or *Cancel* to exit.

- If the user selects more than 2,000 signals among the selected signals, when clicking Next, a prompt will appear: **Each template supports up to 2,000 points for optimal performance. Reduce your selection and click Next again**. .It should be noted that branch signals may contain multiple signals.

4. Selecting the Alarms

The page layout is identical to Step 3. (As shown in the **Figure 13.67** below)

Figure 13.67 Selecting Alarms for Template



The left column displays a tree structure of all alarms parsed from the .mib file, sorted by name in ascending order. All are selected by default. The bottom displays **Selected alarms: XX / XX**.

- If no main file is specified, filenames serve as root nodes.
- If a main file is specified, only its results are shown.

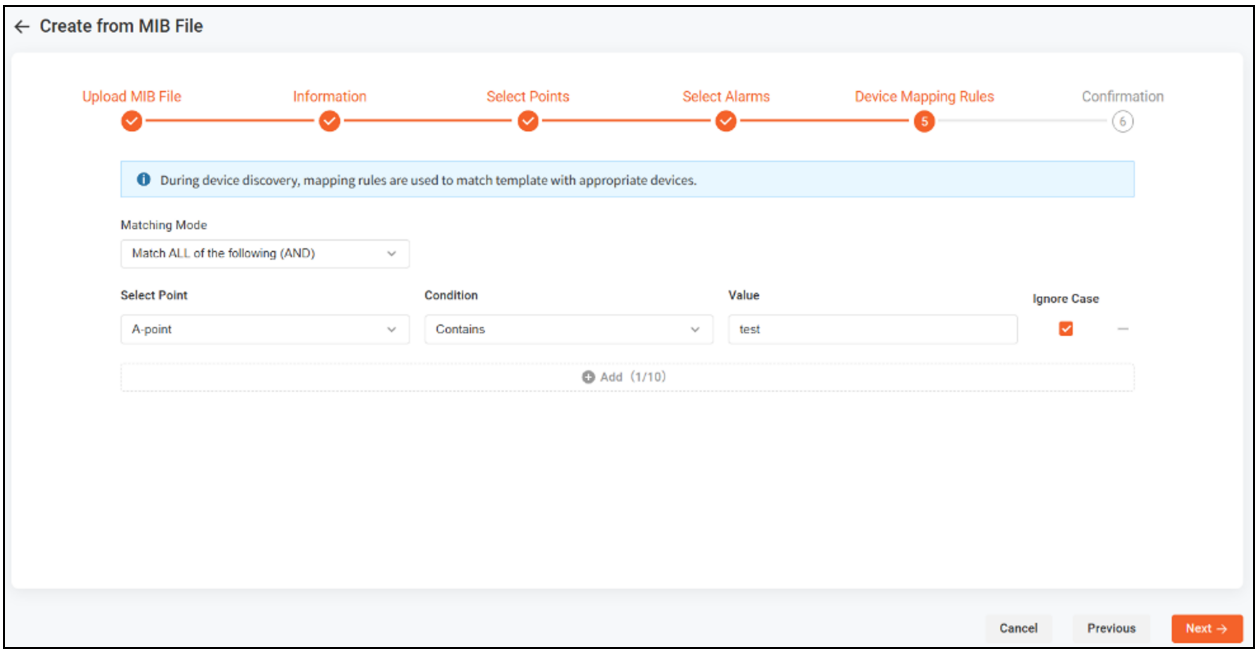
The top search box supports fuzzy searches by alarm name. Click (+) to open the **Add Alarm** drawer; manual alarms are grouped under **Custom Alarm.**

The right column displays alarm details. The Alarm OID field is read-only. Incomplete mandatory fields trigger a warning icon and block the Next action. Click *Next* to proceed to Step 5. Click *Back* to return to Step 3 or *Cancel* to exit.

5. Device Mapping Rules (As shown in the **Figure 13.68** on the facing page)

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.68 Configuring the Device Mapping Rules



Instructional text: **During the device discovery process, mapping rules are used to match the current template with devices.**

Matching Mode: Drop-down list. Default: **Match ALL of the following (AND).** This defines the logic between multiple rules. The rule list contains: Select Point, Condition, Value, and Ignore Case. Click *Add* to create a rule (up to 10 rules). Click *Next* to proceed. Click *Back* to return to Step 4 or *Cancel* to exit.

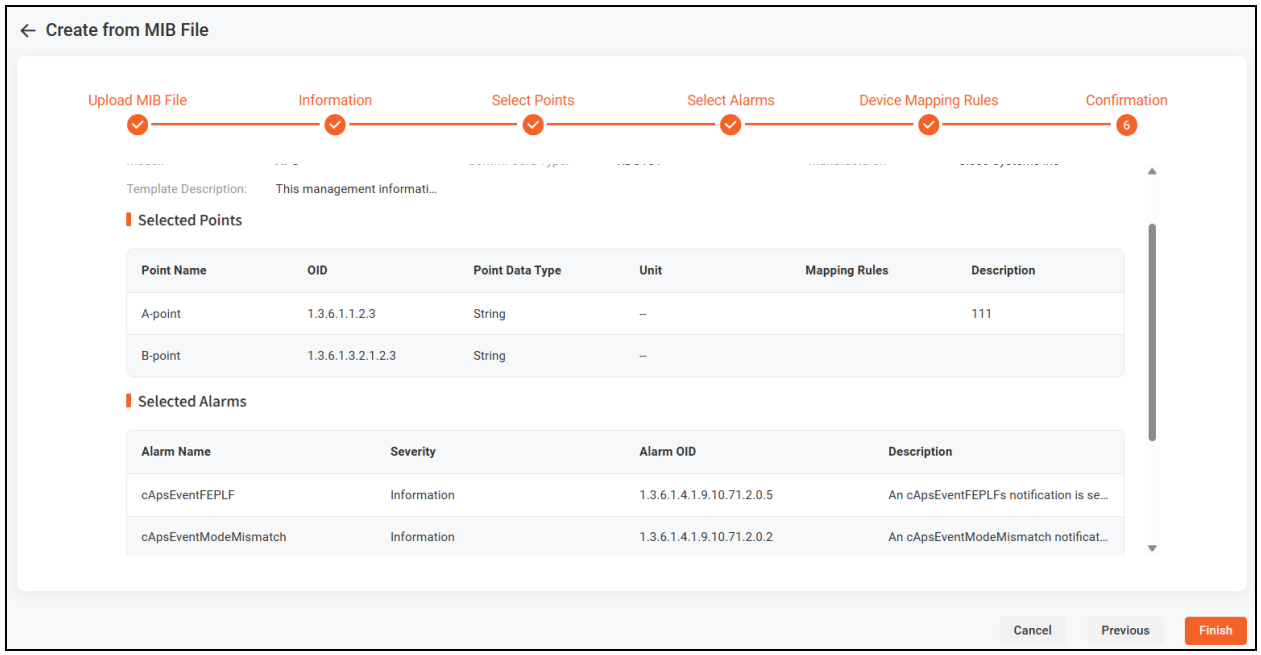
6. Previewing & Confirming

This page summarizes the configurations from the previous five steps, including basic info, selected data points, alarms, and mapping rules.

Review the information and click *Save*. The platform creates the template and prompts **Added successfully** before returning to the template list. (As shown in the **Figure 13.69** on the next page).

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.69 Previewing & Confirming the Template



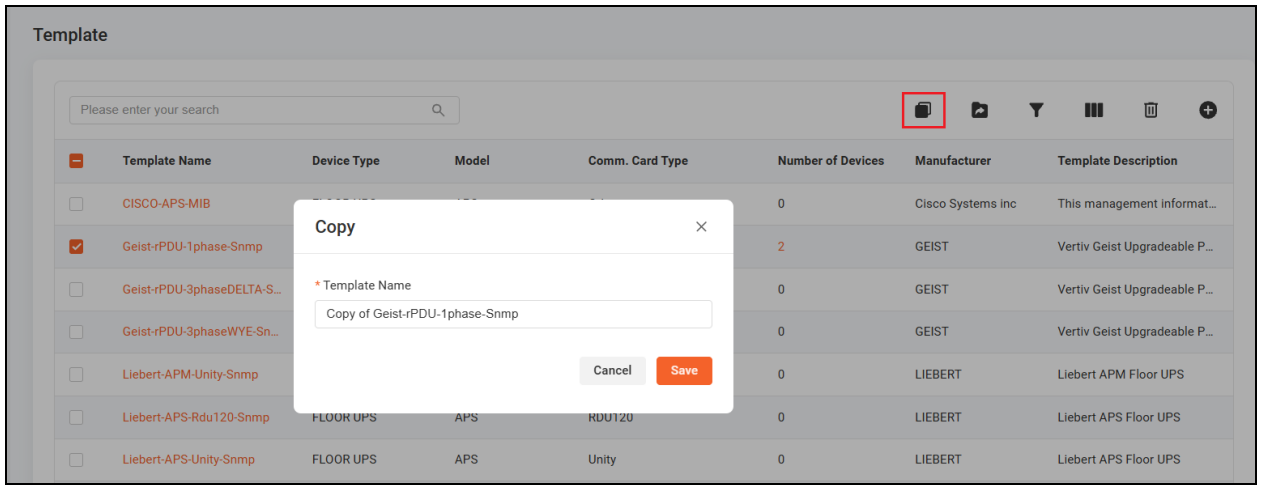
NOTE: The platform automatically creates a corresponding asset template under the relevant category. Devices monitored using this template will automatically associate with that asset template.

Click *Back* to return to Step 5 or *Cancel* to exit.

7. Copying the Template

On the **Data Collection Template Management** list page, select a template and click the **Duplicate** icon in the upper-right corner. (As shown in the **Figure 13.70** below).

Figure 13.70 Duplicate Template Icon



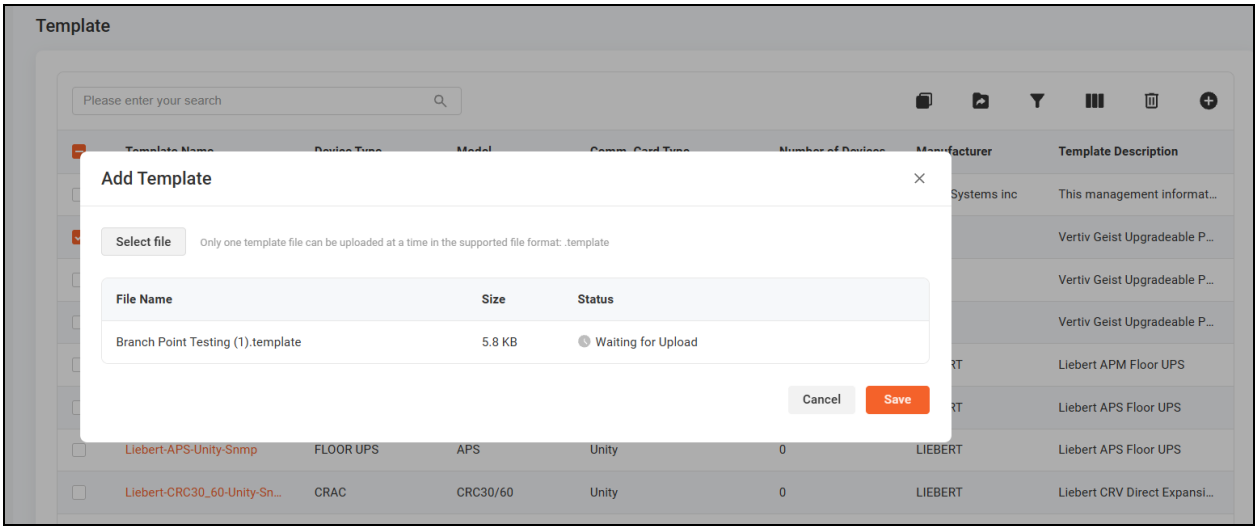
Template Name: Default is **Original Name - Copy**. You can modify this (1–64 characters). If a duplicate name exists, the platform appends (X) to ensure uniqueness. If the result exceeds 64 characters, the original name is truncated. Click *Save* to duplicate. The new template appears at the top of the list. Click *Cancel* to exit.

© 2026 Vertiv Group Corp. All Rights Reserved.

8. Importing the Template

On the **Data Collection Template Management** list page, click (+) and select Import Template, then click *Start*. (As shown in the **Figure 13.71** below).

Figure 13.71 Import Template Option



Instructional text: **Only one template file can be uploaded at a time. Supported format: .template**. Click *Select File* to choose a .template file.

- **Batch Limit:** Only one file per upload.
- **Format Requirement:** Only .template is supported.
- **Size Limit:** Maximum 5MB.

Click *Save* to upload. Upon success, the platform creates the template using the filename as the default template name. If data is corrupted, the platform prompts **Template file data error**. Upon successful import, the dialog box closes, and the new template appears at the top of the list. Click *Cancel* to exit.

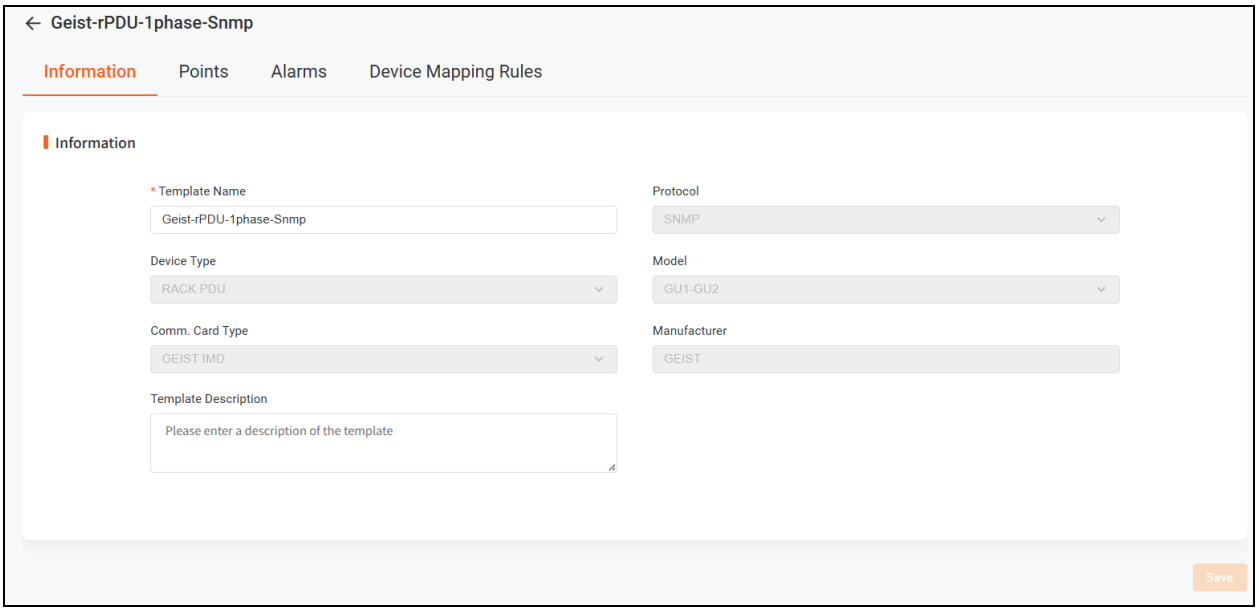
Editing a Template

1. Editing the Basic Information

In the **Data Collection Template Management** list, click a *template name* to enter the Edit Template page. The page title displays the current template name. Four tabs are provided: **Basic Information, Data Points, Alarms**, and **Device Mapping Rules**. The **Basic Information** tab is displayed by default. (As shown in the **Figure 13.72** on the next page).

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.72 Editing the Template - Basic Information



The **Basic Information** tab contains the following fields:

- **Template Name:** Mandatory. Displays the current template name. 1–64 characters. If left blank, the platform prompts **Must be 1–64 characters**. If the name duplicates an existing template, **Value already exists** is displayed.
- **Template Description:** Optional. 0–1000 characters.
- **Protocol:** Non-editable. Displays the communication protocol (default: SNMP).
- **Device Type:** Non-editable. Displays the associated device category.
- **Manufacturer:** Non-editable. Displays the equipment manufacturer.
- **Model:** Non-editable. Displays the equipment model.
- **Interface Card Type**: Non-editable. Displays the adapted communication card type.

After modifying the **Template Name** or **Template Description**, click *Save* in the bottom-right corner. The button will show a loading state during processing and return to a grayed-out state upon a successful **Saved successfully** notification.

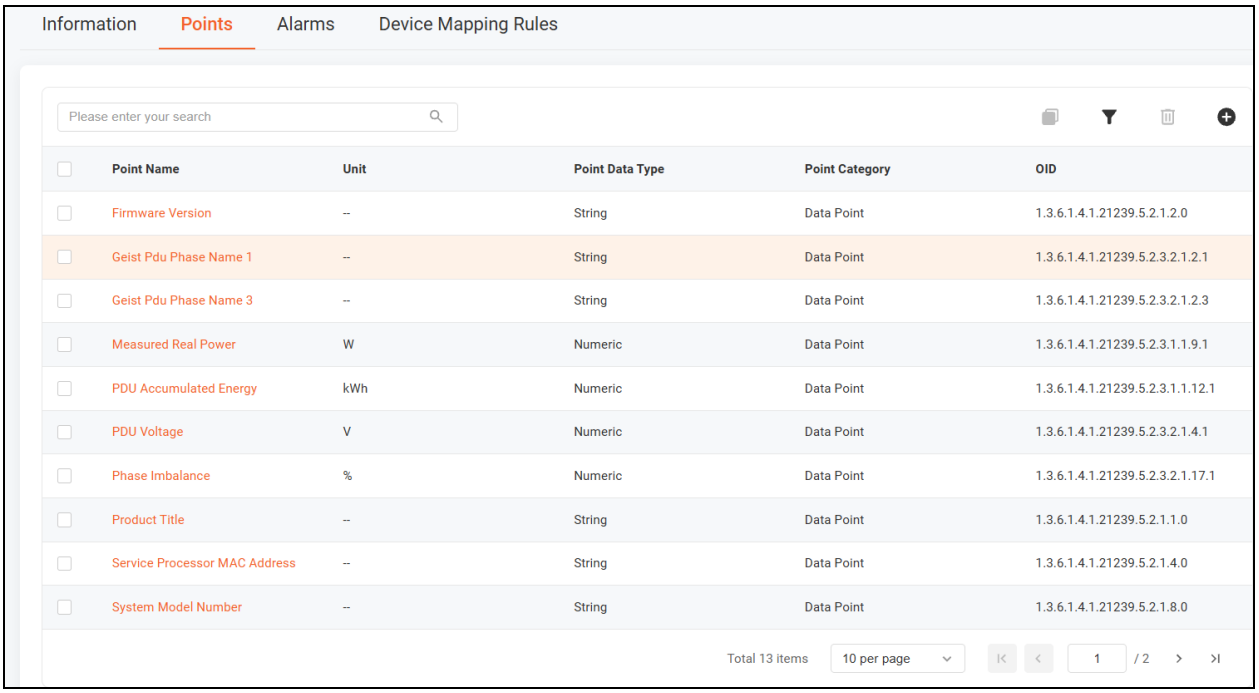
2. Editing the Data Points

Select the Data Points tab to manage the telemetry points for the template. All additions, modifications, or deletions are automatically synchronized to the Zero Engine.

NOTE: Changing a data point type or deleting a point will permanently remove all associated historical data stored on the devices. (As shown in the Figure 13.73 on the facing page).

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.73 Editing the Template Data Points



2.1 Data Point List Management

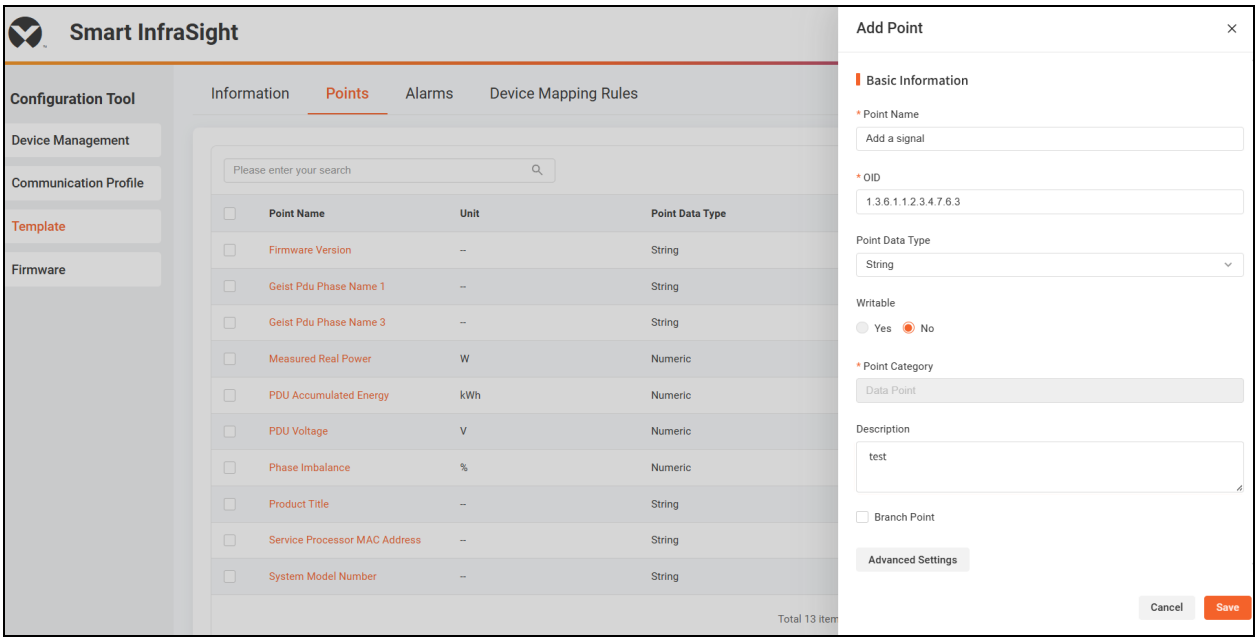
- **Search**: Use the top search box to perform fuzzy searches by Data Point Name or OID. Results are sorted by name in ascending order.
- **Filter**: Click the *Filter* icon to filter the list by Data Type or Category.
- **List View**: Displays **Data Point Name**, **Unit**, **Data Type, Category**, and **OID**. Click a *name* to open the edit interface.

2.2 Adding and Editing the Data Points

Click (+) icon to open the Add Data Point drawer and configure the Basic Information: (As shown in the **Figure 13.74** on the next page).

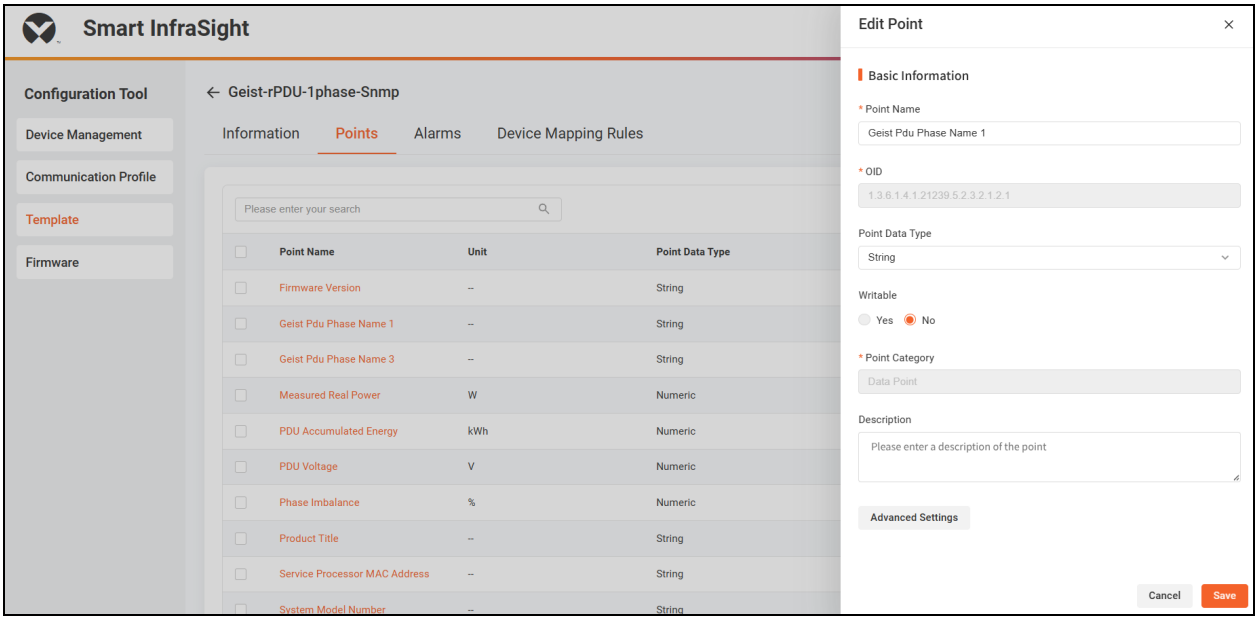
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.74 Adding the Data Point



Click on the *signal name* to open the editing interface. (As shown in the **Figure 13.75** below).

Figure 13.75 Editing the Data Points



- **Data Point Name:** Mandatory. 1–64 characters. Must be unique within the same template.
- **OID:** Mandatory. Default: 1.3.6.1. 1–128 characters. Supports dot (.) and pipe (|) characters.
- **Description:** Optional. 0–1000 characters.

© 2026 Vertiv Group Corp. All Rights Reserved.

- **History Interval:** Defines the storage policy. Options: Off, Every 1 hour, Every 30 minutes, Every 10 minutes, or Every 3 minutes. This is disabled if the Data Type is String.
- **Writable:** Select Yes or No to define control permissions.
- **Data Type:** Select Numeric, String, or Enumerated.
- **Category:** Automatically determined by the platform based on Writable status and Data Type:

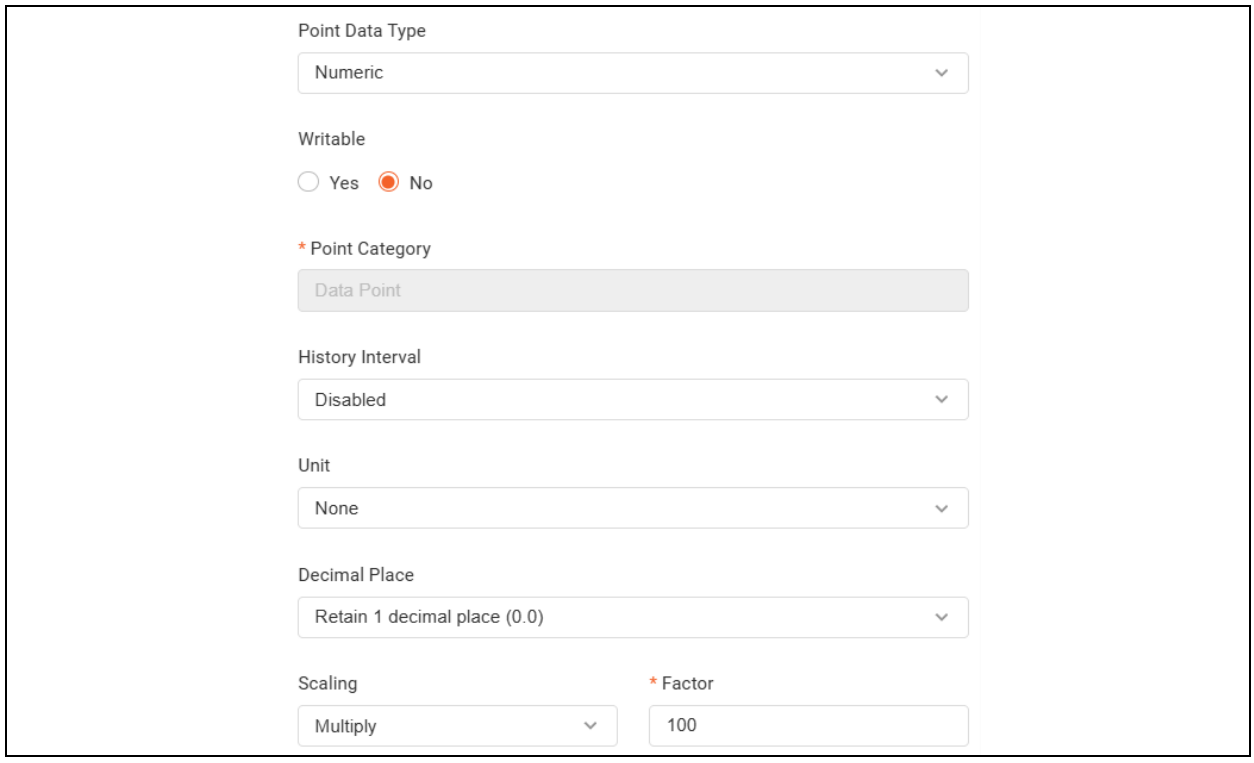
    1. If Writable is **No**, the category is **Data Point**.
    2. If Writable is **Yes** and the type is **Numeric** or **String**, the category is **Config Point**.
    3. If Writable is **Yes** and the type is **Enumerated**, the category is **Control Point**.

2.3 Type-Specific Configurations

- Numeric:

    1. **Unit**: Search by name or symbol in the drop-down list.
    2. **Decimal Place**: Set to 0–3 decimal places.
    3. **Scaling**: Supports None, **Multiply**, and **Divide**. If Multiply/Divide is selected, enter a Factor (1–9999). The platform calculates: Final Value = Original Value * Factor. (As shown in the **Figure 13.76** below).

Figure 13.76 Numeric Data Point Configuration



- Enumerated:

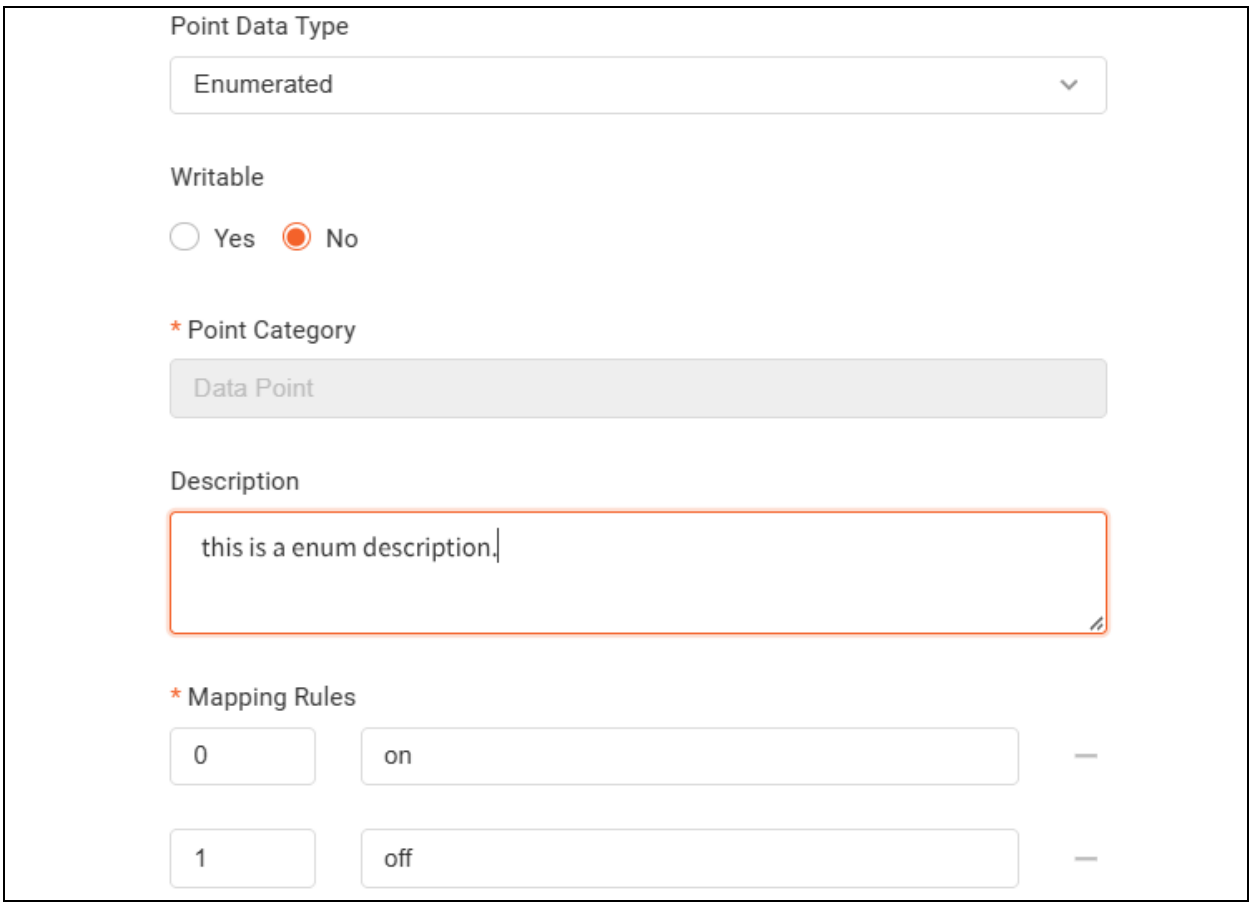
    1. Click *Add* to configure Mapping Rules. (As shown in the **Figure 13.77** on the next page)
    2. **Original Value:** Enter the integer returned by the device (0–99).

© 2026 Vertiv Group Corp. All Rights Reserved.

3. **Mapping Value:** Enter the status description (1–128 characters), e.g., **Running** or **Stopped**.

4. Supports up to 30 mapping rules.

Figure 13.77 Enumerated Data Point Mapping Rules



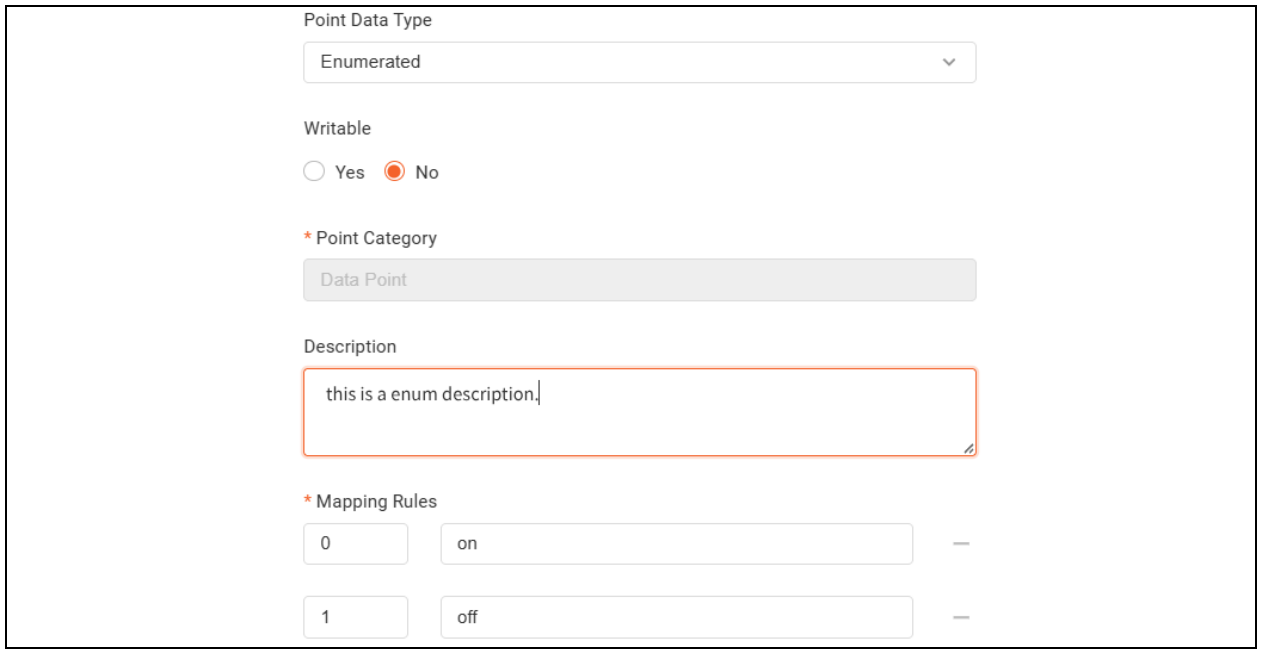
2.4 Branch Data Point Configuration

Check **Branch Data Point** to bulk-generate points with shared attributes:

- Enter the **Min Branch Index** (default: 1) and Max Branch Index (default: 100), ranging from 0 to 500.
- The platform auto-generates a list where names follow the **Root Name: branch XX** format and OIDs follow **Root OID.index**.
- Select the required branches and click *Save*. (As shown in the **Figure 13.78** on the facing page)

© 2026 Vertiv Group Corp. All Rights Reserved.

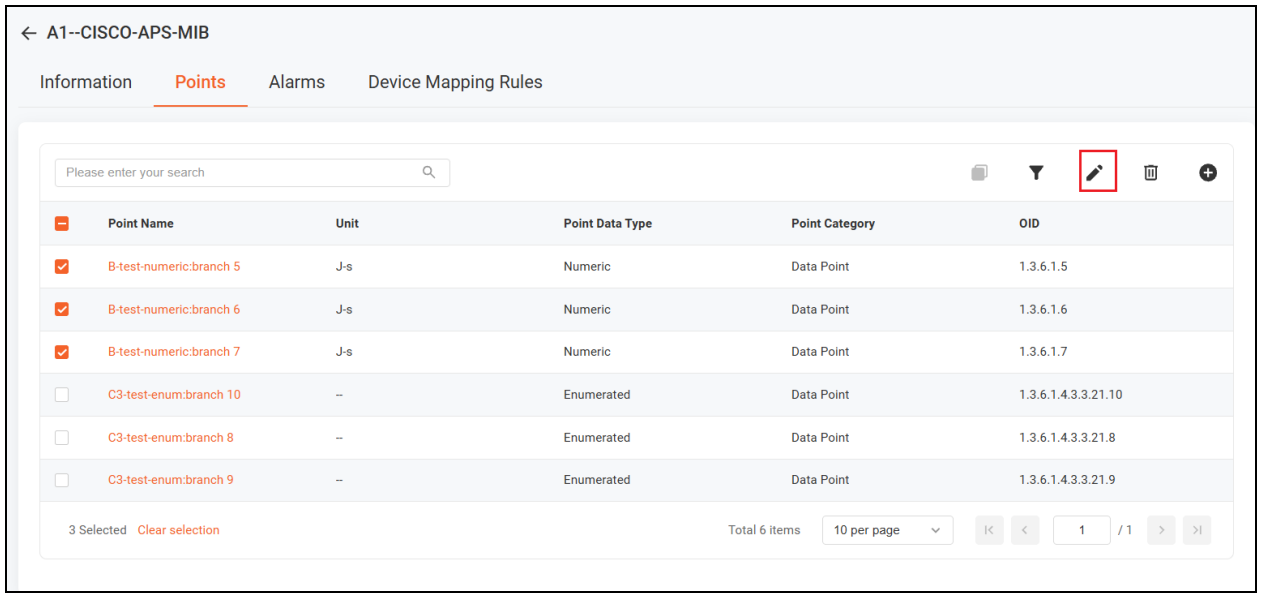
Figure 13.78 Branch Data Point Configuration



2.5 Bulk Edit Signals

In the Points list, select the checkboxes of the points to be edited in bulk. The number of selected points is displayed at the bottom of the page. Once the selection is complete, click the *Edit* (pencil icon) in the upper-right toolbar to open the Batch edit dialog. As shown in **Figure 13.79** below .

Figure 13.79 Batch Edit Data Points Dialog



The information banner shows the number of selected points affected by the changes.

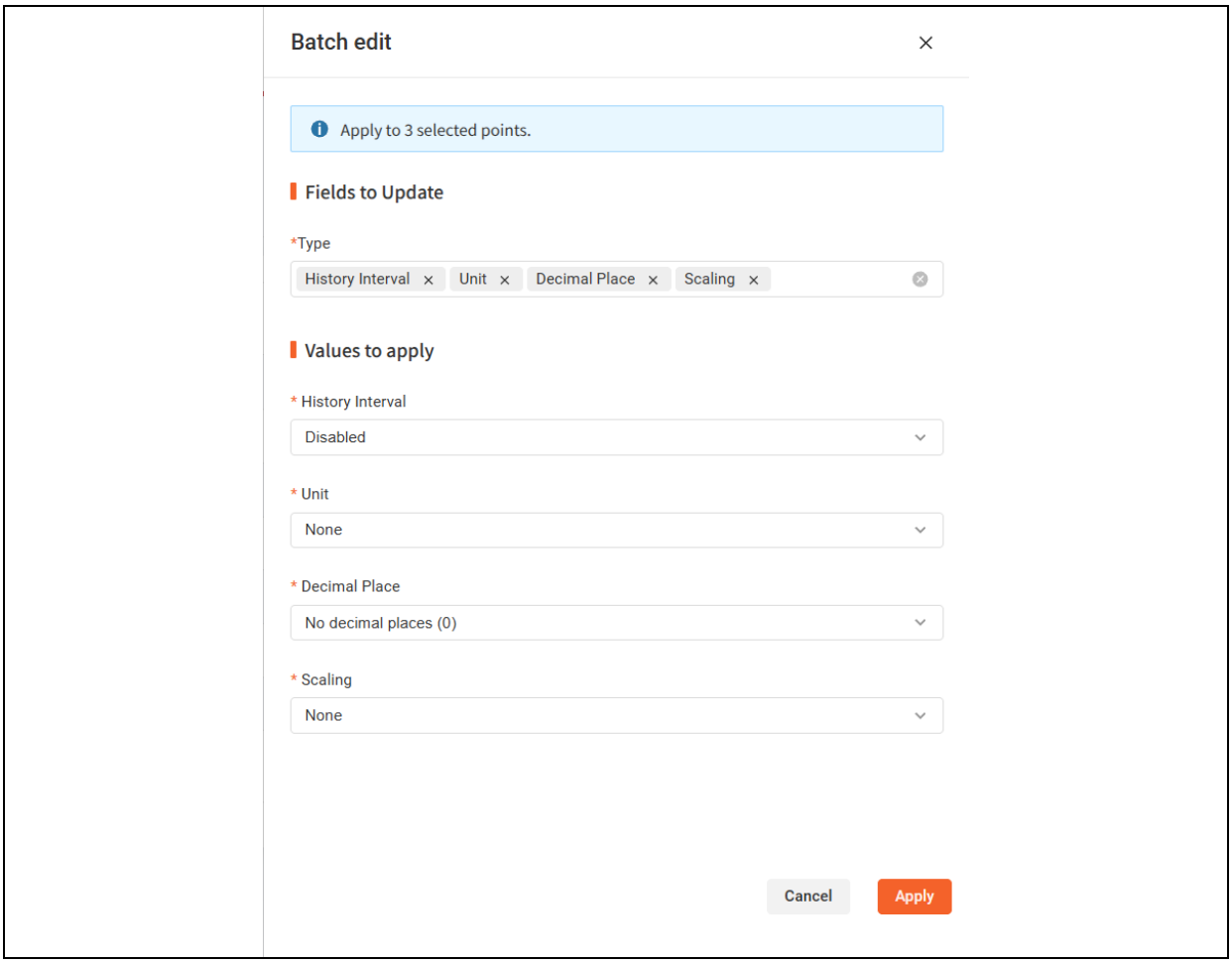
© 2026 Vertiv Group Corp. All Rights Reserved.

In the Fields to Update section, click the Type drop-down and select the fields to be modified in this batch operation. Only the selected fields appear in the Values to apply section below, unselected fields are hidden and their original values on each point remain unchanged.

In the Values to apply section, configure the target values according to the data type of the selected points:

For Numeric data points, the following fields are available:

Figure 13.80 Batch Edit Numeric Data Points

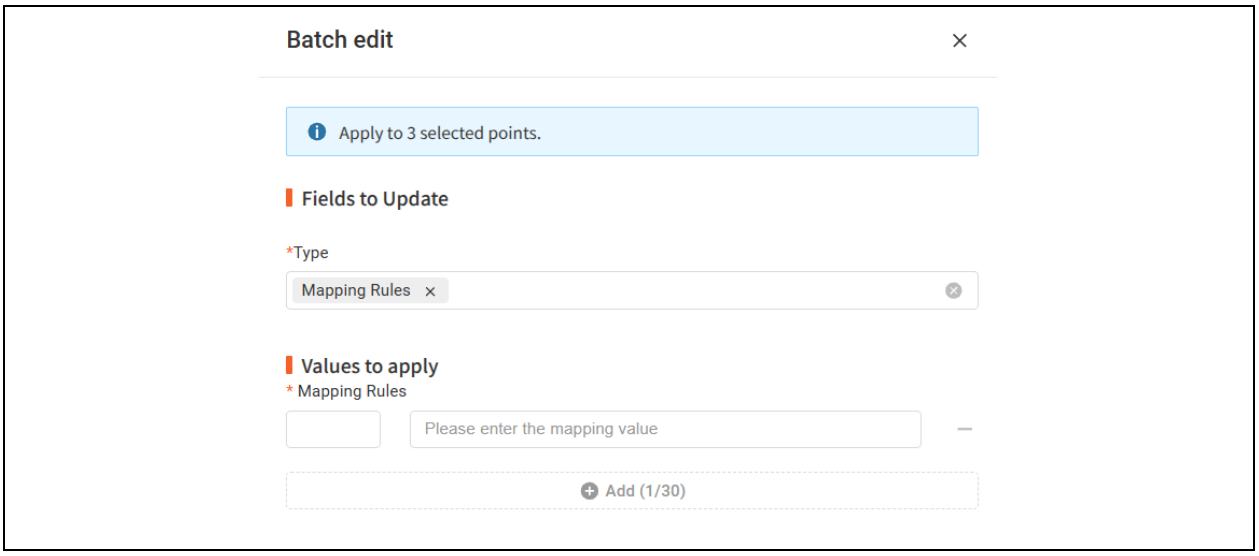


- **History Interval:** Sets the historical data collection interval. The drop-down options include Disabled and various time period options.
- **Unit:** Sets the engineering unit for the data points. Defaults to None.
- **Decimal Place:** Sets the number of decimal places displayed. Defaults to No decimal places (0).
- **Scaling:** Sets the value scaling factor. Defaults to None.

For Enumerated data points, the following field is available.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.81 Batch Edit Enumerated Data Points

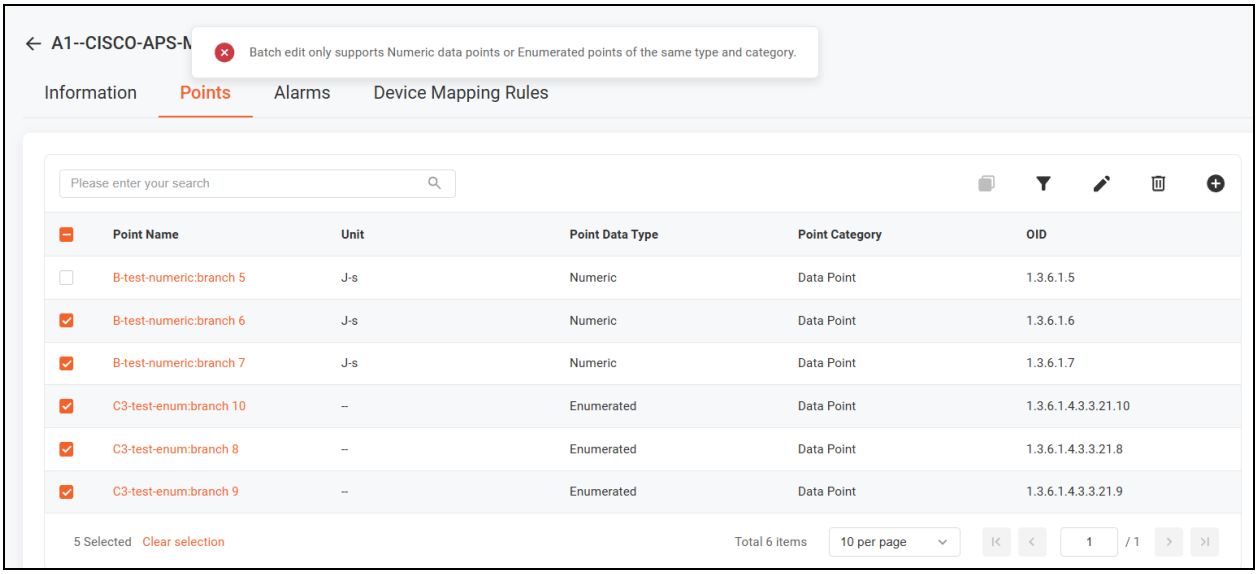


- **Mapping Rules:** Enter enumeration value and mapping text pairs row by row. Click *Add* to insert a new row. Up to 30 mapping rules can be added.

After confirming the settings, click *Apply* to submit. Click *Cancel* or the (X) in the upper-right corner to close the dialog without making any changes.

NOTE: Batch edit only supports Numeric data points or Enumerated data points of the same type and category. If the selected points contain a mix of different data types or include unsupported point types, an error message — Batch edit only supports Numeric data points or Enumerated points of the same type and category. — will appear at the top of the page and the Batch edit dialog will not open.

Figure 13.82 Batch Edit Error Prompt



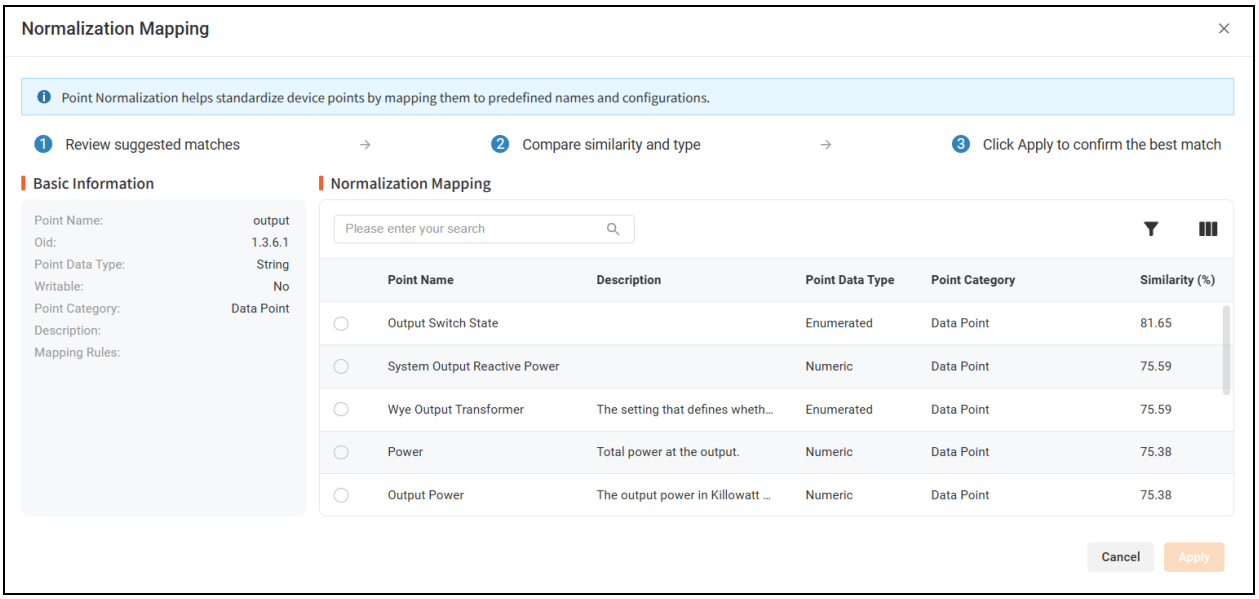
© 2026 Vertiv Group Corp. All Rights Reserved.

2.6 Advanced Settings (Normalization Mapping)

Click **Advanced Settings** to perform standardization:

- The platform retrieves matches from the standard library based on the current name.
- Review suggested matches, including description, type, category, and similarity percentage.
- Click *Apply* to auto-fill standardized configurations. Items already used in the template will be disabled. (As shown in **Figure 13.83** below).

Figure 13.83 Advanced Settings - Normalization Mapping



2.7 Copy and Delete Operations

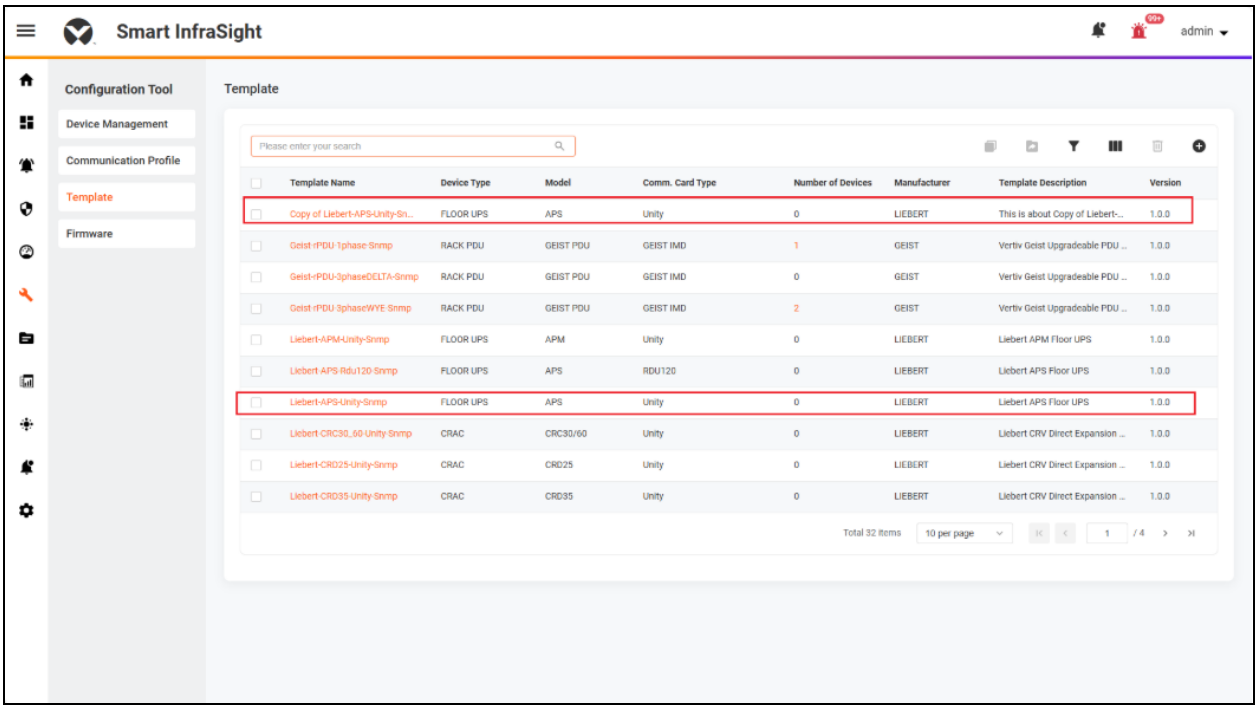
• **Copy**: Click the *Duplicate* icon in the Action Column to open the drawer with pre-filled information.

• **Delete**: Click the *Delete* icon for a single record, or select multiple records and click the *bulk Delete* icon at the top. Confirm in the dialog box to proceed.

• **Version:** The template version remains unchanged from the previous version after duplication. (As shown in the **Figure 13.84** on the facing page).

© 2026 Vertiv Group Corp. All Rights Reserved.

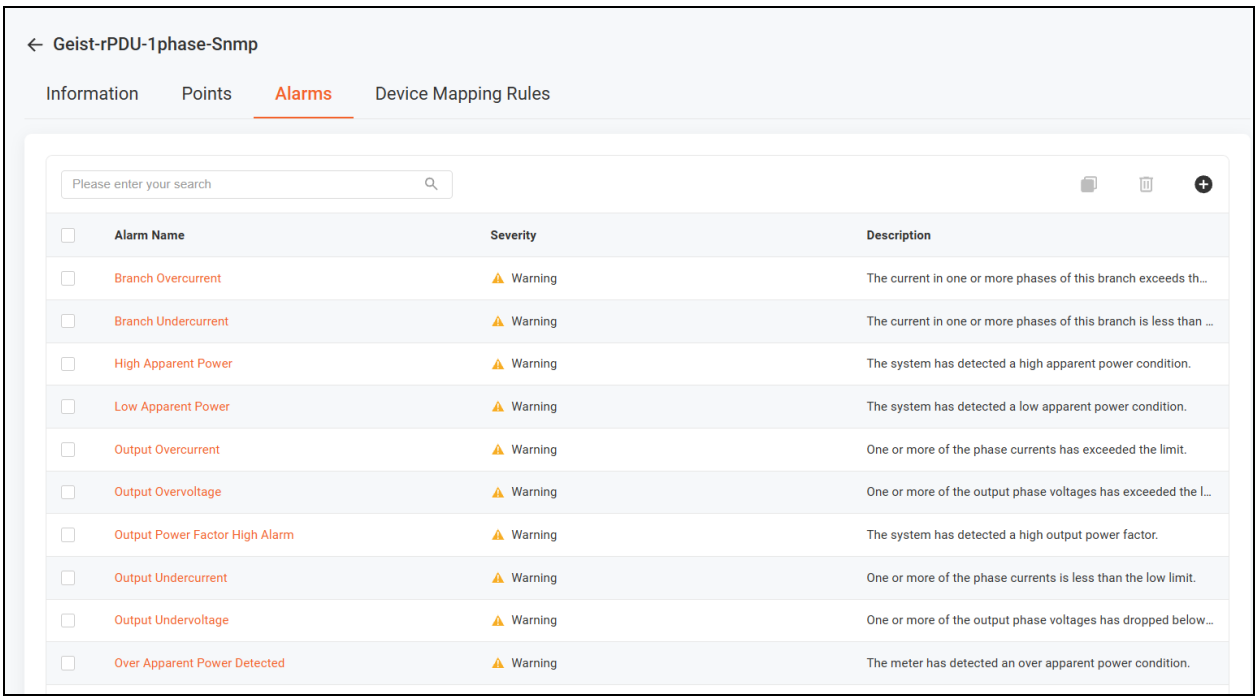
Figure 13.84 Copy Template



3. Edit Alarms

Select the **Alarms** tab to configure alarm items. Use the top search box for fuzzy searches by **Alarm Name**. (As shown in the **Figure 13.85** below).

Figure 13.85 Editing the Template - Alarms

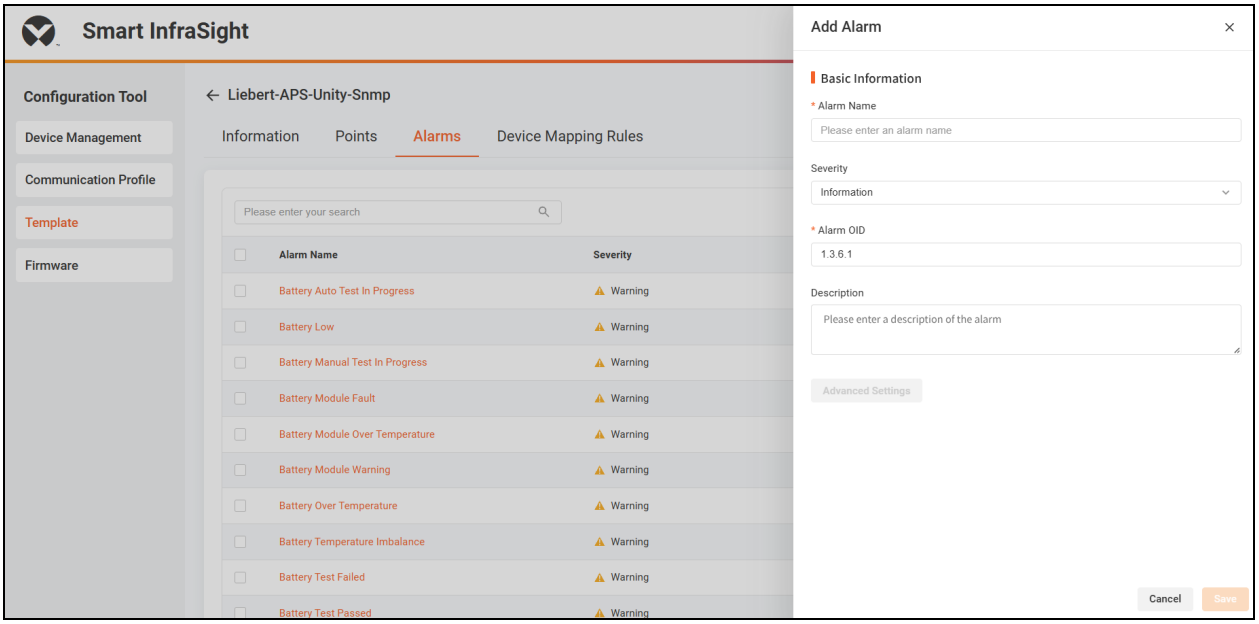


© 2026 Vertiv Group Corp. All Rights Reserved.

3.1 Adding an Alarm

Click (+) icon and configure the following in the **Add Alarm** drawer: (As shown in the **Figure 13.86** below).

Figure 13.86 Adding an Alarm Configuration



- **Alarm Name:** Mandatory. 1–64 characters. Must be unique.
- **Severity:** Select Information, Warning, or Critical.
- **Alarm OID:** Mandatory. Default: 1.3.6.1. Supports 1–128 characters and special characters (.) or (|).

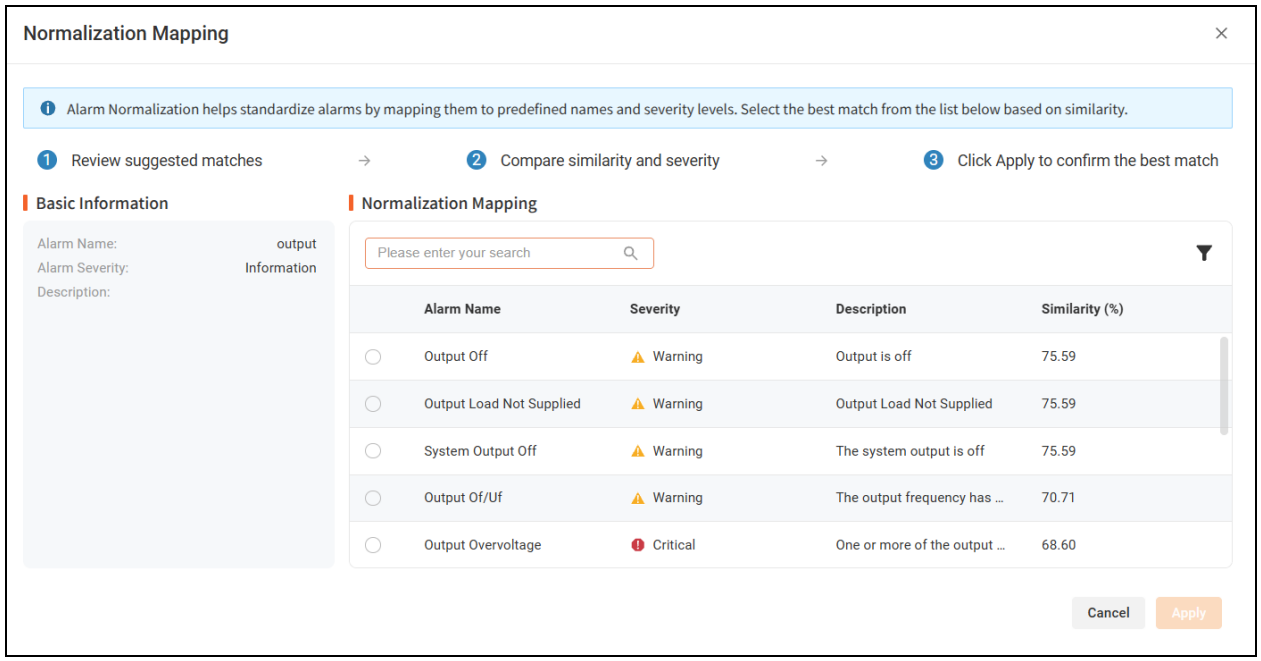
  NOTE: For Unity/RDU101/RDU120 interface cards, only this field is displayed.
- **Description:** Optional. 0–1000 characters.

3.2 Advanced Settings (Normalization Mapping)

Click *Advanced Settings* to calculate similarity with the standard library. Select the best match based on similarity (%) and click *Apply* to sync the name, severity, and description. (As shown in the **Figure 13.87** on the facing page).

© 2026 Vertiv Group Corp. All Rights Reserved.

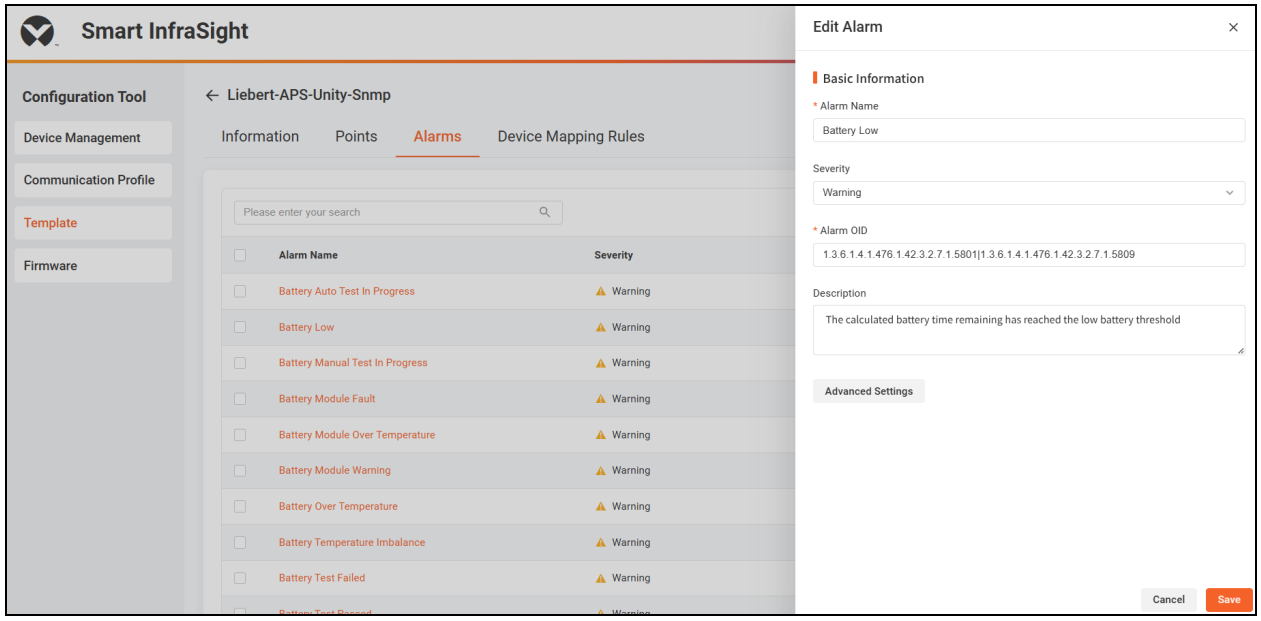
Figure 13.87 Alarm Normalization Mapping



3.3 Editing and Duplicating the Alarms

- **Edit:** Click an *alarm* name to modify settings. If the alarm has active instances on any device, the platform will block edits until all instances are cleared. (As shown in the **Figure 13.88** below).

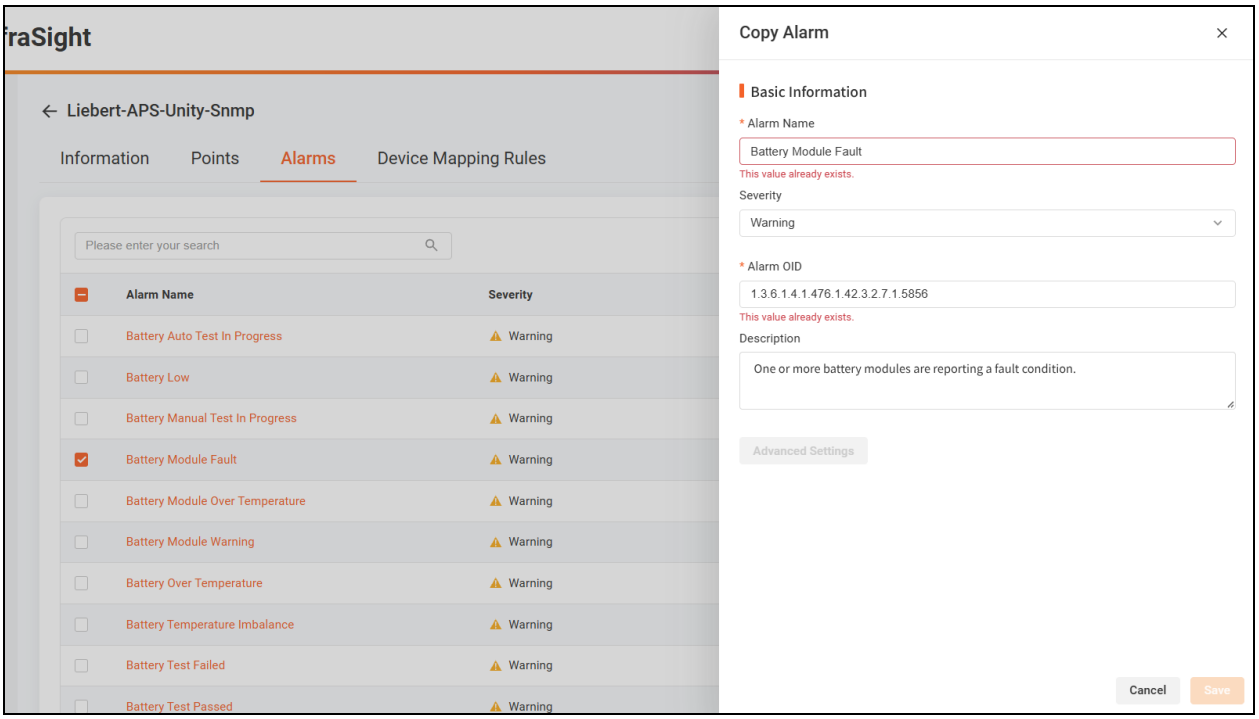
Figure 13.88 Editing the Alarm Configuration



- **Duplicate:** Click the *Duplicate* icon to pre-fill a new alarm form. You must change the name before saving. (As shown in the **Figure 13.89** on the next page).

© 2026 Vertiv Group Corp. All Rights Reserved.

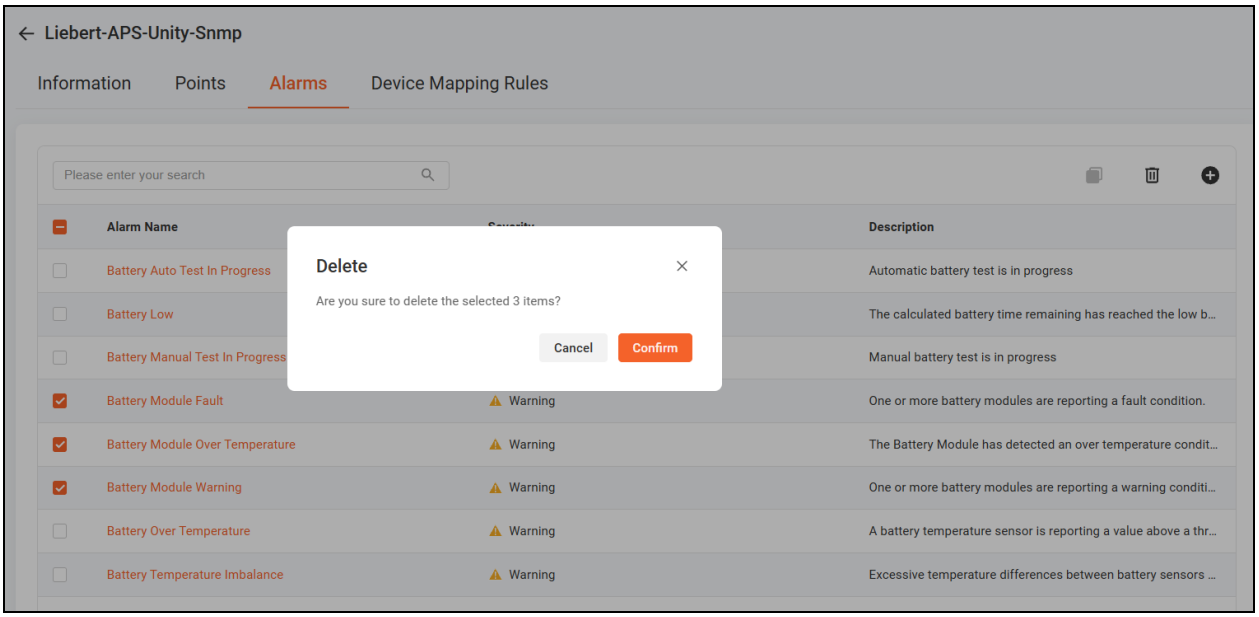
Figure 13.89 Duplicating an Alarm Configuration



3.4 Deleting an Alarm

Click the *Delete* icon for single or bulk deletion. The platform syncs the change to the Zero Engine and clears current active alarms while retaining historical records. (As shown in the **Figure 13.90** below).

Figure 13.90 Alarm Deletion Confirmation



© 2026 Vertiv Group Corp. All Rights Reserved.

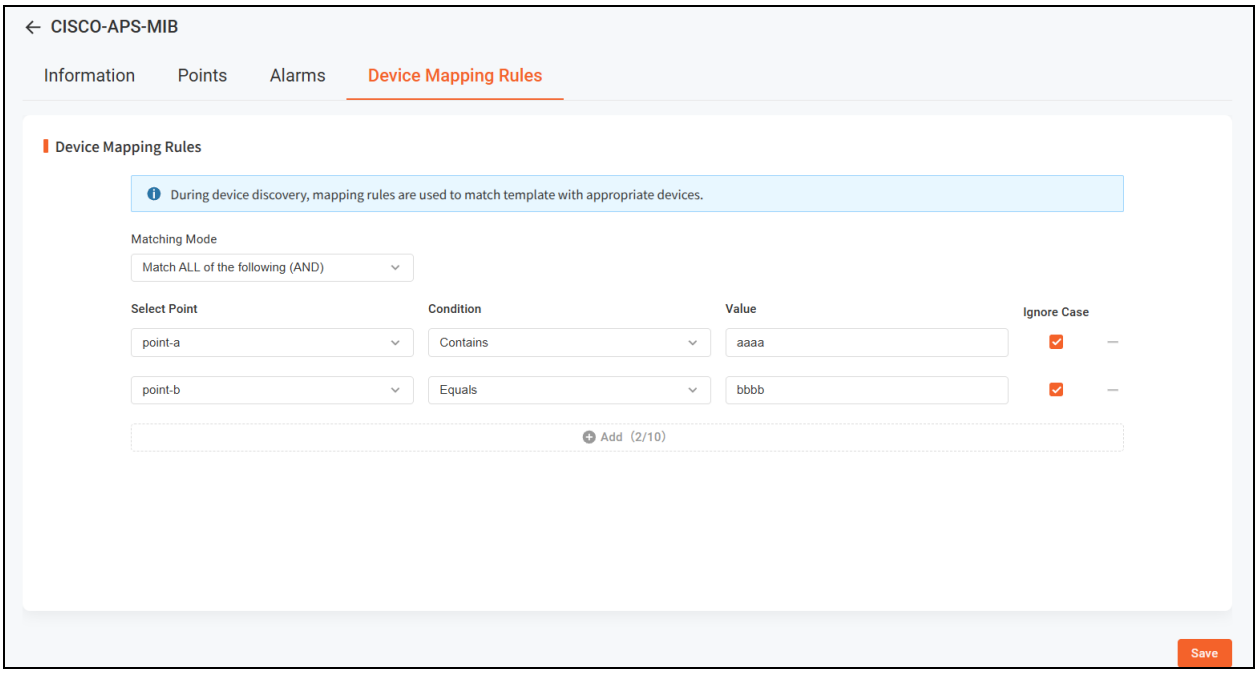
3.5 Specific Interface Card Configurations

- **GEIST IMD**: Configure Alarm Threshold Type (High/Low) and Specific-Trap.
- **Other SNMP**: Configure **Enterprise OID**, **Specific-Trap**, and **Variable Bindings** for both **Active Criteria** and **Clear Criteria**. Rules include: **Equals**, **Not Equals**, **Exists**, **Not Exists**, and **Contains**. **Ignore Case** is enabled by default.

4. Editing Mapping Rules

Select the **Device Mapping Rules** tab. These rules identify devices during the discovery process to match them with the correct template. (As shown in the **Figure 13.91** below).

Figure 13.91 Editing Template - Device Mapping Rules



4.1 Set Matching Mode

- **Match ALL of the following (AND):** Device must meet all conditions.
- **Match ANY of the following (OR):** Device must meet at least one condition.

4.2 Configure Conditions

Click *Add* to create up to 10 rules:

- **Select Point**: Choose a defined data point from the template.
- **Condition**: Options include **Equals**, **Contains**, **Exists**, **Not Exists**, and **Regex**.
- If **Exists** or **Not Exists** is selected, the **Value** and **Ignore Case** fields are disabled.
- If **Regex** is selected, **Ignore Case** is disabled.
- **Value:** Enter the matching string (1–64 characters).
- **Ignore Case:** Enabled by default to perform case-insensitive matching.

© 2026 Vertiv Group Corp. All Rights Reserved.

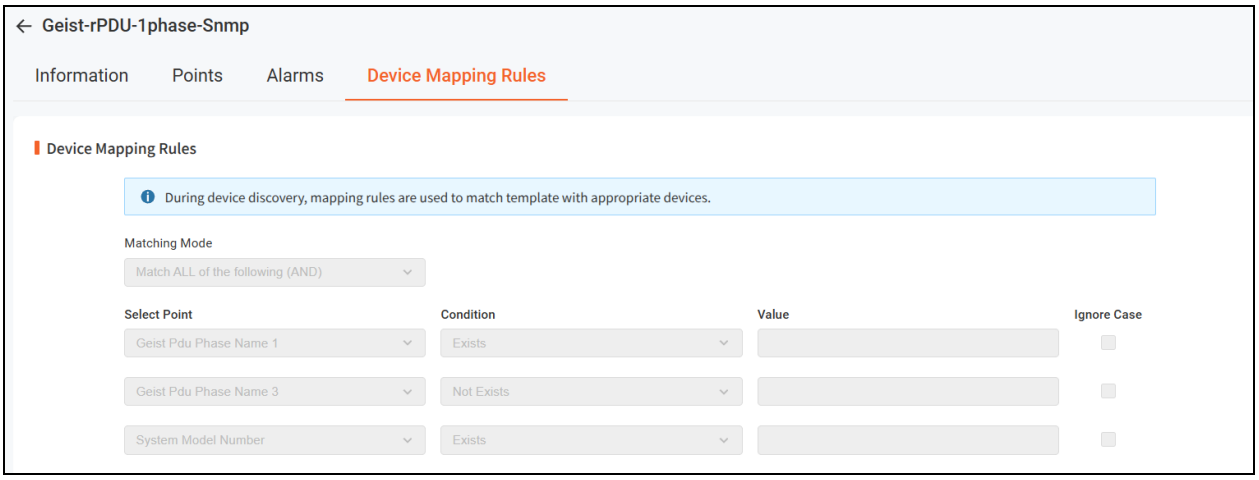
4.3 Save and Navigation Guard

- Click *Save* to apply changes. Click *Cancel* to revert to the last saved state.
- If you attempt to switch tabs or leave the page without saving, a **Tip** dialog box will appear: **The current changes are not saved. Are you sure you want to leave the current page?**

4.4 Constraints and Logic

- **Read-only Restriction:** Mapping rules for system-built-in templates or imported .template files are non-editable. (As shown in the **Figure 13.92** below).

Figure 13.92 Non-editable Mapping Rules



- **Matching Priority:** During discovery, the platform checks templates sequentially. The first template with matching rules is applied, and the search stops.
- **Permissions**: Only users with **Manage Template** permissions can edit these rules.

13.2.4 Firmware

The Firmware page is located under the Configuration Tool module and is used to centrally manage all device firmware files imported into the platform.

Firmware List

After navigating to the Firmware page, the main area displays all firmware records currently in the platform as a list. The list columns include **Name, Model, Version, Revision Date, Author, Latest, Notes,** and **Actions**.

Search: Enter a keyword in the Search field above the list. The platform performs a full-field match search across all columns and filters the results in real time.

Actions: In the Actions column, click on the ellipses (⋮) on the corresponding firmware row to expand the action menu, which includes the following options:

View Details: Navigate to the details page of the firmware to view its complete information.

Edit: Navigate to the edit page to modify the firmware's basic information.

Delete: Delete the firmware record.

Download: Download the firmware file to your local machine.

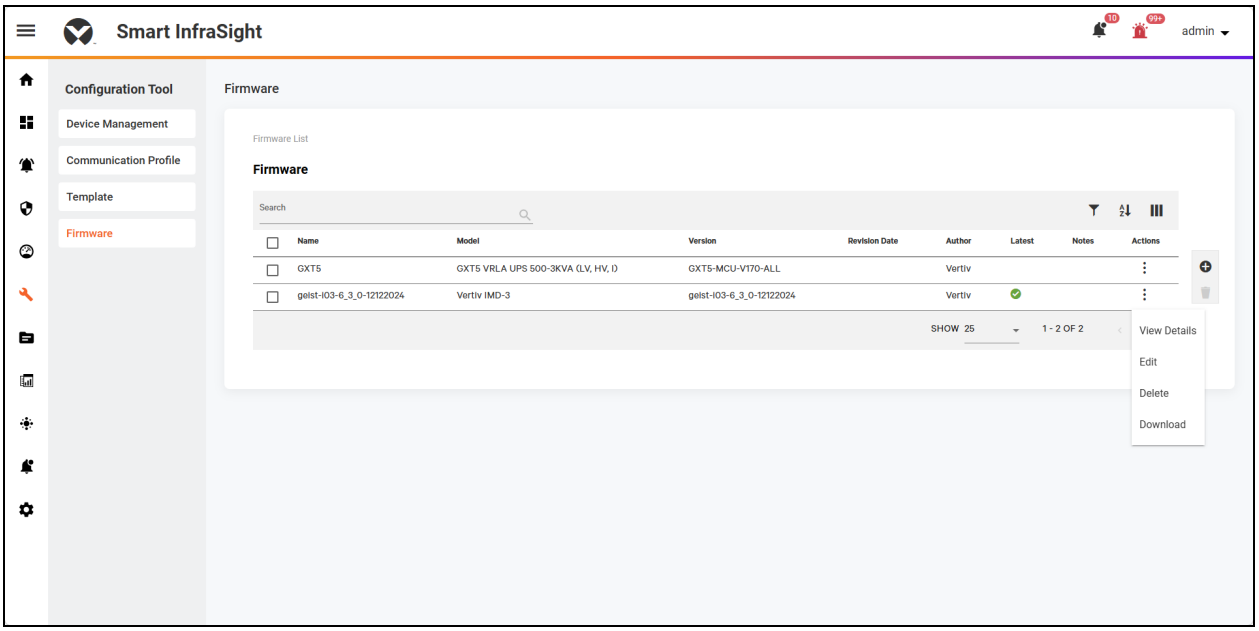
© 2026 Vertiv Group Corp. All Rights Reserved.

Pagination: The bottom of the list displays the current page range and total record count (e.g., **1 - 2 OF 2**). Use the SHOW drop-down list to adjust the number of records displayed per page, with a default of 25 records per page. Click the pagination arrows to navigate between pages.

Add Firmware: On the Firmware List page, click (+) icon on the right side of the list to navigate to the Add Firmware page.

Delete Selected: Select one or more firmware records by checking the checkboxes on the left side of the list, then click *Delete* Selected on the right side of the list. The platform will batch delete all selected firmware records. Check the *checkbox* in the list header to select all records on the current page at once.

Figure 13.93 Firmware List - Selected Deletion



Filter: Click the *filter* icon to the right of the Search field. A filter condition row expands above the list, containing the following three configuration fields:

Filter Type: Use the drop-down list to select the field to filter by. Available options include **Name, Model, Version, Revision Date, Latest, Notes**, and **Author**.

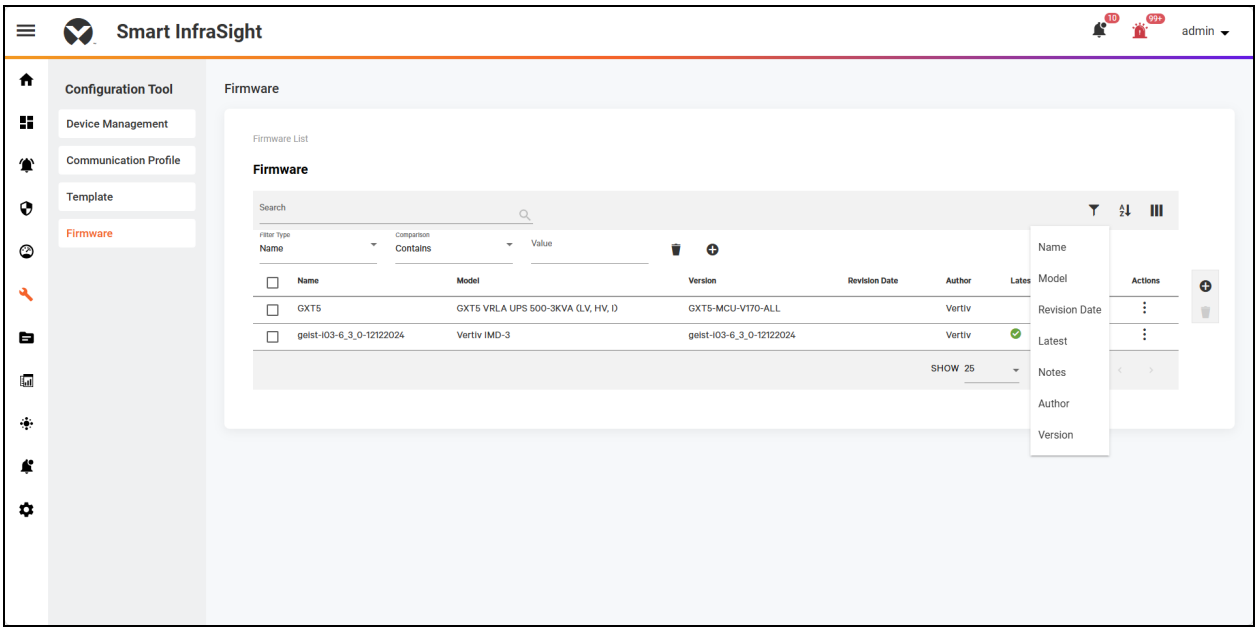
Comparison: Use the drop-down list to select the matching method. The default is **Contains**.

Value: Enter the specific filter value in the input field.

Once configured, the list automatically refreshes and displays only the firmware records that meet the specified conditions. Click (+) icon on the right side of the filter condition row to add a new filter rule for multi-condition filtering, as shown in **Figure 13.94** on the next page . Click the *trash can* icon to remove the corresponding filter condition row.

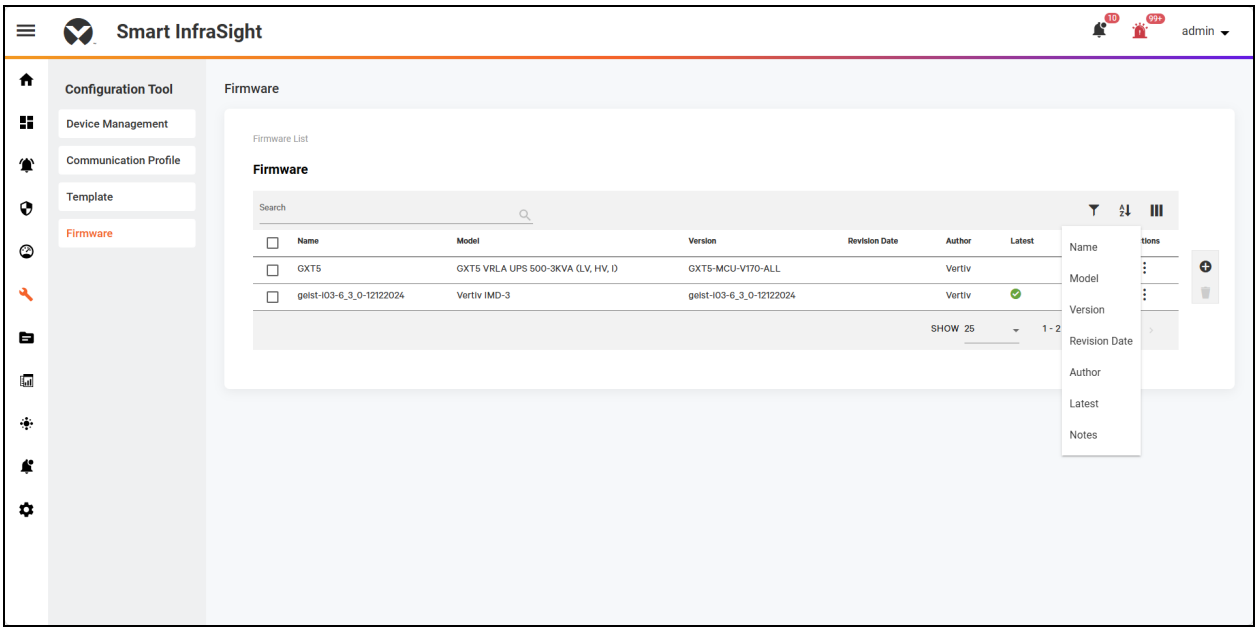
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.94 Firmware List Filter



Sort: Click the *sort* icon to expand the sort field drop-down list. Available fields include **Name, Model, Version, Revision Date, Author, Latest**, and **Notes**. Once a field is selected, the list sorts all firmware records by that field. As shown in **Figure 13.95** below .

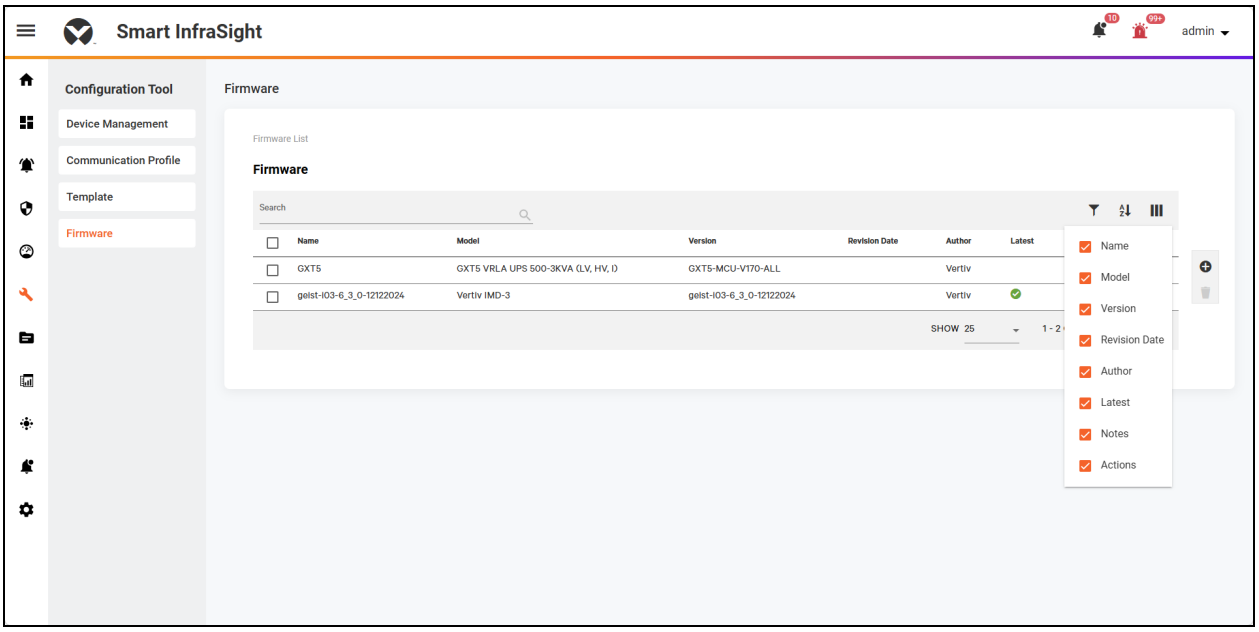
Figure 13.95 Firmware List Sort



Columns: Click the *columns* icon to expand the column visibility control panel, which lists all available columns: **Name**, **Model**, **Version**, **Revision Date**, **Author**, **Latest**, **Notes**, and **Actions**. Each column has a checkbox preceding it. A checked checkbox indicates the column is visible in the list; unchecking it hides the corresponding column. By default, all columns are checked. As shown in **Figure 13.96** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 13.96 Firmware List Columns



Add Firmware

On the Firmware List page, click (+) to navigate to the Add Firmware page. The left side of the page contains the firmware information fields, and the right side contains the firmware file upload area. The fields are described as follows:

Name (required): Enter the name of the firmware.

Version (required): Enter the version number of the firmware. Check Latest to mark this firmware as the latest version for the selected model.

Model (required): Use the drop-down list to select the device model corresponding to the firmware. Available models are grouped by product series as follows:

GXT5 :

- GXT5
- GXT5 VRLA
- GXT5 VRLA UPS 500-3KVA (LV, HV, I)
- GXT5 VRLA UPS 5KVA-10KVA (MV)
- GXT5 VRLA UPS 15KVA-20KVA (MV)
- GXT5 VRLA UPS 5KVA-10KVA (HV, I)
- GXT5 VRLA UPS 16KVA-20KVA (I)
- GXT5 Li-Ion
- GXT5 Lithium-Ion UPS 1000-3000VA (LV, I)
- GXT5 Lithium-Ion UPS 5KVA-10KVA (MV)

IntelliSlot :

- Liebert IntelliSlot Unity Card
- Liebert IntelliSlot RDU101 Card

© 2026 Vertiv Group Corp. All Rights Reserved.

- Liebert IntelliSlot RDU120 Card

IMD :

- Vertiv IMD-3
- Vertiv IMD-5

Revision Date (optional): Click the calendar icon to select the revision date of the firmware.

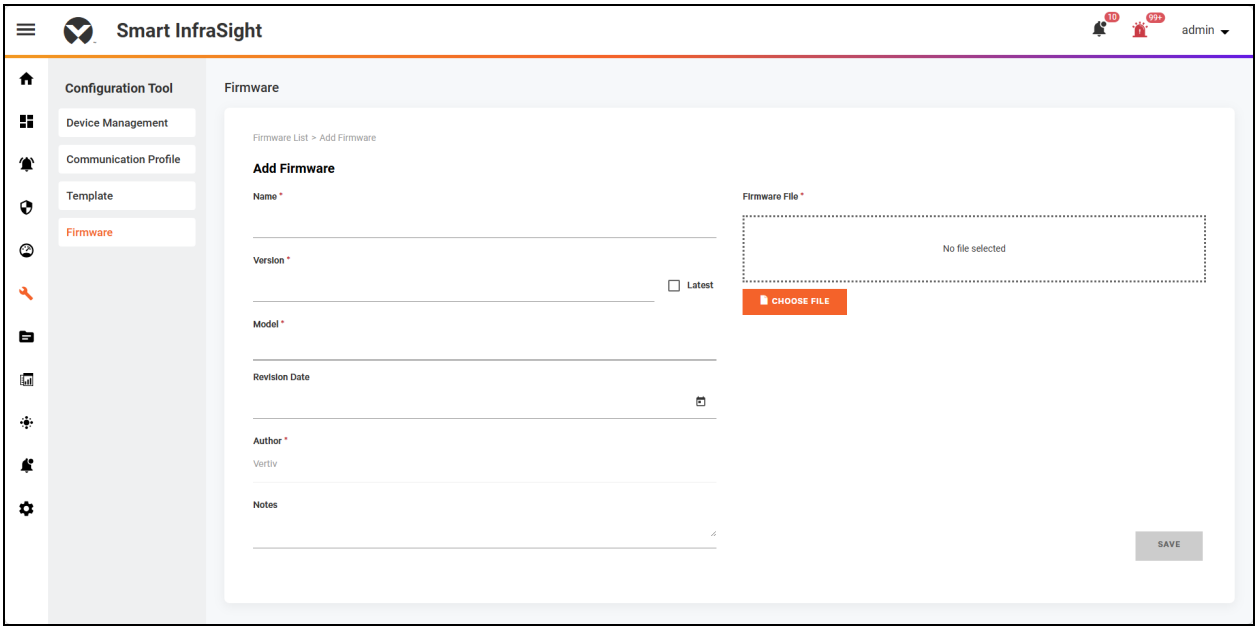
Author (required): Defaults to Vertiv and cannot be modified.

Notes (optional): Enter any additional information or remarks about the firmware.

Firmware File (required): Click Choose File in the upload area on the right to select a firmware file from your local machine. Once uploaded successfully, the file name is displayed in the upload area.

After completing all required fields and uploading the firmware file, click *Save* in the bottom-right corner of the page to finish adding the firmware. As shown in **Figure 13.97** below .

Figure 13.97 Adding Firmware



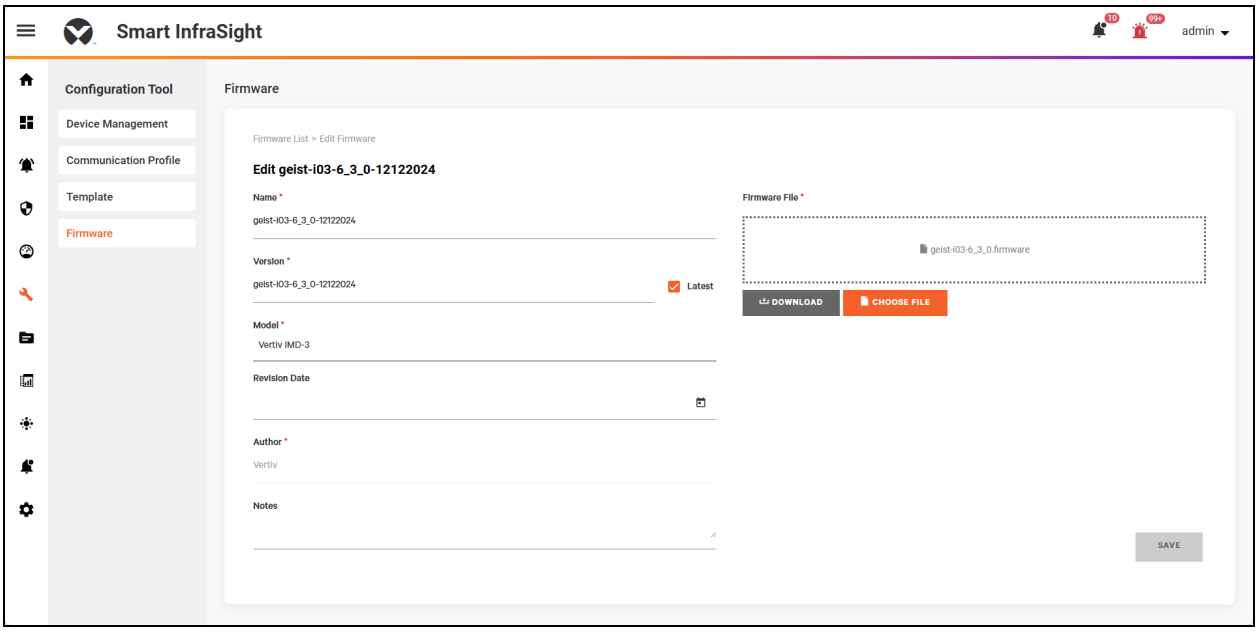
Editing Firmware

In the **Actions** column, click on the ellipses (⋮) on the corresponding firmware row, then click *Edit* in the action menu to navigate to the Edit Firmware page. The page layout and field structure are identical to the Add Firmware page. All current values are automatically populated in their respective fields. The **Author** field defaults to Vertiv and cannot be modified.

Edit the fields as needed. To replace the firmware file, click *Choose File* in the upload area on the right to upload a new file. To download the currently associated firmware file, click *Download*. Once all modifications are complete, click *Save* in the bottom-right corner of the page to submit the changes. As shown in **Figure 13.98** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

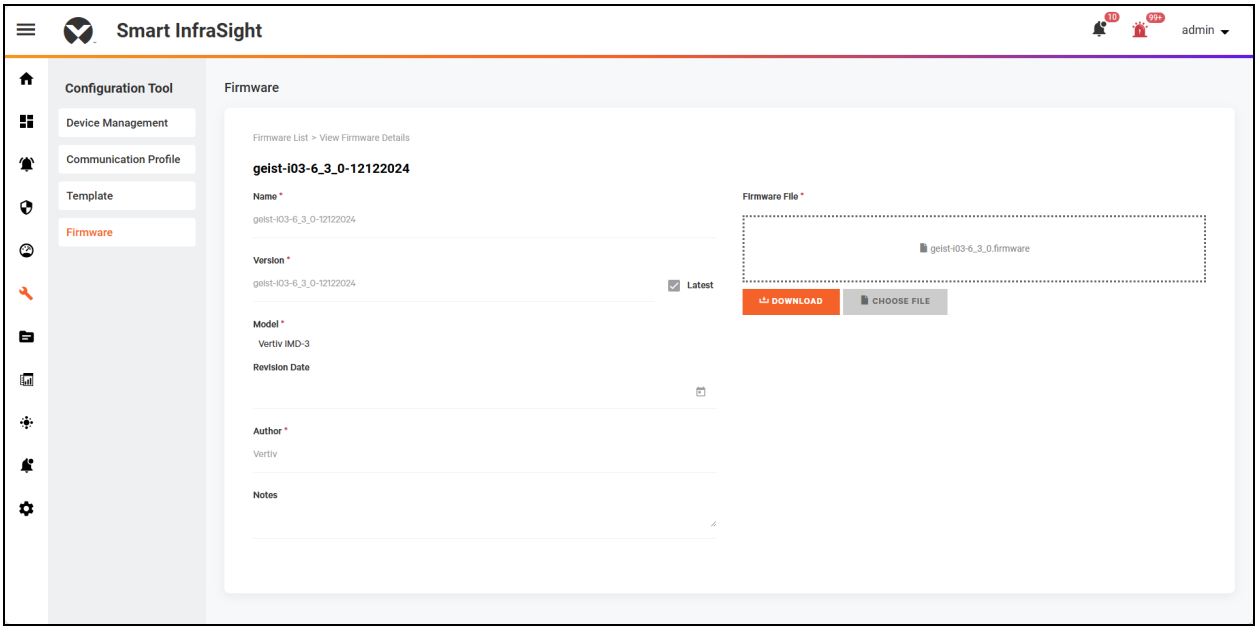
Figure 13.98 Editing the Firmware



Viewing the Firmware Details

In the Actions column, click on the ellipses (⋮) on the corresponding firmware row, then click *View Details* in the action menu to navigate to the Firmware Details page. The page displays the complete information of the firmware in read-only format, including **Name, Version, Latest status, Model, Revision Date, Author, Notes**, and the associated **Firmware File** on the right. All fields are non-editable, and **Choose File** is grayed out. To download the current firmware file, click *Download* below the upload area on the right. As shown in **Figure 13.99** below .

Figure 13.99 Viewing the Firmware Details



© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

14 Asset Management

14.1 General

14.1.1 Overview

Asset management in Vertiv™ 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.

14.1.2 Functional modules

Refer to this manual for the detailed description of the following functional modules of asset management in Detailed Features below.

- Add an Asset
- Asset Import
- Asset Export
- Review Assets
- Edit the Asset
- Delete the Asset
- Warranty Notifications
- Asset rack and de-rack records

14.2 Detailed Features

14.2.1 Asset Management

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 14.1** 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 Vertiv™ SmartAisle™ 3 sites.

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 number, 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 14.1 Adding an Asset

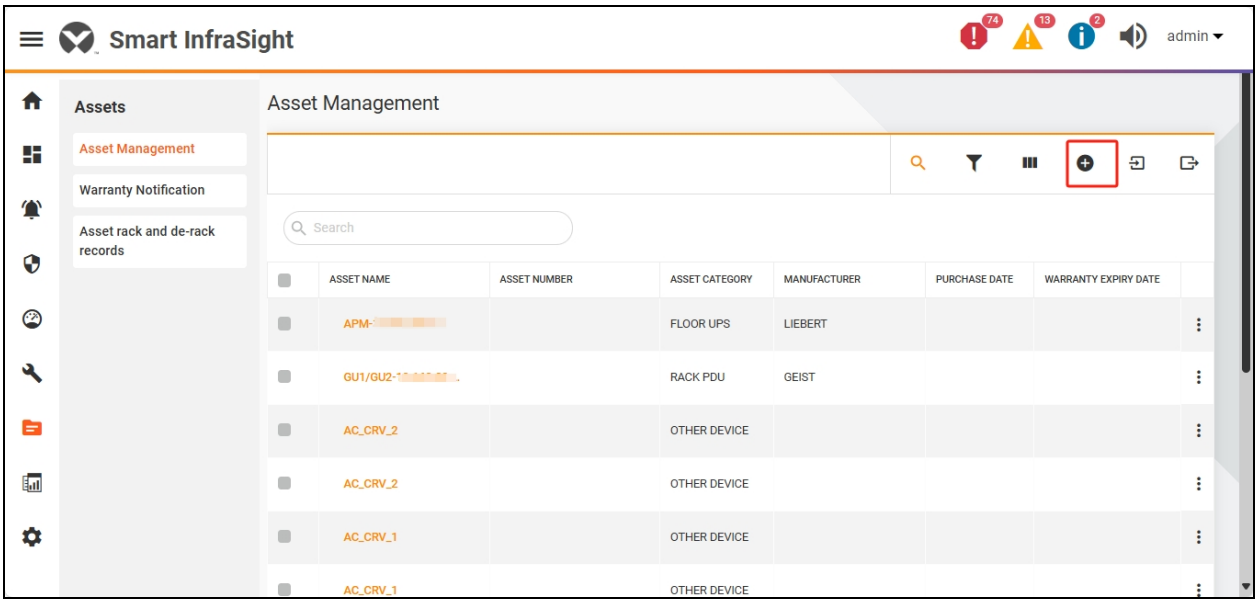
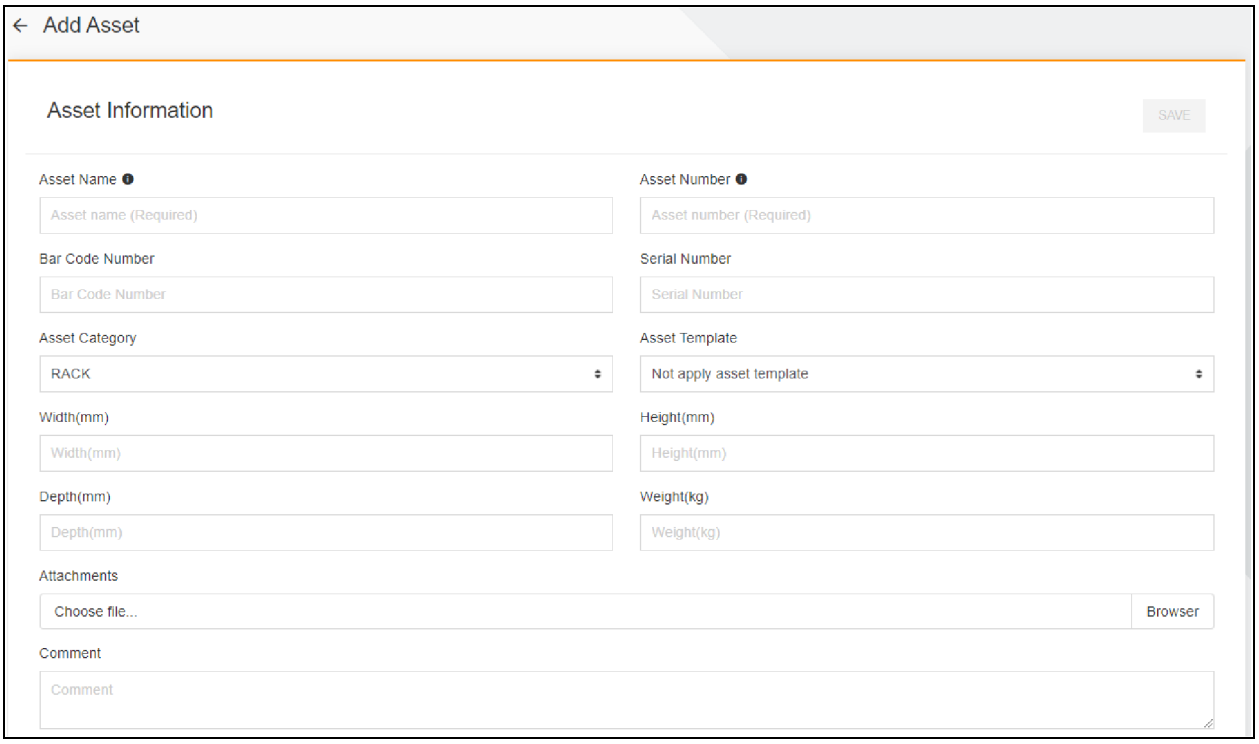


Figure 14.2 Adding an Asset - Attachment and Location



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 14.3** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 14.3 Asset Import



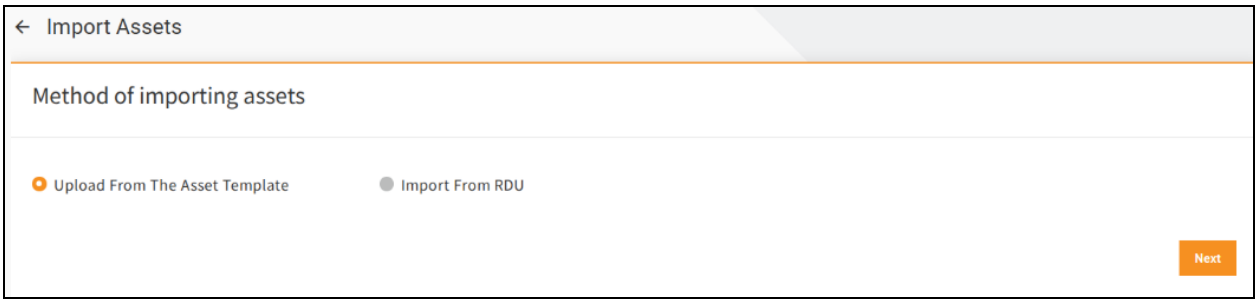
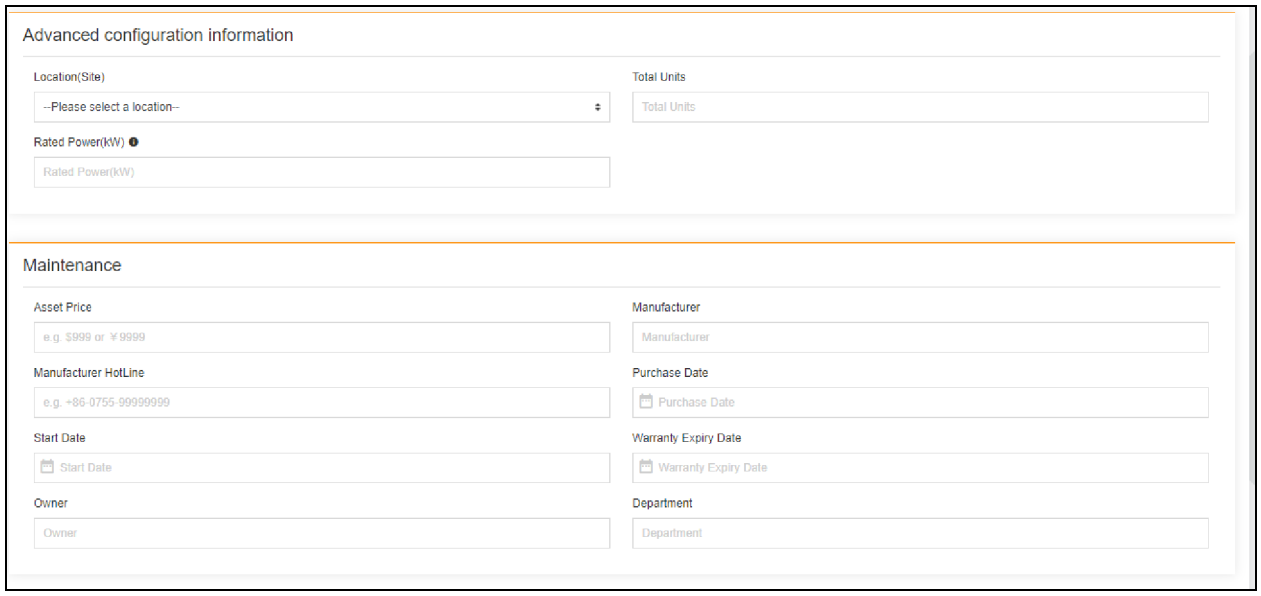


Figure 14.4 Asset Import - Selecting a File



© 2026 Vertiv Group Corp. All Rights Reserved.

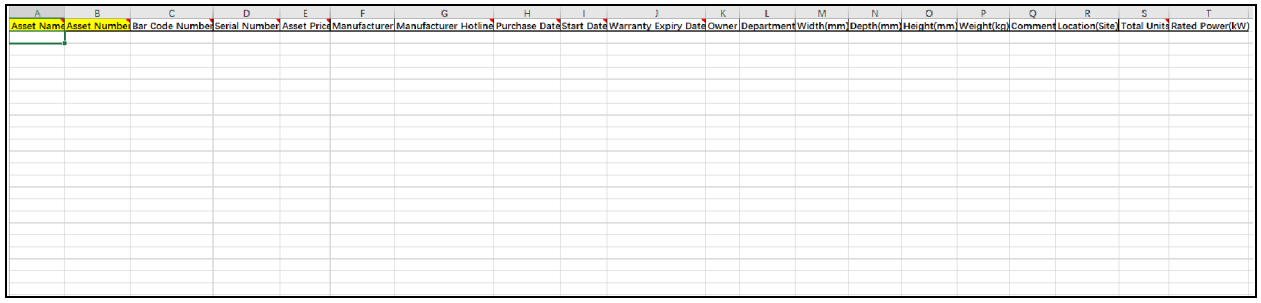
Figure 14.5 Asset Import Successful



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 asset numbers are unique. And then click *Browse* to select your completed Excel file, then click *Import*.

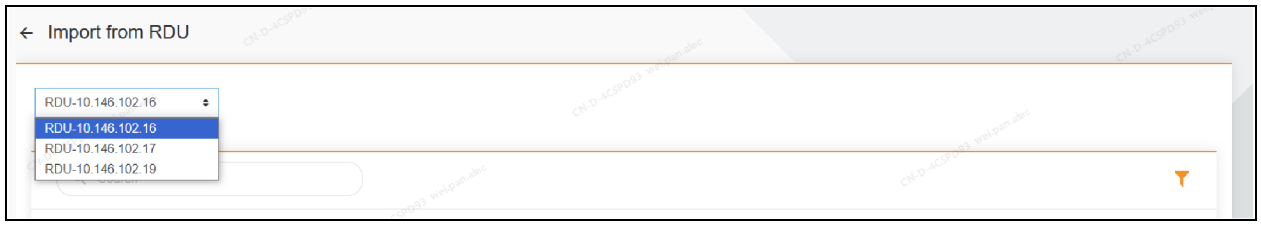
NOTE: The cabinet/battery cabinet cannot be imported to Vertiv™ SmartAisle™ 3 sites.

Figure 14.6 Asset List



If you choose to import from RDU as shown in **Figure 14.7** below , click *Next* to enter the import from RDU interface. There is an RDU selection box at the top; you can import assets from different RDUs, and the asset list only shows assets with a U-position height above 0.

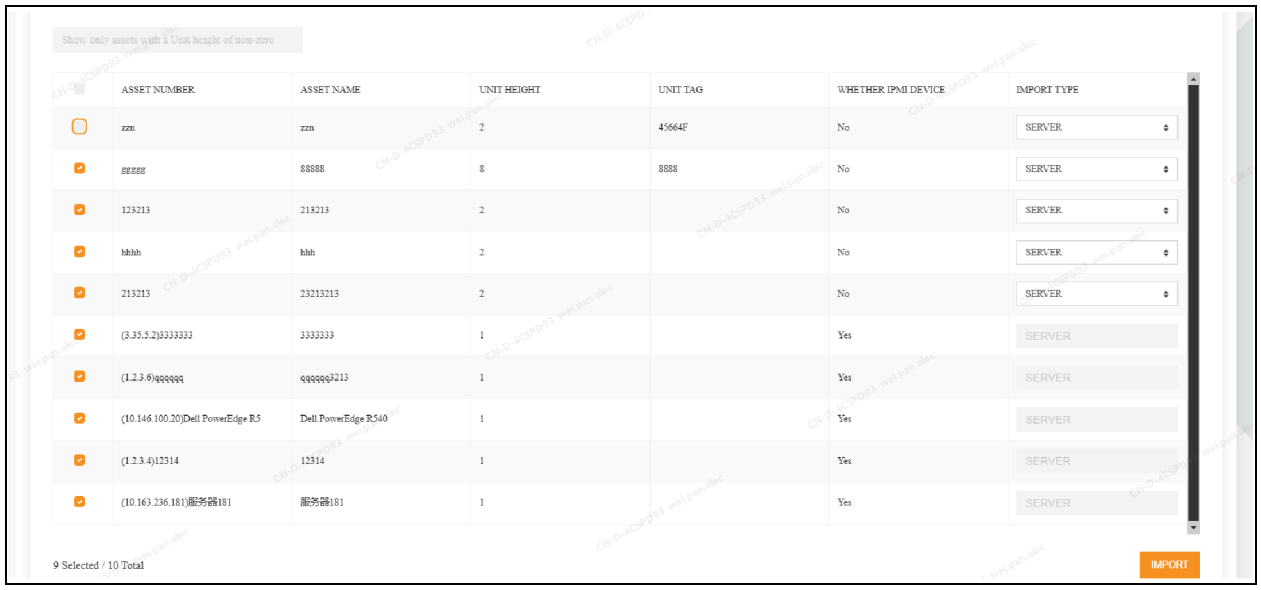
Figure 14.7 Importing Assets from RDU



© 2026 Vertiv Group Corp. All Rights Reserved.

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 14.8** below .

Figure 14.8 Selecting Assets



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 14.9** below .

Figure 14.9 Exporting Assets

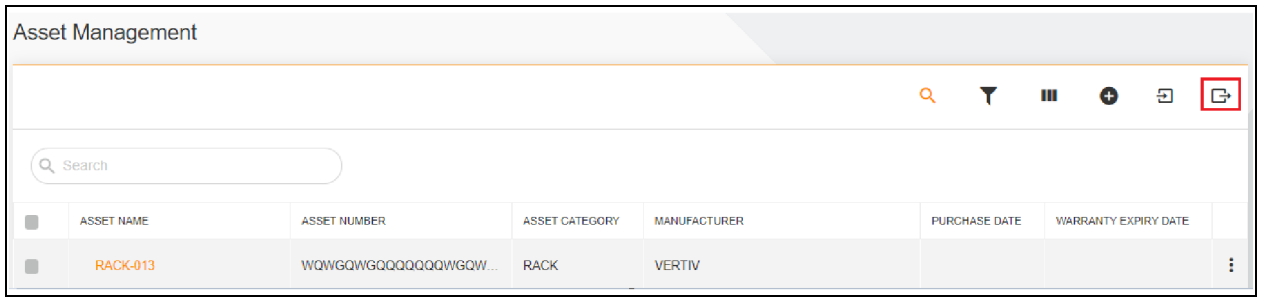
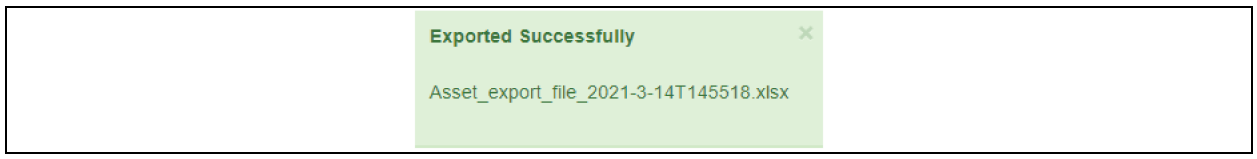
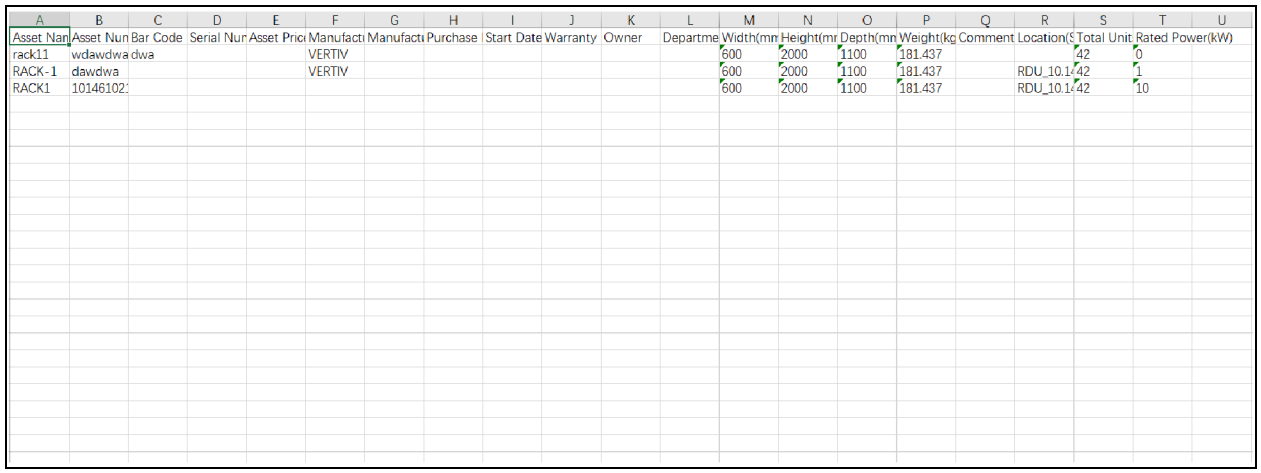


Figure 14.10 Filter Assets for Export



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 14.11 Exported Asset File View



Asset Nan	Asset Nun	Bar Code	Serial Nur	Asset Prio	Manufacti	Manufacti	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

14.2.2 Warranty Notification

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 14.12** below .

Figure 14.12 Warranty Notification



To turn on notifications, check the *box* as shown in **Figure 14.13** on the facing page . Then choose the person who should receive the email (make sure their email address is already set up). Click *Save* to activate the Warranty Notification feature.

Keep in mind, this will only work if the asset's maintenance expiration date has already been set.

The Warranty Notification email reminder system operates as follows:

1. Starting three months before the asset's maintenance expiration date, an email is sent to the selected person on the 1st of each month.
2. If the first email fails to send, the system will try one more time.
3. If both attempts fail, no more emails will be sent for that month. The system will try again on the 1st of the next month.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 14.13 Enabling Warranty Notifications



14.2.3 Asset Rack and De-Rack Records

The U-position Asset Manager allows users to monitor and track changes in rack-mounted assets by recording when assets are installed (racking) and removed (de-racking). It supports multiple sites and U-level asset management, and offers an export function for these records.

© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

15 Reports

15.1 General

15.1.1 Overview

Reports are divided into two categories: Basic Reports and Custom Reports. They are designed for users to query and analyze data and alarms generated by the data center monitoring platform. This chapter describes how to configure and view each report type. The Custom Reports feature is designed to meet users' needs for flexible analysis and personalized presentation of data center monitoring data. Unlike Basic Reports, which provide fixed templates, Custom Reports allow users to select data sources, visualization components, and layout options based on their actual business requirements, enabling the creation of more targeted analytical reports. Custom Reports also support automated export scheduling. The platform automatically generates reports according to the schedule and recurrence settings configured by the user, and delivers them by email to designated recipients, enabling unattended scheduled report distribution.

15.1.2 Functional modules

The Reports module is organized into the following functional sections. For detailed descriptions of each section, refer to Detailed Features below.

- Basic Reports — Device History Report
- Basic Reports — Alarms Record
- Basic Reports — Device Control Report
- Basic Reports — Automation Report
- Basic Reports — Door Access
- Custom Reports – Custom Reports
- Custom Reports – Archived

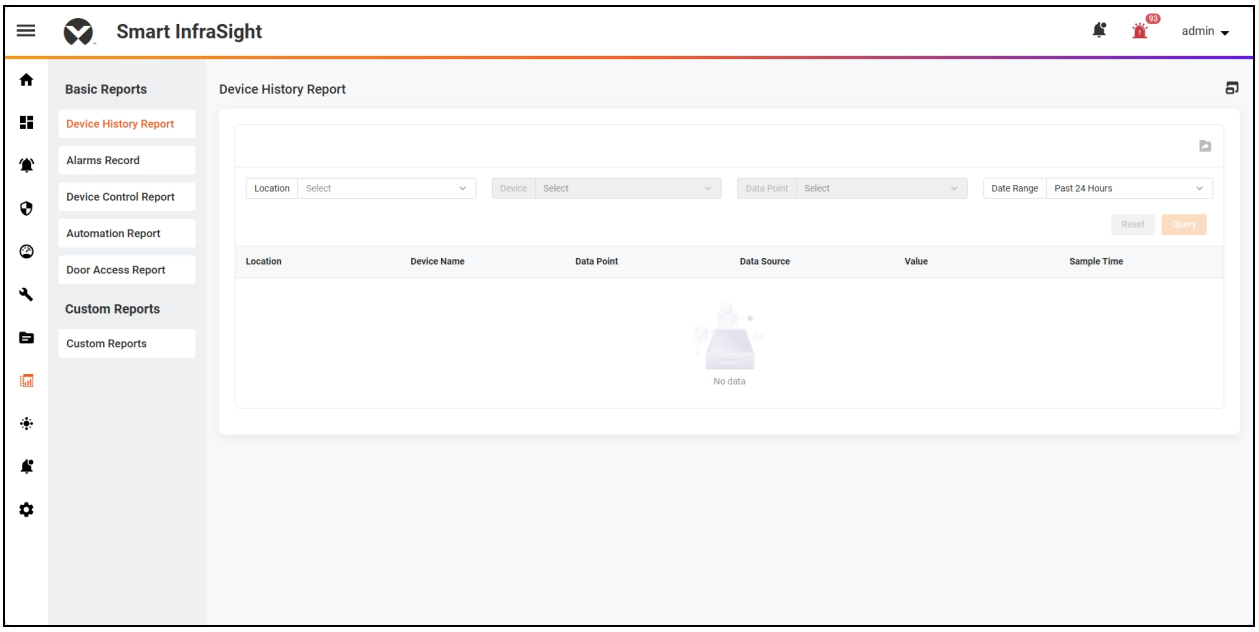
15.2 Detailed Features

15.2.1 Device History Report

To find the history of a device under any site, click *Reports*, then under the Basic Reports section, click *Device History Report* to enter the Device History Report page, as shown in **Figure 15.1** on the next page .

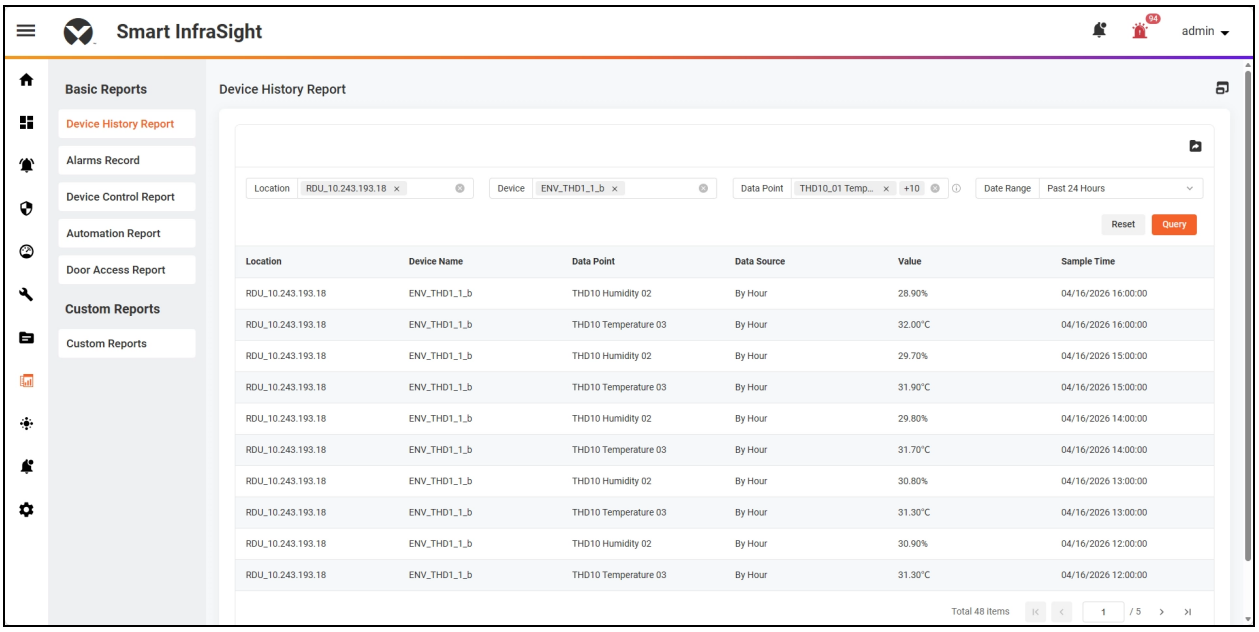
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.1 Device History Report Page



From the Location drop-down list, select a site (required). From the Device drop-down list, select a device within the selected site. From the Data Point drop-down list, select one or more data points under the selected device. If no data point is selected, the platform queries all data points under the device by default. From the Date Range drop-down list, select the desired query time range. Click the *Query* icon to retrieve the results, as shown in **Figure 15.2** below .

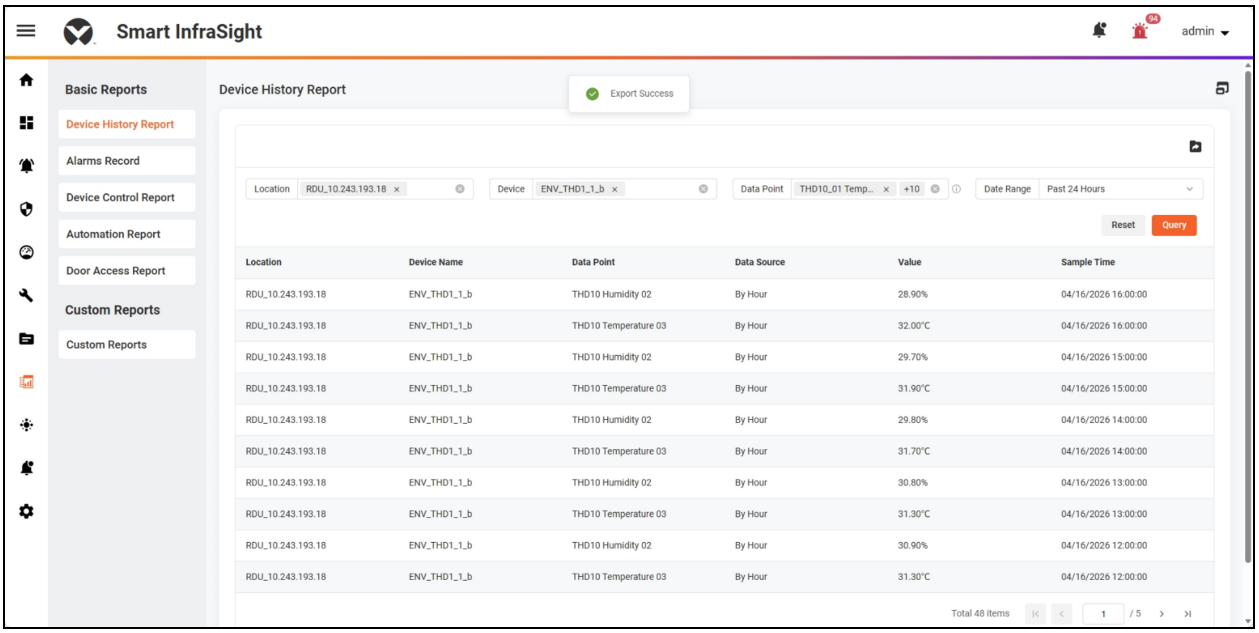
Figure 15.2 Device History Report Query



After clicking *Query* and confirming that the selected filters return results, click the *download* icon in the upper-right corner to export the report, as shown in **Figure 15.3** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.3 Export Device History Report



NOTE:

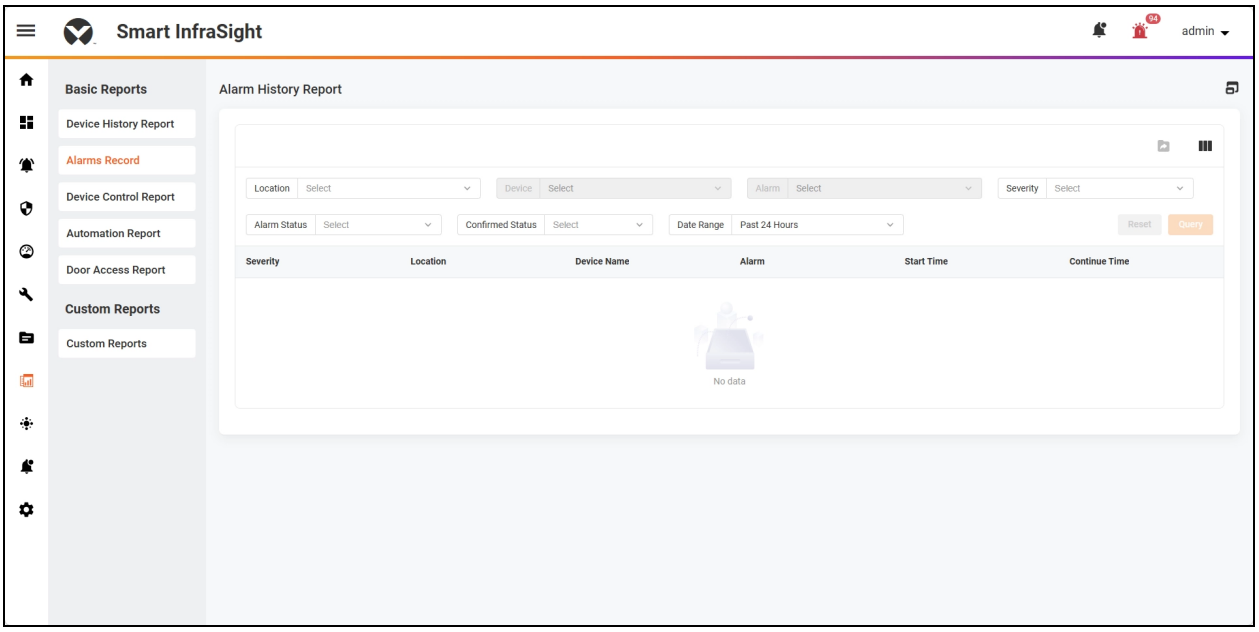
1. **The number of selections for Location, Device, and Data Point must not exceed 8 each.**
2. **Location is required. If Device or Data Point is not specified, the platform returns data for all devices or all data points under the selected location by default.**
3. **The Device History Report can be downloaded only after clicking Query and receiving query results.**
4. **Data point values are displayed with a default precision of two decimal places.**
5. **For standardized FLOOR_PDU and UPS devices, the report displays non-branch data points only, not all data points.**

15.2.2 Alarms Record

Click *Reports*, then under the Basic Reports section, select *Alarms Record* to open the Alarm History Report page, as shown in Figure 15.4 on the next page .

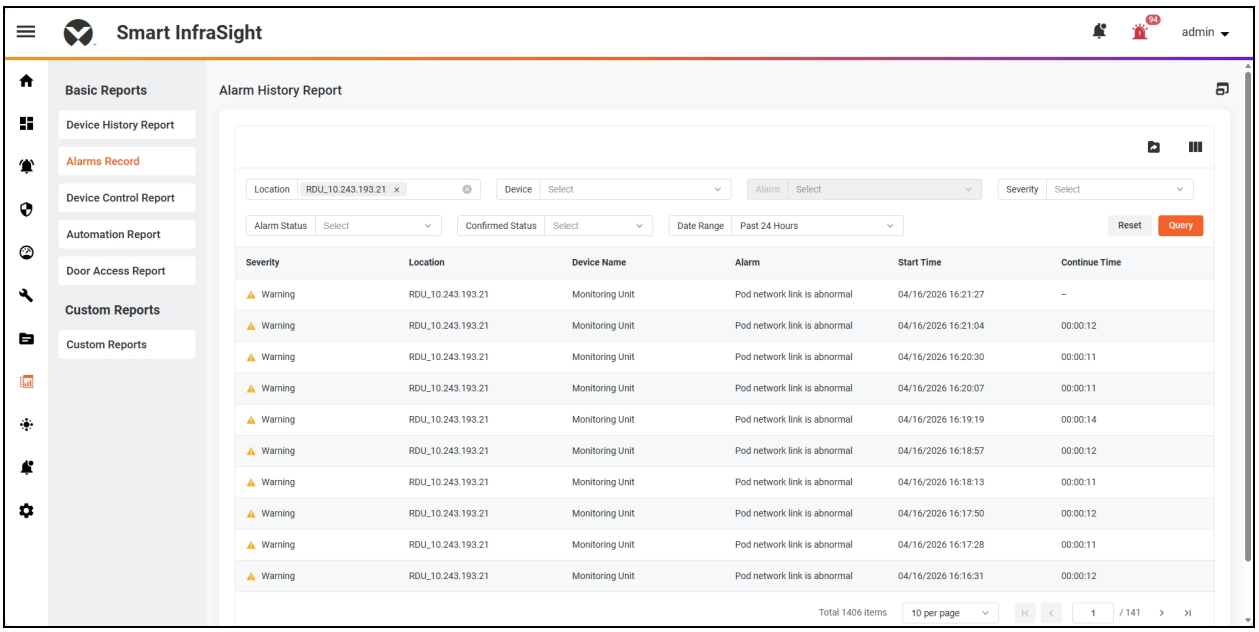
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.4 Alarm History Report



From the Location drop-down list, select a site (required). From the Device drop-down list, select a device within the selected site. From the Alarm drop-down list, select one or more alarms under the selected device. From the Severity, Alarm Status, and Confirmed Status drop-down lists, select the desired alarm severity, alarm status, and acknowledgment status respectively (single selection). If no option is selected, the platform returns all records by default. From the Date Range drop-down list, select the desired query time range. The default time range is Past 24 Hours. Click *Query* to retrieve alarm records matching the selected location, device, alarm, severity, alarm status, confirmed status, and date range, as shown in **Figure 15.5** below .

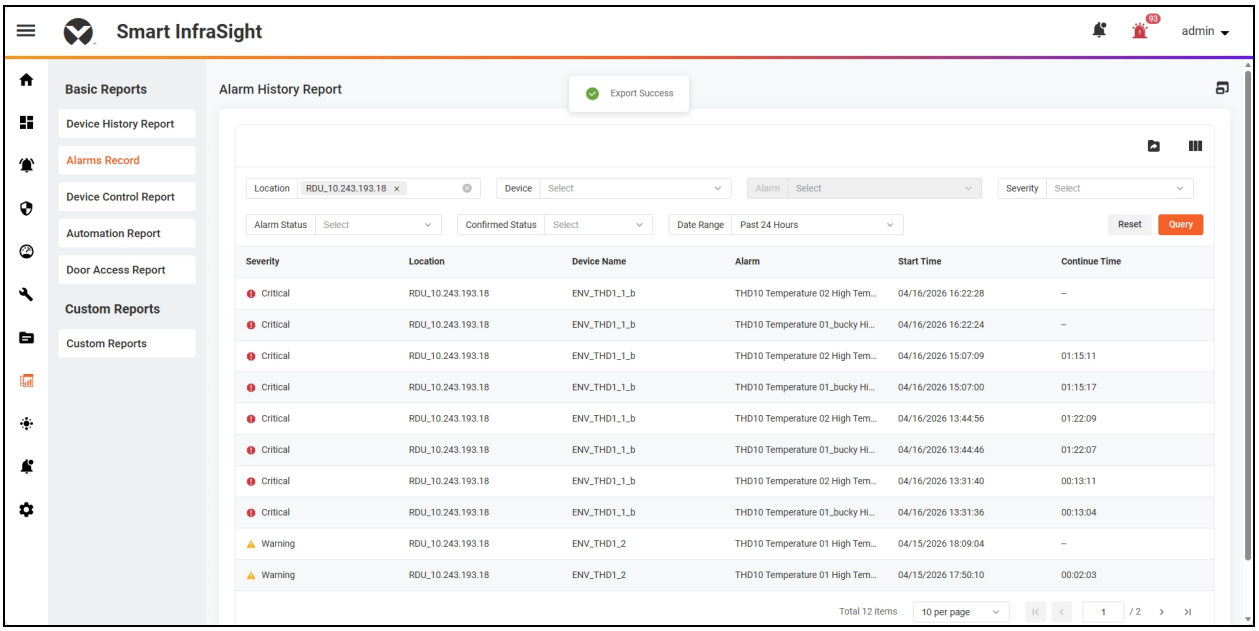
Figure 15.5 Alarm History Report Query Results



© 2026 Vertiv Group Corp. All Rights Reserved.

To download the Alarm History Report, click *Query* and confirm that the selected filters return results, then click the *Export* icon in the upper-right corner to export the report, as shown in **Figure 15.6** below .

Figure 15.6 Export Alarm History Report



NOTE:

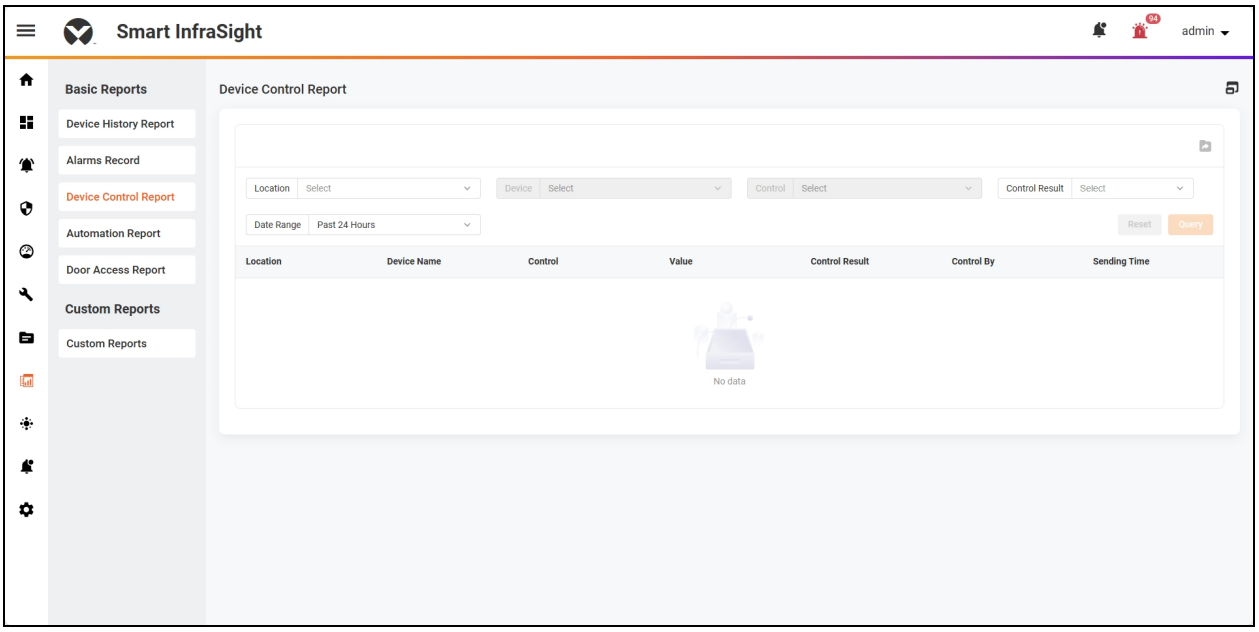
1. **Location is required. If any other filter is not specified, the platform returns all records by default.**
2. **The Alarm History Report can be downloaded only after clicking Query and receiving query results.**

15.2.3 Device Control Report

Navigate to Reports, then under the Basic Reports section, click *Door Access Report* to open the Door Access Report page, as shown in **Figure 15.7** on the next page .

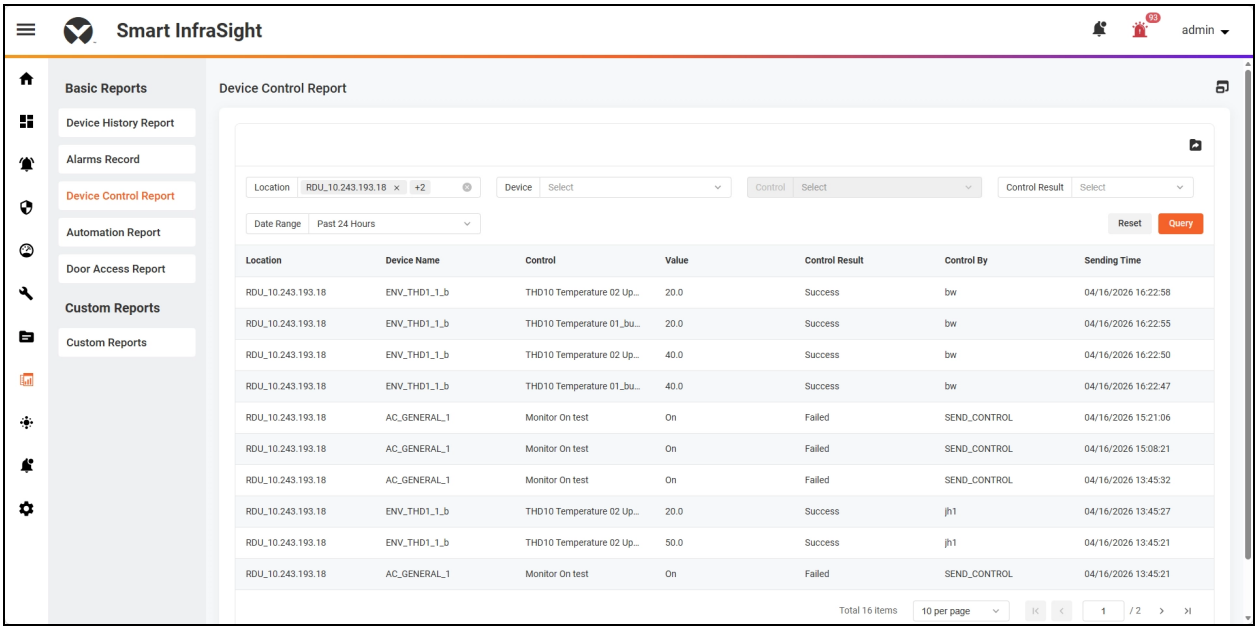
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.7 Device Control Report



From the Location drop-down list, select a site (required). From the Device drop-down list, select a device within the selected site. From the Control drop-down list, select one or more control signals under the selected device. From the Control Result drop-down list, select either Success or Failed to filter records by control outcome (single selection). If no option is selected, the platform returns all records by default. From the Date Range drop-down list, select the desired query time range. The default time range is Past 24 Hours. Click *Query* to retrieve device control records matching the selected location, device, control signal, control result, and date range, as shown in Figure 15.8 below .

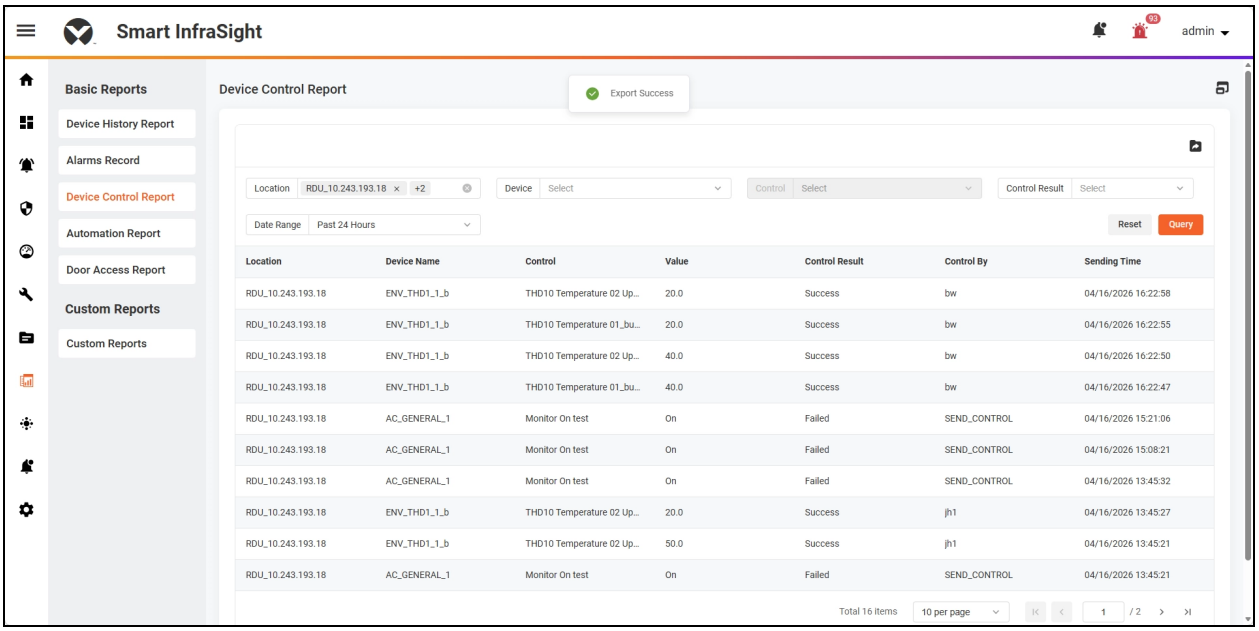
Figure 15.8 Device Control Report Query Results



© 2026 Vertiv Group Corp. All Rights Reserved.

To download the Device Control Report, click *Query* and confirm that the selected filters return results, then click the *download* icon in the upper-right corner to export the report, as shown in Figure 15.9 below .

Figure 15.9 Export Device Control Report



NOTE:

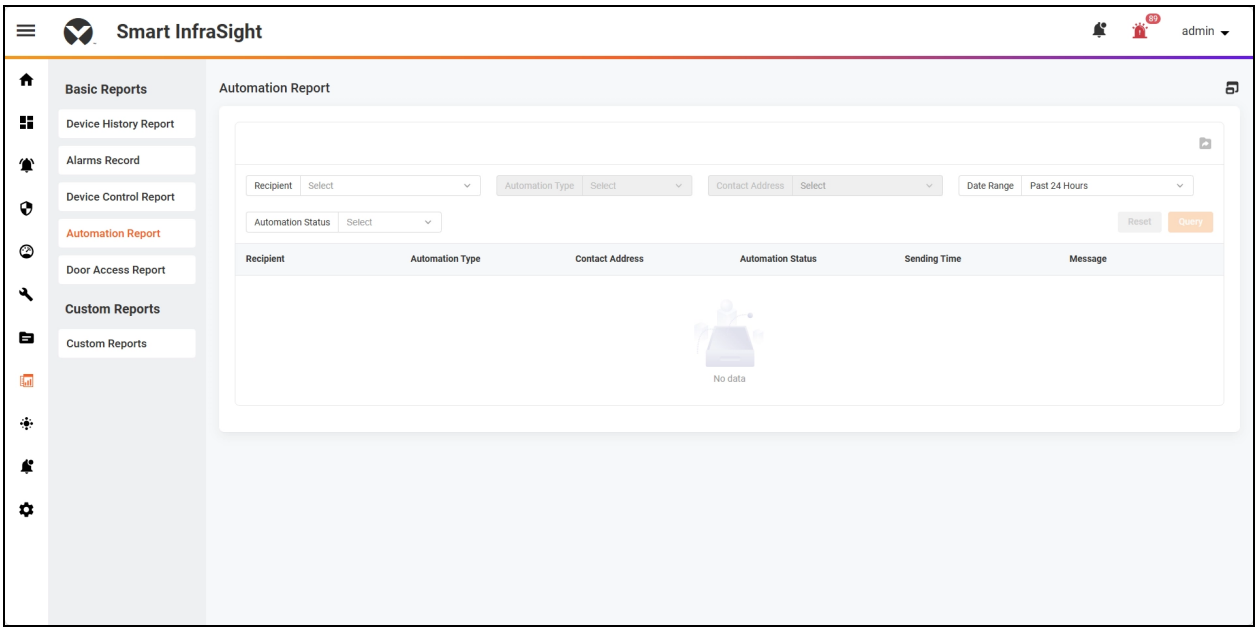
1. **The number of selections for Location, Device, and Control must not exceed 8 each.**
2. **Location is required. If any other filter is not specified, the platform returns all records by default.**
3. **The Device Control Report can be downloaded only after clicking Query and receiving query results.**

15.2.4 Automation Report

Navigate to Reports, then under the Basic Reports section, click *Automation Report* to open the Automation Report page, as shown in Figure 15.10 on the next page .

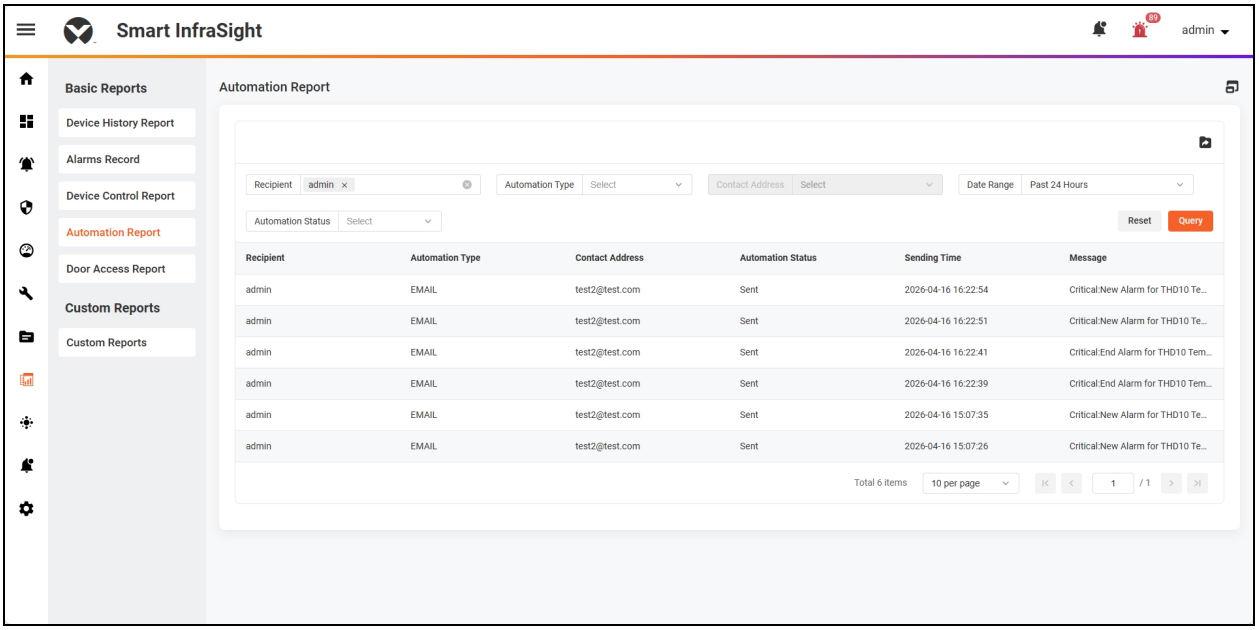
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.10 Automation Report



From the Recipient drop-down list, select a recipient (required). From the Automation Type drop-down list, select the notification type. From the Contact Address drop-down list, select the delivery address associated with the selected recipient. From the Automation Status drop-down list, select the desired delivery status (single selection). If no option is selected, the platform returns all records by default. From the Date Range drop-down list, select the desired query time range. Click *Query* to retrieve alarm notification records matching the selected recipient, automation type, contact address, automation status, and date range, as shown in **Figure 15.11** below .

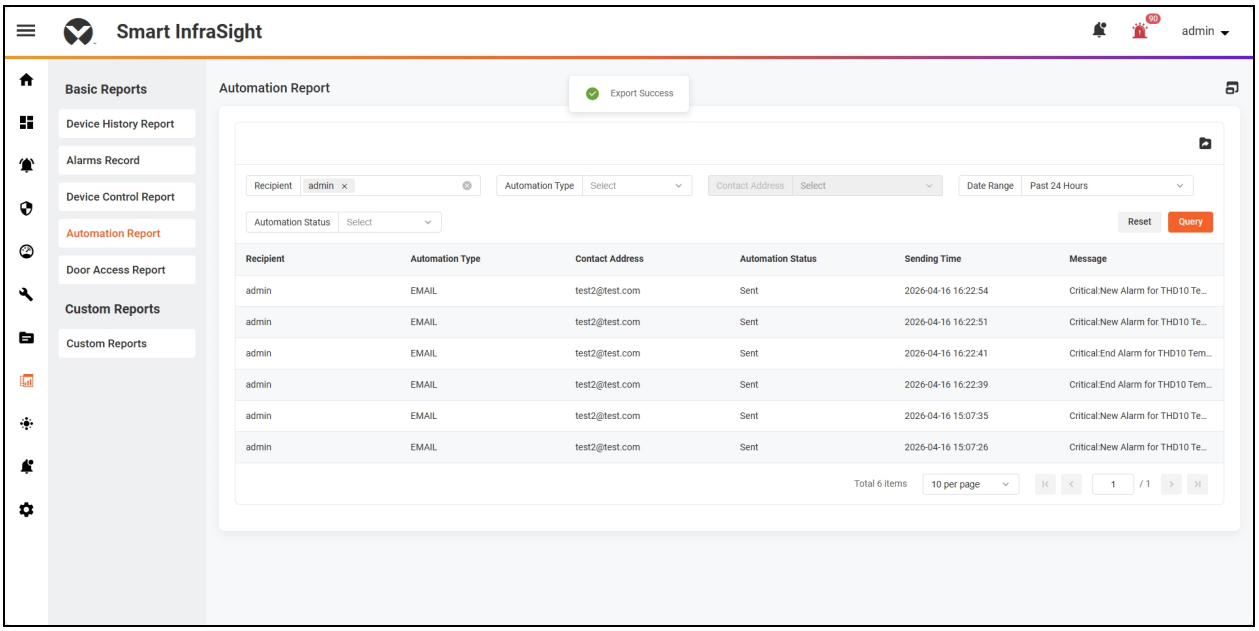
Figure 15.11 Automation Report Query Results



© 2026 Vertiv Group Corp. All Rights Reserved.

To download the Automation Report, click *Query* and confirm that the selected filters return results, then click *Export* in the upper-right corner to export the report, as shown in **Figure 15.12** below .

Figure 15.12 Export Automation Report



NOTE:

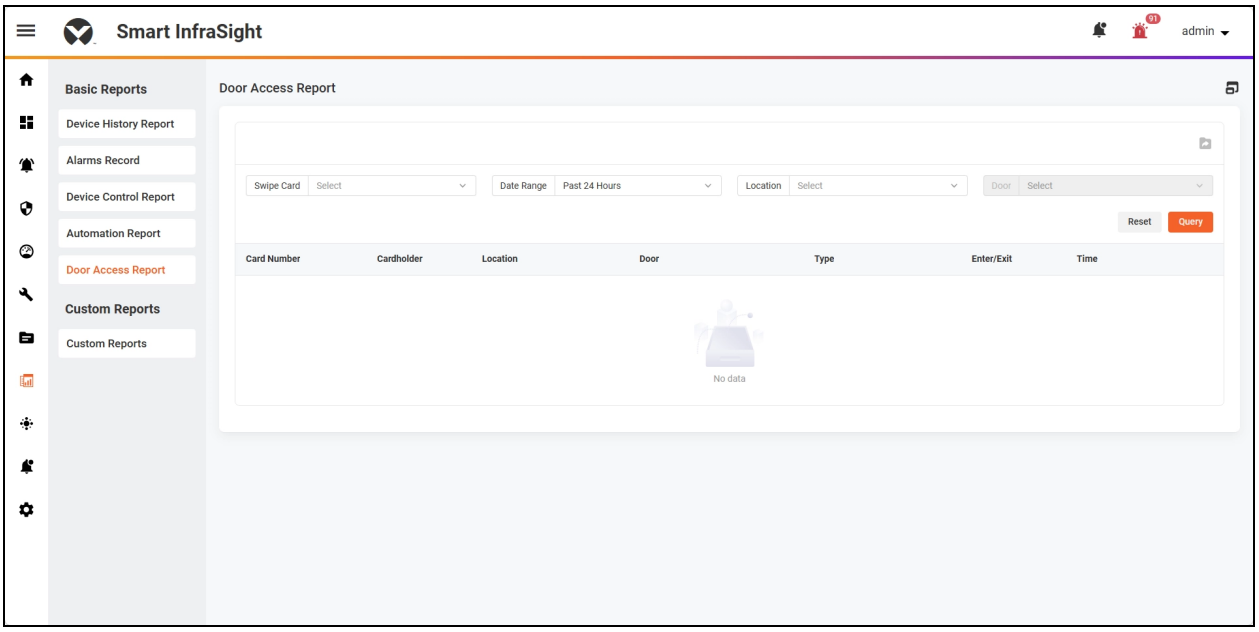
1. **The number of selections for Recipient and Contact Address must not exceed 8 each.**
2. **Recipients are required. If any other filter is not specified, the platform returns all records by default.**
3. **The Automation Report can be downloaded only after clicking Query and receiving query results.**

15.2.5 Door Access Report

Navigate to Reports, then under the Basic Reports section, then click *Door Access Report* to open the Door Access Report page, as shown in **Figure 15.13** on the next page .

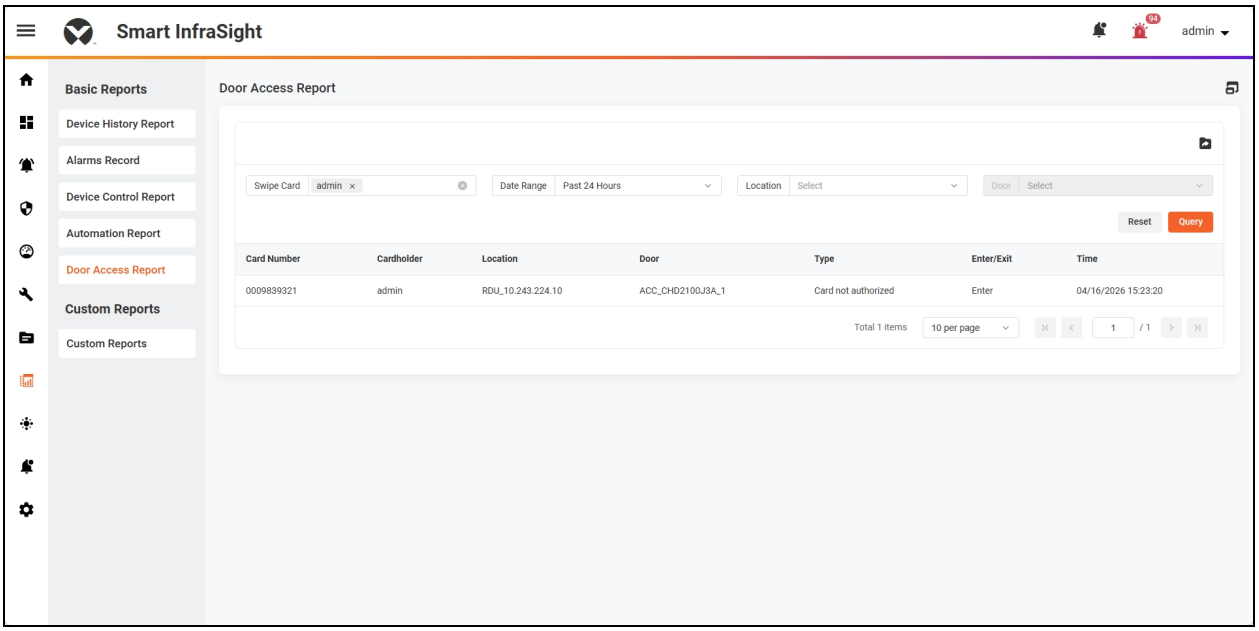
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.13 Door Access Report



From the Swipe Card drop-down list, select a cardholder. From the Location drop-down list, select a site. From the Door drop-down list, select a door device within the selected site. From the Date Range drop-down list, select the desired query time range. The default time range is Past 24 Hours. Click *Query* to retrieve door access records matching the selected cardholder, door, location, and date range, as shown in Figure 15.14 below .

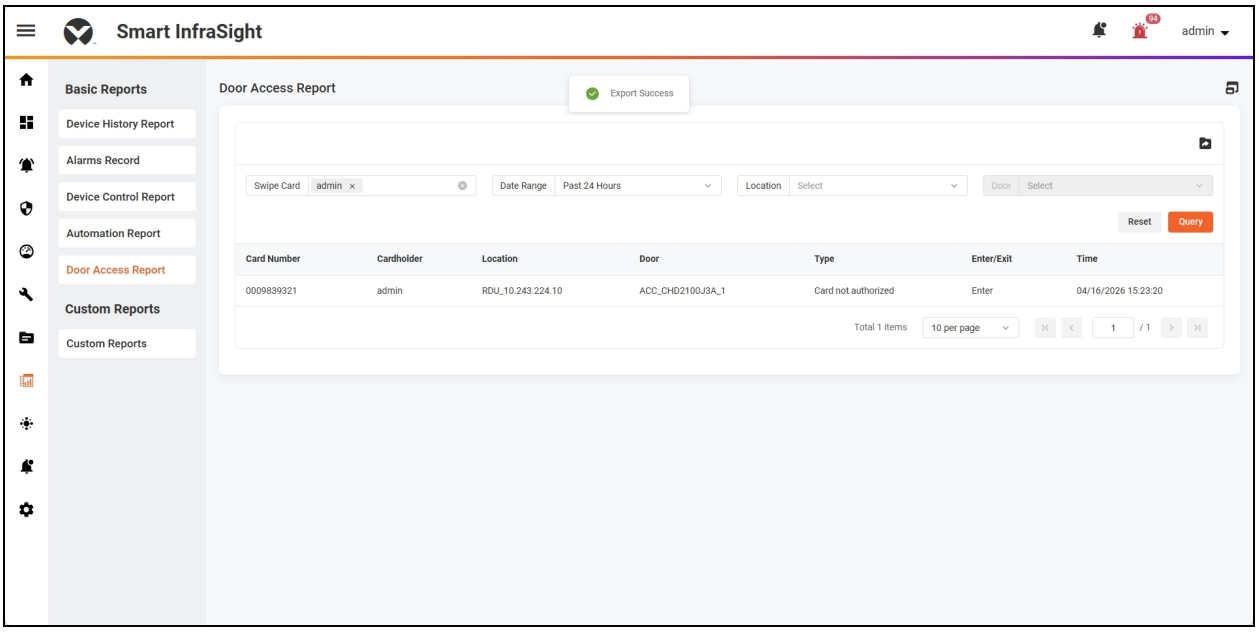
Figure 15.14 Door Access Report Query Results



To download the Door Access Report, click *Query* and confirm that the selected filters return results, then click the *download* icon in the upper-right corner to export the report, as shown in Figure 15.15 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.15 Export Door Access Report



NOTE:

1. **The number of selections for Location, Door, and Swipe Card must not exceed 8 each.**
2. **The Door Access Report can be downloaded only after clicking Query and receiving query results.**

15.2.6 Custom Reports

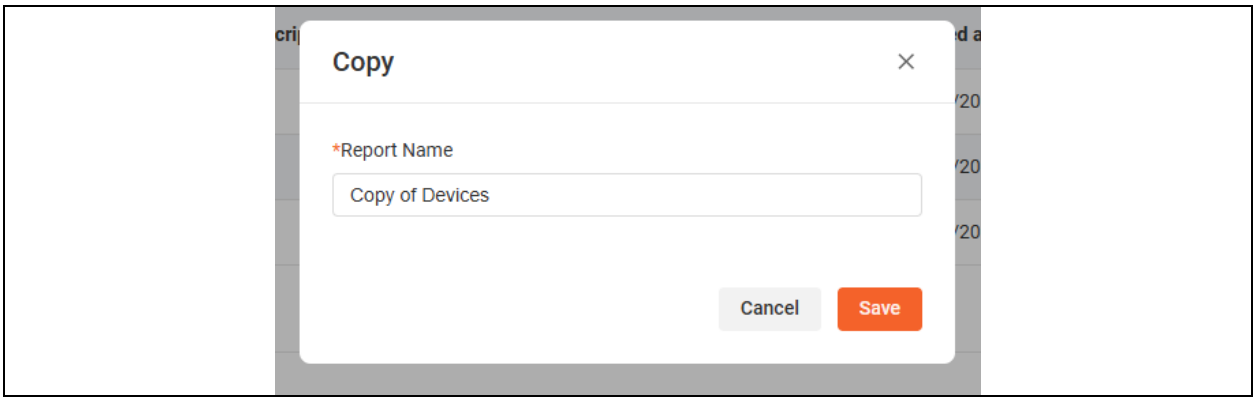
Custom Reports List

1. After navigating to the Custom Reports tab, the list displays all created custom reports in a table. The column fields are described as follows:
2. Report Name: The custom name of the report, displayed as a hyperlink. Click it to open the report details.
3. Description: Supplementary information about the report, entered during creation. This field can be left blank.
   - Creator: The account name of the user who created the report.
   - Created at: The date and time the report was created.
   - Group: The name of the group the report belongs to, used for categorized management.
   - Schedule: The automatic generation cycle of the report. Supports multiple frequency combinations, including daily, weekly, and monthly. For example: Weekly, Tue and Thu at 04 : 10 PM +08:00 (BeiJing,Hong Kong SAR) | 4:10 PM Local
4. Enter a report name keyword in the search bar above the list to quickly filter for the target report.
5. To filter by group, click *Filter* above the list and select the target group name from the drop-down list. The list automatically refreshes to display only the reports within that group. Click (X) next to the group tag to clear the current filter.
6. After selecting one or more report records, the following actions become available in the operation area at the top-right of the list:

© 2026 Vertiv Group Corp. All Rights Reserved.

- **Copy**: Copies the selected report and generates a duplicate with the same configuration. Only one record can be selected at a time for this operation; the button is grayed out when multiple records are selected. After clicking *Copy*, a dialog box opens, allowing you to name the duplicate. See **Figure 15.16** below .

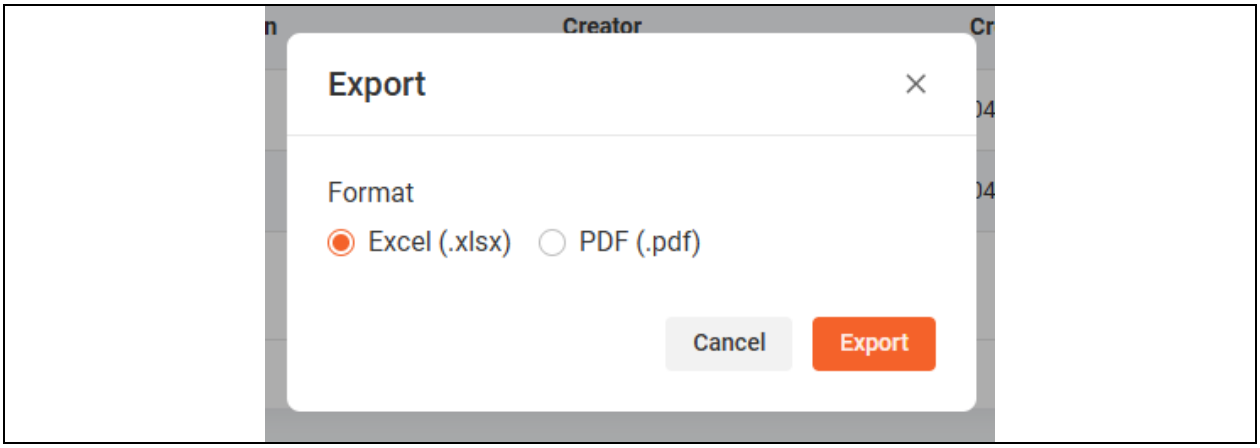
Figure 15.16 Copy Window



- **Export**: Exports the selected report as a file. Only one record can be selected at a time for this operation; the button is grayed out when multiple records are selected. After clicking *Export*, an export dialog box appears. In the Format field, select the export format:
  - a. **Excel (.xlsx)**: Exports the report as an Excel spreadsheet file (selected by default).
  - b. **PDF (.pdf)**: Exports the report as a PDF file.

After selecting a format, click *Export* to confirm, or click *Cancel* to cancel the operation and close the dialog box. See **Figure 15.17** below .

Figure 15.17 Export Window

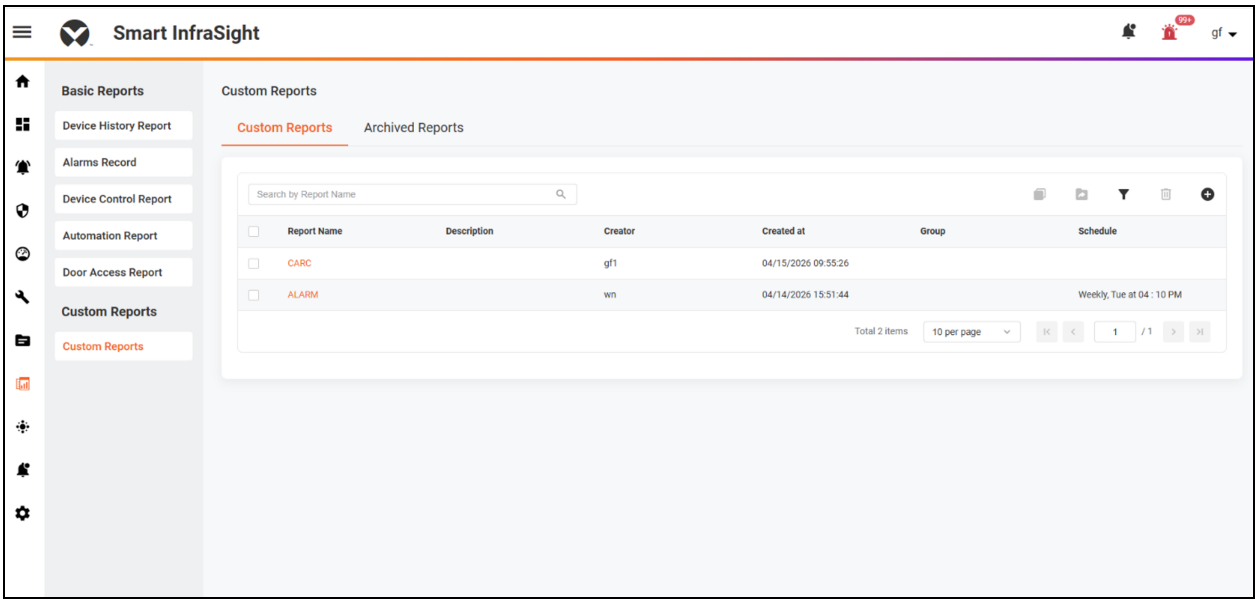


- **Delete**: Deletes the selected reports. A confirmation dialog box appears before the operation proceeds. This action is irreversible; proceed with caution.
- **Add**: Creates a new custom report. You can click this button directly without selecting any records.

7. The total number of records is displayed at the bottom of the list. Use the **rows per page** drop-down list to adjust the number of entries displayed per page, and use the pagination controls to navigate between pages. You can also enter a target page number directly in the page number input box to jump to that page. See **Figure 15.18** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.18 Copy Custom Report



Add Custom Reports

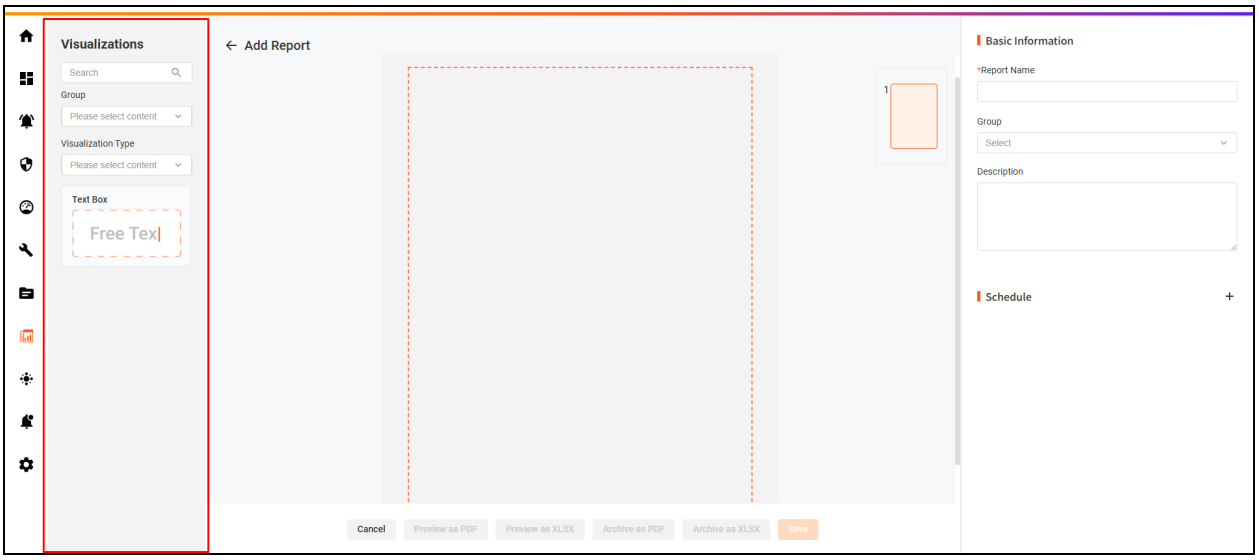
Visualization (Left Side)

The left panel is the **Visualizations** panel, which lists all components available for report layout. It includes a unique **Text Box** component and chart components sourced from the Visualization Center module described in Visualization on page 343 / Below the Text Box, chart components sourced from Visualization Center (see Visualization on page 343) are listed in order.

1. Enter a name keyword in the search bar at the top to perform a fuzzy search for visualization components. Search results are sorted by name in ascending order.
2. Use the following two filter criteria to narrow down the component list:
   - **Group**: Select a group from the drop-down list to display only the components within that group.
   - **Visualization Type**: Select a component type from the drop-down list to filter components by type.
3. The **Text Box** component is pinned as the first item below the filter area. After dragging the **Text Box** onto the central canvas, you can freely enter plain text content within the component. The Text Box supports plain text input only; text formatting options such as font type, font size, bold, and italic are not supported.
4. Below the **Text Box**, chart components sourced from Visualization Center (see Visualization on page 343) are listed in order. Each component card displays the visualization name and a thumbnail preview for quick identification. Components are grouped by their assigned group, and both groups and components are sorted by name in ascending order. Components that have not been assigned to a group are categorized under **Unallocated**.
5. Drag the required component from the left panel into the valid area within the page margins on the central canvas to add it to the current report page. Components that have already been added to the canvas do not support direct content editing on the canvas. See **Figure 15.19** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

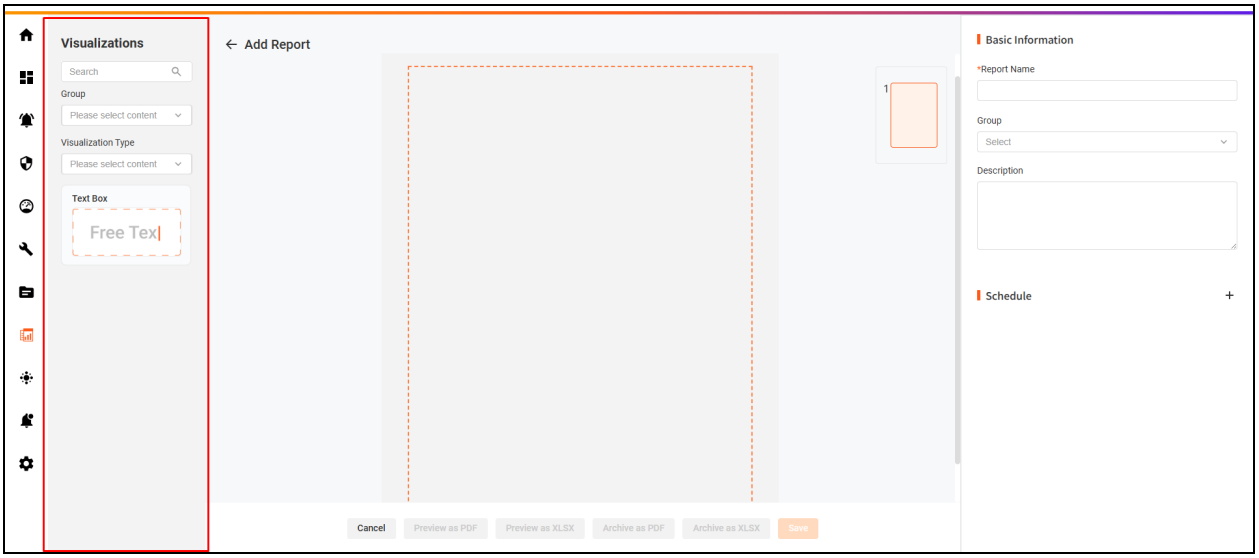
Figure 15.19 Dragging Visualizations from Left Panel



Canvas (Center)

The central area of the page is the canvas, which displays the report page in A4 size. Page margins are applied on all sides, and an orange dashed border identifies the valid area where components can be placed. See Figure 15.20 below .

Figure 15.20 Place Visualizations in the Central Area

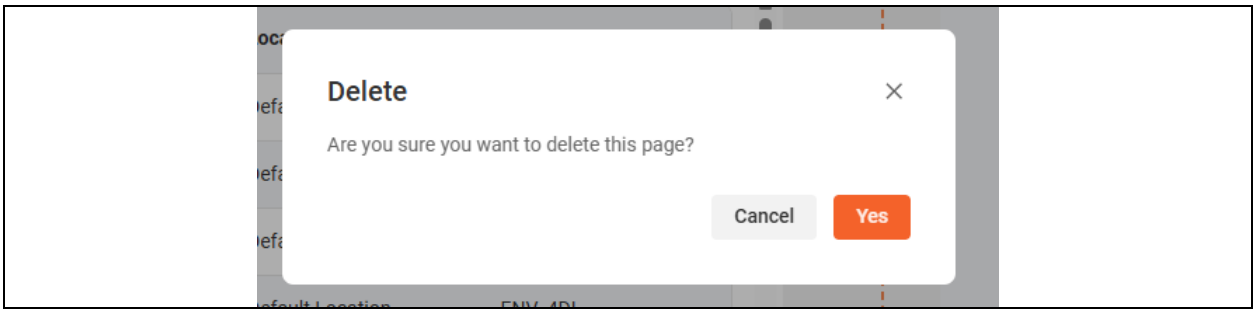


1. Drag components from the Visualizations panel on the left into the orange dashed border to add them to the current page.

    - When a report contains multiple pages, a (X) delete icon is displayed in the top-right corner of each canvas. Click (X) to delete the page. If components have already been placed on that page, the platform displays a confirmation dialog box asking whether to confirm the deletion. Once confirmed, the page and all its content are permanently deleted. When only one page remains in the report, the (X) icon is automatically hidden. See Figure 15.21 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.21 Page Deletion Window



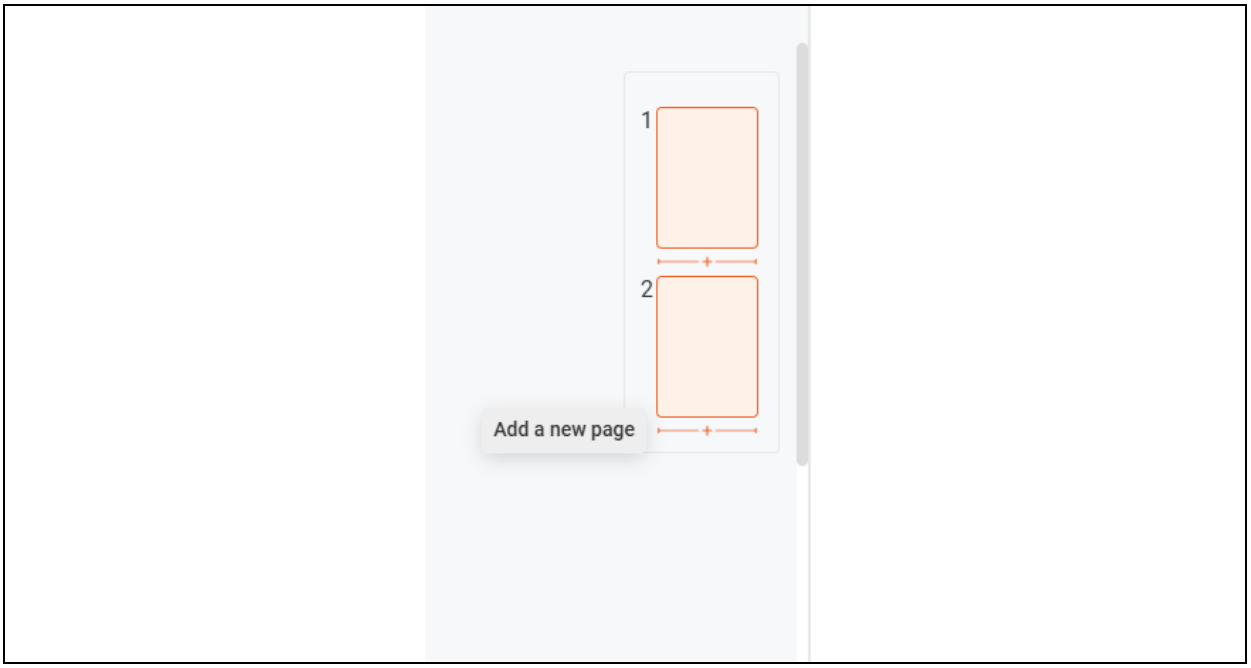
2. Components that have been added to the canvas support the following operations:

- Drag the edges or corners of a component to freely resize it.
- Press and hold a component to reposition it anywhere on the current page.
- Click (X) in the top-left corner of a component to remove it from the current page.

3. To the right of the canvas is the page thumbnail navigation panel. Pages are listed vertically as numbered thumbnails and support the following operations:

- Drag a *thumbnail* to reorder pages. The corresponding page positions on the canvas are updated simultaneously.
- Click a *thumbnail* to quickly navigate to the corresponding page.
- When scrolling through pages, the thumbnail corresponding to the current page is highlighted automatically.
- Hover over any thumbnail to reveal + icons above and below it. Click (+) to insert a new page above or below that page. A report supports a maximum of 20 pages. Once this limit is reached, the (+) icon is automatically hidden. See **Figure 15.22** below .

Figure 15.22 Adding a New Page

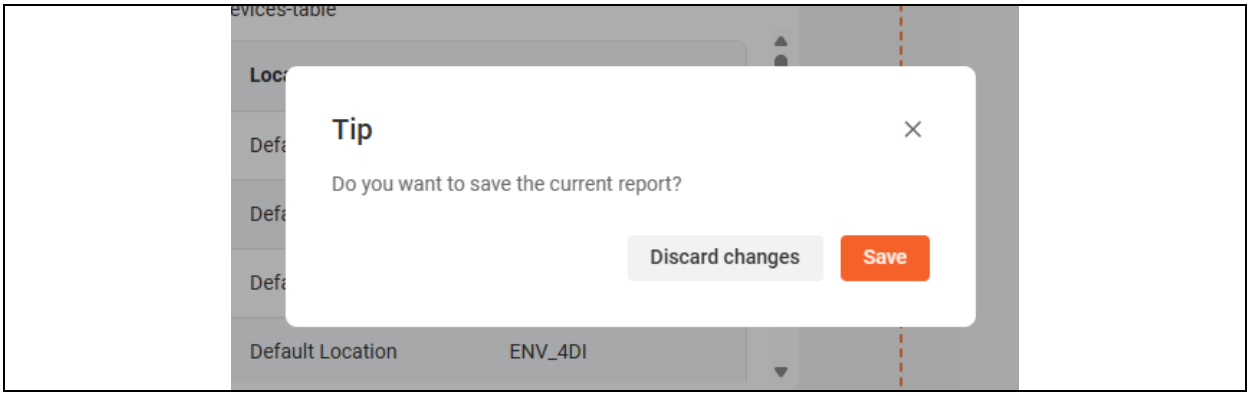


4. The following actions are available at the bottom of the page:

© 2026 Vertiv Group Corp. All Rights Reserved.

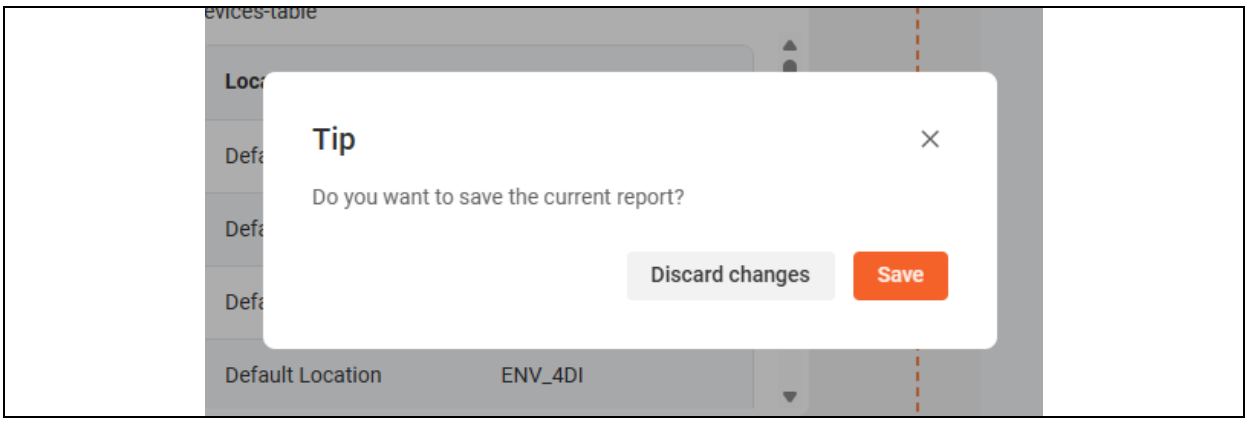
- **Cancel**: Cancels the current edit and returns to the report list. If there are unsaved changes, a confirmation dialog box appears with the following options:
  a. **Save:** Saves the current report and returns to the list page.
  b. **Discard Changes**: Returns to the list page without saving. See **Figure 15.23** below .

Figure 15.23 Tip Window for Unsaved Report Changes



- **Preview as PDF:** Downloads the current report as a PDF file. This action is grayed out and unavailable when no components have been placed on any page.
- **Preview as XLSX:** Downloads the current report as an Excel file. This action is grayed out and unavailable when no components have been placed on any page, or when the pages contain only Text Box components.
- **Archive as PDF:** Downloads the current report as a PDF file and saves it to Archived Reports. This action shall be disabled if no components are placed on any page.
- **Archive as XLSX:** Downloads the current report as an Excel file and saves it to Archived Reports. This action shall be disabled if no components are placed on any page, or if all pages contain only Text Box components.
- **Save:** Saves the current report and remains on the current editing page so you can continue editing. If there are unsaved changes and another navigation action is triggered, the platform displays a confirmation dialog box with the following options:
  - a. **Save**: Saves the report and proceeds with the navigation.
  - b. **Discard Changes:** Proceeds with the navigation without saving. See **Figure 15.24** below .

Figure 15.24 Tip Window for Unsaved Report Changes During Navigation



© 2026 Vertiv Group Corp. All Rights Reserved.

Basic Information Panel (Right Side)

The right side of the page contains the Basic Information configuration panel, used to enter the report's fundamental attributes. The fields are described as follows:

- **Report Name (Required):** Enter a custom name for the report.
- **Group:** Select the group the report belongs to from the drop-down list. This field can be left blank.
- **Description**: Enter supplementary information about the report. This field can be left blank.

Below **Basic Information** is the **Schedule** section, used to configure the report's automatic export and delivery schedule. By default, no schedules are configured. A maximum of 10 schedules can be added to a single report. Once this limit is reached, the + button is grayed out and unavailable. Configured schedules are displayed as a list, with each row showing a summary of that schedule.

1. Click (+) to the right of **Schedule** to open the **Add Schedule** dialog box. The fields are described as follows:

• **Recipients** (Required): Select the users or contact email addresses to receive the report email from the drop-down list. Multiple selections are supported.

• **Format** (Required): Select the export file format from the drop-down list. Multiple selections are supported. Available options are:

a. PDF
b. XLSX

• **Time Zone** (Required): Select the time zone for schedule execution from the drop-down list. Defaults to the local time zone of the current user's computer.

• **Time** (Required): Select the specific time for each delivery. Defaults to the current time.

• **Repeat** (Required): Select the delivery frequency from the drop-down list. Defaults to Daily. Available options are:

- **a. Daily**: The schedule runs every day. The Repeat On field automatically selects all days (Sun through Sat). If any day is deselected, Repeat automatically switches to Weekly, and the previously selected days are retained.
- **b. Weekly**: Freely select one or more days in the Repeat On field. At least one day must remain selected. If all seven days are selected, Repeat automatically switches to Daily.
- **c. Monthly:** Displays a Select Date field. Select the specific date of each month for execution from the drop-down list. This field is empty by default.
- **Repeat On (Required)**: Displays a day-of-week selector showing Sun, Mon, Tue, Wed, Thu, Fri, and Sat. Multiple selections are supported. At least one day must be selected.

2. Once all required fields are completed, a schedule summary is automatically displayed in the bottom-left corner of the dialog box:

- When **Repeat** is set to **Daily**: Will be sent daily at {time} {timezone offset} ({timezone name}) | Local time: {local time}.
- When **Repeat** is set to **Weekly**: Will be sent every {day of week} at {time} {timezone offset} ({timezone name}) | Local time: {local time}.
- When **Repeat** is set to **Monthly**: Will be sent monthly on {date list} at {time} {timezone offset} ({timezone name}) | Local time: {local time}.

3. After confirming the configuration, click *OK* to save the schedule. Click *Cancel* or (x) in the top-right corner to close the dialog box without saving.

© 2026 Vertiv Group Corp. All Rights Reserved.

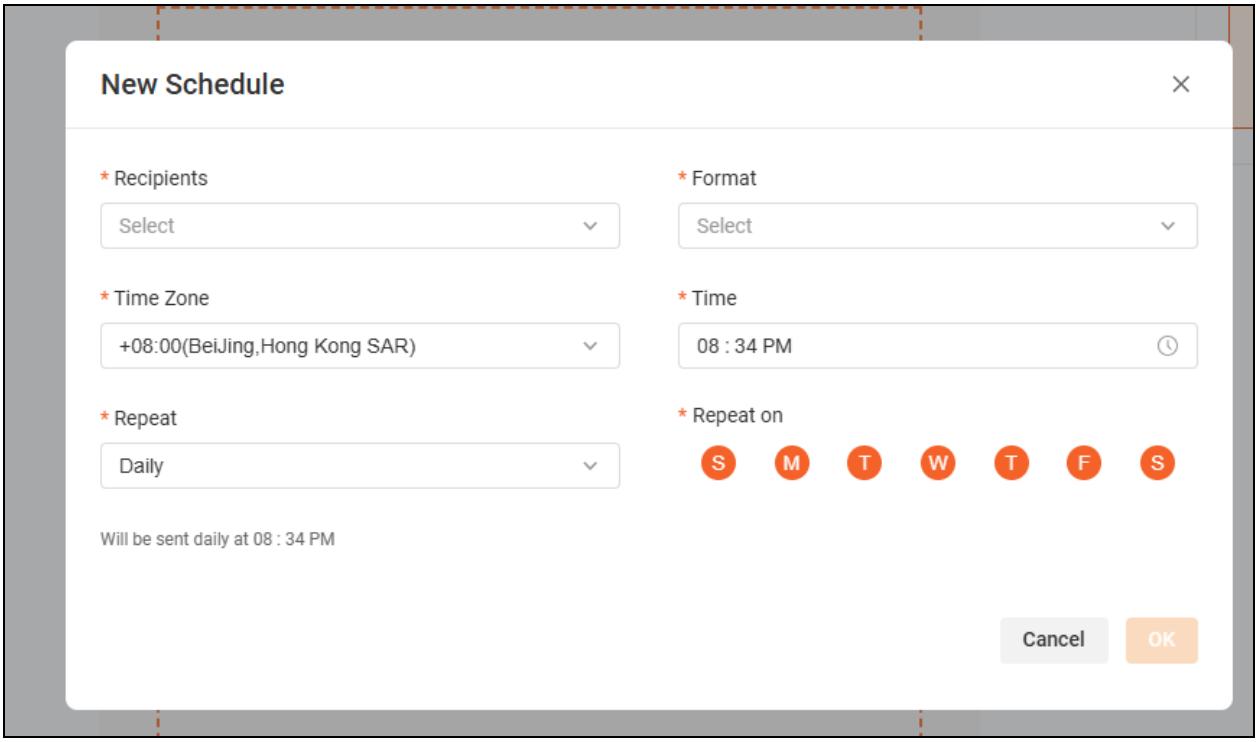
4. Click an existing schedule row to open the **Edit Schedule** dialog box and modify that schedule.

5. Click (−) to the right of a schedule row. The platform displays a confirmation dialog box with the message: **Are you sure you want to delete this schedule?**

- Click *Yes*: Deletes the schedule.
- Click *No*: Closes the dialog box without making any changes.

After a schedule is triggered, the platform automatically generates the report file in the selected format and sends it to all specified recipients via email. The attachment file is named in the following format: Report Name_Timestamp.PDF/.XLSX. See **Figure 15.25** below .

Figure 15.25 New Schedule Configuration Dialog



Edit Custom Reports

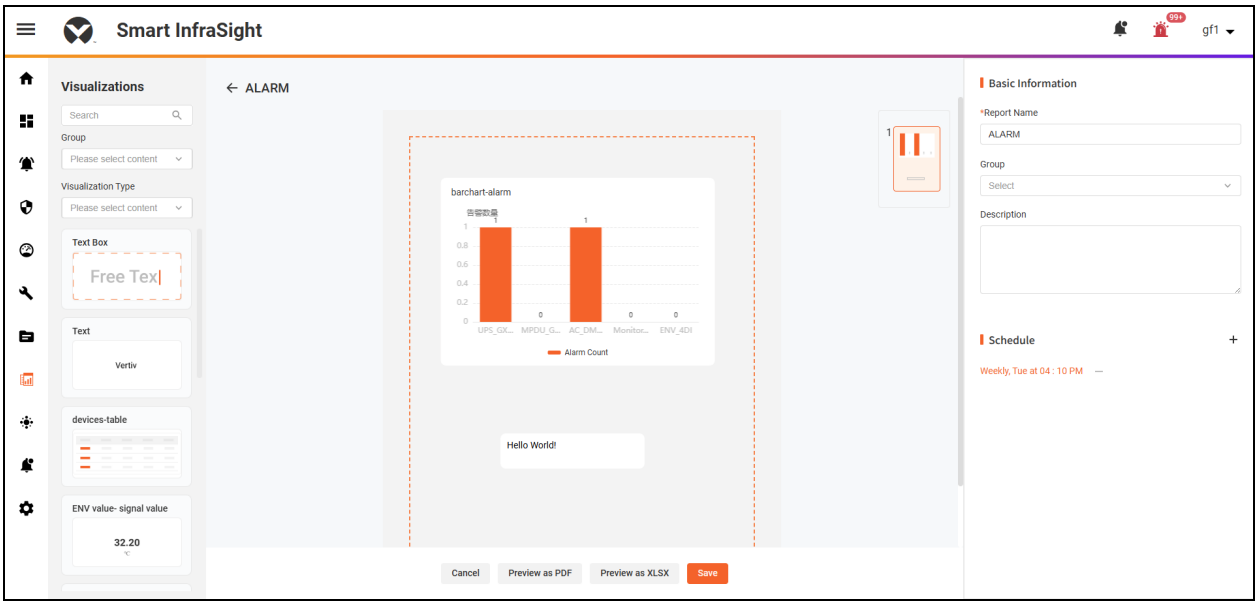
The Edit Report page has an identical layout and functionality to the Add Report page, with the following differences:

To access the Edit Report page, click the report name under Report Name in the report list. The layout and operations of the Edit Report page are identical to those of the Add Report page (see the previous section). The differences are described as follows:

1. The page title at the top initially displays the **report name** instead of **Add Report**.
2. The canvas area, **Basic Information** panel, and **Schedule** section automatically load the previously saved content of the report. You can modify the content directly on this basis.
3. Click *Save* to overwrite and save the latest content of the current report. After saving, the platform remains on the current editing page. See **Figure 15.26** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.26 Editing the Custom Report



Archived Reports

Click the *Archived Reports* tab to switch to the archived report list page. Archived reports include reports saved to Archived Reports by the Archive as PDF and Archive as XLSX actions, as well as reports automatically generated and sent to users according to a configured schedule. These reports are saved within the platform for users to view and download at a later time.

1. The list displays all archived report files in a table. The column fields are described as follows:

- **Name**: The name of the archived report.
- **Description**: Supplementary information about the report. This field can be left blank.
- **Created At**: The date and time the archived report was generated.
- **File Type**: The export format of the report. Supported formats are PDF and XLSX.
- **Group**: The name of the group the report belongs to.

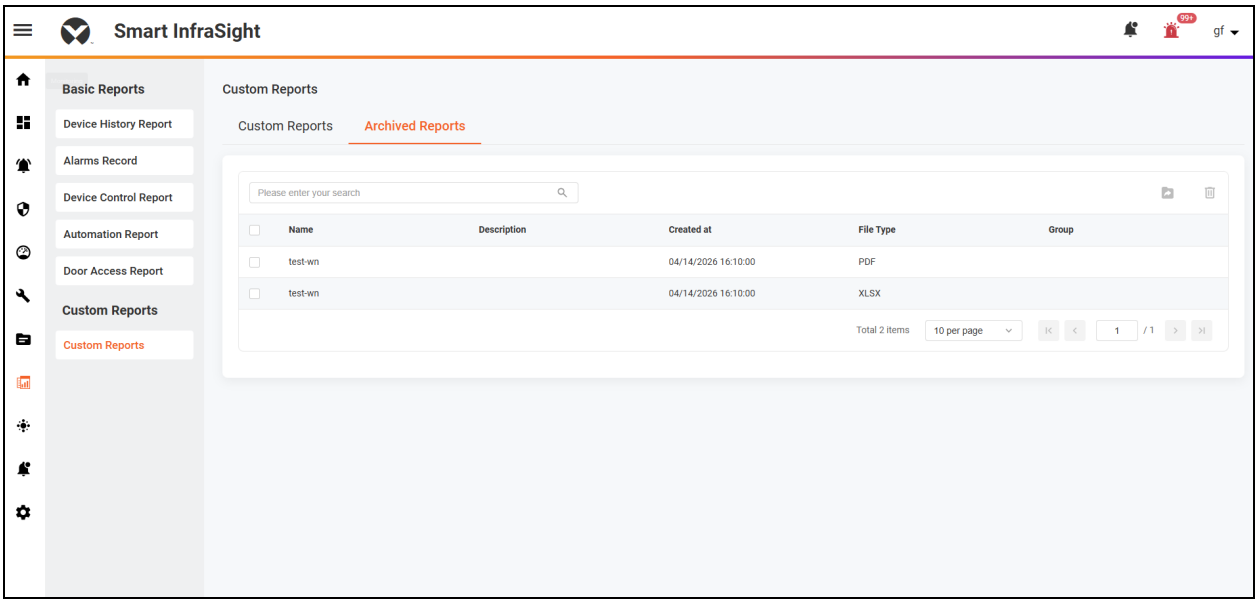
2. Enter a keyword in the search bar to quickly filter for the target archived report.
3. After selecting one or more report records in the list, the following actions become available in the operation area at the top-right:

- **Export**: Downloads the selected archived report file to your local machine. Only one record can be selected at a time for this operation; the button is grayed out and unavailable when multiple records are selected.
- **Delete**: Deletes the selected archived reports. A confirmation dialog box appears before the operation proceeds. This action is irreversible; proceed with caution.

4. The total number of archived reports is displayed at the bottom of the list. Use the rows-per-page drop-down list to adjust the number of entries displayed per page, and use the pagination controls to navigate between pages. You can also enter a target page number directly in the page number input box to jump to that page. See **Figure 15.27** on the next page).

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 15.27 Archived Reports Page



© 2026 Vertiv Group Corp. All Rights Reserved.

16 Visualization

16.1 General

16.1.1 Overview

The Visualization Center is a module in Vertiv™ Smart InfraSight™ that provides a library of reusable visual components. These visualizations can be configured once and placed across multiple areas of the system, including the Dashboard, the SNMP Site Monitoring Homepage, and the Custom Report, ensuring consistency across all data displays.

The Visualization Center is accessible from the left navigation bar. Click the *Visualization Center* icon (located below the Reports icon) to open the module.

Supported Visualization Types

The following visualization types are supported:

Table 16.1 Supported Visualization Types

Number	Visualization Type	Description
1	Time Series	Visualize how one or more metrics change over time
2	Bar Chart	Compare aggregated values across multiple groups
3	Pie Chart	Show each part's share of a total
4	Gauge	Highlight a single real-time or aggregated metric on a dial
5	Simple Value	Display a single value in large, prominent text
6	Table	Present structured data in multiple columns with sorting and summaries
7	Text	Show static or dynamic text using macro variables
8	Image	Embed a static image on the canvas

Overall Workflow

1. Open *Visualization Center*. Create and save the *chart*. Open the *target Dashboard*, Monitoring page, or Report. Drag and drop the chart into place.

Flow : Create → Edit → Use.

16.1.2 Functional Modules

Table 16.2 Functional Modules

Module	Description
Visualization List	Displays all created visualizations in List View or Grid View. Support search, filter, and delete operations.
Add Visualization	Allows users to create a new visualization by selecting a type, configuring data sources, and previewing the result.
Edit Visualization	Allows users to modify an existing visualization. The Visualization Type cannot be changed after saving.
Export to Excel	Exports the visualization data to an Excel file based on the configurations.
Use Visualization	Use visualization allows users to use the created visualization across the pages like Dashboard, Monitoring Homepage, and Reports.

© 2026 Vertiv Group Corp. All Rights Reserved.

16.2 Detailed Features

This section describes all configuration options and behaviors available in the Visualization Center in detail.

16.2.1 Visualization List

When you open the Visualization Center, the Visualization List Grid View page is displayed by default, where all created chart components are managed, as shown in Figure 16.1 on the facing page .

Grid View

In Grid View, each visualization is displayed as a card containing the following information:

- Visualization Name
- Description
- Group
- Number of Uses
- Preview image of the visualization
- Date and Time
- Creator

The search, filter, and delete features available in Grid View.

Search: Enter a keyword in the search box to search by Visualization Name or Description. The search supports fuzzy matching.

Visualization Type filter: Select a visualization type from the dropdown to filter the list by type.

Group filter: Select a group from the dropdown to filter the list by group. When filters are selected, a clear (X) icon appears next to the selected value. Click on the (X) icon to clear the selection and return to the default state, which displays all groups.

Delete: Click the *delete* icon. A popup window opens with the message, Are you sure to delete the selected x items?, and two buttons: Discard and OK. Click *OK* to delete the visualization, or click *Discard* to return to the previous state.

Group Management: Groups organize visualizations and enable filtering in the reference panels of Dashboard, Monitoring, and Report. The following rules apply.

• When no group is selected, the system shows all visualizations.

• The system has one built-in group, Unallocated, which cannot be deleted. Visualizations with no assigned group are automatically placed here.

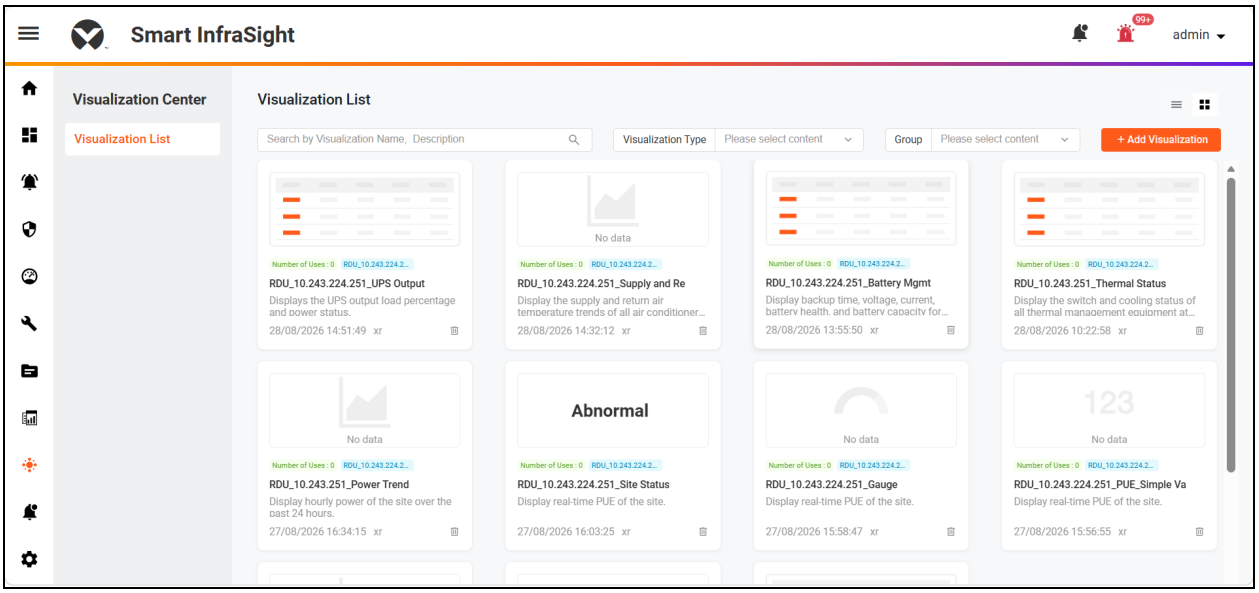
• User-created groups appear in the dropdown in alphabetical order (A–Z).

When we click on any portion of the card, it will redirect to the edit visualization page with prefilled information with its type.

The Visualization List page shows the search bar, Visualization Type and Group filters, view toggle, and Add Visualization button, as shown in Figure 16.1 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.1 Visualization List (Grid View)



List View

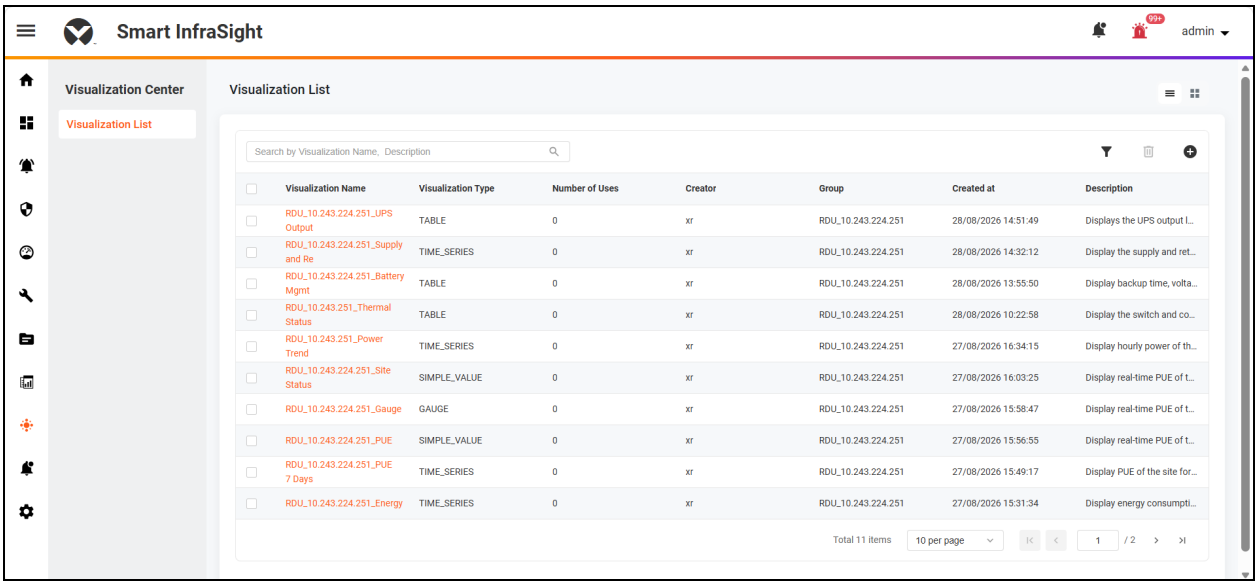
When you click on the toggle button, the **Visualization List** page is displayed as shown **Figure 16.2** on the next page .

The List View displays all available visualizations in a table format. The table contains the following columns, from left to right:

Column	Description
Multi-select checkbox	For bulk operations
Visualization Name	Click to open the edit page
Visualization Type	e.g., Time Series, Bar Chart
Number of Uses	Total number of places where this component is used
Creator	The user who created this component
Group	The group this visualization belongs to
Created At	Timestamp; sorted in descending order by default (newest first)
Description	Text description of the visualization

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.2 Visualization List (List View)



The list is sorted by **Created At** in descending order by default, with the most recently created visualization appearing first. The list displays **10 rows per page**.

Searching and Filtering

The Visualization List supports the following search and filter options, as shown in **Figure 16.2** above .

- **Search**: Enter a keyword in the search box to search by Visualization Name or Description. The search supports fuzzy matching.
- **Visualization Type filter**: Select a visualization type from the dropdown to filter the list by type.
- **Group filter**: Select a group from the dropdown to filter the list by group. When the filters are selected, a clear (X) icon appears next to the selected value. Click on the (X) icon to clear the selection and return to the default state, which displays all groups.

NOTE: The Group dropdown displays Unallocated and all user-created groups, sorted alphabetically (A–Z).

Pagination

The pagination bar is displayed at the bottom of the Visualization List. It shows the total number of items, the current page, and the total number of pages. Use the navigation controls to move between pages or enter a page number directly in the page number input field.

Visualization Access Permissions

Visualization access permissions control what actions a user can perform on visualizations. There are two types of permissions: View and Edit.

© 2026 Vertiv Group Corp. All Rights Reserved.

Permission Types

View Permission:

View permission allows users to access the Visualization Center and view visualizations. Users can view visualizations in the Dashboard, Monitoring Center, and Report Canvas. This permission provides read-only access, meaning users can view the data but cannot make any changes.

Edit Permission:

Edit permission allows users to modify visualizations, including updating configuration, adding or removing data, and saving changes. Users with edit permission automatically have view permission by default.

Figure 16.3 Visualization List

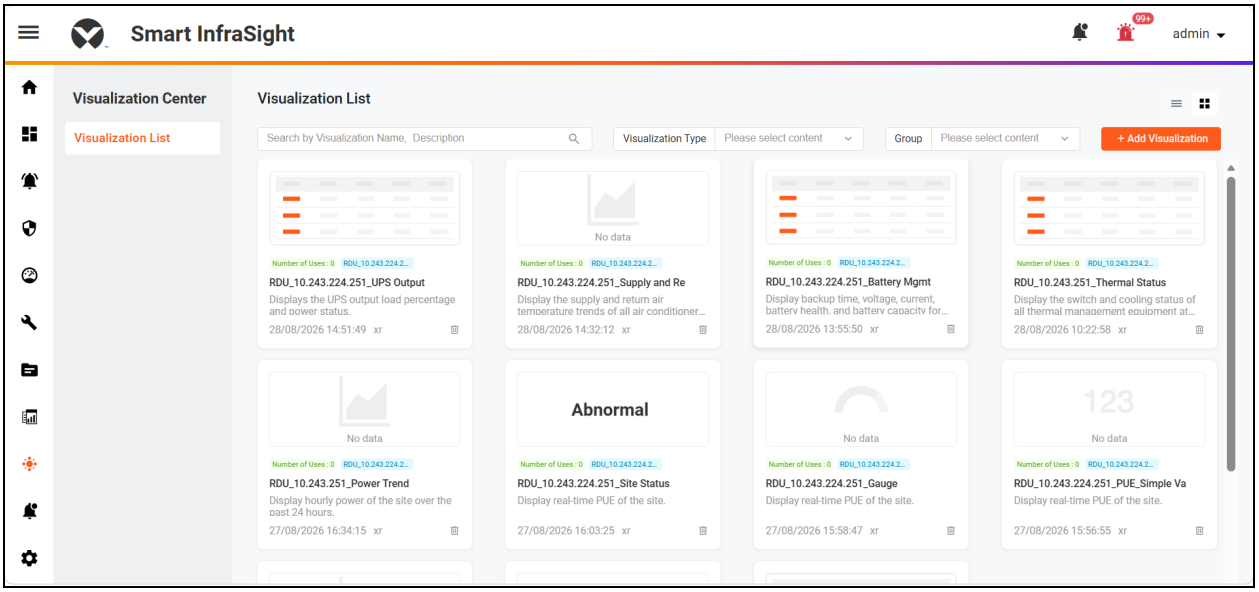
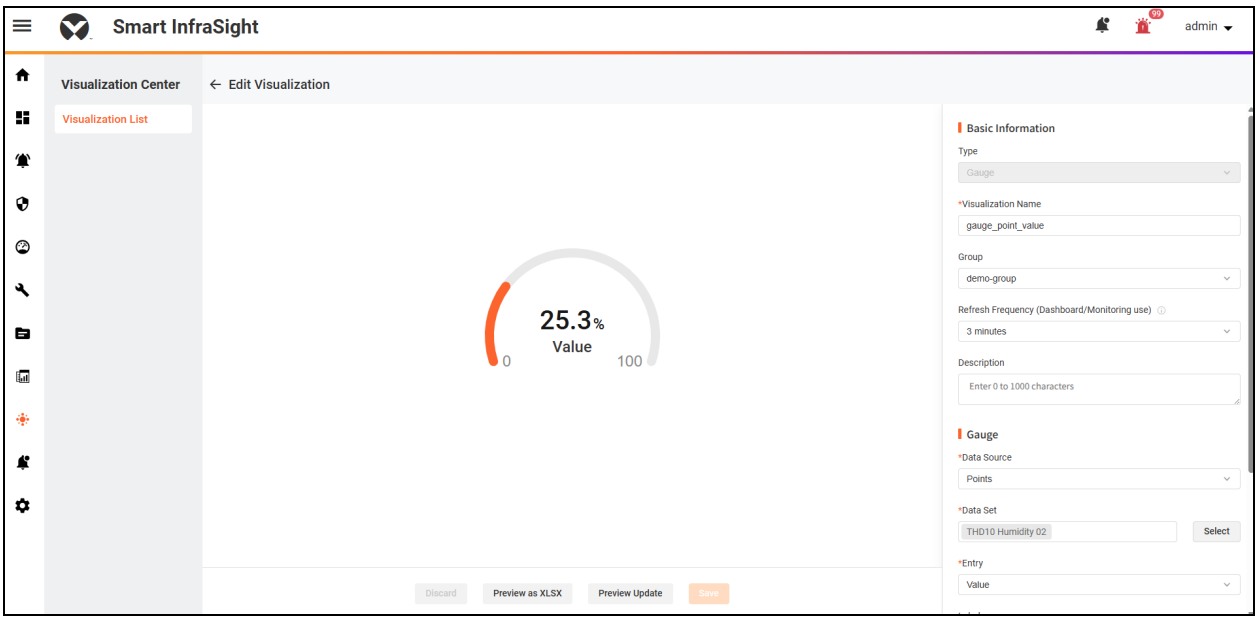


Figure 16.4 Editing Visualization



© 2026 Vertiv Group Corp. All Rights Reserved.

Permission Behavior

View permission can be assigned independently.

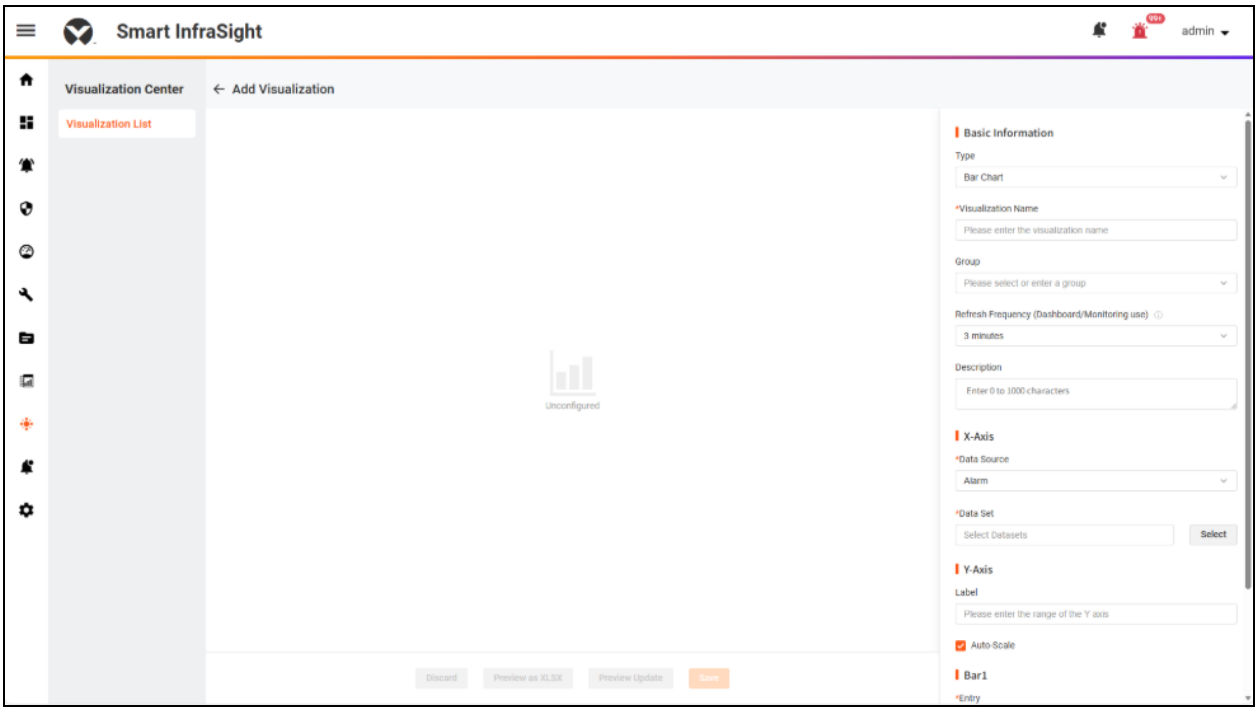
Edit permission cannot exist without view permission. When edit permission is enabled, view permission is automatically granted.

Users without view permission cannot access the visualization.

16.2.2 Creating a Visualization

To create a new visualization, click the *(+) Add Visualization button* on the Visualization List page. The Add Visualization page opens, as shown in Figure 16.5 below .

Figure 16.5 Adding a Visualization



The Add Visualization page is divided into two main sections:

Visualization Canvas (center): Displays a live preview of the visualization as it is being configured.

Configuration Panel (right side): Contains the Basic Information fields and type-specific configuration settings.

To return to the Visualization List page, click the back arrow (←) at the top left of the page.

Basic Information

The Basic Information section is displayed at the top of the Configuration Panel for all visualization types. Complete the following fields:

Visualization Type: Select the visualization type from the dropdown. The following options are available:

© 2026 Vertiv Group Corp. All Rights Reserved.

- Bar Chart (default)
- Time Series
- Pie Chart
- Gauge
- Simple Value
- Table
- Text
- Image

NOTE: Once a visualization has been saved, the Visualization Type cannot be changed during the Edit journey. During the Add journey, switching the type displays the following prompt:

Switching the type will clear all selected options. Do you want to continue?

Click *Yes* to proceed and clear all previously selected options or click *Cancel* to close the popup and retain the current selections.

Visualization Name (Required): Enter a name for the visualization. The name must be between 1 and 32 characters. Duplicate names are not allowed.

Group (Optional): Select an existing group from the dropdown or enter a new group name to create a new group. This field is optional. Group names must be between 0 and 32 characters and must be unique. If no group is selected, the visualization is assigned to the Unallocated group by default.

Refresh Frequency (Required): Select the interval at which the visualization updates automatically when placed on a Dashboard or Monitoring Homepage. The following options are available:

- 3 minutes
- 10 minutes
- 30 minutes

NOTE: The Refresh Frequency field is not displayed for Text and Image visualization types, as it is not applicable to these types.

Description (Optional): Enter an optional description for the visualization. The description can be between 0 and 1000 characters.

Data Source and Entry

A data source defines where the visualization data originates, such as alarms, assets, devices, probes, or other system entities.

A metric (Entry) represents the specific business value or indicator to be displayed from the selected data source, such as alarm duration, alarm count, device status, or probe values.

The relationship between them is straightforward: users must first select a data source, and then choose the corresponding metric from that data source.

The list of available metrics dynamically changes based on the selected data source, ensuring that only relevant options are displayed.

The available entries depend on the selected data source, as described in the following table:

© 2026 Vertiv Group Corp. All Rights Reserved.

Data Source	Available Entries
Alarm	Duration, Acknowledgement Duration, Severity, Device Name, Site, Location, Ended at, Started at
Asset	Position, U Height, Over-Warranty Duration, Purchase Date, Warranty Expiry Date, Name, Site, Location, Start Date
Device	Alarm Count (active), Name, Site, Location
Location	Device Count, Rack Count, Alarm Count, Name
Site	Location, Device Count, Rack Count, Alarm Count (active), Status, Name
Points	Value, Unit, Storage Interval, Storage Threshold, Name, Device, Site, Location
Rack	Total U of the Rack, Available U, Occupied U, Top/Middle/Bottom & Top/Middle/Bottom Temperature and Humidity (Front & Rear), Rated Power, Total Power, Name, Site, Location
IPMI Device	IP Address, Located Rack, Site, Location, Name
Power Consumption	Value, Name, Site
PUE	Value, Name

NOTE: Locations that do not have any Sites directly under them are not displayed in the selection list.

© 2026 Vertiv Group Corp. All Rights Reserved.

Selecting a Data Set

Where applicable, click the *Select* button next to the Data Set field to open the Data Set Selection popup. The popup displays available data sets based on the selected data source, which may be presented in a hierarchical (tree) structure or a flat list depending on the data source. The popup supports search functionality, with results sorted in ascending order. The right panel displays the currently selected items. Click *OK* to confirm the selection or cancel the popup without saving.

Roll Up - In Depth

Roll Up is the time-based data aggregation mechanism in the Visualization Center. It groups raw data into summary values at a chosen time of granularity, making trends and patterns easier to read.

When Do Roll Up Fields Appear?

Roll Up fields are not always visible. They appear automatically only when the selected combination of **Visualization Type + Data Source + Entry** supports time-based aggregation. If this combination does not support it, the fields are hidden.

This means:

- Not every Entry has a time dimension. Descriptive fields such as device name or IP address cannot be aggregated and will not trigger Roll Up fields to appear.
- If Roll Up fields disappear after switching the Data Source or Entry, this is expected behavior, not a bug.
- Switching back to a combination that supports aggregation will restore the fields automatically.

Roll Up configuration consists of two fields: **Roll Up Interval** and **Roll Up Method**.

Roll Up Interval

Defines the time granularity at which raw data points are grouped and summarized.

Option	Granularity	Each Data Point Represents
Hourly (default)	Calendar hour	HH: 00:00 – HH: 59:59
Daily	Calendar day	00:00:00 – 23:59:59
Weekly	Calendar week	Monday 00:00:00 – Sunday 23:59:59
Monthly	Calendar month	1st day 00:00:00 – last day 23:59:59
Real-time	No aggregation	Fetches the current live value (Gauge and Simple Value only)

The following rules apply to Roll Up Interval

- All aggregations are calculated using the server's UTC time to ensure consistent results across users in different time zones.
- For display purposes, aggregated data points are labeled with the start of the aggregation period. For example, daily aggregation for January 13 is displayed at 00:00:00 on January 13, even though the aggregation is completed at 23:59:59.
- If the selected time range does not align exactly with aggregation period boundaries - for example, the range starts mid-week, but the interval is Weekly - partial periods at the start or end are expected and handled correctly.

Roll Up Method

Defines how multiple raw data points within each interval are combined into a single value.

© 2026 Vertiv Group Corp. All Rights Reserved.

Option	Calculation	Typical Use Case
Average (default)	Arithmetic mean of all values in the interval	Trend analysis for continuous metrics such as temperature or humidity
Maximum	Highest value recorded in the interval	Peak monitoring, for example maximum power draw
Minimum	Lowest value recorded in the interval	Low-point analysis, for example minimum temperature
Sum	Total of all values in the interval	Cumulative totals, for example energy consumption

NOTE: When Sum is selected, the system first adds the raw values and then converts the unit. For example: 30°C + 30°C + 30°C = 90°C → 194°F. Summing temperature values is physically meaningless, but the system does not restrict this combination. Users are responsible for ensuring their configuration is logically appropriate.

Special Constraint for Time Series

Time Series charts have an additional dependency: the available Roll Up Interval options are constrained by the selected Time Range. This prevents meaningless combinations — for example, a 1-hour time window with Monthly aggregation would yield only one data point with no useful reference.

The available combinations are as follows:

Time Range	Hourly	Daily	Weekly	Monthly
Last Hour	✓ Default	—	—	—
Last 24 Hours	✓	✓	—	—
Last 7 Days	✓	✓	✓	—
Last 30 Days	—	✓	✓	✓
Custom (≤ 30 days)	✓	✓	✓	✓

NOTE: When the selected Roll Up Interval becomes unavailable due to a Time Range change, the system automatically resets the Roll Up Interval to the nearest available option.

Page Buttons

The four buttons at the bottom of the create and edit pages are independent of each other — as long as the form is valid, any button can be clicked at any time in any order.

Button	Description
Save	Saves the current configuration and automatically updates the preview image
Preview	Refreshes the left canvas to reflect the current configuration (does not save)
Preview as XLSX	Generates and downloads an Excel file based on the current configuration and data (does not save)
Discard	Discards all unsaved changes on the current page.

When clicking *Discard* with unsaved changes, a confirmation prompt appears:

Discard

Are you sure you want to Discard?

Buttons: Yes / No

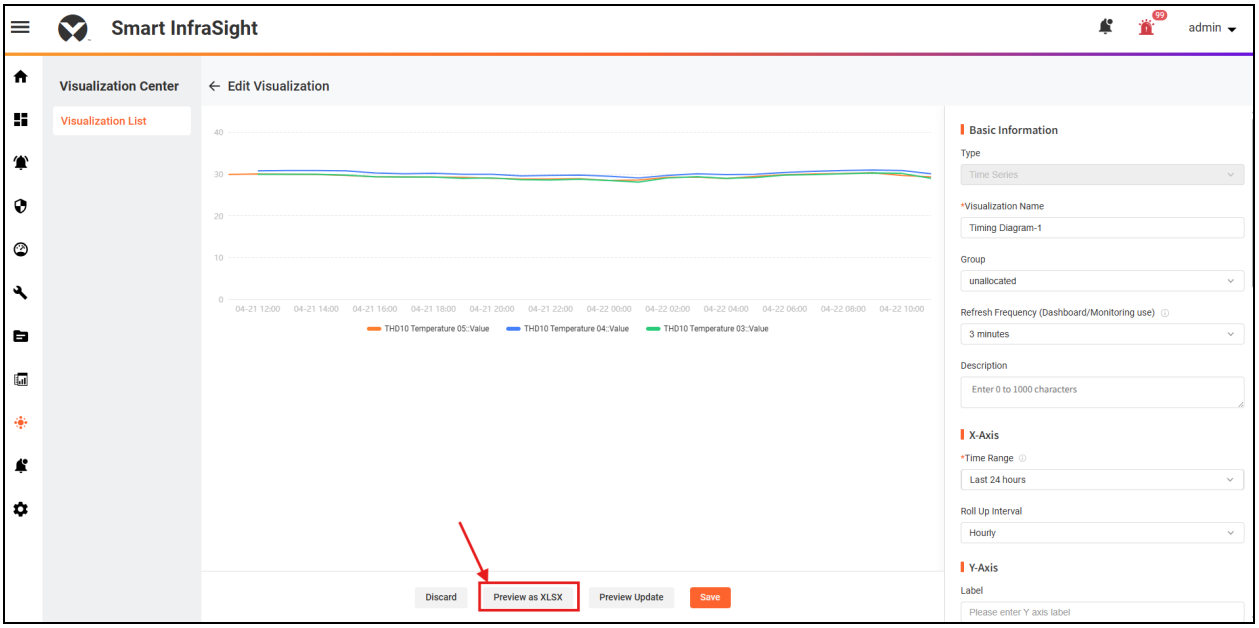
© 2026 Vertiv Group Corp. All Rights Reserved.

Clicking *Yes* displays **The changes have been discarded**. A similar prompt appears when leaving the page via the back button, a menu link, or other navigation while unsaved changes exist.

16.2.3 Export to Excel

Clicking the Preview as XLSX button generates the visualization data in Excel format and opens a file save dialog, allowing users to choose the location and download the file for further analysis. You can export the Excel file either after saving the visualization or directly preview the data in Excel without saving.

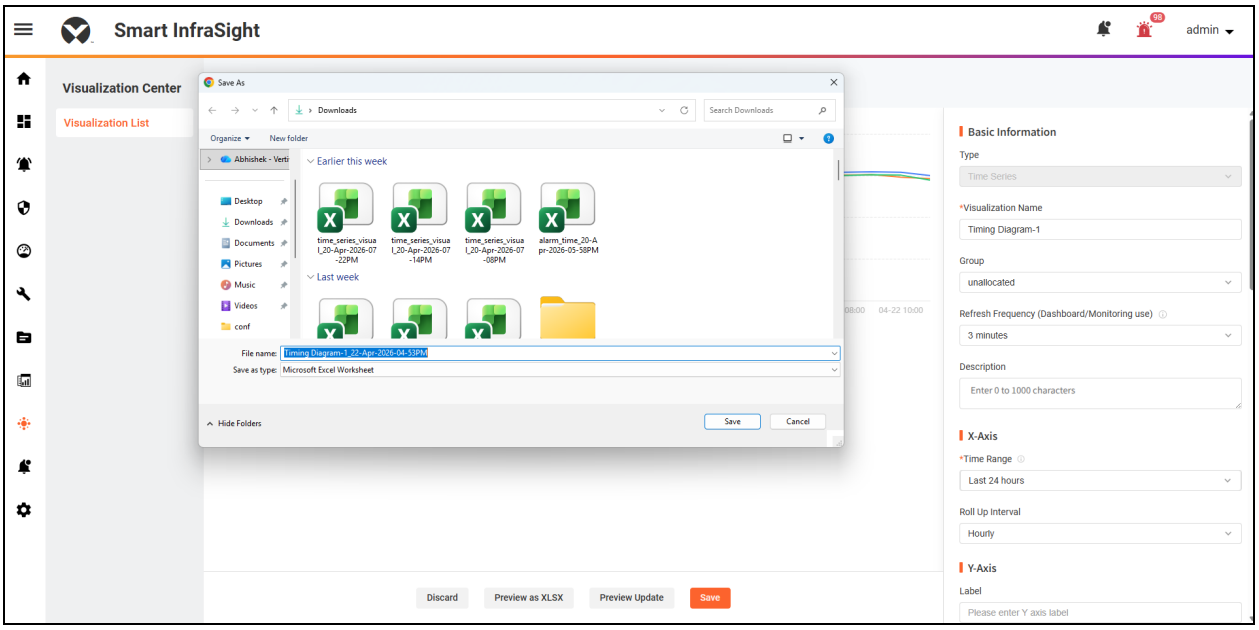
Figure 16.6 Preview as XLSX



Click on **Preview as XLSX** to open the file save dialog and select the download location.

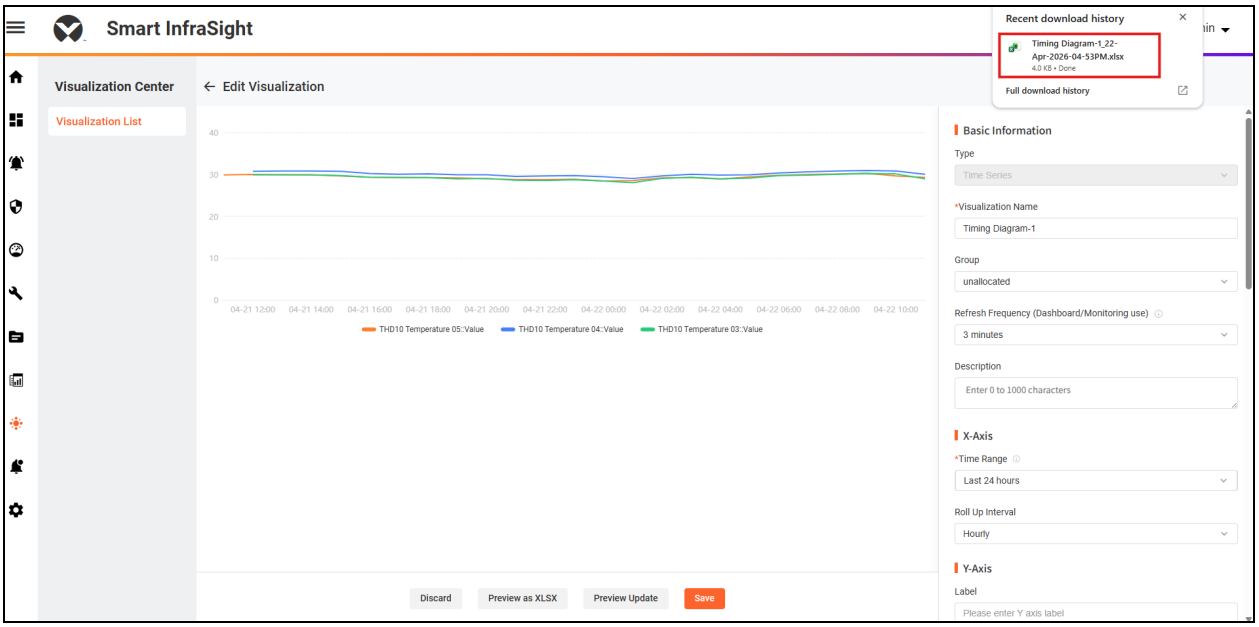
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.7 Exporting the Excel File



After selecting the download location, click *Save* to download the Excel file.

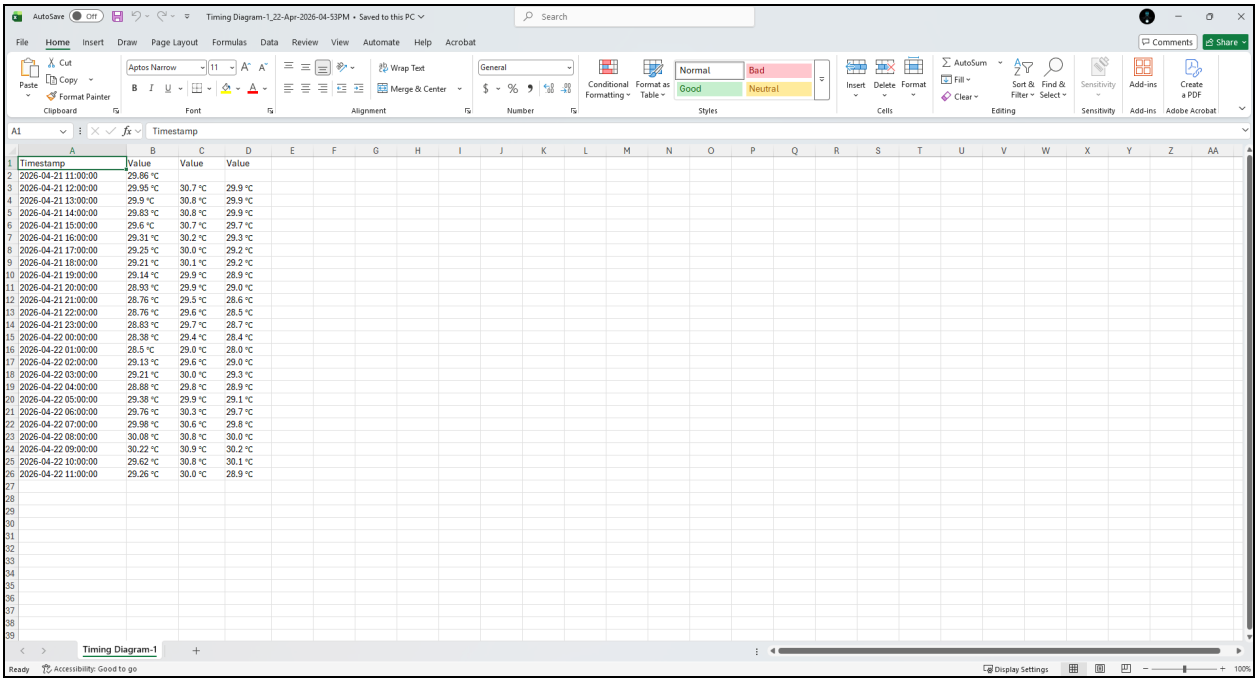
Figure 16.8 Downloading the Excel File



After the download is complete, you can view the data in the Excel file.

© 2026 Vertiv Group Corp. All Rights Reserved.

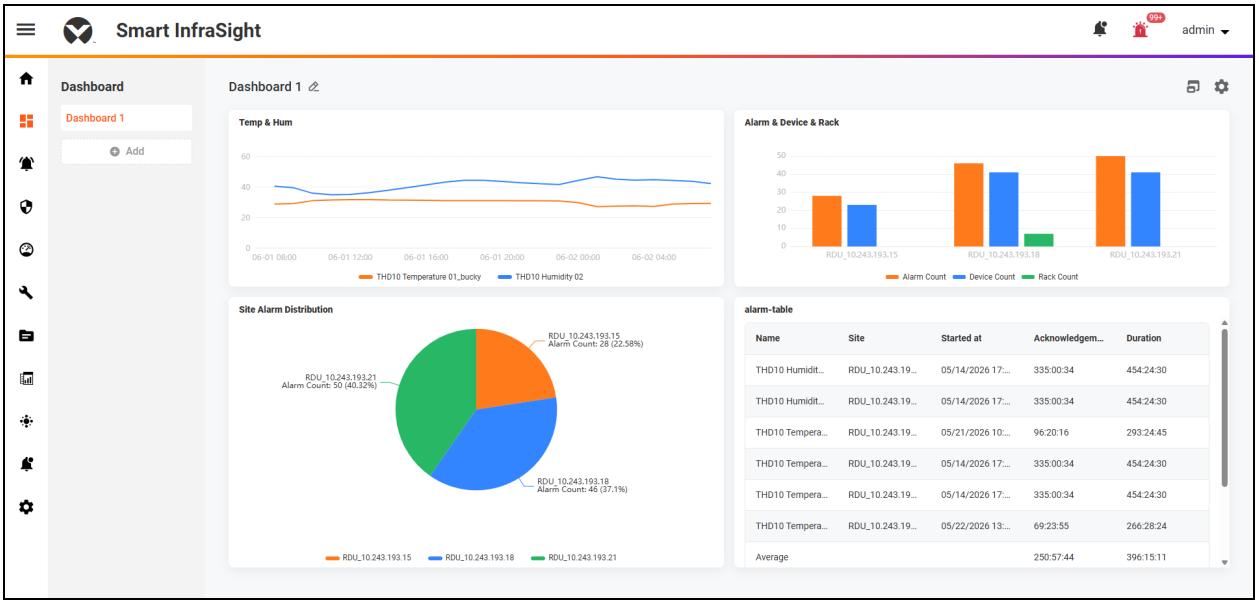
Figure 16.9 Viewing the Excel File



16.2.4 Visualization Usage

Dashboard: Visualizations can be added to dashboards to provide a consolidated view of key metrics, allowing users to monitor multiple charts in a single screen for quick analysis.

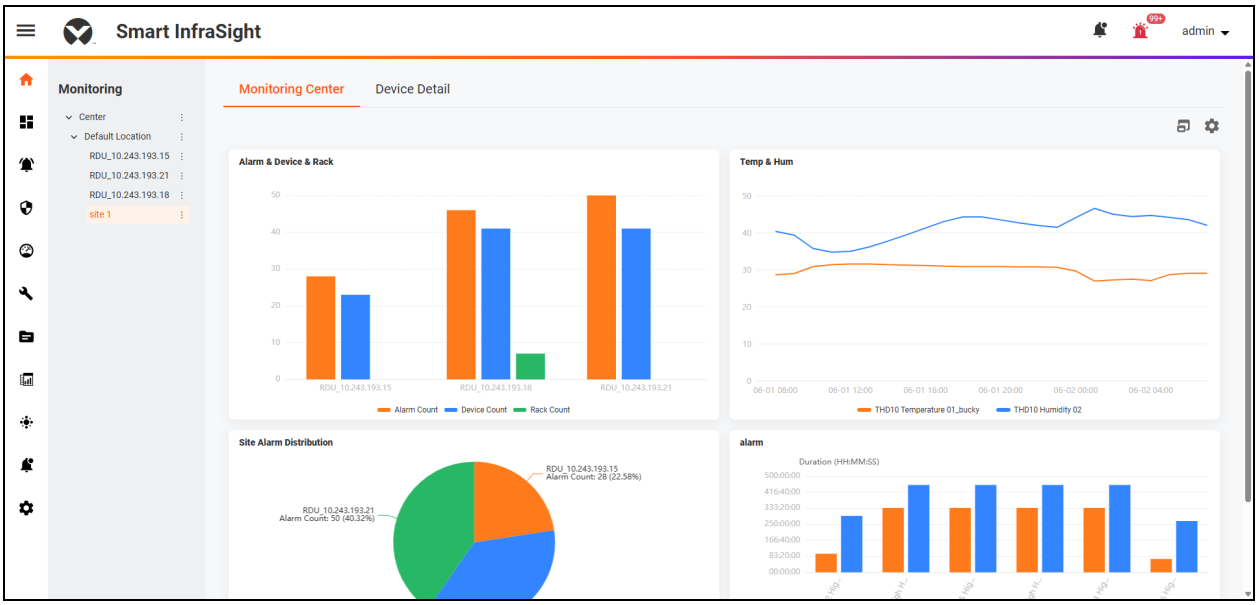
Figure 16.10 Dashboard



SNMP Monitoring Homepage: Visualizations can be used in the SNMP Monitoring Homepage to display real-time or near real-time data for SNMP-enabled devices and sites, helping users continuously track system status and performance.

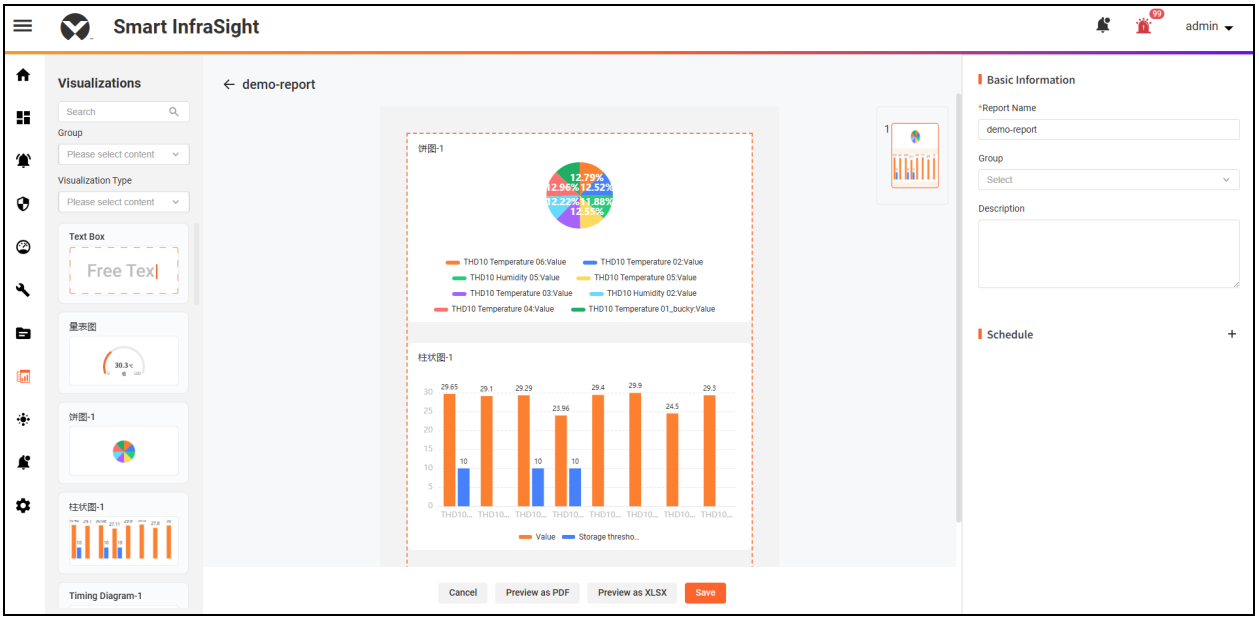
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.11 SNMP Monitoring Homepage



Report: Visualizations can be added to reports to present data in a structured and shareable format, enabling users to analyze, export, and communicate insights through customized report layouts.

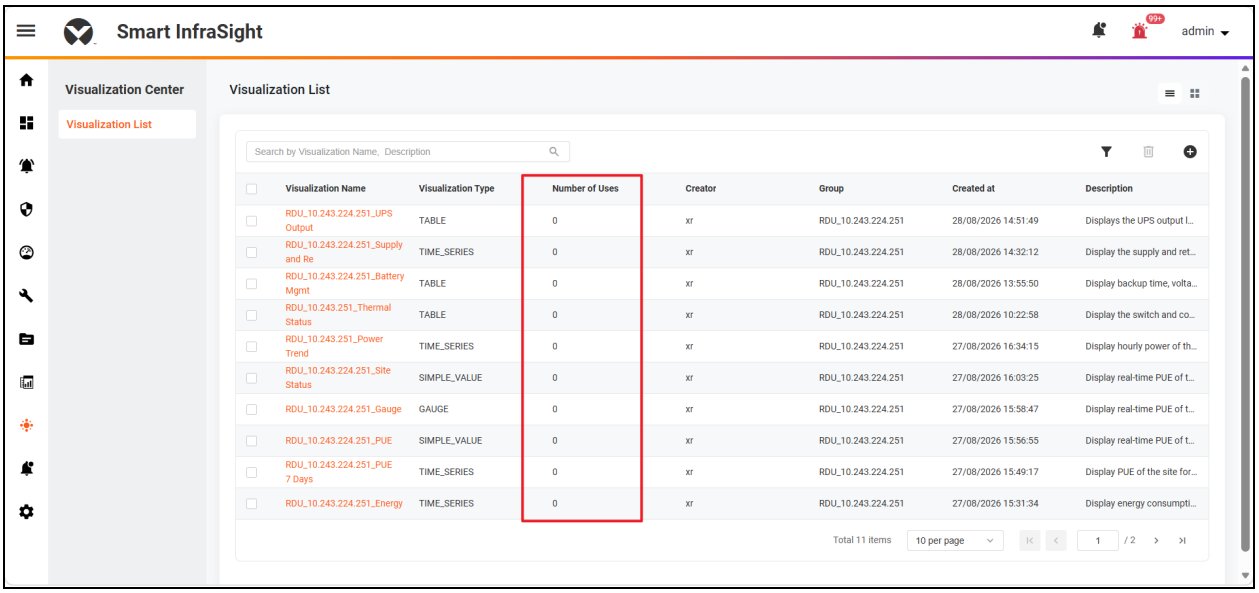
Figure 16.12 Report



Usage Tracking: Users can track the usage of each visualization through the Number of Uses column in the Visualization List, which indicates how frequently a visualization is utilized across the system.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.13 Usage Tracking

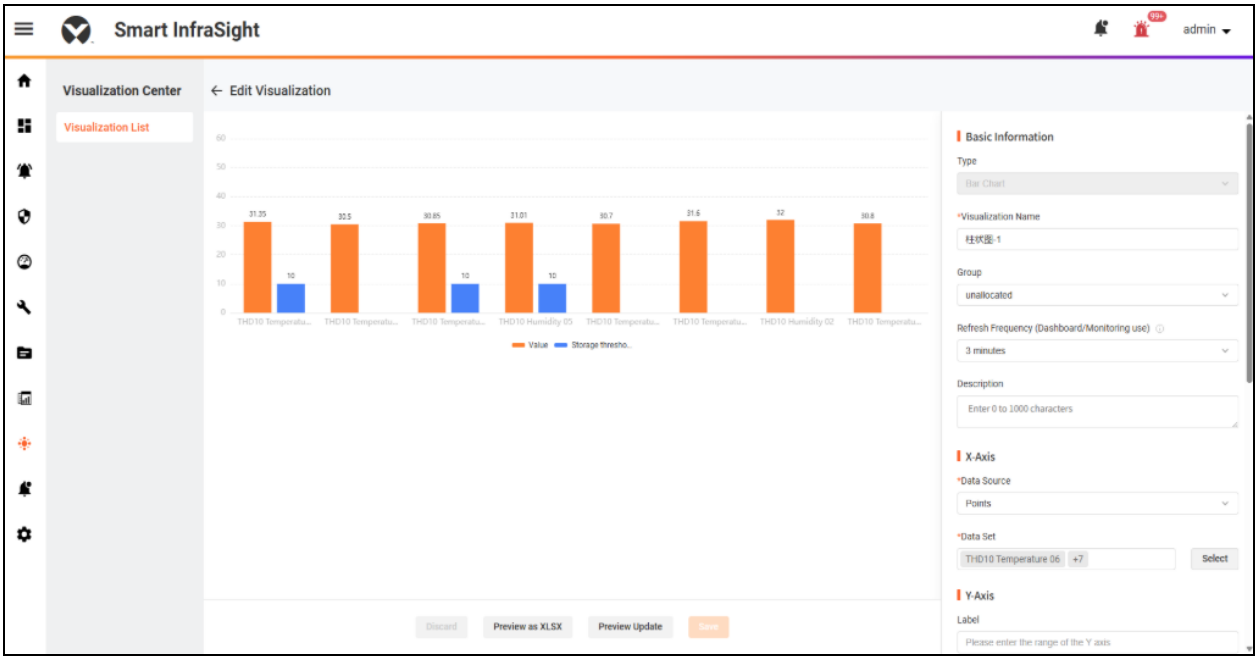


16.3 Visualization Type

16.3.1 Bar Chart

After selecting **Bar Chart** as the visualization type and completing the Basic Information fields, configure the following settings, as shown in **Figure 16.14** below .

Figure 16.14 Bar Chart



© 2026 Vertiv Group Corp. All Rights Reserved.

1. Configure X-Axis

Data Source: Select the data source for the bar chart.

Data Set: Click the *Select* button to open the Data Set Selection popup and select the dataset. Each entry row added in the Bar section corresponds to one bar on the chart.

2. Configure Y-Axis

Label: Enter an optional label for the Y-axis. The label can be between 0 and 32 characters.

Auto-Scale: The **Auto-Scale** checkbox is selected by default. When Auto-Scale is enabled, the Y-axis scale is set automatically. To define a fixed scale, clear the **Auto-Scale** checkbox and enter values in the **Upper Range** and **Lower Range** fields. Both fields are mandatory and accept values between -99,999,999 and +99,999,999.

3. Configure Bar

Each bar entry represents one bar on the chart. By default, one bar row is displayed. Multiple bars can be added.

For each bar, configure the following fields:

• **Entry**: Select the entry for this bar.

• **Label**: Enter an optional label for this bar. The label can be between 0 and 32 characters. If left empty, the entry name is used as the label.

The following controls are available for each bar row:

↑ **(Move Up)**: Moves the bar one position up in the order. This control is not displayed for the topmost bar.

— **(Remove)**: Removes the bar row. This control is not displayed when only one bar remains.

To add a bar, click the *Add Bar* button at the bottom of the Bar section.

NOTE: If a bar has no data, it is not displayed on the chart. Bars with mismatched units cannot be saved.

4. Roll Up

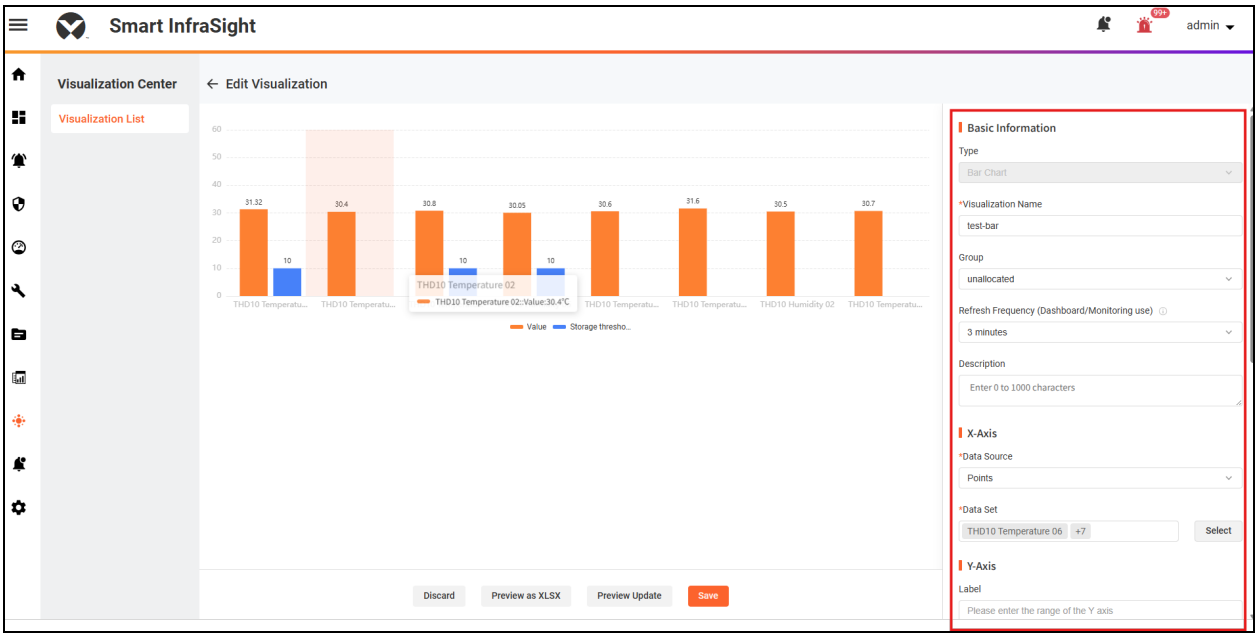
If applicable, configure the following roll-up fields:

- **Time Range:** Select the time range. Options: Last Hour (default), Last 24 Hours, Last 7 Days, Last 30 Days, Custom (maximum 30 days).
- **Roll Up Method:** Select the aggregation method used to calculate values within each interval, such as Average, Sum, Minimum, or Maximum, which determines how multiple data points are combined into a single value.

Add Visualization page for Bar Chart type showing the preview canvas, Basic Information panel, X-Axis Data Source and Data Set fields, and Y-Axis Label field. As shown in **Figure 16.15** on the facing page .

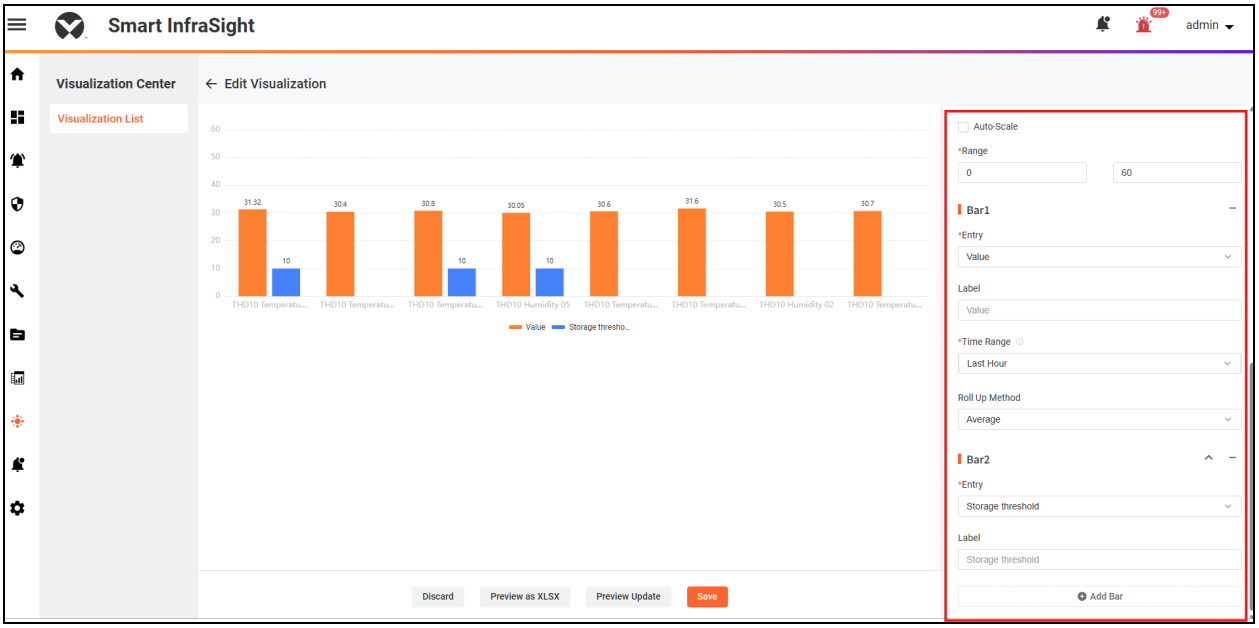
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.15 Bar Chart Configuration



Bar Chart configuration panel showing Y-Axis Auto-Scale checkbox, Bar section with Entry and Label fields, move-up and remove icons, and the Add Bar (1/30) button. As shown in **Figure 16.16** below .

Figure 16.16 Bar Chart Configuration

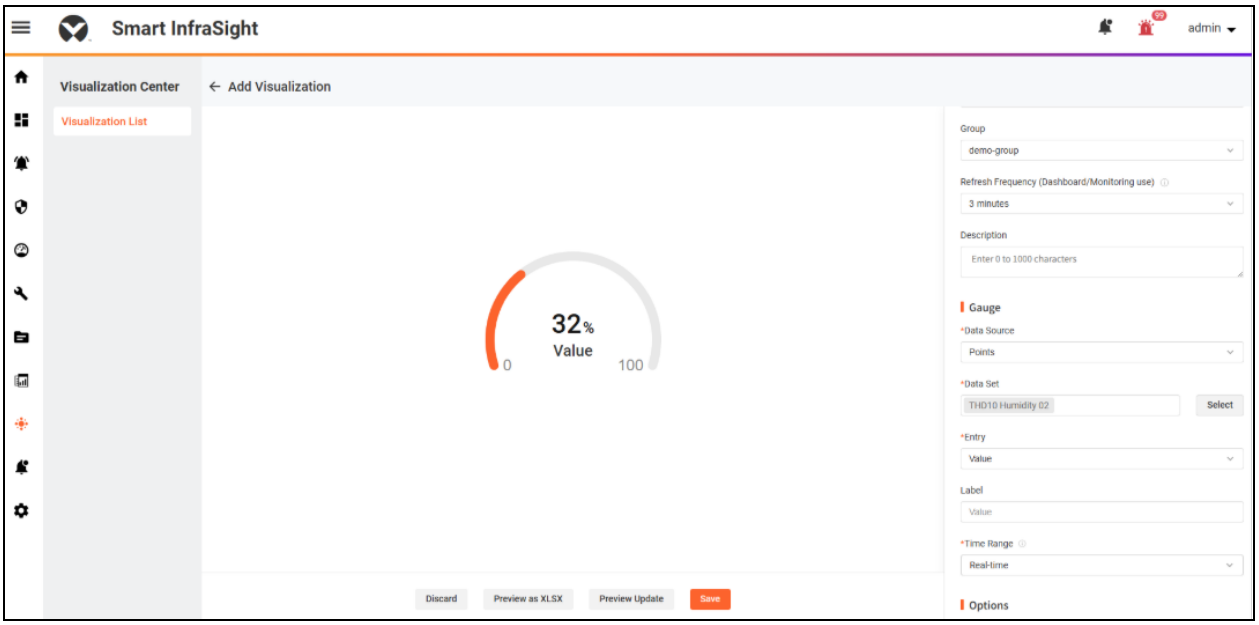


16.3.2 Gauge

After selecting **Gauge** as the visualization type and completing the Basic Information fields, configure the following settings, as shown in **Figure 16.17** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.17 Gauge



The Gauge visualization supports only one metric. No **Add** button is available.

1. Gauge Configuration

Configure the following fields in the **Gauge** section:

Data Source: Select the data source.

Data Set: Click the *Select* button to open the Data Set Selection popup and select the dataset.

Entry: Select the *entry*. The entry value and unit are displayed in the center of the gauge.

Label: Enter an optional label. The label can be between 0 and 32 characters and is displayed on hover.

Time Range: Select the time range. Options: **Real-time** (default), Last Hour , Last 24 Hours, Last 7 Days, Last 30 Days, Custom (maximum 30 days).

Roll Up Method: Select the aggregation method used to calculate values within each interval, such as Average, Sum, Minimum, or Maximum, which determines how multiple data points are combined into a single value.

2. Options

Configure the following fields in the **Options** section:

Range: This field is mandatory. Enter the minimum value in the left input box and the maximum value in the right input box. Both values must be integers between –10,000,000 and +10,000,000. The minimum value must be less than the maximum value. If the minimum value is greater than or equal to the maximum value, the following error message is displayed:

The minimum value needs to be less than the maximum value.

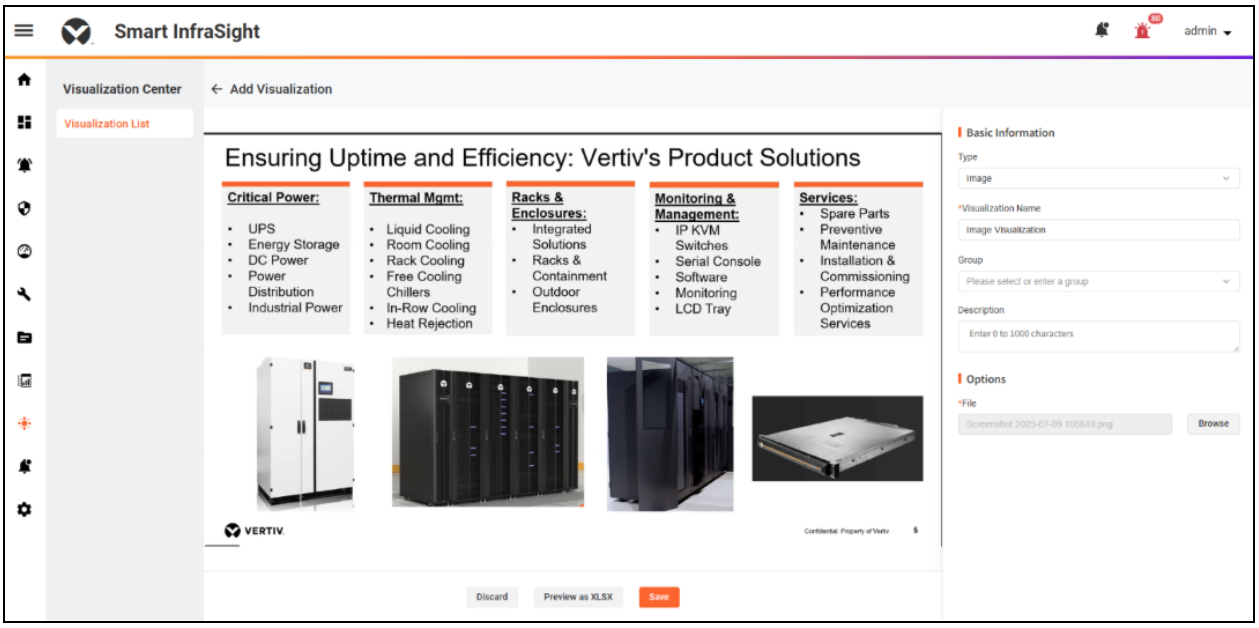
Unit: The unit is auto-filled based on the selected dataset and entry. If no unit is applicable, the field displays (--).

© 2026 Vertiv Group Corp. All Rights Reserved.

16.3.3 Image

After selecting Image as the visualization type and completing the Basic Information fields, configure the following settings in the **Options** section, as shown in **Figure 16.18** below .

Figure 16.18 Image



NOTE: The Refresh Frequency field is not displayed for the Image visualization type.

IMPORTANT: The visualization canvas updates in **Real Time** when a file is selected. No **Preview Update** button is displayed for this type.

File: This field is mandatory. Click the *Browse* button to open the system file browser and select an image file. The following file formats are supported: .jpg, .jpeg, .png. The maximum file size is **3 MB**.

When a valid file is selected, the file name is displayed in the file input field, and the image preview is updated automatically in the visualization canvas.

The following error messages may be displayed:

Invalid file format. Allowed formats: .jpg, .jpeg, .png — displayed when the selected file is not supported.

The size of the uploaded file cannot exceed 3 MB — displayed when the selected file exceeds the maximum size limit.

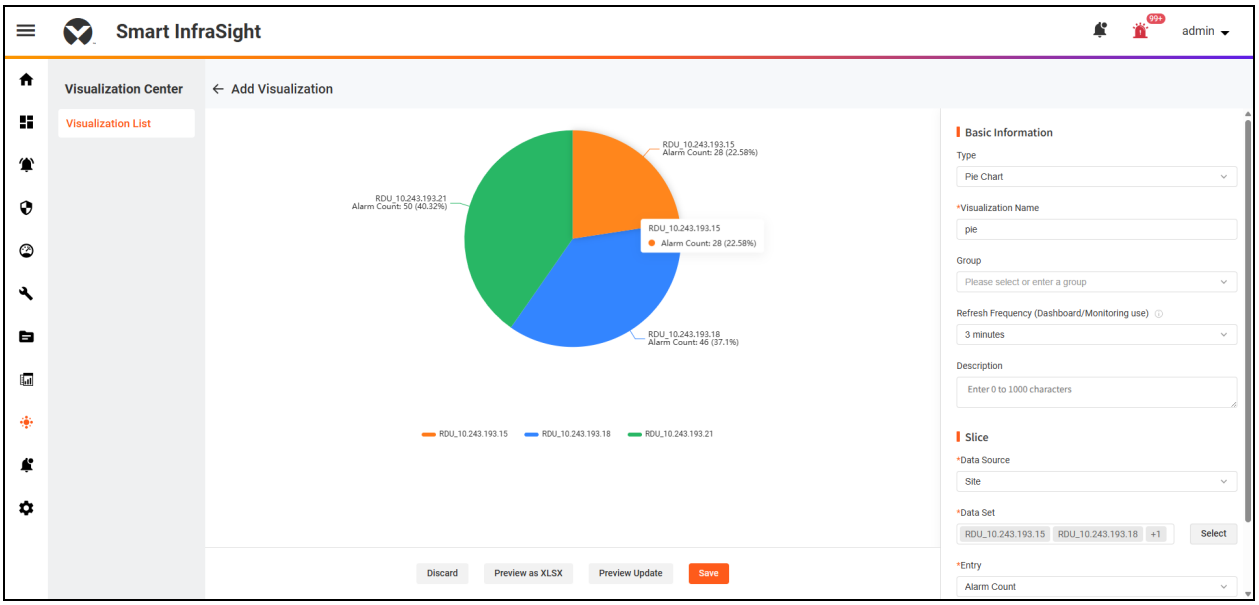
Add Visualization page for Image type showing the image preview canvas and Options section with the mandatory File field and Browse button. As shown in **Figure 16.18** above .

16.3.4 Pie Chart

After selecting **Pie Chart** as the visualization type and completing the Basic Information fields, configure the following settings in the **Slice** section, as shown in **Figure 16.19** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.19 Pie Chart



Each slice in the pie chart corresponds to one selected dataset. Configure the following fields:

Slice Configuration

The Slice section defines the data that the Pie Chart displays. Each row in the Slice list represents one slice of the pie, corresponding to one dataset.

IMPORTANT! How Slices Work in a Pie Chart: A Pie Chart has exactly one Entry (metric) for the entire chart. Multiple slices are created by selecting multiple datasets — not by selecting multiple entries. Every slice shows the value of the same entry for a different dataset. For example, if the entry is Total Power, each slice shows the total power of a different rack. The pie as a whole shows how total power is distributed across all selected racks.

Data Source: Select the data source for the pie chart.

Data Set: Click the *Select* button to open the Data Set Selection popup. Each selected dataset corresponds to one slice in the pie chart. Selected datasets are displayed as tags in the field.

Entry: Select a single entry for the entire pie chart. The entry determines the value used for all slices. The unit is displayed outside the Slice section.

Label: Enter an optional label. The label can be between 0 and 32 characters and is displayed on hover.

Time Range: Select the time range. Options: Last Hour (default), Last 24 Hours, Last 7 Days, Last 30 Days, Custom (maximum 30 days).

Roll Up Method: Select the aggregation method used to calculate values within each interval, such as Average, Sum, Minimum, or Maximum, which determines how multiple data points are combined into a single value.

NOTE: The Entry field applies to the entire pie chart, not to individual slices. The remove control is not displayed when only one slice row remains.

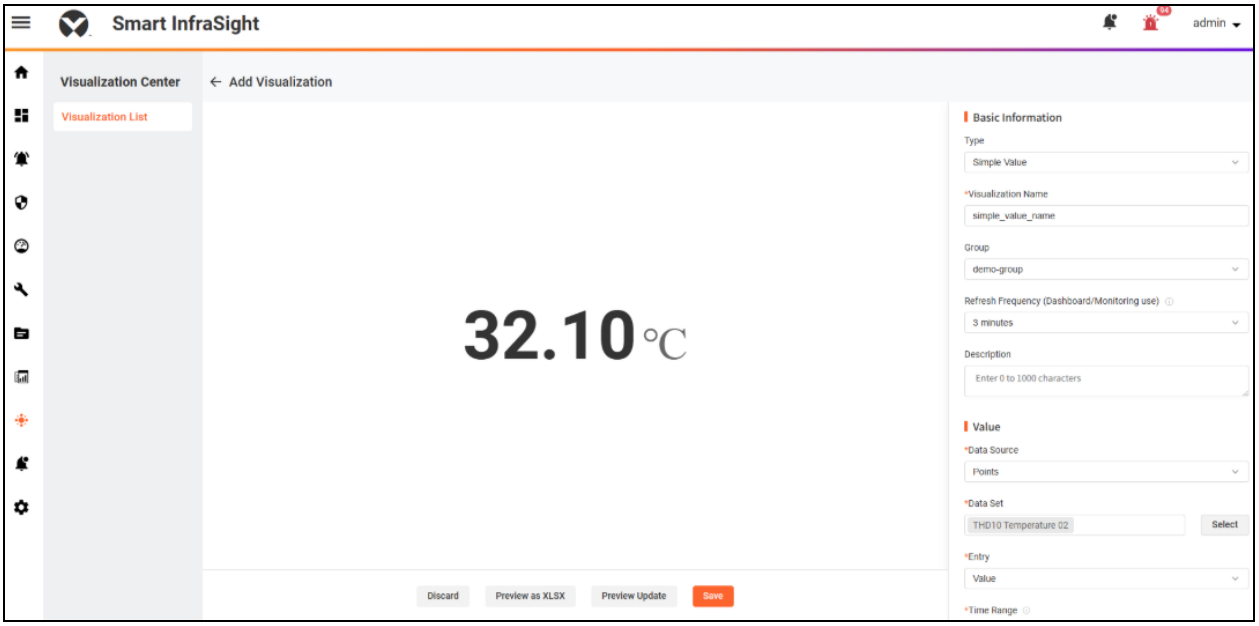
© 2026 Vertiv Group Corp. All Rights Reserved.

16.3.5 Simple Value

The Simple Value visualization displays a single large numeric value from a monitored data point — such as temperature, power consumption, or any sensor reading. It is ideal for at-a-glance monitoring.

How to Create a Simple Value Visualization

Figure 16.20 Simple Value



After selecting **Simple Value** as the visualization type and completing the Basic Information fields, configure the following settings, as shown in **Figure 16.21** on the next page .

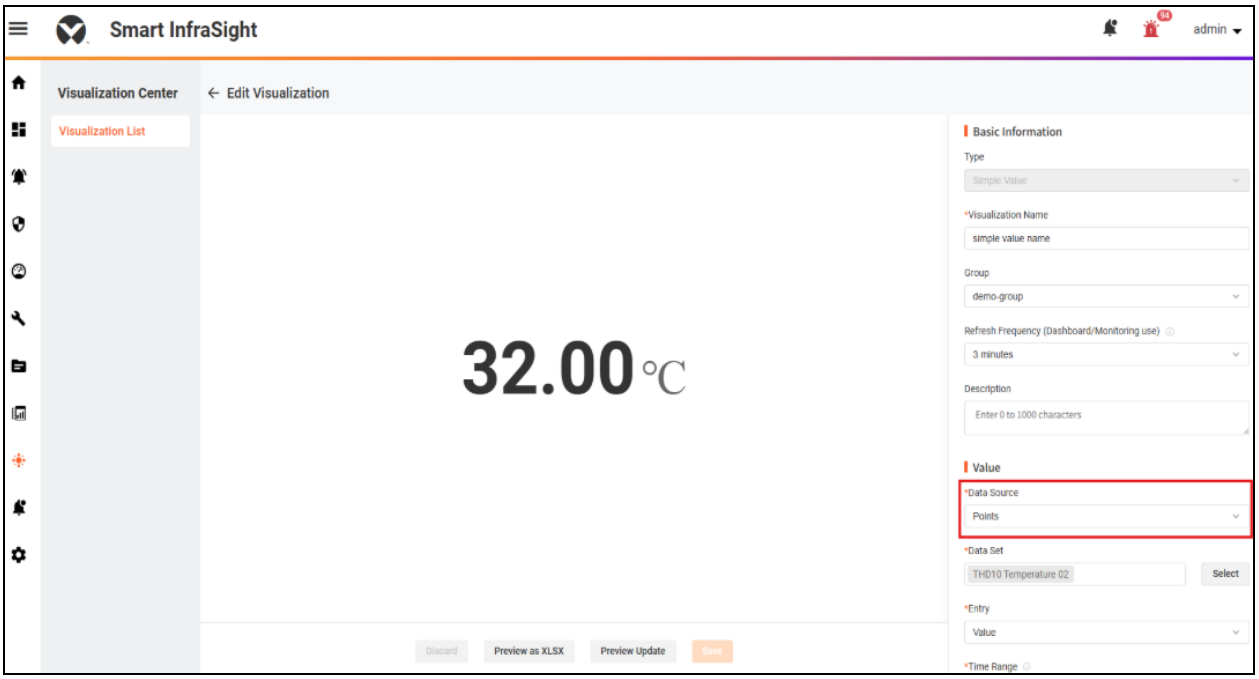
1. Simple Value Configuration

Configure the following fields in the **Value** section:

Data Source: Select the data source.

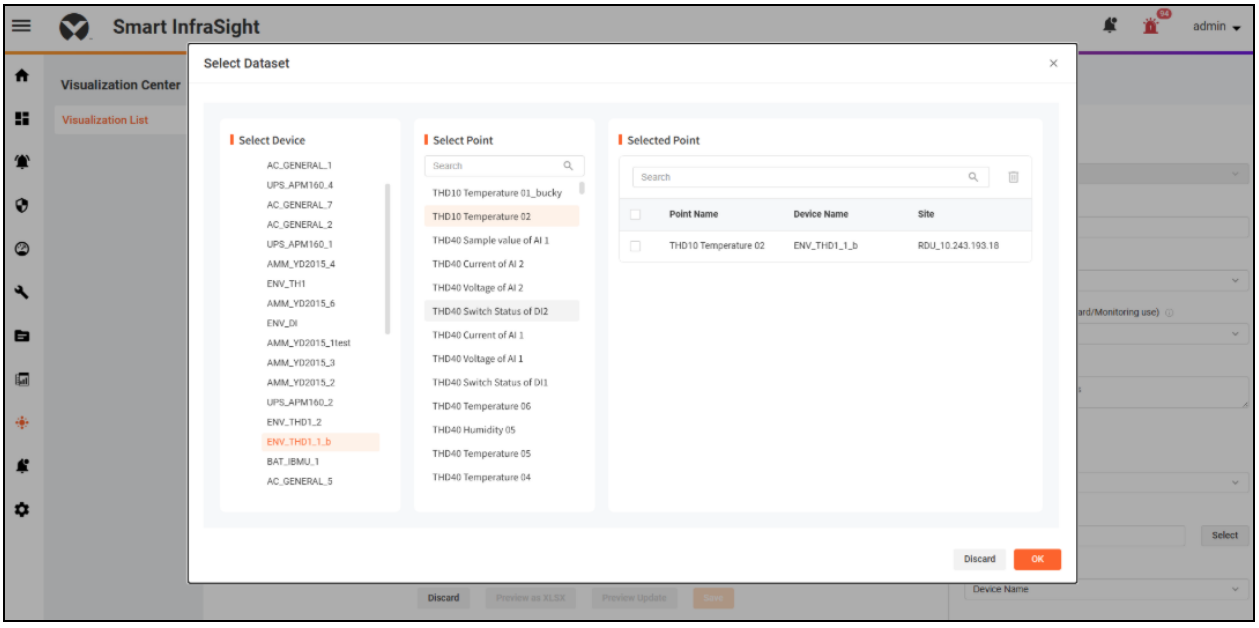
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.21 Simple Value Configuration



Data Set: Click the *Select* button to open the Data Set Selection popup and select the dataset. Selected datasets are displayed as tags in the field.

Figure 16.22 Simple Value Configuration



Entry: Select the entry. The entry value and unit are displayed in the center of the canvas.

Time Range: Select the time range. Options: Last Hour (default), Last 24 Hours, Last 7 Days, Last 30 Days, Custom (maximum 30 days).

© 2026 Vertiv Group Corp. All Rights Reserved.

Roll Up Method: Select the aggregation method used to calculate values within each interval, such as Average, Sum, Minimum, or Maximum, which determines how multiple data points are combined into a single value.

16.3.6 Table

After selecting Table as the visualization type and completing the Basic Information fields, configure the following settings. As shown in figure below.

1. Correlation

Correlate On: Select the correlation mode from the dropdown.

Time Correlation: Data is correlated based on time. A Timestamp column is added. Roll Up fields (Time Range and Roll Up Interval) are displayed. Data is aggregated over time.

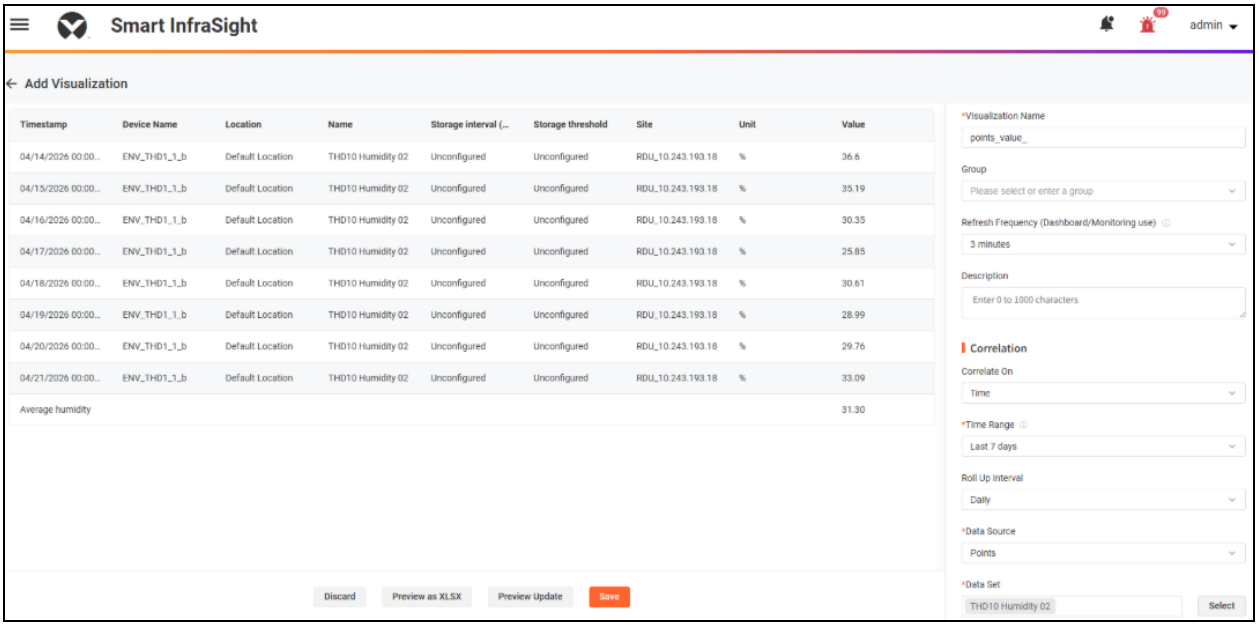
Roll-Up Configuration:

Time Range: Select duration. Options include Last Hour (default), Last 24 Hours, Last 7 Days, Last 30 Days, and Custom (up to 30 days).

Roll Up Interval: Select the interval used to aggregate data over time.

NOTE: When the statistical dimension is Time and the Value metric is selected, a Timestamp column will be additionally displayed in the leftmost column of the table.

Figure 16.23 Table

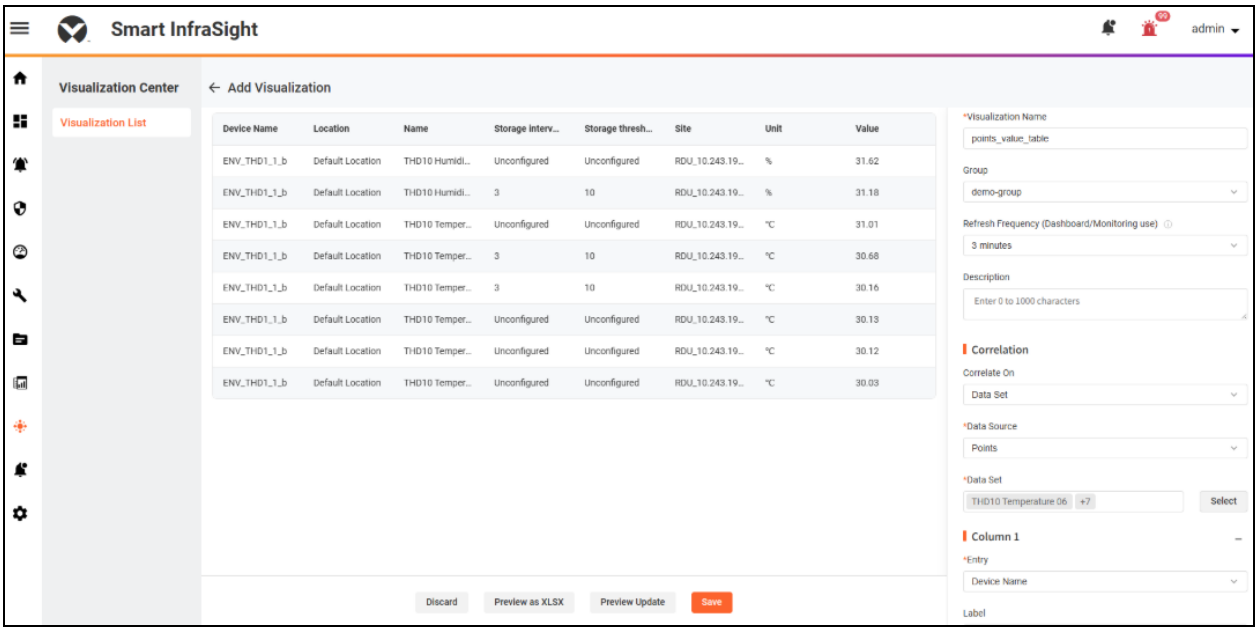


Column Configuration: Based on the selected data source, columns are generated from the available entry series of that data source; for example, selecting the **Points** data source provides columns such as Device Name, Location, Name, Storage interval (min), Storage threshold, Site, Unit, value.

Data Set Correlation (Default): Data is correlated based on selected datasets.

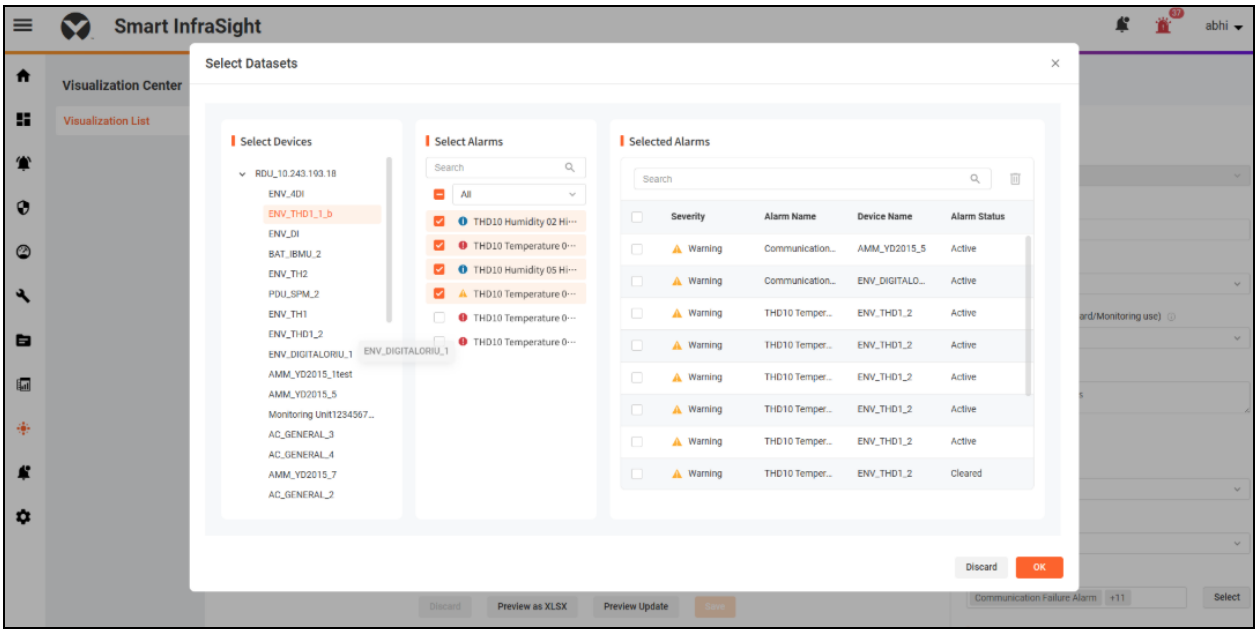
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.24 Table Configuration



Data Source and Data Set

Figure 16.25 Table Configuration (Continued)



Data Source: Select the data source for the table.

Data Set: Click the *Select* button to open the Data Set Selection popup and select the dataset. Selected datasets are displayed as tags in the field.

© 2026 Vertiv Group Corp. All Rights Reserved.

2. Columns

By default, one column (Column 1) is displayed. Subsequent columns are labeled Column 2, Column 3, and so on. For each column, configure the following fields:

Entry: Select the entry for this column. This field is mandatory.

Label: Enter an optional label for the column header. The label can be between 0 and 32 characters. If left empty, the entry name is used as the column header.

Hidden: Select the **Hidden** checkbox to hide the column in the table view. Hidden columns are still included in exported Excel files.

The following controls are available for each column:

↑ (Move Up): Moves the column one position to the left. This control is not displayed for the leftmost column.

— (Remove): Removes the column. This control is not displayed when only one column remains.

To add a column, click the *Add* Column button.

3. Sorting

Configure the following sorting fields:

Sort By: Select the column to sort by. This field is mandatory.

Sort Order: Select the sort direction. Options: Ascending (default), Descending. This field is mandatory.

4. Summary Row

Summary rows are optional and can be added to display aggregate values at the bottom of the table. Multiple summary rows can be added. For each summary row, configure the following fields:

Type: Select the aggregation method. This field is mandatory. Options: Average (default), Sum, Minimum, Maximum.

Name: Enter an optional name for the summary row. The name can be between 0 and 32 characters. If left empty, the selected Type is used as the row label.

To add a summary row, click the *Add* Summary Row button. To remove a summary row, click the — icon on the right side of the summary row header.

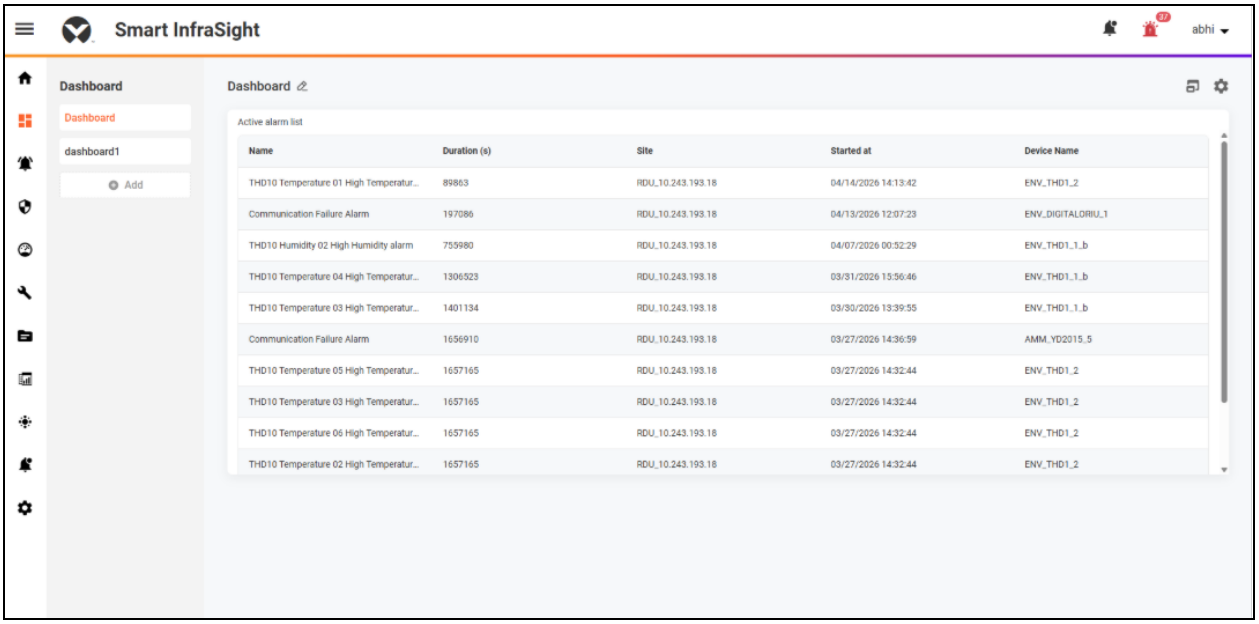
Add Visualization page for Table type showing the preview canvases for Data Set and Time correlation modes, Basic Information panel, and Correlation section.

Table configuration panel showing the Column configuration with Hidden checkbox, Sorting section, and Summary Row section with Type and Name fields.

© 2026 Vertiv Group Corp. All Rights Reserved.

5. Data source supported by Table

Figure 16.26 Table Displayed on the Dashboard



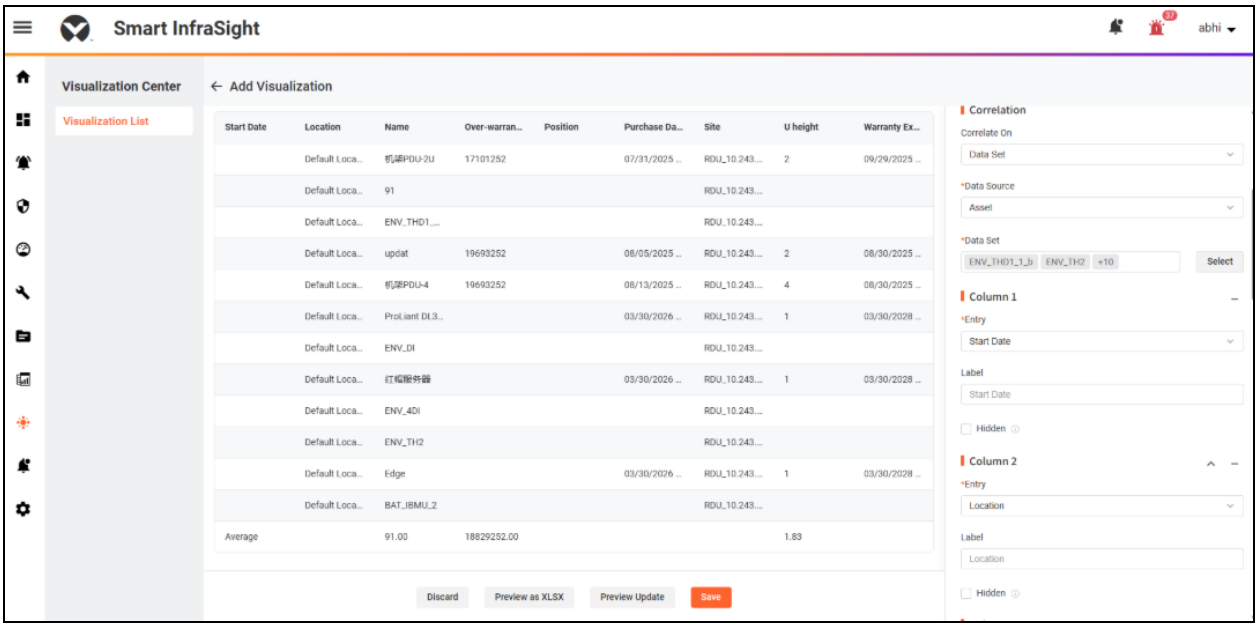
Asset Data

When the Asset data source is selected, the table supports a total of 9 entry points, including fields such as

- Start Date
- Name
- Over-warranty Duration
- Position
- Purchase Date
- Site
- U Height
- Warranty Expiry Date
- Location

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.27 Table with Asset Data Sources



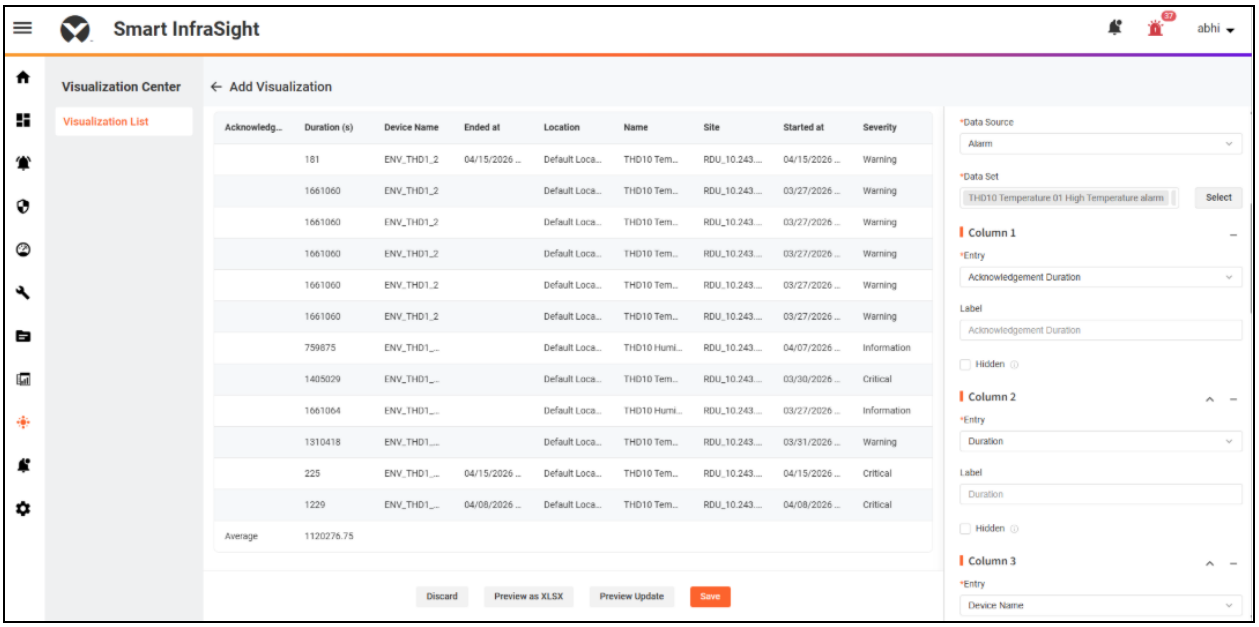
Alarm Data

When the Alarm data source is selected, the table supports multiple entry points such as

- Acknowledgment Duration
- Duration
- Device Name
- Ended at
- Location
- Name
- Site
- Started at
- Severity

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.28 Table with Alarm Data Sources



Device Data

When the Device data source is selected, the table supports entry points such as

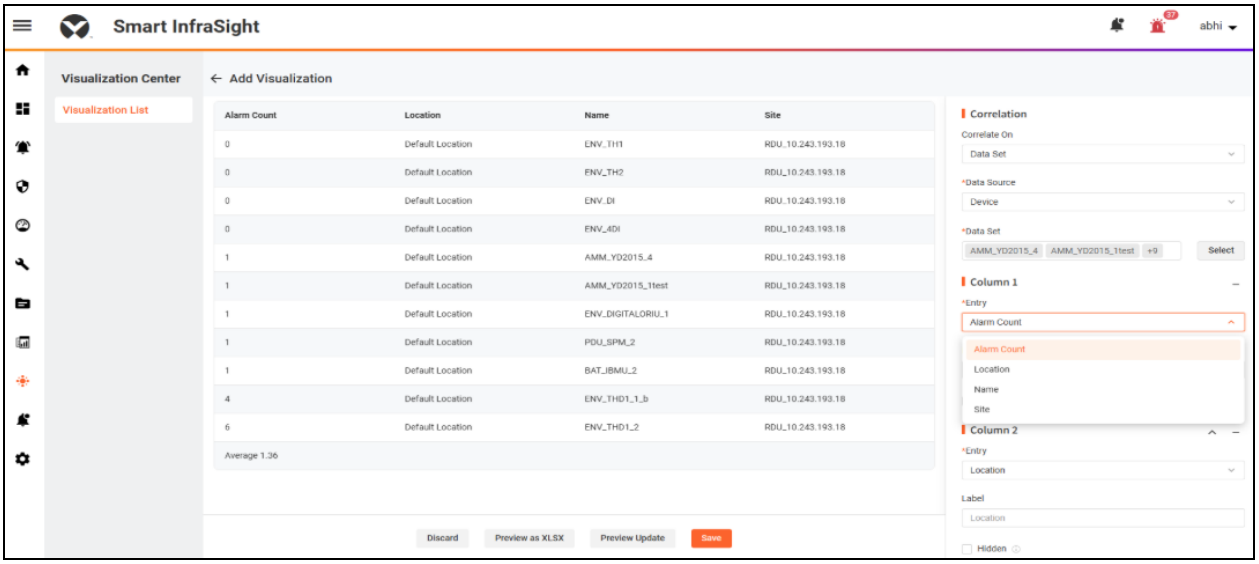
Alarm Count

Location

Name

Site

Figure 16.29 Table with Device Data Sources



© 2026 Vertiv Group Corp. All Rights Reserved.

IPMI Device Data

When the IPMI Device data source is selected, the table supports entry points such as

IP Address

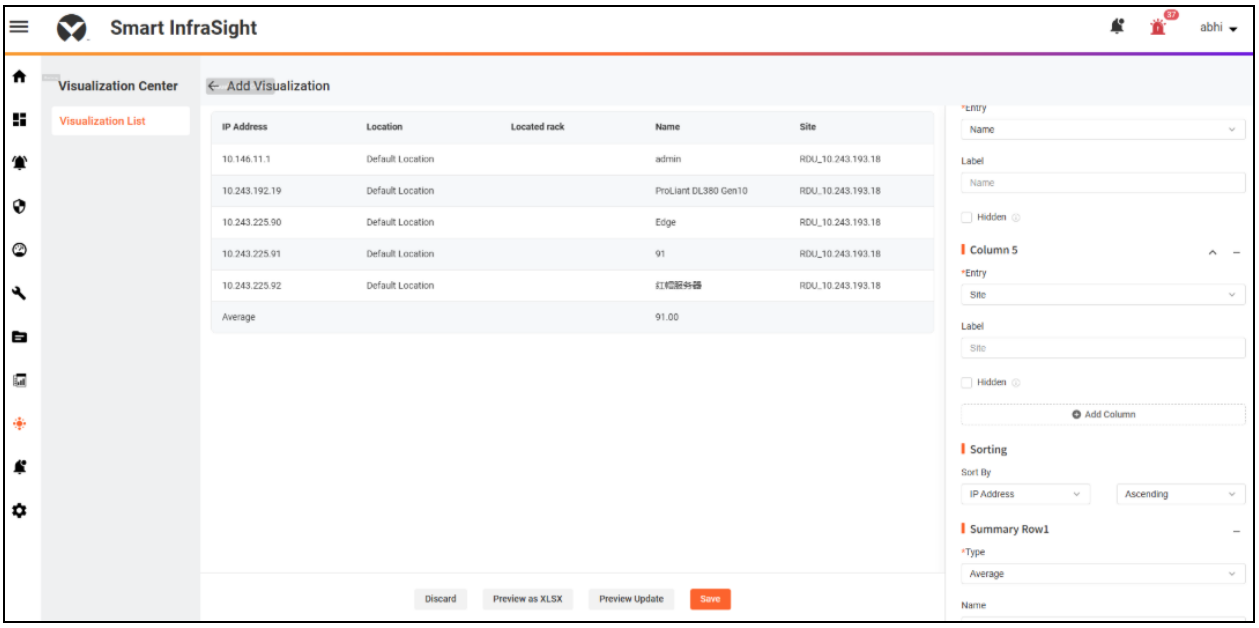
Location

Located Rack

Name

Site

Figure 16.30 Table with IPMI Device Data Sources

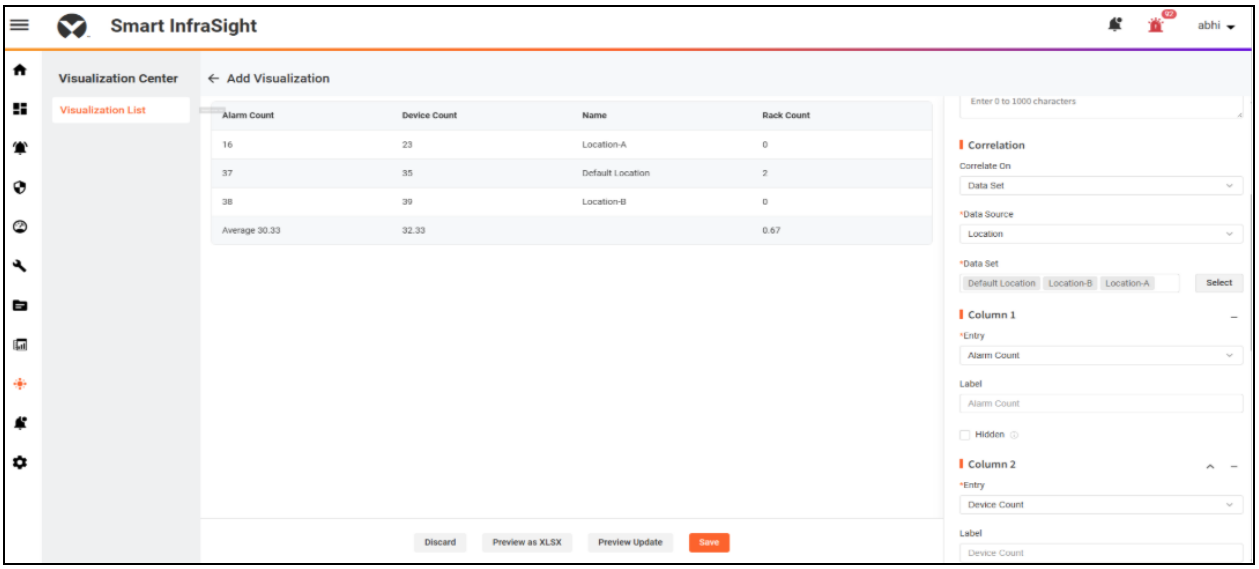


Location Data

When the Location data source is selected, the table supports entry points such as Alarm Count, Device Count, Name, and Rack Count.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.31 Table With Location Data Sources



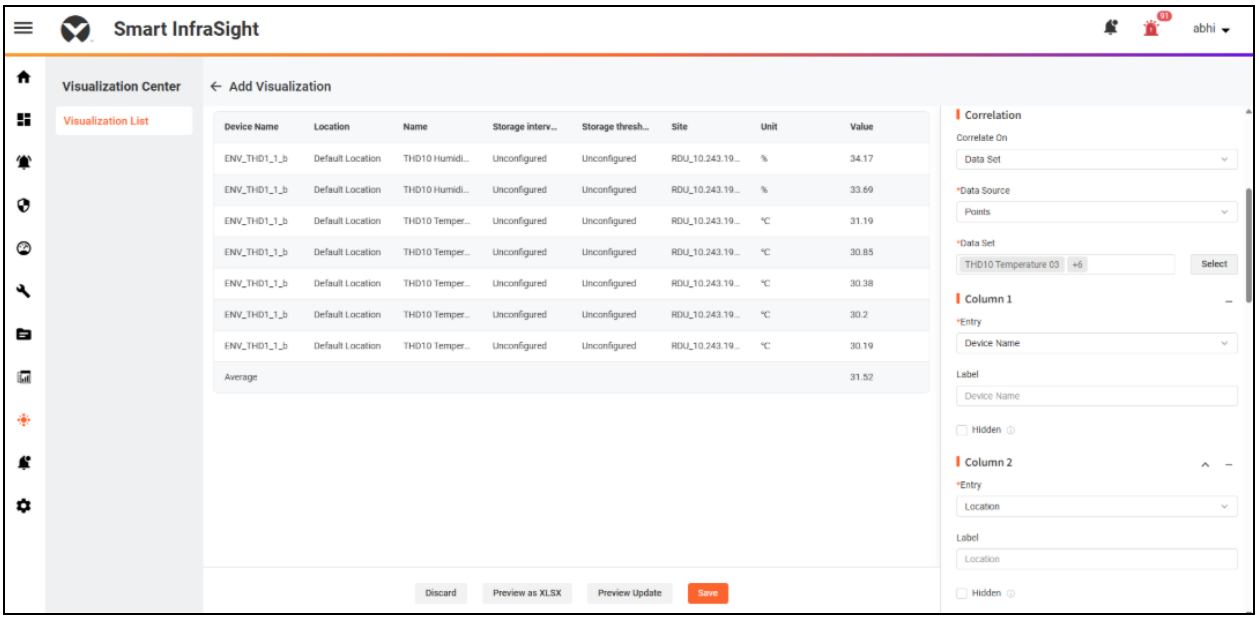
Points Data

When the Points data source is selected, the table supports entry points such as

- Device Name
- Location
- Name
- Storage Interval
- Storage Threshold
- Site
- Unit
- Value

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.32 Table with Points Data Sources



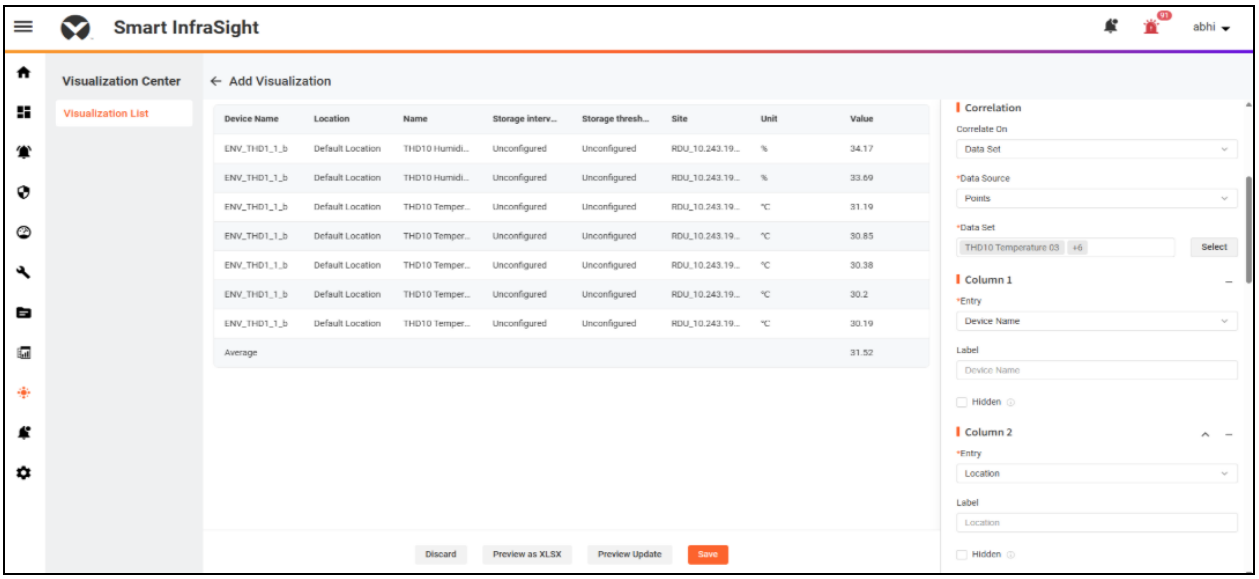
Site Data Source

When the Site data source is selected, the table supports entry points such as

- Alarm Count
- Device Count
- Location
- Rack Count
- Status
- Name

© 2026 Vertiv Group Corp. All Rights Reserved.

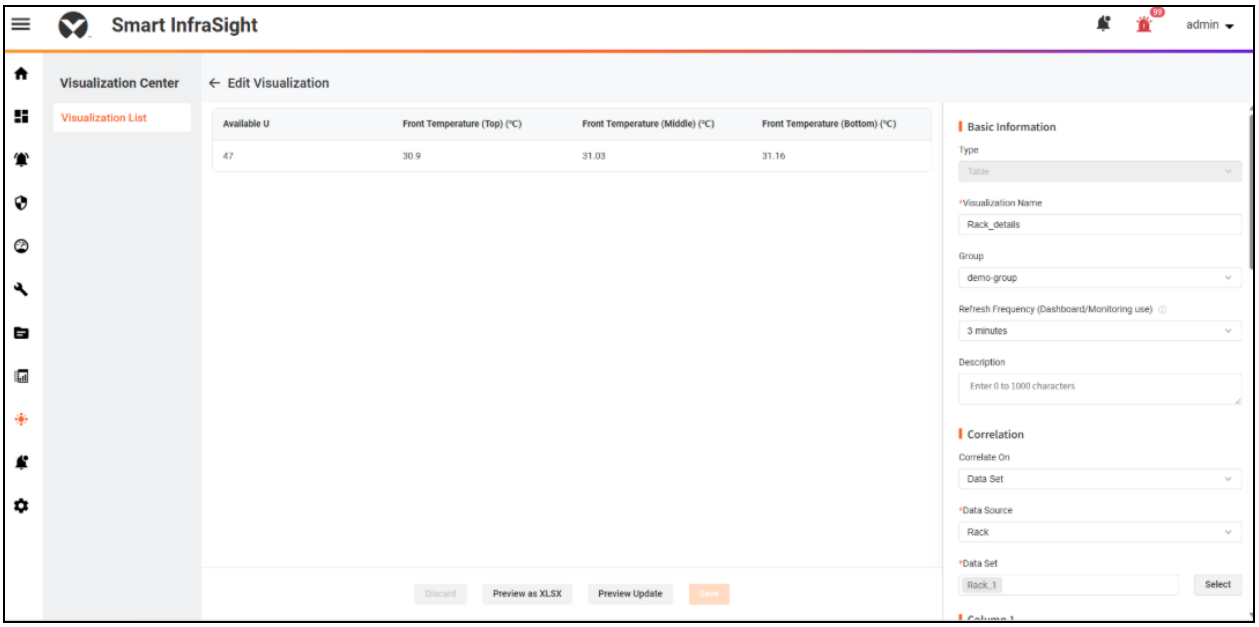
Figure 16.33 Table with Site Data Sources



Rack Data Source

When the Rack data source is selected, the table supports multiple entry points such as Available U, Occupied U, Total U of the rack, Rated Power, Total Power, Location, Name, Site, and various front and rear temperature and humidity metrics (Top, Middle, Bottom).

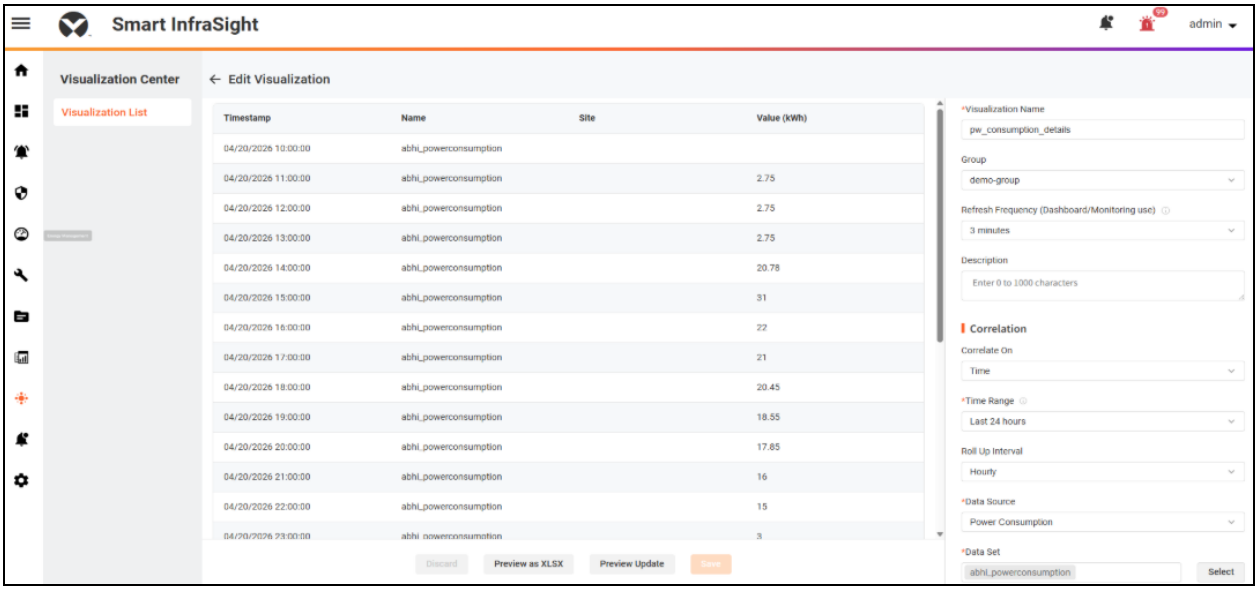
Figure 16.34 Table with Rack Data Sources



© 2026 Vertiv Group Corp. All Rights Reserved.

Power Consumption Data Source

Figure 16.35 Table with Power Consumption Data Sources



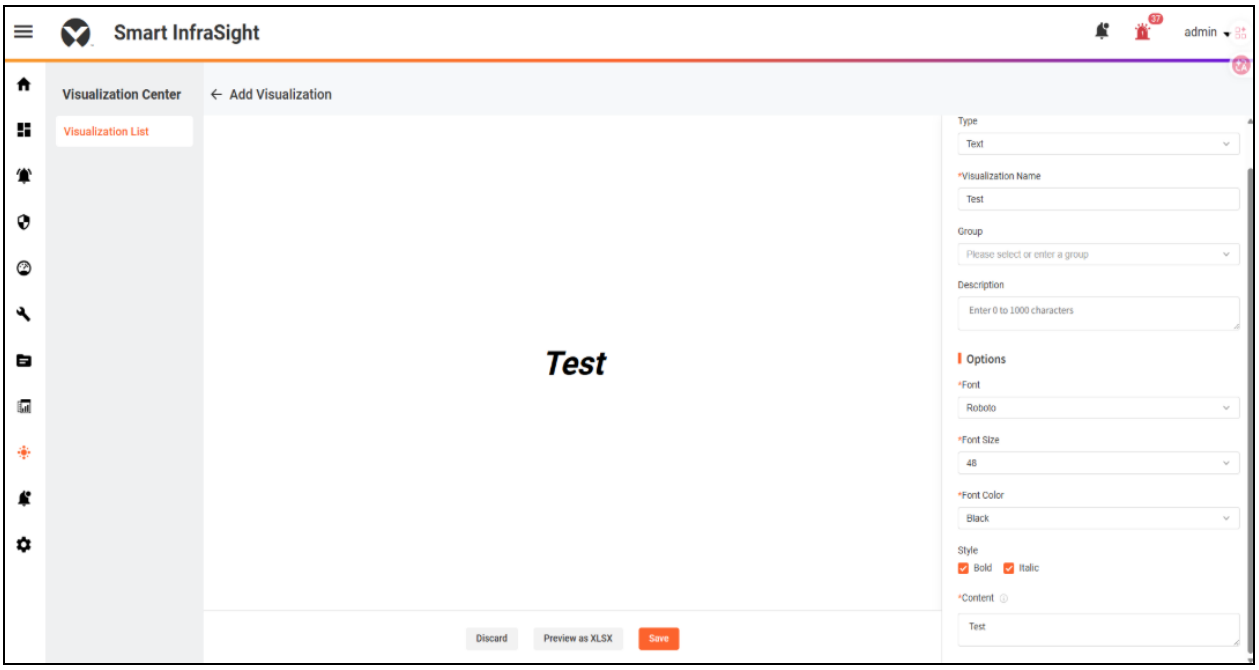
When the Power Consumption data source is selected, the table supports entry points such as Name, Site, and Value. When the correlation dimension is set to Time and a metric is selected, the data table will include a Timestamp column. You can choose the correlation mode based on your requirements.

16.3.7 Text

After selecting **Text** as the visualization type and completing the Basic Information fields, configure the following settings in the **Options** section, as shown in **Figure 16.36** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 16.36 Text



Add Visualization page for Text type showing the real-time text preview canvas and Options section with Font, Font Size, Font Color, Style, and Content fields.

NOTE: The Refresh Frequency field is not displayed for the Text visualization type.

IMPORTANT! The visualization canvas updates in Real time as you modify the configuration. No Preview Update button is displayed for this type.

Configure the following fields:

Font: Select the font from the dropdown. The following options are available:

- Roboto (default)
- Source Han Sans SC

Font Size: Select the font size from the dropdown. The following options are available: 8, 9, 10 (default), 11, 12, 14, 16, 18, 20, 22, 24, 26, 28, 36, 48.

Font Color: Select the font color from the dropdown. The following options are available: Black (default), Grey, Red, Orange, Yellow, Blue, Green, Purple.

Style: Select one of the following style options:

- Bold
- Italic

Content: Enter the text content to be displayed. This field is mandatory. The content must be between 1 and 5000 characters.

© 2026 Vertiv Group Corp. All Rights Reserved.

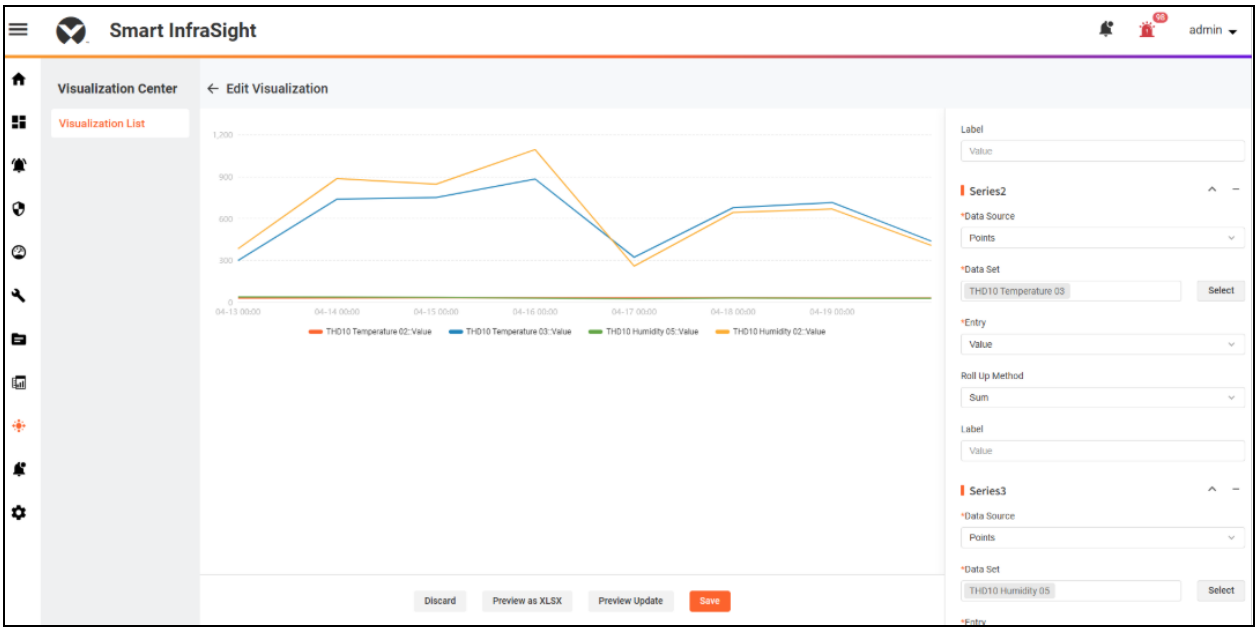
Macro	Description	Example
{TITLE}	Inserts the visualization title	Sample Visualization Title
{DATE}	Inserts the current date and time	2025-12-12 12:31:00
{DATE=YYYY-MM-dd}	Custom date format	2025-12-12
{DATE=YYYY}	Year only	2025
{DATE=MM-dd}	Month and day only	12-12
{DATE=hh:mm:ss}	Time only	12:31:00
{DATE=hh:mm}	Hours and minutes only	12:31
{DATE=EEE dd MMM, YYYY hh:mm:ss zzz}	Full date with time zone	Fri 12 Dec, 2025 12:31:00 +08:00

Click the *information* icon next to the Content field to view the available macros that can be inserted into the content. The following macros are supported.

16.3.8 Time Series

After completing the Basic Information section, configure the settings specific to the Time Series chart. This section walks through its use case, configuration steps, and key notes, as shown in **Figure 16.37** below .

Figure 16.37 Time Series



Step 1. Configure the X-Axis

Time Range (Required): Select the time range for the X-axis. This field is mandatory. The following options are available:

- Last Hour (default)
- Last 24 Hours
- Last 7 Days

© 2026 Vertiv Group Corp. All Rights Reserved.

- Last 30 Days
- Custom (maximum 30 days; select a start date and end date)

NOTE: The time is calculated based on the server time zone.

Roll Up Interval (Required): Select the roll-up interval for the X-axis. This field is mandatory. The available options depend on the selected Time Range, as described below:

- Hourly
- Daily
- Weekly
- Monthly

Step 2. Configure the Y-Axis

Label: Enter an optional label for the Y-axis. The label can be between 0 and 32 characters. The placeholder text reads: **Please enter Y axis label.**

Auto-Scale: The **Auto-Scale** checkbox is selected by default. When Auto-Scale is enabled, the Y-axis scale is set automatically based on the data values.To define a fixed scale, clear the Auto-Scale checkbox and enter values in the **Upper Range** and **Lower Range** fields that appear. Both fields are mandatory and accept values between –99,999,999 and +99,999,999.

Step 3. Configure Series

Each series represents one line on the Time Series chart. By default, one series row is displayed. To add additional series, click on the *Add Series* button at the bottom of the Series section.

For each series, configure the following fields:

- **Data Source:** Select the data source for this series.
- **Data Set**: Click the *Select* button to open the Data Set Selection popup and select one or more datasets. Selected datasets are displayed as tags in the field.
- **Entry**: Select the entry to be plotted for this series.
- **Roll Up Method:** Select the aggregation method used to calculate values within each interval, such as Average, Sum, Minimum, or Maximum, which determines how multiple data points are combined into a single value.
- **Label:** Enter an optional label for this series. The label can be between 0 and 32 characters. If left empty, the entry name is used as the label by default.

To remove a series, click the (—) icon on the right side of the series header. The remove icon is not displayed when only one series remains.

NOTE: If a series has no data for the selected time range, the corresponding line is not displayed on the chart. Series with mismatched units cannot be saved.

Add Visualization page for Time Series type showing the preview canvas, Basic Information panel, X-Axis and Y-Axis configuration.

Time Series configuration panel showing two Series blocks with Data Source, Data Set, Entry and Label fields, and the Add Series button.

© 2026 Vertiv Group Corp. All Rights Reserved.

Series Configuration (Multiple Data Sources Support):

Users can configure multiple series using different data sources and corresponding data points within a single visualization. Each series allows selection of a point-based data source, dataset (e.g., temperature points), entry (e.g., value), and roll-up method (e.g., average). All added series are plotted together on the same chart, enabling comparison of multiple data points from various sources.

Figure 16.38 Time Series Configuration

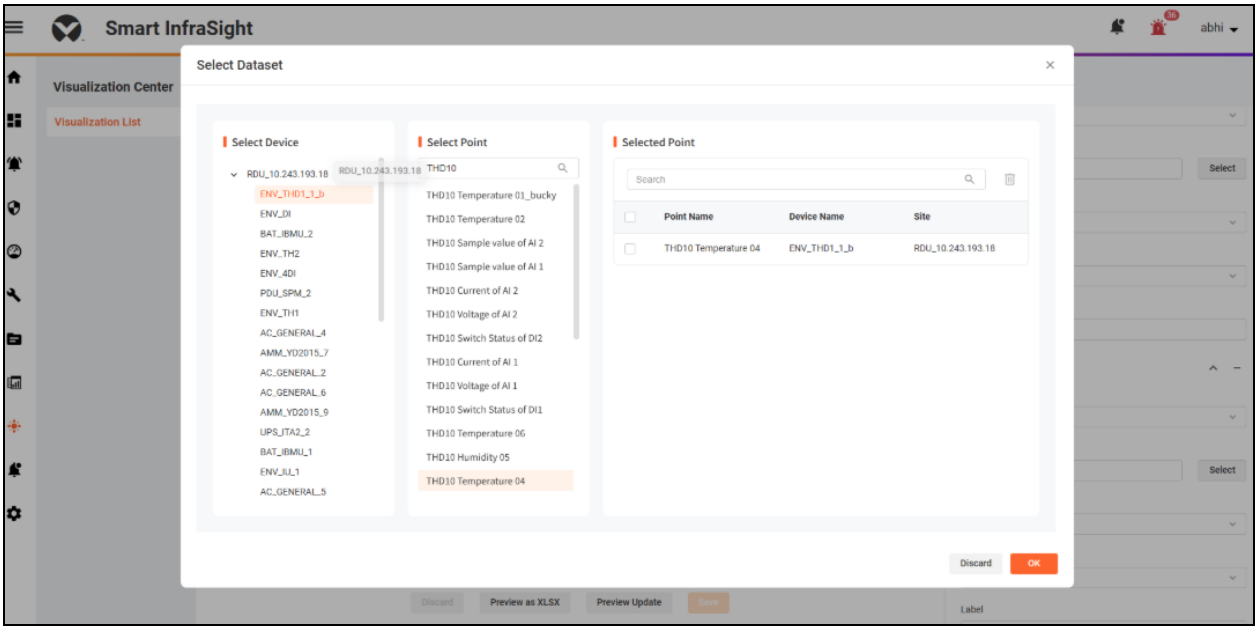
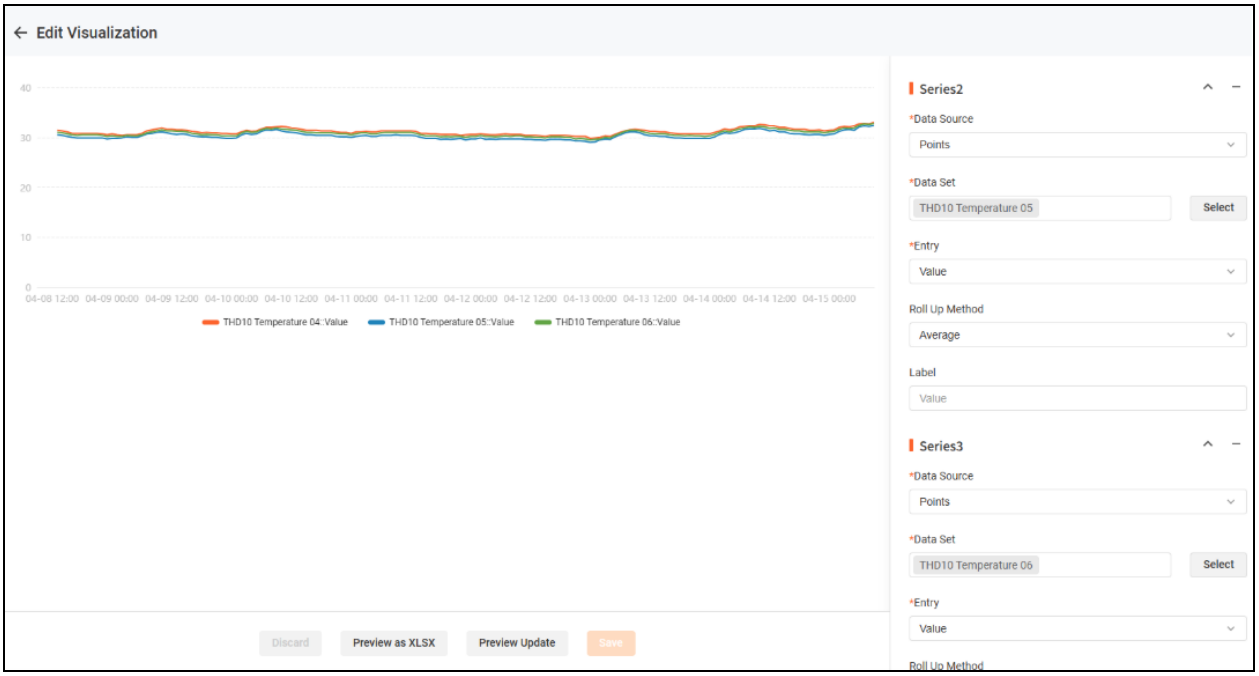


Figure 16.39 Time Series Configuration (Continued)



© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

17 Notification Hub

17.1 Overview

The Notification Hub module is located in the left navigation bar and contains three sub-tabs: Outbound Notifications, Notification History, and General Settings. It is used to configure outbound notifications (email, SMS, and voice) for platform events that require notification, such as alarms. This chapter describes how to configure notifications, view notification history, and manage notification settings.

17.1.1 Functional modules

The Notification Hub consists of the following feature modules. For detailed information on each module, refer to Detailed Features below.

1. Outbound Notifications

2. Notification History

3. Notification Settings – Notification Language

4. Notification Settings – Email Server

5. Notification Settings – SMS Modem

6. Notification Settings – Voice

17.2 Detailed Features

17.2.1 Outbound Notifications

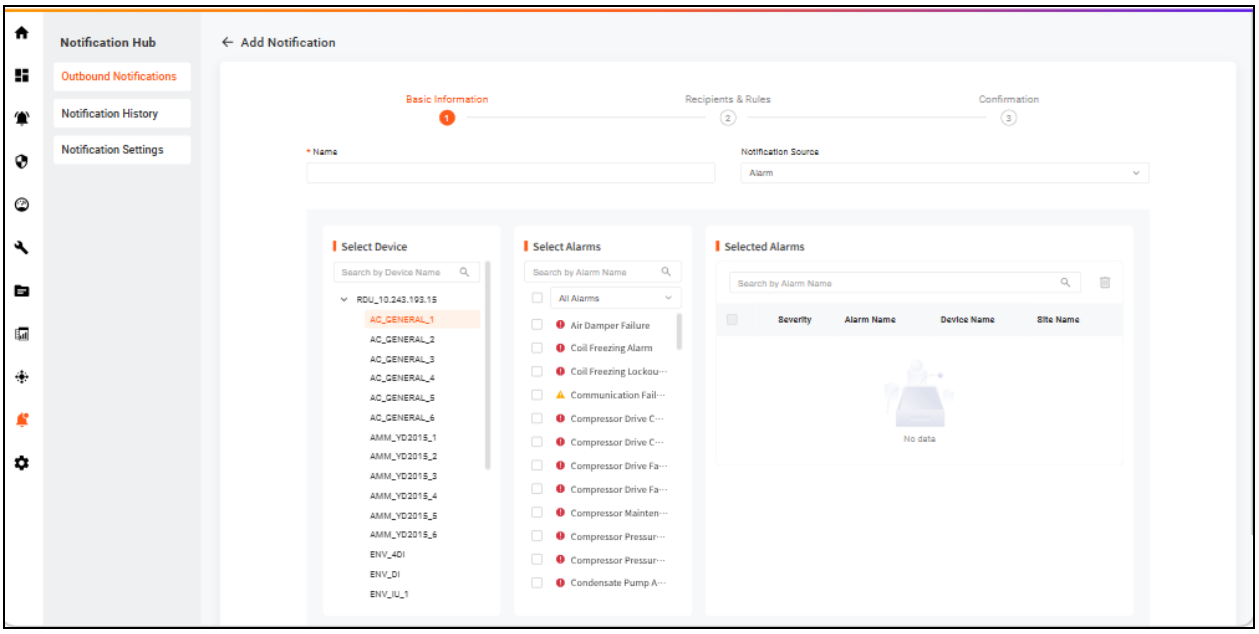
The Outbound Notifications tab is used to create, manage, and view outbound notifications sent via email, SMS, and voice. It serves as the central entry point for managing all platform notification configurations. When a notification configuration is triggered, the platform sends notifications to the configured recipients via email, SMS, or voice.

Adding a Notification Configuration

To add a notification configuration, go to **Notification Hub > Outbound Notifications** and click (+) icon. The notification creation wizard opens, displaying a three-step progress indicator at the top of the page**: Basic Information → Recipients & Rules → Preview & Confirm**. As shown **Figure 17.1** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 17.1 Add Notification Configuration — Basic



1. When **Notification Source** is set to **Alarm**:

Step 1: Basic Information

In the **Name** field, enter a name for the notification configuration. The name must be 1–32 characters. The **Notification Source** drop-down list defaults to **Alarm**.

Complete the alarm binding in the alarm selection area at the bottom of the page. This area is divided into three sections:

Select Devices: Displays the available device list in a tree structure. Click a *node* to expand its child devices. Click a device name to select it.

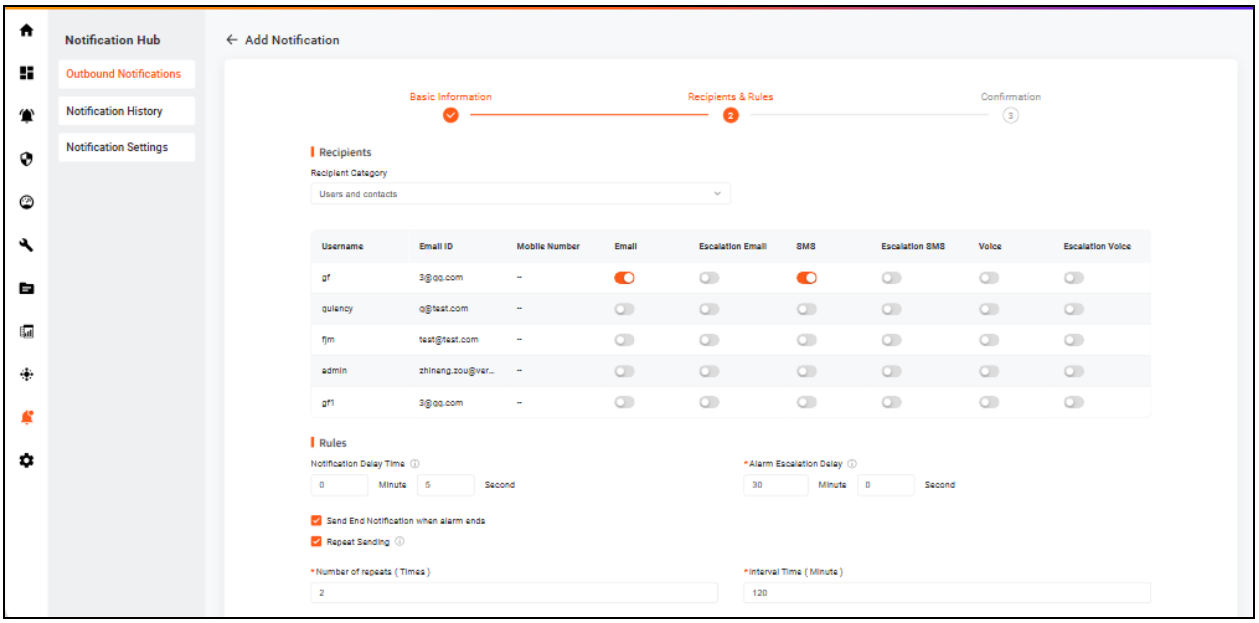
Select Alarms: Displays the alarms associated with the selected devices. Each alarm displays a severity icon. You can search by alarm name and select multiple alarms. Select All Alarms to select all alarms under the current device at once.

Selected Alarms: Displays a summary of all selected alarms, including the **Severity, Alarm Name, Device Name**, and **Site Name** columns. You can search by alarm name. To remove an alarm, select it and click the delete icon in the upper-right corner.

After completing alarm selection, click *Next* in the lower-right corner to proceed to Step 2. As shown in **Figure 17.2** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 17.2 Add Notification Configuration — Recipients & Rules



Step 2: Recipients & Rules

From the **Recipient Type** drop-down list, select the recipient scope. Available options are: **Users and Contacts**, **Users Only**, and **Contacts Only**. The recipient table below is automatically populated based on your selection. Each row represents one user or contact. Rows cannot be added or deleted manually.

The table includes the following columns: **Username**, **Email**, **Mobile Number**, **Email**, **Escalation Email**, **SMS**, **Escalation SMS**, **Voice**, and **Escalation Voice**. The columns from **Email** to **Escalation Voice** are toggle switches, disabled by default. Enable them as needed. If an email address or mobile number exceeds the column width, it is truncated. Hover over the cell to view the full value. If a user has multiple mobile numbers, SMS and voice notifications are sent to all numbers.

You must enable at least one notification channel (email, SMS, or voice) for at least one recipient before proceeding to the next step.

In the **Rules** section, configure the following:

Notification Delay Time: The delay between when an alarm is triggered and when the notification is sent. Enter the duration in minutes and seconds. Range: 0 seconds to 30 minutes 59 seconds. Default: 0 minutes 5 seconds. If a delay is configured, the notification triggers only after the delay period has elapsed.

Alarm Escalation Delay Time: The waiting period before an escalation notification is triggered. Default: 30 minutes 0 seconds. Range: 0 seconds to 1440 minutes 59 seconds.

Send End Notification When Alarm Ends: When selected, the platform automatically sends an end notification when the alarm is cleared. Selected by default.

Repeat: When selected, the following fields appear:

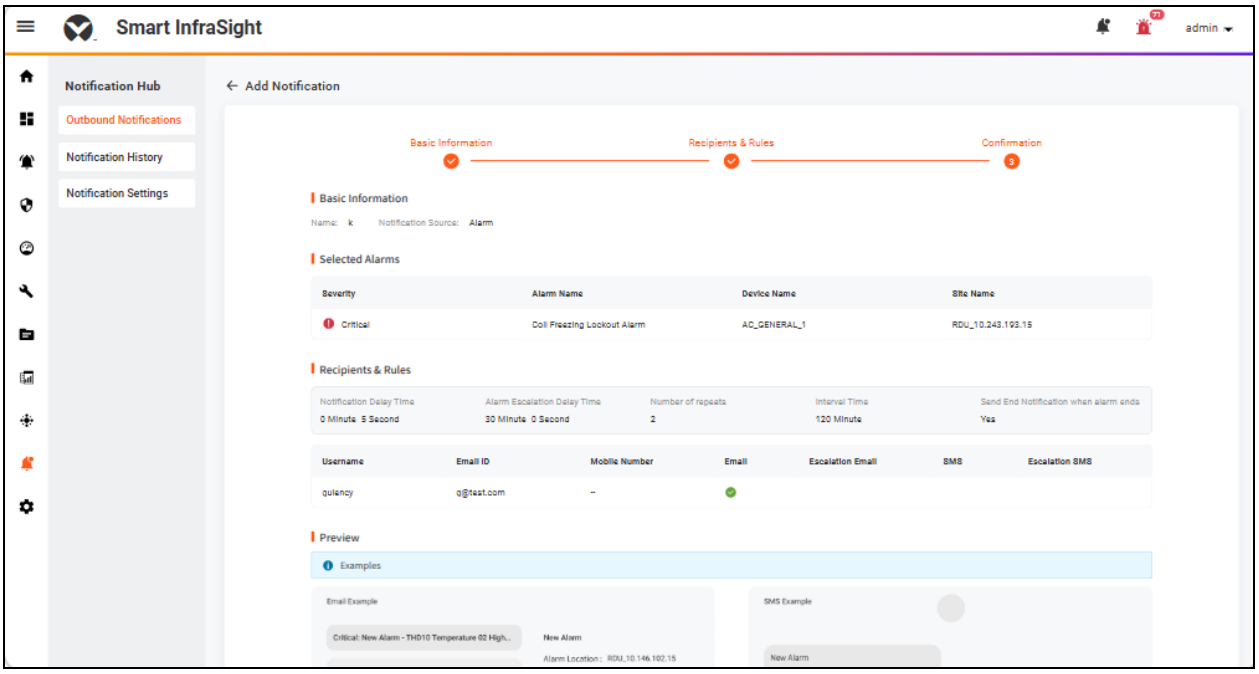
a. Number of Repeats: The number of repeat notifications. Range: 1–10. Default: 2.

b. Interval (min): The interval between each repeat. Range: 10–480 minutes. Default: 120 minutes.

After completing the configuration, click *Next* in the lower-right corner to proceed to Step 3. As shown in **Figure 17.3** on the next page . Click *Previous* to return to the previous step. Click *Cancel* to exit the wizard and return to the list page.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 17.3 Add Notification Configuration — Recipients & Rules



Step 3: Preview & Confirm

This page displays a read-only summary of all configurations, organized into the following four sections:

Basic Information: Displays the **Name** and **Notification Source**.

Selected Alarms: Lists all selected alarms in a table, including Severity, Alarm Name, Device Name, and Site Name.

Recipients & Rules: Displays the rule parameters (notification delay time, alarm escalation delay time, number of repeats, interval, and end notification setting) and the recipient table, consistent with Step 2.

Preview: Displays sample email and SMS notification templates. Templates cannot be edited on this page.

After confirming all information, click *Save* to complete the configuration. The platform displays an operation result message: a success message if the configuration is saved successfully, or a failure message if it fails. Click *Previous* to return to the previous step and make changes. Click *Cancel* to exit the wizard and return to the list page.

Viewing the Notification Configuration List

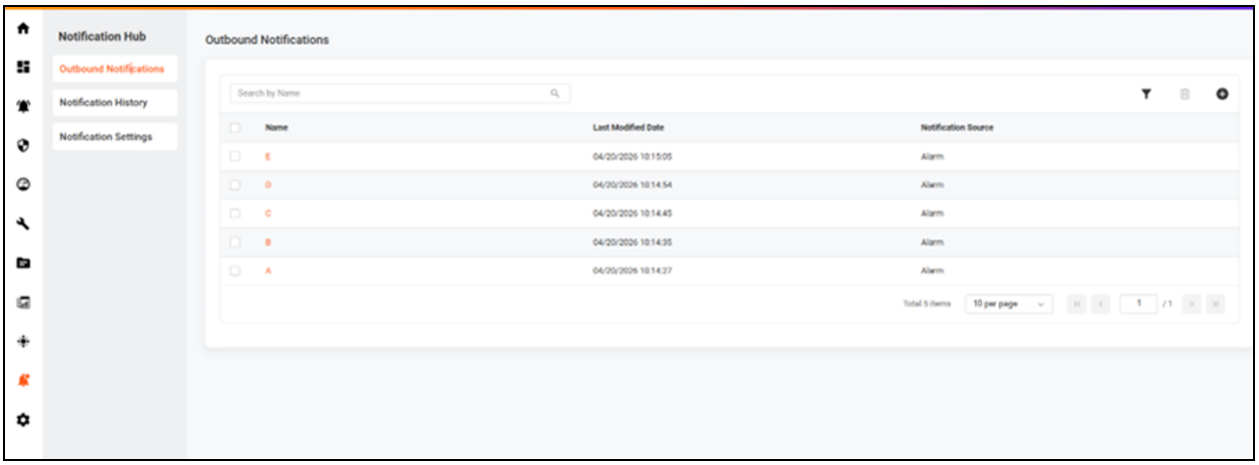
To view the notification configuration list, go to **Notification Hub > Outbound Notifications**. The list page displays all configured notifications. As shown in **Figure 17.4** on the facing page .

The list includes the following columns: **Name**, **Last Modified,** and **Notification Source**. By default, the list is sorted by creation time in descending order. The list supports pagination, and the number of records displayed per page is adjustable.

Enter a keyword in the search bar to perform a fuzzy search by **Name**. Click the *filter* icon in the upper-right corner to filter the list by **Notification Source**. Click a *Name* in the list to view or edit the corresponding notification configuration. Select one or more records and click the *delete* icon in the upper-right corner to batch delete the selected notifications.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 17.4 Notification Configuration — List



The notification list contains the following information:

1.Name: The name of the notification configuration.

2.Last Modified: The timestamp of the most recent update.

3.Notification Source: The type of the notification configuration.

4.Search Bar: Performs a fuzzy search by **Name**.

5.Filter Button: Opens the filter panel, allowing filtering by **Notification Source**.

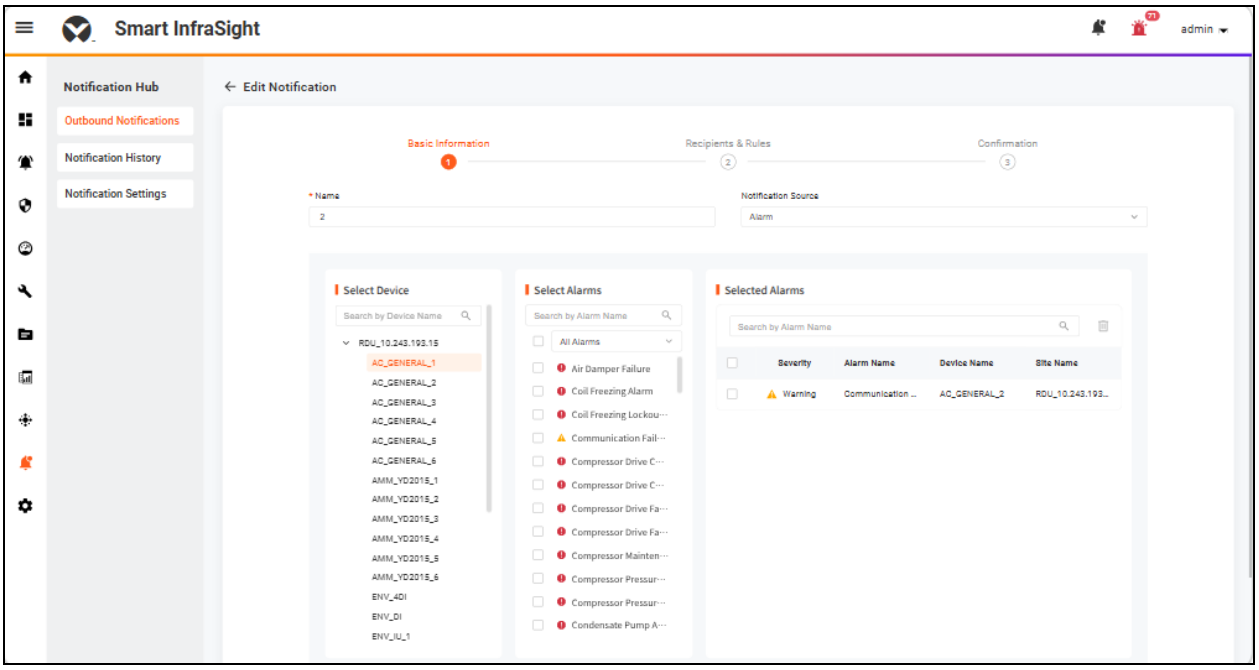
6.Pagination: Displays the total number of records and page count. You can navigate to a specific page to browse records.

Editing a Notification Configuration

To edit a notification configuration, go to **Notification Hub > Outbound Notifications**, then click the *name* link of the target configuration to open the edit page. As shown in **Figure 17.5** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 17.5 Notification Configuration — Edit

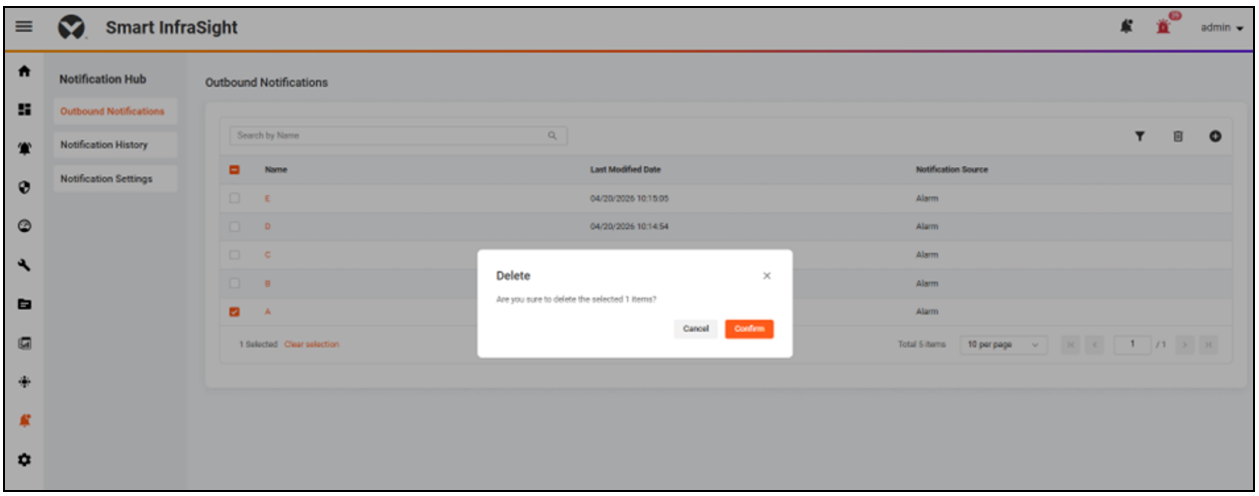


The editing process is the same as adding a notification configuration. Refer to Adding a Notification Configuration on page 381.

Batch Deleting Notification Configurations

To batch delete notification configurations, go to **Notification Hub > Outbound Notifications**, select the notification records to be deleted, and click the delete icon in the upper-right corner. A confirmation dialog will appear with the message: **Are you sure you want to delete the selected N item(s)?** Click *OK* to confirm the deletion — the page will display a success message. Click *Cancel* to close the dialog and return to the list page.

Figure 17.6 Notification Configuration — Batch



© 2026 Vertiv Group Corp. All Rights Reserved.

17.2.2 Notification History

Notification History records all outbound notifications sent by the platform. Each notification trigger generates an independent record. In Notification History, you can view the notification configuration that was triggered, the notification actions sent, and the recipients.

Querying Notification Records

1. Trigger Source: Alarm

The page displays historical records in a list format, as shown in **Figure 17.7** on the next page . The list includes the following columns: Send Time, Trigger Source - Alarm, Trigger Source - Device, Notification Name, Recipient, Notification Type, and Notification Method.

The list is sorted by Send Time in descending order by default. Sorting by Send Time and Notification Name is supported, and pagination is available.

Enter keywords in the search bar to perform a fuzzy search on records by **Notification Name**. The page provides a **Time Range** dropdown for filtering notification records by **Sent Time**. The available options include **Last 24 Hours, Last 72 Hours, Last Week, Last 30 Days**, and **Custom**. When Custom is selected, users can specify a start time and end time for a precise search. Click the *filter* icon in the upper-right corner to filter records by **Notification Type**.

Notification History is retained for 90 days by default. Users can configure the retention period in Section Data Retention on page 433. If the retention policy is set to Never Delete, notification history will be retained indefinitely.

If the same notification is sent through multiple channels, the Notification Method column will list all channels simultaneously, e.g., **SMS, Voice, Email**.

The notification record list contains the following information:

1.Send Time: The time the notification was sent.

2.Trigger Source - Alarm: The name of the alarm that triggered the notification. If the alarm has been deleted, (--) is displayed.

3.Trigger Source - Device: The name of the device that triggered the notification.

4.Notification Name: The name of the notification configuration that was triggered.

5.Recipient: All users to whom this notification was sent.

6.Notification Type: The alarm event type that triggered this notification (Alarm Generated, Alarm Repeated, Alarm Escalated, Alarm Cleared).

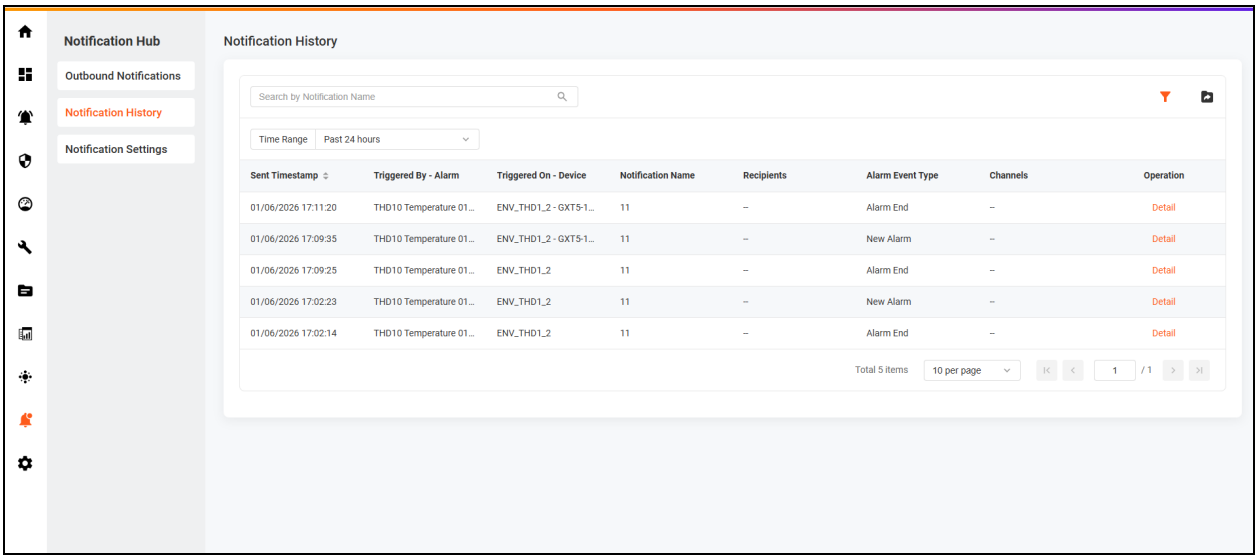
7.Notification Method: All notification channels used (Email, SMS, Voice).

8.Action: Click *Details* to view the full details of the notification record.

9.Search Bar: Performs a fuzzy search by Notification Name.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 17.7 Notification Records — List



Click *Details* in the Action column to open the detail page for that notification record, as shown in **Figure 17.8** on the facing page .

The top of the notification detail page displays the notification name. Click the *back arrow* in the upper-left corner to return to the list page.

The Basic Information section displays the following fields:

Notification Name: The configuration name of the notification.

Send Time: The timestamp when this notification was triggered.

Trigger Source - Alarm: The name of the alarm that triggered this notification. If the alarm has been deleted, (--) is displayed.

Trigger Source - Device: The name of the device that generated the alarm.

Notification Type: The event type of this notification. Possible values: Alarm Generated, Alarm Repeated, Alarm Escalated, Alarm Cleared.

Notification Content: The body content of this notification. Content exceeding the display width is truncated; hover to view the full content.

Subject (Email Only): The subject line of the email notification. Content exceeding the display width is truncated.

The Notification Method section displays delivery details for each channel in tab format. Tabs include: Email, SMS, and Voice. Click the corresponding tab to switch views.

The Email tab table contains the following columns:

Recipient: The recipient's username.

Email Address: The recipient's email address.

Status: The delivery result. Success indicates the email was delivered successfully; Failed indicates delivery failure.

The SMS tab table contains the following columns:

Recipient: The recipient's username.

© 2026 Vertiv Group Corp. All Rights Reserved.

Phone Number: The mobile number that received the SMS.

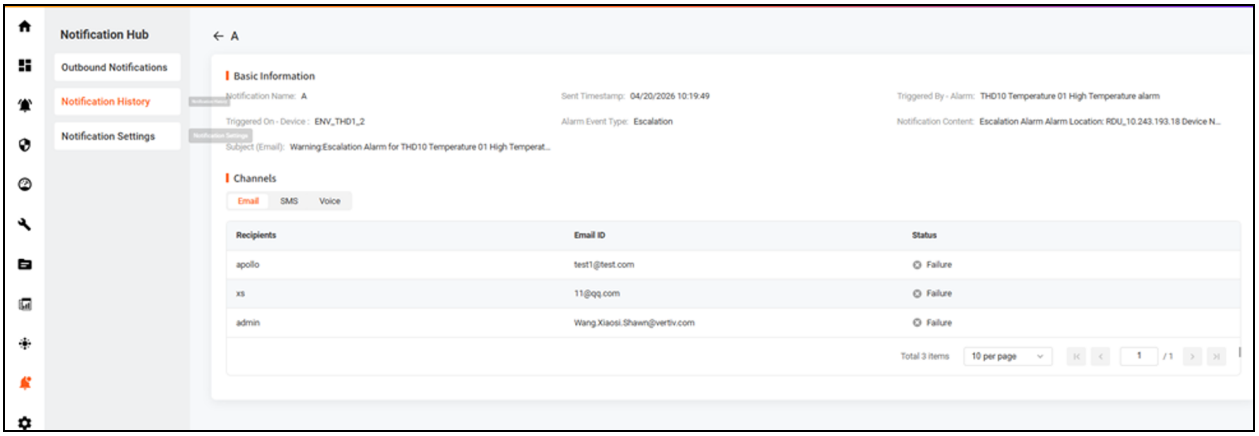
Status: The delivery result. Success indicates the SMS was delivered successfully; Failed indicates delivery failure.

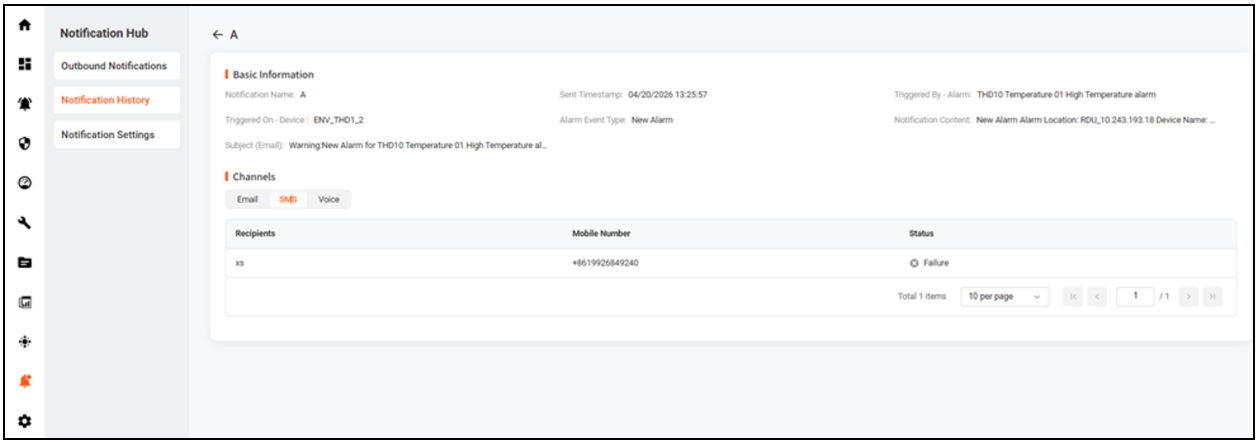
The Voice tab table follows the same structure as the SMS tab, displaying the recipient, phone number, and delivery status for voice notifications.

If a single user has multiple phone numbers, each number generates an independent record. The delivery status of each channel is independent — the same user may show Success for the Email channel and Failed for the SMS channel.

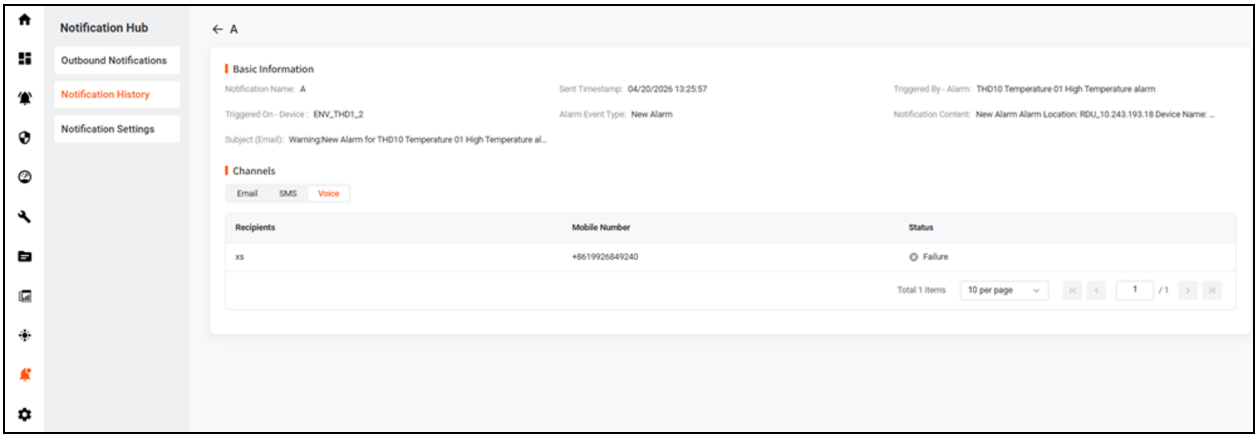
NOTE: The notification status shown in the Notification History list only indicates whether the platform has successfully dispatched the notification request. It does not guarantee that the recipient has actually received the notification. The actual delivery result is determined by the Status column for each channel on the detail page.

Figure 17.8 Notification Records — Details





© 2026 Vertiv Group Corp. All Rights Reserved.



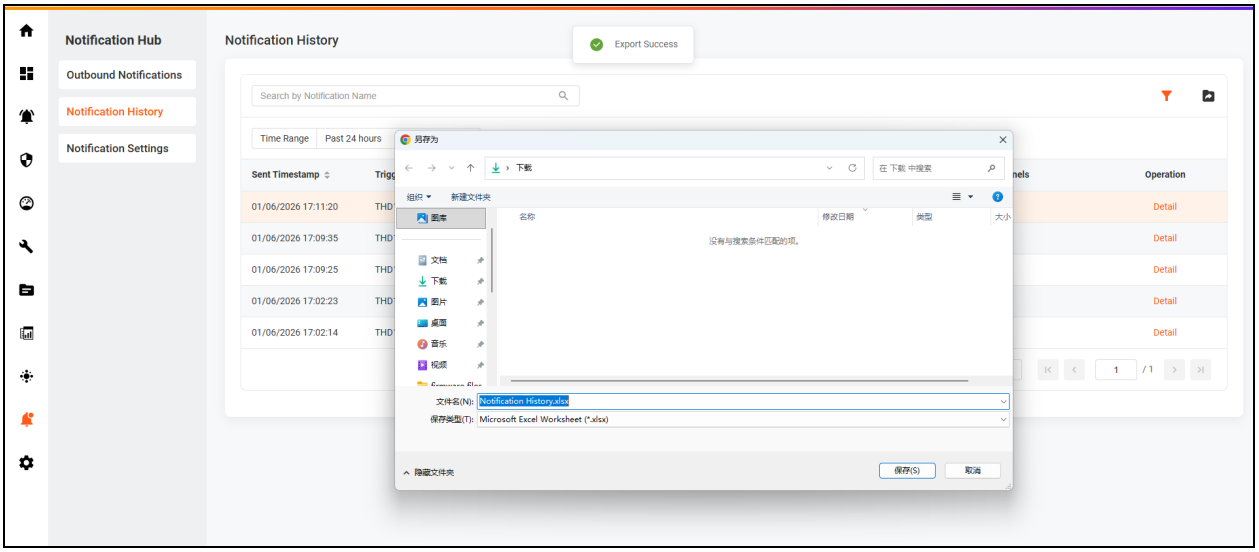
Export Notification History

Click the *Export* icon in the upper-right corner of the list to export notification history records that match the current search criteria to an Excel file (Notification History.xlsx).

The exported file includes all records that match the current search keyword, time range, and filter conditions.

After the export is completed successfully, a confirmation message is displayed, and the file is automatically downloaded to the local device. As shown in **Figure 17.9** below .

Figure 17.9 Notification History— Export



17.2.3 Notification Settings

Notification Language

The General Settings tab contains four sub-tabs: Notification Language, Email Server, SMS Modem, and Voice Modem. The notification language setting defines the language used for notification content. The content of email, SMS, and voice notifications is all controlled by the notification language setting.

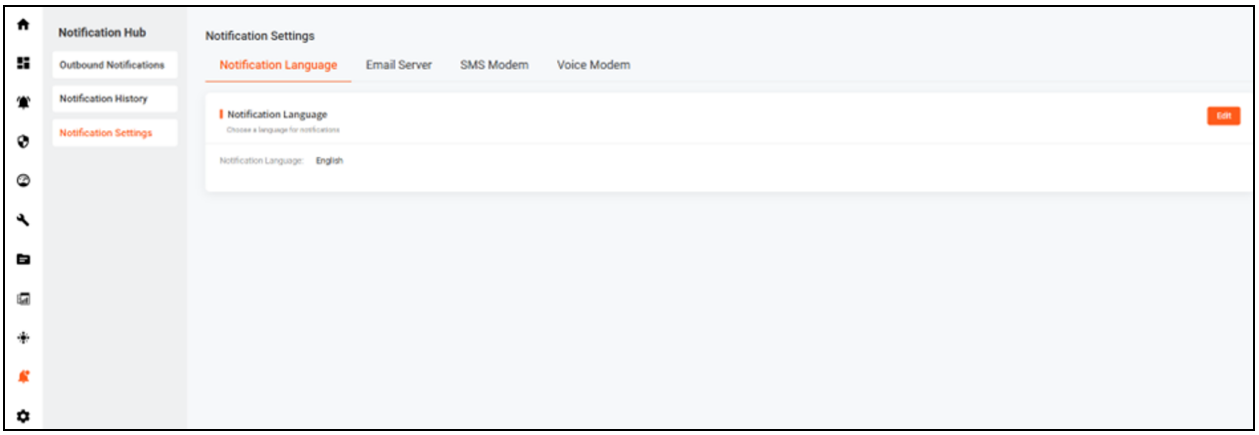
© 2026 Vertiv Group Corp. All Rights Reserved.

Viewing Notification Language

Go to Notification Hub then click on *Notification Settings*, then click the *Notification Language* sub-tab. The page displays the current notification language configuration. Field descriptions are as follows:

Notification Language: The language used by the platform to send notifications. Currently supports Chinese and English. The default is English. As shown in **Figure 17.10** below .

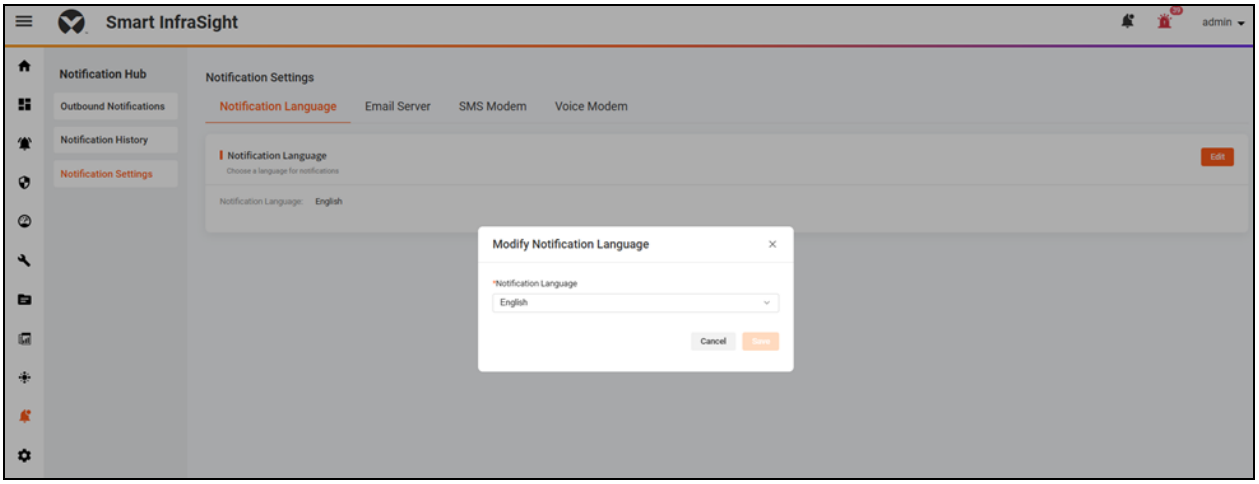
Figure 17.10 Notification Language Settings — View



Editing Notification Language

Go to Notification Hub then Click on *Notification Settings*, then click the *edit* button. The Modify Notification Language dialog will appear. Select the target language from the Notification Language dropdown, click *OK* to save, or click *Cancel* to close the dialog without making changes. As shown in **Figure 17.11** below .

Figure 17.11 Notification Language Settings — Edit



Email Server

The email server configuration is a prerequisite for the email notification feature, ensuring that email notifications function properly. Before using the email notification feature, the email server information must be configured in advance.

© 2026 Vertiv Group Corp. All Rights Reserved.

Viewing Email Server Configuration

Click the *Email Server* sub-tab. The page displays the current email server configuration, which is used for sending alarm notifications and password reset emails. As shown in **Figure 17.12** below . Field descriptions are as follows:

Email Server Address: The IP address or hostname of the email server.

Email Server Port: The communication port number of the email server.

Sender Email: The sender email address used by the platform when sending notification emails.

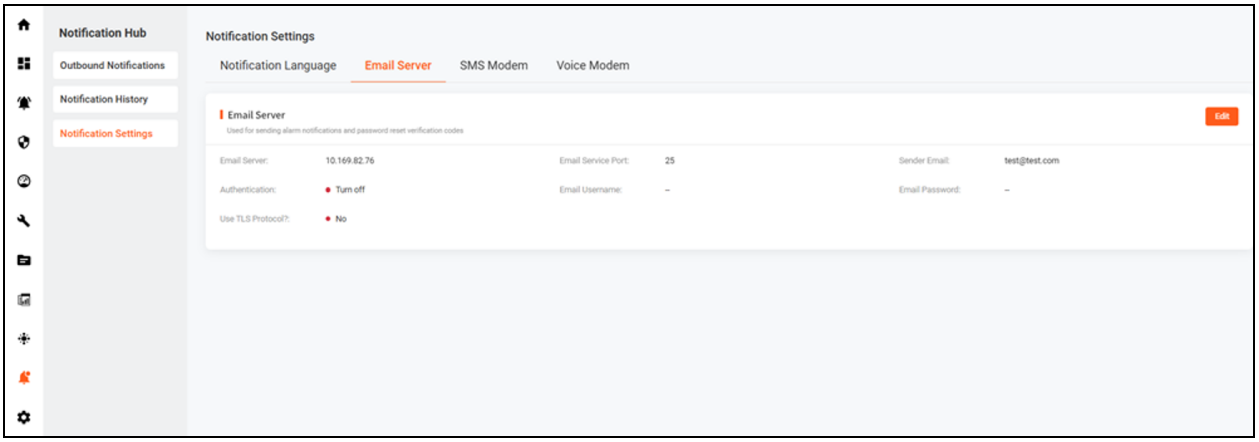
Authentication: Indicates whether email server access authentication is enabled. Status is either Enabled or Disabled.

Email Username: Displays the configured username when authentication is enabled; displays (—) when disabled.

Email Password: Displays the configured password when authentication is enabled; displays (—) when disabled.

Use TLS Protocol: Indicates whether TLS encrypted transmission is enabled. Status is either Yes or No.

Figure 17.12 Email Server — View



Editing Email Server Configuration

Go to Notification Hub then click on *Notification Settings*, then click on *Email Server*, then click the *edit* button. The Edit Email Server dialog will appear, as shown in **Figure 17.13** on the facing page . Field descriptions are as follows:

Email Server Host: Select the address type (IPv4 or Domain Name) and enter the server address in the input field on the right. Required.

Email Server Port: Enter the server port number. Required.

Sender Email: Enter the sender email address. Required.

Use TLS Protocol: Single selection — choose Yes or No. Required.

Email Server Authentication: When checked, the following two required fields are expanded:

a. Email Username: Enter the username for authentication.

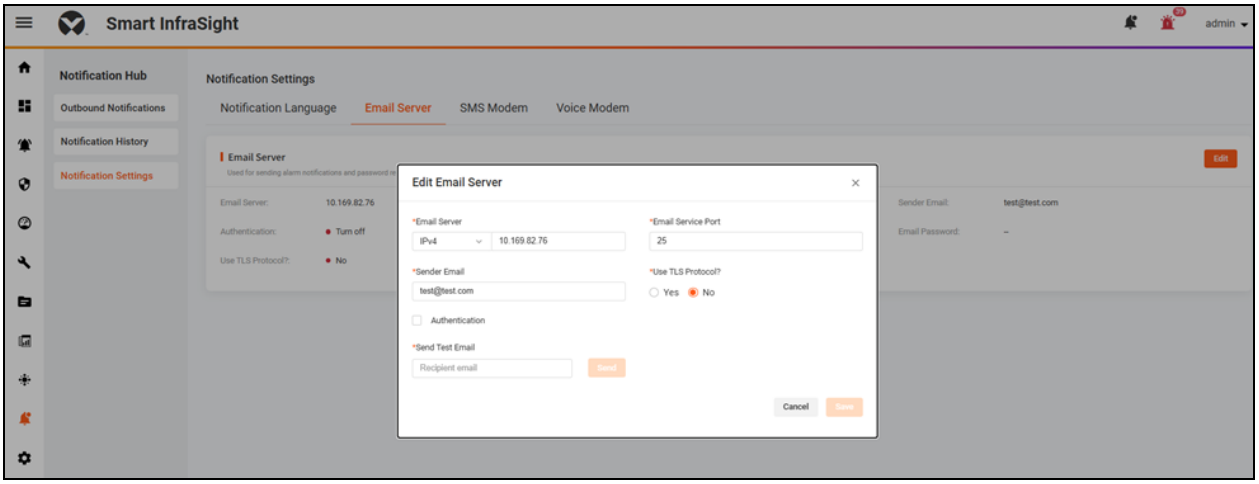
b. Email Password: Enter the corresponding password. Click the *icon* on the right to toggle password visibility.

Send Test Email: Enter a recipient email address in the input field and click *Send* to send a test email to the specified address, verifying that the current configuration is functional. If the test fails, the configuration cannot be saved. If the test succeeds, the Save button becomes active and the configuration can be saved.

© 2026 Vertiv Group Corp. All Rights Reserved.

Click *Save* to submit the configuration, or click *Cancel* to close the dialog without making changes.

Figure 17.13 Email Server — Edit



SMS Modem

The SMS modem configuration is a prerequisite for the SMS notification feature, ensuring that SMS notifications function properly. Before using the SMS notification feature, the SMS modem information must be configured in advance. Only the TD-8411 model SMS modem is supported.

Viewing SMS Modem Configuration

Click the SMS Modem sub-tab. The page displays the current SMS modem configuration. Only the TD-8411 model SMS modem is currently supported. As shown in **Figure 17.14** on the next page . Field descriptions are as follows:

Operating System: The current device operating system, displayed as Linux. Not editable.

Port: The modem connection port.

Baud Rate: The serial communication rate.

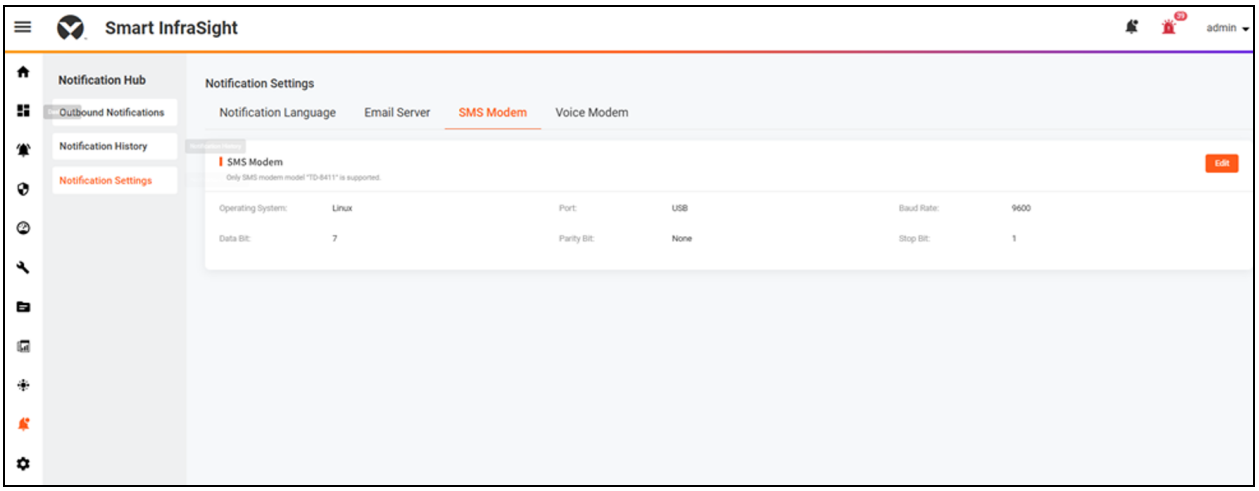
Data Bits: The number of serial data bits.

Parity: The serial parity check method.

Stop Bits: The number of serial stop bits.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 17.14 SMS Modem — View



Editing SMS Modem Configuration

Go to Notification Hub, then click on *Notification Settings* then click on *SMS Modem*, then click the *edit* button. The Edit SMS Modem dialog will appear, as shown in **Figure 17.15** on the facing page . Field descriptions are as follows:

Operating System: Displays the current operating system. Grayed out and not editable.

Port: Select the connection port from the dropdown. Required.

Baud Rate: Select the communication rate from the dropdown. Required.

Data Bits: Select the number of data bits from the dropdown. Required.

Parity: Select the parity check method from the dropdown. Required.

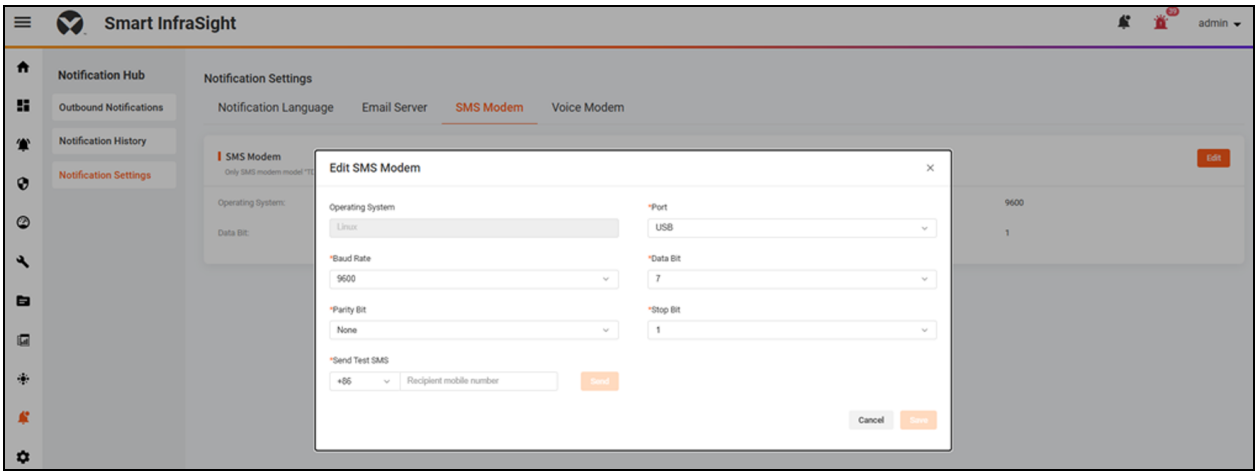
Stop Bits: Select the number of stop bits from the dropdown. Required.

Send Test SMS: Select the country code from the dropdown (default: +86), enter the recipient's phone number in the input field on the right, and click Send to send a test SMS, verifying that the current configuration is functional. If the test fails, the configuration cannot be saved. If the test succeeds, the Save button becomes active and the configuration can be saved.

Click *Save* to submit the configuration, or click *Cancel* to close the dialog without making changes.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 17.15 SMS Modem — Edit



Voice Modem

The voice modem configuration is a prerequisite for the voice notification feature, ensuring that voice notifications function properly. Before using the voice notification feature, the voice modem information must be configured in advance.

Viewing Voice Modem Configuration

Click the *Voice Modem* sub-tab. The page displays the current voice modem configuration. Only the CH-M3G7M7 model voice modem is currently supported. As shown in Figure 17.16 on the next page . Field descriptions are as follows:

If no voice modem is configured:

Enable Voice Modem: Displays No.

If a voice modem is configured:

Operating System: The current device operating system, displayed as Linux. Not editable.

Port: The modem connection port.

Baud Rate: The serial communication rate.

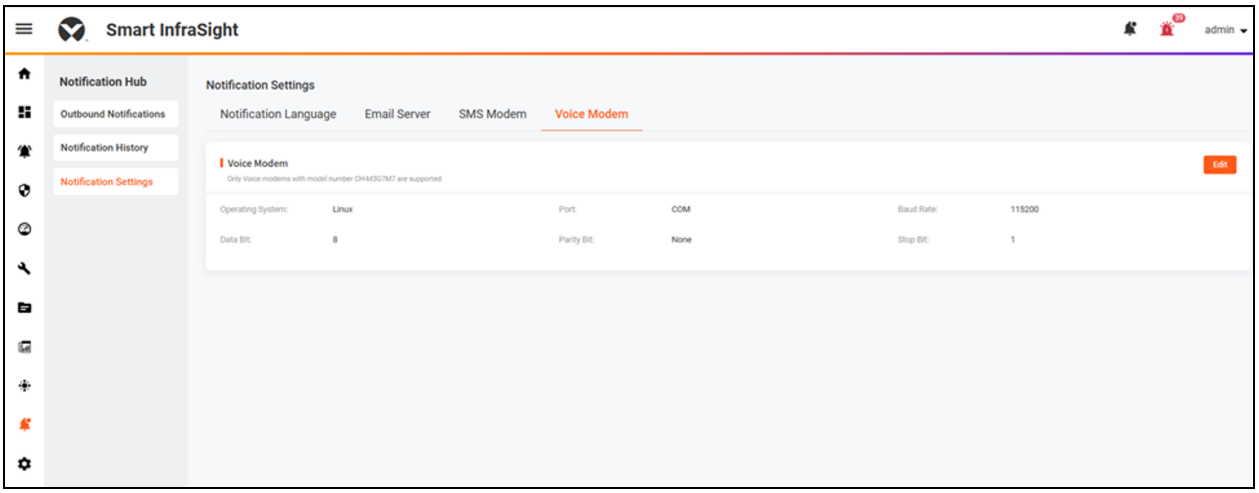
Data Bits: The number of serial data bits.

Parity: The serial parity check method.

Stop Bits: The number of serial stop bits.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 17.16 Voice Modem — View



Editing Voice Modem Configuration

Go to Notification Hub, then click on *Notification Settings* then click on *Voice Modem*, then click the *edit* button. The Edit Voice Modem dialog will appear, as shown in **Figure 17.17** on the facing page . Field descriptions are as follows:

If the voice modem is not enabled:

Enable Voice Modem: Unchecked

If the voice modem is enabled:

Enable Voice Modem: Checked

Operating System: Displays the current operating system. Grayed out and not editable.

Port: Select the connection port from the dropdown. Required.

Baud Rate: Select the communication rate from the dropdown. Required.

Data Bits: Select the number of data bits from the dropdown. Required.

Parity: Select the parity check method from the dropdown. Required.

Stop Bits: Select the number of stop bits from the dropdown. Required.

Send Test Voice: Select the country code from the dropdown (default: +86), enter the recipient's phone number in the input field on the right, and click Send to initiate a test voice call, verifying that the current configuration is functional. If the test fails, the configuration cannot be saved. If the test succeeds, the Save button becomes active and the configuration can be saved.

Click *Save* to submit the configuration, or click *Cancel* to close the dialog without making changes.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 17.17 Voice Modem — Edit

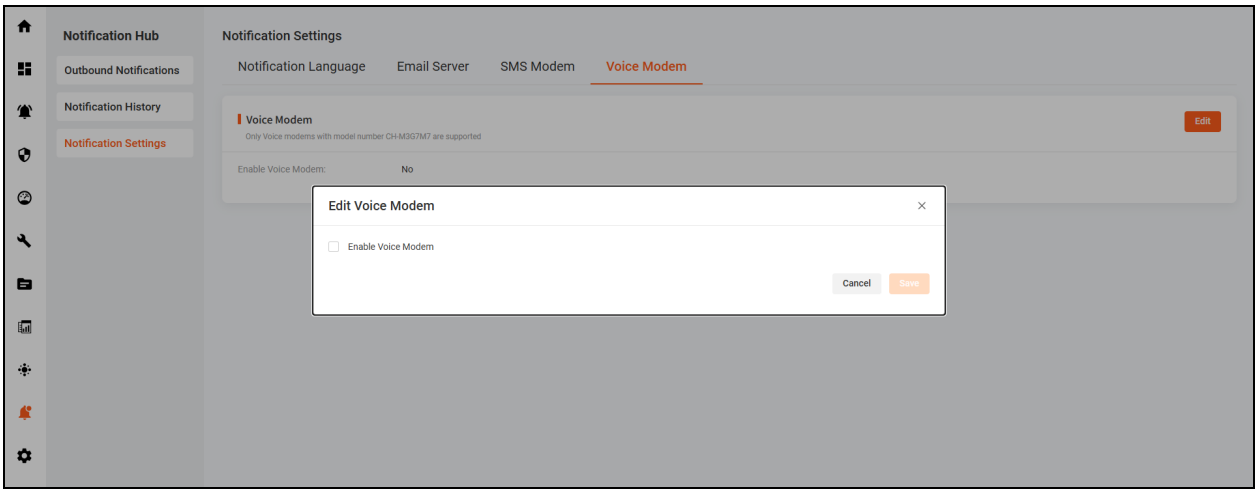
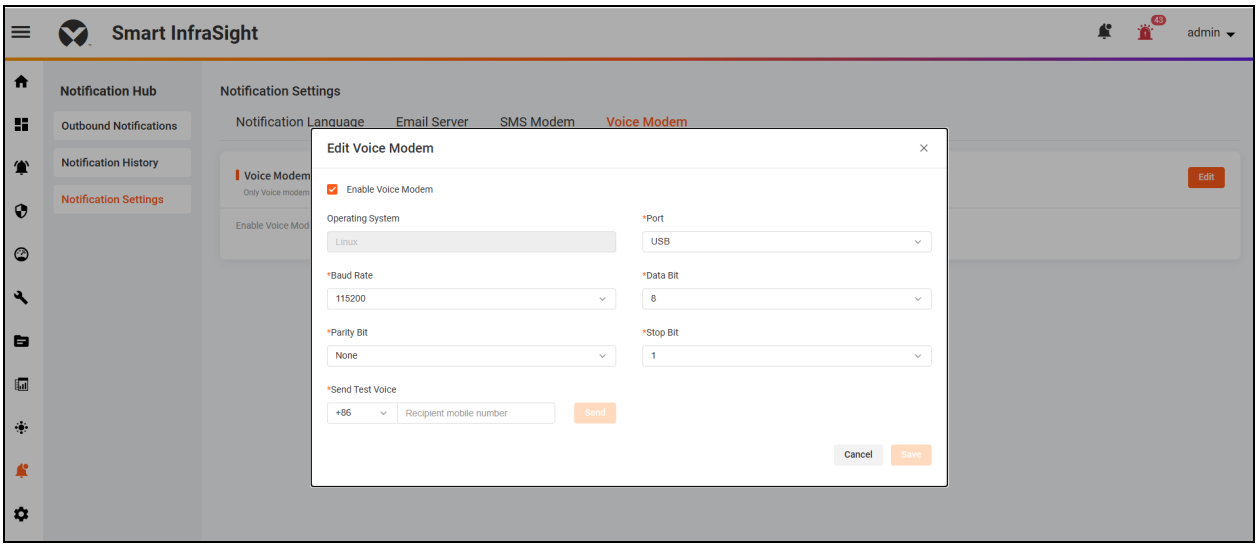


Figure 17.18 Voice Modem — Configuration



© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

18 System Configuration

18.1 General

18.1.1 Overview

The System Configuration module is a core feature of the Smart InfraSight Platform used to manage platform users, permissions, security policies, and system maintenance. You can use this module to create and manage user accounts and user groups, define roles and permissions, and configure password policies to enforce security standards. The platform also supports AD/LDAP integration for enterprise user authentication, SSL certificate management, session timeout settings, and license management. Additionally, you can perform system backup and restore, upgrade the platform, and review audit logs to trace all user operation.

18.1.2 Functional Modules

Smart InfraSight System Configuration includes the following functional modules. For detailed descriptions of each module, refer to the Detailed Features below.

- Users: Create, edit, delete, and manage local and AD/LDAP user accounts. Configure user credentials, contact information, user group assignments, and localization settings.
- User Groups: Create and manage user groups to organize users and assign roles that define their access permissions.
- Roles: Define roles with specific permission sets to control user access to platform features and pages.
- Address Book Contacts: Manage contact information including names, phone numbers, and email addresses for alarm notifications and system communications.
- Password Policy: Configure global password security rules including complexity requirements, expiration policies, account lockout settings, and first-login password change enforcement.
- Server Settings: Configure session timeout settings and replace the platform SSL certificate for secure connections.
- License: View current license usage for RDU devices, door access, cameras, and SNMP devices, and perform license upgrades to expand capacity limits.
- Backup And Upgrade: Perform full database backup and restore operations, and upgrade the platform by uploading upgrade packages.
- Audit Logs: View and export records of all user operations performed within the platform, with support for filtering by time range, operator, and operation category.
- AD/LDAP: Configure AD/LDAP connections to integrate enterprise directory services for user authentication and management.

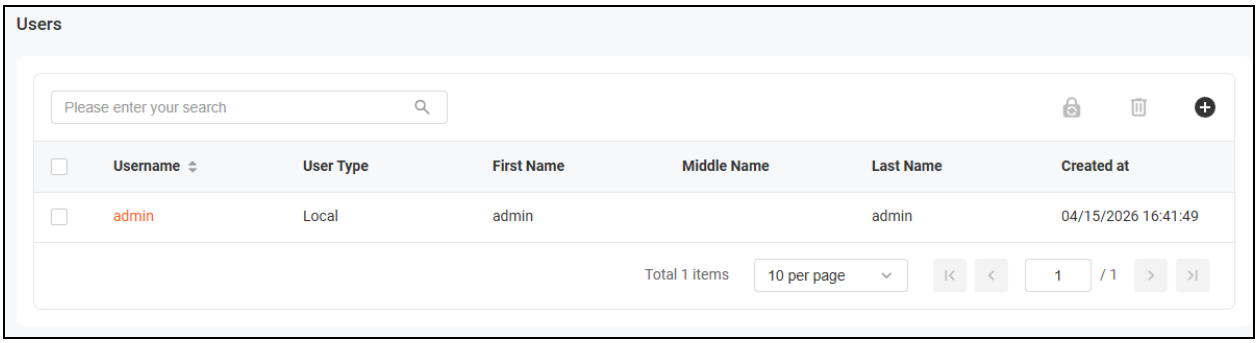
18.2 Detailed Features

18.2.1 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 18.1 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.1 List of Users



Adding the Users

After entering the User List page, click the *Add* User button in the upper-right corner to navigate to the Add User page, as shown in Figure 18.2 on the facing page .

The default user type is Local. In the user information form, fill in the following fields:

- Username (Required)
- First Name (Optional; no character restrictions)
- Middle Name (Optional; no character restrictions)
- Last Name (Optional; no character restrictions)
- Password (Required)
- Confirm Password (Required)
- Email (Required)
- Mobile Number (Optional)follows:

The User Group (Required) and Localization Settings must also be configured for the user.

Username requirements: Must be unique. Length: 1–32 characters. The following characters are not permitted '"|/.`

Password format requirements: Length: 10–108 characters. Must contain at least one uppercase letter, one lowercase letter, one digit, and one special character. The Confirm Password field must match the Password field exactly.

When the Send Password Change Email check box is selected, the username and password are sent to all email addresses associated with the current user upon saving. The email uses the language configured in Notification Settings under Notification Language Setting. The email content is as follows:

- Topic: Smart Infrasight New User
- Content: Your user XXX in the Smart Infrasight system (XX.XX.XX.XX) has been created by the system administrator. Please use the temporary password XXXX to log in and set a new password after logging in. Do not disclose your temporary password to others.

When the user logs in with the initial password, the system automatically redirects to the Change Password page to prompt the user to set a new password.

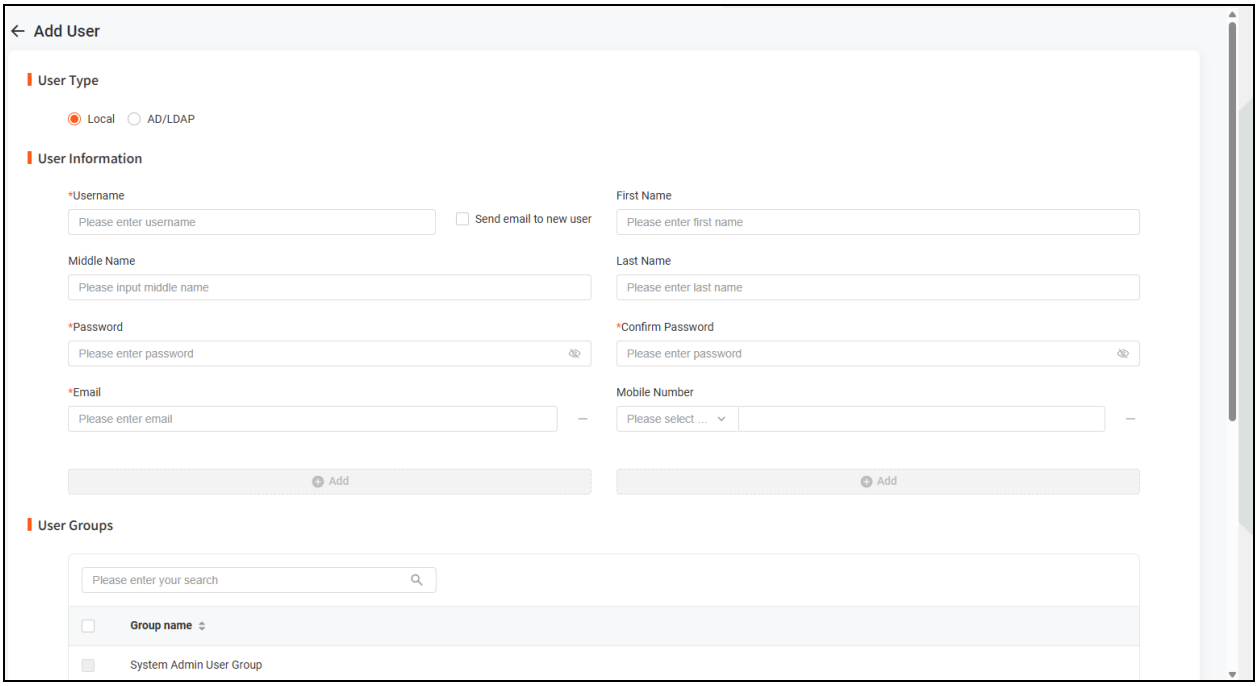
© 2026 Vertiv Group Corp. All Rights Reserved.

Email format requirements: Must be a standard email format. The prefix can contain digits, letters, underscores, and hyphens. The suffix must contain at least two segments separated by dots. The top-level domain must be 2–4 characters. Neither the prefix nor the suffix may end with _, -, or .. Multiple email addresses can be added for a single user, but duplicate emails under the same user are not permitted.

Mobile number format requirements: After selecting the country code, enter a valid mobile number for that country. Multiple mobile numbers can be added for a single user, but duplicate mobile numbers under the same user are not permitted.

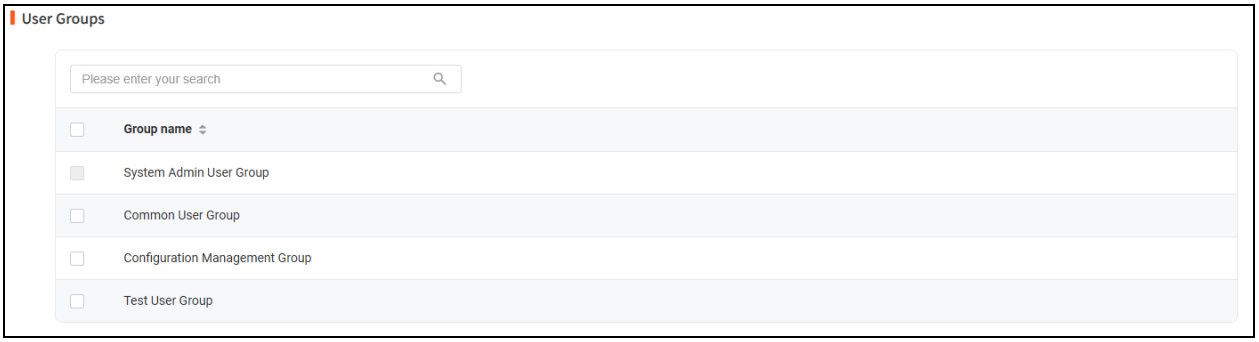
NOTE: Once saved, the username cannot be modified. If the username field is left blank, a prompt indicates that the username is a required field and the Save button remains disabled. If the email address is not provided, the Save button remains disabled. If no user group is selected, the Save button remains disabled.

Figure 18.2 Adding the User



Select the user group to which the user needs to be assigned by checking the checkbox on the left side of the desired user group, as shown in Figure 18.3 below .

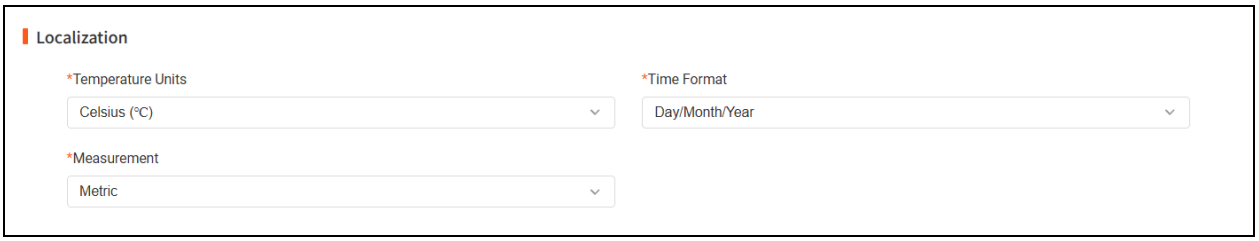
Figure 18.3 Selecting the User Group



© 2026 Vertiv Group Corp. All Rights Reserved.

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), The default localization configuration for new users inherits the admin user's localization settings. After logging in, users can modify their localization settings by clicking their username in the upper-right corner of the system and navigating to User Profile, as shown in **Figure 18.4** below .

Figure 18.4 Localized Configuration



After completing the new user information, click *Save* to finish creating the user. The user can then use their credentials to log in to the platform.

Editing the User

After entering the User List page, click the username of the user whose information you want to edit to navigate to the Edit User page, as shown in **Figure 18.5** below .

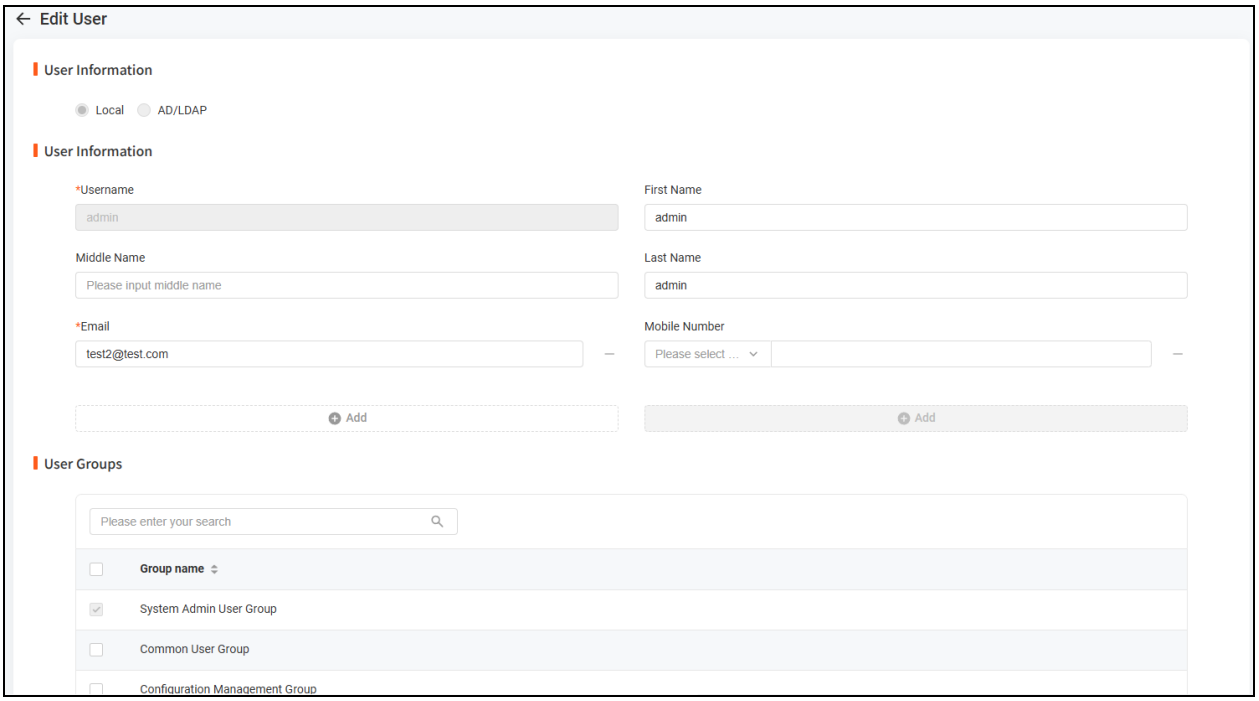
Figure 18.5 Editing the User



On the Edit User page, all fields are editable except User Type and Username, as shown in **Figure 18.6** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

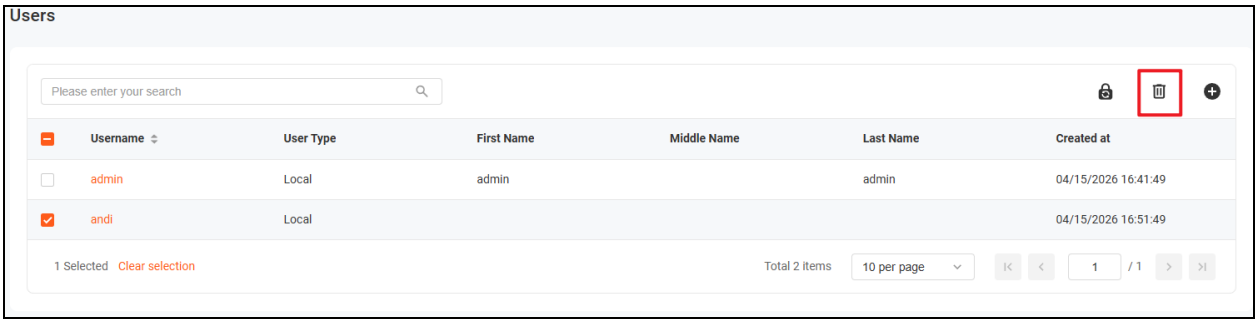
Figure 18.6 Editing the User Page



Deleting the User

After entering the User List page, select the users you want to delete by checking their checkboxes, then click the Delete button in the upper-right corner of the list to proceed with the deletion, as shown in **Figure 18.7** below .

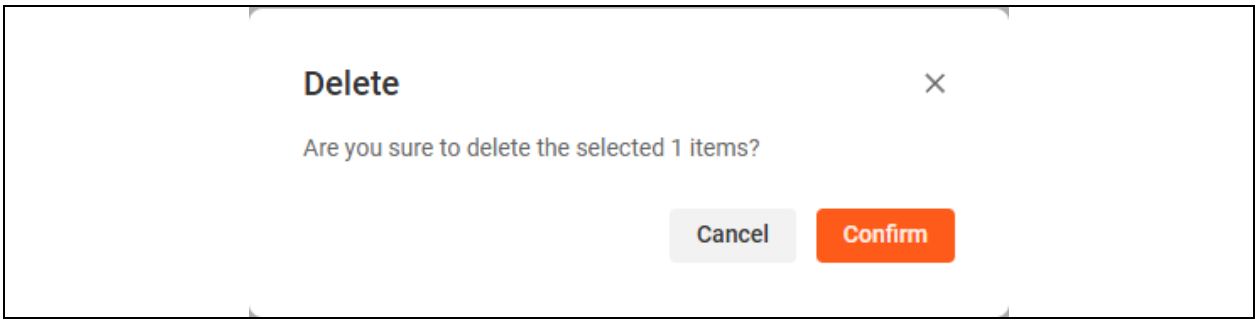
Figure 18.7 Deleting the User Entry



After clicking Delete, a dialog displays the number of users selected for deletion. Click *Confirm* to complete the deletion, as shown in **Figure 18.8** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.8 User Deletion Window

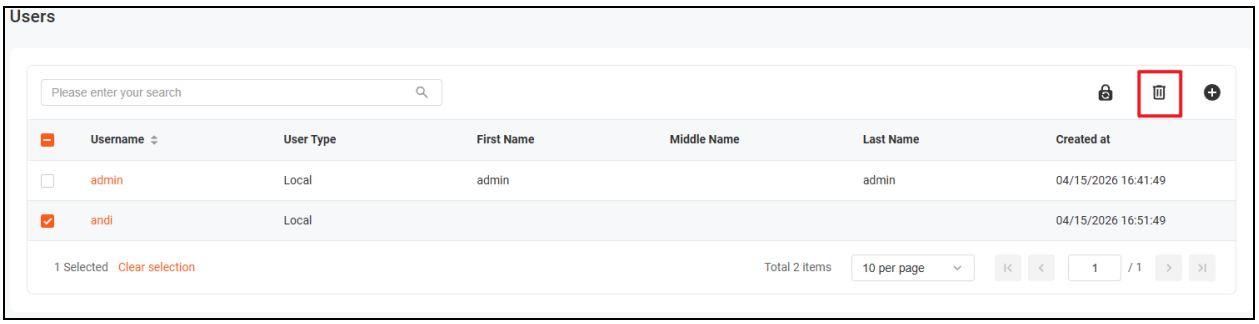


NOTE: The admin user cannot be deleted. Only other users can be deleted.

Reset the User's Password

After entering the User List page, select the user whose password you want to reset, then click the *Reset* Password button in the upper-right corner of the list to proceed with the password reset operation, as shown in Figure 18.9 below . The reset password operation applies to a single user only. If multiple users are selected, the button is disabled.

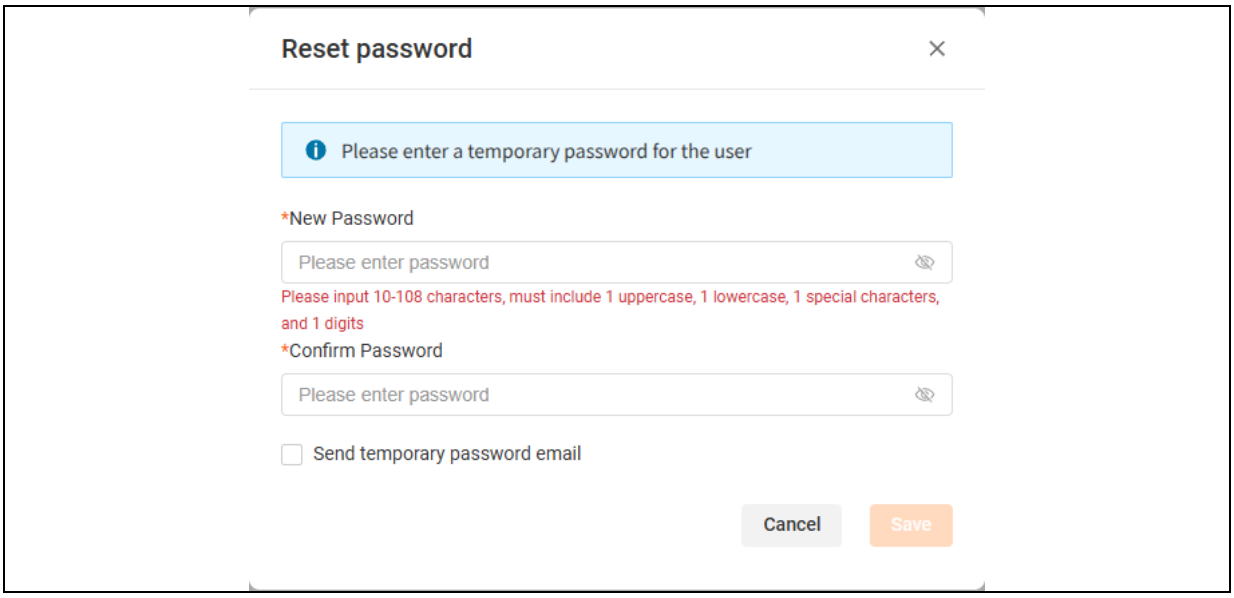
Figure 18.9 Resetting the Password Entry



After clicking the button, a Reset Password dialog appears. Enter the new password and confirm password in the dialog, then click *Save* to change the user's password to the entered temporary password, as shown in Figure 18.10 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.10 Resetting the User's Password



If the Send Password Change Email check box is selected, the temporary password is sent to all email addresses associated with the current user upon saving. The email uses the language configured in Notification Settings under Notification Language Setting. The email content is as follows:

- Subject: Smart Infrasight Temporary Password
- Content: Your password for user XXX in the Smart Infrasight system (XX.XX.XX.XX) has been reset by the system administrator. Please log in with the temporary password XXXX and set a new password after logging in. Do not disclose your temporary password to others.

When the user successfully logs in with the temporary password, the system automatically redirects to the Change Password page to guide the user to set a new password.

NOTE: The new password must not match any of the last 10 previous passwords.

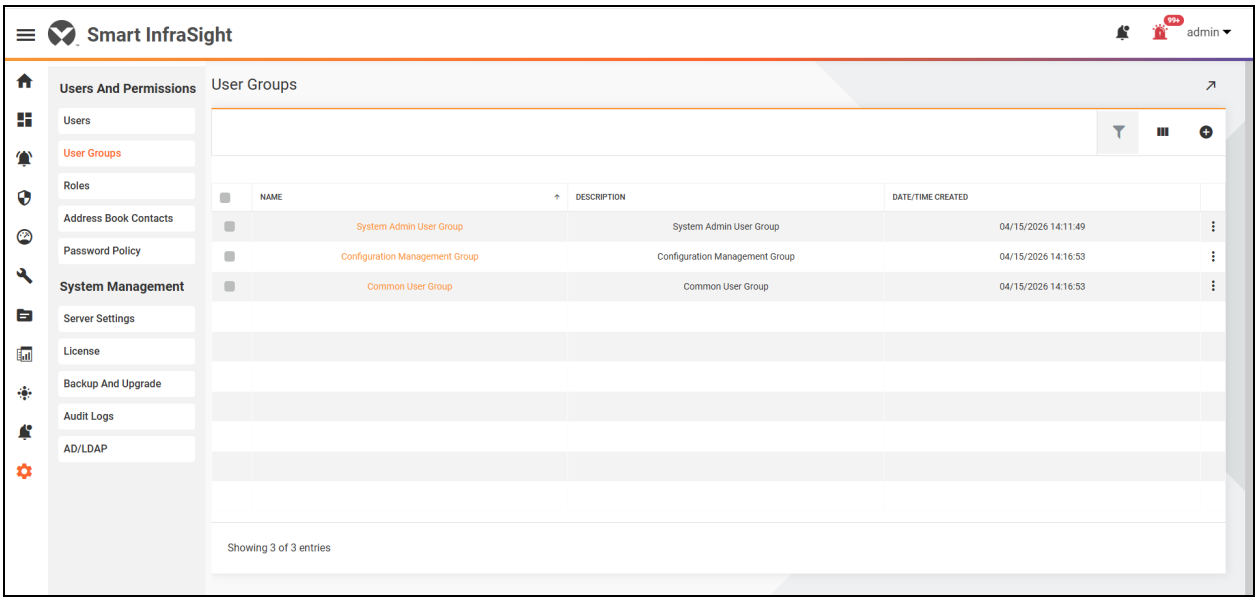
18.2.2 List of User Groups

User Group List

In System Settings, go to User Groups to view the List of the three default user groups currently in the Platform. Default user groups cannot be deleted, and the System Administrator user group cannot be edited, as shown in Figure 18.11 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.11 User Group List

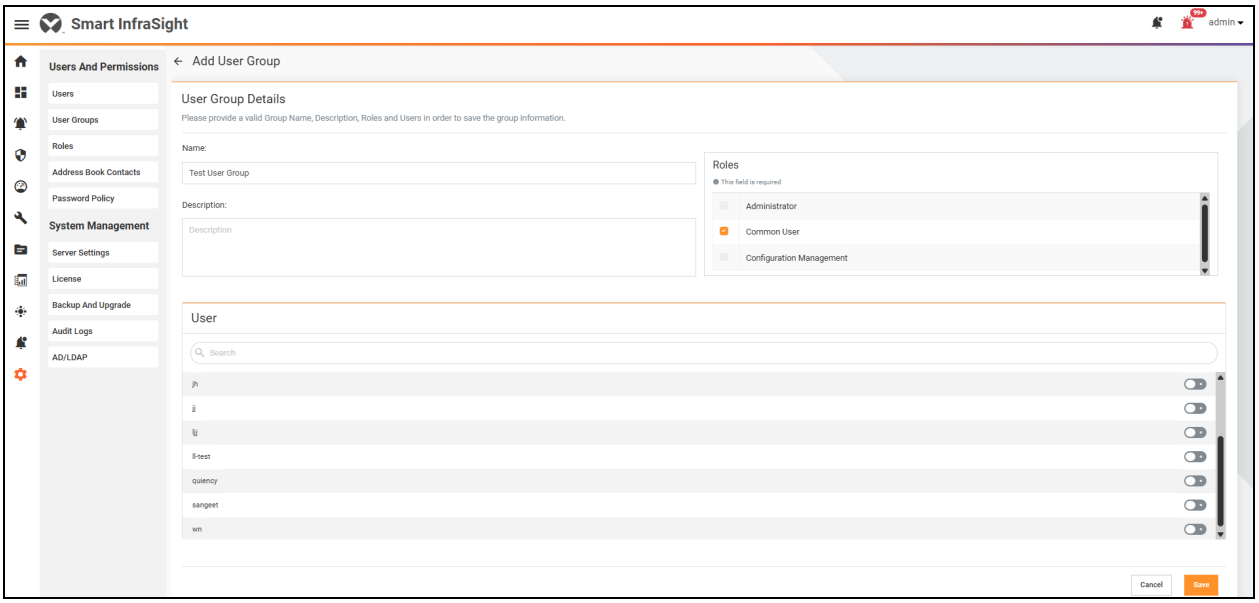


Add User Group

1. Navigate to System Settings, go to User Groups.
2. Click the *Add* button in the upper-right corner.
3. In the interface, enter the following details to add the user group:
   - Name: Required; maximum 64 characters.
   - Description: Optional; maximum 128 characters.
   - Role: Required; supports multiple selections. The Administrator Role cannot be selected by default.
   - User: Optional.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.12 Adding a User Group



NOTE:

1. User group names must be unique.

2. In English environments, names must not contain special characters such as vertical bars (|), single quotes ('), double quotes ("), or slashes (/).

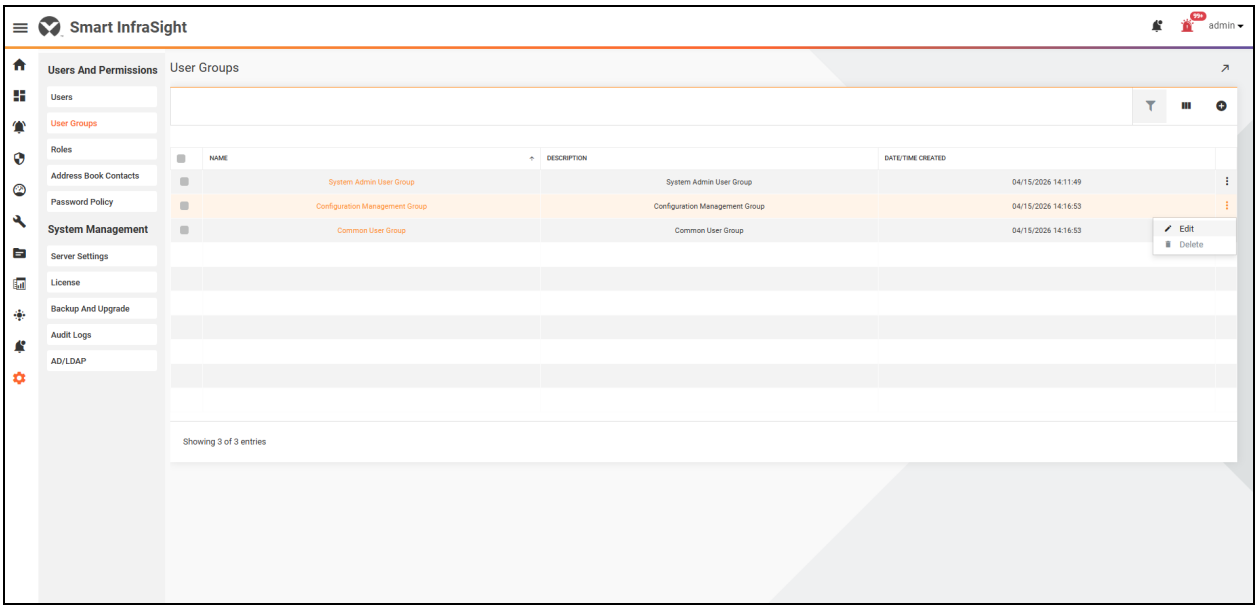
3. In Chinese environments, names must not contain special characters such as vertical bars (|), spaces, or slashes (/).

Editing the User Group

1. In the User Groups List, click the *More* icon on the right side of the target row and select *Edit*.
2. In the edit interface, modify the user group information. The Name and Role fields are mandatory.
3. Click *Save* to complete the modification.

© 2026 Vertiv Group Corp. All Rights Reserved.

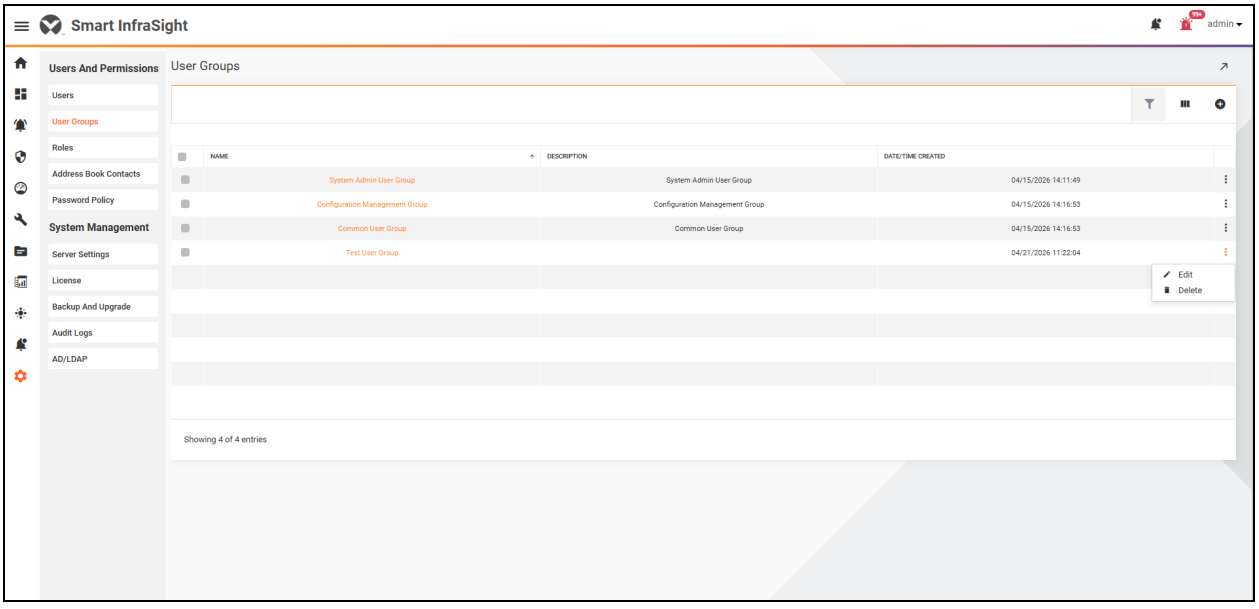
Figure 18.13 Editing the User Group



Deleting a User Group

In the **User Groups List**, click the *More* icon on the right side of the target row and select *Delete*. As shown in **Figure 18.14** below .

Figure 18.14 Deleting a User Group



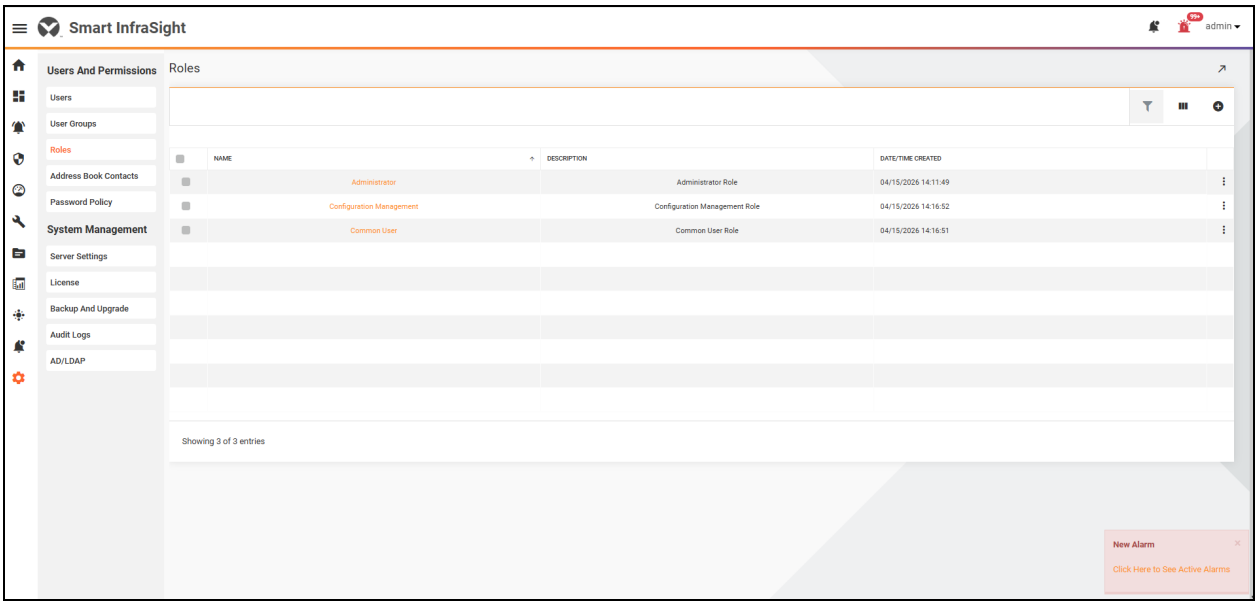
NOTE: The three default user groups cannot be deleted, and custom user groups can be deleted.

© 2026 Vertiv Group Corp. All Rights Reserved.

18.2.3 Roles

Go to **System Settings**, then click on *Role* to view the **List** of roles. The Platform contains three default roles that cannot be deleted or modified, as shown in **Figure 18.15** below .

Figure 18.15 List of Roles

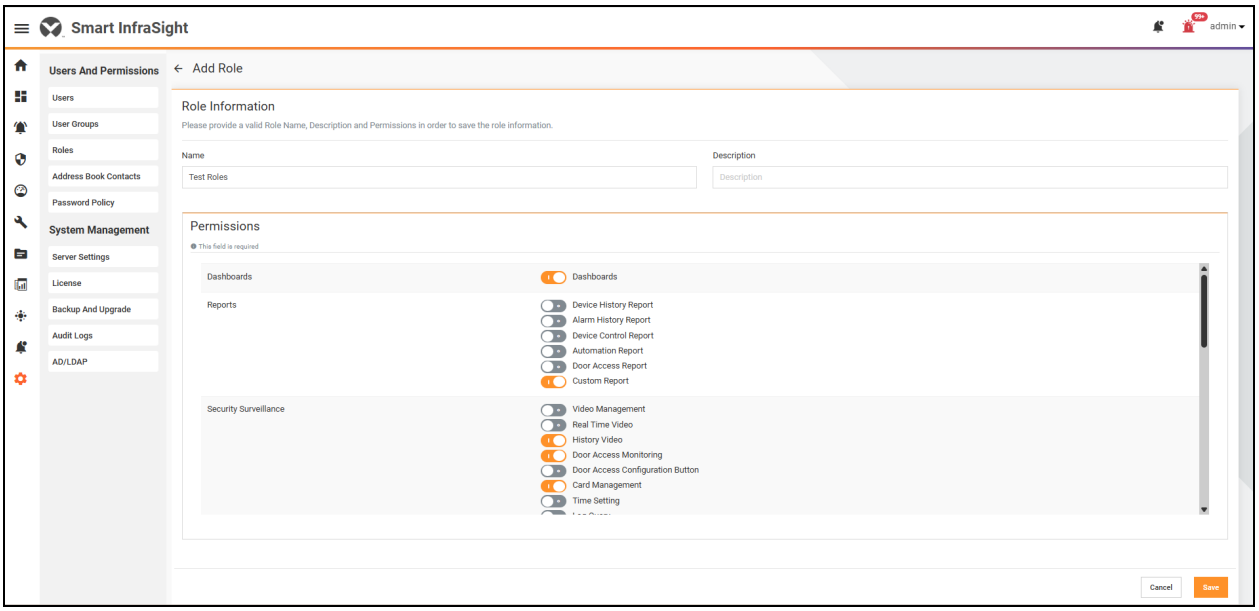


Adding a Role

1. Navigate to System Settings > Role and click the *Add* button in the upper-right corner.
2. In the interface, enter the following details to add the role:
   - **Name**: Required; maximum 64 characters.
   - **Description**: Optional; maximum 128 characters.
   - **Permission**: Required. By default, the **Platform** selects **Contacts**, **Current Alarms**, **Historical Alarms**, and **Monitoring** page permissions, as shown in **Figure 18.16** on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.16 Adding a Role



NOTE:

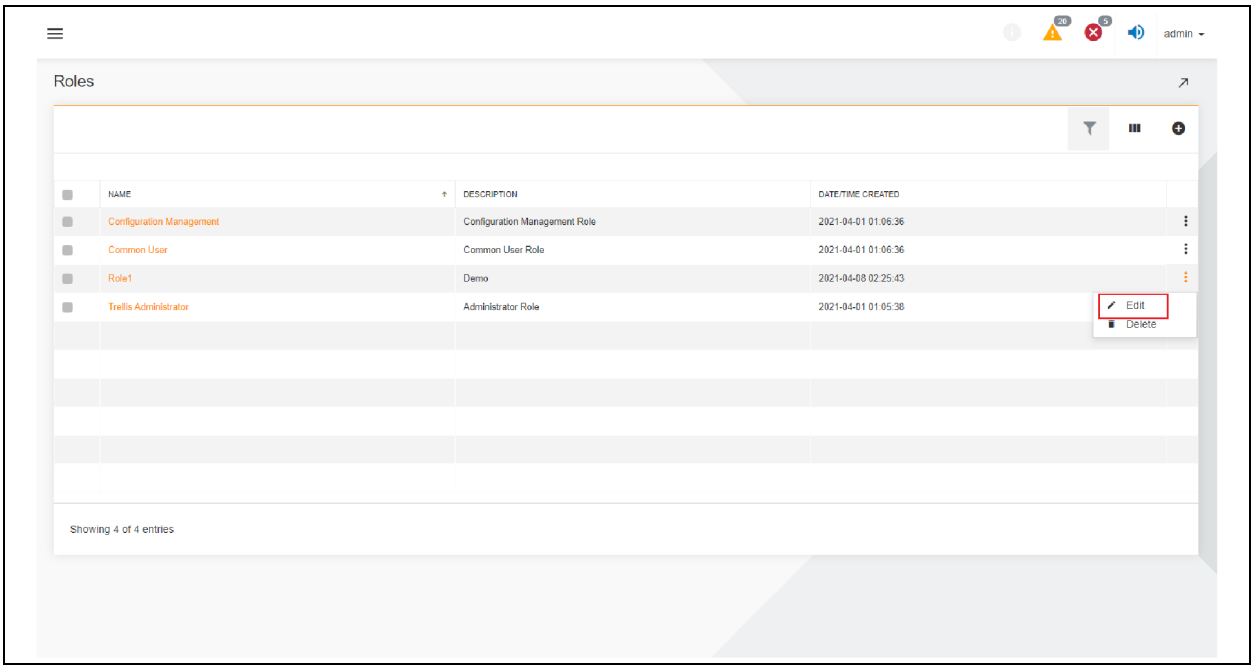
1. **Role names must be unique.**
2. **Role names must not contain English special characters, including vertical bars (|), single quotes ('), double quotes ("), or slashes (/).**
3. **The default selected permissions are mandatory for all users and cannot be edited.**

Editing the Role

1. In the **Role** list interface, click the *More* icon on the right side of the target row and select *Edit*.
2. In the **Dialog box**, modify the role information. The **Name** field is mandatory.
3. Click *Save* to complete the update, as shown in **Figure 18.17** on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

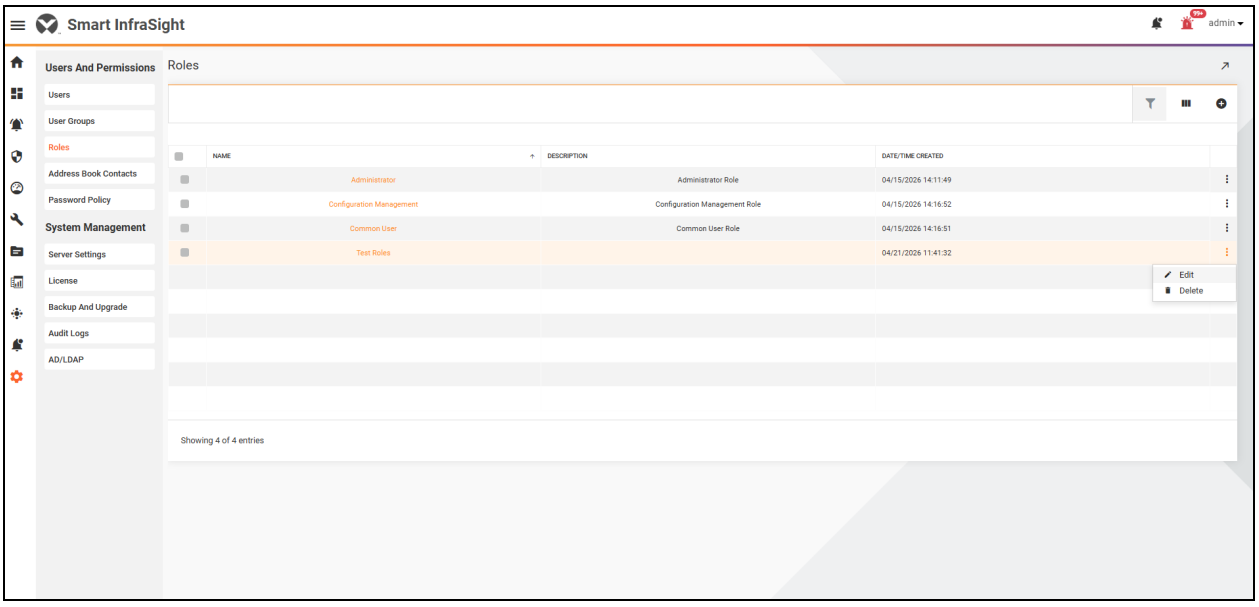
Figure 18.17 Editing the Role



Deleting the Role

In the **Role** list interface, click the *More* icon on the right side of the target row and select *Delete*, as shown in **Figure 18.18** below .

Figure 18.18 Deleting a Role



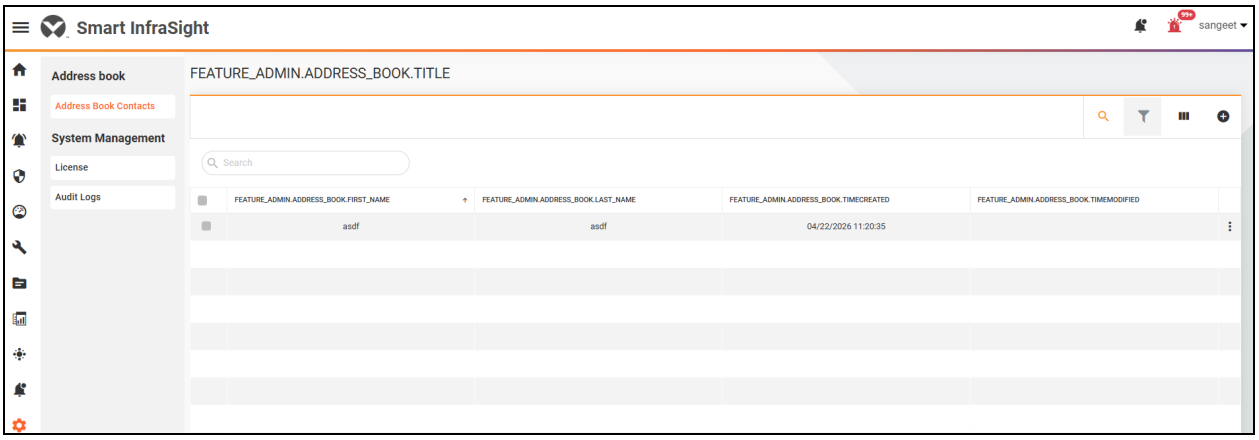
NOTE: The three default roles cannot be deleted, and custom roles can be deleted.

© 2026 Vertiv Group Corp. All Rights Reserved.

18.2.4 Address Book Contacts

In the **Contacts** module, **O&M** admins can centrally manage the basic information, phone numbers, and email addresses of personnel. This ensures the **Platform** can accurately reach the relevant stakeholders when it triggers an **Alarm** or sends a notification.

Figure 18.19 View Contacts List



Navigate to the **Contacts** page to view a List of all created contact information.

- **Default List Columns: Name, Creation Time**, and **Modification Time**.
- **Search and Filter:** Enter a name in the top search box for fuzzy matching. Click the *Column Configuration* icon to customize which fields are displayed in the List.

Add Contact

Click the (+) icon in the upper-right corner to enter the **Add Contact to Contacts** page:

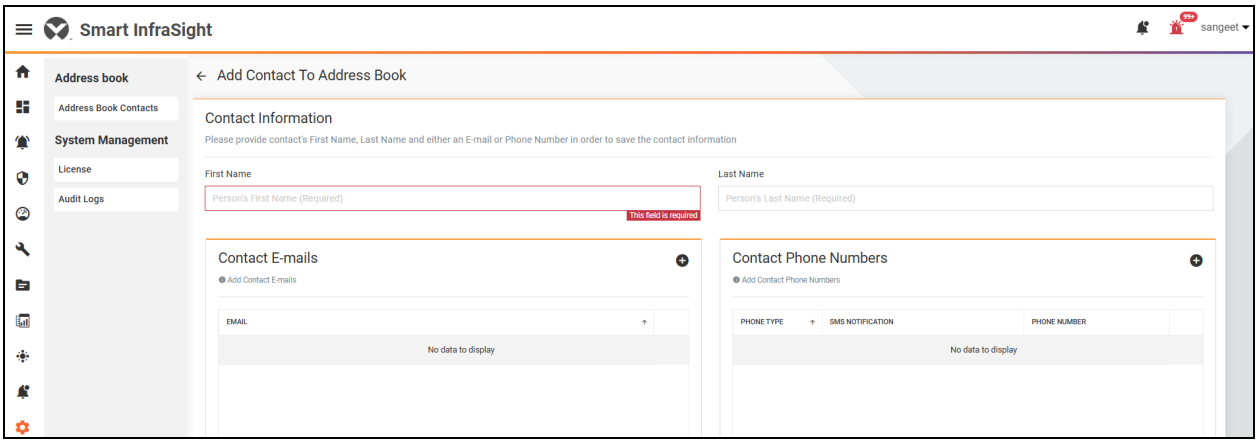
- **Complete Basic Information:** In the **Contact Information** area, enter the legal name in the **Last Name** and **First Name** text boxes. Both fields are required.
- **Add Email Address:**
  1. Click the (+) icon in the **Contact Email** area.
  2. In the **Add Contact Email Dialog box**, enter a valid **Email** address.
  3. Click *Add* to save the entry. You can add multiple email addresses for a single contact.

Add Phone Number:

1. Click the (+) icon in the Contact Phone area.
2. In the **Add Contact Phone Number Dialog box,** select the **Phone Type** (e.g., Personal).
3. Toggle the **SMS Notification** switch as needed. If enabled, the **Platform** will send **Alarm** text messages to this number.
4. In the **Phone Number** area, select the country code and enter the full mobile or landline number.
5. Click *Add* to save the entry.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.20 Adding a Contact



Editing the Contact Information

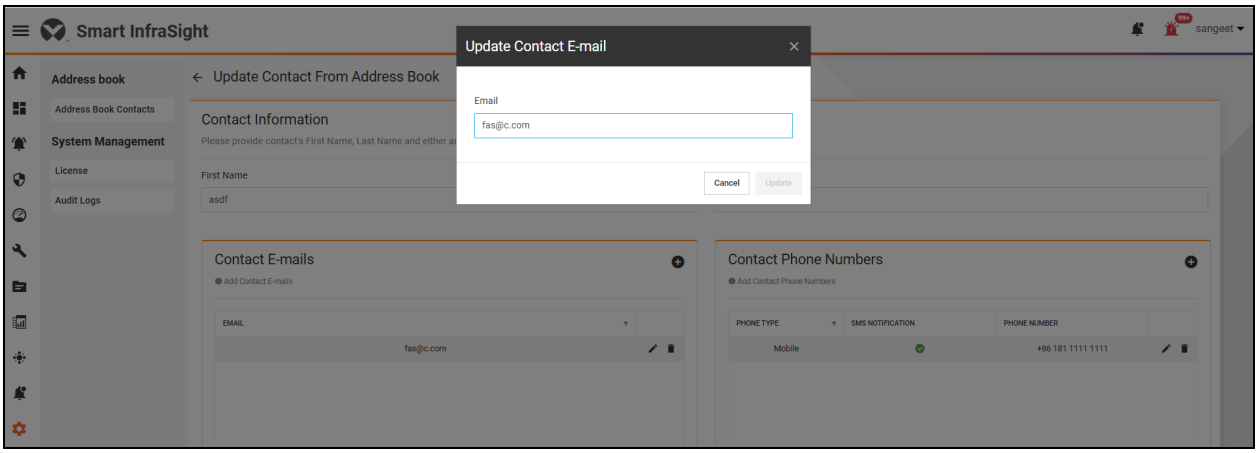
To modify contact details, use one of the following methods to enter the edit interface:

Method 1: Select the checkbox on the left side of the List. In the action bar that appears above the **List**, click the *Edit* icon (pencil shape).

Method 2: Click the *More* icon (ellipses (⋮)) on the far right of the target row and select *Edit* from the **Drop-down list**.

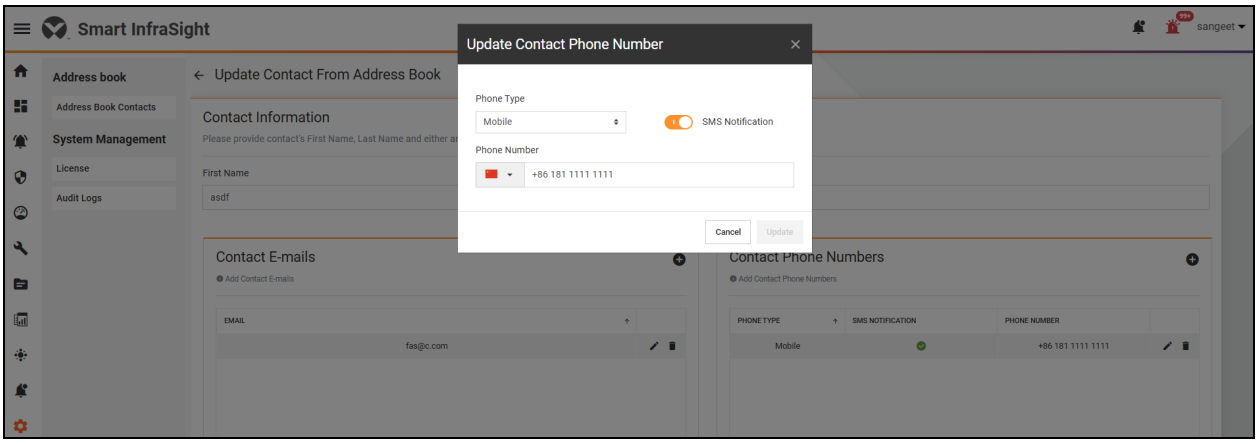
In the edit page, you can modify the name or perform Edit or Delete actions on bound email addresses and phone numbers.

Figure 18.21 Edit Contact Email



© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.22 Edit Contact Phone Number



Deleting a Contact

- **Single Delete**: Click the *More* icon in the action column of the List and select *Delete*.
- **Batch Delete**: Select the *checkboxes* for one or more contacts, click the Delete icon (trash can shape) in the action bar above the List, and click OK in the confirmation Dialog box.

After deleting a contact, all associated phone and email **Alarm Notification** rules may become invalid. Confirm the contact is not currently assigned to any active notification tasks before deletion.

Figure 18.23 Deleting a Contact

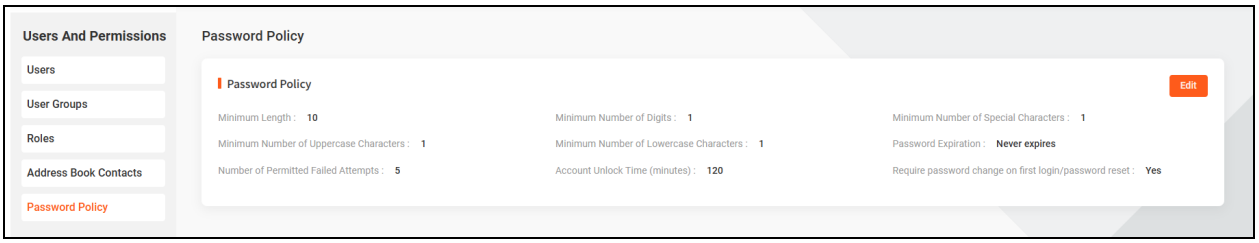


18.2.5 Password Policy

Click *Password* Policy in the Users And Permissions menu to view the global password security rules of the platform. All user passwords must comply with the constraints configured here, including Minimum Length, Minimum Number of Digits, Minimum Number of Special Characters, Minimum Number of Uppercase Characters, Minimum Number of Lowercase Characters, and Password Expiration. In addition, security policies such as Number of Permitted Failed Attempts, Account Unlock Time (minutes), and Require password change on first login/password reset can also be configured.

© 2026 Vertiv Group Corp. All Rights Reserved.

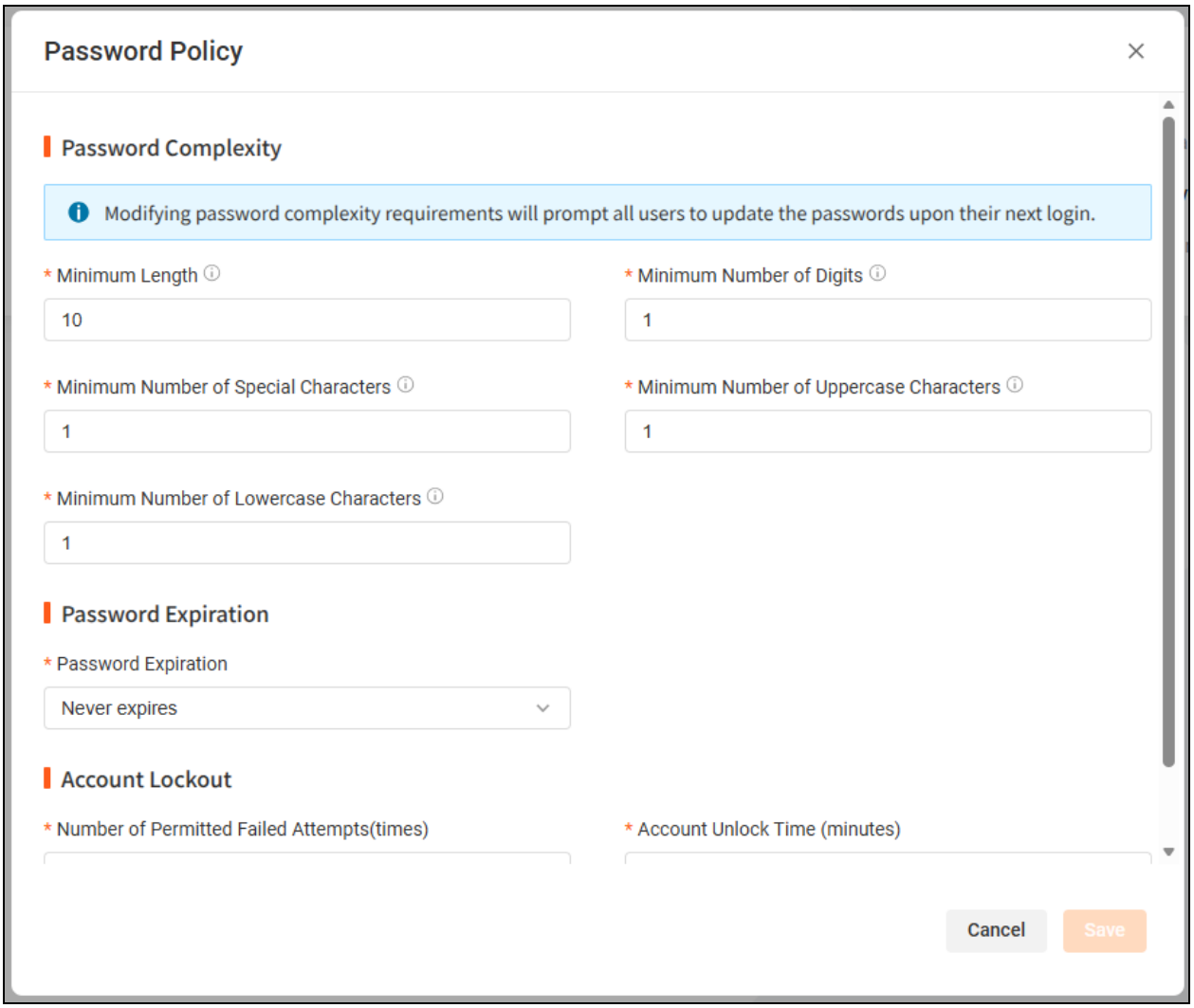
Figure 18.24 Password Policy



NOTE: The viewing and editing of Password Policy is only available to the super administrator admin.

The administrator can click the *Edit* button in the upper-right corner to open a dialog box, in which the administrator can edit the Password Policy settings. After the password policy is modified, all users will be required to change their passwords upon their next login. The dialog box contains the following fields:

Figure 18.25 Password Policy Configuration



The Password Policy is divided into four sections, all of which can be configured:

© 2026 Vertiv Group Corp. All Rights Reserved.

1. Password Complexity: Once saved, all users' subsequent passwords must comply with the latest complexity requirements, including passwords for newly created users and passwords after reset. The complexity requirements include Minimum Length, Minimum Number of Digits, Minimum Number of Special Characters, Minimum Number of Uppercase Characters, and Minimum Number of Lowercase Characters.

NOTE: Modifying password complexity requirements will prompt all users to update their passwords upon their next login.

2. Password Expiration: The default setting is Never Expires, meaning the password is permanently valid and will not expire. When switched to Expires Periodically, two additional input fields will appear: Password Expires After (days) and Password Expiration Reminder Time (days), with default values of 365 days and 7 days respectively. Once configured, when the reminder time is reached, a prompt will appear after the user logs in, reminding the user to change their password as soon as possible. If the password has already expired and has not been changed, the system will forcibly redirect the user to the change password page upon their next login.

3. Account Lockout: The default Number of Permitted Failed Attempts (times) is 5, and the default Account Unlock Time (minutes) is 120. This means that after 5 consecutive incorrect password attempts, the account will be locked for 120 minutes, during which the user cannot log in again.

4. Require password change on first login/password reset: When this option is checked, new users or users whose passwords have been reset must change their password upon first login before accessing the system. When unchecked, no password change is required upon first login.

18.2.6 Server Settings

The server settings have only one tab: Security Settings.

In Security Settings, you can:

- Set *Session Timeout Settings* i.e., how long a user can stay logged in before they are automatically logged out.
- Replace the system's SSL certificate.

The system uses a default self-signed SSL certificate. You can replace it with your own verified certificate to make your network connection more secure.

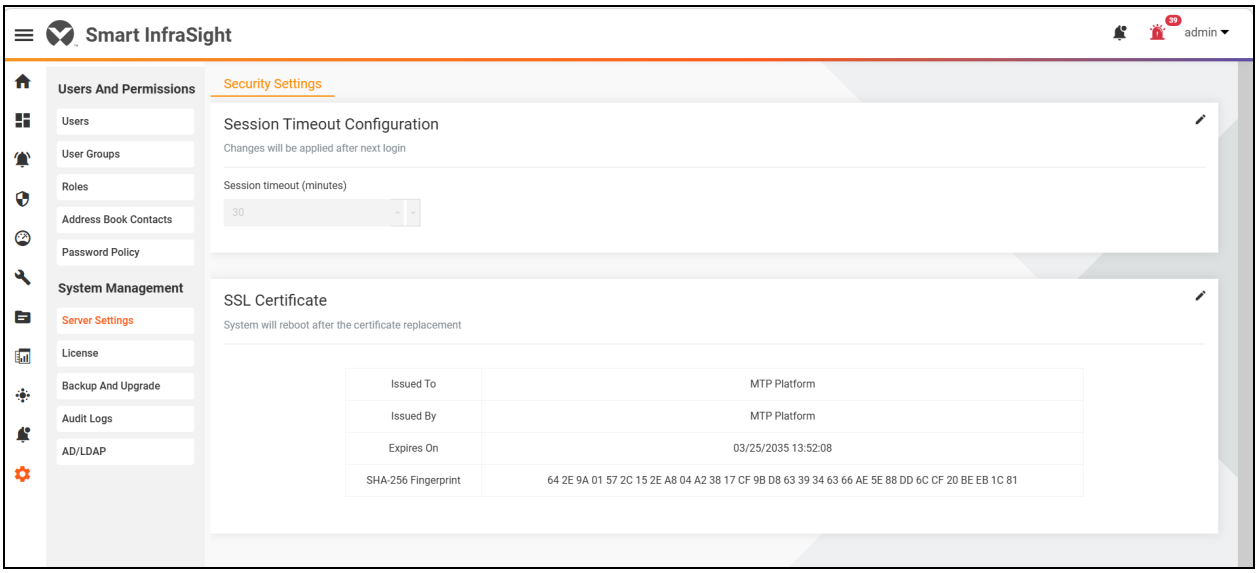
Security Settings

Session Timeout Settings

Click on the menu *System Config*. Then click on the *Server settings*, with the Security Settings tab selected as default. As shown in Figure 18.26 on the facing page .

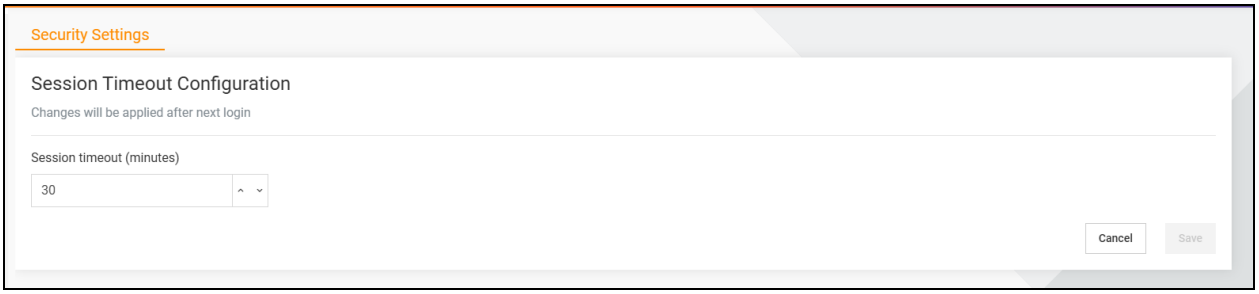
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.26 Security Settings



To set the session timeout, click *Edit* icon in the upper-right corner, then the input box will become editable, as shown in Figure 18.27 below .

Figure 18.27 Session Timeout Configuration



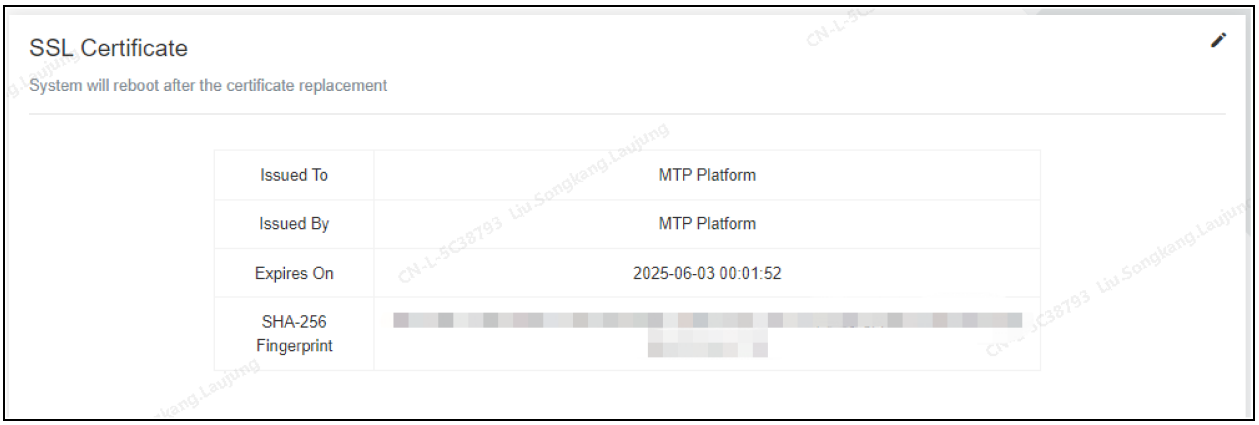
Set the Session Timeout period, which can be maximum of 1440 minutes (1 day), then click *Save*. The changes will take effect immediately.

Replacing the SSL Certificate

The SI system uses a self-signed certificate by default. You can upload a trusted certificate signed by a certification authority to replace the original certificate, as shown in Figure 18.29 on the next page .

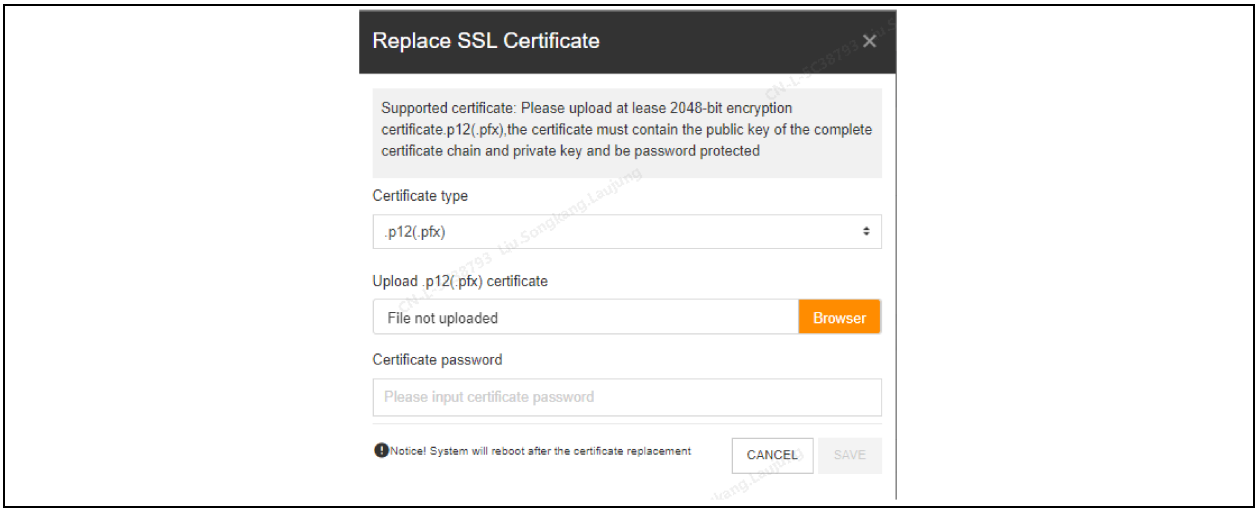
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.28 SSL Certificate Window



To do this, click *Edit* icon in upper-right corner to open the Replace Certificate window, as shown in Figure 18.29 below .

Figure 18.29 Replacing SSL Certificate Window



18.2.7 License

RDU License Management (License Management) has two main functions: the first is to display the number of monitorable RDU devices, Door Access Number, RDU Number, Camera Number, and SNMP device count, along with their current usage; the second is to perform License Upgrade to expand the maximum limits for RDU Devices Number, Door Access Number, RDU Number, and Camera Number. Licenses are provided to Smart InfraSight based on the product model, covering RDU Number, Door Access Number, Camera Number, and RDU Devices Number. The following three License types are available:

1. Basic: The default RDU Number is 32. After a License Upgrade, the RDU Number can be expanded to 96. The RDU Devices Number is 500. The default Door Access Number is 32, which can be upgraded to a maximum of 500. The default Camera Number is 32, which can be upgraded to a maximum of 500.

2. Essential: The default RDU Number is 128. After a License Upgrade, the RDU Number can be expanded to 384. The RDU Devices Number is 800. The default Door Access Number is 64, which can be upgraded to a maximum of 800. The default Camera Number is 64, which can be upgraded to a maximum of 800.

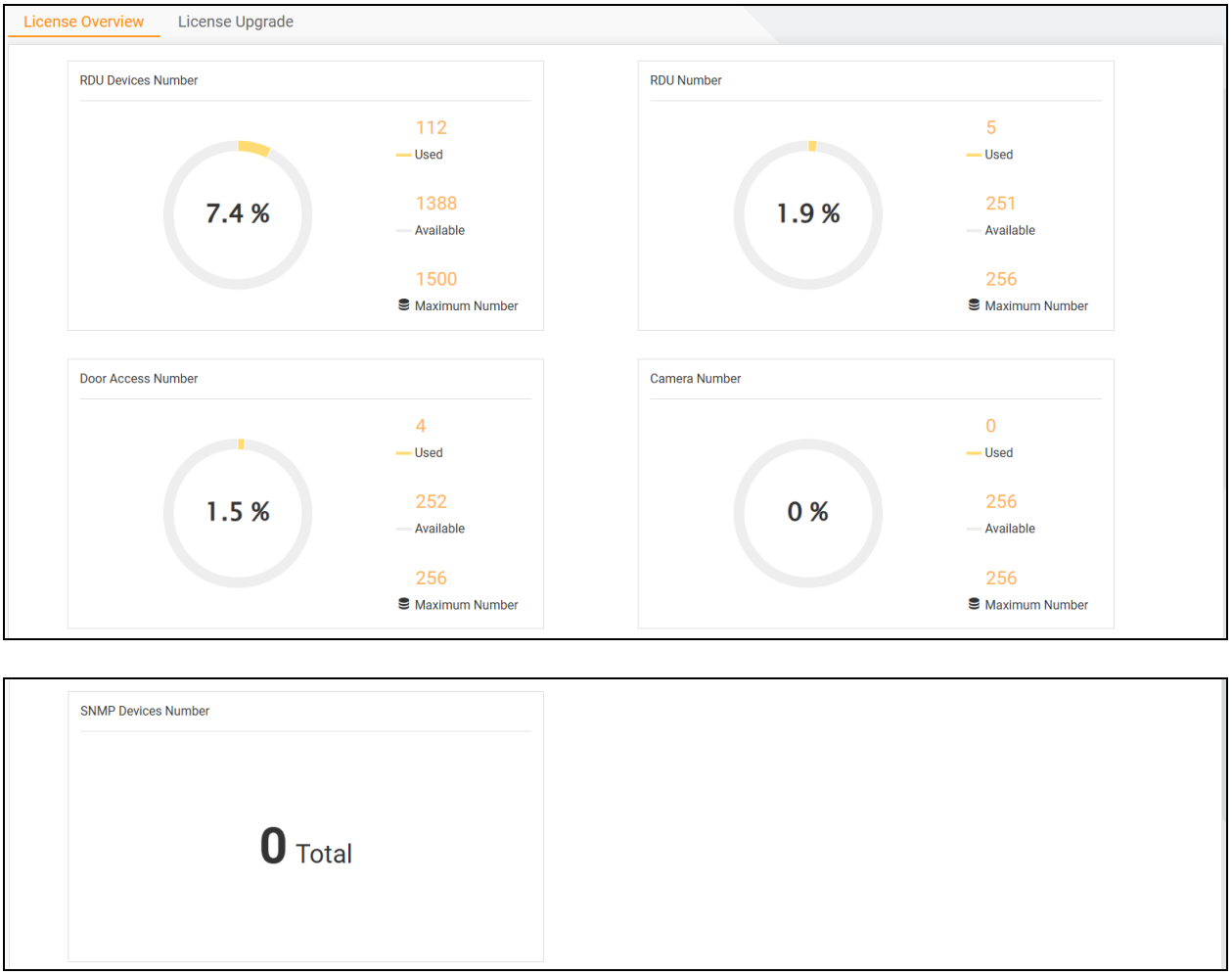
© 2026 Vertiv Group Corp. All Rights Reserved.

3. **Premium**: The default RDU Number is 256. After a License Upgrade, the RDU Number can be expanded to 768. The RDU Devices Number is 1500. The default Door Access Number is 256, which can be upgraded to a maximum of 1500. The default Camera Number is 256, which can be upgraded to a maximum of 1500.

License Overview

The **License Overview** tab displays the RDU Devices Number, Door Access Number, RDU Number, Camera Number, and SNMP Devices Number, along with their current usage. For each category, the platform displays the **Used**, **Available**, and **Maximum Number**. The percentage shown in the chart represents the ratio of Used to Maximum Number. SNMP Devices Number is displayed for reference only and is not subject to any limit.

Figure 18.30 License Overview



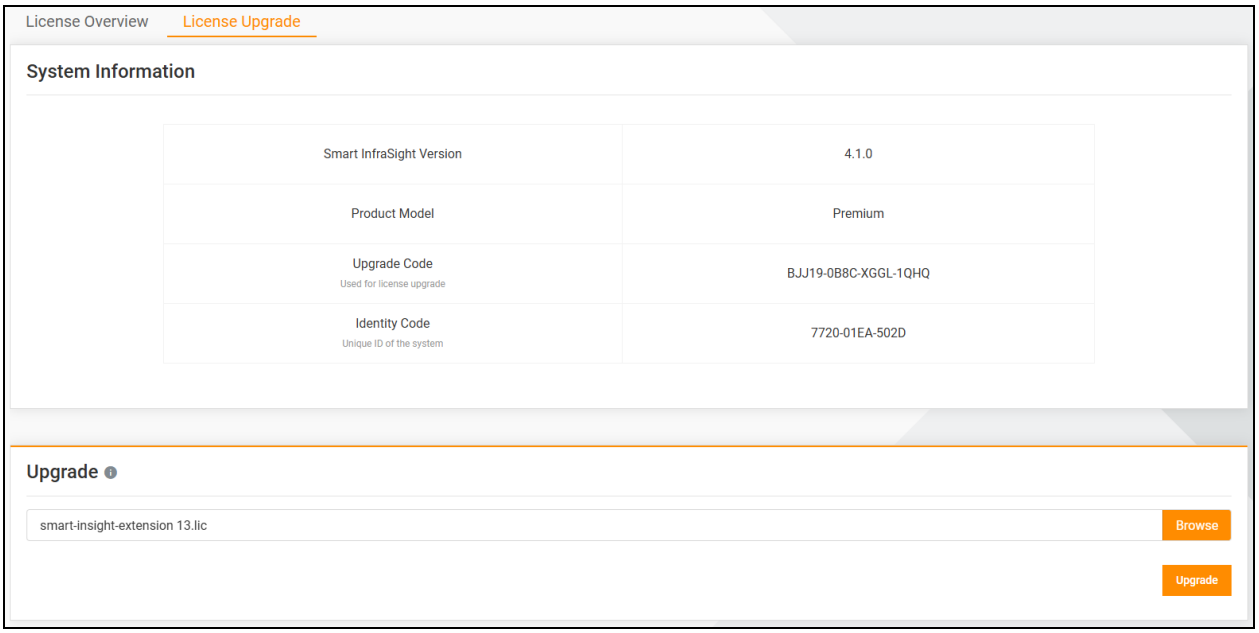
License Upgrades

The License Upgrade tab expands the maximum limits for RDU Devices Number, Door Access Number, RDU Number, and Camera Number. This page is divided into two sections. The upper section displays platform information: **System Version, Product Model, Upgrade Code**, and **Feature Code**. The lower section is the license upgrade area. Upload a license file in this section, then click *upgrade* to apply the upgrade. The **Confirm Upgrade** button is disabled when the input field is empty.

© 2026 Vertiv Group Corp. All Rights Reserved.

NOTE: The license file is generated based on the Upgrade Code. To obtain a license file, provide the Upgrade Code to Vertiv technical support.

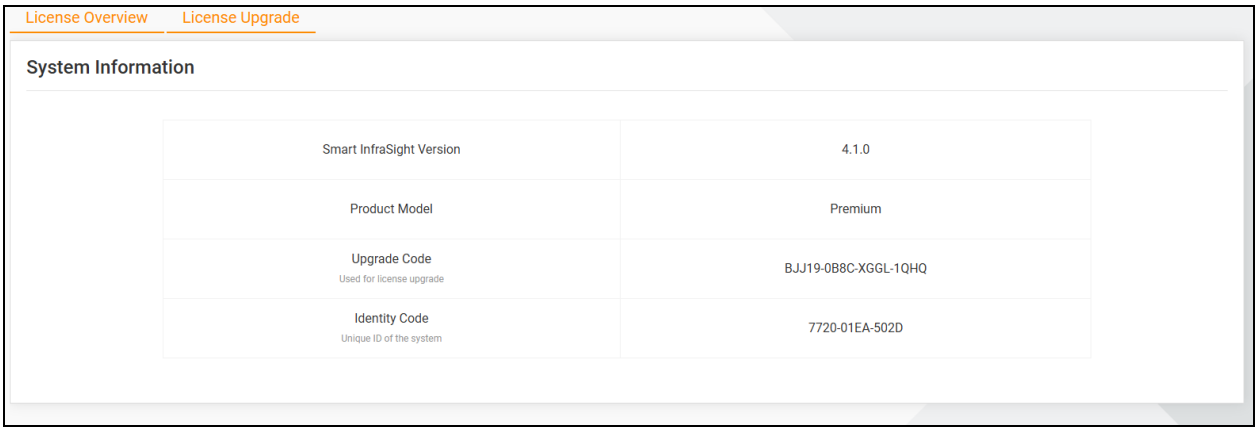
Figure 18.31 License Upgrade



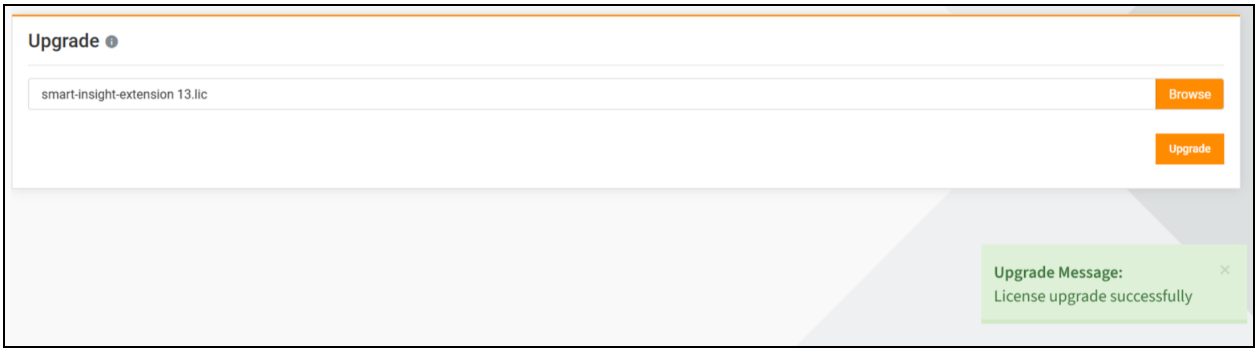
Upgrade Successful

When the license file is valid, the upgrade succeeds and a notification appears in the lower-right corner with the message: License upgrade successfully. After a successful upgrade, the Maximum Number is updated accordingly.

Figure 18.32 Upgrade successful



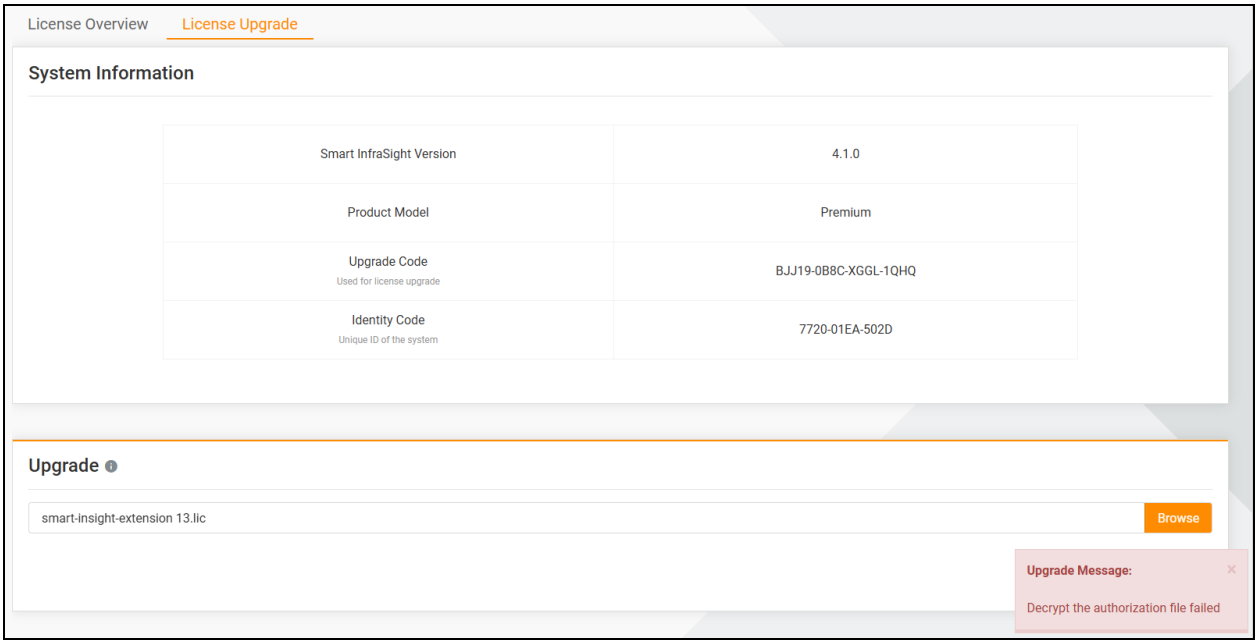
© 2026 Vertiv Group Corp. All Rights Reserved.



Upgrade Failed

When the license file is invalid, the upgrade fails and a notification appears in the lower-right corner indicating the upgrade failure. Contact Vertiv technical support promptly.

Figure 18.33 Upgrade failed



18.2.8 Backup and Upgrade

Backup and Restore provides three main functions: backup, restore, and system upgrade. This feature provides a fundamental safeguard for platform data and offers an interface for system upgrades, facilitating the delivery of new features and bug fixes.

Backup And Restore performs local backup operations. The target of local backup and restore is the server on which Smart InfraSight is installed. This means backing up files to the Smart InfraSight server and restoring the database using backup files stored on that server.

Backup uses a full backup method — each backup captures all data across all databases. Restore uses a full overwrite method, writing the contents of the restore file into the database and clearing all existing data. Restore carries inherent risk. Back up the original data before performing a restore to prevent data loss in the event of an error during the restore process.

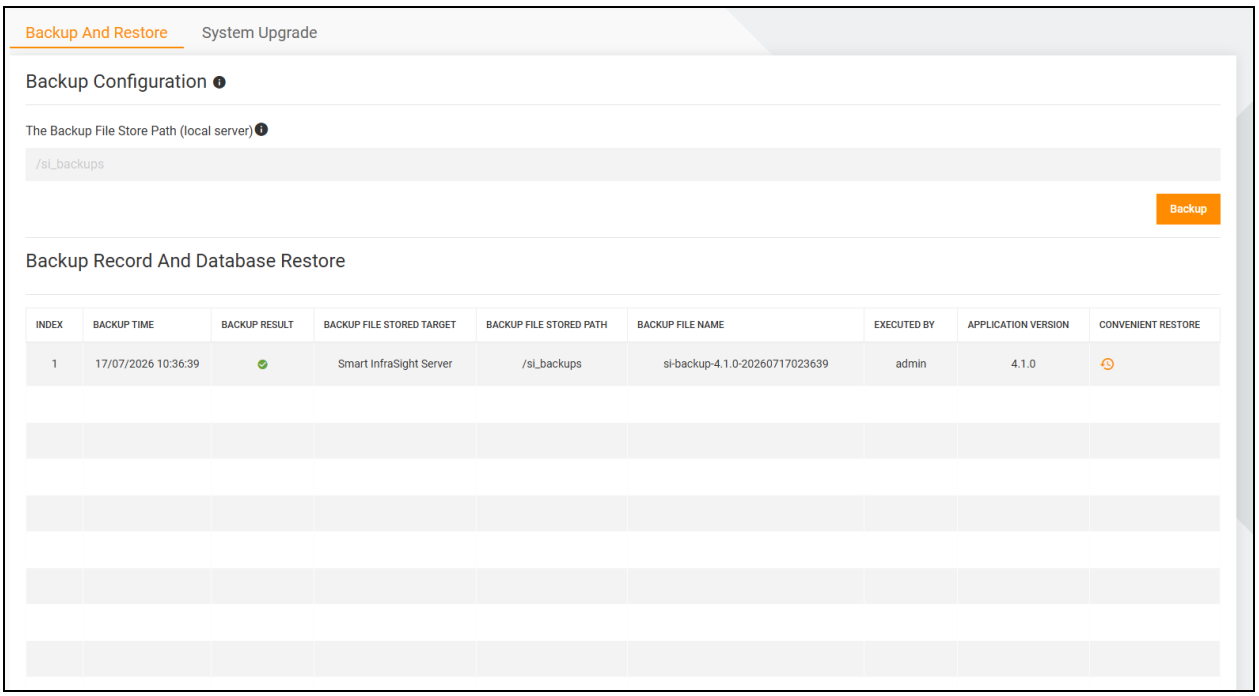
System Upgrade provides an interface for upgrading the platform by uploading an upgrade package.

© 2026 Vertiv Group Corp. All Rights Reserved.

Backup And Restore

In System Settings, go to Backup And Upgrade, then click on *Backup And Restore*. As shown in **Figure 18.34** below .

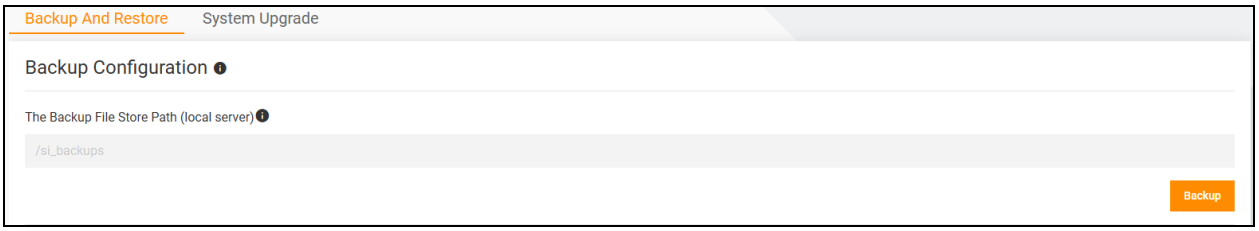
Figure 18.34 Backup and Upgrade



Backup

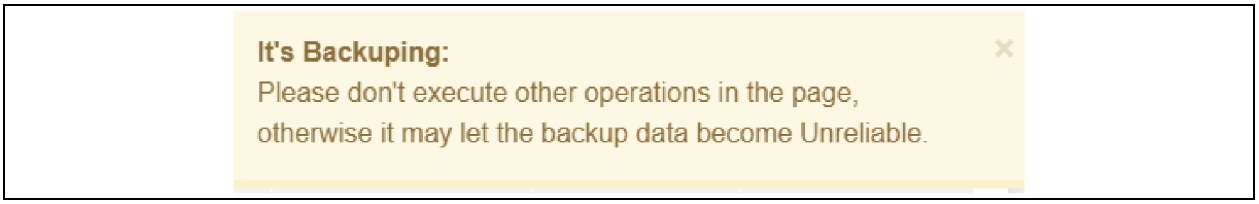
Back up to the server on which Smart InfraSight is installed, as shown in **Figure 18.35** below .

Figure 18.35 Backup



The platform automatically configures a default path. Click ***Backup*** to perform a backup. The backup file is automatically saved to the /var/lib/docker/volumes/si_backups directory on the Smart InfraSight server, as shown in **Figure 18.36** below .

Figure 18.36 Backup Execution Prompt



© 2026 Vertiv Group Corp. All Rights Reserved.

NOTE:

1. During a backup operation, do not perform any other configuration operations, as this may affect data accuracy and reliability. Keep the platform running throughout the process.

2. If you need to perform remote backups, please refer to this document: SI Remote Backup and Restore Guide.pdf

Backup Record And Database Restore

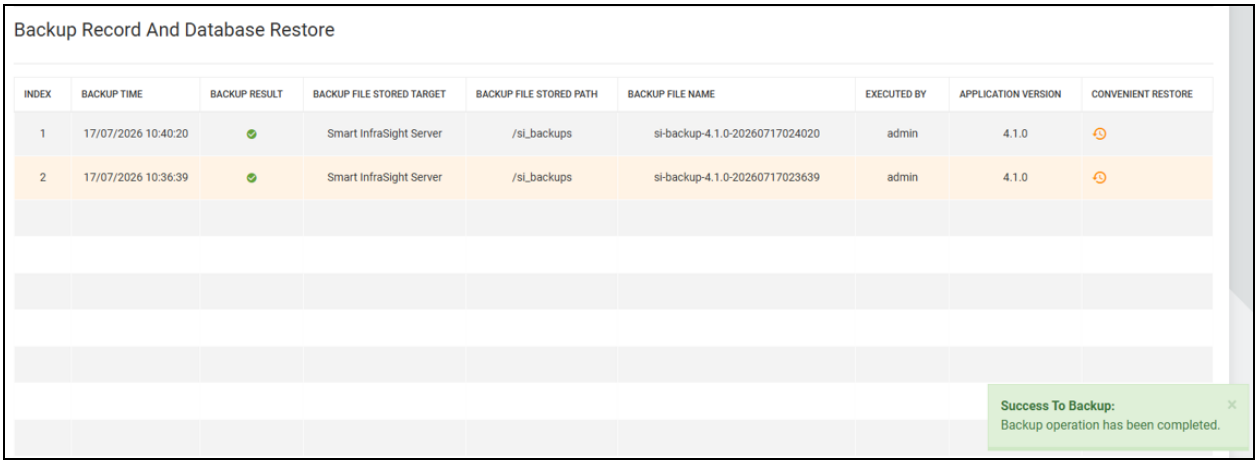
Backup in progress, as shown in Figure 18.37 below .

Figure 18.37 Back up Records



Backup successful, as shown in Figure 18.38 below .

Figure 18.38 Backup popup



Restore

In System Settings go to Backup And Upgrade, then Backup And Restore, then click on *Backup Record And Database Restore*.

NOTE:

1. A restore operation overwrites all local data and carries the risk of local data loss. Back up local data before performing a restore.

2. During a restore operation, do not perform any other configuration operations, as this may affect data accuracy and reliability. Keep the platform running and maintain network connectivity throughout the process.

3. Only the admin user can perform a restore operation.

4. If a remote restore is needed, please refer to the SI Remote Backup and Restore Guide.pdf.

© 2026 Vertiv Group Corp. All Rights Reserved.

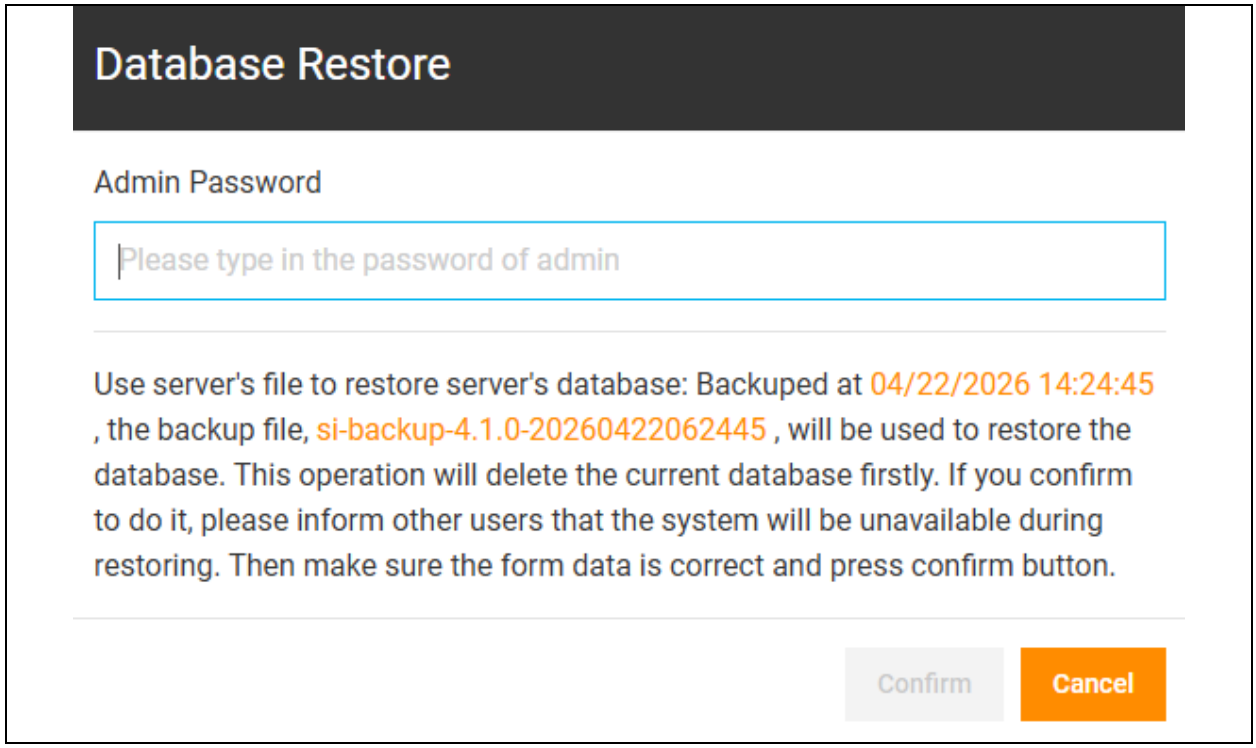
Convenient Restore — Local Restore

1. Click the *restore* icon the **Convenient Restore** column.

INDEX	BACKUP TIME	BACKUP RESULT	BACKUP FILE STORED TARGET	BACKUP FILE STORED PATH	BACKUP FILE NAME	EXECUTED BY	APPLICATION VERSION	CONVENIENT RESTORE
1	04/22/2026 14:24:45	✓	Smart InfraSight Server	/si_backups	si-backup-4.1.0-20260422062445	admin	4.1.0	↺

2. Enter the admin user password, then click *Confirm Restore*.

Figure 18.39 Entering the Administrator Password



System Upgrade

This feature enables users to easily and efficiently upgrade the system on the web interface by loading upgrade file.

Application Scenarios:

Minor Version Upgrade: Access the latest functional optimizations and user experience enhancements.

Bug Fixes: Resolve system software faults or defects identified during daily operations.

Security Patching: Patch known security vulnerabilities to enhance the overall security and defense capabilities of the system.

NOTE: Upgrade file must be provided by system maintenance or technical support personnel.

© 2026 Vertiv Group Corp. All Rights Reserved.

System Upgrade

In System Settings go to Backup and Upgrade, then System Upgrade, as shown in **Figure 18.40** below .

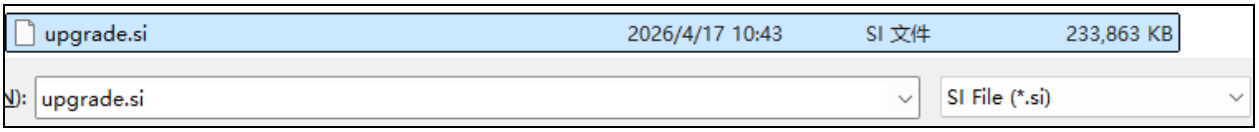
NOTE: Performing an upgrade stops all services and makes the page unavailable. Wait for the platform upgrade to complete before performing any further operations.

Figure 18.40 System Upgrade



1. Click *Browse*, select the upgrade file as shown in **Figure 18.41** below , The upgrade file must have a .si extension.

Figure 18.41 Selecting the Upgrade file



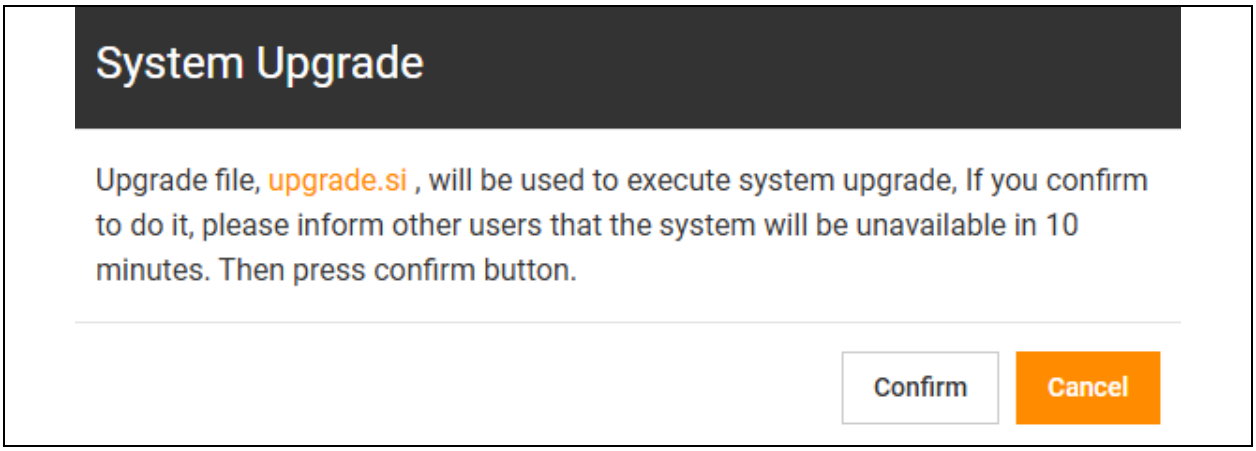
2. Click the on the *Upgrade* icon to upgrade.

Figure 18.42 Start upgrade



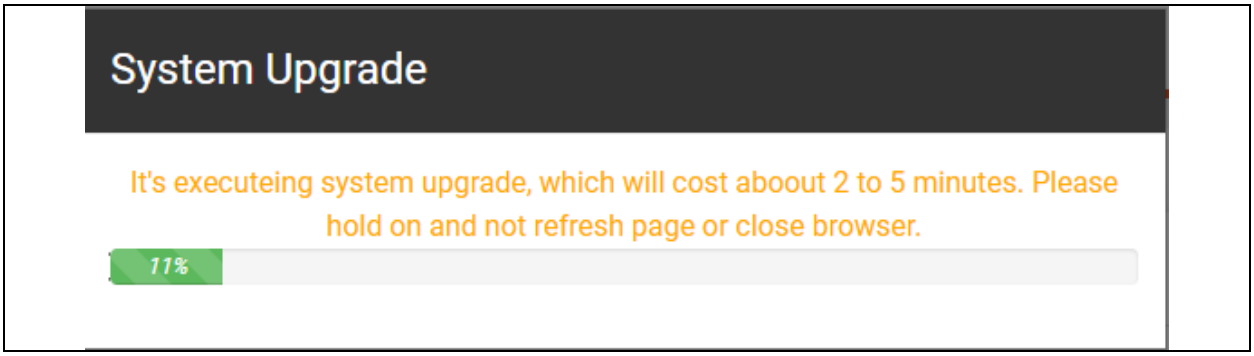
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.43 Upgrade prompt



3. The platform begins the upgrade process. Wait for it to complete.

Figure 18.44 Waiting for Platform Upgrade



18.2.9 Audit Logs

The Audit Log page records all user operations performed within the platform, enabling administrators to conduct compliance reviews and trace operational history. In the left navigation pane, go to **System Management > Audit Log** to open the Audit Log page.

Log records are displayed in a table with the following four columns:

Timestamp: The exact date and time when the operation occurred, in MM/DD/YYYY HH:mm:ss format. Records are sorted from newest to oldest by default. Click the Timestamp column header to toggle the sort order.

Operation Category: The business category to which the operation belongs, such as User Authentication, Firmware Upgrade, Service Management, and System Configuration.

Operator: The username of the user who performed the operation. For operations triggered automatically by the platform, this field displays **system**.

Description: A detailed description of the operation. The content varies depending on the operation category.

By default, the page displays all log records from the past 24 hours. To narrow the query scope, use the filter options at the top of the page:

© 2026 Vertiv Group Corp. All Rights Reserved.

1. In the **Time Range** drop-down list, select a target time period. Available options include: Last 24 Hours, Last 72 Hours, Last Week, Last 30 Days, and Custom. Selecting Custom opens a dialog box where you can set the start and end times. If the query returns more than 10,000 records, the platform displays a warning prompt.

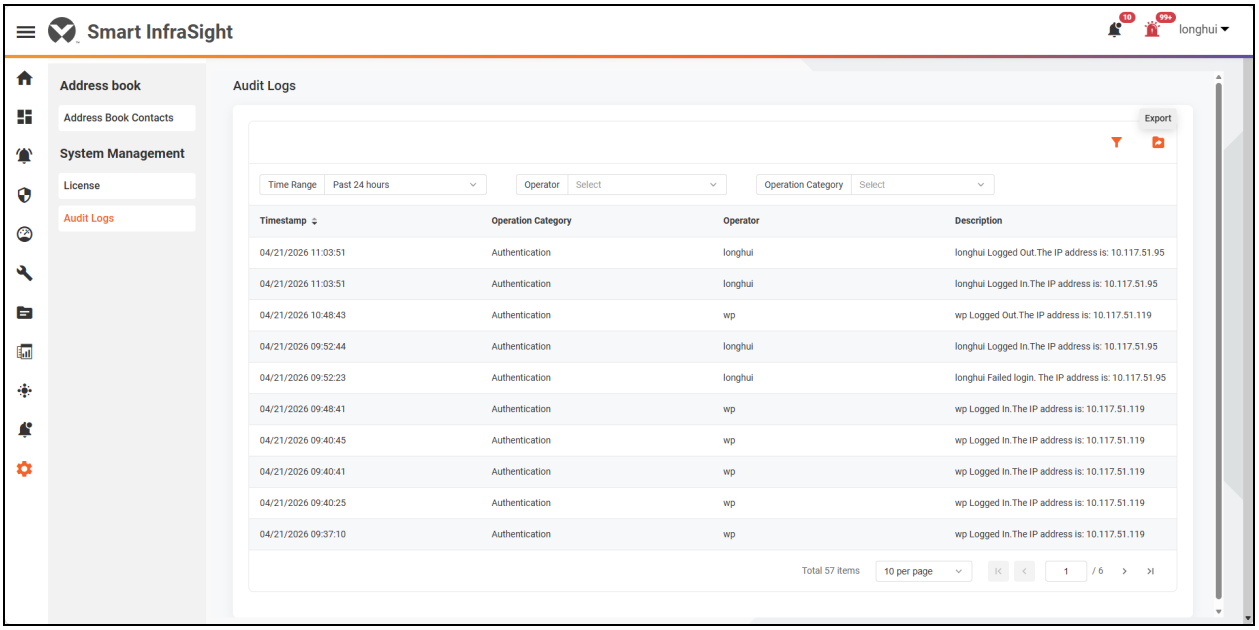
2. In the **Operator** drop-down list, select one or more target users. Multiple selections are supported. The default value is all users.

3. In the **Operation Category** drop-down list, select a target operation category. The default value is all categories.

Filter conditions can be used in combination. The page refreshes automatically upon configuration and displays the matching log records.

To export the current log data, click *Export* in the upper-right corner of the page. The platform exports the records that match the current filter conditions.

Figure 18.45 Audit Logs - Export



© 2026 Vertiv Group Corp. All Rights Reserved.

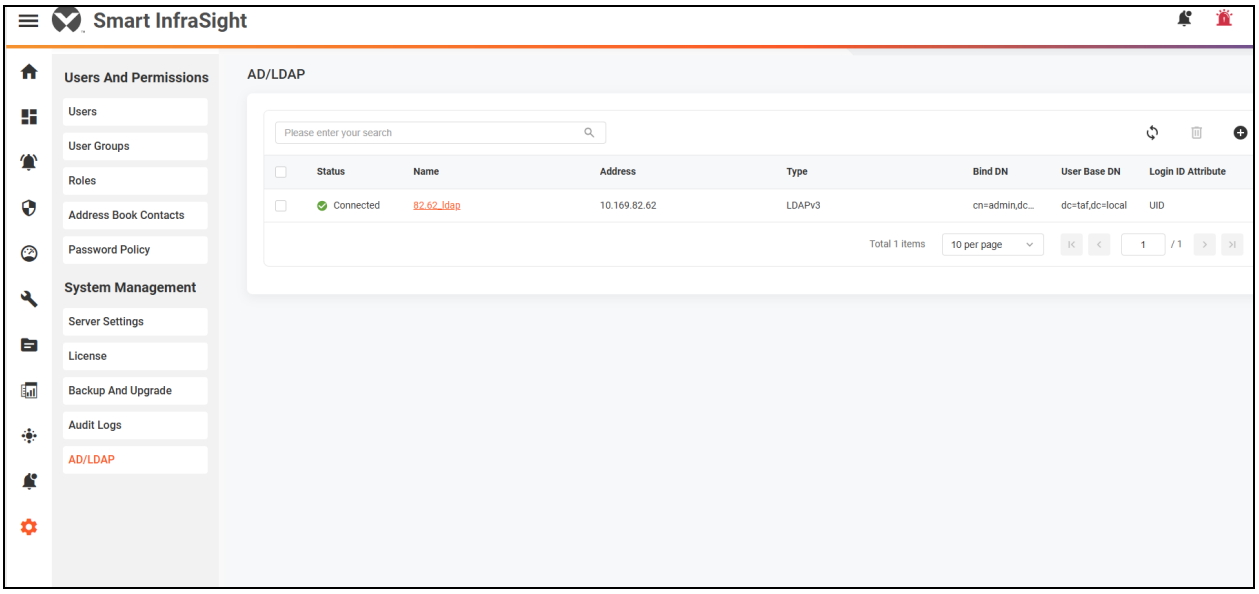
18.2.10 AD/LDAP

Configure AD/LDAP Connections

In System Settings, go to AD/LDAP.

After entering the page, you can view a list of all configured AD/LDAP connections and the current communication status of each connection with the server (Connected / Loading / Disconnected).

Figure 18.46 AD/LDAP

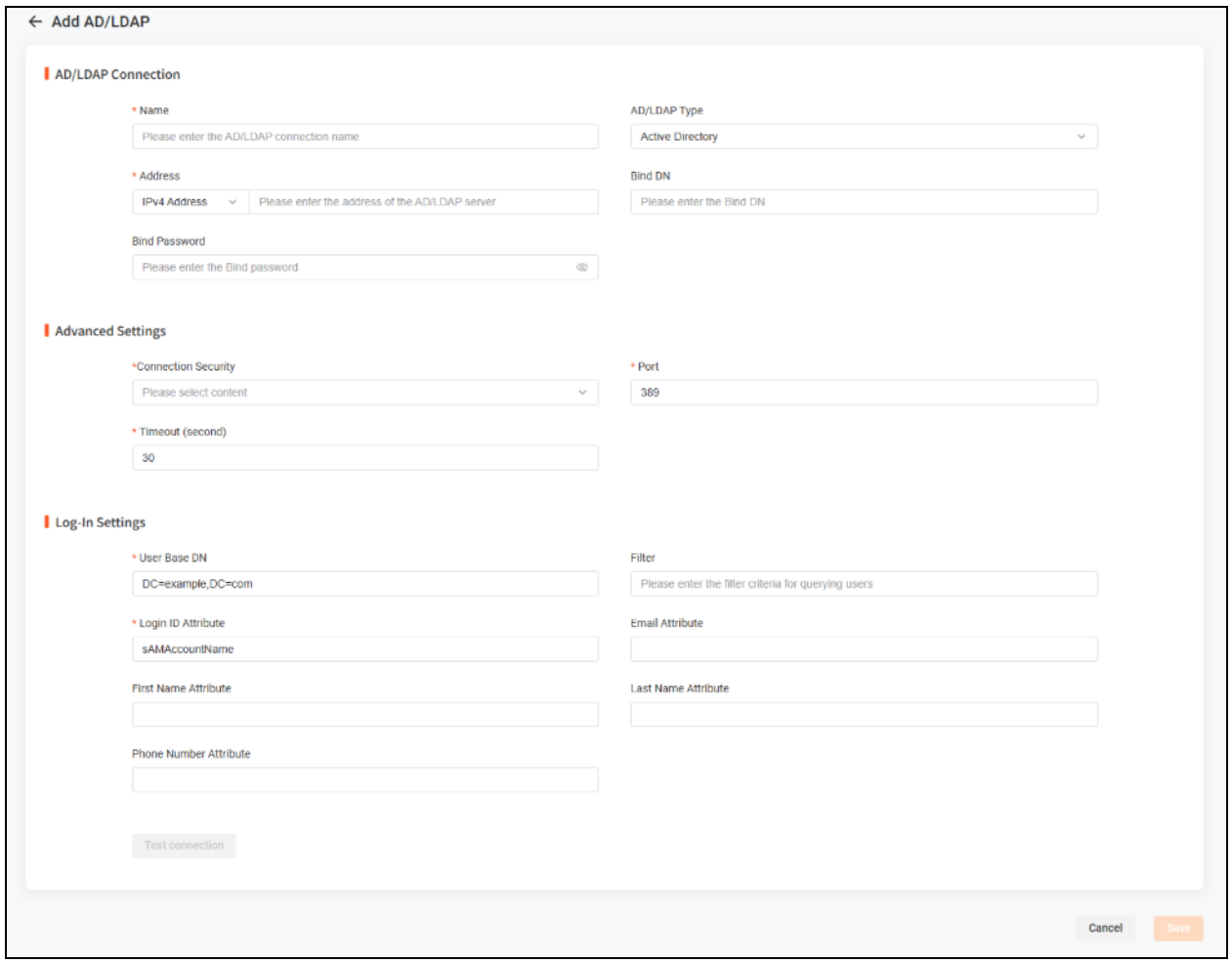


© 2026 Vertiv Group Corp. All Rights Reserved.

Adding a Connection

Click *Add* on the page to enter the new connection page, then complete the configuration by following the steps below.

Figure 18.47 AD/LDAP - Add a Connection



Step 1: Enter Basic Information

Name: Enter a unique, easily identifiable name for the connection, for example, **HQ AD**.

AD/LDAP Type: Select **Active Directory** or **LDAPv3** based on your organization's environment.

Address: Select the address type (**IPv4** or **Domain Name**) and enter the server address, for example, 192.168.1.1 or ldap.example.com.

Bind DN and Bind Password: Enter the administrator account credentials used to query the AD/LDAP server, for example, CN=Admin,OU=users,DC=example,DC=com. This account is used for searching users, adding users, and testing the connection.

Step 2: Configure Connection Security (Advanced Settings)

Under **Connection Security**, select an encryption method:

© 2026 Vertiv Group Corp. All Rights Reserved.

None (Plaintext LDAP): Data is transmitted without encryption. This option poses a security risk and is not recommended for production environments.

StartTLS or SSL (LDAPS): When enabled, upload the AD/LDAP server certificate file (supported formats: .pem, .crt, .cer, and other common formats).

Also enter the **Port** (default: 389 for LDAP, 636 for SSL) and **Timeout** (default: 30 seconds).

Step 3: Configure User Query Scope

User Base DN: Specify the root directory for querying users in AD/LDAP, for example, DC=example,DC=com. The platform searches for users within this directory.

Filter (Optional): Use a filter to narrow the query scope, for example, to query only users in a specific department. Example: (&(objectclass=user)(memberof=cn=admins,dc=mycompany)).

Login ID Attribute: Specify which AD/LDAP field is used as the user's login username. The default is sAMAccountName for Active Directory, and uid for LDAPv3.

Other Attributes (Optional): Configure additional attribute fields such as email, phone number, and display name. When importing users, the platform automatically retrieves and populates these fields from AD/LDAP into the user profile.

Step 4: Test and Save

After completing the configuration, click *Test connection*. The platform attempts to connect to the server and verify that the configuration is correct.

After a successful test, the Save button becomes active. Click *Save* to complete the configuration and return to the connection list.

If the test fails, the platform displays the specific reason, such as server unreachable, Bind DN authentication failure, User Base DN query failure, or invalid certificate file. Check the corresponding configuration items based on the error message.

Edit a Connection

Click a *connection name* in the connection list to enter the edit page. Note the following when editing:

The Bind Password is not displayed. If no change is required, leave the field blank and the platform retains the existing password.

If the certificate file is not re-uploaded, the existing certificate is retained. Uploading a new file replaces the existing certificate.

Delete a Connection

Select one or more connections in the list and click *Delete*.

NOTE: If the selected connection has associated users, it cannot be deleted. Go to the user management page and delete all associated users before deleting the AD/LDAP connection.

Refresh Connection Status

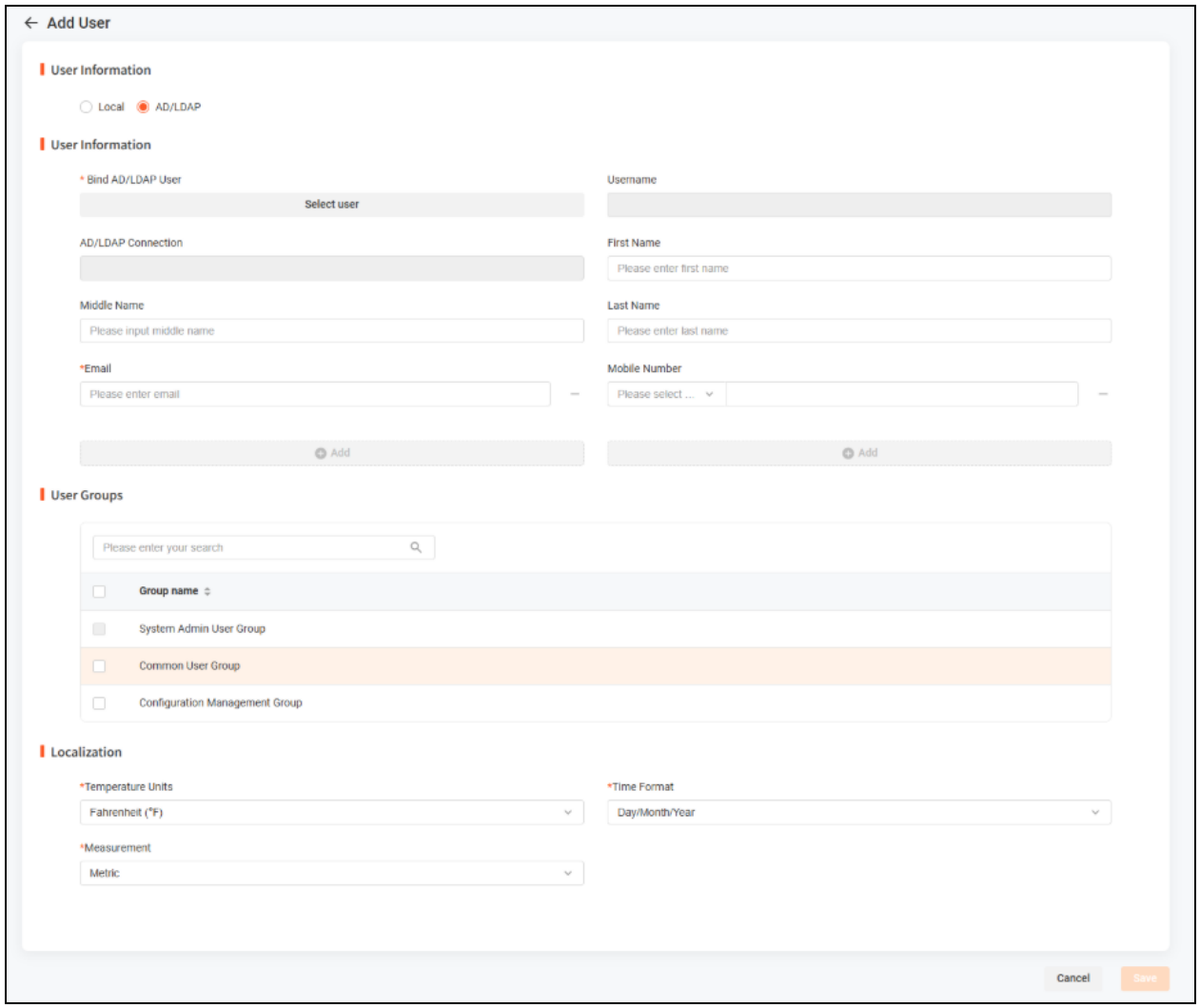
Click *Refresh* on the list page to manually refresh the communication status of all connections with the AD/LDAP server.

Add AD/LDAP Users

In Users & Permissions go to Users, then click on *Add*.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.48 AD/LDAP - Add Users



On the new user page, set the user type to AD/LDAP, then follow the steps below.

Step 1: Associate an AD/LDAP User

Click *Select User* to open the user selection dialog box:

Select the **AD/LDAP** connection to search from in the drop-down list.

Enter the user's name in the search box (exact match). The search results display the user's name and email address.

Select the target user and click *Apply* to complete the association.

Step 2: Confirm and Supplement User Information

After associating the user, the platform automatically retrieves and populates the following information from AD/LDAP:

Username: Automatically populated based on the Login ID Attribute. This field is read-only and serves as the user's login account.

© 2026 Vertiv Group Corp. All Rights Reserved.

AD/LDAP Connection: Automatically displays the name of the connection from which the user originates. This field is read-only.

Email, Phone Number, Display Name, etc. Automatically populated based on the attribute fields configured in the connection. Administrators can modify these fields manually as needed.

NOTE: The middle name is not retrieved automatically from AD/LDAP. Enter it manually if required.

Step 3: Assign a User Group and Save

In the User Group section, assign the user to a user group (required). Click *Save* to create the user and return to the user list.

User Login

After the AD/LDAP user configuration is complete, users can log in directly on the SI login page using their enterprise account credentials. No additional steps are required.

Login failure descriptions:

If the username or password is incorrect, the platform displays the message: Incorrect username or password.

If login fails multiple consecutive times, the account is temporarily locked. The platform displays the message: Too many failed login attempts. Please try again later. Wait for a period of time before attempting to log in again.

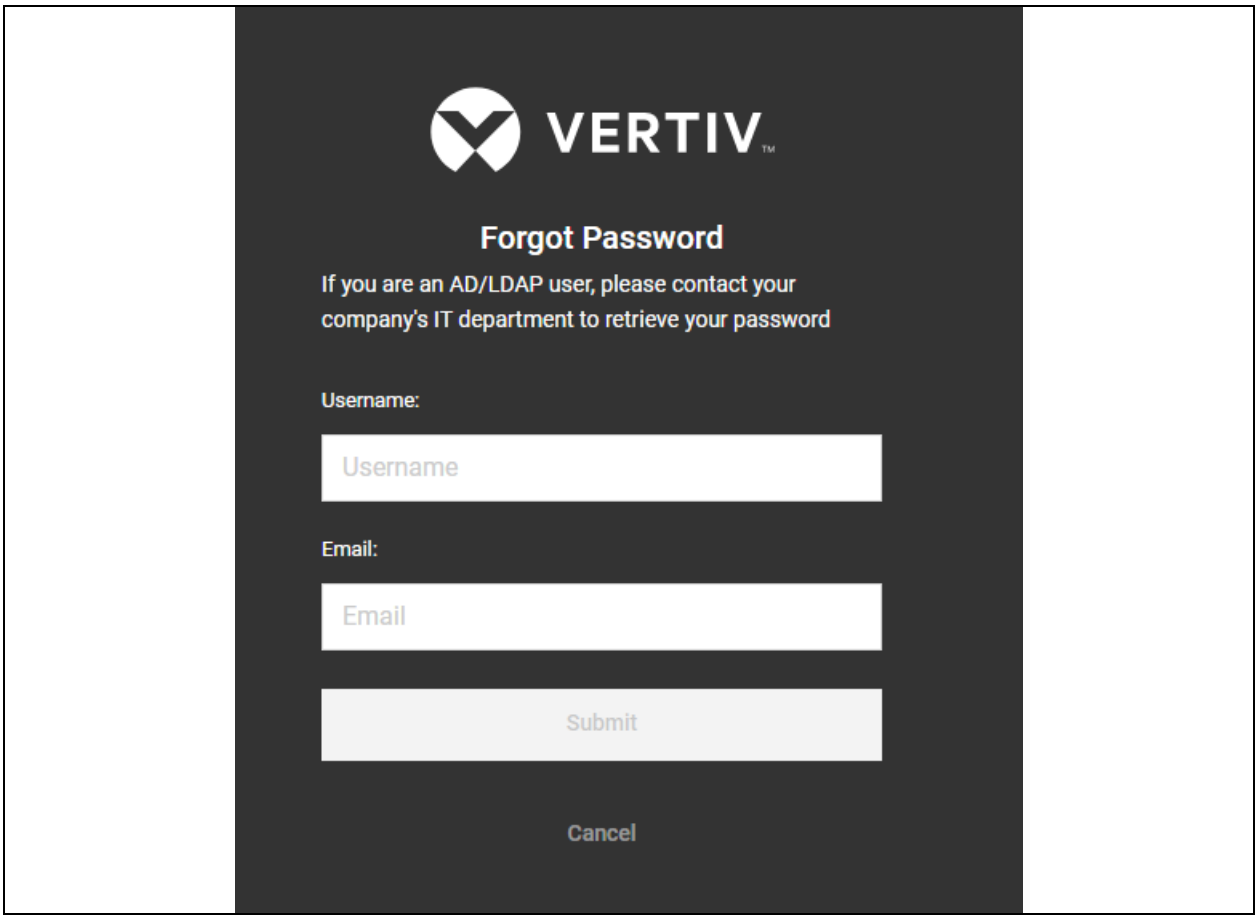
Password-related notes:

AD/LDAP user passwords are managed by the enterprise AD/LDAP server. To change or recover a password, contact your IT department. The SI platform does not support password changes through the platform for AD/LDAP users. The related options (Change Password, Reset Password) are not available for AD/LDAP users.

On the Forgot Password page, AD/LDAP users can refer to the on-page instructions to contact the IT department for assistance.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.49 AD/LDAP - User Login



Handling Expired Bind DN Credentials

The Bind DN account is used for administrator operations (searching users, adding users, and testing connections) and is unrelated to regular user login. Even if the Bind DN password expires, existing AD/LDAP users can still log in to the SI platform normally.

If the Bind DN password expires, administrators receive a prompt when performing operations such as adding users. To resolve this, go to the edit page of the corresponding AD/LDAP connection, update the Bind Password, and click *Save* to restore normal functionality.

18.2.11 Data Retention

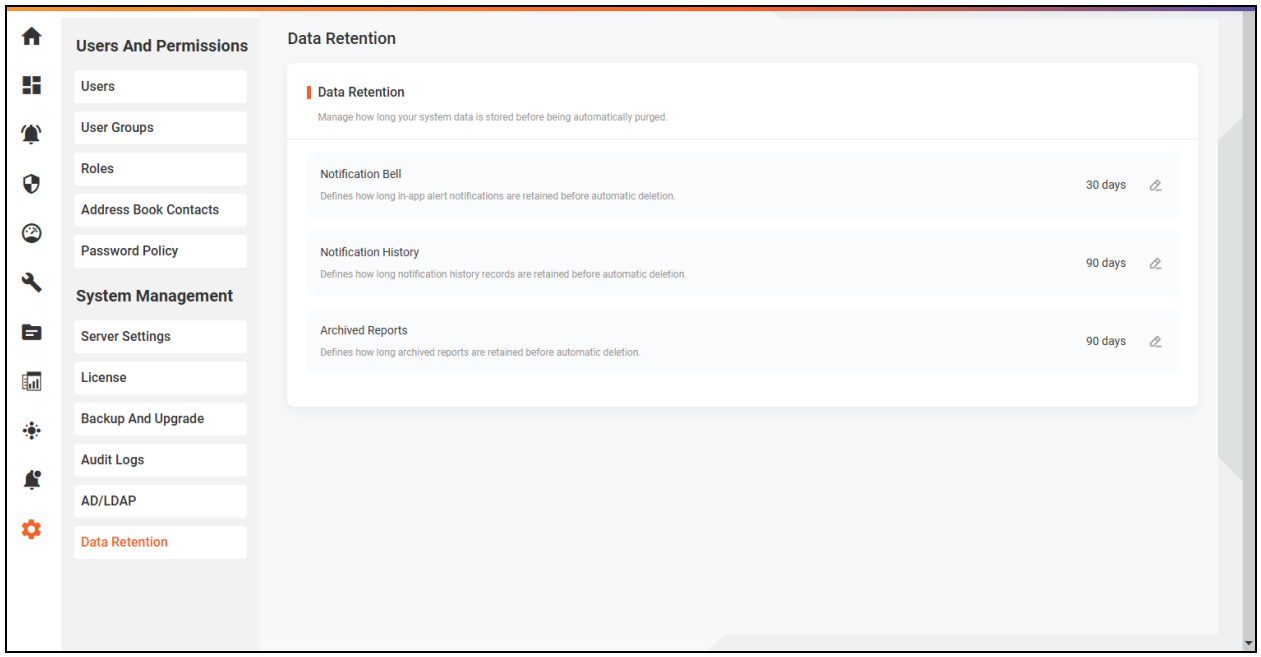
Configure Data Retention Policies

Entry: System Management -> Data Retention

After you open this page, you can view and manage how long three types of system data are stored. This feature controls how long system data is kept; data that exceeds the configured retention period is automatically removed by the system.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.50 Data Retention



The system supports retention policies for the following three data types:

Data Type	Description	Default Retention Period
System Notifications	Defines how long in-app alarm notifications are kept before they are automatically deleted.	30 days
Notification History	Defines how long notification history records are kept before they are automatically deleted.	90 days
Archived Reports	Defines how long archived reports are kept before they are automatically deleted.	90 days

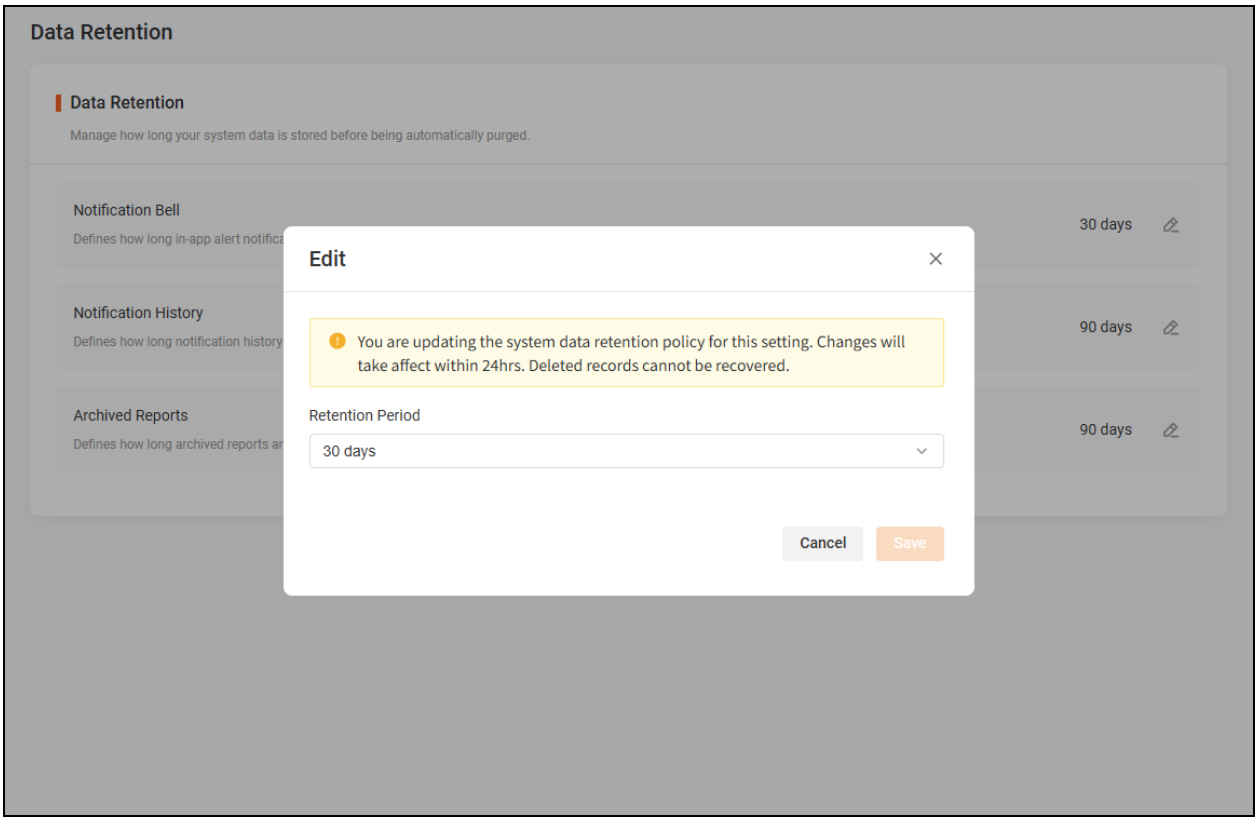
NOTE: The values above are the system's initial defaults. If an administrator has already changed a policy, the page shows the currently effective retention period, which may differ from the default.

Modify Data Retention Policies

In the data retention list, click the *Edit* icon to the right of the target data type. The Edit dialog opens.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.51 Editing the Data Retention Policy



A yellow notice appears at the top of the dialog:

You are updating the system data retention policy for this setting. Changes will take effect within 24 hours, and deleted records cannot be recovered.

Set the retention period as needed, then click *Save* to apply your changes. To discard changes, click *Cancel* or the close button in the upper-right corner of the dialog.

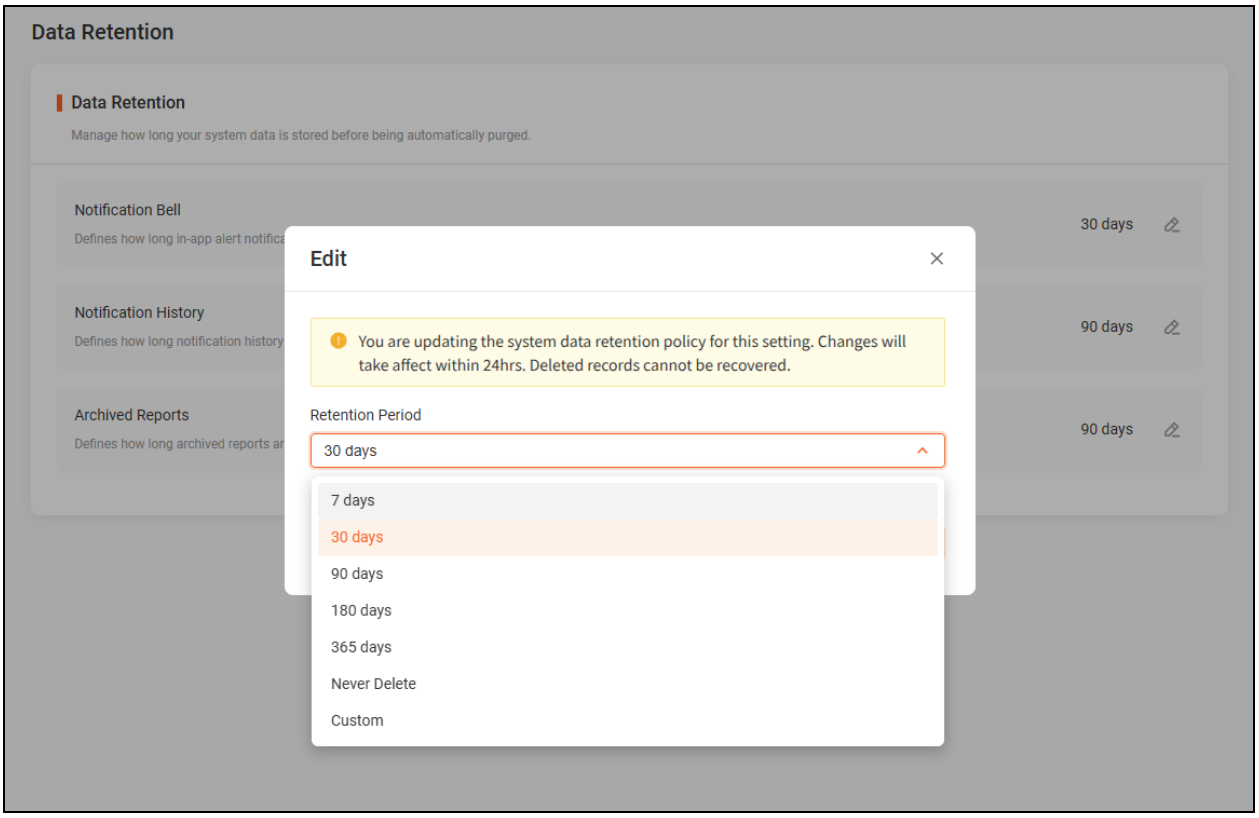
Step 1: Select a Retention Period

In the Retention Period drop-down list, choose a suitable duration. Available options include:

- 7 days
- 30 days
- 90 days
- 180 days
- 365 days
- **Never Delete:** The system will not automatically remove this type of data.
- **Custom**: The administrator specifies a retention period between 1 and 1825 days.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.52 Retention Policy Options



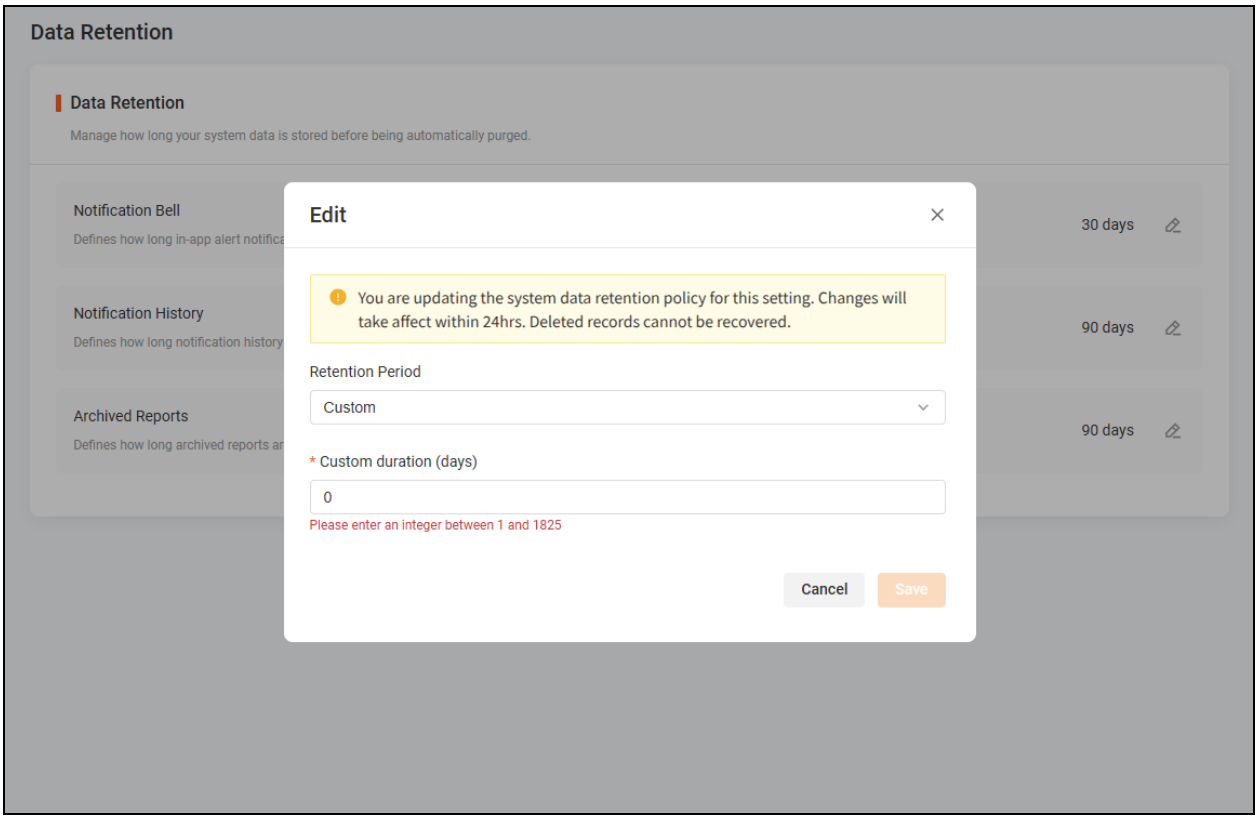
Step 2: Enter a Custom Duration (only when Custom is selected)

When **Retention Period** is set to **Custom**, you must enter **Custom Duration (Days)**:

- Enter an integer between 1 and 1825 (up to approximately 5 years).
- If the value is invalid (for example, 0 or out of range), the field shows: **Please enter an integer between 1 and 1825,** and *Save* remains unavailable until a valid value is entered.

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 18.53 Custom Retention Period



Step 3: Save and Apply

After you confirm the retention period, click *Save* to complete the configuration.

- After a successful save, the list updates to show the new retention period for that data type.
- Policy changes are applied by the system's background cleanup task **within 24 hours**. Until then, data may still be cleaned up under the previous policy.
- Once data is automatically deleted because it exceeded the retention period, it **cannot be recovered**. Set retention periods according to your compliance and operational requirements.

NOTE:

Retention policies for the three data types (System Notifications, Notification History, and Archived Reports) are independent. Each must be edited and saved separately.

If you shorten a retention period, the system may delete records outside the new retention window after the policy takes effect. Proceed with caution.

If you select Never Delete, that data type is retained indefinitely and may continue to consume storage space. Consider disk capacity and operational policy before using this option.

© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

19 Frequently Asked Questions

19.1 Browsers Supported by Smart InfraSight™

Table 19.1 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	

19.2 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.

19.3 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.

19.4 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.

19.5 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

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.

19.6 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.

19.7 Engineering Considerations when Connecting Smart InfraSight™ to the RDU

The Vertiv™ 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 19.2 Normalized Equipment Scope

Normalized Equipment Scope: 2019-04-23					
Device type	TAF type	Model	The name of the RDU driver		
			SmartAisle(Smart Aisle 2 , Smart Aisle 3)	SmartRow2	SmartCabinet2
Temperature and humidity are transmitted Sensors	SENSOR_ ENVIRONMENT	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]]★	-
air conditioning	COOLING	CRV+	ENP_AC_CRV+[COM☆]	ENP_AC_SRVII [COM★]]	ENP_AC_SMC [COM]
		CRV	ENP_AC_CRV[COM]		
		PEX+	Not supported		
		DME		ENP_AC_DME3000 [COM]	
UPS	UPS	APM150	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]	

© 2026 Vertiv Group Corp. All Rights Reserved.

Table 19.2 Normalized Equipment Scope (continued)

Normalized Equipment Scope: 2019-04-23					
Device type	TAF type	Model	The name of the RDU driver		
			SmartAisle(Smart Aisle 2 , Smart Aisle 3)	SmartRow2	SmartCabinet2
UPS	UPS	ITA		ENP_UPS_ITA16_20K [COM]	
					ENP_UPS_ITA1_3K [COM]
				ENP_UPS_ITA30_40K [COM]]★	
		eXL	Not supported		
		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		Not supported	
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™.

19.8 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:

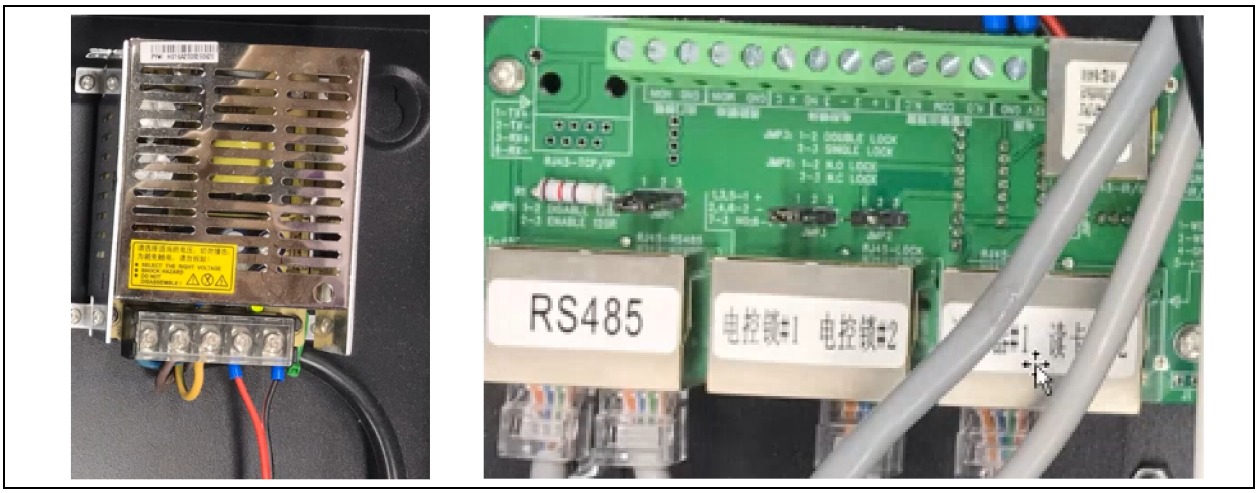
1. Diagram of the Configuration Process and Device

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 19.1 on the next page .

 © 2026 Vertiv Group Corp. All Rights Reserved.

Figure 19.1 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 the 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

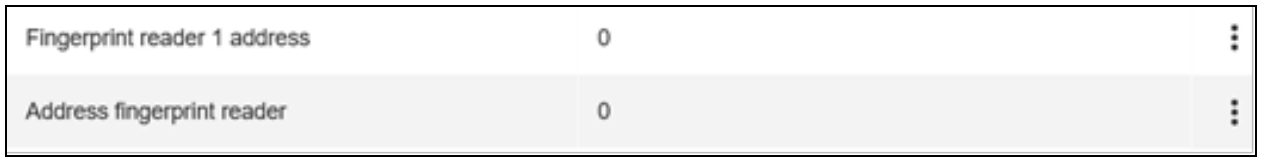
1. Select ES5200 (example) under Security, Access Control, Device List.

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 **Figure 19.2** on the facing page .

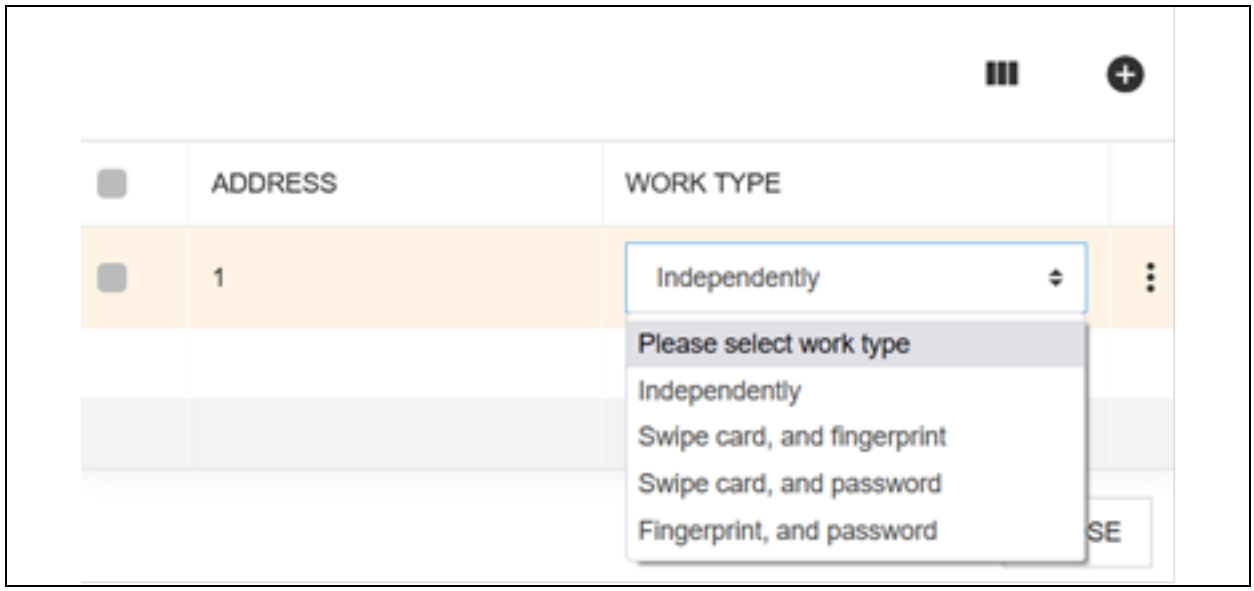
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 19.2 Setting the Address of the Card Reader



3. The working mode of the fingerprint reader can also be set as shown in the Figure 19.3 below .

Figure 19.3 Setting the Working Mode of the Card Reader



19.9 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.

19.10 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

19.11 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.

19.12 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.

19.13 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.

19.14 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.

19.15 Error Message - Alarm Push 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.

19.16 SI IP Change Causes Firmware Upgrade Unavailability for resolution

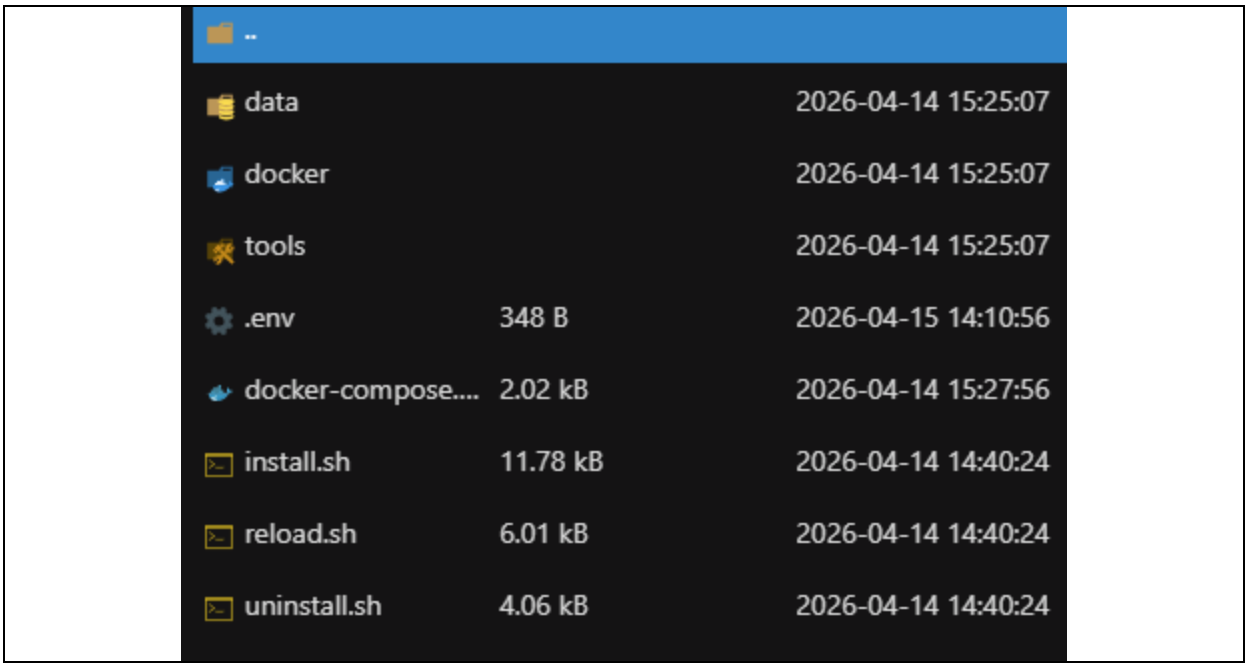
Issue: After SI is installed, changing the IP address of the SI server will cause the firmware upgrade feature to become unavailable.

Solution: Follow the steps below to resolve the issue.

1. Log in to the SI server, navigate to the /opt/trellissmartinfrasight/_installation/fm directory, and locate the reload.sh script.

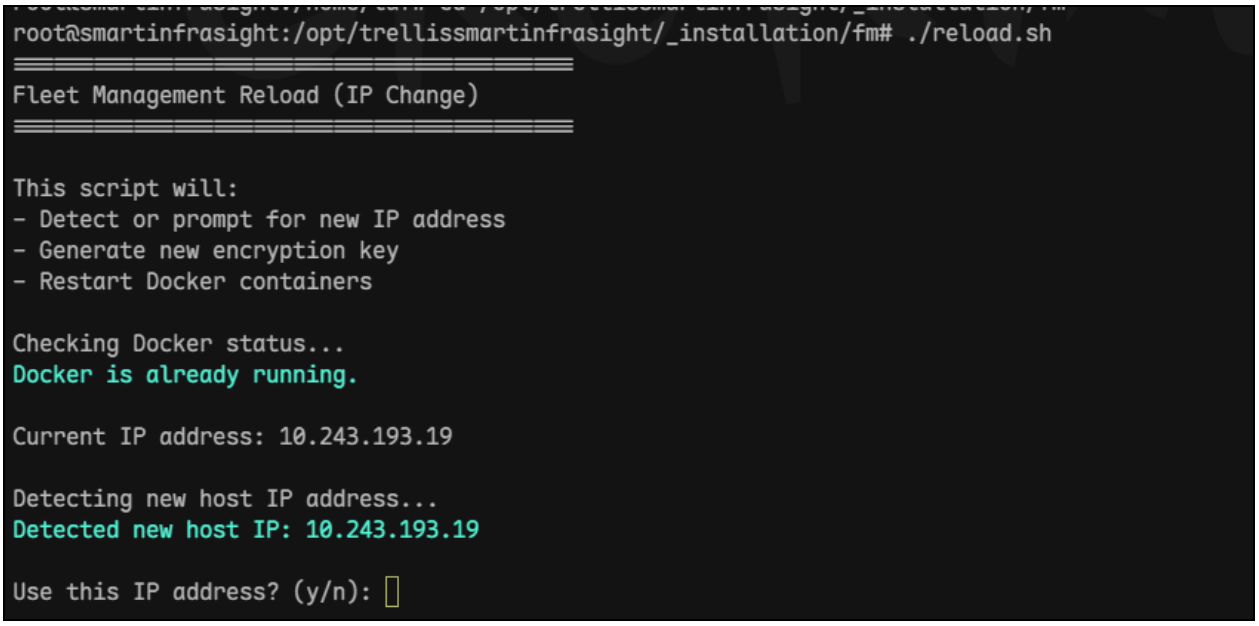
© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 19.4 Log into SI Server



2. Execute reload.sh.

Figure 19.5 Run reload.sh

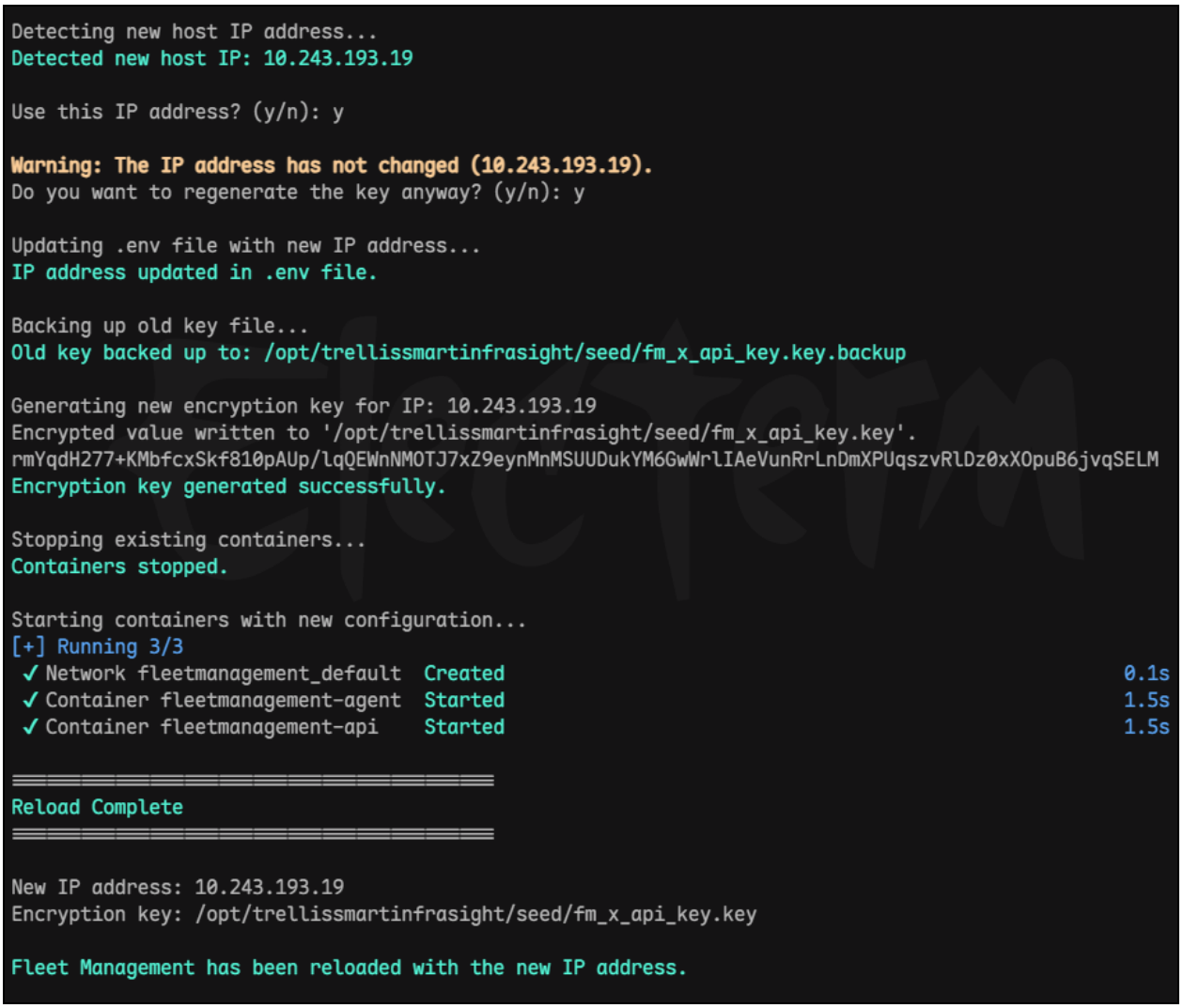


3. Confirm the IP address.

If the IP address automatically detected by the script matches the actual IP address of the SI server, enter y to confirm at each prompt. Once completed, the firmware upgrade can be performed again, as shown in the Figure 19.6 on the next page .

© 2026 Vertiv Group Corp. All Rights Reserved.

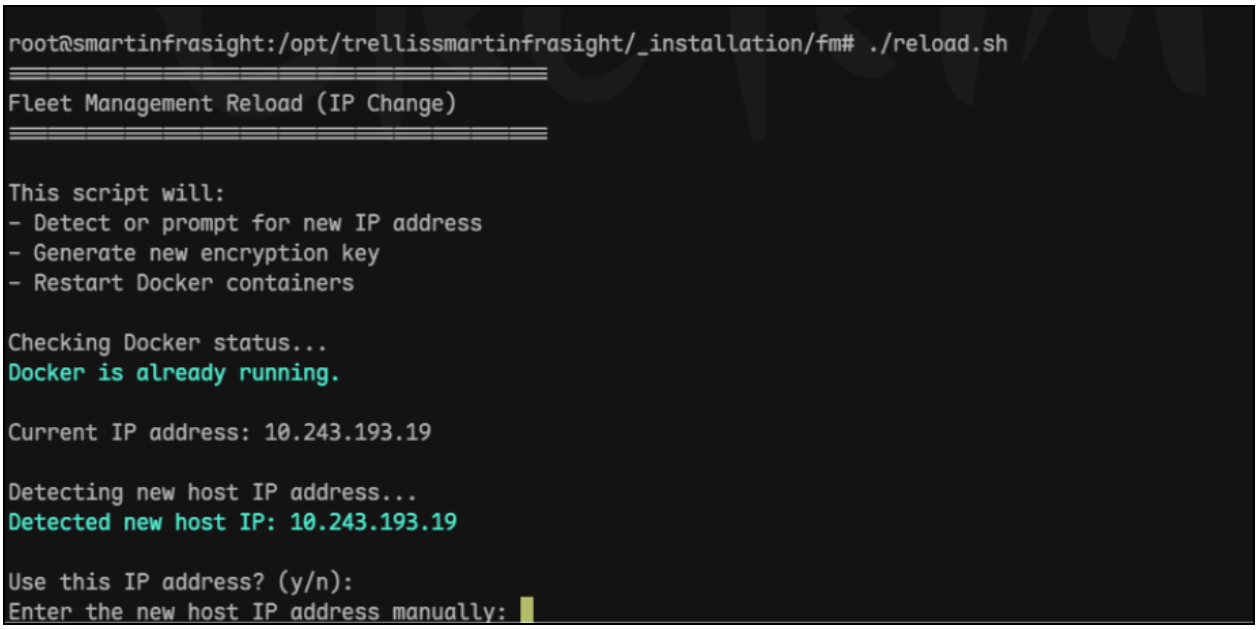
Figure 19.6 IP Address Confirmation



If the IP address automatically detected by the script does not match the actual IP address of the SI server, enter n, then manually enter the actual IP address of the SI server, as shown in the Figure 19.7 on the facing page .

© 2026 Vertiv Group Corp. All Rights Reserved.

Figure 19.7 IP Address Correction



19.17 Failed to Set IP Door Access Wait Time

Issue: When running on Windows WSL, setting parameters such as the door open wait time on IP access control devices fails. Basic operations (e.g., adding devices, viewing status) work normally.

Solution:

Run the following commands to set the Docker bridge MTU to 1400:

```
BRIDGE="br-$(docker network inspect ferret-network -f '{{.Id}}' | cut -c1-12)"
sudo ip link set "$BRIDGE" mtu 1400
```

NOTE: This change is temporary and will be lost after Docker restarts. For a persistent fix, add "mtu": 1400 to /etc/docker/daemon.json, then run sudo systemctl restart docker and restart the services.

© 2026 Vertiv Group Corp. All Rights Reserved.

This page intentionally left blank

© 2026 Vertiv Group Corp. All Rights Reserved.

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/

Vertiv.com | Vertiv Headquarters, 505 N Cleveland Ave, Westerville, OH 43082 USA

©2026 Vertiv Group Corp. All rights reserved. Vertiv™ and the Vertiv logo are trademarks or registered trademarks of Vertiv Group Corp. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions.

AV-50012_REVB_09-26