EDCM

V600R022C00

User Manual

Date **2022-02-25**

Contents

1 Getting Started

This section describes how to use the NetEco.

1.1 Logging In to or Logging Out of the NetEco

This section describes the operating environment requirements of the NetEco client and provides guidance for users to log in to or log out of the NetEco client.

1.1.1 Operating Environment Requirements

To ensure that users can browse and perform operations on the NetEco client, the PC must meet certain requirements.

Table 1-1 lists the requirements for the operating environment.

Table 1-1 Operating environment requirements

Configuration Item	Basic Configuration Requirement
CPU	I5-7500 or later

Configuration Item	Basic Configuration Requirement
Memory	8 GB
Operating system	Windows 10 Professional 64-bit

Configuration Item	Basic Configuration Requirement
Browser	You are advised to use the Chrome browser (stable channel edition) or Firefox browser (ESR edition) of the latest version. • If the user accesses the NetEco server through a proxy server, configure the proxy server as follows: For Chrome: 1. Click  in the upper right corner of the browser and choose **Settings**. 2. On the **Settings** page, click **Advanced**, and then click **Open proxy settings** under **System**. 3. In the **Internet Properties** dialog box, click **LAN settings**. In the **Proxy server** dialog box, select **Use a proxy server for your LAN**, set **Address** and **Port**, and click **OK**. 4. Close the **Settings** tab page. For Firefox: 1. Click  in the upper right corner of the browser and choose **Options**. 2. On the **Options** page, click **Advanced**, and then click **Settings** under **Network**. 3. In the displayed **Connection Settings** dialog box, select **Manual proxy configuration**, set **HTTP proxy** and **Port**, and click **OK**. 4. Close the **Options** tab page. **NOTE** To ensure that the proxy server can access the NetEco server, the network bandwidth must meet the following requirements: Uplink (from the browser to the NetEco server) data rate: ≥ 100 kbit/s; downlink (from the NetEco server to the browser) data rate: ≥ 100 Mbit/s • To set exceptions for pop-up windows of the browser, perform the following steps: For Chrome: 1. Click  in the upper right corner of the browser and choose **Settings**. 2. On the **Settings** page, click **Privacy and security** under **Advanced**, and click **Pop-ups and redirects** under **Site settings** in sequence. 3. In the **Pop-ups and redirects** dialog box, click **Add**. 4. In the **Add a site** dialog box, enter **https://server IP address:server port number (https://10.10.10.1:31943 for example)**, and click **Add**. 5. Close the **Settings** tab page. For Firefox:

Configuration Item	Basic Configuration Requirement
	1. Click in the upper right corner of the browser and choose **Options**. 2. On the **Options** page, click **Content** and **Exceptions** under **Pop-ups** in sequence. 3. In the **Allowed Sites** dialog box, set **Address of website** to **https://server IP address:server port number (https://10.10.10.1:31943 for example)**, click **Allow**, and then click **Save Changes**. 4. Close the **Options** tab page.

1.1.2 Logging In to the NetEco (Through HUAWEI CLOUD)

Log in to the NetEco through HUAWEI CLOUD.

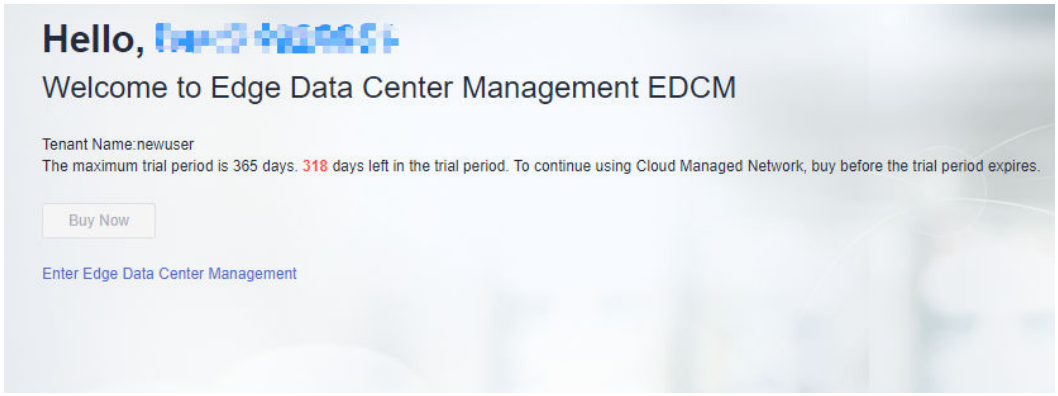
Prerequisites

- You have created a trial use order.
- The mobile number entered by the tenant has received the NetEco organization, password, and address.

Procedure

Step 1 Click **Enter Edge Data Center Managment** to enter the NetEco.

Figure 1-1 Entering the Enter Edge Data Center Managment page



Step 2 Enter **Organization**, **User Name**, and **Password**, and click **Log In**.

NOTE

- When you log in to the system for the first time, **Organization** is the same as **User Name** and is the tenant name entered during tenant creation, that is, the initial username of HUAWEI CLOUD. This user is the administrator of the tenant and has the highest operation rights. After the first login, you need to change the password to ensure access security.
- If the number of online users reaches the maximum number supported by the system, a message is displayed indicating that you cannot log in. In this case, contact the administrator.
- If you enter incorrect passwords for three consecutive times, a verification code is required at the fourth time. If you enter incorrect passwords for five consecutive times, the account or IP address will be locked for 10 minutes.

----End

1.1.3 Logging In to the NetEco (Through the WebUI)

Log in to the NetEco through the WebUI.

Prerequisites

- You have created a trial use order.
- The mobile number entered by the tenant has received the NetEco organization, password, and address.

Procedure

Step 1 In the address bar of a browser, enter **https://edcm2.hwocloud.com** and press **Enter**.

NOTE

- You are advised to use the Chrome browser (stable channel edition) or Firefox browser (ESR edition) of the latest version.
- You are advised to set the resolution of a PC screen to 1920 x 1080 or higher.
- When you log in to the NetEco for the first time, the web browser displays a certificate error. For details, see **6.1 How Do I Handle the Problem of Certificate Error or Security Alarm Displayed in the Web Browser**.

Step 2 Enter **Organization**, **User Name**, and **Password**, and click **Log In**.

NOTE

- When you log in to the system for the first time, **Organization** is the same as **User Name** and is the tenant name entered during tenant creation, that is, the initial username of HUAWEI CLOUD. This user is the administrator of the tenant and has the highest operation rights. After the first login, you need to change the password to ensure access security. If the number of online users reaches the maximum number supported by the system, a message is displayed indicating that you cannot log in. In this case, contact the administrator.
- If you enter incorrect passwords for three consecutive times, a verification code is required at the fourth time. If you enter incorrect passwords for five consecutive times, the account or IP address will be locked for 10 minutes.

----End

1.1.4 Logging Out of the NetEco

This section describes how to log out of the NetEco.

Prerequisites

You have logged in to the NetEco.

Procedure

Step 1 Move the cursor to the  icon in the upper right corner of the home page and click **Log Out**.

Step 2 In the displayed **Log Out** dialog box, click **Yes**.

The account is logged out, and the login page is displayed.

----End

1.2 Setting NetEco Communications Parameters on the ECC800-Pro

The ECC800-Pro can connect to the NetEco only after communications parameters are set on the ECC800-Pro WebUI.

Prerequisites

- You have obtained the IP address of the ECC800-Pro as well as the user name and password used for WebUI login.
- You have obtained the IP address of the NetEco server.

Procedure

Step 1 Enter **https://monitoring IP address** (such as **https://192.168.1.10**) in the address box of the browser, and then press **Enter** to enter the Web login page.

Step 2 On the login page, enter the user name and password, select a language, and click **Log In**.

NOTE

- If you do not perform any operation within 10 minutes after logging in to the system, you will be logged out due to timeout.
- A maximum of three users can log in to the ECC800-Pro WebUI at the same time.

Step 3 Choose **System Settings** > **NMS Application**.

Step 4 Click the **NetEco** tab. In the **Communication Parameters** area, set parameters such as **Server IP**, **Port number**, and **Network port for link setup**, and click **Submit**.

NOTE

The parameters to be set for the ECC800-Pro vary according to the software version. Set the parameters based on the actual version.

Table 1-2 NetEco parameters

Parameter Name	Value
Server IP	Set this parameter to the IP address of the NetEco server. **NOTE** The NetEco IP address and the ECC800-Pro IP address must be configured in the same network to ensure normal connection between the NetEco and the ECC800-Pro.
Port number	31220
Network port for link setup	WAN_1

----End

1.3 Connecting a Device (Through the App, Recommended)

You can use an app to connect a site to the NetEco for management. This method is recommended because it is more convenient.

1.3.1 Installing the NetEco App

This section describes the requirements for the NetEco app running environment and how to download and install the NetEco app.

App Running Environment Requirements

- Device: Only Android mobile phones are supported.
- Operating system: Android 8.0 or later. The system cannot be rooted. The system memory is 1 GB or above/larger.
- The device supports a web browser and can connect to the Internet at a rate of 500 kbit/s or higher.
- Enough space is available for installing new applications.
- The battery power is sufficient.

NOTE

The device supports display at mainstream resolutions, such as 1920 x 1080 and 2340 x 1080. To ensure the stability of each function, 1920 x 1080 is recommended. It is strongly recommended that Android mobile phones provided by global mainstream vendors, such as SAMSUNG and HUAWEI, be used.

Installing the App

NOTE

Currently, the NetEco app supports only the Android version.

- Obtaining the software installation package from the Huawei AppGallery and installing the app
  a. Go to **Huawei AppGallery** (website: **https://appgallery.huawei.com**) and search for NetEco.
  b. Tap **Download** to obtain the app installation package.
  c. Install the app as prompted.

     After the installation is complete, the NetEco app icon is displayed on the home screen of the mobile phone.
- Installing the NetEco app by scanning the QR Code

  On the NetEco screen, tap  in the upper left corner and use your mobile phone to scan the QR code in the lower right corner.

Figure 1-2 NetEco app QR code

1.3.2 (Optional) Replacing the App Certificate on a Mobile Device

This section describes how to replace the preset security certificate in the NetEco app on a mobile device. Preset Huawei certificates apply only to commissioning scenarios. For security purposes, apply for certificates from the certification authority (CA) and use them to replace the preset certificates. Using the same certificate for a long time increases the probability of being cracked. Replace the current certificate periodically.

Prerequisites

- The NetEco app has been installed.

- You have applied for a new certificate file **server.cer** from the CA.

  NOTE

  server indicates the name of the certificate file, which can be renamed.

Procedure

Step 1 Import the obtained digital certificate to the **cer** directory in the NetEco folder of the mobile client.

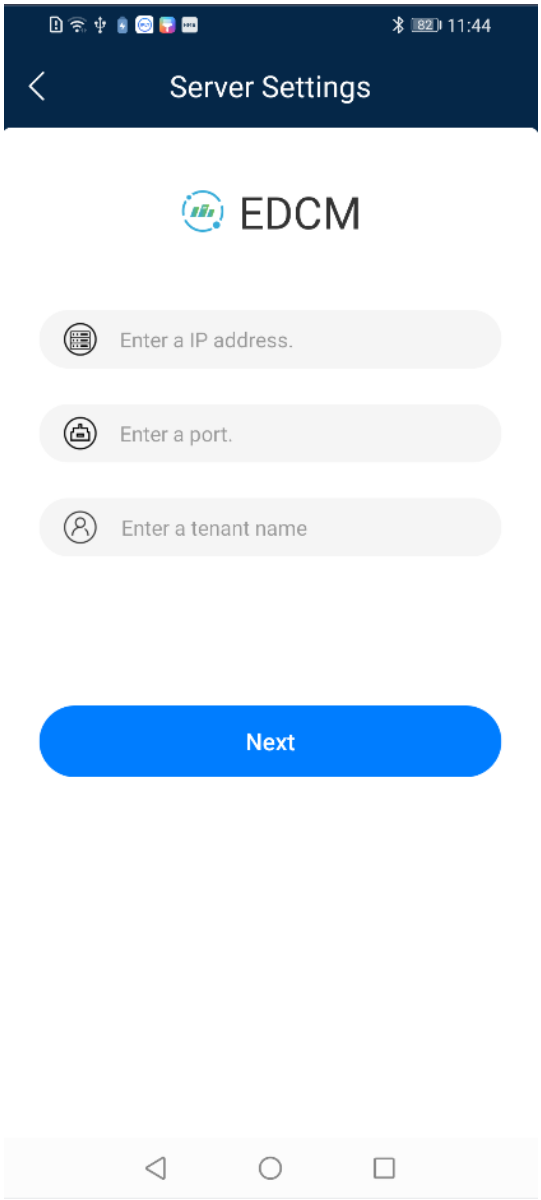
Step 2 At the first login, select **EDCM** in the **System Service** area on the **Select Application** screen.

Step 3 On the **Server Settings** screen, set server information such as the tenant name, login address, and port number, and tap **Next**.

NOTE

Tenant Name is the tenant name registered on HUAWEI CLOUD.

Figure 1-3 NetEco Server Settings



Step 4 On the **Login** screen, tap ••• in the upper right corner.

Step 5 In the lower part of the **Login** screen, tap **Replace Certificate**.

Step 6 On the **Select File** screen, select the new certificate and tap **ALLOW** in the displayed dialog box.

----End

1.3.3 Logging In to the NetEco App

After the app is correctly installed on the mobile device, you can log in to the NetEco server through the app.

Prerequisites

- The device has connected to a WiFi or mobile network.
- The NetEco app has been installed. For details, see **1.3.1 Installing the NetEco App**.
- You have obtained the tenant name, user name, and password for logging in to the NetEco app, and have changed the initial password.
- You have obtained the IP address and port number of the NetEco server.

Procedure

Step 1 On the mobile device, click the NetEco app icon.

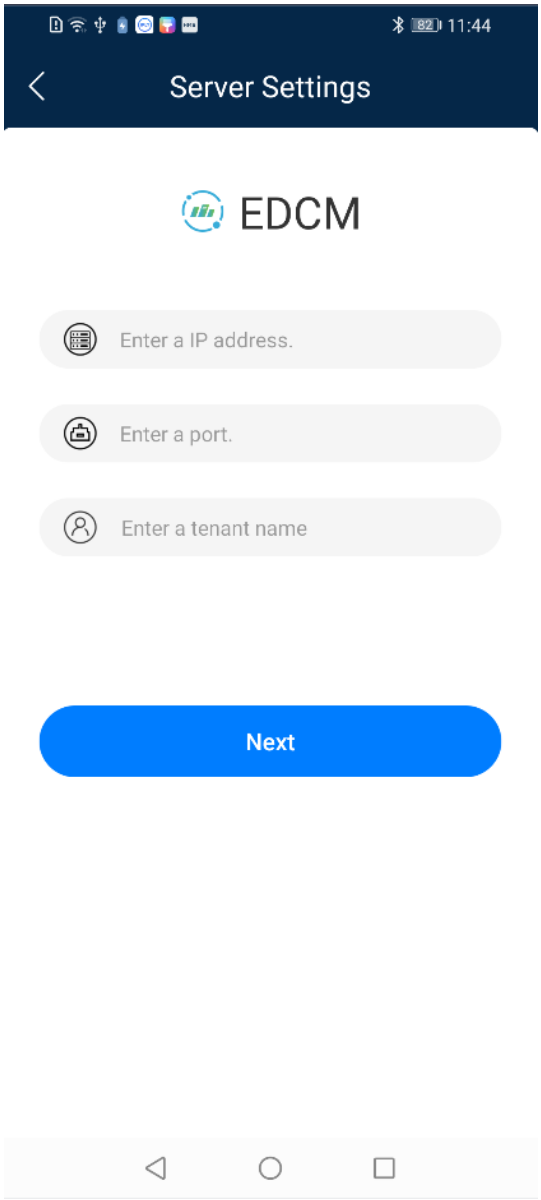
Step 2 At the first login, select **EDCM** in the **System Service** area on the **Select Application** screen.

Step 3 On the **Server Settings** screen, set server information such as the tenant name, login address, and port number, and tap **Next**.

NOTE

Tenant Name is the tenant name registered on HUAWEI CLOUD.

Figure 1-4 NetEco Server Settings



Step 4 On the **Login** screen, enter **User Name** and **Password**.

NOTE

- **User Name** is the tenant name registered on HUAWEI CLOUD.
- If you fail to log in to the system for three consecutive times, the system automatically displays **Verification Code**.

Step 5 Tap **Log In**.

After logging in to the NetEco app, enable or disable the **Push notifications** function as prompted. For details, see **6.6 How Do I Enable or Disable the Message Push Function**.

NOTE

During the operation, if no data is displayed on the screen or a message is displayed indicating that the network is abnormal, check whether the WiFi or mobile network connection of the mobile terminal is normal. If the network connection is normal, check whether the user is forcibly logged out on the NMS.

If a Huawei mobile phone is used, the **Push notifications** function is enabled by default in the NetEco app.

----End

1.3.4 Connecting to a Site

You can connect the site to the NetEco through the NetEco app.

Prerequisites

- You have logged in to the NetEco.
- NetEco communications parameters have been set on the ECC800-Pro.

Procedure

Step 1 On the NetEco app screen, tap  in the upper right corner.

Step 2 On the site creation screen, enter the DC information as prompted.

Figure 1-5 Creating a site

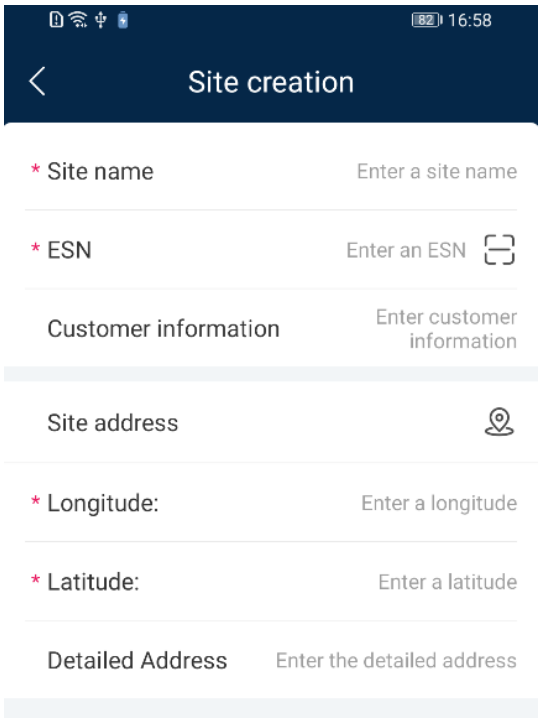


Table 1-3 Parameter description

Parameter	Description
Site name	Name of a site
ESN	ESN of the ECC controller **NOTE** Tap and scan the QR code on the ECC controller to obtain its ESN.
Customer information	Name of a customer
Site address	Address of a site
Longitude	Longitude of a site. You can manually enter the value or use the GPS to locate the site.
Latitude	Latitude of a site. You can manually enter the value or use the GPS to locate the site.
Detailed address	Detailed address of a site

Step 3 Tap **OK**.

----End

1.4 Connecting a Device (Through the WebUI)

You can use a WebUI to connect a site to the NetEco for management.

1.4.1 Adding a Management Domain

Before adding a device, you need to create a management domain based on the planned relationship between the management domain and the device.

Context

The NetEco presets management domains such as parks, equipment rooms, subnets, cabinets, buildings, and floors.

- If the managed device is FusionModule800 or FusionModule2000, the management domain to be added is **Modular**.
- If the managed device is FusionModule500, the management domain to be added is **FusionModule500**.
- If the managed device is the FusionDC1000A, the management domain to be added is **Container**.

Procedure

Step 1 Choose **Device Management** > **Configuration** > **Planning Configuration**.

Step 2 In the navigation tree, select the node to which you want to add a management domain.

Step 3 In the **Domain** area under the navigation tree, drag the management domain to be added to the configuration area.

Step 4 On the right of the **Planning Configuration** page, set **Management Info** of the management domain by referring to **1.4.3.1 Basic Parameters of a Management Domain**, and click in the upper right corner of the page.

NOTE

When creating a management domain, you need to enter **Location**, **Longitude**, and **Latitude** in the **Management Info** area. Otherwise, the specific location of the device cannot be displayed on the **View** page.

----End

1.4.2 Adding a Device Through Automatic Discovery

You can add the ECC800-Pro to the smart module, AIO container, and FusionModule500 management domain through automatic discovery.

Prerequisites

- A management domain has been created. For details, see **1.4.1 Adding a Management Domain**.
- You have obtained device parameters.
- The ECC800-Pro is properly connected.

Procedure

Step 1 Choose **Device Management** > **Configuration** > **Planning Configuration**.

Step 2 On the **Planning Configuration** page, click in the upper left corner.

Step 3 On the **Uncreated Device Information** page, click **Access** in the **Operation** column.

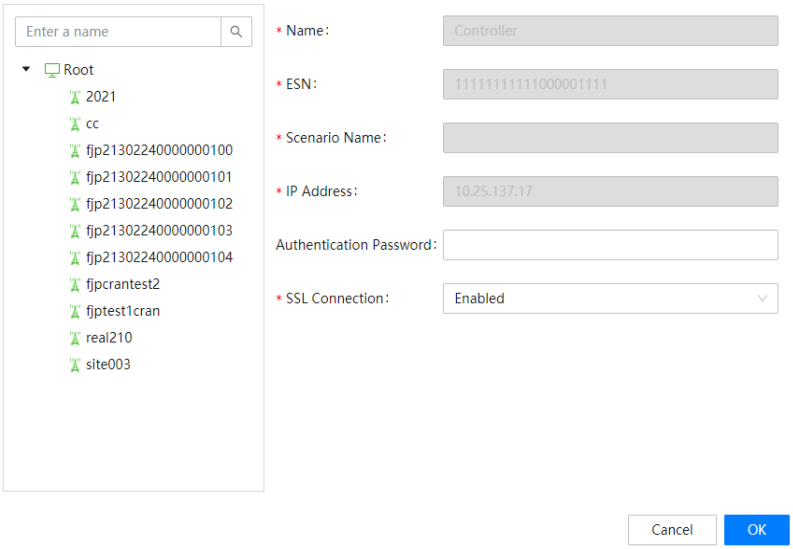
Step 4 In the **Device Integration** dialog box, set parameters for the ECC800-Pro device by referring to **Figure 1-6**, and click **OK**.

You can view the task information, including **Type**, **Device Name**, **Region**, **Progress**, **Status**, **Start Time**, **End Time**, and **Information** in the displayed **Progress** page. You can view the operation details in **Information**.

NOTE

- After the management domain is successfully bound to the ECC800-Pro, all devices under the ECC800-Pro will be displayed on the **Planning Configuration** page and their names can be manually modified. However, devices under the ECC800-Pro cannot be moved or deleted. You can only delete all devices under the ECC800-Pro by deleting the ECC800-Pro.
- The following lists the management domains that can be bound to different types of ECC800-Pro systems:
  - The ECC800-Pro whose system type is **FusionModule500** can be bound to a FusionModule500 management domain.
  - The ECC800-Pro whose system type is **FusionModule800**, **FusionModule2000**, or **FusionModule5000** can be bound to a smart module.
  - The ECC800-Pro whose system type is **FusionModule1000A** (the layout mode is available for the FusionModule1000A) can be bound to an AIO container.
- After in-room monitoring is set on the ECC800-Pro, the access actuators and cameras synchronized to the NetEco will be displayed in the smart modules (smart modules created in the equipment room, outlet, subnet, or container cluster) in the same positions as where they are deployed on the ECC800-Pro. After the access actuator and camera are deleted from the ECC800-Pro, the access actuators and cameras synchronized to the NetEco are displayed only in the list of devices that are not deployed in the smart module.

Figure 1-6 Adding the ECC800-Pro through automatic discovery



NOTE

- If you do not specify **Authenticate Password**, the site is created using the default password. If you correctly specify **Authenticate Password**, the site is created using the specified password.
- During ECC800-Pro device synchronization, all opened NetEco pages are locked. In this period, you cannot perform any operations on these pages, and **Loading device profile. Please try it later.** is displayed. The locking duration varies. Perform operations based on the actual operation result.
- After ECC800-Pro device synchronization, you can check or configure **Management Info**, **Assets Info**, device information, and layout information of the device in the corresponding smart module in the **Planning Configuration** page as required.
- When modifying the switch states of air conditioners that use the BIN4 protocol on the **Planning Configuration** page, you need to enter the password on the NetEco.

----End

Follow-up Procedure

After adding an ECC800-Pro device, you can perform operations on the device on the **Planning Configuration** page. The operations are as follows:

- Modifying device parameters

  Select the added device and configure parameters in the right pane as required. Click  in the upper right corner.

  NOTE

  Names of the devices accessed through the ECC800-Pro comply with the following rules:

  - For devices that are synchronized to the NetEco through the ECC800-Pro for the first time, if the names of the devices are not changed on the NetEco or ECC800-Pro WebUI, their default names are displayed.
  - Device names modification on the ECC800-Pro WebUI will be synchronized to the NetEco. However, device names modification on the NetEco will be synchronized to the ECC800-Pro WebUI.
- Deleting a device

  Click a device and click **Delete** under  to delete the device.
- Viewing the device view

  Click the device and choose **Manage** under  to go to the device **Overview** page and view the device view.

1.4.3 Planning Configuration Interface Reference

This section describes the parameters in the **Planning Configuration** page.

1.4.3.1 Basic Parameters of a Management Domain

This section describes the basic parameters to be set when you create a management domain on the NetEco client.

Configure parameters as required. The parameter marked with an asterisk (*) is mandatory.

Table 1-4 Park, building, container, subnet, and FusionModule500 parameter configuration

Parameter Name	Description	Setting Requirement
Parent Object	Upper-level management domain name	The system automatically identifies this name.
Type	Management domain type	The system automatically identifies this type.
Name	Management domain name	The value is a string of 1 to 128 characters.
Manufacturer	Manufacturer of the device	The value is a string of 0 to 64 characters. **NOTE** This parameter needs to be set when the domain is **FusionModule500**.
SN	Serial number of the created management domain	The value is a string of 0 to 128 characters.
Location	Physical location of the created management domain	The value is a string of 0 to 64 characters.
Plan Power (kW)	Total power for the created management domain	The value is a floating number ranging from 1 to 10,000,000 (three decimal places). **NOTE** This parameter needs to be set when the domain is **Park** or **Building**.
Description	Description of the created management domain	The value is a string of 0 to 512 characters.
Longitude	Longitude of the position where the created management domain is located	Value range: –180 to +180. A maximum of 10 decimal places are allowed.
Latitude	Latitude of the position where the created management domain is located	Value range: –90 to +90. A maximum of 10 decimal places are allowed.

Table 1-5 Parameters for the Room and Site

Parameter Name	Description	Setting Requirement
Parent Object	Upper-level management domain name	The system automatically identifies this name.
Type	Management domain type	The system automatically identifies this type.
Room Type	Equipment room type, including DG Plant, High Volt. Distribution Plant, Low Volt. Distribution Room, Power Transformer Plant, UPS & Battery Room, Service Room, and Cooling Plant.	Select the room type as required.
Design Type	Site design type. You can set this parameter to floor planning or background planning.	Select the site design type as required. **NOTE** This parameter needs to be set when the domain is **Site**.
Name	Management domain name	The value is a string of 1 to 128 characters.
Planned Rack Position	Planned number of cabinet places in the created management domain. The number of cabinets in the equipment room cannot exceed the planned number of cabinet places.	The value is an integer ranging from 1 to 2000. **NOTE** The value of **Planned Rack Position** can be modified after it is set. The number of cabinets cannot exceed its planned number. Therefore, you should set enough number of planned cabinets to meet requirements in cabinet creation.

Parameter Name	Description	Setting Requirement
Wire Laying	Cabling of the created management domain	Select **UpLine** or **Downline** from the down-down list box.
SN	Serial number of the created management domain	The value is a string of 0 to 128 characters.
Address	Address of the created management domain	The value is a string of 0 to 128 characters.
Department	Department of the created management domain	The value is a string of 0 to 128 characters.
City	Name of the city where the created management domain is located	The value is a string of 0 to 128 characters.
Country	Name of the country where the created management domain is located	The value is a string of 0 to 64 characters.
Level	Level of the created management domain	Select **Tier 1**, **Tier 2**, **Tier 3**, **Tier 4**, **A**, **B**, or **C** from the drop-down list box.
Description	Description of the created management domain	The value is a string of 0 to 512 characters.
Owner	Management personnel for the created management domain	The value is a string of 0 to 64 characters.

Parameter Name	Description	Setting Requirement
Longitude	Longitude of the position where the created management domain is located	Value range: –180 to +180. A maximum of 10 decimal places are allowed.
Latitude	Latitude of the position where the created management domain is located	Value range: –90 to +90. A maximum of 10 decimal places are allowed.
City Power Supply Mode	City power supply mode of the created management domain	Select **Dual power supply** or **Single power supply** from the drop-down list box.
Voltage Type (VAC)	Voltage system of the created management domain	Select **110V**, **220V**, or **380V** from the drop-down list.
UPS Working Mode	UPS working mode of the created management domain	Select **N**, **N+X(X=1~N)**, **2N**, or **2(N+1)** from the drop-down list box.
Has Generator	Whether a generator is installed in the created management domain	Select **Single Generator**, **Dual Generator**, or **NULL** from the drop-down list box.
Input Voltage	Input voltage of the created management domain	Select **6KV**, **10KV**, or **35KV** from the drop-down list box. **NOTE** This parameter needs to be set when the domain is **Site**.
Output Voltage	Output voltage of the created management domain	Select **110V**, **220V**, **380V**, or **400V** from the drop-down list box. **NOTE** This parameter needs to be set when the domain is **Site**.

Parameter Name	Description	Setting Requirement
Plan Power (kW)	Total power supply for the created management domain	The value is a floating number ranging from 1 to 10,000,000 (three decimal places).
Frequency	Mains power frequency of the created management domain	Select **50Hz** or **60Hz** from the drop-down list box.
Cooling Mode	Refrigerating mode of the created management domain	Select **Water Cooled Direct Expansion**, **Air Cooled Direct Expansion**, **Chilled-water refrigeration**, **Double-cold Source**, or **Free cooling** from the drop-down list.
Air-Distribution	Air supply mode of the equipment room	Select **Underfloor Air Distribution**, **Horizontal Air Distribution**, **Side displacement Air-distribution**, **Vertical Overhead Air Distribution**, **Horizontal overhead Air-distribution**, or **Fresh air convection** from the drop-down list box.
Plan Refrigerating Capacity (kW)	Cooling power of the created management domain	The value is a floating number ranging from 1 to 10,000,000 (three decimal places).

Table 1-6 Parameters for the Container management domain

Parameter	Description	Setting Requirement
Parent Object	Upper-level management domain name	The system automatically identifies this name.
Type	Type of the added container	The system automatically identifies this type.
Container Type	Type of the container you can add	Select **Device Container**, **Cooling Container**, **Generator Container**, **Power Container**, **NOC Container**, **AIO Container**, **Container Cluster**, or **Transformer**.
Name	Name of the container	The value is a string of 1 to 128 characters.

Parameter	Description	Setting Requirement
SN	SN of the added container	The value is a string of 0 to 128 characters.
Box Size	Size of the container	Select **20-Feet** or **40-Feet**.
Location	Physical location of the added container	The value is a string of 0 to 64 characters.
Description	Description of the added container	The value is a string of 0 to 512 characters.
Left Image, Right Image, Back Image	You can set **Left Image**, **Right Image**, and **Back Image** of a container.	**NOTE** The container on the view uses the default image. To manually change the background image of the container, contact the technical support to obtain the image. If the background image of the container is not set, **Not Uploaded** is displayed. After the background image of the container is uploaded, **Wait Save** is displayed. After you click  in the upper area of the current page, **Uploaded** is displayed. After the background image of the container is set, you can perform the following operations to check the setting in the **View** page. Method: Click  on the right of the position column. In the displayed **Upload Image** dialog box, click . Select the obtained image on the local PC and click **OK**. To delete the uploaded background image, click  , and then click **Clear** in the displayed **Upload Image** dialog box.
Count	You can select the number of containers to be combined.	You can combine two to twenty equipment containers. **NOTE** This parameter needs to be set when **Container Type** is **Container Cluster**.
Children Name	You can set the name of a container.	The value is a string of 1 to 30 characters. **NOTE** This parameter needs to be set when **Container Type** is **Container Cluster**.

Table 1-7 Parameters for the Modular management domain

Name	Description	Setting Requirement
Parent Object	Management domain name of the smart module	The system automatically identifies this name.
Type	Type of a smart module	The system automatically identifies this type.
Name	Name of the smart module.	The value is a string of 1 to 128 characters.
Manufacturer	Manufacturer of the device	The value is a string of 0 to 64 characters.
Direction	Direction of the device	The default value is **Horizontal**. Select **Horizontal** or **Vertical** from the drop-down list box.
Layout	Layout of the device	The default value is **single-row wide aisle1**. Select **single-row wide aisle1**, **single-row wide aisle2**, **dual-row wide aisle**, **single-row narrow aisle1**, **single-row narrow aisle2**, or **single-row dual aisle** from the drop-down list box.
Half-Size Cabinet	Number of half-sized cabinets in each row of the smart module	The default value is **11**. Number of half-sized cabinets in each row of the smart module. The value is an integer ranging from 4 to 50.
Location	Position of the smart module in the management domain	The value is a string of 0 to 64 characters.
Install Mode	Installation mode of the smart module	The default value is **Floor Installation**. Select **Floor Installation**, **Cabinet Installation**, **Wall Installation**, or **Ceiling Installation**.
Wire Type	Cabling mode of the smart module	The default value is **Ascending Line**. Select **Ascending Line**, **Down Line**, or **Floor Line**.
Airflow Type	Heat dissipation channel of the smart module.	The default value is **Vertical Under-Floor Air-Distribution**. Select **Vertical Under-Floor Air-Distribution**, **Horizontal Displacement Air-Distribution**, **Side Displacement Air-Distribution**, **Vertical Overhead Air-Distribution**, **Horizontal Overhead Air-Distribution**, or **Natural Convection Overhead Air-Distribution**.

Name	Description	Setting Requirement
Aisle Size	Width of the aisle in the smart module	The default value is **1200**. The value is an integer ranging from 0 to 65,535.
Height	Height of the smart module	The default value is **2300**. Select **2300**, **2500**, or **2800** from the drop-down list box.
Aisle Containment Type	Aisle containment type of a smart module	The default value is **Cold Aisle**. Select **Hot Aisle** or **Cold Aisle** from the drop-down list box.

1.4.3.2 Basic Device Parameters

This section describes the basic parameters that need to be set when you create a device on the NetEco client.

They include but are not limited to the following parameters. Configure parameters as required. The parameter marked with an asterisk (*) is mandatory.

Table 1-8 Description of device parameters

Attribute	Parameter	Description
Management Info	Parent Object	Name of the management domain to which the device belongs
	Type	Type of the device
	Name	Name of the device The value is a string of 1 to 128 characters.
	Med Node	Node ID used at the mediation layer
	Protocol Type	Protocol version for the device

Attribute	Parameter	Description
	IP Address	It must be an IPv4 address in the X.X.X.X format, where X is a number ranging from 0 to 255. In addition, 0.0.0.0 is not allowed. ● When the device protocol is MODBUS_TCP, set the IP address of the data collector to which the device connects. ● When the device protocol is MODBUS_RTU, set the IP address of the data collector to which the device connects. ● When the device protocol is Simple Network Management Protocol (SNMP), set the IP address of the device. ● When the device protocol is CInterface, set the IP address of the device.
	Port	The value is an integer ranging from 0 to 65,535. ● When the device protocol is MODBUS_TCP, set the corresponding port of the device. The port is **502** by default. ● When the device protocol is MODBUS_RTU, set the port number of the data collector to which the device connect. ● When the device protocol is SNMP, set the corresponding port of the device. The port is **161** by default. ● When the device protocol is CInterface, set the corresponding port of the device.
	Device Address	The value is an integer ranging from 0 to 255. ● When the device protocol is MODBUS_TCP or MODBUS_RTU, set the address of the device. ● When the device protocol is SNMP, the device address parameter does not exist. ● When the device protocol is CInterface, the device address parameter does not exist. **NOTE** The value combination of the **IP Address**, **Port**, and **Device Address** must be unique to each device.

Attribute	Parameter	Description
	Out Time	Time when testing the connection times out. The default value is three seconds. The value is an integer ranging from 1 to 60. **NOTE** • When the NMS delivers a heartbeat message to the device, the device determines that the device does not respond if the duration exceeds the value of this parameter. • This parameter affects the detection speed when the device is disconnected. The heartbeat is invalid only when the time specified in **Out Time** is reached. In this case, the device may be disconnected. • This parameter affects the packet response success rate of the device. If the device takes 2 seconds to respond to the NMS and **Out Time** is set to less than 2 seconds, the device does not receive any response.
	Security Name	Name of a user **NOTE** Specify this parameter when configuring devices that support the SNMPv3 protocol.
	Context Name	Context name of the managed object The value is a string of 0–60 characters and cannot contain special characters ,"#%&'+/\;<=>?.
	Authentication Protocol	Set this parameter to the value of **Authentication Protocol** configured on the device. The default value is **SHA**. The **SHA** and **MD5** protocols are supported. **NOTE** Specify this parameter when configuring devices that support the SNMPv3 protocol. **NOTICE** MD5 is an insecure protocol. SHA is recommended.
	Authentication Password	Set this parameter to the authentication password configured on the device. Value range: a–z, A–Z, 0–9, _ (8–15 characters, at least two types of characters, different from the user name or its reverse) **NOTE** Specify this parameter when configuring devices that support the SNMPv3 protocol. You are advised to set **Authentication Password** and **Privacy Password** to different values.

Attribute	Parameter	Description
	Privacy Protocol	Set this parameter to the value of **Privacy Protocol** configured on the device. The default value is **AES128**. The **AES128** and **CBC_DES** protocols are supported. **NOTE** Specify this parameter when configuring devices that support the SNMPv3 protocol. **NOTICE** DES is an insecure protocol. AES is recommended.
	Privacy Password	Set this parameter to the proprietary protocol key configured on the device. Value range: a–z, A–Z, 0–9, _ (8–15 characters, at least two types of characters, different from the user name or its reverse) **NOTE** Specify this parameter when configuring devices that support the SNMPv3 protocol. You are advised to set **Authentication Password** and **Privacy Password** to different values.
	Context Engine ID	Context engine ID of the managed object The value is a string of 0–60 characters and cannot contain special characters ,"#%&'+/\;<=>?.
	Read Community	Set this parameter to the read community configured on the device. Modifying the community per three months is advised. **NOTE** Specify this parameter when configuring devices that support the SNMPv1/v2 protocol.
	Write Community	Set the write community configured on the device. Modifying the community per three months is advised. **NOTE** Specify this parameter when configuring devices that support the SNMPv1/v2 protocol.

Attribute	Parameter	Description
	Connection Mode	Connection mode of a device. You can set this parameter to **Non-SSL Connection** or **SSL Connection**. If you modify the connection mode on the NMS, you must modify the connection mode on the device WebUI accordingly. **NOTE** • The connection mode settings for the NMS and device must be the same. • By default, **Connection Mode** is set to **SSL Connection** for the NMS and device.
	Authentication Password	Re-authentication password for the NMS and device 1. Click **Modify**. 2. In the displayed dialog box, enter **New Password** and **Confirm Password**. **NOTE** • The password must contain 8 to 32 characters. • The password includes at least three of the following types: lowercase letters, uppercase letters, digits, and special characters (~!@#^*_={}:,./?-`$). If the password does not comply with the rules, please change the password on the device side. Change the password periodically (every three or six months) to improve system security and prevent security risks, such as violent password cracking. 3. Select a value for **Send To Device**. **NOTE** If you select **YES**, the re-authentication password for the NMS and device is changed at the same time. If you select **NO**, only the re-authentication password for the NMS is changed. 4. Click **OK**. **NOTE** You can only change the re-authentication password for the ECC800-Pro.
	Camera Code	The camera code specified in the intelligent video surveillance system contains 15 digits. For details, see *Device Installation and Commissioning Guide*. **NOTE** The camera code is the value of **Device ID** whose last three digits are replaced with **101**. For example, if the value of **Device ID** is **878719000000000**, the value of **Camera Code** is **878719000000101**.

Attribute	Parameter	Description
Bind AccessController	AccessController	When creating a fingerprint controller, you can set whether to bind the fingerprint controller to the corresponding access controller. **NOTE** • The fingerprint controller must be bound to the TycoSun access controller for use. • The access controller to be bound must be in single-card mode.
	Door Passage	When creating a TycoSun access controller, **Door Passage** is **Enabled** by default. You can set **Door Passage** to **Enabled** or **Disabled** as required. **NOTE** When creating a fingerprint controller, if a door passage whose status is **Enabled**, the fingerprint controller can bind the door passage.
Setting UPS	UPS	When creating an iBOX, you can set whether to bind UPSs in the same management domain.
Electricity Info	Rated Power (kW)	Rated power consumption of a device The value is a floating number ranging from 0 to 65,535 (three decimal places).
	Power Mode	Click ▼, and choose **Single power supply** or **Dual power supply**.
Asset Info	Model	Model of the device. The value is a string of 0 to 64 characters.
	Manufacturer	Manufacturer of the device The value is a string of 0 to 64 characters.
	Serial Number	Serial number of the device upon delivery The value is a string of 0 to 64 characters.
	Lock Number	The value of this parameter cannot be modified.
	Weight (kg)	Weight of the device
	SN	Device number The value is a string of 0 to 64 characters.
	Location	Location of the device in the management domain The value is a string of 0 to 64 characters.
	Airflow Type	Select **Front to Rear**, **Bottom to Top**, **Side Left to Side Right**, **Side Right to Side Left**, or **Front to Top**.

Attribute	Parameter	Description
	Status	Device status Select **Enabled**, **Power-on**, **Power-off**, **Idle**, or **Offline**.
	Project No.	The value is a string of 0 to 64 characters.
	Start Date of Use (yyyy-MM-dd)	Device activation time
	Temperature Range (°C)	Temperature range in which the device works properly The value can be modified.
	Owner	The value is a string of 0 to 64 characters.
	Department	The value is a string of 0 to 64 characters.
	Installation Mode	The installation modes of different devices are different. Select the installation mode as required. Select **Floor Build In**, **Cabinet Build In**, **Wall Build In**, or **Ceiling installation**. The cabinet and PDU also support installation modes of **Antistatic floor installation** and **Cement floor installation**.
	Wire Type	Select **Ascending Line**, **Down Line**, or **Floor Line**.
Status Info	Start Date Of Use (yyyy-MM-dd)	Start date of use of the device
	Last Maintenance (yyyy-MM-dd)	Last maintenance time of the device
Extended Info	Rated Output Power (kW)	Rated output power of the device The value is an integer ranging from 0 to 65,535.
	Rated Cooling Capacity (kW)	Rated cooling capacity of the device
	Distribution Area	Select **Inlet Side** or **Outlet Side**.
	Install Height (m)	Select **0.6**, **1.2**, or **1.8**.

Attribute	Parameter	Description
	Temperature Range (°C)	Temperature range in which the device works properly The value can be modified.
	Installation Mode	The installation modes of different devices are different. Select the installation mode as required. Select **Floor Build In**, **Cabinet Build In**, **Wall Build In**, or **Ceiling installation**. The cabinet and PDU also support installation modes of **Antistatic floor installation** and **Cement floor installation**.
Protocol Info	Number of Heartbeats	Indicates that the device is disconnected for *N* consecutive heartbeat failures. The default value is **3**. The value is an integer ranging from 1 to 3. **NOTE** This parameter affects the speed at which the NMS detects device disconnection.
	Heartbeat Period (s)	Interval for the NMS to send heartbeat detection messages to the device to determine whether the device is connected. The value is an integer ranging from 1 to 10,000. **NOTE** The default value varies according to protocols.
	Sending Interval (ms)	Interval at which the device sends each packet. The default value is 600 ms. The value is an integer ranging from 50 to 10,000. **NOTE** This parameter affects the packet processing efficiency. Based on the response efficiency of the device, the device can process a packet within the interval specified by **Sending Interval (ms)**, which is the highest efficiency.
	Receiving Timeout (ms)	Indicates the timeout period for the NMS to receive packets from the device. The default value is 1000 ms. The value is an integer ranging from 500 to 10,000.

2 Device Management

Through device management, the layout and running status of devices on the network can be displayed in real time.

2.1 Device View

You can set views for the system to intuitively display equipment positions and running status.

2.1.1 Device View

You can set views for the system to intuitively display equipment positions and running status. This facilitates status monitoring for the entire network.

2.1.1.1 Managing Views

The **View** page displays the layout and running status of devices in the equipment room, and monitors the running status of devices on the entire network in real time. In addition, the system intuitively displays the physical environment of devices in the management domain view in 2D or 2.5D mode, facilitating efficient O&M and quick fault locating.

Prerequisites

- The device has been connected to the NetEco.
- You have the operation rights for **View**.

Context

CAUTION

- Exercise caution when shutting down the smart cooling product. Doing so may cause devices and equipment room overheating, which will damage the devices.
- Exercise caution when powering off the rPDU or PDU2000. Doing so may affect the power supply to equipment, which will interrupt services.

Procedure

Step 1 Choose **Device Management** > **Device Vew** > **View**.

Step 2 On the **View** page, view the overview information about managed objects on the entire network.

Table 2-1 Operation task

Operation	Description	Procedure
Modifying scenario names	Perform this operation when you want to modify the name of a scenario.	1. Click  in the upper left corner of the page. The **Scenario-based Configuration** dialog box is displayed. 2. Click  in the **Operation** column to modify the scenario name, and click **OK**.

Operation	Description	Procedure
Viewing the overview of managed objects on the entire network	You can view the number of nodes with alarms of each severity, number of nodes without alarms, total number of alarms, and maintenance information. In addition, you can scan the QR code to install the NetEco app.	• In the upper left area of the page, view the number of nodes with alarms of each severity and the number of nodes without alarms. • In the **Alarm** area on the right of the page, view the total number of alarms and the number of alarms of each severity for managed objects on the entire network. • In the **Maintenance** area on the right of the page, view the maintenance information about the managed objects on the entire network. • In the **Download APP** area on the right of the page, you can scan the QR code to install the NetEco app.

Step 3 View the management domain view.

1. Access the management domain.
   - Method 1: Click the search box on the left of the page. In the expanded navigation tree, select a management domain.

     NOTE

     To query and select a management domain by setting search criteria, perform the following operations:

     - In the **Recommended Filter** area, click **Connection Status: Connected** or **Connection Status: Disconnected**, and then click the name of the management domain.
     - Enter a keyword in the text box, click  , and click the management domain name.
   - Method 2: Double-click the management domain icon to access the management domain.
2. To view the detailed information about a management domain and the information about all the devices in the management domain, perform the following operations as required.

Table 2-2 Viewing the management domain view

Operation	Description	Procedure
Switching to the 2D or 2.5D mode	The 2D or 2.5D mode displays the layout of devices, device running status, alarm status, and signal counter status in the management domain on a plane.	Click  on the toolbar on the left.
Viewing the overview information about a management domain	You can view basic information about sub-management domains or devices in a management domain, and information about **Statistics of Faulty Devices**, **License Consumption**, and **Statistics of Disconnected Devices** in the management domain.	1. Click  on the toolbar on the left. 2. On the **Overview** page, you can perform the following operations: ▪ You can click a device name to go to the device view page and click a management domain to go to the management domain view page of the device. ▪ You can click the device running status icon in the **Alarm Status** column to go to the **Alarm** tab page of the device and view the current alarm information of the device. ▪ The value of **License Consumption** is the total number of licenses consumed by devices in the management domain. **NOTE** If the device is a non-intelligent device, redirection is not supported.
Viewing counter monitoring information	You can view the real-time monitoring counter signal information about IT cabinets in the management domain, and view or modify the device monitoring view to learn about the running status of devices based on the real-time signals of the devices.	1. Click  on the toolbar on the left to view the real-time monitoring counter signal information about the IT cabinets. 2. In the **Signal** dialog box, click  in the **Operation** column to view the monitoring view. **NOTE** To modify a monitoring view, click **Modify** in the **Monitoring View** dialog box.

Operation	Description	Procedure
Adding a control element	An entry for directly adding control elements is provided on the **View** page.	Click  on the toolbar on the left and drag the control to a proper position in the view. For details, see **2.1.1.2 Adding Control Elements**. **NOTE** You can add controls in the toolbox to the management domain only when  is displayed.
Configuring a monitoring view	You can view and modify the monitoring view to learn the running status of a device. Only signal counters of key devices can be modified.	Click  on the toolbar on the left. For details, see **2.1.1.3 Configuring a Monitoring View**.
Viewing camera information	If cameras have been added to the management domain, you can view camera information and play video.	Click  on the toolbar on the left to view camera information. To play a video, click the name of an online camera in the **Name** column.

Operation	Description	Procedure
Viewing environment information about a management domain	The following lists the devices and methods for measuring the temperature and humidity of the environment module. – Air conditioner: average supply air and return air temperature and humidity – Sensor/Collector: The sensor/collector with temperature and humidity counters collects the reported temperature and humidity values and participates in calculation. If a smart module is deployed, the statistics result is displayed by cold aisle and hot aisle. ▪ Click **Environment** for a device except cabinets. In the displayed **Average temperature and humidity change curve** dialog box, you can view the average temperature and humidity in 24 hours, top 10 highest temperature and humidity values, and top 10 lowest temperature and humidity values of the management domain.	In the right pane of the page, view the environment information about the management domain.

Operation	Description	Procedure
	▪ Click **Environment** for a cabinet. In the displayed **Average temperature change curve** dialog box, you can view the average temperature of the cabinet in 24 hours. You can click **Avg Temperature (Front)** or **Avg Temperature (Back)** to display or hide the trend chart. If an item is highlighted, the corresponding trend chart is displayed.	

Operation	Description	Procedure
	NOTE If the management domain is a smart module, the status of the smoke detector and water sensor is displayed. If the management domain is a cabinet, the status of the smoke detector and door status sensor is displayed. – A door status sensor state can be **Closed**, **Opened**, **Unknown**, or **Not Configured**. **Unknown** indicates that the door status sensor is bound to indicators and the door status information is not obtained. **Not Configured** indicates that no door status sensor control is created or no counter is bound. You can click  on the left of the page. For details about how to configure a door status sensor control, see **2.1.1.2 Adding Control Elements**. On the 2.5D view page, the door status sensor state is displayed in **Environment** after the **Door state** counter is bound to the door status sensor control. – The water sensor state can be **Normal**, **Alarm**, or **Not Configured**. **Not Configured** indicates that no water sensor control is created or no counter is bound. You can click  on the left of the page. For details about how to configure a water sensor control, see **2.1.1.2 Adding Control Elements**. On the 2.5D view page, the water sensor state is displayed as **Normal** or **Alarm** in **Environment** after the appropriate counter and alarm are bound to the water sensor control (the bound alarm must be an uncleared alarm in the current alarm list). – The smoke detector	

Operation	Description	Procedure
Querying management domain alarms	By default, the number of uncleared alarms collected by alarm severity and device type in the equipment room is displayed. **NOTE** The device types are as follows: – Power supply: PDU, UPS, ATS, DG, transformer, battery string, and rPDU – Cooling: water chiller, pump, cooling tower, and air conditioner – Environment: sensors, such as the water sensor, smoke detector, and temperature and humidity sensor in equipment rooms or smart modules – Security: access controller and camera – Others: alarms reported by the ECC	1. In the right pane of the page, view the alarm information about the management domain. 2. Click **Alarm** to go to the **Current Alarms** page.

Step 4 View the device view.

1. Enter the device view.
   - Method 1: Click the search box on the left of the page. In the expanded navigation tree, select a device in the equipment room.
   - Method 2: Double-click the device name on the **View** page.

   Displays device information such as overview, alarms, and signals, helping you learn about the device status in real time and handle abnormal data to better understand the device running status.
2. View details about the device view and perform the following operations as required.

   NOTE

   For Air conditioner_NetCol5000-A025_BIN4 and Air conditioner_NetCol5000-A042_BIN4, if an alarm is generated for the internal fan, heater, electronic expansion valve, humidifier, air filter, compressor, or external fan of the air conditioner, the corresponding component is displayed in the color set for the alarm severity in the air conditioner logical flow diagram.

Table 2-3 Operation task

Operation	Description	Procedure
Viewing basic device information	Displays the basic device information, energy flow diagram, and real-time data of some counters, and provides a quick entry for modifying device configuration information.	In the left pane of the page, view the basic information, energy flow diagram, and real-time data of some counters of devices. **NOTE** If you need to modify the device configuration information, click **Edit** to go to the **Planning Configuration** page.
Viewing monitoring counters for devices	You can set device monitoring counters to effectively monitor devices for timely handling of abnormal data.	1. Select a device and click  in the upper right corner of the page. 2. In the **Setting** dialog box, select counters and click **OK**.
Viewing the comprehensive analysis of devices	Displays the changes of concerned counters in trend charts, status charts, and comparison charts, helping you understand the comprehensive analysis of devices in a timely manner.	On the **Comprehensive Analysis** tab page in the upper part of the page, view the comprehensive analysis of devices. **NOTE** To display multiple comprehensive analysis tab pages and set the chart style or layout, click  in the upper right corner of the tab page.
Viewing KPI information	Displays concerned KPIs in a list. You can set the display of more KPIs, and view and modify the monitoring views of KPIs to learn about the detailed running status of devices. Only signal counters of key devices can be modified.	1. On the **KPI** tab page in the upper area of the page, click  . 2. Select the counter to be bound and click **OK**. 3. Click  in the **Operation** column to display the monitoring view of the counter.

Operation	Description	Procedure
Viewing control signal information	Displays the AO/DO signal of the device in a list. You can set the display of more control signals, and view and modify the monitoring views of control signals to learn about the detailed running status of devices. Only signal counters of key devices can be modified.	1. On the **Signal** tab page in the lower part of the page, click  . 2. Select the counter to be bound and click **OK**. 3. Click in the **Operation** column to display the monitoring view of the counter. 4. Click in the **Operation** column to set the real-time control signal value and deliver the signal remotely.
Viewing device signals	Allows you to view real-time device running signals to learn about the device running status.	1. On the **Signal** tab page in the lower part of the page, view the monitoring signal information about devices. 2. Click in the **Operation** column of the device signal value counter. In the displayed **Monitoring View** dialog box, view and modify the monitoring view.
Managing device alarms	Allows you to view and handle device alarms in a timely manner.	On the **Alarm** tab page in the lower part of the page, view the alarm details of the device.

----End

2.1.1.2 Adding Control Elements

You can add control elements and view control details on the **View** page. Each control can describe objects in the equipment room view, monitor devices in real time, and link to other view pages.

Prerequisites

You have the operation rights for **View**.

Procedure

Step 1 Choose **Device Management** > **Device Vew** > **View**.

Step 2 Click the search box on the left of the page to expand the navigation tree and select a management domain.

Step 3 On the toolbar on the left, click and drag the control to a proper position in the view.

NOTE

The 2.5D view button is unavailable in the park, building, and floor views.

Step 4 In the **Property Panel** dialog box, set the basic properties of the control in the **Basic Properties** area.

Table 2-4 Setting control attributes

Operation	Procedure
Binding counters	1. Click ··· next to **Counter**. 2. In the **Select Data** dialog box, select the managed objects and counters to be added and click **OK**.
Binding alarms	1. Click ··· next to **Current Alarm**. 2. In the **Select Data** dialog box, select the alarm to be bound, and then click **OK**. **NOTE** You can bind a maximum of 20 alarms to a device in the equipment room. After alarms are bound to a device, the counter control icon is displayed in the color of the alarm with the highest severity when alarms are raised for the device.
Setting control icons	• If you select a door status sensor or status control, click **Settings** and set the real-time value and status icon according to the plan. • If the selected control is not a door status sensor or status control, you can click **Custom** and perform the following operations in the **Select Image** dialog box: – Click , select a local image to be uploaded, and click **OK**. – Click the image to be displayed on the right, and then click **OK**. **NOTE** To apply the configured counter control icon to the counter control created on the NetEco, perform the following operations: 1. Click **Apply to Others**. 2. In the displayed **Select Control** dialog box, select the counter control created on the NetEco. 3. Click **OK**.

Step 5 In the **Extended Properties** area, set extended attributes of the control and click .

Step 6 Move the mouse to the top of the control to display the control measurement information.

NOTE

- To modify the basic properties or extended properties of a control, perform the following operations:
  1. Double-click the control icon.
  2. In the **Property Panel** dialog box, modify the basic properties or extended properties of the control, and then click .
- To delete a control, click the control icon, choose , and click **Delete**.

----End

2.1.1.3 Configuring a Monitoring View

Provides functions such as setting the layer of the view page.

2.1.1.3.1 Managing the Service Layer

On the **View** page, you can select a service layer to quickly switch the service layer view to be displayed.

Procedure

Step 1 Choose **Device Management** > **Device Vew** > **View**.

Step 2 Click the search box on the left of the page to expand the navigation tree and select a management domain.

Step 3 Click on the toolbar on the left.

Step 4 On the **Monitor View Config** page, choose **Business Layer Management**.

NOTE

To reselect a management domain, click **Choice** on the **Business Layer Management** page.

Step 5 On the **Business Layer Management** page, perform the following operations based on the application scenario.

Table 2-5 Managing the service layer

Operation	Procedure
Managing service layers	• Adding a service layer 1. Click **Add**. 2. In the **Add Layer** dialog box, set **Service Layer Name** and click **OK**. • Modifying a service layer In the **Service Layer** area, select a service layer, change the service layer name, and click **Save**. • Deleting a service layer In the **Service Layer** area, select a service layer and click **Delete**.
Monitoring signal of the management control	• Adding a monitoring signal for the control 1. In the **Service Layer** area, select a service layer and click **Create**. 2. In the **Create control** dialog box, set **Device** and **Measurement Object**, and then click **Next**. 3. Set **Measurement Counter** and **Control Type**, and then click **OK**. • Modifying the monitoring signal of the control 1. In the **Service Layer** area, select a service layer and click **Edit** in the **Operation** column. 2. In the **Property Panel** dialog box, modify the basic attributes and extended attributes, and then click **OK**. **NOTE** To apply the basic or extended properties of the control to other management domains and devices, click **Apply to Others**. • Deleting the monitoring signal of a control In the **Service Layer** area, select a service layer, select one or more monitoring counters, and click **Delete**.

----End

Follow-up Procedure

After the service layer configuration is complete, click **Back to View** in the upper right corner of the **Business Layer Management** page to return to the view. On the **View** page, you can view the service layer view.

1. Click the search box on the left of the page to expand the navigation tree and select a management domain.
2. Click  on the toolbar on the left to switch to the 2D view.
3. Click  on the toolbar on the left to view the corresponding service layer view.

2.1.1.3.2 Setting the Quick Navigation Bar

On the **View** page, you can customize the navigation bar. After a quick navigation bar is added, the navigation bar can be displayed on the **View** page, helping users quickly switch the view angle.

Procedure

Step 1 Choose **Device Management** > **Device Vew** > **View**.

Step 2 Click the search box on the left of the page to expand the navigation tree and select a management domain.

Step 3 Click on the toolbar on the left.

Step 4 On the **Monitor View Config** page, choose **Quick Navigation Config**.

Step 5 On the **Quick Navigation Config** page, perform the following operations based on the application scenario.

Table 2-6 Managing the navigation bar

Operation	Procedure
Managing the navigation bar	• Adding a navigation bar 1. Click **Add**. 2. In the **Add Navigation Bar** dialog box, set **Navigation bar name** and click **OK**. • Modifying a navigation bar In the **Navigation Bar** area, select a navigation bar, change the navigation bar name, and click **Save**. • Deleting a navigation bar In the **Navigation Bar** area, click **Delete**.
Managing quick navigation	• Adding quick navigation 1. In the **Navigation Bar** area, choose a navigation bar and click **Create**. 2. In the **Create Quick Navigation** dialog box, set the related parameters, and then click **OK**. • Modifying quick navigation 1. In the **Navigation Bar** area, click in the **Operation** column. 2. In the **Property Panel** dialog box, modify the related parameters, and then click **OK**. • Deleting quick navigation In the **Navigation Bar** area, select one or more quick navigation records, and click **Delete**.

----End

2.1.1.3.3 Setting View Display Parameters

You can set parameters such as the display mode of the navigation tree and view, whether to display the O&M index, and overview.

Procedure

Step 1 Choose **Device Management** > **Device Vew** > **View**.

Step 2 Click the search box on the left of the page to expand the navigation tree and select a management domain.

Step 3 Click on the toolbar on the left.

Step 4 On the **Monitor View Config** page, choose **Data Center View Settings**.

Step 5 On the **Data Center View Settings** page, set related parameters and click **Apply**.

----End

2.1.1.3.4 Device Page Settings

On the **View** page, you can view the energy flow diagram of key devices by default and set the display effect of the page.

Procedure

Step 1 Choose **Device Management** > **Device Vew** > **View**.

Step 2 Click the search box on the left of the page to expand the navigation tree and select a management domain.

Step 3 Click on the toolbar on the left.

Step 4 On the **Monitor View Config** page, choose **Device Page Settings**.

Step 5 On the **Device Page Settings** page, click **Create** in the upper right corner.

Step 6 In the **Create** dialog box, set the related parameters, and then click **OK**.

NOTE

To delete a created device page, select one or more device pages and click **Delete**.

----End

2.1.2 Battery Management

This section describes how to check the SOH of batteries and battery groups in the root node, or in a building, equipment room, or other region, handle abnormal batteries in a timely manner.

Prerequisites

Battery devices communicate with the NetEco properly.

Procedure

Step 1 Select **Device Management** > **Device View** > **Battery Management**.

Step 2 Check battery SOH, take lead-acid batteries as an example.

NOTE

Under the root node, click the position of the faulty battery or the name of the battery group to go to the battery group information page.

- Check the SOH of a battery group under the management domain.

  In the navigation tree on the left, choose the root node, building or equipment room to check the status of a faulty battery or a faulty battery group in the whole region.

- Check the SOH of a battery group under the device.

  In the navigation tree on the left, choose the device to check the status of basic information, a faulty battery, a faulty battery group in the whole region.

- Check the SOH of a single battery group.

  In the navigation tree on the left, choose the battery group to check the overview and historical trend of the group. You can view the battery group in real time in chart, table, or discharge curve form. The number of batteries in that group is also displayed.

  NOTE

  – Click  to sort battery strings by counter.
  – Click the battery to go to the **Battery analysis** page. You can view the battery status in chart or table form. Besides, data can be exported from that page.
  – Lithium ion battery relative to lead-acid battery, **Highest Temperature** and **Lowest Temperature** and **Highest Voltage** and **Lowest Voltage** are measured.

----End

Follow-up Procedure

You can perform the following operations on the **Check the battery health status** page.

Operation	Procedure
Checking historical data	• Click the name of a counter to set whether to display the counter in the view. If the name is highlighted, the counter is displayed in the historical trend chart. If the name is unavailable, the counter is not displayed in the chart. • Click ,select a data area to display the data of the specified area. • Click to restore the zoomed view. • Click to restore the zoomed page. • Click to save the historical trend chart as a picture. • Click to check the SOH in tables.
Exporting Historical Data	• Exporting Historical Battery String Data Click in the lower right corner of **History Trend** to export the historical battery string data. • Exporting Historical Battery Data – Click a battery in the table view. On the **Battery Analysis** page that is displayed, click **Export** to export historical battery data. – Click in the upper right corner of the table view, In the displayed **Battery Analysis**, On the page, click **Export** and export historical battery data.

2.2 Configuration

This section describes how to configure device management.

2.2.1 Planning Configuration

On the **Planning Configuration** page, you can create, modify, and delete management domains and devices.

2.2.1.1 Relocating Management Domains or Devices

You can use the relocate function to relocate the management domain or device to be relocated to the target management domain.

Procedure

Step 1 Choose **Device Management** > **Configuration** > **Planning Configuration**.

Step 2 On the **Planning Configuration** page, click **Relocate** on the toolbar.

Step 3 In the **Relocate Domain or Device** dialog box, select the management domain or device to be relocated and the target management domain, and then click **OK**.

----End

2.2.1.2 Synchronizing Device Configuration Data to the NetEco

When the configuration data of a device changes, you can use the synchronization function of the NetEco to synchronize the data on the NetEco with the data on the device. This ensures data consistency between the NetEco and the device.

Prerequisites

The device is properly connected.

Context

After a device is created, the NetEco automatically synchronizes configuration data from the device when the network connection is normal. In this case, the configuration data on the NetEco is the same as that on the device. In the subsequent maintenance, you may need to modify the configuration parameters on the device directly. This may result in the inconsistency of the configuration data between the device and the NetEco. To ensure data consistency, the NetEco provides two synchronization modes: automatic synchronization and manual synchronization. For details, see **Table 2-7**.

Table 2-7 Device configuration data synchronization modes and mechanisms

Synchronization Mode		Synchronization Mechanism	Advantages and Disadvantages
Automatic synchronization	Periodic automatic synchronization	The NetEco initiates data synchronization to the device once every five days.	The synchronization time is fixed, which can ensure data synchronization to some extent. However, the synchronization period is long.

Synchronization Mode		Synchronization Mechanism	Advantages and Disadvantages
	Triggered automatic synchronization	When the configuration data of a device changes or a component is added to or removed from a device, the device sends a synchronization notification to the NetEco. After receiving the notification, the NetEco immediately initiates data synchronization.	Due to network problems, the NetEco may fail to receive synchronization notifications and therefore cannot initiate data synchronization in a timely manner.
Manual synchronization		Data synchronization is initiated immediately.	Data can be synchronized in time.

Procedure

Step 1 Choose **Device Management** > **Configuration** > **Planning Configuration**.

Step 2 On the **Planning Configuration** page, click .

Step 3 In the **Synchronize** dialog box, select a device, and then click **OK**.

----End

2.2.2 Managing Device Signals

You can change the name of a counter through signal management to identify the counter more easily.

Prerequisites

- You have the **Signal Management** permission.
- You have logged in to the NetEco client using a web browser.

Procedure

Step 1 Choose **Device Management** > **Configuration** > **Signal Management**.

Step 2 In the navigation tree on the left, select the device to be modified and perform the following operations as required.

Table 2-8 Managing signals

Operation	Description	Procedure
Customizing signals	You can customize device signals, bind signal data sources, and modify or delete signals.	1. On the **Sampling**, **Statistics**, or **Configuration** tab page, click **Customize Signal**. 2. On the **Customize Signal** page, perform the following operations as required: – Customizing signals a. On the **Sampling Signals** or **Statistical Signals** tab page, click **Create Signal**. b. In the **Create** dialog box, click **Add**. c. Set signal parameters and click **Save**. – Binding signal data source On the **Sampling Signals** or **Statistical Signals** tab page, select one or more signals and click **Batch Bind**. Or click in the **Operation** column. – Modifying signals On the **Sampling Signals** or **Statistical Signals** tab page, click in the **Operation** column. – Deleting signals On the **Sampling Signals** or

Operation	Description	Procedure
		Statistical Signals tab page, select one or more signals and click **Delete**. Or click in the **Operation** column.

Operation	Description	Procedure
Managing signals	You can modify parameters such as the signal name and collection period as required. In addition, you can apply the modified signal parameters to devices of the same type in batches.	• Modifying a single signal On the **Sampling**, **Statistics**, or **Configuration** tab page,, modify the related parameters of the signal, and then click **Apply**. • Modifying signals in batches On the **Sampling**, **Statistics**, or **Configuration** tab page, modify the related parameters of the signal, and then click **Batch Apply**. **NOTE** • If you have modified signal parameters but have not clicked **Apply** or **Batch Apply**, you can click **Revoke** to restore the original parameter settings. • If you have modified signal parameters and clicked **Apply** or **Batch Apply**, you can click **Revert** to restore the original parameter settings. • The **View**, **Planning Configuration**, and **Historical Data** pages will display the modified signal names of counters. (On the **Historical Data** page, if you select a single device, the modified counter name is displayed. If you select multiple devices, the default counter name is displayed.)

----End

2.3 Alarm Management

The NetEco provides management functions such as monitoring network alarms, querying alarms or events, and setting remote alarm notifications. These functions help you quickly detect, locate, and rectify network faults.

2.3.1 Viewing and Handling Current Alarms

On the **Current Alarms** page, O&M personnel can view current alarms that are updated in real time to learn the latest alarm status and handle the alarms.

2.3.1.1 Viewing Current Alarms

The **Current Alarms** page displays current alarms that are updated in real time.

Context

- If a new alarm is reported and the number of current alarms exceeds the upper capacity threshold, alarm management enables the mechanism of processing full current alarm cache and moves some alarms to the historical-alarm list.
- When you go to the **Current Alarms** page for the first time, alarms in the alarm list are sorted in descending order of **Arrived On** by default.
- The newly reported alarms are displayed in bold on the page.
- The background color of cleared alarms is green by default.
- You can only monitor and view alarms of authorized MOs.
- A maximum of 200 **Current Alarms** pages can be opened.

Procedure

- Monitoring alarms
  a. Choose **Device Management** > **Alarms Management** > **Current Alarms** from the main menu.
  b. **Table 2-9** describes alarm monitoring methods.

Table 2-9 Alarm monitoring methods

Task	Task Description
Monitoring alarms using the alarm list	On the **Current Alarms** page, monitor the alarms reported by all NEs and systems in real time.
Monitoring alarms using alarm indicators	The alarm indicators in the upper right corner of the **Current Alarms** page show the number of critical alarms, number of major alarms, number of minor alarms, and number of warning alarms.

Task	Task Description
Monitoring alarms using the statistics panel	Click  in the upper right corner of the **Current Alarms** page to view the alarm statistics charts. The statistical result is obtained based on the filtered alarms. The **Top 10 Alarms**, **Duration**, **Top 10 Alarm Sources**, **Severity**, and **Status** statistical charts can be displayed on the statistics panel. Four statistical charts can be displayed at the same time. You can click  in the upper right corner of the statistics panel and then select the chart to be displayed from the drop-down menu in the upper right corner of each chart. On the statistics panel, you can click any statistical result to quickly display the alarms that meet the condition. If you close the statistics panel, the filter criteria selected on the panel are automatically deselected. **NOTE** • Alarm management allows a maximum of 10 statistics panels to be opened by online users concurrently. • You can click  in the upper right corner of the statistics panel to manually refresh the statistical data. Within 10 minutes after you open the statistics panel or manually refresh the statistical data, the system automatically refreshes the data every minute.

- Querying alarms
  a. Choose **Device Management** > **Alarms Management** > **Current Alarms** from the main menu.
  b. You can click **Template Management** in the upper left corner of the page to view all filter templates and select a filter template from the **Quick Filter** panel. Users with the **Administrators** role can manage templates saved by all users.

     The following types of templates are provided:

     - **Favorite**: You can add the templates that you often use to your favorites.
     - **Custom**: The template is customized by the current user. You can set whether to share the template with other users. You can set a custom template as the key template. The alarms that are filtered using the key template are displayed in both the emergency maintenance notification list and alarm list.
     - **Shared**: Such a template can be shared with other users.

- **Default**: Default filter template.
- **Other**: Filter templates that are not shared by other users. Other templates are visible only to users assigned the **Administrators** role.

NOTE

The filter templates on the **Current Alarms**, **Historical Alarms**, and **Masked Alarms** pages are independent of each other and cannot be shared.

c. If the filter templates under **Template Management** do not meet your requirements, click **Filter** in the upper left corner of the **Current Alarms** page to set filter criteria. Set filter criteria and click OK to search for the alarms to be concerned about and handled.

d. Click **Save** or **Save As** to save the current filter criteria as a filter template. Not only the filter criteria, but also the alarm display column information and the combo sorting information configured by users are saved in the filter template.

e. Export current alarms. Alarms can be exported to an .xlsx or .csv file. When the exported file format is set to .xlsx and the number of alarms exceeds 100,000, the file is exported as a .zip package. When the exported file format is set to .csv and the number of alarms exceeds 10,000, the file is exported as a .zip package.

- Export some alarms: Select the alarms to be exported, click **Export**, and choose **Selected**.
- Export all alarms: Click **Export** and choose **All**.

NOTE

Only the information about the alarm columns displayed on the page can be exported. You can click in the upper right corner of the alarm list to set the alarm columns to be displayed.

Parameter Description

For details about parameters on the alarm filter panel, see **Table 2-10**.

Table 2-10 Description of parameters on the alarm filter panel

Parameter	Description
Alarm name	Name of the alarms to be queried. You can import or export the selected alarms or export all alarms when adding alarms.
Alarm source	Device or NE where an alarm is generated. If multiple alarm source conditions are set, the filtering result is the union of all the conditions. That is, all the alarms that meet any of the conditions are displayed on the page.
Severity	Alarm severity, including critical, major, minor, and warning. By default, all alarm severities are selected. You must select at least one alarm severity.

Parameter	Description
Alarm status	Alarm status, including the acknowledgment and clearance status, maintenance status, and validity status. This parameter is not displayed on the **Masked Alarms** page.
Last occurred	Time when the alarm last occurred. This parameter is displayed as **Occurred** in **Alarm Logs**, **Masked Alarms**, and **Historical Alarms**, indicating the last occurrence time of an alarm.
Cleared	Time when an alarm is cleared. You can set this parameter in the **Advanced settings** area on the **Alarm Logs** or **Historical Alarms** page. This parameter is not displayed on the **Masked Alarms** page.

Parameter	Description
Advanced settings	You can set alarm parameters to filter desired alarms. If advanced criteria are set, the filtering result is determined by the intersection of all the criteria. That is, only the alarms that meet all the advanced criteria are displayed. Operators (case-sensitive): • **contains**: Filters the alarms that contain the specified character string. • **does not contain**: Filters alarms that do not contain the specified character string. • **begins with**: Filters alarms that begin with the specified character string. • **ends with**: Filters alarms that end with the specified character string. • **is in**: Filters the alarms that are the same as the specified character string. For example, in the **Location Info** area, set **Operator** to **is in** and set **Value** to *XXX*. In this case, the location information of the filtered alarms contains *XXX*, and the alarms whose location information contains *XXX***123** are not displayed. • **is not in**: Filters alarms that are different from the specified character string. For example, in the **Location Info** area, set **Operator** to **is not in** and set **Value** to *XXX*. In this case, the location information of the filtered alarms does not contain *XXX*, and the alarms whose location information contains *XXX***123** are displayed. • **is blank**: Filters the alarms if their values of this parameter are empty. • **is not blank**: Filters the alarms if their values of this parameter are not empty. To improve the maintenance efficiency, you are advised to retain the default settings of **Associated alarm ID**, that is, **Root alarms**, **Aggregated alarms**, and **Normal alarms** are selected. This parameter is not displayed on the **Masked Alarms** or **Historical Alarms** page. Meanings of the options: • **Normal alarms**: Indicates that the alarm does not have root alarms or correlative alarms and aggregated alarms or original alarms. • **Root alarms**: Alarm that causes multiple correlative alarms. • **Correlative alarms**: Alarm that is generated due to the root alarm. • **Aggregated alarms**: After an alarm that meets the aggregation rules is reported, a new alarm is generated, which corresponds to multiple original alarms.

Parameter	Description
	• **Original alarms**: Alarms that meet the aggregation rules correspond to an aggregated alarm.

For details about parameters in the alarm list, see **Table 2-11**.

Table 2-11 Description of parameters in the alarm list

Name	Description
Alarm Serial Number	Alarm SN. When an alarm is generated, it may be modified multiple times. For example, its severity may change or it may be cleared. The SN uniquely identifies an alarm.
Alarm Matched Rule Name	An alarm meets the rule and is handled according to the rule settings.
Occurrences	Number of occurrences or merged times for an alarm of an alarm source, that is, the repeated or merged alarms have the same location information and alarm ID. This parameter helps users to increase concerns on the alarm. This parameter is not displayed on the **Masked Alarms** or **Historical Alarms** page.
Alarm Source	Device or NE that generates an alarm.

Name	Description
Name	Name of an alarm. An alarm name tells what faults occur on an alarm source. For example, the high CPU usage alarm can be known by its name that the alarm is sent from the CPU. The meanings of the icons displayed next to alarm names are as follows: •  : This icon is displayed when an alarm is a root alarm. You can expand the row that contains the alarm in the list to view its correlative alarms. •  : This icon is displayed when an alarm is a correlative alarm. You can expand the row contains the alarm in the list to view its root alarms. •  : This icon is displayed when an alarm is an aggregated alarm. •  : This icon is displayed when an alarm is an original alarm. •  : This icon is displayed when an alarm is an invalid alarm. •  : This icon is displayed when an alarm is in the maintenance state. •  : This icon is displayed when the alarm is a toggling alarm. Expand **Filter criteria** and set **Toggling Identifier** in the **Advanced settings** area to filter alarms. •  : This icon is displayed when an alarm reference page is available for an alarm. Click this icon to view the alarm reference page. •  : This icon is displayed when an alarm has remarks. Click the alarm name to view the remarks on the alarm details page.
Alarm ID	ID of an alarm, which corresponds to the alarm name.
Severity	Four alarm severities: critical, major, minor, and warning.
Acknowledgment Status	Acknowledgment status of the alarm. Available options are: • **Acknowledged** • **Unacknowledged** This parameter is not displayed on the **Masked Alarms** page.
Clearance Status	Clearance status of an alarm. Available options are: • **Cleared** • **Uncleared** This parameter is not displayed on the **Masked Alarms** page.

Name	Description
Toggling Times	Number of times that alarms that meet the toggling conditions are reported during the toggling. This parameter is not displayed on the **Masked Alarms** page.
Possible Causes	Possible causes of an alarm, which can provide guidance for alarm handling.
Maintenance Status	Maintenance status of an alarm. For example, the **NORMAL** state means that the alarm source is running normally instead of being commissioned or upgraded. This parameter is not displayed on the **Masked Alarms** page.
Acknowledged On	Time when an alarm is acknowledged. This parameter is not displayed on the **Masked Alarms** page.
Cleared On	Time when an alarm is cleared. This parameter is not displayed on the **Masked Alarms** page.
Alarm Source Identifier	Identifier allocated by alarm management to the source system.
Alarm Source Type	Type of the NE where an alarm is generated.
Type	Type of an alarm, indicating the type of the cause which triggers the alarm.
Operation	Operations that users can perform on the alarm. ● Acknowledge the alarm ● Clear the alarm ● Send notifications by emails ● Send SMS message notifications ● Set masking rules ● Set an identification rule ● Set a notification rule ● Set an intermittent/toggling rule ● Set an aggregation rule ● Switch the view
Location Info	Information that helps you quickly locate the location where the alarm is generated.

Name	Description
First Occurred	If the alarm is a merged alarm, the time when it first occurred is displayed. If the alarm is not a merged alarm, its generation time is displayed. This parameter is not displayed on the **Masked Alarms** or **Historical Alarms** page.
Arrived On	Time when the alarm arrives at alarm management.
Last Occurred	If the alarm is a merged alarm, its last occurrence time is displayed. If the alarm is not a merged alarm, its generation time is displayed. On the **Masked Alarms** and **Historical Alarms** pages, this parameter is displayed as **Occurred**.
Acknowledged By	User who acknowledges the alarm. If the alarm is unacknowledged, the user who unacknowledges the alarm is displayed in the **Acknowledged By** column. This parameter is not displayed on the **Masked Alarms** page.
Cleared By	User who clears the alarm. This parameter is not displayed on the **Masked Alarms** page.
Handler	Username of the current alarm handler. The O&M personnel can assign alarms to handlers. This parameter is not displayed on the **Masked Alarms** page.
Auto Clear	Whether an alarm can be automatically cleared. • **Yes**: The alarm can be automatically cleared. After the fault that triggers the alarm is rectified, **Clearance Status** of the alarm automatically is changed to **Cleared**. • **No**: The alarm cannot be automatically cleared. After the fault that triggers the alarm is rectified, you must manually clear the alarm. This parameter is not displayed on the **Masked Alarms** page.
Other Information	Information irrelevant to alarm locating to help users understand the alarm.
Comments	Alarm comments entered by users. The comments cannot exceed 512 characters. Setting method: Select an alarm and click **Comment** to enter comments.
Reason ID	ID of the alarm cause.

Name	Description
Clearance Type	Alarm clearance type: • **(Blank)**: uncleared. • **normal clear**: A device fault is rectified and alarm management receives a clear alarm. Then the alarm is automatically cleared. • **restore clear**: After a device restarts, alarm management detects whether a fault exists. The original fault alarm is automatically cleared. • **manual clear**: An alarm is manually cleared. • **configure clear**: A resource object is deleted, and the alarms generated by the resource object are automatically cleared. • **correlation clear**: When receiving a root alarm of uncleared correlative alarms, alarm management handles the alarms using a correlation rule, reports the root alarm, and automatically clears the correlative alarms. The clearance type of the correlative alarms is correlation clearance. • **clear from system**: The system clears earlier alarms according to the full-cache processing rule because the storage space is limited. • **status switch clear**: Because the device status switches, the active alarm in the previous status is automatically cleared and is reported again in the device status after the switch. The clearance type of the active alarm in the previous status is status switch clearance. • **alarm synchronization-based clear**: During alarm synchronization, if some uncleared alarms exist in alarm management but cannot be found in the alarms synchronized from NEs, these uncleared alarms are automatically cleared. This parameter is not displayed on the **Masked Alarms** page.
Validity	The default value is **Valid**. You can set it to **Invalid** on the **Identification Rules** page. This parameter is not displayed on the **Masked Alarms** page.
Duration	Duration from **Last Occurred** to **Cleared On**. This parameter is not displayed on the **Masked Alarms** page.
Resource ID	ID of the alarm source.
Device Category	Alarm source categories.

Name	Description
Threshold Rule	Threshold for reporting an alarm, that is, the threshold of the fault-related measurement indicator. For example, the "High Ambient Temperature" alarm is reported when the ambient temperature exceeds the threshold.
Threshold Information	When a threshold-crossing alarm is reported, the alarm generation value is displayed in the threshold information. When the threshold-crossing alarm is cleared, the alarm generation and clearance values are displayed in the threshold information. **NOTE** The clearance value is displayed in the threshold information only when the threshold-crossing alarm is cleared.

For details about the parameters on the **Alarm Information** tab page, see **Table 2-12**.

Table 2-12 Description of the Alarm Information tab page

Tab Page	Description	Operation Method
Alarm Details	For details about alarm parameters, see . **NOTE** If the alarm reference is available, click the link next to **Causes and Suggestions** to switch to the alarm reference page.	To set the parameters to be displayed on the **Details** tab page, click **Select Fields** in the upper right corner of the **Details** tab page.
Handling and Experience	• On the **Handling** tab page, you can view alarm handling recommendations pre-configured in alarm management. • On the **Experience** tab page, you can view or modify alarm handling experience.	To modify the experience records, click **Experience**. On the tab page that is displayed, click **Modify**, record the experience, and then click **Save**.
Comments	On the **Comments** tab page, you can add comments for the alarm.	To modify comments, click **Modify** in the upper right corner of the tab page, enter comments, and then click **Save**.

Tab Page	Description	Operation Method
Handling Records in Last 2 Months	You can view all manual operations performed on the alarm in the last two months for O&M personnel to handle alarms.	-
Root Alarms/ Correlative Alarms	• If the reported alarm is a root alarm, the **Correlative Alarms** tab page is displayed. You can view its correlative alarms. • If the reported alarm is a correlative alarm, the **Root Alarms** tab page is displayed. You can view its root alarms. • If the reported alarm is a root alarm and a correlative alarm, the **Root Alarms** and **Correlative Alarms** tab pages are displayed.	-
Aggregated Alarm/ Original Alarms	• If the reported alarm is an aggregated alarm, the **Original Alarms** page is displayed. You can view the alarms that have been aggregated into this alarm. • If the reported alarm is an original alarm, the **Aggregated Alarm** tab page is displayed. You can view the alarm into which it has been aggregated.	-

For details about the parameters on the **Template Management** panel, see **Table 2-13**.

Table 2-13 Buttons on the Template Management panel

Button	Description	Operation Method
Search Template	You can search for a filter template based on the template name, name of the user who created the template, or comments.	1. On the **Quick Filter** panel, enter a template name, username, or comment in the search box. 2. Click to search the template.
Share/ Unshare	You can share or cancel the sharing of custom templates. You can also select a template shared by other users from the **Shared** area. The administrator can share or cancel the sharing of all templates except the default templates. Other users can only share or cancel the sharing of custom templates. • : The template is not shared. • : The template is shared.	1. On the **Quick Filter** panel, select the desired template. 2. Click the icon next to the template name.
Add to Favorites/ Remove from Favorites	You can add a template to or remove a template from your favorites. The favorite template will be displayed in the **Favorite** area. You can only perform the following operations on the preset templates: **Add to Favorites**, **Remove from Favorites**, **Set as Default Template**, or **Cancel Default Template**. • : The template is not added to favorites. • : The template is added to favorites.	
Set as Default Template/ Cancel Default Template	You can set or cancel the default template for the current page. Filtered alarms will be displayed based on the default template when you enter this page. The template marked with is the default template.	1. On the **Quick Filter** panel, select the desired template. 2. Click next to the template or click and choose **Set as Default Template** or **Cancel Default Template**.

Button	Description	Operation Method
Rename	Renames a filter template. The administrator can rename all the templates except the templates in the **Default** area. Other users can rename only custom templates.	1. On the **Quick Filter** panel, select the desired template. 2. Click on the right of the template. 3. Choose **Rename** from the displayed menu. 4. In the dialog box that is displayed, enter the new template name.
Modify Comments	Modifies the comments of a filter template. The administrator can modify the comments of all templates except the templates in the **Default** area. Other users can modify only the comments of the custom templates.	1. On the **Quick Filter** panel, select the desired template. 2. Click on the right of the template. 3. Choose **Modify Comments** from the displayed menu. 4. In the dialog box that is displayed, modify the comments.
Delete	Deletes a filter template. The administrator can delete all the templates except the templates in the **Default** area. Other users can delete only custom templates.	1. On the **Quick Filter** panel, select the desired template. 2. Click on the right of the template. 3. Choose **Delete** from the displayed menu.
Open Template on New Tab	A new tab page is opened and the list of the alarms or events that are filtered using the filter template is displayed on the new tab page.	1. On the **Quick Filter** panel, select the desired template. 2. Click on the right of the template, or click and choose **Open Template on New Tab**.

2.3.1.2 Handling Alarms

In alarm management, O&M personnel can perform operations on alarms, such as specifying a handler, acknowledging alarms, and clearing alarms, to facilitate troubleshooting.

Prerequisites

You have the following operation permissions: **Alarm Operation**, **Clear Alarm** and **Synchronize NE Alarms**.

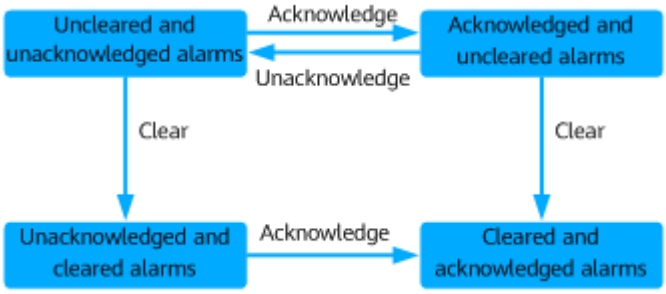
Context

Alarm management comprises the following alarm operations: acknowledging alarms, clearing alarms, changing alarm severities, and setting alarms to the invalid or maintenance state. **Table 2-14** describes alarm acknowledgement and clearance operations. **Figure 2-1** shows the relationships between alarm statuses.

Table 2-14 Alarm handling operations

Parameter	Function	Description
Acknowledge	Identifies the user who handles an alarm to avoid one alarm being handled by multiple users.	After an alarm is acknowledged, the alarm will be or has been handled. When the alarm is acknowledged, the alarm status is changed from unacknowledged to acknowledged. If you want another engineer to handle the alarm, you can unacknowledge the alarm. When the alarm is unacknowledged, the alarm status is changed from acknowledged to unacknowledged.
Clear	Identifies whether the fault that causes an alarm is rectified.	When a fault occurs on the interconnected NE or in the system, an alarm is generated. When the fault is rectified, a clear alarm is generated and the alarm is cleared. If the system fails to receive the clear alarm or the alarm cannot be automatically cleared due to a network fault, you need to manually clear the alarm. When you manually clear the alarm, an alarm clearance command is sent from alarm management, and then the corresponding NE or system clears the corresponding alarm.

Figure 2-1 Alarm status relationship



Based on the alarm acknowledgment and clearance status, alarms are classified into:

- Current alarms: include uncleared and unacknowledged alarms, acknowledged and uncleared alarms, and unacknowledged and cleared alarms. O&M personnel can monitor and handle alarms that they are concerned about on the **Current Alarms** page.
- Historical alarms: include alarms that have been cleared and acknowledged. Historical alarms are a data source for network performance optimization. O&M personnel can query and collect statistics on alarms.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Current Alarms** from the main menu.

Step 2 On the **Current Alarms** page, you can perform the following operations:

Operation	Scenario	Operation
Viewing alarm details	Obtains key alarm information, including alarm names, repair recommendations, and location information, to facilitate fault diagnosis and troubleshooting.	In the alarm list, select an alarm and click ⌄ below the list to view the alarm details.
Manually acknowledging an alarm	An acknowledged alarm indicates that the alarm is being handled by the user whose name is displayed in the **Acknowledged By** column. When the alarm is acknowledged, the alarm status is changed from unacknowledged to acknowledged.	You can select one or more alarms and click **Acknowledge** above the alarm list. You can also click ✓ in the **Operation** column of the row that contains the desired alarm. After you have acknowledged an alarm, the username is displayed in the **Acknowledged By** column.

Operation	Scenario	Operation
Specify a handler	Assigns the O&M personnel to handle an alarm.	In the alarm list, select an alarm and click ••• in the **Operation** column to select a user to handle the alarm. After the alarm is acknowledged, the username is displayed in the **Handler** column.
Manually clearing alarms	Some alarms cannot be automatically cleared. Therefore, you need to clear the alarms manually after the faults are rectified.	You can select one or more alarms and click **Clear** above the alarm list. You can also click in the **Operation** column of the row that contains the desired alarm. • If an alarm has been acknowledged after being cleared, the alarm will be moved to the **Historical Alarms** page. • If an alarm has not been acknowledged after being cleared, it is retained on the **Current Alarms** page, with a green background. **NOTE** The cleared alarm cannot be restored. Exercise caution when performing the operation.
Recording maintenance experience	After handling an alarm, the O&M personnel can record the handling experience for future reference in a timely manner. Choose **Device Management > Alarms Management > Alarm Settings** from the main menu. In the navigation pane, choose **Experience** to manage the experience records.	In the alarm list, select an alarm, click below the list, and click **Modify** in the **Experience** area.
Quick entries for setting alarm rules	O&M personnel can quickly set rules related to an alarm from the quick entries. Only authorized users can perform related operations. For details about the rules, see **Table 2-15**.	In the **Operation** column that contains a desired alarm, click ••• to select a rule to be set.

Table 2-15 Introduction to quick entries for rules

Rule	Description
Send Email Notification	The information about the selected alarms is immediately sent to O&M personnel by email. **NOTE** To send notifications to relevant personnel, you need to enter their personal information, such as mobile numbers and email addresses. You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the user's personal information is fully protected.
Send SMS Message Notification	The information about the selected alarm is immediately sent to the O&M personnel by SMS message. **NOTE** To send notifications to relevant personnel, you need to enter their personal information, such as mobile numbers and email addresses. You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the user's personal information is fully protected.
Set Masking Rule	You can set an alarm masking rule to mask alarms that you are not concerned about. The masked alarms will not be displayed on the **Current Alarms** page.
Set Identification Rule	After an identification rule is set, the system automatically sets a status identifier for the alarms that match the rule. When monitoring or querying alarms, you can set filter criteria to filter out the alarms. For example, you can set the alarms generated in commissioning scenarios to **Maintenance status**.
Set Notification Rule	The system automatically sends the information about alarms that meet the rule conditions to O&M personnel based on the notification method and content template set in the rule. In this way, the O&M personnel can learn about the alarm information and take corresponding measures in a timely manner.
Setting Intermittent/ Toggling Rule	After a rule is set, intermittent or toggling alarms can be discarded or masked to reduce interference caused by repetitive alarms.
Set Aggregation Rule	After an aggregation rule is set, the system automatically aggregates the repeated alarms reported within the specified period into one alarm.

----End

Parameter Description

Table 2-16 Buttons in the alarm operation bar

Button	Description
Auto Refresh	• Enable: Alarms on the current page are refreshed in real time. By default, alarms are refreshed every 3 seconds. • Disable: Locks the alarms on the current page. In this case, only the alarm information on the current page is updated. If other alarms are reported, the alarms are not displayed on the page.
Quick Filter	Displays selected alarms quickly.
Refresh interval	Changes the automatic refresh interval. When an alarm is reported to the NMS, the NMS obtains the alarm reporting frequency.
Combo Sorting	Sorts alarms by multiple alarm fields. A maximum of four alarm fields can be set.
Clear	When the fault that triggers an alarm is rectified but the alarm is not cleared automatically, click **Clear** to manually clear the alarm. After the alarm is cleared, its status is changed to **Cleared**.
Acknowledge/ Unacknowledge	After an alarm is acknowledged, the alarm will be or has been handled. When the alarm is acknowledged, the alarm status is changed from unacknowledged to acknowledged. If you want another engineer to handle the alarm, you can unacknowledge the alarm. When the alarm is unacknowledged, the alarm status is changed from acknowledged to unacknowledged.
Specify Handler	Specifies the user who handles the alarm. The specified handler is displayed in the **Handler** column. The options are as follows: **Myself**, **Other Users**, and **Cancel**.
Comment	Edits the comments of an alarm.
Export	Alarms can be exported to an .xlsx or .csv file. When the exported file format is set to .xlsx and the number of alarms exceeds 100,000, the file is exported as a .zip package. When the exported file format is set to .csv and the number of alarms exceeds 10,000, the file is exported as a .zip package. A maximum of five users can export some alarms at a time, and a maximum of two users can export all alarms at a time.

Button	Description
Set as Invalid/Set as Valid	Sets selected alarms as invalid alarms or valid alarms. When monitoring or querying alarms, you can set filter criteria to filter out such alarms, improving alarm handling efficiency. The O&M personnel can set alarms that they are not concerned about as invalid alarms.
Set as Under Maintenance/Set as Normal	Sets selected alarms to the maintenance or normal state. When monitoring or querying alarms, you can set filter criteria to filter out such alarms, improving alarm handling efficiency. For example, you can set the alarms generated in commissioning scenarios to **Maintenance status**.
Send Email Notification	Immediately sends information about the selected alarms to O&M personnel by email. **NOTE** To send notifications to relevant personnel, you need to enter their personal information, such as mobile numbers and email addresses. You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the user's personal information is fully protected.
Send SMS Message Notification	Immediately sends the information about the selected alarm to the O&M personnel by SMS message. **NOTE** To send notifications to relevant personnel, you need to enter their personal information, such as mobile numbers and email addresses. You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the user's personal information is fully protected.

2.3.2 Historical Alarms

By analyzing historical alarms, users can understand device running statuses and determine whether rules are properly configured.

Prerequisites

- By default, 20,000 historical alarms can be displayed. When the number of alarms exceeds the upper limit, the first 20,000 alarms are displayed based on the filter criteria and sorting. If you want to query other alarms, you can modify the filter criteria and sort the alarms.
- You can only monitor and view alarms of authorized MOs.
- A total number of 30 **Historical Alarms** pages can be opened concurrently by online users.

Procedure

1. Choose **Device Management** > **Alarm Management** > **Historical Alarms**.

2. On the **Historical Alarms** page, click **Filter** to expand the panel and set filter criteria to find desired historical alarms.
3. Click **Save** or **Save As** to save the current filter criteria as a filter template.

   You can click **Template Management** in the upper left corner of the page to view all filter templates and select a filter template from the **Quick Filter** panel. Users with the **Administrators** role can manage templates saved by all users.

   The following types of templates are provided:

   - **Favorite**: You can add the templates that you often use to your favorites.
   - **Custom**: Filter templates customized by the current user, which can be shared to other users.
   - **Shared**: Available filter templates shared by other users.
   - **Other**: Filter templates that are not shared by other users. These templates are visible only to users with the **Administrators** role.

   NOTE

   The filter templates on the **Current Alarms**, **Historical Alarms** pages are independent from each other and cannot be shared.
4. Export historical alarms. Alarms can be exported to an .xlsx or .csv file. When the export file format is set to .xlsx and the number of alarms exceeds 100,000, the file is exported as a .zip package. When the exported file format is set to .csv and the number of alarms exceeds 10,000, the file is exported as a .zip package.
   - Export some alarms: Select the alarms to be exported, click **Export**, and choose **Selected**.
   - Export all alarms: Click **Export** and choose **All**.

2.3.3 Masked Alarms

By analyzing masked alarms, users can understand device running statuses and determine whether rules are properly configured.

Prerequisites

- By default, 20,000 masked alarms can be displayed. When the number of alarms exceeds the upper limit, the first 20,000 alarms are displayed based on the filter criteria and sorting. If you want to query other alarms, you can modify the filter criteria and sort the alarms.
- You can create an alarm masking rule to mask alarms that you are not concerned about. The masked alarms will be displayed on the **Masked Alarms** page or discarded.
- Masked alarms are not deleted from the masked alarm list when the corresponding masking rules are disabled or deleted.
- You can only monitor and view alarms of authorized MOs.

Procedure

1. Choose **Device Management** > **Alarm Management** > **Masked Alarms**.
2. On the **Masked Alarms** page, click **Filter** to expand the panel and set filter criteria to find desired masked alarms.

3. Click **Save** or **Save As** to save the current filter criteria as a filter template.

   You can click **Template Management** in the upper left corner of the page to view all filter templates and select a filter template from the **Quick Filter** panel. Users with the **Administrators** role can manage templates saved by all users.

   The following types of templates are provided:

   - **Favorite**: You can add the templates that you often use to your favorites.
   - **Custom**: Filter templates customized by the current user, which can be shared to other users.
   - **Shared**: Available filter templates shared by other users.
   - **Other**: Filter templates that are not shared by other users. These templates are visible only to users with the **Administrators** role.

   NOTE

   The filter templates on the **Current Alarms**,**Historical Alarms**, **Masked Alarms** pages are independent from each other and cannot be shared.

4. Export masked alarms. Alarms can be exported to an .xlsx or .csv file. When the export file format is set to .xlsx and the number of alarms exceeds 100,000, the file is exported as a .zip package. When the exported file format is set to .csv and the number of alarms exceeds 10,000, the file is exported as a .zip package.
   - Export some alarms: Select the alarms to be exported, click **Export**, and choose **Selected**.
   - Export all alarms: Click **Export** and choose **All**.

2.3.4 Sync Alarm

You can manually create an alarm synchronization task on the NetEco to ensure that the alarms on the NetEco are consistent with the device alarms and quickly detect concerned alarms. If a device is disconnected from the NetEco and then reconnected to the NetEco again, you are advised to manually synchronize device alarms.

Prerequisites

You have the **Synchronize Alarms** operation rights.

Procedure

Step 1 Choose **Device Management** > **Alarm Management** > **Sync Alarm**.

Step 2 In the displayed **Sync Alarms** window, select the device name.

Step 3 Perform the following operations based on service requirements:

- Sync Current Alarms:Click **Sync Alarm**. Historical alarms can be synchronized only when the selected devices include controllers. You can select **Synchronize historical alarms simultaneously** as required, set the synchronization period, and click **OK** to deliver the synchronization task.
- Viewing synchronization tasks: Click **Query Task** to query the data of alarm synchronization tasks.

NOTE

The NetEco supports daily alarm synchronization. For details, contact technical support engineers.

----End

2.3.5 Alarm Setting

You can set alarm rules to customize alarm monitoring policies as required, improving troubleshooting efficiency.

2.3.5.1 Setting Colors for Alarms

You can set colors for different alarm or event severities to easily identify the concerned alarms or events.

Context

After the colors for alarms or events at different severities are set, the alarm indicator colors and the colors in the **Severity** column of the alarm list or event list are displayed in the configured colors.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Personalization** > **Color Settings**.

Step 3 On the **Color Settings** page, set the colors for alarm and events at different severities.

Step 4 Click **OK**.

----End

2.3.5.2 Setting Alarm Display Modes

When you need to identify alarms in different states more conveniently, you can set the alarm display mode as required to quickly identify concerned alarms.

Context

After the alarm display mode is set, the parameter in the **Severity** column in the alarm list or event list is displayed in the specified style. Alarms in different states are displayed in the specified background colors.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Personalization** > **Alarm Display Mode**.

Step 3 On the **Alarm Display Mode** page, set the mode and background colors for alarms and events in different states.

- **Icon**: Severity icon and parameter in the **Severity** column in the alarm list or event list. The colors of the severity icon are displayed by severity. The alarm background colors are displayed by state.
- **Column background**: In the alarm list or event list, the background colors of the parameters in the **Severity** column are displayed by severity. The alarm background colors are displayed by state.
- **Row background**: The background colors of the unacknowledged and uncleared alarms are displayed by severity, whereas the background colors of the alarms in other states are displayed by state. The alarm background colors are displayed by severity.

Step 4 Click **OK**.

----End

2.3.5.3 Setting Alarm Sounds

You can set different alarm sounds for alarm at different severities or specify alarm sound for different alarm names to facilitate alarm monitoring. When an alarm is generated, the sound box on your PC produces a corresponding sound.

Context

By default, four alarm sounds are provided: Critical/Sound by alarm name: Critical.mp3; Major: Major.mp3; Minor: Minor.mp3; Warning: Warning.mp3.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Personalization** > **Alarm Sounds**.

Step 3 On the **Alarm Sounds** page, set different sounds for alarms at different severities.

- Click  to listen to the selected sound file.
- Click  . In the **Custom Alarm Sound** dialog box that is displayed, upload, view, or delete a custom alarm sound file.
- Click  and select the alarms for **Sound by alarm name**. A maximum of 20 alarms can be selected.

Step 4 Set **Alarm Status** for alarms at different severities for which the system will play sounds.

When an alarm whose status is the specified one at the specified severity is reported or the status of an alarm changes to the specified status, the system plays the corresponding alarm sound.

Step 5 Set the duration for playing the alarm sound. When an alarm is reported, the corresponding alarm sound is automatically stopped after being played for the specified duration. At the same time, the alarm indicator keeps blinking for the specified duration even the alarm sound is muted. When all alarms at the severity

that trigger the corresponding alarm sound are cleared or acknowledged, the alarm sound and the blinking of the alarm indicator are stopped. When an alarm specified in **Sound by alarm name** is cleared or acknowledged, the alarm sound and the blinking of the alarm indicator are not stopped.

Step 6 Select whether to enable the sound setting. If the sound setting is disabled, the sound is not played when an alarm at the corresponding severity is reported.

Step 7 Click **OK**.

NOTE

When an alarm meets both the Sound by alarm name rule and the severity (Critical, Major, Minor, or Warning) rule, and both the rules are enabled, the alarm sound set in the sound by alarm name rule is played for the alarm.

----End

2.3.5.4 Setting Alarm Font Colors

You can set font colors for read and unread alarms to distinguish alarms.

Context

The newly reported alarms are all unread alarms.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Personalization** > **Font Colors**.

Step 3 Sets the font colors for read and unread alarms.

Step 4 Click **OK**.

----End

2.3.5.5 Highlighting Alarms

If alarms at a severity are not handled within the specified period of time, that is, the alarm status remains unchanged, the alarms are highlighted in the alarm list according to the highlight settings.

Context

- The highlight function takes effect only for current alarms.
- In the alarm list, the font color of the alarms that meet the highlight conditions is  .

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Personalization** > **Highlight**.

Step 3 On the **Highlight** page, set **Effective Time (min)** and **Alarm Status**. After an alarm at the severity is generated, the alarm is highlighted if the duration of the alarm in the specified status is greater than or equal to the specified effective time.

Step 4 Select whether to enable the function of highlighting alarms at the corresponding severity.

Step 5 Click **OK**.

----End

2.3.5.6 Monitoring Alarms Based on Emergency Maintenance Notification

You can view the alarms reported by the system and MOs. However, O&M personnel tend to first handle alarms reported by MOs that they managed, or they may ignore or handled some important alarms in a delayed manner because they are not familiar with the alarms reported by MOs. As a result, system exceptions occur. Therefore, alarm management provides **Emergency Maintenance Notification**. The **Emergency Maintenance Notification** dialog box is used to monitor alarms and remind O&M personnel to handle alarms in manner.

Prerequisites

An emergency maintenance notification template has been configured on the system, and the emergency maintenance notification function has been enabled on the PowerEcho page.

Context

- The **Emergency Maintenance Notification** panel can be displayed on any PowerEcho page.
- A maximum of five key alarms can be displayed on the **Emergency Maintenance Notification** panel.
- In addition to the system administrator, a maximum of 49 users can view the **Emergency Maintenance Notification** panel.
- The notification panel or  is displayed only when there are uncleared alarms that match the emergency maintenance notification template.

Procedure

Step 1 When alarms specified by **Emergency Maintenance Notification** are reported, the **Emergency Maintenance Notification** panel is displayed in the lower right corner of the page. If you clear the **Pop up when notification received** check box,  is displayed in the lower right corner of the page. You can click the icon to expand the notification panel.

Step 2 On the **Emergency Maintenance Notification** panel, view the key information about the alarms, such as the alarm name and alarm source.

Step 3 Click **Detail** to switch to the **Current Alarms** page. The alarms on the **Current Alarms** page are filtered by **Emergency Maintenance Notification**.

Step 4 Click an alarm name to view the alarm details and handle the alarm. Cleared alarms are not displayed on the **Emergency Maintenance Notification** panel.

----End

2.3.5.7 Setting Global Alarm Indicators

When you need to learn about the overall situation of alarms on all pages in real time and quickly open the alarm list page, you can enable the global alarm indicators. After this function is enabled, the alarm indicators on the current alarms page are displayed on all pages. You can use the alarm indicators to quickly open the current alarms page and filter alarms at a severity, facilitating alarm monitoring.

Context

- The settings take effect immediately, and remain valid on other clients after the current user logs in to them. However, the settings are invalid for other users.
- A maximum of 150 pages that have global alarm indicators can be opened at the same time.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Personalization** > **Global Alarm Indicators**.

Step 3 Enable or disable the global alarm indicators, and click **OK**.

----End

2.3.5.8 Configuring Masking Rules

You can set an alarm masking rule to mask alarms or events that you are not concerned about. New alarms or events meeting the masking rules will not be displayed on the **Current Alarms**, **Historical Alarms**, or **Event Logs** page. For example, when upgrading a device, you can set an alarm masking rule to mask alarms that require no attention.

Prerequisites

You have the following operation permissions: **Set Masking Rules**.

Context

- After a rule is created successfully, if **Alarm sources** is set to **All alarm sources** or **Event sources** is set to **All event sources** in the rule, only the users whose managed objects are **All Objects** can modify or delete the rule. Other users can only modify or delete the rule in which **Alarm sources** is set to **Custom alarm sources** or **Event sources** is set to **Custom event sources**.

- A rule is valid only to the alarms or events reported after the rule is enabled. Alarms meeting the conditions reported before the rule takes effect will not be masked, and alarms meeting the conditions reported after the rule takes effect will be displayed in the masked alarm list or discarded.
- The masking rules are used to mask alarms based on the redefined name attributes. If both name redefinition rule and masking rule are set for an alarm, the name redefinition rule will take effect before the masking rule takes effect.
- A maximum of 1000 masking rules can be created.
- If all of the following conditions are met, the masking rule will mask all alarms or events, and alarms or events cannot be reported.
  - The masking rule is enabled.
  - All alarm or event sources are selected in the masking rule.
  - All alarm or event severities are selected in the masking rule.
  - **Designated alarms** or **Designated events** is not selected, and advanced conditions are not set in the masking rule.
  - The time filter condition is not set in the masking rule.
- By default, the rules are sorted by the enabled and disabled states, and the rules in the same state are sorted by update time in descending order.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Masking Rules**.

Step 3 On the **Masking Rules** page, click **Create** and select **Alarm Masking Rules** or **Event Masking Rules**.

Step 4 In the **Basic Information** area, set the rule name, description, and whether to enable the rule.

Step 5 In the **Conditions** area, set the alarms or events to be masked, and their severities and alarm or event sources. Set advanced conditions to filter the alarms or events for the rule to take effect based on parameters.

NOTE

- **All alarm sources** or **All event sources** is available only for users whose managed objects are **All Objects**.
- In **Alarm sources** or **Event sources**, you can select **All alarm sources** or **All event sources** to mask the alarms or events that meet the conditions and are generated by the system and all MOs. Therefore, exercise caution when performing this operation.

Step 6 In the **Time Filter** area, set the time and period for the rule to take effect.

Step 7 In the **Action** area, set the handling policy for the masked alarms or events. Set **Masked alarms** to **Discard** or **Displayed on Masked Alarms**.

NOTE

- When an event masking rule is created, masked events can only be discarded.
- If **Discard** is selected, the alarms will not be displayed. Therefore, exercise caution when performing this operation.

Step 8 In the **Other** area, set the priority for the rule.

Step 9 Click **OK**.

----End

Related Tasks

- Deleting a rule: You can select a redundant rule from the rule list and click **Delete** to reduce the rule maintenance workload.
- Enabling/disabling a rule: You can select a rule that is not used temporarily from the rule list and click **Disable**. To use a disabled rule, select the rule and click **Enable**.
- Migrating rules: You can click **Export** on the rule page of the source system to export rules. Then, click **Import** in the target system to import the rule file exported from the source system to the target system.
- Backing up, collecting statistics on, and reviewing rules, and modifying rules in batches: You can click **Export** on the rule page to export rules and back up, review, and collect statistics on the rules. If you need to modify rules in batches, you can modify the rules in batches in the exported rule file. Then, click **Import** on the rule page to import the modified rule file.

Task Example

Scenario

O&M personnel plan to commission device A at 01:00 AM every Monday in April 20*XX*. Each commissioning is completed within two hours, during which services of device A are interrupted. Alarms generated during this period are predictable and do not need to be handled. You need to configure masking rules to mask these alarms.

Procedure

1. On the **Masking Rules** page, click **Create** and select **Alarm Masking Rules**.
2. In the **Basic Information** area, enter the rule name.
3. In the **Conditions** area, select **Custom alarm sources** and add device A to the custom alarm sources.
4. In the **Time Filter** area, set **By period** to **20*XX*-04-01 00:00:00** to **20*XX*-04-30 23:59:59**, set **By day** to **Mon**, and set **By time** to **01:00** to **03:00**.
5. In the **Action** area, set **Masked alarms** to **Displayed on Masked Alarms**.
6. Retain the default settings for other parameters.
7. Click **OK**.

Result

The alarms generated by device A from 01:00 AM to 03:00 AM every Monday in April 20*XX* are not displayed on the **Current Alarms**, **Alarm Logs**, and **Historical Alarms** pages. You can view the masked alarms on the **Masked Alarms** page.

Parameter Description

The following uses the parameters for creating an alarm rule as an example, and they are similar to those for creating an event rule.

Table 2-17 Parameters for creating an alarm masking rule

Item	Parameter	Description
Conditions	Alarms	• If you select **Designated alarms**, the rule takes effect only for the alarms you added. **Alarm ID** and **Group Name**: Unique identifiers of an alarm. • If you do not select **Designated alarms**, the rule takes effect for all alarms by default.
	Alarm sources	• **All alarm sources**: If this option is selected, the rule takes effect for the alarms generated by all alarm sources. • **Custom alarm sources**: If this option is selected, the rule takes effect only for the alarms of specified alarm sources.
	Advanced conditions	Restrictions on items such as location information and alarm source type. For example, if you want to filter alarms by location information, select **Location Info** and **contains** and enter the alarm location information in the text box.
Time Filter	By period	Time range within which the rule will take effect. By default, **Server time** is selected.
	By day	Days on which the rule takes effect in a week.
	By time	Period for the rule to take effect in a day.
Action	Masked alarms	• Displayed on the **Masked Alarms** page: The masked alarms will be displayed on the page opened by choosing **Service Monitor** > **Alarms** > **Masked Alarms** from the main menu. • **Discard**: Masked alarms will be deleted. If **Discard** is selected, the alarms will not be displayed. Therefore, exercise caution when performing this operation.
Other	Priority	Sets the priorities for alarm masking rules.
Change History	-	After a masking rule is created successfully, you can click a rule name and view the change history of the rule in the **Change History** area. This item is not displayed when you create a rule.

2.3.5.9 Configuring Intermittent/Toggling Rules

After the intermittent/toggling rule is set, the alarms that last for a short period of time or are frequently reported can be discarded or displayed on the **Masked Alarms** page to reduce interference caused by repetitive alarms.

Prerequisites

You have the following operation permissions: **Set Intermittent/Toggling Rules**.

Context

- A rule is valid only to the alarms reported after the rule is enabled.
- Before setting rules, you need to understand the following concepts:
  - Original alarm: The alarms that meet the conditions in the intermittent/toggling rules are original alarms.
  - Intermittent policy: When the interval between alarm generation and alarm clearance is less than a specific period, the alarm is considered as an intermittent alarm. The period is called intermittent period.
  - Toggling policy: When the number of times that an alarm (with the same alarm ID) is reported by the same alarm source in a specified period reaches the trigger condition, the toggling handling is started. You can set the action to generate a toggling alarm or avalanche alarm, or redefine the original alarm severity. When the number of times that the alarm is reported by the same alarm source in the specified period reaches the termination condition, the toggling handling is terminated. After the toggling ends, the generated toggling or avalanche alarm is automatically cleared. If the original alarms are not cleared, the last original alarm is reported.
- If the interval between the time when an alarm is generated and the time when the alarm is received is longer than 30 minutes, the alarm does not match the intermittent/toggling rule even if the alarm meets the conditions.
- A maximum of 1000 intermittent/toggling rules can be created.
- By default, the rules are sorted by the enabled and disabled states, and the rules in the same state are sorted by update time in descending order.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Intermittent/Toggling Rules**.

Step 3 On the **Intermittent/Toggling Rules** page, click **Create**.

Step 4 In the **Basic Information** area, set the rule name, description, and whether to enable the rule.

Step 5 In the **Conditions** area, set the alarm severities, alarms, and alarm sources for the rule to take effect. Set advanced conditions to filter the alarms for the rule to take effect based on alarm parameters.

Step 6 In the **Time Filter** area, set the time and period for the rule to take effect as required.

Step 7 In the **Analysis Type** area, select **Intermittent analysis** or **Toggling analysis** or both as required.

Step 8 In the **Intermittent Policy** and **Toggling Policy** areas, configure the policies.

- **Intermittent Policy**: Sets an intermittent period and action. For example, if the intermittent period is set to **30** and the policy action is set to **Discard**, the alarm is discarded when the interval between the generation and clearance of the alarm is less than 30 seconds.
  - **Period**: If the interval between the alarm generation time and alarm clearance time is less than the set period, the alarm meets the intermittent policy.
  - **Action**: The action for handling the alarm that meets the intermittent policy can be set to **Discard** or **Displayed on Masked Alarms**.
- **Toggling Policy**: Sets the toggling trigger condition, termination condition, and handling policy. The differences between toggling alarms and avalanche alarms are as follows:
  - Toggling alarm: A new alarm is generated. The alarm is identified as a toggling alarm. The alarm information is the same as that of an original alarm. You can set **Toggling Identifier** in the **Advanced settings** area on the filter panel to filter the alarms.
  - Avalanche alarm: ALM-132 Avalanche alarm is generated.

Step 9 In the **Other** area, set the priority for the rule.

Step 10 Click **OK**.

----End

Related Tasks

- Deleting a rule: You can select a redundant rule from the rule list and click **Delete** to reduce the rule maintenance workload.
- Enabling/disabling a rule: You can select a rule that is not used temporarily from the rule list and click **Disable**. To use a disabled rule, select the rule and click **Enable**.
- Migrating rules: You can click **Export** on the rule page of the source system to export rules. Then, click **Import** in the target system to import the rule file exported from the source system to the target system.
- Backing up, collecting statistics on, and reviewing rules, and modifying rules in batches: You can click **Export** on the rule page to export rules and back up, review, and collect statistics on the rules. If you need to modify rules in batches, you can modify the rules in batches in the exported rule file. Then, click **Import** on the rule page to import the modified rule file.

Task Example

Scenario

A minor alarm M lasts for a short period of time or is reported frequently. The cause may be that an NE or service switches between the normal state and the abnormal state repeatedly. To reduce the interference of such alarms, you can set an intermittent/toggling rule to handle the alarms using the following policies:

- Intermittent policy: If alarm M is reported and cleared within 30 seconds, this alarm is discarded.
- Toggling policy: If the number of times that alarm M is generated within 60 seconds is greater than 2, the toggling handling is triggered. If the number of times that alarm M is generated within 60 seconds is less than or equal to 0, the toggling handling is terminated.

Procedure

1. On the **Intermittent/Toggling Rules** page, click **Create**.
2. In the **Basic Information** area, enter the rule name.
3. In the **Conditions** area, select **Designated alarms**. Click **Add Alarm** and select **M**, which indicates that the intermittent/toggling rule is performed on alarm M. After the alarm M is displayed in **Selected**, click **OK**.
4. In the **Analysis Type** area, select **Intermittent analysis** and **Toggling analysis**.
5. In the **Intermittent Policy** and **Toggling Policy** areas, configure the policies.
   - **Intermittent Policy**: Set **Period (s)(T)** to **30** and **Action** to **Discard**.
   - **Toggling Policy**: Set **Period (s)(T1)** to **60** and **Generated alarms** to **2** for **Trigger condition**, **Period (s)(T2)** to **60** and **Generated alarms** to **0** for **Termination condition**, and **Handling policy** to **Generate a toggling alarm and discard original alarms generated after toggling**.
6. Click **OK**.

Result

If alarm M is cleared within 30 seconds after being reported, it is discarded. If the M alarm is reported frequently, the original alarms generated after the toggling policy is triggered are discarded and a new toggling alarm is generated.

2.3.5.10 Configuring Aggregation Rules

If alarms or events are reported repeatedly within a specified period, users can configure rules to aggregate them into one, thereby reducing interference. When monitoring or viewing alarms, you can select **Aggregated alarms** to filter out original alarms that have been aggregated and focus only on the alarms you need to handle.

Prerequisites

You have the following operation permissions: **Set Aggregation Rules**.

Context

- A rule is valid only to the alarms or events reported after the rule is enabled.
- In an aggregation rule, when the number of times that the same alarm or event (with the same alarm or event ID) is reported by the same NE in a specified period meets the trigger condition, an aggregation is triggered and a new aggregated alarm is generated. The alarms that meet all the conditions of the alarm aggregation rule are the original alarms. When an aggregated alarm is generated based on the rule, the correlative alarms are marked as original alarms. To view all original alarms, you can select **Original alarms** for **Associated alarm ID** when setting the filter criteria for current alarms.

- If an aggregated alarm generated based on the alarm aggregation rule is cleared, its correlative original alarms are cleared. If the original alarms are cleared, their correlative aggregated alarms are also cleared. To handle an aggregated alarm, handle the faults corresponding to the original alarms one by one.
- A maximum of 1000 custom aggregation rules can be created.
- By default, the rules are sorted by the enabled and disabled states, and the rules in the same state are sorted by update time in descending order.
- If the interval between the time when an alarm is generated and the time when the alarm arrives at the NMS is longer than 5 minutes, the alarm does not match the aggregation rule even if the alarm meets the conditions.
- On the page for creating an event aggregation rule, only the **Generate an aggregated alarm** and **Generate an aggregated alarm and mask all original events** options are provided in the **Aggregation Action** area. The information about the aggregated alarm generated based on the event aggregation rule is the same as that of an original event. The original events of the aggregated alarm cannot be viewed.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Aggregation Rules**.

Step 3 Create an aggregation rule.

1. On the **Aggregation Rules** page, click **Create**, and choose the desired rule type from the drop-down menu.
2. In the **Basic Information** area, set the rule name, description, and whether to enable the rule.
3. In the **Conditions** area, set the name, sources, and advanced conditions of the target alarm or event. If alarms or events reported by the selected alarm or event source meet the configured advanced conditions, aggregation analysis is performed.
4. In the **Aggregation Parameters** and **Aggregation Action** areas, set aggregation parameters and aggregation action. For details about the parameters, see **Table 2-18**.
5. Click **OK**.

----End

Related Tasks

- Deleting a rule: You can select a redundant rule from the rule list and click **Delete** to reduce the rule maintenance workload.
- Enabling/disabling a rule: You can select a rule that is not used temporarily from the rule list and click **Disable**. To use a disabled rule, select the rule and click **Enable**.
- Migrating rules: You can click **Export** on the rule page of the source system to export rules. Then, click **Import** in the target system to import the rule file exported from the source system to the target system.

- Backing up, collecting statistics on, and reviewing rules, and modifying rules in batches: You can click **Export** on the rule page to export rules and back up, review, and collect statistics on the rules. If you need to modify rules in batches, you can modify the rules in batches in the exported rule file. Then, click **Import** on the rule page to import the modified rule file.

Parameter Description

The following uses the parameters for creating an alarm rule as an example, and they are similar to those for creating an event rule.

Table 2-18 Parameters for creating an alarm aggregation rule

Item	Parameter	Description
Aggregation Parameters	Aggregation scope	**Intra-NE**: Aggregates alarms that are from the same alarm source and meet the conditions.
	Key parameters	Sets a location information matching condition. When the location information of reported alarms meet the condition, the system determines whether the alarms are aggregated. • **Specified property**: The condition is met when the values of properties in the location information of original alarms matches the settings in the condition. • **Full match**: The condition is met when the location information of original alarms is the same. **NOTE** Only the location information conditions can be set for **Key parameters**.
	Trigger condition	In a specified period, when the number of alarms that meet aggregation conditions is greater than or equal to **Generated alarms**, an aggregation is triggered.
	Termination condition	In a specified period, when the number of alarms that meet aggregation conditions is less than or equal to **Generated alarms**, the aggregation is terminated.

Item	Parameter	Description
Aggregation Action	Aggregation action	• **Generate an aggregated alarm**: A new aggregated alarm is generated, and the original alarms are marked as the original alarms and reported to the upper-layer NMS. • **Generate an aggregated alarm and mark all original alarms as correlative alarms**: A new aggregated alarm is generated, and all original alarms are marked as correlative alarms. • **Generate an aggregated alarm and mask all original alarms for NMS**: A new aggregated alarm is generated, and the original alarms are marked as the original alarms. In this case, the original alarms are not reported to the upper-layer NMS. • **Generate an aggregated alarm after aggregation and always display all original alarms on Masked Alarms**: All original alarms are displayed on the **Masked Alarms** page regardless of whether aggregation is triggered, and an aggregated alarm is generated after aggregation is triggered. • **Generate an aggregated alarm and discard all original alarms**: A new aggregated alarm is generated, and all original alarms are discarded. • **Generate an aggregated alarm and discard all original alarms after aggregation**: If a new aggregated alarm is generated, the original alarms reported after the aggregation are discarded. • **Report original alarms without aggregated alarms**: No aggregated alarms or original alarms are generated, and original alarms are not masked as original alarms. If this option is selected, you can customize the severity of original alarms in the **Original alarm settings** area.

Item	Parameter	Description
	Aggregated alarm settings	**Alarm sources**: • **NE**: Reports an aggregated alarm whose alarm source is NE. The location information of the aggregated alarm contains rule ID and original alarm information. Other information of the aggregated alarm is the same as that of an original alarm. • **OSS**: An aggregated alarm, **ALM-832 Parallel Alarm Exceeds the Limit**, whose alarm source is OSS is reported. **Reserved fields of Location Info**: After this parameter is set, the specified fields are displayed in the **Other Information** column of the aggregated alarm list. You can also customize some fields of an aggregated alarm, for example, customizing the severity.
	Original alarm settings	This option is displayed when **Report original alarms without aggregated alarms** is selected for **Aggregation action**. You can set the severity of original alarms.

2.3.5.11 Configuring Correlation Rules

If an alarm causes other alarms, you can use the correlation rule to define the correlation between alarms. When O&M maintenance personnel monitor or view alarms, they can set a correlation rule to filter out correlative alarms and focus only on root alarms.

Prerequisites

You have the following operation permissions: **Set Correlation Rules**.

Context

- A rule is valid only to the alarms reported after the rule is enabled.
- After the rule is enabled, the NetEco needs to analyze alarm relationships, which affects the time for reporting alarms to the NetEco.
- A maximum of 1000 custom correlation rules can be created.
- The default correlation rules can be enabled or disabled, but cannot be modified or deleted.
- If the interval between the time when an alarm is generated and the time when the alarm arrives at the NMS is longer than 5 minutes, the alarm does not match the correlation rule even if the alarm meets the conditions.

- By default, the rules are sorted by the enabled and disabled states, and the rules in the same state are sorted by update time in descending order.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Correlation Rules**.

Step 3 On the **Correlation Rules** page, click the **Default** tab. On the tab page that is displayed, check whether a rule meeting requirements exists.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 On the **Default** tab page, enable or disable rules as required.

Step 5 Create a custom correlation rule.

1. On the **Correlation Rules** page, click **Custom** and then click **Create**.
2. In the **Basic Information** area, set the rule name, description, and whether to enable the rule.
3. In the **Alarms** area, select root alarms and correlative alarms and set actions.
   - **Root alarms**: Alarm that causes multiple correlative alarms.
   - **Correlative alarms**: Alarm that is generated due to the root alarm.
4. In the **Conditions** area, click **Create** to create a correlation rule between the root alarm and the correlative alarms.
5. In the **Other** area, set the generation interval between the root alarms and their correlative alarms and the priority of the rule.

   A correlation is true only if the generation interval between the root alarm and the correlative alarm is shorter than or equal to the specified period.
6. Click **OK**.

----End

Related Tasks

- Deleting a rule: You can select a redundant rule from the rule list and click **Delete** to reduce the rule maintenance workload.
- Enabling/disabling a rule: You can select a rule that is not used temporarily from the rule list and click **Disable**. To use a disabled rule, select the rule and click **Enable**.
- Migrating rules: You can click **Export** on the rule page of the source system to export rules. Then, click **Import** in the target system to import the rule file exported from the source system to the target system.
- Backing up, collecting statistics on, and reviewing rules, and modifying rules in batches: You can click **Export** on the rule page to export rules and back up, review, and collect statistics on the rules. If you need to modify rules in batches, you can modify the rules in batches in the exported rule file. Then, click **Import** on the rule page to import the modified rule file.

Task Example

Scenario

When the connection of an NE is faulty, the NE reports alarm M periodically. At the same time, a large number of connection interruption alarms N are generated by this NE or other NEs because of the connection interruption. The type of alarm N is the same as that of alarm M. In this case, you only need to handle alarm M instead of alarm N. By setting a correlation rule, you can set the alarm N generated later than the alarm M to a correlative alarm.

Procedure

1. On the **Correlation Rules** page, click **Custom** and then click **Create**.
2. In the **Basic Information** area, enter the rule name.
3. In the **Alarms** area, set **Root alarms** to alarm M and **Correlative alarms** to alarm N.
4. In the **Conditions** area, click **Create**. Set the following condition: The occurrence time of alarm N is later than the occurrence time of alarm M. Click **OK**.
5. Click **OK**.

Result

When the occurrence time of alarm N is later than that of alarm M, alarm M is the root alarm of alarm N. In this case, choose **Current Alarms** from the main menu and open the **Filter** tab page. In the **Advanced settings** area, click **Associated Alarm ID**, and then set **Operator** to **is in** and **Value** to **Normal alarms** and **Root alarms**. After the query is started, the correlative alarm N is not displayed in the current alarm list. You only need to handle the root alarm M.

Parameter Description

Table 2-19 Parameters for creating a correlation rule

Item	Parameter	Description
Alarms	Root alarms	Alarm that causes multiple correlative alarms. The following actions can be selected for the root alarms, which are the operations performed on the root alarms when the alarms that meet the conditions are reported. • **None** • **Raise alarm severity by 1**

Item	Parameter	Description
	Correlative alarms	Alarms caused by the root alarm. The following actions can be selected for correlative alarms, which are the operations performed on correlative alarms when the alarms that meet the conditions are reported. • **Redefine severity as Critical** • **Redefine severity as Major** • **Redefine severity as Minor** • **Redefine severity as Warning** • **Discard** • **None**
Conditions	Including Location Info and Alarm Source Type	You can set conditions for each parameter.
	Comparison mode	Select a comparison mode. • **Value**: indicates that an alarm attribute is compared with a specified value. • **Alarm**: indicates that the attribute value of an alarm is compared with that of the other alarm.
Other	Period	Generation interval between the root alarm and its correlative alarms. When the period is less than or equal to the specified value, the selected root alarm and its correlative alarms form a root-correlative relationship.
	Priority	Priority for a rule to take effect.

2.3.5.12 Configuring Auto Acknowledgement Rules

When the number of current alarms reaches the threshold, the system processes the full current alarm cache and moves current alarms to the historical alarm list. To prevent the important alarms in the full current alarm list from being processed, the system automatically acknowledges the current alarms in the

cleared status based on an acknowledgement rule specified by users and converts them to historical alarms.

Prerequisites

You have the following operation permissions: **Set Auto Acknowledgement Rules**.

Context

- Auto acknowledgement rules take effect only for unacknowledged and cleared alarms. Alarms cleared before immediate acknowledgement is enabled are not affected.
- A maximum of 1000 auto acknowledgement rules are supported in the system. Four preset rules exist in the system and a maximum of 996 rules can be created.
- If an alarm complies with auto acknowledgement rules in both the delayed and immediate modes, the system acknowledges the alarm in immediate mode.
- By default, the rules are sorted by the enabled and disabled states, and the rules in the same state are sorted by update time in descending order.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Auto Acknowledgement Rules**.

Step 3 In the auto acknowledgement rule list, the first four rules are preset for automatically acknowledging alarms by severity. Check whether the rules already meet the requirements.

- If yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Enable an auto acknowledgement rule by alarm severity. For example, when the auto acknowledgement rule for major alarms is enabled, the cleared but unacknowledged major alarms will be acknowledged automatically.

In the auto acknowledgement rule list, the first four rules are preset. Only users who can manage all resources can enable or disable these rules.

1. Select the auto acknowledgement rule required based on the severity and click **Enable**.
2. In the **Mode** column, view the acknowledgement mode of the rule.
   - **Immediate**: indicates that alarms will be automatically acknowledged immediately after being cleared.
   - **Delayed**: indicates that alarms will be automatically acknowledged based on the settings in the **Change Delay** area after being cleared.

Step 5 Create a custom auto acknowledgement rule.

1. On the **Auto Acknowledgement Rules** page, click **Create**.

2. In the **Basic Information** area, set the rule name, description, and whether to enable the rule.
3. In the **Conditions** area, set the alarm severities, alarms, and alarm sources for the rule to take effect. Set advanced conditions to filter the alarms for the rule to take effect based on alarm parameters.

   NOTE

   All alarm sources is available only for users whose managed objects are **All Objects**.
4. In the **Other** area, set the acknowledgement mode for the rule.
5. Click **OK**.

Step 6 On the **Auto Acknowledgement Rules** page, click **Change Delay** and set the parameters. If the acknowledgement mode is set to **Delay**, the system automatically acknowledges alarms based on the configuration in the **Change Delay** area.

1. Click **Change Delay** and set **Execute at** and **Duration**.
2. Click **Apply**.

----End

2.3.5.13 Configuring Identification Rules

After an identification rule is set, the system automatically sets alarms that match the rule to the maintenance or invalid state. When monitoring or querying alarms, you can set filter criteria to filter out the alarms. For example, you can set the status of alarms generated during commissioning to **Maintenance** so that O&M personnel do not need to spend time on these alarms.

Prerequisites

You have the following operation permissions: **Set Identification Rules**.

Context

- A rule is valid only to the alarms reported after the rule is enabled.
- Before an identification rule takes effect, **Validity** is set to **Valid** and **Maintenance Status** is set to **NORMAL** by default. The **NORMAL** state corresponds to the **Normal** state.
- A maximum of 1000 identification rules can be created.
- By default, the rules are sorted by the enabled and disabled states, and the rules in the same state are sorted by update time in descending order.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Identification Rules**.

Step 3 On the **Identification Rules** page, click **Create**.

Step 4 In the **Basic Information** area, set the rule name, description, and whether to enable the rule.

Step 5 In the **Conditions** area, set the alarm severities, alarms, and alarm sources for the rule to take effect. Set advanced conditions to filter the alarms for the rule to take effect based on alarm parameters.

NOTE

All alarm sources is available only when the user can manage all resources.

Step 6 In the **Time Filter** area, set the time and period for the rule to take effect as required.

Step 7 In the **Action** area, select the status of alarms you want to identify.

Step 8 Click **OK**.

----End

Related Tasks

- Deleting a rule: You can select a redundant rule from the rule list and click **Delete** to reduce the rule maintenance workload.
- Enabling/disabling a rule: You can select a rule that is not used temporarily from the rule list and click **Disable**. To use a disabled rule, select the rule and click **Enable**.

Parameter Description

Table 2-20 Parameters for creating an identification rule

Item	Parameter	Description
Conditions	Alarms	• If you select **Designated alarms**, the rule takes effect only for the alarms you added. **Alarm ID** and **Group Name**: Unique identifiers of an alarm. • If you do not select **Designated alarms**, the rule takes effect for all alarms by default.
	Alarm sources	• **All alarm sources**: If this option is selected, the rule takes effect for the alarms generated by all alarm sources. • **Custom alarm sources**: If this option is selected, the rule takes effect only for the alarms of specified alarm sources.
	Advanced conditions	Restrictions on items such as location information and alarm source type. For example, if you want to filter alarms by location information, select **Location Info** and **contains** and enter the alarm location information in the text box.
Time Filter	By period	Time range within which the rule will take effect. By default, **Server time** is selected.

Item	Parameter	Description
	By day	Days on which the rule takes effect in a week.
	By time	Period for the rule to take effect in a day.
Action	Set alarm identity as	• **Maintenance status**: identifies the alarms generated due to NE commissioning or maintenance. • **Invalid**: identifies useless alarms that O&M personnel judge from previous experience. When monitoring or querying alarms, you can set filter criteria to filter out alarms that are in the **Maintenance** or that are **Invalid**.

2.3.5.14 Setting Alarm Name Groups

You can add multiple alarm or event names to a name group. When setting filter criteria for querying or collecting statistics on alarms or events, you can select a name group to perform operations on multiple alarms or events at a time.

Context

Only the users with the **Administrator** role can modify or delete all name groups. Other users can only modify or delete the name groups created by themselves.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Alarm/Event Name Group**.

Step 3 On the **Alarm/Event Name Group** page, click **Create** and select **Alarm Name Group** or **Event Name Group**.

Step 4 Set the name of the group.

Step 5 In the **Members** area, click **Add Alarm** or **Add Event**, select the alarms or events to be contained in the name group. After the alarms or events are displayed in **Selected**, click **OK**.

Step 6 Click **OK**.

----End

2.3.5.15 Configuring Unhandled Alarm Severity Rules

If some alarms that require special attention are not handled for a long time (that is, the alarms are not cleared or acknowledged for a long time), you need to raise the alarm severity. If some alarms that do not require special attention are not handled for a long time, you can lower the alarm severity. You can create

unhandled alarm severity rules to change the severity of alarms that are not handled within a specified period.

Context

- After a rule is enabled, it takes effect for the alarms reported before and after the rule is enabled.
- After the alarm severity is changed, the alarm severity displayed in the alarm list is the new one. However, when you select an alarm for other rules, the alarm severity displayed is still the original one.
- A maximum of 2000 unhandled alarm severity rules can be created.
- By default, the rules are sorted by the enabled and disabled states, and the rules in the same state are sorted by update time in descending order.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Unhandled Alarm Severity Rules**.

Step 3 On the **Unhandled Alarm Severity Rules** page, click **Create**.

Step 4 In the **Basic Information** area, set the rule name, description, and whether to enable the rule.

Step 5 In the **Conditions** area, set the alarm name, alarm ID, group name, and alarm status.

Step 6 In the **Handling Policy** area, set **Trigger condition** and **Action**.

Step 7 In the **Other** area, set the priority for the rule.

Step 8 Click **OK**.

----End

Related Tasks

- Deleting a rule: You can select a redundant rule from the rule list and click **Delete** to reduce the rule maintenance workload.
- Enabling/disabling a rule: You can select a rule that is not used temporarily from the rule list and click **Disable**. To use a disabled rule, select the rule and click **Enable**.

2.3.5.16 Configuring Notification Rules

O&M personnel cannot browse alarms or events on the alarm management page when they are out of office, for example, during off-work hours or business trips. Notification rules enable O&M personnel to receive SMS or email notifications about concerned alarms or events so that they can handle alarms in real time.

Prerequisites

- You have completed the notification configuration. The navigation path is as follows: Choose **System** > **System Settings** > **Notifications** from the main menu.
- You have the following operation permissions: **Set Notification Rules**.

Context

- Notifications by email and SMS message are sent through third-party servers and devices. Therefore, the sending capability (such as the delay when the notifications arrive) varies with the third-party servers and devices.
- The delay time cannot be set on the page for creating an event notification rule.
- By default, the rules are sorted by the enabled and disabled states, and the rules in the same state are sorted by update time in descending order.
- A maximum of 1000 notification rules can be created.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Notification Rules**.

Step 3 On the **Notification Rules** page, click **Create** and select **Alarm Notification Rules** or **Event Notification Rules**.

Step 4 In the **Basic Information** area, set the rule name, description, and whether to enable the rule.

Step 5 In the **Conditions** area, set the severities, alarm status, alarms or events, and alarm or event sources for the rule to take effect. Set advanced conditions to filter the alarms or events for the rule to take effect based on the parameters.

NOTE

All alarm sources or **All event sources** is available only for the users who can manage all resources.

Step 6 In the **Time Filter** area, set the time and period for the rule to take effect as required.

Step 7 Set the notification method and content, recipient time zone, and recipients. When the alarms set in the rule are reported, the system sends notifications to users of specified groups by email or SMS message. **Table 2-21** describes the parameters for creating a notification rule.

NOTE

To send notifications to relevant personnel, you need to enter their personal information, such as mobile numbers and email addresses. You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the user's personal information is fully protected.

Step 8 Click **OK**.

----End

Related Tasks

- Deleting a rule: You can select a redundant rule from the rule list and click **Delete** to reduce the rule maintenance workload.
- Enabling/disabling a rule: You can select a rule that is not used temporarily from the rule list and click **Disable**. To use a disabled rule, select the rule and click **Enable**.
- Migrating rules: You can click **Export** on the rule page of the source system to export rules. Then, click **Import** in the target system to import the rule file exported from the source system to the target system.
- Backing up, collecting statistics on, and reviewing rules, and modifying rules in batches: You can click **Export** on the rule page to export rules and back up, review, and collect statistics on the rules. If you need to modify rules in batches, you can modify the rules in batches in the exported rule file. Then, click **Import** on the rule page to import the modified rule file.

  NOTE

  When the notification rules are exported, the email addresses and phone numbers of the recipient users are exported. You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the user's personal information is fully protected.

Parameter Description

The following uses the parameters for creating an alarm rule as an example, and they are similar to those for creating an event rule.

Table 2-21 Parameters for creating a notification rule

Item	Parameter	Description
Conditions	Alarms	• If you select **Designated alarms**, the rule takes effect only for the alarms you added. **Alarm ID** and **Group Name**: Unique identifiers of an alarm. • If you do not select **Designated alarms**, the rule takes effect for all alarms by default.
	Alarm sources	• **All alarm sources**: indicates that this rule takes effect for the alarms generated by all alarm sources. • **Custom alarm sources**: indicates that this rule takes effect only for the alarms of specified alarm sources.

Item	Parameter	Description
	Advanced conditions	Restrictions on items such as location information and alarm source type. For example, if you want to filter alarms by location information, select **Location Info** and **contains** and enter the alarm location information in the text box.
Time Filter **NOTE** By default, the rule takes effect at any time.	By period	Time range within which the rule will take effect. By default, **Server time** is selected.
	By month	Month for the rule to take effect in a year.
	By day	Days on which the rule takes effect in a week.
	By time	Period for the rule to take effect in a day.
Notification Method	Email	Indicates that notifications will be sent by email. You need to select a notification template.
	SMS message	Indicates that notifications will be sent by SMS message. You need to select a notification template.
	Delay (min)	Indicates that you can set the delay time for sending a notification. The system records the time when the alarm arrives at the alarm management system. If the alarm is cleared within the delay time after the alarm arrives at the system, no notification is sent. Otherwise, the notification is sent.
Recipient Time Zone	Recipient time zone	Indicates the time zone of the user who receives the notification. When the time zone of the recipient is different from that of the server, the alarm generation time in the notification is converted based on the time zone of the recipient. The daylight saving time (DST) is not supported.
Recipient Groups	Recipient groups	Sets the user groups for receiving the notification.

2.3.5.17 Configuring Notification Templates

When the default notification template does not meet your requirements, you can create a notification template and use it when configuring notification rules. The system fills the alarm information in an email or SMS message based on the notification template and sends the email or SMS message to related users.

Prerequisites

You have the following operation permissions: **Set Notification Rules**.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Notification Templates**.

Step 3 On the **Notification Templates** page, click **Create**.

Step 4 In the **Basic Information** area, enter the template name and description.

Step 5 In the **Notification Method and Content** area, select **Email** or **SMS message** as the notification method, and set the important information of the notification, such as, severity, name, and occurrence time.

- If you select **New alarms + new cleared alarms** for **Subtitle**, a notification email can contain multiple alarms or events. The maximum size of an email is 2 MB. If the size of an email exceeds the maximum size, the email is split into multiple emails. When you create a notification rule, an email can contain a maximum of 200 alarms or events. If **Delay (min)** is set in the rule, the number of alarms in an email is not limited to 200.
- If you deselect **New alarms + new cleared alarms** for **Subtitle**, only one alarm or event is sent in a notification email.

NOTE

The contents in black in the template are fixed fields displayed in emails or SMS messages. Users can modify them as required. The contents in blue show alarm information and vary depending on alarms. You can add the contents in blue by selecting the labels below rather than manually editing them.

The meaning of **Occurred** varies in the following scenarios:

- Generally, when an alarm is reported, this parameter refers to the report time, corresponding to the **First Occurred** field on the **Current Alarms** page.
- When a merged alarm is reported, this parameter refers to the report time of the merged alarm, corresponding to the **Last Occurred** field on the **Current Alarms** page.
- When an alarm clear notification is sent, this parameter refers to the time when the alarm is generated, corresponding to the **Last Occurred** field on the **Alarm Logs** page.

Step 6 Click **OK**.

----End

2.3.5.18 Managing Handling Experience

After handling an alarm, record the handling experience to the handling experience database for future reference or guidance.

Prerequisites

You have the **Record Experience** permission**.**

Context

- The handling experience on the **Alarm Settings** > **Experience** page is the same as that in the alarm details.
- A maximum of 10,000 experience records can be created.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Experience**.

Step 3 On the **Experience** page, click **Create**.

Step 4 Select the alarm whose handling experience needs to be created. If the page about the corresponding alarm reference exists for the alarm, a link to the alarm reference is provided next to the alarm name. **Table 2-22** describes parameters for creating handling experience.

Step 5 Enter experience.

Step 6 Click **OK**.

----End

Related Tasks

You can import or export alarm handling experience for statistics, review, and migration. On the **Experience** page, click **Export** or **Import** to export or import experience.

Parameter Description

Table 2-22 Parameters for creating experience

Parameter	Description
Alarm name	Name of an alarm.
Alarm ID	ID of an alarm.
Group name	Alarm group ID, which is assigned by NEs or devices that report alarms.

2.3.5.19 Setting the Current Alarm Threshold Warning

When the number of current alarms reaches the maximum capacity, the system moves some current alarms to the historical-alarm list based on the full-cache processing rule. To prevent important alarms from being moved to the historical-alarm list, you can set a threshold for current alarms. When the number of current alarms reaches a specified threshold, an alarm is reported to prompt users to handle the current alarms.

Prerequisites

Only users with the **Administrators** role can set the current alarm threshold warning.

Context

To prevent excessive current alarms from deteriorating system performance, alarm management provides a full-alarm processing rule. When the number of current alarms in the database reaches the upper threshold, alarm management applies the following rules to move some alarms to the historical alarm list until the number of alarms falls to 90% of the upper threshold.

- Alarms are moved to the historical-alarm list in the following sequence: cleared alarms, acknowledged and uncleared ADMC alarms, acknowledged and uncleared ADAC alarms, and unacknowledged and uncleared alarms.
- For alarms of the same type, the earlier alarms are moved to the historical alarm list first.
- In a distributed system, when the NE alarms are reported to different nodes and the processing of the full current alarm cache is triggered, the alarms are moved to the historical alarm list in descending order of the node alarm quantity. The more alarms are reported to a node, the higher the priority of the node is. For example, if an NE is connected to node A and node B, and the alarm quantity on node A is more than node B, the processing of the full current alarm cache is performed only on node A.

Procedure

Step 1 Choose **Device Management** > **Alarms Management** > **Alarm Settings** from the main menu.

Step 2 In the navigation pane, choose **Current Alarm Threshold Warning**.

Step 3 Select whether to send an alarm when the number of current alarms reaches the threshold and set the thresholds for generating and clearing alarms.

- **Generation threshold**: When the ratio of the number of current alarms to the maximum capacity is greater than or equal to the specified threshold, ALM-157 The Number of Current Alarms Reaches the Threshold is generated.
- **Clearance threshold**: When the ratio of the number of current alarms to the maximum capacity is less than the specified threshold, ALM-157 The Number of Current Alarms Reaches the Threshold is cleared. The clearance threshold cannot be higher than the generation threshold.

Step 4 Click **Apply**.

----End

2.3.5.20 Redefine Alarm

To quickly search for and handle key device alarms to which you pay special attention, you can redefine these alarms. The NetEco provides five types of alarm redefinition rules: redefine alarm name, redefine alarm type, redefine alarm severity, redefine alarm causes and redefine handling suggestions.

Table 2-23 description of the function of redefining alarms.

Table 2-23 Function of Redefining Alarms

Task Description	Operation entry	Procedure
Configuring Redefinition Alarms	1. Choose **Device Management** > **Alarm Management** > **Alarm Settings**. 2. In the navigation tree on the left, choose **Redefine Alarm**. 3. Set search criteria to filter alarm data.	1. In the device tree and select a target device. 2. Click the operation column  . 3. Enter the redefinition alarm information according to the actual situation, and then click **OK** . **NOTE** After saving redefinition alarms, the redefined alarm status is changed to enabled after the synchronization is complete.
Clearing Redefining Alarm Rules **NOTE** After saving redefinition alarms, the alarm redefinition rule can be cleared.		Use either of the following methods to clear redefinition alarms: • On the **Redefine Alarm** page, Click  in the row where the indicator to be cleared is located. • On the **Redefine Alarm** page, Select the target data to be cleared and click **Clear** above the page.

Task Description	Operation entry	Procedure
Enabling or disabling Redefining Alarm Rules		Use either of the following methods to enable or disable redefinition alarms: • On the **Redefine Alarm** page, click  or  the row of the target data row to be enabled. • On the **Redefine Alarm** page, select the target data for which redefinition alarm rules need to be enabled, click **Enable** or **Disable** in the upper part of the page.
Refresh the redefined alarm		On the **Redefine Alarm** page, click **Refresh** in the upper part of the page to refresh the redefined alarm page.
Batch Redefinition Rule Application		On the **Redefine Alarm** page, click  in the operation column for the target alarm in the active alarm list to apply alarm rules configured specified in the alarm rule to other rules in batches.

Task Description	Operation entry	Procedure
Batch Apply to Devices		1. Select a target device from the device tree. • If you need to apply a specified alarm rule to alarms of other devices of the same type, select the alarm rule record and click **Batch Apply to Devices**. On the displayed page, select **Selected** for **Selected items**. • If you need to apply all alarm rules of the target device to alarms of other devices of the same type, click **Batch Apply to Devices**. On the displayed page, select **Select All** for **Selected items**. 2. Set the application items and application scope. • If you need to apply a specified alarm rule of the target device to the alarms of all devices of the same type, select **All Objects** for **Application scope**. • If you need to apply a specified alarm rule of the target device to the alarms of specified devices of the same type, select **Custom** for **Application scope** and select the

Task Description	Operation entry	Procedure
		devices to which the alarm rule is to be applied in the management domain area. 3. Click **OK**.

2.3.5.21 Threshold Alarm

This section describes the management of thresholds. When managing site components, you can customize threshold alarms for some key counters. You can set multiple threshold ranges for the same counter based on the alarm severity, including critical, major, minor, and warning.

Prerequisites

You have the operation rights for **Set Threshold Rules**.

Context

- You can set performance counter thresholds for certain components of NEs.
- The thresholds can be set based on the alarm severity, including **Critical**, **Major**, **Minor**, and **Warning**.
- After the threshold rule is set, the rule is enabled by default.
- After the file is exported, you can edit rules locally. Multiple rules correspond to one alarm name. The rule upper or lower thresholds are displayed in one rule. If one rule corresponds to one alarm name, you are advised to copy and insert the current signal data. The rule upper or lower thresholds are displayed in two rules.

Procedure

Step 1 Choose **Device Management** > **Alarm Management** > **Alarm Settings**.

Step 2 In the navigation tree on the left, click the **threshold alarm**.

Step 3 In the device tree and select a target device, choose **Real-Time Signals**, **Statistics Signals** or **Custom Signals**.

Step 4 Click  in the **Operation** column of the target data. The **Set Rule** dialog box is displayed.

Step 5 Set the alarm name.

- If multiple rules correspond to one alarm name, enter **Alarm Name.**
- If one rule corresponds to one alarm name. Click  to enable the customized threshold setting.

Step 6 Select the threshold rule and set the rule parameters and duration. For details about parameters, see **Table 2-25**.

Step 7 Click **OK**.

Table 2-24 Operations related to threshold rules

Tasks	Operation
Clear a threshold rules	Use either of the following methods to clear a threshold alarm: • Click  for the counter whose threshold alarm needs to be cleared. • Select the counter whose threshold alarm needs to be cleared, and click **Clear** in the upper part of the page.
Enable or disable a threshold rules	Use either of the following methods to enable a threshold alarm: • Click  or  for the counter whose threshold alarm needs to be enabled. • Select the counter whose threshold alarm needs to be enabled, and click **Enable** or **Disable** in the upper part of the page.
Customize threshold rules **NOTE** You can custom threshold alarms only the **Custom Signals** tab page.	1. Click **Advanced** and set Signal Name and Expression. 2. Click **Next.** 3. Set the alarm name. – If multiple rules correspond to one alarm name, enter **Alarm Name.** – If one rule corresponds to one alarm name. Click  to enable the customized threshold setting. 4. Select the threshold rule and set the rule parameters and duration. For details about parameters, see **Table 2-25**. 5. Click **OK**.
Deleting Customized Signals and Counters **NOTE** You can delete a custom counter only the **Custom Signals** tab page.	1. Delete a custom counter. – Click  in the row that contains the custom counter to be deleted. – On the current page, select the custom counters to be deleted and click **Clear** in the upper part of the page. 2. In the displayed dialog box, click **OK**.

Tasks	Operation
Batch Apply to Counters	In the **Threshold Alarm** window, click  in the Operation column for the target alarm in the active alarm list to apply the threshold conditions specified in the rule to other alarm rules with the same type of threshold condition. **NOTE** Meaning of the same type of threshold condition: • If the threshold condition of a selected rule is of the numeric type, the rule can only be batch applied to the rules whose threshold condition is the numeric type. • If the threshold condition of a selected rule is of the enumerated type, the rule can only be batch applied to the rules whose threshold condition is the enumerated type.
Batch Apply to Devices	In the **Threshold Alarm** window, click **Batch Apply to Devices** below the active alarm list to apply the selected alarm rules to other devices in batches. **NOTE** You can select either of the following options for batch application: • All objects: The rules are applied to all existing and future devices of the same type. • Custom: The rules are applied to devices of the same type under the current root node. Rules for applying an empty rule: for two devices of the same type, if the threshold condition content in a rule of one device is not set, and the rule is applied to the other device's rule for which the threshold condition content has been set, the threshold condition content set for the rule of the other device will be cleared.
Exporting data	1. Click **Export**. 2. In the displayed dialog box, select export range and export data. 3. Click **OK**.
Importing data	1. Click **Import**. 2. In the displayed dialog box, click **Upload**. 3. In the **Upload** dialog box, click the file to be uploaded. 4. Select a local file and click **OK**.
Refresh threshold alarms	In the **Threshold Alarm** window, click **Refresh** in the upper part of the page to refresh threshold alarms.

Table 2-25 Parameters for setting performance counter thresholds

Parameter	Description
Alarm name	Name of a threshold alarm. After **Alarm name** is selected, corresponding threshold alarms can be generated when performance counter measurement results meet alarm triggering conditions. You can set the alarm name as required.
Upper Threshold for *XX* Alarm	Upper threshold for a performance counter, which can be set as required. *XX* indicates the alarm severity. If the measured performance counter is greater than or equal to the upper-threshold, an alarm of the corresponding severity is generated. The value of this parameter must meet the following conditions: ● The value for triggering an upper-threshold alarm is greater than that for clearing the upper-threshold alarm. ● The value for triggering a high-level upper-threshold alarm is greater than that for triggering a low-level upper-threshold alarm.
Lower Threshold for *XX* Alarm	Lower threshold for a performance counter, which can be set as required. *XX* indicates the alarm severity. If the measured performance counter is less than or equal to the lower threshold, a lower-threshold alarm of the corresponding severity is generated. The value of this parameter must meet the following conditions: ● The value for triggering a lower-threshold alarm is less than or equal to the one for clearing the lower-threshold alarm. ● The value for triggering a high-level lower-threshold alarm is less than that for triggering a low-level lower-threshold alarm.
Condition for Clearing Upper	Threshold for clearing an upper-threshold alarm, which can be set as required. If the measured performance counter is less than or equal to this threshold, the upper-threshold alarm of the corresponding severity is cleared. The value for clearing an upper-threshold alarm must be less than or equal to the one for triggering the upper-threshold alarm.
Condition for Clearing Lower	Threshold for clearing a lower-threshold alarm, which can be set as required. If the measured performance counter is greater than or equal to this threshold, the lower-threshold alarm of the corresponding severity is cleared. The value for clearing a lower-threshold alarm must be greater than or equal to the one for triggering the lower-threshold alarm.

Parameter	Description
Duration	Duration refers to the time at which the threshold condition needs to be reached continuously for generating an alarm for a signal. If the value of a signal reaches the threshold condition continuously within that time specified by this parameter, a corresponding threshold alarm is generated. If the duration is 10s, the corresponding threshold alarm is generated when all signals reach the threshold within 10s.

----End

2.4 Predefined Big Screen

2.4.1 Predefined Big Screen

The predefined big-screen monitoring function allows users to display monitoring services such as topologies on high-resolution screens, facilitating the display of monitoring information and IT O&M effects of multiple smart modules.

Prerequisites

- You have the operation rights of **View**, **Predefined Screen** and **Predefined Screen Setting**.
- You have the operation rights of **View**, **Single Line**, **Chiller Group Control**, **Energy Analysis**, and **View Access Control Events**.
- You have the management domain permissions for equipment rooms, outlets, and containers.

Procedure

Step 1 Choose **Device Management** > **Big Screen Monitor** > **Predefined Big Screen**.

Step 2 Select the equipment room for which you want to set the predefined big screen.

1. Click  in the upper part of the navigation tree.
2. In the displayed dialog box, select the equipment room for which you want to set the predefined big screen.

   NOTE

   Only one predefined big screen can be created for an equipment room.
3. Click **Yes**.

Step 3 Set the company name and logo, and predefine the greetings and display time format on the big screen.

1. Click  in the upper left corner to set the company name and logo.
2. Click  above the topology to set the predefined big screen greeting.

3. Click  in the upper right corner to set the time format.

Step 4 Set the service type and equipment room view display mode.

1. Click  in the upper right corner of a service in the monitoring view to set the service data type.

   NOTE

   - You must have the operation rights of **Energy Analysis** to view **PUE**, **Power Consumption Comparison**, and **Power Consumption Trend**.
   - You must have the operation rights of **View Access Control Events** to view **Access Event**.
   - You must have the operation rights of **View** to view **Alarm Information**.

2. Click  in the upper right corner of the topology to select the view display mode, and determine whether to show or hide the single-line electrical diagram and chiller group control. When **Choose View Mode** is set to **3D**, you can perform operations in **Table 2-26**.

   NOTE

   You must have the operation rights of **View**, **Single Line**, and, **Chiller Group Control** to view the 2D, 2.5D, and 3D topology views, single-line electrical diagrams, and chiller group control diagrams.

Table 2-26 view operation tasks

Operation	Description	Procedure
Adjusting views	Adjust the view effect to stay in the optimal view.	Zoom and rotate the view.
View details about the smart module in the equipment room.	The 3D view supports the drill-down function to view details about smart modules in the equipment room.	Double-click the smart module or device to be viewed to drill down, and right-click to return to the previous layer.
Viewing the space, power distribution, and cooling capacity of a cabinet	Display the space, power distribution, and cooling capacity of each cabinet in 3D mode.	Select **Power**, **Cooling** or **Space** on the right of the view.
Setting wall display status	Make equipment room walls transparent to highlight information about other devices in the equipment room.	Select **Transparent** on the right of the view.

Operation	Description	Procedure
Setting the Device Display Status	The sensors and cameras connected to the equipment room are displayed in the 3D topology.	Select **Device Location** on the right of the view, and then click the button for displaying the device.

3. View KPIs of key devices in the lower part of the topology.

Step 5 Click **Save**.

Step 6 In the displayed dialog box, enter the name of the predefined big screen and click **OK**.

----End

Follow-up Procedure

In the navigation tree on the left, choose a predefined big screen and perform the following operations:

If You Need to...	Then...
Modify the unit screen name.	Click  . When the status becomes editable, you can modify the unit screen name.
Delete a unit screen.	Click  to delete a predefined big screen.

3 O&M Management

You can learn about the running status of all sites.

3.1 Availability Management
The NetEco provides the site report function to allow you to learn about the running status of all sites in real time and analyze and handle problems in the sites.

3.2 Security
The NetEco provides functions such as access control management and video management to ensure physical security of devices and environments and help you detect and handle exceptions in a timely manner.

3.1 Availability Management

The NetEco provides the site report function to allow you to learn about the running status of all sites in real time and analyze and handle problems in the sites.

3.1.1 Viewing a DC Report

This function allows you to view a DC report, including the overview, DC statistics, and alarm statistics.

Procedure

Step 1 Choose **Maintenance Management** > **Availability Management** > **Net DC Report**.

Step 2 On the **DC Report** page, view the overview, DC statistics, and alarm statistics.

In the **Alarms** area, click the alarm rectangle to go to the **Current Alarms** page to view detailed alarm information. For details about how to handle alarms, see **2.3.1.2 Handling Alarms**.

----End

3.2 Security

The NetEco provides functions such as access control management and video management to ensure physical security of devices and environments and help you detect and handle exceptions in a timely manner.

3.2.1 Access Control Management

The access control management module configures and manages access control devices and monitors access events to control and audit access rights, improving the security management capability of each management domain.

3.2.1.1 Managing Access Control Devices

You can create access control devices and remotely open and close the door of an access control device to effectively manage the access control device.

Prerequisites

You have the operation rights for **Access Control Management**.

Procedure

Step 1 Choose **Maintenance Management** > **Security Protection** > **Access Control Management**.

Step 2 In the navigation tree on the left, choose **Device Management** and perform the following operations based on the scenario.

Table 3-1 Managing access control devices

Operation	Description	Procedure
Creating an access control device	Before managing access control devices, you need to connect the access control devices to the NetEco.	1. Click **Create**. 2. On the **Planning Configuration** page, create an access control device. For details, see **1.4.2 Adding a Device Through Automatic Discovery**. After an access control device is created successfully, you can view the device on the **Device Management** page.

Operation	Description	Procedure
Remotely opening a door	You can remotely open a door under an access controller.	Click  in the **Operation** column. **NOTE** The door is automatically closed within 6 seconds after the door is remotely opened.
Remotely closing a door	You can remotely close a door under an access controller.	• Remotely closing a single door Click  in the **Operation** column. • Remotely closing doors in batches Click **Remotely close door(s) in batches**.

----End

3.2.1.2 Managing Access Control Events

You can query the access records and event records of a specified access control device within a specified time range, and export the query results to a PC for storage.

Prerequisites

You have the operation rights for **Access Control Management**.

Procedure

Step 1 Choose **Maintenance Management** > **Security Protection** > **Access Control Management**.

Step 2 In the navigation tree, choose **Access Event**.

Step 3 Select an access control device, set the search criteria, and click **Search**.

- **Access Records**: users' door opening/closing records on the device side
- **Event Records**: all event records related to devices, including door opening/closing records and door open alarm records

By default, the access records or event records of all access control devices within 24 hours on the current day are displayed. To export access records or event records, click **Export**.

NOTE

- If the event records on the NetEco are inconsistent with those on the device, you can click **Sync Log** to synchronize the log information on the device to the NetEco.
- For card swiping on an access controller, the card number, user name, and user ID are recorded for a valid card, and only the card number is recorded for an invalid card.

----End

3.2.2 Video Management

The video management module provides functions such as camera management and parameter setting.

3.2.2.1 Managing Cameras

You can view camera details, create cameras, and play videos.

Prerequisites

- You have the operation rights for **Camera Management**.
- Before playing videos from cameras managed by the video subsystem, you need to set video playback parameters. For details, see **6.5 How Do I Set Video Playback Parameters on the Video Surveillance Subsystem?**.

Procedure

Step 1 Choose **Maintenance Management** > **Security Protection** > **Camera Management**.

Step 2 In the navigation tree on the left, choose **Camera Information**.

Step 3 On the **Camera Information** page, you can perform operations as required.

- Viewing camera information

  The detailed information about all cameras is displayed.

- Creating a camera

  Table 3-2 Creating a camera

Operation	Procedure
Creating a directly connected camera	1. Select **Directly connected camera** from the drop-down list box in the upper left corner of the page. 2. On the **Planning Configuration** page, create a directly connected camera. For details, see **Adding a Device Through Automatic Discovery**.

Operation	Procedure
Creating a camera in automatic discovery mode	1. Select **Video surveillance subsystem** from the drop-down list box in the upper left corner of the page. 2. On the **Video Surveillance Subsystem** page, click **Create**. 3. In the **Creating a Video Subsystem** dialog box, select a video subsystem type, set related parameters according to **Table 3-3**, and click **Test**. **NOTE** If the test fails, check whether the parameters are correctly set. 4. Click **Save**.

Table 3-3 Parameters of the video subsystem

Parameter	Description	Example
IP	IP address of the video subsystem	192.168.8.10
Port	Port number of the video subsystem	9900

Parameter	Description	Example
User Name	User name for logging in to the client of the video subsystem **NOTE** – The NetEco needs to have browse and query permissions. Configure the video system users with browse and query permissions. – You are advised to use a new user created in the video subsystem to connect to the camera. Before the connection, ensure that the initial password of the user has been changed and the user has successfully logged in to the video subsystem. – You are advised to set the number of clients that can be logged in to by the user on the video subsystem to a value greater than 5. Otherwise, when the user has logged in to the video subsystem, the user cannot connect to the video subsystem through the NetEco.	Admin
Password	User password for logging in to the client of the video subsystem.	Change_Me

- Playing videos

  Click the name or  of an online camera.

  NOTE

  On the **View** page, click  to view the camera information. Click the name of an online camera in the **Name** column to play videos.

----End

3.2.2.2 Viewing live videos

You can record suspicious images and alarm-triggered images, take snapshots, and view real-time videos to monitor sites for visualized site management.

Prerequisites

- You have the operation rights for **Camera Management**.
- You have added cameras. For details, see **3.2.2.1 Managing Cameras**.
- Communication is normal between cameras and the NetEco.

  NOTE

  For a camera managed by the video surveillance subsystem, ensure that the time of the video surveillance subsystem server is consistent with the NetEco server time.
- Before playing video from cameras managed by the video surveillance subsystem, you need to set video playback parameters. For details, see How Do I Set Video Playback Parameters on the Video Surveillance Subsystem?.

Procedure

Step 1 Choose **Maintenance Management** > **Security Protection** > **Camera Management**.

Step 2 In the navigation tree on the left, choose **Live Video**.

NOTE

If the Firefox browser is used, perform the following operations before playing a video for the first time (Firefox 78 is used as an example):

1. In the displayed **Confirm** dialog box, click **Yes**.
2. In the two dialog boxes that are displayed, click **Advanced**, and then click **Accept Risk and Continue**.

Step 3 You can click a video source to view video in full screen, record video, and take snapshots.

Table 3-4 Operation tasks

Operation	Procedure
Viewing videos in full screen	Click to display the video in full screen. To exit the full screen mode, right-click the mouse or press **Esc**.
Recording videos	1. Click in the lower right corner and select **Start Recording**. 2. In the **Recording Length** dialog box, set the video recording duration and click **OK**. **NOTE** • The video can be recorded in up to nine split screens. You can select one, four, or nine split screens as required. • After the recording time is set, the camera automatically stops video recording after the specified recording time. During video recording, you can click in the lower right corner and choose **Stop Recording**.

Operation	Procedure
Taking snapshots	Click  in the lower right corner and select **Capture Manually**.
Setting groups	Enable grouping  , select the group name from the drop-down list box, and view the video of the group. ● Creating a group 1. Click **Create**. 2. Set related parameters and click **OK**. ● Deleting a group: Select one or more groups and click **Delete**. ● Modifying a group 1. Click **Modify** in the **Operation** column of the target group. 2. Modify related parameters and click **OK**.

----End

4 System

This section describes the operations related to the system.

4.1 System Settings

This section describes the operations related to system settings.

4.1.1 System Configuration

You can refresh the system time, display the view, configure the protocol switch, and change the FTP password by system configuration.

4.1.1.1 Refreshing System Time

The system supports refreshing the NetEco server time and the client time simultaneously.

Procedure

Step 1 Choose **System** > **System Setting** > **System Configuration**.

Step 2 In the navigation pane on the left, choose **System Configuration** > **System Time**.

Step 3 On the **System Time** page, click **Refresh** to refresh the NetEcoserver time and the client time.

NOTICE

The NetEco server time and the client time are automatically refreshed once every 1 second. The refresh stops when you close the page.

----End

4.1.1.2 Modifying the FTP Password

This section describes how to modify the FTP password. To improve user security, users are advised to change their passwords periodically.

Prerequisites

You have the operation rights for **FTP password Setting**.

Context

The following figure shows the default information about the ftpuser and nftpuser users, as shown in **Table 4-1**.

Table 4-1 Default information about the ftpuser and nftpuser users

User	Initial Password	Description
ftpuser	Random password	• Common user. • The **ftpuser** user is an FTP service operator responsible for file transfer between the NetEco server and clients or NEs.
nftpuser	Random password	• Common user. • User **nftpuser** is used for uploading and downloading files for the NMS to access the NetEco through the LAN.

Procedure

Step 1 Choose **System** > **System Setting** > **System Configuration**.

Step 2 In the left navigation pane of the **System Configuration** page, click **FTP Password Setting**.

Step 3 Set the user name and password, and click **Confirm**.

NOTICE

When you log in to the system for the first time, the passwords of users ftpuser and nftpuser are random. You need to reset the passwords.

----End

4.1.2 Notifications

The notifications feature allows the system to send messages remotely. Users can set parameters related to notifications to enable the system to communicate with the short message service gateway (SMSGW), short message service (SMS) modem, or mail server. In this way, users can obtain important function notifications in a timely manner, such as alarms and events, in the form of SMS messages or emails.

4.1.2.1 Third-Party App Notification Settings

The NetEco can send alarm notifications to O&M personnel through the enterprise WeChat public account (service account).

4.1.2.1.1 Setting the WeChat Notification Server

This topic describes how to set notifications on WeChat.

Prerequisites

- The enterprise WeChat official account or individual WeChat test account has been created, and information such as appid and appsecret of the official account has been obtained.
- The NetEco user has the operation rights for **Notifications**.
- You have obtained a valid WeChat certificate from the WeChat official account platform (**https://mp.weixin.qq.com/**) and imported it to **NetEcoNBIService-Wechat Certificates**. Import the WeChat certificate. For details, see **4.3.1.1 Managing Service Certificates**.
- The network connection between the NetEco and WeChat official account platform (api.weixin.qq.com) is normal.

NOTE

- The WeChat official account platform uses the common domain name **api.weixin.qq.com** for interconnection. Ensure that the NetEco server can access the domain name as a client. The NetEco does not need to function as the server to be accessed by the domain name.
- To use the enterprise WeChat official account, you need to add the public IP address of the NetEco to the IP address whitelist of the official account.

Procedure

Step 1 Choose **System** > **System Settings** > **Notifications** from the main menu.

Step 2 On the **Notifications** page, choose **Third-Party App Notification Settings** > **Server Configuration** on the left. The **Server Configuration** page is displayed.

Step 3 On the **Server Configuration** page, set parameters for the NetEco system and WeChat Official Account server by referring to the following table.

Table 4-2 Setting Server parameters

Parameter	Description	Default Value
Notify method	Indicates the notification mode used for interconnecting with a third-party app server. Currently, only **WeChat Official Account** is supported.	WeChat Official Account
Official account for receiving notifications	Indicates the official account that receives the notifications.	Custom enterprise official account
Official account App ID	Indicates the ID of the official account that needs to receive notifications.	N/A
Official account App Secret	Indicates the key of the official account that needs to receive notifications.	N/A
Enable	The system sends third-party app notifications only when server parameter settings are enabled.	No

Step 4 Click **Apply**.

----End

4.1.2.1.2 Configuring WeChat Notification Users

This topic describes how to configure WeChat notification users.

Prerequisites

- O&M personnel who need to receive alarm notifications have followed the Official Account.
- The NetEco user has the operation rights for **Notifications**.

Procedure

Step 1 Choose **System** > **Systems Settings** > **Notifications** from the main menu.

Step 2 On the **Notifications** page, choose **Third-Party App Notification Settings** > **Offical Account User**.

Step 3 On the **Offical Account User** page, click **Sync Users**.

----End

4.1.2.1.3 Configuring WeChat Notification Rules

This topic describes how to configure WeChat notification users.

Prerequisites

- The NetEco user has the operation rights for **Notifications**.
- The WeChat notification server has been enabled.
- The notification users have been created.
- The alarm notification template ID set in the Official Account has been obtained.

Procedure

Step 1 Choose **System** > **Systems Settings** > **Notifications** from the main menu.

Step 2 In the navigation pane on the left, choose **Third-Party App Notification Settings** > **Notification Rule**.

Step 3 On the **Notification Rule** page, click **Create**.

Step 4 On the **Create Notification Rule** page, set notification rule parameters and click **Test**.

- If the users receive the WeChat test notification, the test is successful.
- If the test is abnormal, check whether the configuration parameters are correct and whether the network connection is normal. If the configuration and network are normal but the test still fails, contact technical support engineers.

Step 5 Click **OK**.

----End

4.1.2.1.4 Configuring WeChat Notification User Groups

You can configure WeChat official account user groups to classify users and facilitate user management.

Prerequisites

- O&M personnel who need to receive alarm notifications have followed the Official Account.
- The NetEco user has the operation rights for **Notifications**.

Procedure

Step 1 Choose **System** > **Systems Settings** > **Notifications** from the main menu.

Step 2 On the **Notifications** page, choose **Third-Party App Notification Settings** > **Offical Account User Group.**

Step 3 On the **Offical Account User Group** page, click **Create**.

Step 4 On the **Creating a User Group** page, set parameters such as **Group Name** and click **OK**.

----End

4.2 System Management

This section describes system management operations.

4.2.1 User Management

User management provides functions such as user rights management, area management, and user maintenance and monitoring.

The user management function allows users with different responsibilities to be granted proper permissions and allows users to adjust permissions based on service changes. This ensures that users have the necessary permissions to perform related tasks, thereby ensuring that other management tasks are carried out in an orderly manner, preventing unauthorized operations and insecure operations.

4.2.1.1 User Authorization

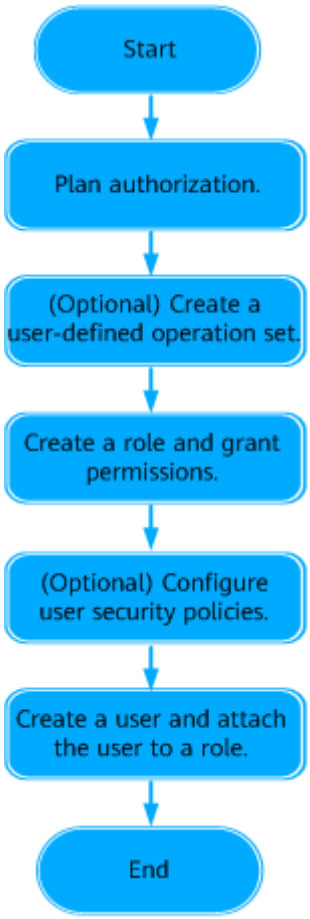
After system installation and commissioning, security administrators need to grant different operation rights to users of different roles based on service planning.

4.2.1.1.1 Authorization Process

This section describes the user authorization process and methods.

Figure 4-1 shows the user authorization process.

Figure 4-1 User authorization process



You can bind a user to role and grant permissions to the user in the following ways:

- Create a role and grant permissions to the role, create a user, and attach the user to the role, as shown in the preceding figure.
- Create a user (not attached to any role), select the user when creating a role, and grant permissions to the role.

4.2.1.1.2 Planning Authorization

Authorization planning classifies users based on their responsibilities. During user authorization, first perform authorization planning to reduce the workload on authorization and permission maintenance. Appropriate authorization planning improves system security and usability.

The authorization planning principles are as follows:

- Users with the same responsibilities are attached to the same role. Users with different responsibilities are attached to different roles.
- If multiple roles require the same application operations, plan a common application operation set for these roles. If not, plan application operation sets or grant application operation rights to each role separately.
- If multiple roles require the same device operations, plan a device operation set for these roles. If not, plan device operation sets or grant device operation rights to each role separately.

4.2.1.1.3 (Optional) Creating a Device Set

To efficiently grant permissions to users who manage same objects from different subnets or device types, security administrators need to plan and create a device set before role authorization.

Prerequisites

Log in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Managed Objects**.

Step 3 On the **Device Sets** tab page, click **Create** and set basic information.

NOTE

You can quickly create a device set by clicking **Copy** in the **Operation** column of a device set and adjusting the information as required.

Step 4 You can choose **Select by Topology** and **Select by Device Type** in **Member Information** to select devices for a device set.

Step 5 Click **OK**.

----End

Related Tasks

You can perform the following operations as required:

- To modify a device set, click the name of the device set, and change members in the device set.

  NOTE

  If the device set to be modified is associated with a user, the modification will take effect the next time the user logs in.

- To delete a device set, click **Delete** in the **Operation** column of the row that contains the device set to be deleted.

  NOTE

  If the device set to be deleted is associated with a user, the user will lose management permissions on all the objects in this set.

4.2.1.1.4 (Optional) Creating a User-defined Operation Set

If operation sets are planned during authorization planning, security administrators need to create user-defined operation sets before user authorization. Authorizing roles using operation sets improves authorization efficiency.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Operation Sets**.

Step 3 On the **Operation Sets** page, click **Create**.

NOTE

You can quickly create an operation set by clicking **Copy** in the **Operation** column of an operation set and adjusting the information as required.

Step 4 On the displayed page, set **Operation set name**, **Type**, and **Description**.

Step 5 Select the operation rights to be included in the operation set from the list of available operation rights.

NOTE

You can delete redundant operation rights from the operation list by selecting these operation rights and clicking **Delete**.

Step 6 On the **Operation Sets** page, click **OK**.

----End

Related Tasks

For details about how to maintain operation set information, see **4.2.1.4.3 Common Operations for Operation Set Information Maintenance**.

4.2.1.1.5 Creating a Role and Granting Permissions

If the default roles provided by the system cannot meet user authorization requirements in the authorization plan, security administrators need to create roles and grant them permissions based on the plan.

Prerequisites

You have logged in to the NetEco as a security administrator.

Context

- If only a few roles are required, create them one by one.
- If multiple roles are required or the roles are obtained from the files exported from other systems, create roles in batches.

Procedure

- Creating a single role

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Roles**.

Step 3 On the **Roles** page, click **Create**.

NOTE

You can quickly create a role by clicking **Copy** in the **Operation** column of a role and adjusting the information as required.

Step 4 On the displayed page, set basic role information.

Step 5 Select the users to be attached to the role.

After role authorization is complete, the users you have selected have the permissions included in this role.

Step 6 Click **Next** and select the managed objects included in the role based on the authorization plan.

- **All Objects**: shows all the resources that can be managed by the system. It is the default managed object provided by the system and cannot be modified or deleted.
- **Subnets**: shows all the subnets that can be managed by the system. If a subnet is selected for a user, this user can manage the subnet and all its managed objects, including devices and subnets.
- **Devices**: If a user needs to manage specified devices, you can grant permissions by device.
- **Resource Groups**: If a resource group is selected for a role, this role can manage all the resources in the group. Resources are grouped by resource type using Resource Groups.

Step 7 Click **Next**. Based on the authorization plan for application-level operation rights and device-level operation rights of the role, set application-level operation rights of the role on the **Application-Level** tab page and set device-level operation rights for each managed object included in the role on the **Device-Level** tab page.

When setting device-level operation rights, select a managed object first. The device operations that can be bound to the managed object are displayed in the **Operations** list box. Then, you can select the devices operations to be authorized.

Step 8 Click **OK**.

----End

- Creating roles in batches

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Roles**.

Step 3 On the **Roles** page, click  and choose **Batch Create Roles**.

Step 4 On the **Batch Create Roles** page, click a template name to download the template.

NOTE

The system provides two template formats: **Role Template.xls** and **Role Template.xlsx**, and you can edit the template in .csv format. Select a template format as required.

Step 5 Fill in role information based on the template.

Step 6 Click . In the displayed dialog box, select the edited template.

Step 7 Click **Create**.

After roles are imported, you can perform the following operations:

1. On the displayed page, view the number of successfully imported roles and the number of roles that fail to be imported.
2. In the **Result** list, view the imported roles and their details.
3. If partial failure occurs, modify the role information that failed to be imported based on the details, and import them again.

Step 8 Click **OK**.

Step 9 Assign permissions to the roles created in batches based on the authorization plan.

1. On the **Roles** page, click a role name.
2. On the **Managed Objects** or **Operation Rights** tab page, click **Edit**, and assign permissions to the role.

----End

Follow-up Procedure

If a user logs in to a third-party system in SSO mode, role information (excluding operation rights) about this user can be synchronized to the third-party system. To ensure that this user has the same operation rights on the third-party system as those on the system, create the same role for the user on the third-party system and bind the same operation rights to the role.

Related Tasks

For details about how to maintain role information, see **4.2.1.4.2 Common Operations for Role Information Maintenance**.

4.2.1.1.6 (Optional) Configuring User Policies

User policies refer to rules for system accesses and operation control. The system provides the default account policy and password policy. After authorization is planned, you need to set user policies if the default account policy or password policy does not meet requirements or if IP address access control or login time control is required for users.

For details about how to configure user policies, see **User Policy Management**.

4.2.1.1.7 Creating a User and Attaching the User to a Role

After a security administrator creates a user and attaches the user to a role, the user has the permissions of this role.

Prerequisites

You have logged in to the NetEco as a security administrator.

Context

- If only a few users are required, create them one by one.
- If multiple users need to be created or users are obtained from the files exported from other systems, create users in batches.
- If a user has logged in to the management system, disabling the user will force a logout of the user. Therefore, exercise caution when performing this operation.

Procedure

- Creating a single user

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 On the **Users** page, click **Create**.

NOTE

You can quickly create a user by clicking **Copy** in the **Operation** column of a user and adjusting the information as required.

Step 4 On the displayed page, set basic user information.

Users are classified into three types: **Local**, **Third-party**, and **Remote**, with different parameters for each user type.

- To create a user for logging in to the local system, set the user type to **Local**.
- In the scenario that a third-party system is connected, set the user type to **Third-party**. Third-party users can log in only through the third-party authentication interface, and are not allowed to log in using a web browser.
- To create a user for interconnecting an LDAP or RADIUS server, locally create a user with the same username as a user on the LDAP or RADIUS server and set the user type to **Remote**.

Step 5 Click **Advanced Settings**, set parameters such as **Max. online sessions**, and click **Next**.

Parameters are described in **Table 4-3**.

Table 4-3 Advanced parameters

Parameter	Description	Value Range
Max. online sessions	Maximum number of online sessions of an account.	By default, this parameter is disabled, indicating that the number of the user login sessions is not limited. If this parameter is enabled, the value range is from 1 to 500. The setting of this parameter is described as follows: ● If **Max. online sessions** is set to **1**, **Login when maximum online sessions already in use** can be **Not allowed** or **Log out of the session**. – **Not allowed**: After the number of online sessions reaches the upper limit, the user cannot log in to the management system. – **Log out of the session**: After the number of online sessions reaches the upper limit, the user's subsequent session causes the logout of a previous session. ● If **Max. online sessions** is set to a value from **2** to **500**, **Login when maximum online sessions already in use** is **Not allowed** and the value cannot be changed.
Account validity	Number of days during which an account can log in to the management system.	By default, this parameter is disabled, indicating that the account is permanently valid. If this parameter is enabled, the value range is from 1 to 180 (unit: day). This user account is not allowed to log in to the management system after the validity period elapses, and the user needs to contact the security administrator.

Parameter	Description	Value Range
Allowed logins	Number of times during which an account can log in to the management system.	By default, this parameter is disabled, indicating that the number of the user account's login times is not limited. If this parameter is enabled, the value range is 0 to 10. The user account is not allowed to log in to the management system after the allowed login times are used up, and the user needs to contact the security administrator.
Auto-logout if no activity within	If a user does not perform any operation within the period specified by this parameter after logging in to the management system, the user will be logged out. This parameter can be set for local users and remote users. The default value for the third-party user is 30 minutes and cannot be changed.	The default value is **30 min**. The value can be **System setting** (subject to the system account policy), **10 min**, **30 min**, **2 h**, **6 h**, **12 h**, **24 h**, **48 h**, or **Unlimited**.
Enable the user policy if no login within a period	If a user does not log in to the management system for the period specified by this parameter, one of the following policies will be taken: • Deleting users • Disabling a user • Unlimited	By default, a user is disabled if the user remains offline for 60 consecutive days. The value range of this parameter is 1 to 1000 days. By default, this parameter is unselected. In this case, the account policy in the system applies to this user. If this parameter is selected, the system deletes or disables a user based on the selected policy when the period during which this user does not log in reaches the value specified by this parameter.

Parameter	Description	Value Range
Compulsory password renewal	Password validity period policy. (This parameter is not displayed during the creation of remote users.) • Password validity (days) • In advance warning before password expires (days) • Min. password usage period (days)	By default, this parameter is unselected. In this case, the password policy in the system applies to this user. If this parameter is selected, the system prompts the user to change its password if the usage period of the password reaches the values specified by this parameter. • The default value of **Password validity (days)** is **90**, and the value range is from 2 to 999. **0** indicates that the password never expires. • The default value of **In advance warning before password expires (days)** is **10**, and the value range is from 1 to 99. • The default value of **Min. password usage period (days)** is **10**, and the value range is from 1 to 999.

NOTE

- If the same parameters are set in **Advanced Settings** and **Account Policy**, the settings in **Advanced Settings** are used.For details about how to set the account policy,see **4.2.4.1 Setting the Account Policy**.
- If the same parameters are set in **Advanced Settings** and **Password Policy**, the settings in **Advanced Settings** are used.For details about how to set the password policy,see **4.2.4.2 Setting the Password Policy**.

Step 6 Select the role to which the user is attached and click **Next**.

Click a role name to view the permissions of the role.

You can create a role and attach the user to the new role. For details about how to create a role, see **4.2.1.1.5 Creating a Role and Granting Permissions**. After creating a role, you can click **Refresh** on the role list page and select the new role for the user from the role list.

NOTICE

When creating a user as the system administrator user, you are advised not to attach the new user to both the **Administrators** and **SMManagers** roles to ensure system security. A user attached to both the **Administrators** and **SMManagers** roles has the maximum permissions of all resources in the system. Exercise caution when using such users to perform operations and do not perform any operations that affect system security. For example, do not share or disclose the names and passwords or names of these users.

Step 7 Select a login time policy and a client IP address policy for the user.

You can also click **Create** to create a login time policy or client IP address policy as needed.

Step 8 Click **OK**.

----End

- Creating users in batches

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 On the **Users** page, click ••• and choose **Import Users**.

Step 4 On the **Import Users** page, click the template name to download the template and enter user information in the template.

NOTE

The system provides two template formats: **User Template.xls** and **User Template.xlsx**, and you can edit the template in .csv format. Select a template format as required.

Step 5 Choose **Create Users** to import users.

NOTE

If the passwords for the non-remote users are not configured in the imported file, set the passwords on the page.

Step 6 Click . In the displayed dialog box, select the edited template.

Step 7 Click **Create**. After the import is complete:

1. On the displayed page, view the number of successfully imported users and the number of users who fail to be imported.
2. In the **Result** list, view the imported users and their details.
3. If partial failure occurs, modify the user information that failed to be imported based on the details, and import them again.

Step 8 Click **OK**.

----End

Related Tasks

For details about how to maintain user information, see **4.2.1.4.1 Common Operations for User Information Maintenance**.

4.2.1.2 Permission Adjustment

Permissions can be maintained after security administrators perform initial user authorization. If the managed resources or users, or user responsibility is changed, security administrators need to adjust user permissions.

4.2.1.2.1 Permission Adjustment After Subnets Are Added

After a subnet is added, security administrators need to plan the user who manages the subnet and device-level operation rights for the new subnet, and then bind the operation rights to the role to which the user is attached.

Prerequisites

- You have logged in to the NetEco as a security administrator.
- Operation rights for the new subnet have been planned.

Context

The operations in this section will change user rights and the changes take effect upon the next login. Exercise caution when performing these operations.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Roles**.

Step 3 Check whether the role has been automatically bound to the operation rights for the new subnet.

- If the parent subnet of the new subnet has been added to the managed objects of the role to which the user is attached and the operation sets bound to the parent subnet contain the operations on the new subnet, the user has the operation rights for the new subnet by default after the subnet is added, and no further action is required.
- If the parent subnet of a new subnet has been added to the managed objects of the role to which the user is attached, but the operation set bound to the parent subnet does not contain operations on the new subnet, the user does not have the operation rights for the new subnet after the subnet is added. In this case, go to **Step 4**.
- If the parent subnet of the new subnet is not added to the managed-object scope of the role to which the user is attached, go to **Step 5** and **Step 6**.

Step 4 Bind the device-level operation rights for the new subnet to the role.

1. On the **Roles** page, click the role name.
2. Go to the **Operation Rights** tab page and click **Device-Level**.

3. Click **Edit**.
4. In the **Authorization Objects** list, select the parent subnet to which you want to add a subnet. In the **Operations** list, select the device operation rights you want to bind to the new subnet.
5. Click **OK**.

Step 5 Add the new subnet to the managed-object scope of the role.

1. On the **Roles** page, click the role name.
2. Switch to the **Managed Objects** tab page and click **Edit**.
3. Go to the **Subnets** tab page and select the new subnet.
4. Click **OK**.

Step 6 Bind operation rights to the new subnet.

1. On the **Roles** page, click the role name.
2. Go to the **Operation Rights** tab page and click **Device-Level**.
3. Click **Edit**.
4. In the **Authorization Objects** list, select the new subnet. In the **Operations** list, select the device operation rights you want to bind to the new subnet.
5. Click **OK**.

----End

4.2.1.2.2 Permission Adjustment After Devices Are Added

After a device is added, security administrators need to plan the user who manages the device and operation rights for the new device, and then bind the operation rights to the role to which the user is attached.

Prerequisites

- You have logged in to the NetEco as a security administrator.
- Operation rights for the new device have been planned.

Context

The operations in this section will change user rights and the changes take effect upon the next login. Exercise caution when performing these operations.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Roles**.

Step 3 Check whether the role has been automatically bound to the operation rights for the new device.

- If the subnet where the new device is located has been added to the managed objects of the role to which the user is attached and the operation sets bound to the subnet contain the operations on the new device, the user

has the operation rights for the new device by default after the device is added, and no further action is required.

- If the subnet where the new device is located has been added to the managed objects of the role to which the user is attached and the operation sets bound to the subnet do not contain the operations on the new device, the user does not have the operation rights for the new device by default after the device is added. In this case, go to **Step 4**.
- If none of the preceding assumptions are satisfied, the new device is beyond the managed objects of the role to which the user is attached. In this case, go to **Step 5**.

Step 4 Bind the operation rights for the new device to the role.

1. On the **Roles** page, click the role name.
2. Go to the **Operation Rights** tab page and click **Device-Level**.
3. Click **Edit**.
4. Select the device operation rights to be bound to the new device.
5. Click **OK**.

Step 5 Add the new device to the managed objects of the role.

1. On the **Roles** page, click the desired role name. Go to the **Managed Objects** tab page.
2. Click **Edit**.
3. Go to the **Devices** tab, and select the new devices.
4. Click **OK**.

Step 6 Bind operation rights to the new device.

1. On the **Roles** page, click the role name. Go to the **Operation Rights** tab page and click **Device-Level**.
2. In the **Authorization Objects** list, select the device by referring to **Step 5**. In the **Operations** list, select the operation rights to be bound to the device.
3. Click **OK**.

----End

4.2.1.2.3 Permission Adjustment After Networking Modification

After networking is modified, operation rights for managed objects involved in the modification may need to be transferred to another role. In this case, security administrators need to adjust the role permissions.

Prerequisites

- You have logged in to the NetEco as a security administrator.
- Operation rights for the subnet whose networking is modified and for the devices on the subnet have been planned.

Context

The operations in this section will change user rights and the changes take effect upon the next login. Exercise caution when performing these operations.

Procedure

Step 1 Check whether the networking is globally reorganized.

- If it is, plan users and roles again.
- If it is not, go to **Step 2**.

Step 2 Handle operation rights for the moved devices.

- If devices are moved out of the network, users who manage the network lose the operation rights for the moved devices. No further action is required.
- If devices are moved to the network, perform permission adjustment by following the instructions provided in **4.2.1.2.2 Permission Adjustment After Devices Are Added**.

----End

4.2.1.2.4 Permission Adjustment After the Objects Managed by Users Are Changed

If the operation rights for an object need to be transferred from one role to another while the managed-object topology is not changed, security administrators need to adjust the managed objects and operation rights of the users.

Prerequisites

- You have logged in to the NetEco as a security administrator.
- Operation rights for the target managed object have been planned.

Context

The operations in this section will change managed objects and operation rights and the changes will take effect upon the next login. Exercise caution when performing these operations.

Procedure

1. Choose **System** > **System Management** > **User Management** from the main menu.
2. In the navigation pane, choose **Roles**.
3. Click a role name, and go to the **Managed Objects** tab page. View the managed objects included in the role and add or delete managed objects based on new requirements.
4. Go to the **Operation Rights** tab page, and modify the device-level operation rights for the modified managed objects.

4.2.1.2.5 Permission Adjustment After Operation Rights of Users Are Changed

If certain operation rights attached to a role need to be added or deleted due to responsibility changes, security administrators need to adjust the role and permissions of this role as needed.

Prerequisites

You have logged in to the NetEco as a security administrator.

Context

- If authorization for the role is not performed based on an operation set, adjust the permissions of the role by modifying the role.
- If authorization for the role is performed based on an operation set, adjust the permissions of the role by modifying the operation set.
- This operation will change the permissions of users attached to this role. Therefore, exercise caution when performing this operation. The permission changes will take effect after next login of these users.

Procedure

- Modifying a role
  a. Choose **System** > **System Management** > **User Management** from the main menu.
  b. In the navigation pane, choose **Roles**.
  c. Click the role to be modified, go to the **Operation Rights** page, and click **Edit**.
  d. View the operation rights included in the role and add or delete operation rights based on new requirements.
- Modifying an operation set
  a. Choose **System** > **System Management** > **User Management** from the main menu.
  b. In the navigation pane, choose **Operation Sets**.
  c. Select an operation set, and then click **Edit**.
  d. View the operation rights included in the operation set and add or delete operation rights based on new requirements.

  NOTE

  One operation may be included in multiple operation sets. Operation rights of a role can be deleted only when the operations are not included in any operation sets attached to this role.

4.2.1.2.6 Permission Adjustment After a User's Role Is Changed

After the position of an employee is changed, security administrators need to adjust the role to which the user account of the employee is attached to change permissions of the employee.

Prerequisites

You have logged in to the NetEco as a security administrator.

Context

- Disabling and deleting users will force a logout of logged-in users. Therefore, exercise caution when performing these operations.
- A position change occurs in the following situations:
  – An employee is recruited.

- The role of an employee (as a user) is changed.
- An employee resigns.

Procedure

- An employee is recruited.
  a. Choose **System** > **System Management** > **User Management** from the main menu.
  b. In the navigation pane, choose **Users**.
  c. On the **Users** page, click **Create**.
  d. On the displayed page, set basic user information and click **Next**.
  e. Select the role to which the user is attached and click **Next**.
  f. Set access control information about the user and click **OK**.
- The role of an employee (as a user) is changed.
  a. Choose **System** > **System Management** > **User Management** from the main menu.
  b. In the navigation pane, choose **Users**.
  c. Click the name of the user whose role is changed and go to the **Roles** tab page.
  d. Click **Edit** in the upper right corner of the page.
  e. Add or delete the role of a user based on the user position changes.
- An employee resigns.
  a. Choose **System** > **System Management** > **User Management** from the main menu.
  b. In the navigation pane, choose **Users**. On the page that is displayed, perform the following operation as required:
     - If you want to retain the account, click **Disable** in the **Operation** column of the row that contains the user to disable the user.
     - If you do not want to retain the account, click **Delete** in the **Operation** column of the row that contains the user to delete the user.

4.2.1.3 Regional User Permission Management

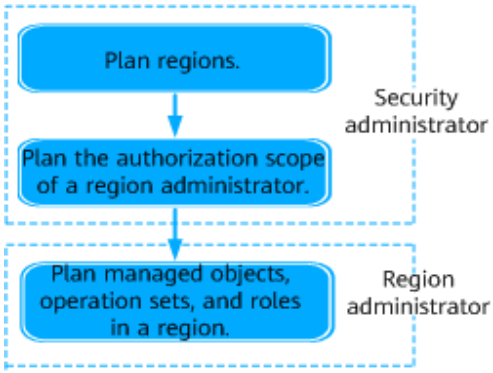
To improve management efficiency, security administrators divide the network into regions based on service requirements and allow different personnel to manage users and services in different regions. In a region, region administrators can create roles, assign permissions to the roles, and attach users to roles to grant them corresponding permissions. This implement user management in the region.

4.2.1.3.1 Planning Authentication in a Region

Before region management, the security administrator must plan authentication in the region properly to reduce the workload of authorization and permission maintenance in regions.

Figure 4-2 shows the process of planning authentication in a region.

Figure 4-2 Process of planning authentication in a region



- Plan regions.

  Plan regions based on physical networking and service requirements. You are advised to plan regions based on administrative zones and managed objects.

  - Plan the users who belong to the same administrative zone to the same region.
  - Plan the administrative zones that have the same managed objects to the same region.
  - A maximum of 20 regions can be planned.
- Plan the authorization scope of a region administrator.

  Each region has region administrators. Plan the operation rights and managed objects of region administrators after planning regions.
- Plan managed objects, operation sets, roles, and users in a region.

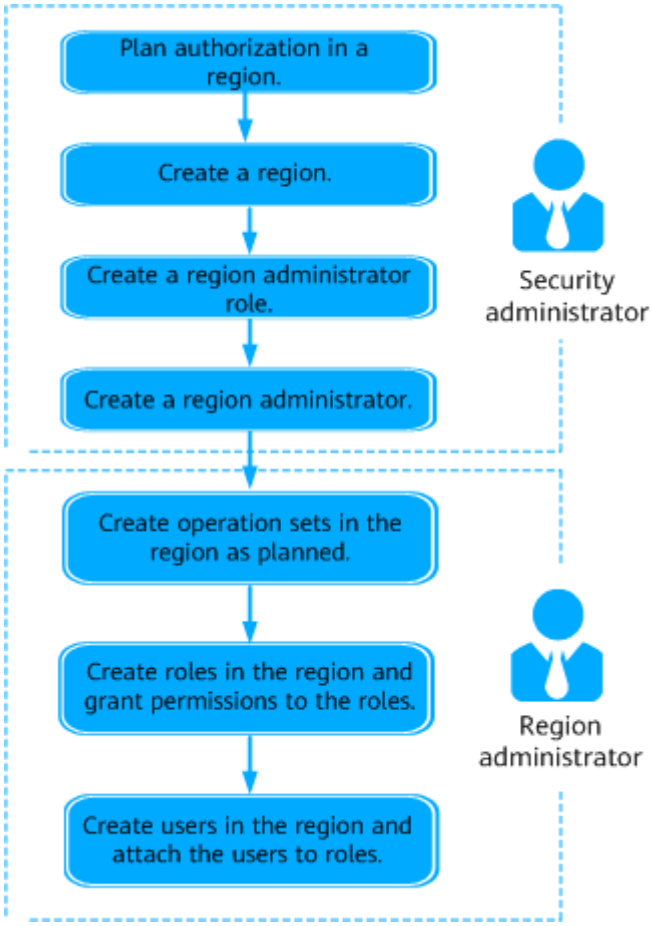
  Plan users who have same responsibilities to the same role. Analyze operation rights required for each role to fulfill their responsibilities and classify the operation rights into operation sets.

4.2.1.3.2 Creating a Region Management Process

This section describes the region management process.

Figure 4-3 shows the region management process.

Figure 4-3 Region management process



4.2.1.3.3 Creating a Region

Security administrators can create regions as planned to facilitate region-based management and improve permission management efficiency.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Regions**.

Step 3 On the page that is displayed, click **+**.

Step 4 In the **Create Region** dialog box, enter basic region information and click **OK**.

NOTE

- Select **Automatically create Region Administrators**. After a region is created, the system automatically generates a region administrator role for this region. By default, this role has the **User Management** and **Query Security Log** permissions.
- If **Automatically create Region Administrators** is not selected, you need to manually create a region administrator role after the region is created. For details, see **4.2.1.3.4 Creating a Region Administrator Role**.

----End

Related Tasks

If you need to modify or delete a region due to service changes, click or in the upper right corner of the region box.

NOTE

Before deleting a region, delete all the users, common roles, and operation sets from the region.

4.2.1.3.4 Creating a Region Administrator Role

After creating a region, security administrators need to create a region administrator role and specify the authorization scope for the region administrator role.

Prerequisites

You have logged in to the NetEco as a security administrator.

Context

If **Automatically create Region Administrators** is not selected when a region is created, you need to manually create the region administrator role for this region.

NOTE

If **Automatically create Region Administrators** is selected, after the region is created, you need to set the authorization scope for the region administrator role that is automatically created.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Regions**.

Step 3 Select the target region and click the **Roles** tab.

Step 4 On the **Roles** tab page. Click **Create** and choose **Region Administrators**.

Step 5 On the **Basic Information** page, set the basic information and click **Next**.

Step 6 On the **Select Mandate-Managed Objects** page, set the managed objects that can be assigned by the region administrator based on the authorization planning.

NOTE

The managed objects of a region administrator can be set by **All Objects** or **Subnets**.

Step 7 On the **Select Mandate-Operation Rights** page, set the permissions that can be assigned by the region administrator based on the authorization planning.

NOTE

The authorization scope of a region administrator can be set by operation set.

Step 8 Click **OK**.

NOTE

The region administrator role has the **User Management** and **Query Security Log** permissions.

----End

Related Tasks

The security administrator can perform the following operations as required:

Exporting roles by region: Click , and choose **Export All Roles**.

NOTE

- If the number of roles exceeds 500, role information is exported to multiple files. That is, each file contains information about a maximum of 500 roles.
- The file is exported in .csv or .xlsx format and downloaded to the local PC as a .zip package.
- Security administrators can export role information of each region.

4.2.1.3.5 Creating a Region Administrator

After creating a region, security administrators need to create a region administrator and attach the region administrator to the region administrator role so that the region administrator has security management permissions on this region.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Regions**.

Step 3 In the region list, click the target region.

Step 4 On the **Users** tab page, click **Create** to create a user.

Step 5 On the displayed page, set basic user information.

Step 6 (Optional) Click **Advanced Settings**, set parameters such as **Max. online sessions**, and click **Next**.

Step 7 On the **Roles** page, select the region administrator role to which this user needs to be attached and click **Next**.

Step 8 Set access control information about the user and click **OK**.

If the current access control information does not meet requirements, you can create the required access control information by referring to **4.2.4.3 Setting a Client IP Address Policy** and **4.2.4.4 Setting a Login Time Policy**.

After security administrators create a region administrator, the new region administrator will be displayed in the user list of the region. The region administrator can use this user account to log in to the NetEco and manage user permissions in the region.

----End

Related Tasks

Security administrators can perform the following operations as required:

- Viewing region administrator information: Click a region administrator name to view basic information, operation rights, and access policies of this administrator.

  NOTE

  Security administrators can view information about all region administrators. Region administrators can only view information about region administrators in their own regions.

- Exporting users in a region: Click , and choose **Export All Users** or **Export Selected Users**.

  NOTE

  - The **Password**, **Mobile number**, and **Email address** fields are not exported. Therefore, the values of these fields are empty in the exported user information file.
  - Security administrators can export information about all the users (including users in regions) in the system.
  - The file is exported in .csv or .xlsx format and downloaded to the local PC as a .zip package.

4.2.1.3.6 Creating Operation Sets in a Region As Planned

Region administrators can create operation sets in a region to improve permission management efficiency in the region.

Prerequisites

You have logged in to the NetEco as a region administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Operation Sets**.

Step 3 On the **Operation Sets** page, click **Create**.

NOTE

You can quickly create an operation set by clicking **Copy** in the **Operation** column of an operation set and adjusting the information as required.

Step 4 On the displayed page, set **Operation set name**, **Type**, and **Description**.

Step 5 Select operations for the operation set.

If unnecessary operations exist in the operation rights list, click **Delete** to delete them.

NOTE

A region administrator can only create operation sets based on the operation rights of a region administrator role.

Step 6 Click **OK**.

----End

Related Tasks

You can adjust the operation rights included in an operation set as required by selecting an operation set and clicking **Edit**.

4.2.1.3.7 Creating a Role in a Region and Granting Permissions

A region administrator can create common roles in the region to centrally grant permissions to users in this region.

Prerequisites

You have logged in to the NetEco as a region administrator.

Context

- If only a few roles are required in a region, create them one by one.
- If multiple roles are required in a region or the roles are obtained from the files exported from other systems, create roles in batches.
- The operations in this section will change user permissions. Exercise caution when performing these operations.

Procedure

- Creating a common role in a region

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Roles**.

Step 3 On the **Roles** page, click **Create**.

NOTE

You can quickly create a role by clicking **Copy** in the **Operation** column of a role and adjusting the information as required.

Step 4 On the displayed page, enter the basic role information, select users to be attached to the role, and click **Next**.

NOTE

If a user has been attached to a regional administrator role, you cannot attach this user to a common role.

Step 5 Select the managed objects included in the role based on the role plan during authorization planning.

- **All Objects**: shows all the resources that can be managed by the system. It is the default managed object provided by the system and cannot be modified or deleted.
- **Subnets**: shows all the subnets that can be managed by the system. If a subnet is selected for a user, this user can manage the subnet and all its managed objects, including devices and subnets.

Step 6 Based on the authorization plan for application-level operation rights and device-level operation rights of the role, set application-level operation rights of the role on the **Application-Level** tab page and set device-level operation rights for each managed object included in the role on the **Device-Level** tab page.

When you set device-level operation rights for a managed object, select the managed object first and then select the device operation sets to be bound to the object. After you select a managed object, device operation sets that can be bound to the object are listed in **Operations**.

Roles in regions can only be authorized by operation set. For details about how to create an operation set in a region, see **4.2.1.3.6 Creating Operation Sets in a Region As Planned**.

Step 7 Confirm role information and click **OK**.

----End

- Creating common roles in a region

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Roles**.

Step 3 On the **Roles** page, click ••• and choose **Batch Create Roles**.

Step 4 On the **Batch Create Roles** page, click a template name to download the template.

The system provides two template formats: **Role Template.xls** and **Role Template.xlsx**, and you can edit the template in .csv format. Select a template format as required.

Step 5 Fill in role information based on the template.

Step 6 Click . In the displayed dialog box, select the edited template.

Step 7 Click **Create**.

NOTE

Security administrators can import roles of all regions. Region administrators can import only roles of their own regions.

After roles are imported, you can perform the following operations:

- On the displayed page, view the number of successfully imported users and the number of users who fail to be imported.
- In the **Result** list, view the imported roles and their details.

Step 8 Click **OK**.

Step 9 Assign permissions to the roles created in batches based on the authorization plan.

1. On the **Roles** page, click a role name.
2. On the **Managed Objects** or **Operation Rights** tab page, click **Edit**, and assign permissions to the role.

----End

Follow-up Procedure

If a user logs in to a third-party system in SSO mode, role information (excluding operation rights) about this user can be synchronized to the third-party system. To ensure that this user has the same operation rights on the third-party system as those on the system, create the same role for the user on the third-party system and bind the same operation rights to the role.

Related Tasks

You can perform the following operations as required:

- Viewing role information in a region: Click the name of the role whose information will be viewed.
- Modifying role information in a region: Click the name of the role whose information will be modified, and then click Edit.
- Deleting roles: To delete a single role, click **Delete** in the **Operation** column of the row that contains this role. To delete roles in batches, select the roles to be deleted and click **Delete**.

  NOTE

  You cannot delete the region administrator role and the role to which the current user is attached.

- Exporting roles: Click , and choose **Export All Roles**.

NOTE

- If the number of roles exceeds 500, role information is exported to multiple files. That is, each file contains information about a maximum of 500 roles.
- A region administrator can export only roles of the region to which the region administrator belongs.
- The file is exported in .csv or .xlsx format and downloaded to the local PC as a .zip package.

4.2.1.3.8 Creating a User in a Region and Attaching the User to a Role

After a region administrator creates a user and attaches the user to a role, the user has the permissions of this role.

Prerequisites

You have logged in to the NetEco as a region administrator.

Context

- If only a few users are required in a region, create them one by one.
- If multiple users are required in a region or the users are obtained from the files exported from other systems, create users in batches.
- The operations in this section involve user permission adjustment, which will force a logout of logged-in users. Therefore, exercise caution when performing this operation.

Procedure

- Creating a single user

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 On the **Users** page, click **Create** to create a user.

NOTE

- You can quickly create a user by clicking **Copy** in the **Operation** column of a user and adjusting the information as required.
- If you are copying a user attached to the region administrator role, the copied user will be detached from the role.

Step 4 On the displayed page, set basic user information.

Step 5 (Optional) Click **Advanced Settings**, set parameters such as **Max. online sessions**, and click **Next**.

NOTE

- If the same parameters are set in **Advanced Settings** and **Account Policy**, the settings in **Advanced Settings** are used.For details about how to set the account policy,see **4.2.4.1 Setting the Account Policy**.
- If the same parameters are set in **Advanced Settings** and **Password Policy**, the settings in **Advanced Settings** are used.For details about how to set the password policy,see **Setting the Password Policy**.

Step 6 Select the role to which the user is attached and click **Next**.

Click a role name to view information about the role, such as the permissions and managed objects included in the role.

NOTE

A user cannot be attached to both the region administrator role and a common role of the region.

Step 7 Set access control information about the user and click **OK**.

NOTE

Third-party users can log in only through the third-party authentication interface. They are not allowed to log in using a web browser.

----End

- Creating users in batches

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 On the **Users** page, click and choose **Import Users**.

Step 4 On the **Import Users** page, click the template name to download the template and enter user information in the template.

NOTE

The system provides two template formats: **User Template.xls** and **User Template.xlsx**, and you can edit the template in .csv format. Select a template format as required.

Step 5 Choose **Create Users** to import users.

NOTE

- If the passwords for the non-remote users are not configured in the imported file, set the passwords on the page.
- Region administrators can import users only to their own regions.

Step 6 Click . In the displayed dialog box, select the edited user information file.

Step 7 Click **Create**. After the import is complete:

- In the displayed dialog box, view the number of successfully imported users and the number of users who fail to be imported.
- In the **Result** list, view the imported users and their details.

Step 8 Click **OK**.

----End

Related Tasks

- Viewing information about users in a region: Select a username and view **Basic Information**, **Roles**, and **Access Policies**.

- Modifying information about users in a region: Select a user name and then click view **Edit**.
- Resetting the password for a user in a region: Click **Reset Password** in the **Operation** column of the row that contains the user whose password needs to be reset.
- Deleting users in a region: To delete a single user, click **Delete** in the **Operation** column of the row that contains the user to be deleted. To delete users in batches, select the users to be deleted, and click **Delete**.

  NOTE

  The current user cannot be deleted.
- Disabling a user in a region: Click **Disable** in the **Operation** column of the row that contains the user to be disabled.
- Enabling a user in a region: Click **Enable** in the **Operation** column of the row that contains the user to be enabled.
- Unlocking users:
  - To unlock a user: Click **Unlock** in the **Operation** column of the row that contains the user.
  - To unlock users in batches: Click ··· and choose **Batch Unlock Users**.

  If the users are not disabled, these users can log in to the NetEco after being unlocked.
- Exporting users in a region: Click ··· , and choose **Export All Users** or **Export Selected Users**.

  NOTE

  - The **Password**, **Mobile number**, and **Email address** fields are not exported. Therefore, the values of these fields are empty in the exported user information file.
  - Security administrators can export information about all the users (including users in regions) in the system.
  - The file is exported in .csv or .xlsx format and downloaded to the local PC as a .zip package.

4.2.1.3.9 Modifying User Information in a Region in Batches

Region administrators can modify user information (such as **Max. online sessions** and **Login Time Policy**) in batches, improving system security.

Prerequisites

You have logged in to the NetEco as a region administrator.

Context

- You can use the following methods to modify user information in batches:
  - Using the **Batch Modify Users** function

    Select the users whose information needs to be modified and click **Batch Modify Users**.
  - Modifying an exported user information file

Export user information as a file, edit the file, and then import it to the system.

- The operations in this section involve user permission adjustment, which will force a logout of logged-in users. Therefore, exercise caution when performing this operation.

Procedure

- Using the **Batch Modify Users** function

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 In the user list, select one or more users, click ***, and choose **Batch Modify Users**.

Step 4 Check that the users on the **User List** page are consistent with those you want to modify, and click **Next**.

NOTE

To modify a user in **User List**, perform the following operations:

- If some users to be modified are not in the list, click **Cancel** and select the users to be modified again.
- If some users who do not need to be modified are in the list, click **Delete** in the **Operation** column of the rows that contain these users to delete them.

Step 5 On the **Modification Items** tab page, modify user information and click **OK**.

NOTE

- You cannot modify your own information.
- A maximum of 100 users can be modified at a time.
- After the login time policy is modified, the users who do not meet the policy requirements will be forcibly logged out.

Step 6 On the **Modification Result** page, view the modification results and details.

----End

- Modifying an exported user information file

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 Select the users whose information needs to be exported, click ***, and choose **Export All Users** or **Export Selected Users**.

NOTE

- The **Password**, **Mobile number**, and **Email address** fields are not exported. Therefore, the values of these fields are empty in the exported user information file.
- Security administrators can export information about all the users (including users in regions) in the system.

Step 4 In the **Select File Format** dialog box, select a file format and click **OK**.

Step 5 Modify the exported user information file.

NOTE

- When modifying the user information file, do not change the sequence of the fields in the file.
- If you change the value of a field to empty or an invalid value, the value of this field will not be changed.
- The following user information cannot be modified:
  - **Type** and **Region** of all users
  - All information about the current user
  - **Password**, **Login Time Policy**, **Client IP Address Policy**, **Personal Client IP Address Policy**, and **Password Validity Period (Days)** of remote users
  - **Password** and **Auto-Logout If No Activity Within** of third-party users

Step 6 Click and choose **Import Users**.

Step 7 In the **Import Users** window, choose **Update Users**.

Step 8 Click , select the modified user information file, and click **Modify**.

Step 9 After the import is complete:

1. On the displayed page, view the number of successfully modified users and the number of users who fail to be modified.
2. In the **Result** list, view the imported users and their details.

Step 10 Click **OK**.

----End

4.2.1.3.10 Moving Roles from the Default Region to Another Region

Security administrators can move roles from the default region to another region. The roles are then managed by the destination region administrator.

Prerequisites

- You have logged in to the NetEco as a security administrator.
- A region has been created. For details about how to create a region, see **4.2.1.3.3 Creating a Region**.

Context

The operations in this section will detach roles from related users, managed objects, and operation rights. Therefore, exercise caution when performing this operation.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Roles**.

Step 3 Select the roles to be moved, click ***, and choose **Move Selected Roles**.

NOTE

Default roles, such as **Administrators** and **SMManagers**, and roles to which the current user is attached cannot be moved.

Step 4 Confirm the roles to be moved in the list. Click **Next**.

Step 5 Select the destination region.

NOTE

After a role is move to another region, related users, managed objects, and operation rights will be detached from the role.

Step 6 Click **Move**. On the **Moving Result** page, view the moving results and details.

After a role is moved, it is displayed in the role list of the destination region.

Step 7 Click **OK**.

----End

Follow-up Procedure

After moving a role out of a region, bind managed objects and operation rights to the role again.

4.2.1.3.11 Moving Users from the Default Region to Another Region

Security administrators can move users from the default region to another region. The users are then managed by the destination region administrator.

Prerequisites

- You have logged in to the NetEco as a security administrator.
- A region has been created. For details about how to create a region, see **4.2.1.3.3 Creating a Region**.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 Select the users to be moved, click ***, and choose **Move Selected Users**.

NOTE

Users attached to default roles, default users, third-party users, remote users, and the current user cannot be moved.

Step 4 Confirm the users to be moved in the list. Click **Next**.

Step 5 Select the destination region.

NOTE

After a user is moved out of the region, related roles will be detached from the user. If the user has logged in to the NetEco, this operation will force a logout of the user. Therefore, exercise caution when performing this operation.

Step 6 Click **Move**. On the **Moving Result** page, view the moving results and details.

After a user is moved, it is displayed in the user list of the destination region.

Step 7 Click **OK**.

----End

Follow-up Procedure

After a user is moved from the default region to another region, attach the user to roles again.

4.2.1.3.12 Moving Roles Out of a Region

When maintaining multiple regions, security administrators need to adjust some roles across regions. For example, security administrators may need to change a role in a region to a role in another region.

Prerequisites

- You have logged in to the NetEco as a security administrator.
- A region has been created. For details about how to create a region, see **4.2.1.3.3 Creating a Region**.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Regions**.

Step 3 Click the region to which to-be-moved roles belong to open the page of this region.

Step 4 Click the **Roles** tab, select the roles to be moved, click , and choose **Move Selected Roles**.

Step 5 Confirm the roles to be moved in the list. Click **Next**.

Step 6 Select the destination region.

NOTE

After a role is moved out of the region, related users, managed objects, and operation rights will be detached from the role. Perform this operation with caution.

Step 7 Click **Move**. On the **Moving Result** page, view the moving results and details.

After a role is moved, it is displayed in the role list of the destination region.

Step 8 Click **OK**.

----End

Follow-up Procedure

After moving a role out of a region, bind managed objects and operation rights to the role again.

4.2.1.3.13 Moving Users Out of a Region

When maintaining multiple regions, security administrators need to adjust the responsibilities of some users across regions. For example, security administrators may need to change a local user in a region to a security administrator or local user of another region.

Prerequisites

- You have logged in to the NetEco as a security administrator.
- A region has been created. For details about how to create a region, see **4.2.1.3.3 Creating a Region**.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Regions**.

Step 3 Click the region to which to-be-moved users belong to open the **User Management** page for the region.

Step 4 Select the users to be moved, click , and choose **Move Selected Users**.

NOTE

Third-party users, remote users, and users attached to a region administrator role cannot be moved.

Step 5 Confirm the users to be moved in the list. Click **Next**.

NOTE

To modify a user in **User List**, perform the following operations:

- If some users to be moved are not in the list, click **Cancel** and select the users to be moved again.
- If some users who do not need to be moved are in the list, click **Delete** in the **Operation** column of the rows that contain these users to delete them.

Step 6 Select the destination region.

NOTE

- After a user is moved, related roles will be detached from the user.
- Moving users out of a region will force a logout of users who have logged in to the NetEco. Therefore, exercise caution when performing this operation.

Step 7 Click **Move**. On the **Moving Result** page, view the moving results and details.

After a user is moved, it is displayed in the user list of the destination region.

Step 8 Click **OK**.

----End

Follow-up Procedure

After a user is moved out of a region, attach the user to roles again.

4.2.1.3.14 Monitoring Users in a Region

User sessions in a region can be monitored so that region administrators can know the online users of this region in the system, access addresses of these users, access time, and roles of the users. When detecting an unauthorized user operation, the system sends a message to the user or forcibly log out the user.

Prerequisites

You have logged in to the NetEco as a region administrator.

Context

- A user session refers to a connection between a user and the system. A session starts when the user logs in to the system and ends when the user logs out of the system. A user can generate multiple sessions.
- Multiple users can log in to the NetEco at the same time. The maximum number of login users is specified by the **Max. online sessions** parameter.
- User sessions in a region can be monitored only by region administrators.
- Users' personal information is not monitored during session monitoring.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Online Users**.

The status information about all online users in the region is displayed in the list.

NOTE

- **Client Name** indicates the name of the client where this session is generated.
- Third-party users do not consume resource control items.

Step 3 Click **Monitor** in the **Operation** column of the target user to view the status of the user.

- The **User Operations** list displays only operations performed after the **Online Users** page is opened. Operations of the monitored users are updated in the **User Operations** list in real time.
- **Level** indicates the risk level of an operation, including **Risk**, **Minor**, and **Warning**. The value of **Level** is the same as that recorded in operation logs.

Step 4 When detecting that a user is performing risky operations, click **Log Out** in the **Operation** column of the user to forcibly log out the user.

NOTICE

This operation involves user login status and may force a logout of logged-in users. Therefore, exercise caution when performing this operation.

Step 5 To send a message to a user, click **Send Message** in the **Operation** column of the user.

----End

4.2.1.4 User Maintenance

Security administrators can maintain user, role, and operation set information, and reset other users' passwords. Users can modify their personal information.

4.2.1.4.1 Common Operations for User Information Maintenance

Common operations for user information maintenance include viewing user information, enabling users, disabling users, deleting users, exporting user information, and modifying user information.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 Perform operations according to **Table 4-4** based on site requirements.

Table 4-4 User maintenance operations

Common Operation	Procedure
Viewing user information	Click a username to view the user information.
Disabling a user	Click **Disable** in the **Operation** column of the row that contains the user you want to disable.
Enabling a user	Click **Enable** in the **Operation** column of the row that contains the user you want to enable.

Common Operation	Procedure
Deleting users	Click **Delete** in the **Operation** column of the row that contains the user to be deleted or select the users to be deleted and click **Delete**. **NOTE** ● Default users, current user, and users attached to the **SMManagers** role cannot be deleted. ● Deleting a logged-in user will force a logout of the user. Therefore, exercise caution when performing this operation.
Importing user information	1. On the **Users** page, click ••• and choose **Import Users**. 2. On the **Import Users** page, click the template name to download the template and enter user information in the template. **NOTE** – The system provides two template formats: **User Template.xls** and **User Template.xlsx**, and you can edit the template in .csv format. Select a template format as required. – When editing a template in .csv format and creating a time policy, add double quotation marks before and after the time policy to ensure that the import is successful. The following shows an example. "NewTimePolicy;start-time:00:00,end-time:23:59;start-date:2017-01-01,end-date:2017-12-31;week:135" 3. Fill in user information based on the template. 4. Set **Import Mode**, and click . In the dialog box that is displayed, select the edited template. 5. Click **Create** or **Modify**. After the import is complete: a. On the displayed page, view the number of successfully imported operation sets and the number of operation sets that fail to be imported. b. In the **Result** list, view the imported users and their details. c. If partial failure occurs, modify the user information that failed to be imported based on the details, and import them again. 6. Click **OK**.
Exporting user information	To export information about all users, click ••• and choose **Export All Users**. To export information about certain users, select these users and click **Export Selected Users**. **NOTE** ● The **Password**, **Mobile number**, and **Email address** fields are not exported. Therefore, the values of these fields are empty in the exported user information file. ● The file is exported in .csv or .xlsx format and downloaded to the local PC as a .zip package.

Common Operation	Procedure
Modifying user information	1. Click the name of the user whose information needs to be modified. 2. Select the tab to be modified and click **Edit** to modify the user information. **NOTE** – **Auto-logout if no activity within**: If a user does not perform any operation within the period specified by this parameter, the user will be logged out. This parameter can be set for local users and remote users and cannot be set for third-party users. – During user modification, setting **Enable account** to **No** for a logged-in user will force a logout of the user. Therefore, exercise caution when performing this operation. 3. Click **OK**.
Unlocking users	• To unlock a user: Click **Unlock** in the **Operation** column of the row that contains the user. • To unlock users in batches: 1. **Optional:** You can change **All statuses** to **Locked** to quickly filter all locked users. 2. Select users to be unlocked. 3. Click ⋯ and choose **Batch Unlock Users**. **NOTE** Default users, unlocked users, current user, and users attached to the **SMManagers** role cannot be unlocked.

----End

4.2.1.4.2 Common Operations for Role Information Maintenance

Common operations for role information maintenance include viewing role information, deleting roles, exporting role information, and modifying role information.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Roles**.

Step 3 Perform operations according to **Table 4-5** based on site requirements.

Table 4-5 Role maintenance operations

Common Operation	Procedure
Viewing role information	Click a role name to view information about this role.
Deleting roles	Click **Delete** in the **Operation** column of the row that contains the role to be deleted or select the roles to be deleted and click **Delete**. **NOTE** • You cannot delete default roles and the roles to which the current user is attached. • Deleting roles will cause the users attached to these roles to lose the permissions of the roles. Therefore, exercise caution when performing this operation.
Exporting role information	Click *** and choose **Export All Roles** to export information about all roles. **NOTE** • If the number of roles exceeds 500, role information is exported to multiple files. That is, each file contains information about a maximum of 500 roles. • The file is exported in .csv or .xlsx format and downloaded to the local PC as a .zip package.
Modifying role information	1. Click the name of a role whose information needs to be modified. 2. Select the tab to be modified and click **Edit** to modify the role information. **NOTE** – You cannot modify the managed objects and operation rights of the roles to which the current user is attached. – You cannot modify the managed objects and operation rights of default roles. – Modifying the role information will change the permissions of users attached to this role. Therefore, exercise caution when performing this operation. The permission changes will take effect upon page refreshing or after next login of these users.
Saving information about role permissions	1. Click the name of the desired role. 2. Click the **Operation Rights** tab. 3. Click **Save** to save the information about the role permissions.

----End

4.2.1.4.3 Common Operations for Operation Set Information Maintenance

Common operations for operation set maintenance include viewing operation set information, deleting an operation set, and modifying operation set information. Importing and exporting operation sets are applicable to system data migration.

Prerequisites

You have logged in to the NetEco as a security administrator or the system administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Operation Sets**.

Step 3 Perform the following operations as needed.

Common Operation	Procedure
Viewing operation set information	Click an operation set name to view details about the operation set.
Deleting an operation set	Click **Delete** in the **Operation** column of the row that contains the operation set. **NOTE** • If the deleted operation set is associated with a user, the user will lose all operation rights included in the deleted operation set. • You cannot delete default operation sets and the operation sets to which the role of the current user is bound.
Modifying operation set information	1. Click the name of an operation set whose information needs to be modified. 2. Click **Edit** and modify the operation rights in the operation set. **NOTE** • If the modified operation set is associated with a user, the change takes effect the next time the user logs in. • You cannot modify operation rights included in default operation sets or the operation sets to which the role of the current user is bound.

Common Operation	Procedure
Importing operation sets **NOTE** Only the system administrator user is authorized to perform this operation.	1. Click ••• and choose **Import Operation Sets**. 2. On the **Import Operation Sets** page, click . 3. In the displayed dialog box, select the .zip file to be imported. 4. Click **Create**. When the import is complete, perform the following operations to check the import result: a. On the displayed page, view the number of successfully imported operation sets and the number of operation sets that fail to be imported. b. In the **Result** list, view the imported operation sets and their details. c. If partial failure occurs, modify the operation set information that failed to be imported based on the details, and import them again. 5. Click **OK** to close the **Import Operation Sets** page.
Exporting all operation sets **NOTE** Only the system administrator user is authorized to perform this operation.	Click ••• and choose **Export All Operation Sets** from the drop-down menu to export all operation sets excluding the full operation sets. In the exported .zip file, a .csv file contains a maximum of 100 operation sets of the same type. If the number of operation sets exceeds 100, the operation sets are exported to multiple files.

----End

4.2.1.4.4 Viewing Authorization Details

By viewing authorization details, security administrators can quickly learn the users or roles to which permissions are granted so that they can adjust their permissions in a timely manner.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Authorization Details**.

Step 3 In the **Authorization Objects** area, select authorization objects.

Step 4 In the **Operations** area, select the names of the permissions to be viewed.

Step 5 In the **Authorized Users and Roles** area, view the users and roles to which the permissions are assigned.

----End

Follow-up Procedure

If you find that the authorization is improper or illegal, adjust the permissions of the users or roles in time. For details, see **4.2.1.2 Permission Adjustment**.

4.2.1.4.5 Modifying User Information in Batches

Security administrators can modify user information (such as **Max. online sessions** and **Login Time Policy**) in batches, improving system security.

Prerequisites

You have logged in to the NetEco as a security administrator.

Context

- You can use the following methods to modify user information in batches:
  - Using the **Batch Modify Users** function

    Select the users whose information needs to be modified and click **Batch Modify Users**.
  - Modifying an exported user information file

    Export user information as a file, edit the file, and then import it to the system.
- The operations in this section involve user permission adjustment, which may force a logout of logged-in users. Therefore, exercise caution when performing this operation.

Procedure

- Using the **Batch Modify Users** function

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 In the user list, select one or more users, click , and choose **Batch Modify Users**.

Step 4 On the **User List** tab page, confirm the users whose information needs to be modified. Then, click **Next**.

Step 5 Select the users information to be modified on the **Modification Items** page as required. Click **OK**. On the **Modification Result** page, view the modification results and details.

If the existing time policies do not meet the requirements, click **Create** to create a policy and then click **Refresh**. Then, you can select the new time policy from the time policy list.

NOTE

- You cannot modify the system administrator user and your own information.
- A maximum of 100 users can be modified at a time.
- After the login time policy is modified, the users who do not meet the policy requirements will be forcibly logged out if **Log out of sessions that do not comply with client IP address or login time policies** is selected in the account policy.

Step 6 Click **OK**.

----End

- Modifying an exported user information file

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 Select the users whose information needs to be exported, click , and choose **Export Selected Users** or **Export All Users**.

Step 4 In the **Select File Format** dialog box, select a file format and click **OK**.

Step 5 Modify the exported user information file.

- When modifying the user information file, do not change the sequence of the fields in the file.
- If you change the value of a field to empty or an invalid value, the value of this field will not be changed.
- The following user information cannot be modified:
  - **Type** and **Region** of all users
  - Your own information and information about the system administrator user
  - **Password**, **Login Time Policy**, **Client IP Address Policy**, **Personal Client IP Address Policy**, and **Password Validity Period (Days)** of remote users
  - **Roles**, **Login Time Policy**, and **Allowed logins** of default users
  - **Password** and **Auto-Logout If No Activity Within** of third-party users

Step 6 Click and choose **Import Users**.

Step 7 In the **Import Users** window, choose **Update Users** to import users.

Step 8 Click , select the modified user information file, and click **Modify**.

Step 9 After the import is complete:

- On the displayed page, view the number of successfully modified users and the number of users who fail to be modified.
- In the **Result** list, view the imported users and their details.

Step 10 Click **OK**.

----End

4.2.1.4.6 Changing Personal Password

If passwords are disclosed or remain unchanged for a long time, users can change their personal passwords by setting personal information. To improve user security, it is recommended that passwords be changed periodically (for example, every three months).

Context

If you cannot change your password, contact the security administrator.

Procedure

Step 1 Choose **System** > **System Settings** > **Personal Settings** from the main menu.

Step 2 In the navigation pane, choose **Change Password**.

Step 3 On the **Change Password** tab page, enter **Old password** and set **New password** and **Confirm password**.

Step 4 Click **Apply**.

NOTE

User information is more secure if a password is changed more frequently. If a user forgets the password due to frequent password changes, contact security administrators to reset the password.

----End

4.2.1.4.7 Modifying Personal Information

When personal information such as mobile numbers and email addresses changes or needs to be supplemented, users can periodically maintain their personal information by setting personal information to ensure its accuracy.

Procedure

Step 1 Choose **System** > **System Settings** > **Personal Settings** from the main menu.

NOTICE

- When you modify your personal information, such as mobile numbers and email addresses, you are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that your personal data is fully protected.
- To ensure the security of personal information, such as mobile numbers and email addresses, these data is anonymized on the page, and HTTPS encryption transmission channels are used.

Step 2 In the navigation pane, choose **Modify Personal Info**.

Step 3 On **Modify Personal Info**, modify personal information as required.

NOTE

If the SMS and email verification codes cannot be obtained, ensure that the remote notification function is configured correctly.

Table 4-6 Parameter description

Parameter	Description	Procedure
Associate Mobile Number	Mobile number associated with a user account.	• Editing the mobile number 1. Click **Edit**. 2. Verify the identity information as prompted and click **Next**. 3. Select a country or region code and enter a new mobile number. 4. Click **Send Code** and enter the obtained verification code to verify that the mobile number is valid. 5. Click **OK**. • Verifying the mobile number 1. Click **Verify**. 2. Click **Send Code** and enter the obtained verification code to verify that the mobile number is valid. 3. Click **OK**.
Associate Email Address	Email address associated with a user account.	• Editing the email address 1. Click **Edit**. 2. Verify the identity information as prompted and click **Next**. 3. Enter a new email address. 4. Click **Send Code** and enter the obtained verification code to verify that the email address is valid. 5. Click **OK**. • Verifying the email address 1. Click **Verify**. 2. Click **Send Code** and enter the obtained verification code to verify that the email address is valid. 3. Click **OK**.

Parameter	Description	Procedure
Auto-Logout If No Activity Within	If a user does not perform any operation within the period specified by this parameter after login, the user will be logged out. This parameter can be set for local users and remote users. The default value for the third-party user is 30 minutes and cannot be changed.	1. Click the drop-down list and select a value for **Auto-Logout If No Activity Within**. 2. Click **Save**.
Max. Online Sessions	You can set the maximum number of online sessions. This parameter is unselected by default, indicating that the maximum number of online sessions of an account is not limited. If this parameter is enabled, the default value is **1**, and the value range is from 1 to 500. ● If this parameter is set to **1**, **Login when maximum online sessions already in use** can be **Not allowed** or **Log out of the session**. ● If this parameter is set to a value from 2 to 500, **Login when maximum online sessions already in use** is set to **Not allowed** and cannot be changed.	1. Select **Max. online sessions** to enable this function. 2. Set the number of maximum online sessions. 3. Click **Save**.
Welcome Message	You can set the information to be displayed upon the next login.	1. Click **Edit**. 2. Enter the information to be displayed upon the next login. 3. Click **OK**.

----End

4.2.1.4.8 Resetting a User Password

If a user forgets the password or cannot change the password, this user needs to contact security administrators to reset the password. If a security administrator

forgets the password, this user needs to contact the system administrator user to reset the password.

Prerequisites

You have logged in to the NetEco as a security administrator or the system administrator.

Context

This operation will force a logout of users who have logged in to the management system and selected **Force logout after password change** in the password policy. Therefore, exercise caution when performing this operation.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Users**.

Step 3 Click **Reset Password** in the **Operation** column of the row that contains the user and reset the password.

NOTICE

- You are not allowed to reset the password for the system administrator user. The password for the system administrator user cannot be retrieved. You can reset the password for the system administrator user only by reinstalling the system. Therefore, remember the password.
- For account security purposes, it is recommended that third-party users contact security administrators to periodically reset their passwords.

----End

4.2.1.5 User Monitoring

User sessions can be monitored so that security administrators can know the online users in the system, access addresses of these users, access time, and roles of the users. When detecting an unauthorized user operation, the system sends a message to the user or forcibly log out the user.

Prerequisites

You have logged in to the NetEco as a security administrator.

Context

- A user session refers to a connection between a user and the system. A session starts when the user logs in to the system and ends when the user logs out of the system. A user can generate multiple sessions.

- The maximum number of online sessions for a user is specified by the **Max. online sessions** parameter.
- Users' personal information is not monitored during session monitoring.

Procedure

Step 1 Choose **System** > **System Management** > **User Management** from the main menu.

Step 2 In the navigation pane, choose **Online Users**.

The information about all online users is displayed in the list.

NOTE

- **Client Name** indicates the name of the client where this session is generated.
- Third-party users do not consume resource control items.

Step 3 Click **Monitor** in the **Operation** column of the target user to view the status of the user.

- The **User Operations** list displays only operations performed after the **Online Users** page is opened. Operations of the monitored users are updated in the **User Operations** list in real time.
- **Level** indicates the risk level of an operation, including **Risk**, **Minor**, and **Warning**. The value of **Level** is the same as that recorded in operation logs.

Step 4 To send a message to a user, click **Send Message** in the **Operation** column of the user. Alternatively, select multiple users and click **Send Message** in the upper right of the user list to send messages to these users.

Step 5 When detecting that a user is performing risky operations, click **Log Out** in the **Operation** column of the user to forcibly log out the user. Alternatively, select multiple users and click **Log Out** in the upper right of the user list to force a logout of these users in batches.

NOTICE

This operation involves user login status and may force a logout of logged-in users. Therefore, exercise caution when performing this operation.

----End

4.2.2 Personal Settings

This feature enables users to customize personal settings.

4.2.2.1 Changing Personal Password

If passwords are disclosed or remain unchanged for a long time, users can change their personal passwords by setting personal information. To improve user security, it is recommended that passwords be changed periodically (for example, every three months).

Context

If you cannot change your password, contact the security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **Personal Settings**.

Step 2 In the navigation pane, choose **Change Password**.

Step 3 On the **Change Password** tab page, enter **Old password** and set **New password** and **Confirm password**.

Step 4 Click **Apply**.

NOTE

User information is more secure if a password is changed more frequently. If a user forgets the password due to frequent password changes, contact security administrators to reset the password.

----End

4.2.2.2 Modifying Personal Information

When personal information such as mobile numbers and email addresses changes or needs to be supplemented, users can periodically maintain their personal information by setting personal information to ensure its accuracy.

Procedure

Step 1 Choose **System** > **System Management** > **Personal Settings**.

NOTICE

- When you modify your personal information, such as mobile numbers and email addresses, you are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that your personal data is fully protected.
- To ensure the security of personal information, such as mobile numbers and email addresses, these data is anonymized on the page, and HTTPS encryption transmission channels are used.

Step 2 In the navigation pane, choose **Modify Personal Info**.

Step 3 On **Modify Personal Info**, modify personal information as required.

NOTE

If the SMS and email verification codes cannot be obtained, ensure that the remote notification function is configured correctly.

Table 4-7 Parameter description

Parameter	Description	Procedure
Associate Mobile Number	Mobile number associated with a user account.	• Editing the mobile number 1. Click **Edit**. 2. Verify the identity information as prompted and click **Next**. 3. Select a country or region code and enter a new mobile number. 4. Click **Send Code** and enter the obtained verification code to verify that the mobile number is valid. 5. Click **OK**. • Verifying the mobile number 1. Click **Verify**. 2. Click **Send Code** and enter the obtained verification code to verify that the mobile number is valid. 3. Click **OK**.
Associate Email Address	Email address associated with a user account.	• Editing the email address 1. Click **Edit**. 2. Verify the identity information as prompted and click **Next**. 3. Enter a new email address. 4. Click **Send Code** and enter the obtained verification code to verify that the email address is valid. 5. Click **OK**. • Verifying the email address 1. Click **Verify**. 2. Click **Send Code** and enter the obtained verification code to verify that the email address is valid. 3. Click **OK**.

Parameter	Description	Procedure
Auto-Logout If No Activity Within	If a user does not perform any operation within the period specified by this parameter after login, the user will be logged out. This parameter can be set for local users and remote users. The default value for the third-party user is 30 minutes and cannot be changed.	1. Click the drop-down list and select a value for **Auto-Logout If No Activity Within**. 2. Click **Save**.
Max. Online Sessions	You can set the maximum number of online sessions. This parameter is unselected by default, indicating that the maximum number of online sessions of an account is not limited. If this parameter is enabled, the default value is **1**, and the value range is from 1 to 500. ● If this parameter is set to **1**, **Login when maximum online sessions already in use** can be **Not allowed** or **Log out of the session**. ● If this parameter is set to a value from 2 to 500, **Login when maximum online sessions already in use** is set to **Not allowed** and cannot be changed.	1. Select **Max. online sessions** to enable this function. 2. Set the number of maximum online sessions. 3. Click **Save**.
Welcome Message	You can set the information to be displayed upon the next login.	1. Click **Edit**. 2. Enter the information to be displayed upon the next login. 3. Click **OK**.

Parameter	Description	Procedure
Display Associate Contact Information Page	This parameter specifies whether the **Associate Contact Information** page is displayed when the user logs in next time. • If this parameter is enabled, the **Associate Contact Information** page is displayed. • If this parameter is disabled, the **Associate Contact Information** page is not displayed.	• Click **Enable**. • Click **Disable**. **NOTE** In SSO mode, contact information can be associated only on the **Associate Contact Information** page. Exercise caution when setting this parameter.

----End

4.2.2.3 Modifying Personal Client IP Address Control Policies

With the **Update ACL Policy** permission, you can configure your personal client IP address control policies. ACL is short for access control list.

Procedure

Step 1 Choose **System** > **System Management** > **Personal Settings**.

Step 2 In the navigation pane, choose **Personal Client IP Address Policies**.

Step 3 On the **Personal Client IP Address Policies** page, view or modify your IP address control policies.

----End

4.2.2.4 Home Settings

After the home page information is configured, the page set by the user is displayed by default upon the next login, which helps users quickly view the menus that they want to follow.

Procedure

Step 1 Choose **System** > **System Management** > **Personal Settings**.

Step 2 In the navigation pane on the left, choose **Home Settings**.

Step 3 Paste the copied page URL to the URL bar on the home page and click **Apply**.

----End

4.2.3 Log Management

By managing fault logs of devices, users can learn the running status of devices.

4.2.3.1 Querying Logs

A log records the operations and major events of the management system. By querying logs, you can learn about the running status and operation details of the management system.

Prerequisites

You have the operation rights for **Log Management**.

Context

Management system logs are classified into security logs, system logs, and operation logs.

- Security logs record security operations that are performed on the management system, such as logging in to the server, changing passwords, creating users, and logging out of the server.
- System logs record the events occurred on the management system, such as abnormal running, network failures, and attacks to the management system. These logs help you analyze the NMS status and rectify faults.
- Operation logs record the user operations that are performed on the management system.

Procedure

Step 1 Choose **System** > **System Management** > **Log Management**.

Step 2 In the navigation tree in the left pane, choose **Security Logs**, **System Logs** or **Operation Logs**.

Step 3 On the page, view the log information, or set search criteria to view specified log information.

After clicking the value in the **Details** column of the target log, you can view logs details.

NOTE

A maximum of 1000 characters can be displayed in **Details**. The excess characters are displayed in the **A-B** form.

The management system server time is used for the filter criteria **Time period**. The value is 24 hours before the current time. For example, if the current time is 11:00:00, November 12, 2020, the default value of time period is from 11:00:00, November 11, 2020 to 11:00:00, November 12, 2020.

----End

Follow-up Procedure

You can export the logs and back them up for future analysis.

NOTICE

Switching between pages will cause log exporting to be interrupted.

If...	Then...
Export all logs	1. Click **Export All** to export all logs. 2. In the **File Download** dialog box, click **Save**. 3. Select a save path and click **Save**. **NOTE** Log files must be saved in **.csv** format.
Export the selected logs	1. In the log list, select the check box before **Event Name** of the required log. 2. Click **Export Selected** to export the selected logs. 3. In the **File Download** dialog box, click **Save**. 4. Select a save path and click **Save**. **NOTE** Log files must be saved in **.csv** format.

4.2.4 User Policy Management

User policies allow you to set access control rules for users. This function improves O&M efficiency and prevents unauthorized users from accessing the system to ensure system security.

4.2.4.1 Setting the Account Policy

Security administrators set login or lockout policies for user accounts as needed to improve system access security. The account policy takes effect for all users.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Policies** from the main menu.

Step 2 In the navigation pane, choose **Account Policy**.

Step 3 On the **Account Policy** page, set the account policy.

NOTE

- If **Enable the user policy if no login within a period** is selected, the system will automatically delete the users who meet the policy. Perform this operation with caution.
- **Auto-logout if no activity within**: If a user does not perform any operation within the period specified by this parameter, the user will be logged out. The setting takes effect only for local and remote users and does not take effect for third-party users. If this parameter is set to **Unlimited**, user sessions will not be automatically logged out.
- If **Show warning upon successful login** is selected, a login warning message is displayed to notify users of rules that should be obeyed after users log in to the system. The warning message provides legal declaration. Security administrators can customize this warning message based on user management regulation.
- To improve account security, you are advised to enable all the items in the account policy.

Step 4 Click **Apply**.

----End

4.2.4.2 Setting the Password Policy

Security administrators set password complexity, change interval, and character limitation as needed to prevent users from setting weak passwords or using a password for a long period of time, improving system access security. The password policy takes effect for all users.

Prerequisites

You have logged in to the NetEco as a security administrator.

Context

- If you disable the password complexity policy items and the item of forcibly changing passwords after they expire, user security reduces. You are advised to enable all password policies provided by the system.
- If the settings of the same policies in the personal policy of a user and the password policy are different, the settings in the personal policy take effect for the user.
- Periodically changing passwords can improve user information security and prevent accounts from being stolen. Exercise caution when disabling the function of periodically changing passwords and modifying a password change period.
- A new password policy does not affect the existing passwords.

Procedure

Step 1 Choose **System** > **System Management** > **User Policies** from the main menu.

Step 2 In the navigation pane, choose **Password Policy**.

Step 3 On the **Password Policy** page, set the password policy. Some of the policy parameters are described in **Table 4-8**.

Table 4-8 Parameter description

Parameter	Description
Force logout upon password reset	When a user password is reset, all online sessions generated by the user will be logged out.
Password cannot be an increasing, decreasing, or interval sequence of digits or letters	When setting a user password, the password must meet the following requirements: • The password cannot be digits or letters in ascending or descending sequence. For example, the password cannot be **abcdef**, **fedcba**, **123456**, or **654321**. • The password cannot contain an ascending or descending arithmetic sequence in consecutive odd digits or even digits. For example, the password cannot be **1a2a3a**, **5a3a1a**, **a2b2c2**, or **2e2c2a**.
Password cannot contain words in password dictionary	When you create a user and set the password, the password cannot contain words in the password dictionary. • No default password dictionary is provided. You can customize a password dictionary. For example, **abcd1234** is a weak password and if it is added to the password dictionary, **abcd1234** cannot be used as a user password. • In a password dictionary file, passwords are separated by line feeds. In the dictionary, a password that contains more than 128 characters is invalid. **NOTE** To update the password dictionary, perform the following steps: 1. Click **Download Password Dictionary** to download the existing password dictionary and modify it as required. 2. Click  and select the modified password dictionary. 3. Click **Upload** to update the password dictionary.

Parameter	Description
Convert strings in password based on conversion rules (refer to help documentation to configure the rules) **NOTE** This parameter is displayed only when **Password cannot contain words in password dictionary** is selected.	If a password contains a character string defined in the string conversion rules, the character string is converted into other characters based on certain rules. The converted password must meet complexity requirements. The string conversion rules define the rules for converting a character or string into an uppercase or lowercase letter. For example, if a rule for converting the string **|-|1234 a** into **x** exists in the string conversion rules, and **xbcd!123** is contained in the password dictionary, and when the policy is enabled, **|-|1234 abcd!123** cannot be used as a user password. **NOTE** • For details about how to configure the string conversion rules, see "Configuring the String Conversion Rules of User Management". • Strings refer to strings consisting of dangerous characters, invisible characters, and characters incurring SQL injection.

Step 4 Click **Apply**.

----End

4.2.4.3 Setting a Client IP Address Policy

A client IP address policy provides a control mechanism for checking the accessibility of the IP address used by an external access request. Security administrators can set client IP address policies as required and bind the policies to specified users. The policies take effect only for the bound users. In this way, users can log in to the management system only from specified IP address segments, which improves system security.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Policies** from the main menu.

Step 2 In the navigation pane, choose **Client IP Address Policies**.

Step 3 On the **Client IP Address Policies** page, click **Create**.

Step 4 Set a client IP address policy and click **OK**.

NOTICE

Exercise caution when you set the client IP address policies for the system administrator user. If the client IP address of the system administrator user is not within the bound IP address range, the user cannot log in again after logout.

----End

4.2.4.4 Setting a Login Time Policy

A login time policy provides a control mechanism for checking the validity time of an external access request during system operation. Security administrators can set login time policies as required and bind the policies to specified users. The policies take effect only for the bound users. In this way, users can log in to the management system only within the specified time segments, which improves system security.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **System Management** > **User Policies** from the main menu.

Step 2 In the navigation pane, choose **Login Time Policies**.

Step 3 On the **Login Time Policies** page, click **Create**.

Step 4 Set the parameters of the login time policy and click **OK**.

NOTE

- The system administrator user is not restricted by the login time policy.
- If the start time is later than the end time for **Effective hours**, the system will automatically set the end time to the next day. For example, if **Effective hours** is set to 16:00–15:00, login is allowed within 16:00–24:00 today and 0:00–15:00 the next day.

----End

4.2.5 Security Configuration

The security configuration function provides the system security baselines (such as protocols, algorithms, and keys), and checks for risks of protocols, keys, and algorithms used by services and service configuration items based on the security baselines. Based on the check results, it provides risk warnings and rectification suggestions. This allows the security capabilities of different services to be monitored in a unified manner and ensures system security.

4.2.5.1 Overview of Security Configuration

This section describes basic information about the security configuration function, including its definition, benefits, scenarios, functions, and principles.

4.2.5.1.1 Definition

The security configuration function monitors service configuration items in a unified manner, checks security configurations, and manages security baselines.

Security baselines consist of a series of security requirements and specifications, including protocols, algorithms, and keys. The security configuration function checks for risks of service configuration items based on security baselines.

4.2.5.1.2 Benefits

The security configuration function allows you to monitor protocols, keys, and algorithms used by services and service configuration items, improving management efficiency. Security administrators can rectify security risks based on the check results to ensure service security.

4.2.5.1.3 Scenarios

During routine maintenance, security administrators can use the security configuration function to check whether the protocols, keys, algorithms, and service configurations used by services meet the security baselines, ensuring service security.

4.2.5.1.4 Functions

The security configuration function allows you to check service configurations and view security baselines.

- Checking service configurations

  Checks whether service configuration items have risks based on security baselines, and provides risk warnings and rectification suggestions.
- Viewing security baselines

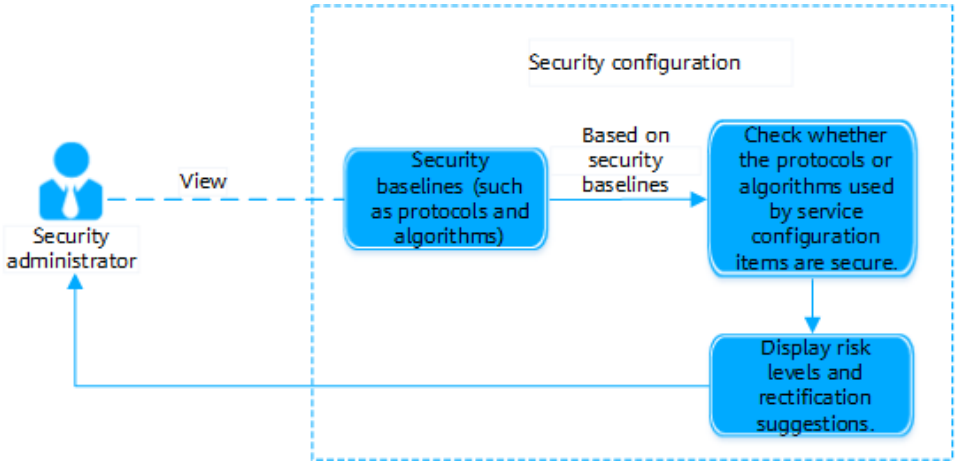
  Displays security protocols and algorithms used by services.

4.2.5.1.5 Principles

The security configuration function checks for risks of service configuration items based on security baselines, and provides risk warnings and rectification suggestions. This helps security administrators detect and handle security risks of services in a timely manner.

Figure 4-4 shows the principles of the security configuration function.

Figure 4-4 Principles of the security configuration function



4.2.5.2 Viewing Security Baselines

A security baseline provides secure protocols and algorithms for services. The system checks whether protocols and algorithms used by services are secure based on the security baseline.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **Security Configuration** from the main menu.

Step 2 In the navigation pane, choose **Security Baseline**.

Step 3 On the **Security Baseline** page, click the card of required baseline.

Step 4 View the configured security baseline.

The security configuration function will check for risks of protocols, keys, and algorithms used by services based on the security baseline, and provide risk warnings and rectification suggestions.

----End

4.2.5.3 Checking Security Configurations

Security administrators can configure check policies based on service security requirements to periodically check whether protocols, keys, and algorithms used by services meet the security baselines, and rectify the risks based on the check results. To meet special requirements such as compatibility requirements, you can configure insecure protocols, keys, and algorithms on the panel for risk details. Exercise caution when performing this operation. For service function security, you are advised to use secure protocols, keys, and algorithms.

Prerequisites

You have logged in to the NetEco as a security administrator.

Procedure

Step 1 Choose **System** > **Security Configuration** from the main menu.

Step 2 On the **Configuration Check** page, check a single item or check items in batches as required.

- Checking a single item

  Click **Check** in the **Operation** column of the row that contains the required item.

- Checking items in batches

  Click **Check Now** to check all items.

  NOTE

  Click **Set Check Time** and set the daily check time. The security configuration function automatically checks service configuration items every day based on the set time.

Step 3 View the check results.

- After the check is complete, view the results in the **Check Result** column.
- In the upper part of the **Configuration Check** page, view the result distribution charts of all check items so that you can learn about the overall risk information.

Step 4 Click the name of a desired configuration item. On the panel that is displayed, view the details about the risk. You can rectify the risk based on the suggestions.

Step 5 **Optional:** If **Configuration Item** can be set on the panel of risk details, set **Configuration Item** based on site requirements and click **Save**.

NOTE

If the modified value contains insecure protocols, keys, or algorithms, security risks may occur. Exercise caution when performing this operation. For service function security, you are advised to use secure protocols, keys, and algorithms.

----End

Related Tasks

- Adding an item to the whitelist: If a service configuration item does not have security risks or is not used, click **Add to Whitelist** in the **Operation** column of the row that contains the item to add it to the whitelist. The security configuration function will exclude items in the whitelist when performing the security check to improve the check efficiency.
- Removing an item from the whitelist: If the security check needs to include a whitelist item, click **Remove from Whitelist** in the **Operation** column of the row that contains the item.

4.3 About

4.3.1 Certificate Management

Certificate Management involves service certificate management, CA interconnection configuration, and certificate application. Service certificates can

be managed (including preconfiguration, import, deletion, and periodic validity check) in a centralized manner, and you can quickly apply for and use the certificates.

4.3.1.1 Managing Service Certificates

This section describes how to import certificates, including identity certificates, trust certificates, and certificate revocation lists (CRLs).

Prerequisites

- The service that requires certificate management has been deployed.
- You have the following permissions: **Query Certificate**, **Import Certificate**, and **Delete Certificate**.
- You have obtained the certificate to be imported or updated and its information, including passwords, certificate type, public key, private key, private key password, and certificate chain of the identity certificate.

Context

If the page for configuring certificates of a service does not contain the **Identity Certificate**, **Trust Certificate**, or **Certificate Revocation List** tab page, the service does not have the corresponding type of certificate and the corresponding tab page does not need to be displayed.

Procedure

Step 1 Choose **System** > **About** > **Certificate Management** from the main menu.

Step 2 In the navigation pane, select **Service Certificate Management**.

Step 3 On the **Services** page, click the service with certificate to be imported.

Step 4 Configure the certificate information based on the certificate type. The identity certificate is used as an example.

1. Click the **Identity Certificate** tab.

   NOTE

   - If the certificate type is trust certificate, click the **Trust Certificate** tab.
   - If the certificate type is certificate revocation list, click the **Certificate Revocation List** tab.

2. Click **Import**.
3. Configure the certificate information.

Step 5 Click **Submit**.

----End

Related Tasks

- Delete certificates

NOTE

Deleting certificates may cause the services that use the certificates to become interrupted. Exercise caution when deleting certificates.

Click in the Operation column of the row that contains the desired certificate to delete the certificate.

- View the certificate update status.

  For an imported certificate, view the certificate update status in **Certificate Update Status**.

  NOTE

  If the **Certificate Update Status** tab page is not displayed for a service, the service does not need to use this function, which is normal.

Follow-up Procedure

Restart the corresponding service for the imported certificate to take effect. For details, see "Uploading and Updating Certificates Using Certificate Management" in *Administrator Guide*.

4.3.1.2 Restoring Historical Certificates

If an identity certificate in use is overwritten by another identity certificate or is deleted by mistake, you can use the historical certificate function to restore the certificate to ensure that services are running properly.

Prerequisites

You have the **Query Certificate** and **Import Certificate** permissions.

Procedure

Step 1 Choose **System** > **About** > **Certificate Management** from the main menu.

Step 2 In the navigation pane, select **Service Certificate Management**.

Step 3 On the **Services** page, click the service with certificates to be imported.

Step 4 Click the **Identity Certificate** tab.

Step 5 Click **Historical Certificates**.

Step 6 On the **Historical Certificates** page, click in the **Operation** column of the row that contains the desired certificate.

Step 7 In the **High Risk** dialog box, read the information carefully and confirm whether to restore the certificate.

- If yes, select **I understand the risk and want to continue**, click **OK**, and go to **Step 8**.
- If no, click **Cancel** to end the operation.

Step 8 In the **Information** dialog box, read information carefully and click **OK**.

----End

Related Tasks

View certificate information.

In the historical certificate list, click > in the row that contains the desired certificate to view the certificate details.

4.3.1.3 Importing Global Shared Certificates

This section describes how to import a certificate revocation list (CRL) to global shared certificates. Services can call interfaces to obtain the CRLs in the global shared certificate list and verify the validity of their certificates based on the obtained CRLs.

Prerequisites

- You have the **Query Global Shared Certificate**, **Import Global Shared Certificate**, and **Delete Global Shared Certificate** permissions.
- You have obtained the CRL to be imported.

Context

The following certificates are displayed in the list of global shared certificates:

- CRLs imported by users
- CRLs obtained from the CRL server interconnected with HiSecCAProxy

Procedure

Step 1 Choose **System** > **About** > **Certificate Management** from the main menu.

Step 2 In the navigation pane, choose **Global Shared Certificates**.

Step 3 On the **Certificate Revocation List** tab page, click **Import**.

Step 4 Configure the certificate information as required.

NOTE

The certificate alias must be the same as the IP address of the MAE NMS to distinguish different NMSs.

----End

Related Tasks

- View certificate information.

  In the global shared certificate list, click > in the row that contains the desired certificate to view the certificate details.
- Delete certificates.

  NOTE

  After a CRL file is deleted, the certificate revoked by this CRL will become valid again. Exercise caution when performing this operation.

To delete an existing global shared certificate, perform either of the following operations:

Method 1: Click  in the **Operation** column of the row that contains the desired certificate to delete the certificate.

Method 2: Select the desired certificates, and click **Delete** in the upper right corner of the **Global Shared Certificates** page to delete the certificates.

4.3.1.4 Configuring CA Interconnection Parameters

This section describes how to configure parameters for interconnecting NetEco with the CA so that you can apply for certificates online using certificate management.

Prerequisites

- You have the following permissions: **Query CA Configuration**, **Manage CA Configuration**, and **Delete CA Configuration**.
- You have obtained the information about the CA server, including the IP address, port number, and the address information.
- You have obtained the certificate information from the CA and have configured on the local system, including the public key, public key certificate chain, private key, private key password, certificate chain of the trusted CA, and CA certificate chain.

Procedure

Step 1 Choose **System** > **About** > **Certificate Management** from the main menu.

Step 2 In the navigation pane, choose **Online Certificate Update** > **CA Interconnection**.

Step 3 Click **Create**.

Step 4 Configure the parameters for interconnecting with the CA as required.

Step 5 Click **OK**.

----End

Related Tasks

- Check and view the connectivity of the CA.

  Click  in the **Operation** column of the row that contains the configured CA to check the connectivity of the CA, and view the result in the **Connection Status** column.

- Modify the CA information.

  NOTE

  Modifying a configured CA may interrupt services between NetEco and the CA and cause a failure to apply for certificates. Therefore, exercise caution when performing this operation.

  Click  in the **Operation** column of the row that contains the configured CA to modify its information.

- Delete the CA.

  NOTE

  Deleting a configured CA will interrupt services between NetEco and the CA and cause a failure to apply for certificates. Therefore, exercise caution when performing this operation.

  Click  in the **Operation** column of the row that contains the configured CA to delete the CA.

4.3.1.5 Configuring CRL Server Parameters

This section describes how to interconnect NetEco with a CRL server. After NetEco is interconnected with a CRL server, you can obtain certificate revocation lists (CRLs) from the server.

Prerequisites

- You have the **Query CRL Server Interconnection**, **Manage CRL Server Interconnection**, and **Delete CRL Server Interconnection** permissions.
- You have obtained the following information about the CRL server to be interconnected:
  - IP address
  - Port number
  - Username
  - Password for the user
  - Trust certificates used to verify the CRL server

Procedure

Step 1 Choose **System** > **About** > **Certificate Management** from the main menu.

Step 2 In the navigation pane, choose **Online Certificate Update** > **CRL Server Interconnection**.

Step 3 Click **Create**.

Step 4 Configure the interconnection parameters as prompted.

Step 5 Click **OK**.

----End

Related Tasks

- Check and view the connectivity of the CRL server.

  Click  in the **Operation** column of the row that contains the configured CRL server to check the connectivity of the CRL server, and view the result in the **Connection Status** column.
- Modify the CRL server information.

NOTE

Modifying a configured CRL server may interrupt services between NetEco and the CRL server and cause a failure to apply for certificates. Therefore, exercise caution when performing this operation.

Click in the **Operation** column of the row that contains the configured CRL server to modify the CRL server information.

- Delete the CRL server.

NOTE

Deleting a configured CRL server will interrupt services between NetEco and the CRL server and cause a failure to apply for certificates. Therefore, exercise caution when performing this operation.

Click in the **Operation** column of the row that contains the configured CRL server to delete the CRL server.

Follow-up Procedure

After NetEco is interconnected with the CRL server and the connectivity is verified normal, check whether the CRL on the server is displayed in the global shared certificate list.

- If yes, the CRL is obtained successfully from the server.
- If no, contact technical support.

4.3.1.6 Creating Certificate Application Templates

This section describes how to create a template for applying for certificates based on the information about the required certificate. By using a template, the repeated configurations of certificate update tasks are reduced, so that you can quickly apply for new certificates.

Prerequisites

- You have the following permissions: **Query Certificate Application Template**, **Manage Certificate Application Template**, and **Delete Certificate Application Template**.
- You have obtained the certificate format, validity period, key algorithm, key length, certificate type, key usage, and extended key usage from the interconnected CA, ensuring that the planned certificate information is correct.
- You have planned the information about the certificate, such as the certificate format, common name (CN), country or region (C), province or state (ST), city (L), organization (O), department (OU), validity period, key algorithm, and key length, subject alternative name, certificate type, key usage, and extended key usage.

Context

- The validity period of a certificate applied from the CA is jointly determined by the customized validity period, validity period of the CA root certificate,

maximum validity period supported by the CA, and validity period of the application template supported by the CA. Generally, the validity period does not exceed the maximum validity period supported by the CA and the validity period of the application template supported by the CA. The actual validity period depends on the interconnected CA.

- **Table 4-9** describes the certificate formats, key algorithms, key lengths, certificate types, key usages, and extended key usages supported by certificate management.

Table 4-9 Certificate information

Parameter	Description
Certificate Format	Format of the certificate. • PEM • PKCS12
Key algorithm	Key algorithm of the certificate. • RSA • ECDSA **NOTE** RSA whose length is 2047 bits or shorter is insecure. You are advised to use the certificate encrypted by RSA whose length is 3072 bits or longer.
Key length	• Length of the RSA certificate key: – 2048 – 3072 – 4096 – 6144 – 8192 • Length of the ECDSA certificate key: – 256 – 384 – 521
Certificate type	Type of the certificate. • End Entity: Select this type if you do not need to use the key corresponding to the certificate to issue the certificate. • CA: Select this type when you need to use the corresponding key to issue a certificate.

Parameter	Description
Key usage	Usage of the certificate key. • Digital signature: Select this usage if the certificate requires identity authentication and data integrity authentication. • Non-repudiation: Select this usage if the certificate requires authentication on the digital signature of the public key to prevent the signing entity from denying its requests. • Key encipherment: Select this usage if the certificate requires an encryption protocol. • Data encipherment: Select this usage if the certificate encrypts its application data. • Key agreement: Select this usage if the public key is used by the sender and receiver to encrypt data during communication through plaintext agreement. • Certificate signing: Select this usage if the public key authenticates the certificate signature. It can only be used as a proxy certificate. • CRL signing: Select this usage if the public key of the certificate is used to verify the signature on the revocation information. • Encipher only: Select this usage if **Key agreement** is selected. The public key is used only for encrypting data during the agreement. • Decipher only: Select this usage if **Key agreement** is selected. The public key is used only deciphering data during the key agreement.
Extended key usage	Extended usage of the certificate key. • Server authentication: TLS WWW server authentication. Select this usage when **Digital signature**, **Key encipherment**, or **Key agreement** in **Key usage** is selected. • Client authentication: TLS WWW client authentication. Select this usage when **Digital signature** or **Key agreement** in **Key usage** is selected. • Email protection: Email protection. Select this usage when the **Digital signature**, **Non-repudiation**, **Key encipherment**, or **Key agreement** in **Key usage** is selected.

Procedure

Step 1 Choose **System** > **About** > **Certificate Management** from the main menu.

Step 2 In the navigation pane, choose **Online Certificate Update** > **Certificate Application Templates**.

Step 3 Click **Create**.

Step 4 Configure the template parameters as required.

Step 5 Click **OK**.

----End

Related Tasks

- Modify the certificate template.

  Click  in the **Operation** column of the row that contains the desired certificate template to modify the template information.
- Delete the certificate template.

  Click  in the **Operation** column of the row that contains the desired certificate template to delete the template.

4.3.1.7 Certificate Update Tasks

This section describes how to apply for certificates by using an existing certificate template or manually configuring certificate information, and how to apply certificates to services. To prevent security issues caused by private key leakage, you need to periodically update the certificates to improve system security. If a certificate is about to expire or the private key of a certificate is leaked, update the certificate immediately.

Prerequisites

- The parameters for interconnecting with the CA have been configured. For details, see **4.3.1.4 Configuring CA Interconnection Parameters**.
- You have the following permissions: **Query Certificate Application Task** and **Manage Certificate Application Task**.
- You have obtained the certificate format, validity period, key algorithm, key length, certificate type, key usage, and extended key usage from the interconnected CA, ensuring that the planned certificate information is correct.
- You have obtained the information about the certificate, such as the certificate format, common name (CN), country or region (C), province or state (ST), city (L), organization (O), department (OU), validity period, key algorithm, and key length, subject alternative name, certificate type, key usage, and extended key usage.

Context

- The time difference between NetEco and the CA must be less than 5 minutes. Otherwise, the certificate application fails.
- For security purposes, the password must meet the following complexity requirements:
  - Contain 8 to 64 characters.

  - Contain at least three of the following: lowercase letters, uppercase letters, digits, and special characters. Only the following special characters are allowed: ~@#^*-_+[{}]:./?

- The validity period of a certificate applied from the CA is jointly determined by the customized validity period, validity period of the CA root certificate, maximum validity period supported by the CA, and validity period of the application template supported by the CA. Generally, the validity period does not exceed the maximum validity period supported by the CA and the validity period of the application template supported by the CA. The actual validity period depends on the interconnected CA.
- **Table 4-10** describes the certificate formats, key algorithms, key lengths, certificate types, key usages, and extended key usages supported by certificate management.

Table 4-10 Certificate information

Parameter	Description
Certificate format	Format of the certificate. • PEM • PKCS12
Key algorithm	Key algorithm of the certificate. • RSA • ECDSA **NOTE** RSA whose length is 2047 bits or shorter is insecure. You are advised to use the certificate encrypted by RSA whose length is 3072 bits or longer.
Key length	• Length of the RSA certificate key: – 2048 – 3072 – 4096 – 6144 – 8192 • Length of the ECDSA certificate key: – 256 – 384 – 521
Certificate type	Type of the certificate. • End Entity: Select this type if you do not need to use the key corresponding to the certificate to issue the certificate. • CA: Select this type when you need to use the corresponding key to issue a certificate.

Parameter	Description
Key usage	Usage of the certificate key. • Digital signature: Select this usage if the certificate requires identity authentication and data integrity authentication. • Non-repudiation: Select this usage if the certificate requires authentication on the digital signature of the public key to prevent the signing entity from denying its requests. • Key encipherment: Select this usage if the certificate requires an encryption protocol. • Data encipherment: Select this usage if the certificate encrypts its application data. • Key agreement: Select this usage if the public key is used by the sender and receiver to encrypt data during communication through plaintext agreement. • Certificate signing: Select this usage if the public key authenticates the certificate signature. It can only be used as a proxy certificate. • CRL signing: Select this usage if the public key of the certificate is used to verify the signature on the revocation information. • Encipher only: Select this usage if **Key agreement** is selected. The public key is used only for encrypting data during the agreement. • Decipher only: Select this usage if **Key agreement** is also selected. The public key is used only deciphering data during the key agreement.
Extended key usage	Extended usage of the certificate key. • Server authentication: TLS WWW server authentication. Select this usage when **Digital signature**, **Key encipherment**, or **Key agreement** in **Key usage** is selected. • Client authentication: TLS WWW client authentication. Select this usage when **Digital signature** or **Key agreement** in **Key usage** is selected. • Email protection: Email protection. Select this usage when the **Digital signature**, **Non-repudiation**, **Key encipherment**, or **Key agreement** in **Key usage** is selected.

Procedure

Step 1 Choose **System** > **About** > **Certificate Management** from the main menu.

Step 2 In the navigation pane, choose **Online Certificate Update** > **Certificate Update Tasks**.

Step 3 Click **Create**.

Step 4 Select the update mode as required.

- Updating using an existing template
  a. (Optional) Create a certificate application template. For details, see **4.3.1.6 Creating Certificate Application Templates**.
  b. Select a template from the **Template** drop-down list.
  c. Configure the parameters as required.

  NOTE

  After a certificate application template is selected, you can change the values of some parameters as required. For example, the validity period set in the certificate application template is five years, but the required validity period of the new certificate is 10 years, you can set the validity period to 10 years when creating a certificate update task.
- Updating without a template

  Configure the parameters as required.

Step 5 Click **OK**.

Step 6 In the list of certificate update tasks, check **Task Status** of the created task.

- Pending: The certificate update task is applying for a new certificate. Refresh the page to view the latest task status.
- Success: The certificate update task is created successfully.
- Failed: The certificate update task fails to be created. Rectify the fault based on the failure causes. In the **Operation** column of the row, click **Query Failure Causes**. In the dialog box that is displayed, click **Details** and rectify the fault based on the details. If the problem persists, contact technical support.

Step 7 (Optional) To apply the obtained certificate to services, perform **Step 7.1** to **Step 7.3**.

1. Click  in the Operation column of the row that contains the certificate.
2. Select the services to which you want to apply the certificates.
3. Click **OK**.
4. In the **High Risk** dialog box, read the information carefully and confirm whether to apply certificate to services.
   - If yes, select **I understand the risk and want to continue**, click **OK**, and go to **Step 7.5**.
   - If no, click **Cancel**.
5. Check whether the certificate is successfully applied to the corresponding service.

   If the message **Certificates applied to services successfully.** is displayed, the certificate is successfully applied to the service. Click **OK**. Otherwise, handle the problem according to the information in the dialog box.

NOTE

The certificate of **APIMLBService** takes effect only after the service is restarted.

----End

4.3.1.8 General Settings of Certificate Management

This section describes general settings of certificate management, including certificate alarm configurations and CRL check.

Prerequisites

You have the **Query Certificate Settings** and **Manage Certificate Settings** permissions.

Context

- Certificate alarm configurations: If the remaining validity period of a certificate reaches the alarm generation threshold, certificate management reports an alarm. If the time unit is day, certificate management checks certificate validity every day, and the default alarm generation threshold is 90 days. If the time unit is hour, certificate management checks certificate validity every 24 hours, and the default alarm generation threshold is 2160 hours. You can change the certificate check interval and the alarm generation threshold as required to prevent frequent alarm reporting. To prevent services from becoming unavailable due to certificate expiration, you need to update the certificate periodically (for example, every three months).
- CRL check: The CRL check function specifies whether to enable the CRL check mechanism. After this function is enabled, the system checks whether any CRL is empty. It is recommended that this function be enabled to ensure security.

Procedure

Step 1 Choose **System** > **About** > **Certificate Management** from the main menu.

Step 2 In the navigation pane, choose **Settings** > **General Settings**.

Step 3 On the **General Settings** page, configure the function information based on site requirements.

Function	Troubleshooting Procedure
Certificate alarm configurations	1. Click **Modify**. 2. Select **Time unit**, and set **Check interval** and **In advance alarm before certificate expires** as required. 3. Click **Save**.
CRL check	Enable or disable the CRL check function as required.

----End

4.3.2 Certificate Authority Service

This chapter provides basic information about Certificate Authority Service and its usage scenarios.

4.3.2.1 Certificate Authority Service Overview

This section provides an overview of the Certificate Authority Service, including its definition, functions, and application scenarios.

4.3.2.1.1 Definition

The Certificate Authority Service is used to issue and manage certificates, helping users quickly obtain and use certificates.

Concepts

- Certificate Authority (CA): An authoritative and impartial third-party organization responsible for issuing, authenticating, and managing certificates. A CA is a tree structure consisting of a root CA and multiple subordinate CAs.
- Certificate Revocation List (CRL): A list of certificates that have been revoked by the issuing CA before their scheduled expiration date. It is a kind of certificate blacklist.
- Root CA: The top-level CA in the CA hierarchy. It is the start point of the entire CA chain of trust. The corresponding CA certificate is self-signed and does not need to be verified by other CAs.
- Subordinate CA: A certificate authority signed by the root CA or other subordinate CAs.
- Certificate chain: An ordered list of certificates from multiple levels of CAs. A certificate chain verifies the certificates issued by the lowest-level CA in the certificate chain.
- End-entity certificate: A certificate that does not use its key to issue other certificates.
- One-way TLS: A secure communication protocol that uses digital certificates to encrypt communication packets. The client uses a trusted certificate to authenticate the server.
- Two-way TLS: The server and the client use a trusted certificate to authenticate each other.
- Endorsement Key (EK): A key generated by the vendor of a Trusted Platform Module (TPM) chip to uniquely identify the TPM chip. According to the Trusted Computing Group (TCG) specifications, the TPM stores the EK certificate issued by a trusted third party to verify the validity of the EK. The EK is important private information and cannot be used for signature.
- Attestation Key (AK): A key used in remote attestation to prevent EKs from being disclosed. It is used to sign measurement data (such as the PCR value) stored in the TPM. An AK certificate is a certificate obtained using the privacy CA protocol, containing information such as the public AK and CA issuer.
- Certificate Signing Request (CSR): Certificate signing request. In Public Key Infrastructure (PKI) systems, a certificate signing request is a message sent

from an applicant to a CA in order to apply for a digital certificate. PKCS#10 defines the syntax of a certificate request, which usually contains the public key for which the certificate should be issued, identifying information (such as a domain name) and integrity protection (such as a digital signature).

4.3.2.1.2 Benefits

The Certificate Authority Service provides functions such as configuring and managing CAs, certificate profiles, and CRLs. It also supports the standard Certificate Management Protocol (CMP) and privacy CA protocol. With the Certificate Authority Service, you can quickly obtain and use certificates, reducing the costs of certificate application.

4.3.2.1.3 Scenario

Based on the functions provided by the Certificate Authority Service, you can quickly obtain and use certificates by setting CA parameters.

NOTE

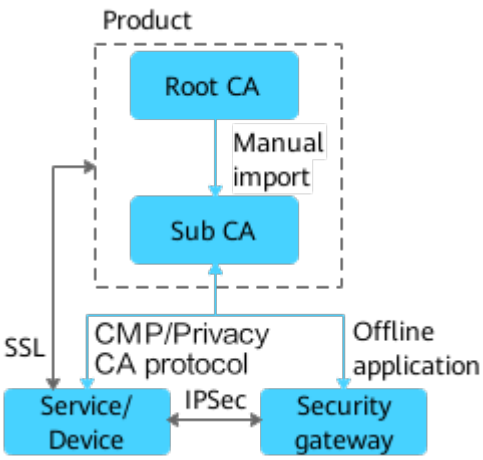
The Certificate Authority Service only issues identity certificates for network management software and devices. It does not issue personal certificates for authentication and signature for individual users.

NetEco CA Independent Networking

As shown in the figure, in the CA independent networking scenario, after the Certificate Authority Service is deployed on the NetEco and a CA is created, end entity certificates can be issued to the NetEco and services or devices. The NetEco and services or devices can apply for certificates from the NetEco CA through CMP or privacy CA protocol, and other devices, such as security gateways, can apply for certificates in offline mode.

This networking applies to small-scale networks where the number of network devices does not exceed the NetEco CA specifications. It does not apply to networks where different devices need to be divided into multiple subdomains.

Figure 4-5 NetEco CA Independent Networking

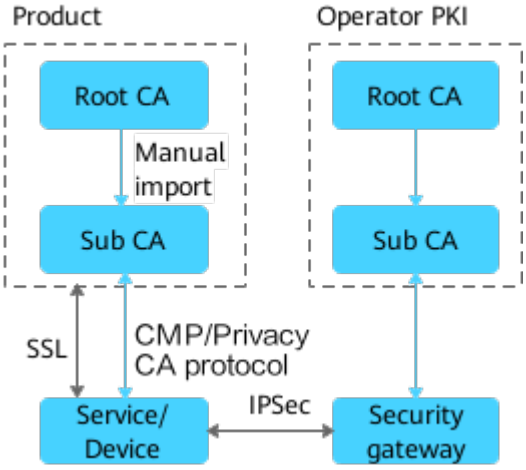


NetEco CA and Operator PKI Co-Networking

As shown in the figure, in the NetEco CA and operator PKI co-networking scenario, the NetEco subordinate CA issues end entity certificates to the NetEco and services or devices, and the operator subordinate CA issues end entity certificates to other devices such as security gateways. The operator PKI root CA certificate needs to be installed offline for services or devices, and the NetEco root CA certificate needs to be installed for other devices such as security gateways so that the mutual authentication can be successful.

This networking applies to the scenario where different subdomains are isolated from each other.

Figure 4-6 NetEco CA and Operator PKI Co-Networking

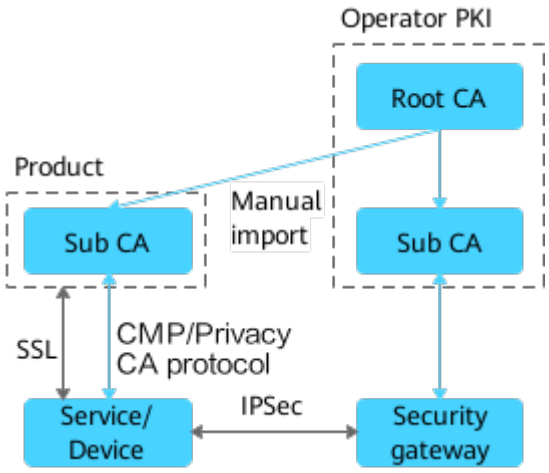


NetEco CA and Operator PKI Co-Networking, with NetEco CA Serving as Operator CA's Subordinate CA

As shown in the figure, in the NetEco CA and operator PKI co-networking scenario where the NetEco CA functions as the operator CA's subordinate CA, the NetEco subordinate CA issues end entity certificates to the NetEco and services or devices; and the operator subordinate CA issues end entity certificates to other devices such as security gateways. The operator PKI root CA certificate needs to be installed offline for services or devices, and also need to be installed on other devices such as security gateways so that the mutual authentication can be successful.

This networking applies to the scenario where a single root CA is used on the entire network, the root CA and subordinate CAs are deployed separately, and subordinate CAs are used to divide subdomains.

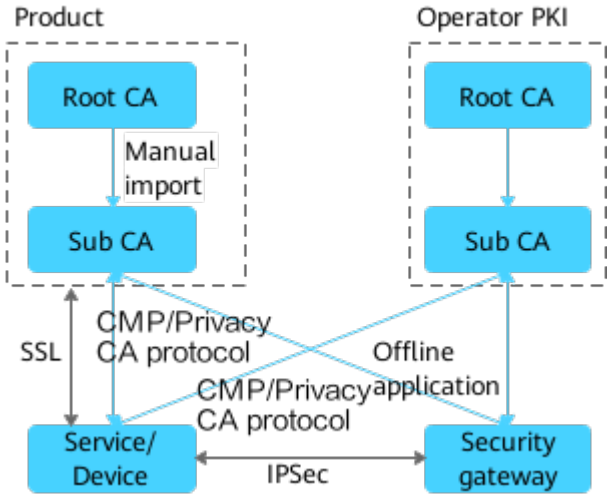
Figure 4-7 NetEco CA and Operator PKI Co-Networking, with NetEco CA Serving as Operator CA's Subordinate CA



NetEco CA and Operator PKI Co-Networking (Multi-Operator Scenario)

As shown in the figure, in the NetEco CA and operator PKI co-networking (multi-operator) scenario, the NetEco and services or devices can apply for certificates from multiple CAs, and different CAs can be deployed for different operators to isolate IPsec tunnels between operators. The NetEco and services or devices can automatically apply for certificates from the NetEco CA through CMP or privacy CA protocol. Other devices, such as security gateways, need to apply for certificates offline. The NetEco CA certificate chain and operator PKI certificate chain need to be installed on services or devices and security gateways. Services or devices support automatic application and manual import in offline mode during the application of end entity certificates through CMP or privacy CA protocol.

Figure 4-8 NetEco CA and Operator PKI Co-Networking (Multi-Operator Scenario)



4.3.2.1.4 Functions

This section describes the functions of the Certificate Authority Service from aspects of PKI management, protocol configuration and certificate application.

Certificate Authority Service Functions

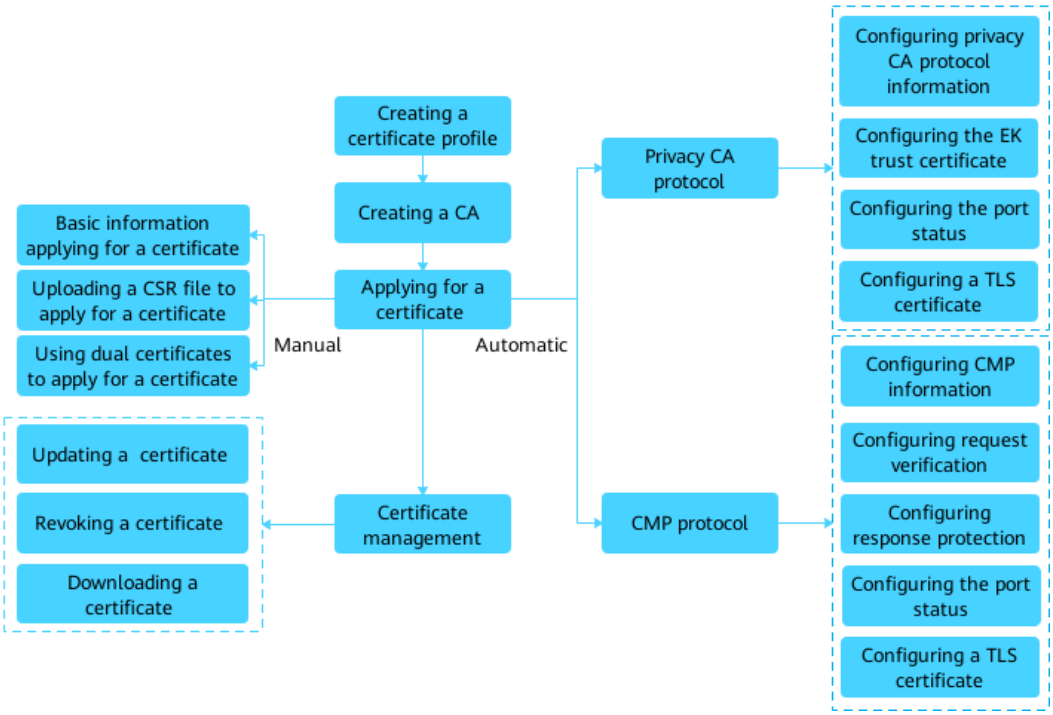
Component	Function	Allows You To...
PKI Management	CertProfile	Configure a certificate profile to avoid repeated configurations when you create a CA and apply for certificates.
	CA	Create and manage CAs in certificate application scenarios.
	Certificate Management	Manage certificates, including certificate revocation, update, and download, and query of certificate details.
	CRL	View the information and status of all CRLs, and download, update, and manually release CRLs.
	Whitelist	Add, import, delete, and query a whitelist. A certificate can be successfully obtained only when the corresponding common name (CN) is whitelisted.
Protocol Configuration	CMP	Configure CMP. Integrity protection for request and response messages is required when you apply for a certificate using CMP.
	Privacy CA Protocol	Configure the privacy CA protocol information and EK trust certificate when applying for a certificate using the privacy CA protocol.
Certificate Application	Certificate Application	On the **Certificate Application** page, you can apply for a certificate in different modes as required.
	Application List	View the certificate application details.
Global Configuration	Port Management	View the current port status and manually enable or disable the HTTP port, TLS one-way authentication port, TLS two-way authentication port or privacy CA protocol port. **NOTE** HTTPS is more secure than HTTP. Therefore, you are advised to select HTTPS (**One-way authentication** or **Two-way authentication**) when configuring CMP.
	TLS Configuration	Configure a TLS certificate to encrypt messages exchanged.
HSM Management		By configuring the Hardware Security Module (HSM), the certificate key will not appear in plaintext outside the device at any time, implementing more secure key management.

4.3.2.1.5 Principles

This section describes the working mechanism of the Certificate Authority Service to help you learn how to apply for certificates.

Figure 4-9 shows the working mechanism of the Certificate Authority Service.

Figure 4-9 Working mechanism of the Certificate Authority Service



When applying for a certificate using the Certificate Authority Service, you need to configure the CA information, certificate profile, whitelist, and CRL as required.

Certificate application methods:

- Manual: You can apply for a certificate by entering basic information, uploading a CSR file, or using dual certificates.
- Automatic: You can apply for a certificate by configuring CMP or privacy CA protocol information.

4.3.2.2 Certificate Authority Service Configuration Procedure

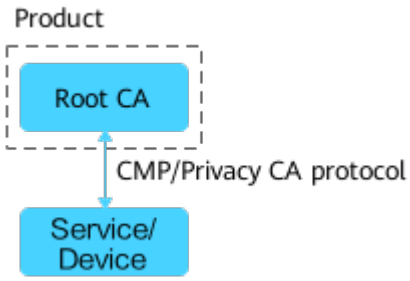
Before using the Certificate Authority Service, you need to understand the configuration process so that you can quickly apply for and use certificates.

Root CA Directly Issuing End Entity Certificates

As shown in the figure, the Certificate Authority Service is enabled on the NetEco and only one CA is deployed. Functioning as both the root CA and lowest-level CA, the CA issues end entity certificates to the NetEco and services/devices. As the lowest-level CA, the root CA can issue only end entity certificates and cannot issue lower-level CAs.

This method applies to small-scale networks where the number of network devices does not exceed the NetEco CA specifications. It does not apply to networks where different devices need to be divided into multiple subdomains.

Figure 4-10 Root CA directly issuing end entity certificates



The configuration procedure is as follows.

Step	Operation	Preparation	Description
1	Create a CA certificate profile.	Certificate profile name, subject information, key usage, and other required information	This step is optional. A root certificate profile is required only when the root CA is created by creating a self-signed certificate. For details, see **4.3.2.3 Configuring a Certificate Profile**. **NOTE** When creating a root certificate profile, set **Certificate level** to **Root CA** and **Path length constraint** to 0. Set other parameters based on site requirements.
2	View root certificate profile details.	N/A	On the **Certificate Profile** page, click the name of a root certificate profile to view its details.

Step	Operation	Preparation	Description
3	Create a root CA.	• In **New self-signed certificate** mode: root CA name, certificate profile, subject, and other required information • In **Upload certificate file** mode: CA name, certificate file in .p12, .pfx, or .jks format, certificate password, and other required information	You can create a root CA by creating a self-signed certificate or uploading a certificate file. For details, see **4.3.2.4 Configuring a CA**. • In **New self-signed certificate** mode, you need to select the root certificate profile created in step 1 and enter the information about the subject configured in the profile. **NOTE** When creating a root CA certificate by creating a self-signed certificate (**New self-signed certificate**), set **Certificate profile** to the root CA certificate profile created in step 1. Set other parameters based on site requirements. • In **Upload certificate file** mode, you need to upload the certificate prepared by yourself. **NOTE** When creating a root CA by uploading a certificate file (**Upload certificate file**), upload the certificate file in .p12, .pfx, or .jks format and enter the password that matches the certificate file. Set other parameters based on site requirements.
4	View root CA details.	N/A	On the **CA** page, click the name of a root CA to view its details. **NOTE** If the subject and issuer of the CA certificate are the same, the CA is a self-signed root CA.

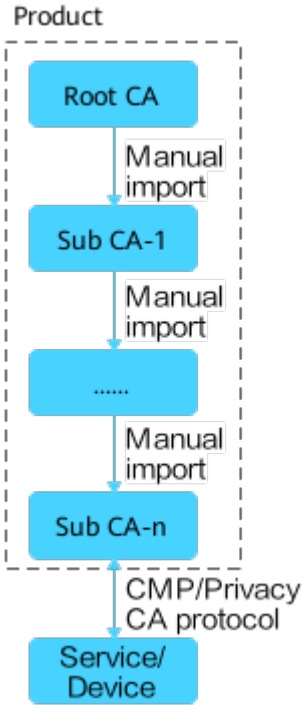
Step	Operation	Preparation	Description
5	Apply for a certificate.	N/A	You can apply for a certificate from the root CA in automatic application mode. The automatic application mode includes using CMP and using the privacy CA protocol. • To apply for a certificate using CMP, you need to configure the port status, TLS certificate, CMP information, request, and responder, and use the CMP request URI to apply for a certificate. For details, see **Global Configuration** and **4.3.2.8 Configuring CMP**. **NOTE** • If the CMP port is an HTTP port, you do not need to configure the TLS certificate. If you select to use the CA to protect messages sent to terminals, you do not need to set response protection on the **Responder Configuration** tab page. Set other parameters based on site requirements. • HTTPS is more secure than HTTP. Therefore, you are advised to select HTTPS (**One-way authentication** or **Two-way authentication**) when configuring CMP. • To apply for a certificate using the privacy CA protocol, you need to configure the port status, TLS certificate, privacy CA protocol information, and EK trusted certificate, and use the privacy CA request URI to apply for a certificate. For details, see **Global Configuration** and **4.3.2.9 Configuring the Privacy CA Protocol**.

Subordinate CA in a Single PKI System Issuing Certificates

As shown in the figure, after the Certificate Authority Service is enabled on the NetEco, both the root CA and subordinate CAs are deployed. The root CA can only issue subordinate CAs offline and cannot issue end entity certificates. The lowest-level subordinate CA can only issue end entity certificates and cannot issue lower-level subordinate CAs. Three methods are available:

- Method 1: The root CA issues multi-level subordinate CAs. Only the lowest-level subordinate CA can issue end entity certificates. The number of subordinate CA levels depends on NetEco resources and specifications. This method applies to the scenario where the network is divided into multiple layers of subdomains.

Figure 4-11 Subordinate CA in a single PKI system issuing certificates - method 1



The configuration procedure is as follows.

Step	Operation	Preparation	Description
1	Create a CA certificate profile.	Certificate profile name, subject information, key usage, and other required information	This step is optional. A root certificate profile is required only when the root CA is created by creating a self-signed certificate. For details, see **4.3.2.3 Configuring a Certificate Profile**. **NOTE** When creating a root certificate profile, set **Certificate level** to **Root CA**. If multiple levels of subordinate CAs are constructed, the value of **Path length constraint** must be greater than 1. Set other parameters based on site requirements.
2	View root certificate profile details.	N/A	On the **Certificate Profile** page, click the name of a root certificate profile to view its details.

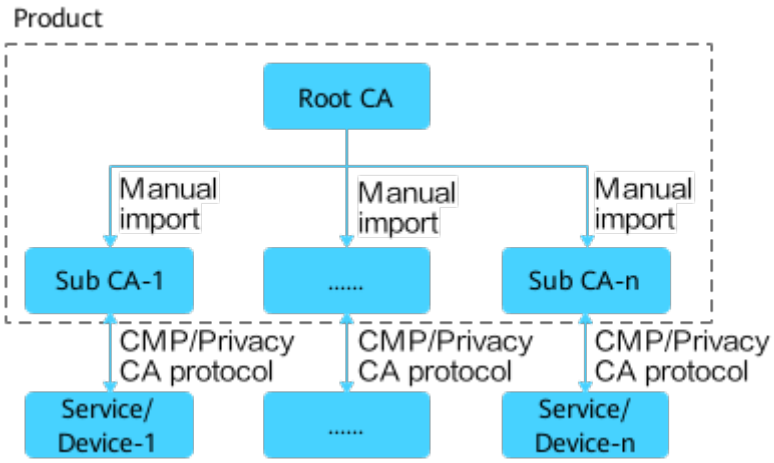
Step	Operation	Preparation	Description
3	Create a root CA.	• In **New self-signed certificate** mode: root CA name, certificate profile, subject, and other required information • In **Upload certificate file** mode: CA name, certificate file in .p12, .pfx, or .jks format, certificate password, and other required information	You can create a root CA by creating a self-signed certificate or uploading a certificate file. For details, see **4.3.2.4 Configuring a CA**. • In **New self-signed certificate** mode, you need to select the root certificate profile created in step 1 and enter the information about the subject configured in the profile. **NOTE** When creating a root CA certificate by creating a self-signed certificate (**New self-signed certificate**), set **Certificate profile** to the root CA certificate profile created in step 1. Set other parameters based on site requirements. • In **Upload certificate file** mode, you need to upload the certificate prepared by yourself. **NOTE** When creating a root CA by uploading a certificate file (**Upload certificate file**), upload the certificate file in .p12, .pfx, or .jks format and enter the password that matches the certificate file. Set other parameters based on site requirements.
4	View root CA details.	N/A	On the **CA** page, click the name of a root CA to view its details. **NOTE** If the subject and issuer of the CA certificate are the same, the CA is a self-signed root CA.

Step	Operation	Preparation	Description
5	Create a subordinate CA.	Subordinate CA name, certificate profile, subject, and other required information	Method 1: On the **CA** page, click **New**, select **Signed by internal CA**, select a CA, and create a subCA for the CA. Method 2: 1. On the **CA** page, create a CA in pending state and download the CSR file corresponding to the CA. 2. On the **Certificate Application** page, apply for a certificate from the root CA by uploading the CSR file and download the certificate. 3. On the **CA** page, upload the downloaded certificate file to the CA in pending state. The CA is activated and becomes the subordinate CA of the root CA. **NOTE** • When constructing multiple levels of subordinate CAs, ensure that the certificate chain structure is correct and repeat the steps for creating a subordinate CA as required. • The root CA and subordinate CAs are created on the same NetEco.
6	View subordinate CA details.	N/A	On the **CA** page, click the name of a subordinate CA to view its details.

Step	Operation	Preparation	Description
7	Apply for a certificate.	N/A	You can apply for a certificate from the root CA in automatic application mode. The automatic application mode includes using CMP and using the privacy CA protocol. • To apply for a certificate using CMP, you need to configure the port status, TLS certificate, CMP information, request, and responder, and use the CMP request URI to apply for a certificate. For details, see **Global Configuration** and **4.3.2.8 Configuring CMP**. **NOTE** ◦ If the CMP port is an HTTP port, you do not need to configure the TLS certificate. If you select to use the CA to protect messages sent to terminals, you do not need to set response protection on the **Responder Configuration** tab page. Set other parameters based on site requirements. ◦ HTTPS is more secure than HTTP. Therefore, you are advised to select HTTPS (**One-way authentication** or **Two-way authentication**) when configuring CMP. • To apply for a certificate using the privacy CA protocol, you need to configure the port status, TLS certificate, privacy CA protocol information, and EK trusted certificate, and use the privacy CA request URI to apply for a certificate. For details, see **Global Configuration** and **4.3.2.9 Configuring the Privacy CA Protocol**.

- Method 2: The root CA issues multiple subordinate CAs. Only the lowest-level subordinate CA can issue end entity certificates. The number of subordinate CAs depends on NetEco resources and specifications. This method applies to the scenario where the network is divided into multiple subdomains.

Figure 4-12 Subordinate CA in a single PKI system issuing certificates - method 2



The configuration procedure is as follows.

Step	Operation	Preparation	Description
1	Create a CA certificate profile.	Certificate profile name, subject information, key usage, and other required information	This step is optional. A root certificate profile is required only when the root CA is created by creating a self-signed certificate. For details, see **4.3.2.3 Configuring a Certificate Profile**. **NOTE** When creating a root certificate profile, set **Certificate level** to **Root CA**. If multiple levels of subordinate CAs are constructed, the value of **Path length constraint** must be greater than 1. Set other parameters based on site requirements.
2	View root certificate profile details.	N/A	On the **Certificate Profile** page, click the name of a root certificate profile to view its details.

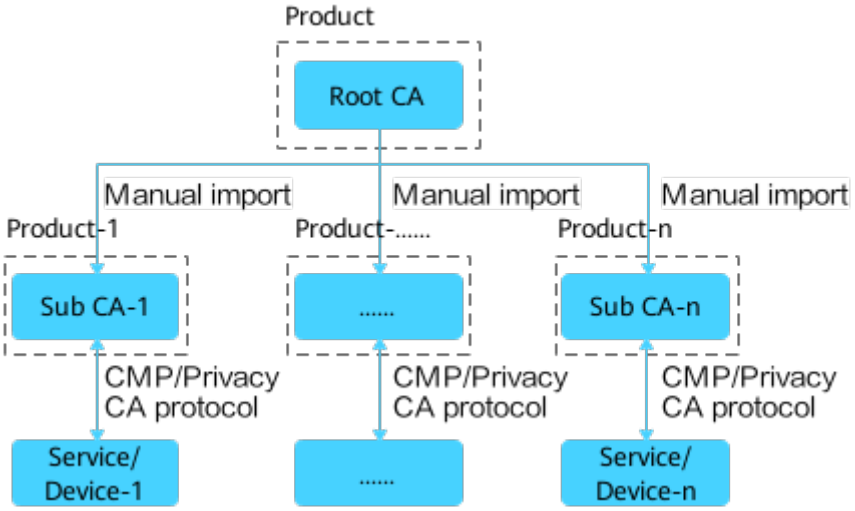
Step	Operation	Preparation	Description
3	Create a root CA.	• In **New self-signed certificate** mode: root CA name, certificate profile, subject, and other required information • In **Upload certificate file** mode: CA name, certificate file in .p12, .pfx, or .jks format, certificate password, and other required information	You can create a root CA by creating a self-signed certificate or uploading a certificate file. For details, see **4.3.2.4 Configuring a CA**. • In **New self-signed certificate** mode, you need to select the root certificate profile created in step 1 and enter the information about the subject configured in the profile. **NOTE** When creating a root CA certificate by creating a self-signed certificate (**New self-signed certificate**), set **Certificate profile** to the root CA certificate profile created in step 1. Set other parameters based on site requirements. • In **Upload certificate file** mode, you need to upload the certificate prepared by yourself. **NOTE** When creating a root CA by uploading a certificate file (**Upload certificate file**), upload the certificate file in .p12, .pfx, or .jks format and enter the password that matches the certificate file. Set other parameters based on site requirements.
4	View root CA details.	N/A	On the **CA** page, click the name of a root CA to view its details. **NOTE** If the subject and issuer of the CA certificate are the same, the CA is a self-signed root CA.

Step	Operation	Preparation	Description
5	Create a subordinate CA.	Subordinate CA name, certificate profile, subject, and other required information	Method 1: On the **CA** page, click **New**, select **Signed by internal CA**, select a CA, and create a subCA for the CA. Method 2: 1. On the **CA** page, create a CA in pending state and download the CSR file corresponding to the CA. 2. On the **Certificate Application** page, apply for a certificate from the root CA by uploading the CSR file and download the certificate. 3. On the **CA** page, upload the downloaded certificate file to the CA in pending state. The CA is activated and becomes the subordinate CA of the root CA. **NOTE** • When constructing multiple subordinate CAs, repeat the steps for creating a subordinate CA as required. • The root CA and subordinate CAs are created on the same NetEco.
6	View subordinate CA details.	N/A	On the **CA** page, click the name of a subordinate CA to view its details.

Step	Operation	Preparation	Description
7	Apply for a certificate.	N/A	You can apply for a certificate from the root CA in automatic application mode. The automatic application mode includes using CMP and using the privacy CA protocol. • To apply for a certificate using CMP, you need to configure the port status, TLS certificate, CMP information, request, and responder, and use the CMP request URI to apply for a certificate. For details, see **Global Configuration** and **4.3.2.8 Configuring CMP**. **NOTE** ◦ If the CMP port is an HTTP port, you do not need to configure the TLS certificate. If you select to use the CA to protect messages sent to terminals, you do not need to set response protection on the **Responder Configuration** tab page. Set other parameters based on site requirements. ◦ HTTPS is more secure than HTTP. Therefore, you are advised to select HTTPS (**One-way authentication** or **Two-way authentication**) when configuring CMP. • To apply for a certificate using the privacy CA protocol, you need to configure the port status, TLS certificate, privacy CA protocol information, and EK trusted certificate, and use the privacy CA request URI to apply for a certificate. For details, see **Global Configuration** and **4.3.2.9 Configuring the Privacy CA Protocol**.

- Method 3: The root CA issues multiple subordinate CAs that are deployed on different NetEcos. Only the lowest-level subordinate CA can issue end entity certificates. Services/devices that have certificates issued by different subordinate CAs must have the root CA certificate installed so that the mutual authentication can be successful. This method applies to the scenario where the NetEco and its services/devices are divided into a subdomain.

Figure 4-13 Subordinate CA in a single PKI system issuing certificates - method 3



The configuration procedure is as follows.

Step	Operation	Preparation	Description
1	Create a CA certificate profile.	Certificate profile name, subject information, key usage, and other required information	This step is optional. A root certificate profile is required only when the root CA is created by creating a self-signed certificate. For details, see **4.3.2.3 Configuring a Certificate Profile**. **NOTE** When creating a root certificate profile, set **Certificate level** to **Root CA**. If multiple levels of subordinate CAs are constructed, the value of **Path length constraint** must be greater than 1. Set other parameters based on site requirements.
2	View root certificate profile details.	N/A	On the **Certificate Profile** page, click the name of a root certificate profile to view its details.

Step	Operation	Preparation	Description
3	Create a root CA.	• In **New self-signed certificate** mode: root CA name, certificate profile, subject, and other required information • In **Upload certificate file** mode: CA name, certificate file in .p12, .pfx, or .jks format, certificate password, and other required information	You can create a root CA by creating a self-signed certificate or uploading a certificate file. For details, see **4.3.2.4 Configuring a CA**. • In **New self-signed certificate** mode, you need to select the root certificate profile created in step 1 and enter the information about the subject configured in the profile. **NOTE** When creating a root CA certificate by creating a self-signed certificate (**New self-signed certificate**), set **Certificate profile** to the root CA certificate profile created in step 1. Set other parameters based on site requirements. • In **Upload certificate file** mode, you need to upload the certificate prepared by yourself. **NOTE** When creating a root CA by uploading a certificate file (**Upload certificate file**), upload the certificate file in .p12, .pfx, or .jks format and enter the password that matches the certificate file. Set other parameters based on site requirements.
4	View root CA details.	N/A	On the **CA** page, click the name of a root CA to view its details. **NOTE** If the subject and issuer of the CA certificate are the same, the CA is a self-signed root CA.

Step	Operation	Preparation	Description
5	Create a subordinate CA.	Subordinate CA name, certificate profile, subject, and other required information	Method 1: On the **CA** page, click **New**, select **Signed by internal CA**, select a CA, and create a subCA for the CA. Method 2: 1. On the **CA** page, create a CA in pending state and download the CSR file corresponding to the CA. 2. On the **Certificate Application** page, apply for a certificate from the root CA by uploading the CSR file and download the certificate. 3. On the **CA** page, upload the downloaded certificate file to the CA in pending state. The CA is activated and becomes the subordinate CA of the root CA. **NOTE** • When constructing multiple subordinate CAs, repeat the steps for creating a subordinate CA as required. • The root CA and subordinate CAs are created on different NetEcos.
6	View subordinate CA details.	N/A	On the **CA** page, click the name of a subordinate CA to view its details.

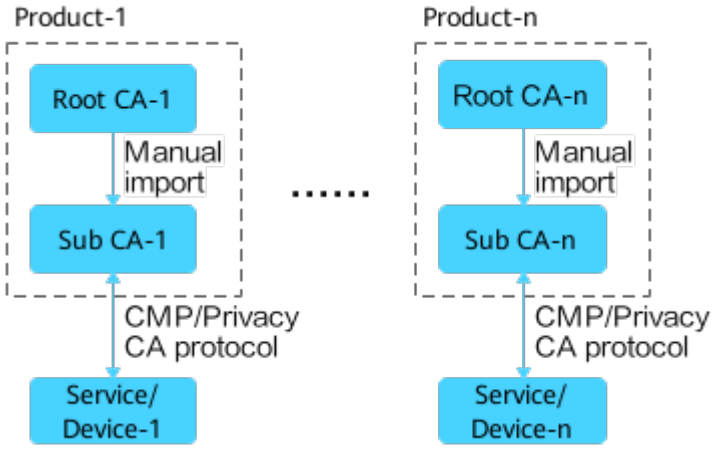
Step	Operation	Preparation	Description
7	Apply for a certificate.	N/A	You can apply for a certificate from the root CA in automatic application mode. The automatic application mode includes using CMP and using the privacy CA protocol. • To apply for a certificate using CMP, you need to configure the port status, TLS certificate, CMP information, request, and responder, and use the CMP request URI to apply for a certificate. For details, see **Global Configuration** and **4.3.2.8 Configuring CMP**. **NOTE** • If the CMP port is an HTTP port, you do not need to configure the TLS certificate. If you select to use the CA to protect messages sent to terminals, you do not need to set response protection on the **Responder Configuration** tab page. Set other parameters based on site requirements. • HTTPS is more secure than HTTP. Therefore, you are advised to select HTTPS (**One-way authentication** or **Two-way authentication**) when configuring CMP. • To apply for a certificate using the privacy CA protocol, you need to configure the port status, TLS certificate, privacy CA protocol information, and EK trusted certificate, and use the privacy CA request URI to apply for a certificate. For details, see **Global Configuration** and **4.3.2.9 Configuring the Privacy CA Protocol**.

Subordinate CA in a Multi-PKI System Issuing Certificates

As shown in the figure, different root CAs are deployed on different NetEcos. The peer root CA certificate needs to be installed on services/devices in different subdomains so that the mutual authentication can be successful. On NetEco-1, the Certificate Authority Service is enabled and root CA-1 is deployed. On NetEco-2, the Certificate Authority Service is enabled and root CA-2 (different from root CA-1) is deployed. The two root CAs are independent of each other. The certificates of root CA-1 and root CA-2 need to be installed on service/device-1 and service/device-2 so that the mutual authentication can be successful.

This method applies to the networking scenario where different subdomains are completely isolated. More subdomains require more root CAs, complicating management.

Figure 4-14 Subordinate CA in a multi-PKI system issuing certificates



The configuration procedure is as follows.

Step	Operation	Preparation	Description
1	Create a CA certificate profile.	Certificate profile name, subject information, key usage, and other required information	This step is optional. A root certificate profile is required only when the root CA is created by creating a self-signed certificate. For details, see **4.3.2.3 Configuring a Certificate Profile**. **NOTE** When creating a root certificate profile, set **Certificate level** to **Root CA**. If multiple levels of subordinate CAs are constructed, the value of **Path length constraint** must be greater than 1. Set other parameters based on site requirements.
2	View root certificate profile details.	N/A	On the **Certificate Profile** page, click the name of a root certificate profile to view its details.

Step	Operation	Preparation	Description
3	Create a root CA.	• In **New self-signed certificate** mode: root CA name, certificate profile, subject, and other required information • In **Upload certificate file** mode: CA name, certificate file in .p12, .pfx, or .jks format, certificate password, and other required information	You can create a root CA by creating a self-signed certificate or uploading a certificate file. For details, see **4.3.2.4 Configuring a CA**. • In **New self-signed certificate** mode, you need to select the root certificate profile created in step 1 and enter the information about the subject configured in the profile. **NOTE** When creating a root CA certificate by creating a self-signed certificate (**New self-signed certificate**), set **Certificate profile** to the root CA certificate profile created in step 1. Set other parameters based on site requirements. • In **Upload certificate file** mode, you need to upload the certificate prepared by yourself. **NOTE** When creating a root CA by uploading a certificate file (**Upload certificate file**), upload the certificate file in .p12, .pfx, or .jks format and enter the password that matches the certificate file. Set other parameters based on site requirements.
4	View root CA details.	N/A	On the **CA** page, click the name of a root CA to view its details. **NOTE** If the subject and issuer of the CA certificate are the same, the CA is a self-signed root CA.

Step	Operation	Preparation	Description
5	Create a subordinate CA.	Subordinate CA name, certificate profile, subject, and other required information	Method 1: On the **CA** page, click **New**, select **Signed by internal CA**, select a CA, and create a subCA for the CA. Method 2: 1. On the **CA** page, create a CA in pending state and download the CSR file corresponding to the CA. 2. On the **Certificate Application** page, apply for a certificate from the root CA by uploading the CSR file and download the certificate. 3. On the **CA** page, upload the downloaded certificate file to the CA in pending state. The CA is activated and becomes the subordinate CA of the root CA. **NOTE** • When constructing multiple subordinate CAs, repeat the steps for creating a subordinate CA as required. • The root CA and subordinate CAs are created on different NetEcos. Pay attention to the matching relationship.
6	View subordinate CA details.	N/A	On the **CA** page, click the name of a subordinate CA to view its details.

Step	Operation	Preparation	Description
7	Apply for a certificate.	N/A	You can apply for a certificate from the root CA in automatic application mode. The automatic application mode includes using CMP and using the privacy CA protocol. • To apply for a certificate using CMP, you need to configure the port status, TLS certificate, CMP information, request, and responder, and use the CMP request URI to apply for a certificate. For details, see **Global Configuration** and **4.3.2.8 Configuring CMP**. **NOTE** • If the CMP port is an HTTP port, you do not need to configure the TLS certificate. If you select to use the CA to protect messages sent to terminals, you do not need to set response protection on the **Responder Configuration** tab page. Set other parameters based on site requirements. • HTTPS is more secure than HTTP. Therefore, you are advised to select HTTPS (**One-way authentication** or **Two-way authentication**) when configuring CMP. • To apply for a certificate using the privacy CA protocol, you need to configure the port status, TLS certificate, privacy CA protocol information, and EK trusted certificate, and use the privacy CA request URI to apply for a certificate. For details, see **Global Configuration** and **4.3.2.9 Configuring the Privacy CA Protocol**.

4.3.2.3 Configuring a Certificate Profile

When creating a CA and applying for certificates, you can configure a certificate profile to avoid repeated configurations and meet certificate application and usage requirements in different scenarios.

Context

- A certificate profile is a set of rules and settings used for certificate application and management. These rules and settings can be simple or complex to meet your varying requirements.
- Predefined profiles are default profiles provided by the system and cannot be deleted or modified. For detailed parameter descriptions, see **Table 4-11**. The

following table describes some parameters in the preset profile. The actual configuration varies according to the information on the page.

Table 4-11 Predefined profile parameters

Certificate level	Label	Description	Key algorithm	Key length	ECDSA key type	Validity	Basic constraints	Key usage	Certificate policy OID	Subject
Root CA	ROOT_CA_PREDEFINED_RSA4096	The root CA is most secure and trusted. To create a root CA certificate, use this profile.	RSA	4096	N/A	40 yeas	• Critical • Type: CA • Path length constraint: None	Digital signature, CRL signature, Certificate signature	2.5.29.32.0	Common name(CN), Country name(C), Organization(O), Organizational unit(OU)
	ROOT_CA_PREDEFINED_ECDSA384		ECDSA	384	ECsecp384r1					
Subordinate CA	SUB_CA_PREDEFINED_RSA4096	This profile is used to apply for a sub-CA certificate from the root CA or a subo	RSA	4096	N/A	25 yeas	• Critical • Type: CA • Path length constraint: 0			

Certificate level	Label	Description	Key algorithm	Key length	ECDSA key type	Validity	Basic constraints	Key usage	Certificate policy OID	Subject
	SUB_CA_PREDEFINED_ECDSA384	rdinate CA. To construct a multi-level CA certificate chain, use this profile.	ECDSA	384	ECsecp384r1					
End entity	END_ENTITY_PREDEFINED_RSA2048	This profile is used to apply for an end entity certificate from the root CA or a subordinate CA. To apply for	RSA	2048	N/A	2 years	• Type: End entity • Path length constraint: None	Digital signature, Content commitment (non-repudiation), Key encipherment, Data encipherment, Key agreement		
	END_ENTITY_PREDEFINED_RSA3072		RSA	3072	N/A					

Certificate level	Label	Description	Key algorithm	Key length	ECDSA key type	Validity	Basic constraints	Key usage	Certificate policy OID	Subject
	END_ENTITY_PREDEFINED_ECDSA256	an end entity certificate, use this profile.	ECDSA	256	EC prime256v1					

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **PKI Management** > **Certificate Profile** from the navigation tree on the left.

Step 3 Click **New** and set required parameters.

For detailed parameter descriptions, see **Table 4-12**.

Table 4-12 Certificate profile parameters

Parameter	Description	Value
Label	Name of a certificate profile.	The name is a string of 1 to 45 characters containing letters, digits, underscores (_), and hyphens (-). The name cannot be **null** or **all** (case insensitive).
Certificate level	Certificate level, which can be root CA, subordinate CA, or end-entity CA.	N/A

Parameter	Description	Value
Description	Description of a certificate profile.	The description is a string of 0 to 128 characters containing digits, uppercase letters, lowercase letters, spaces, and special characters: (, . ! : ; ?).
Subject	Identifiable alias of the certificate user, including **Common name**(CN), **Country name**(C), **Email address** (E), **Organization**(O), **Organizational unit**(OU), **State**(ST), **Locality**(L), **Domain component** (DC), and **User identifier** (UID).	By default, **Common name** is mandatory and cannot be deselected. When you need to fill in the profile subject information, the common name is a string of 1 to 127 characters containing uppercase letters, lowercase letters, digits, spaces, hyphens (-), colons (:), and dots (.). If **Domain component** is selected, a maximum of 4 domain components can be configured at a time when **Domain component** information needs to be set in the profile.
Validity period	Validity period of a certificate profile.	You can set the certificate profile's validity period in units of day, month, or year. The maximum validity period is 18250 days.
Key algorithm	Key algorithm, which can be RSA or ECDSA.	N/A

Parameter		Description	Value
Key length		If RSA is used, the available options are 2048, 3072, 4096, and 8192. If ECDSA is selected, the available options are 256, 384, and 521.	N/A
ECDSA key type		Available options: ECprime256v1, ECsecp256r1, ECsecp384r1, ECsecp521r1. **NOTE** Set this parameter when you select the ECDSA algorithm.	N/A
Subject key identifier		Unique identifier of the subject.	N/A
Authority key identifier	Include issuer and SN	Unique identifier of the key contained in a certificate. It is used to identify multiple pairs of keys of the same issuer.	N/A
Basic constraints		Used to ensure that certificates are used only in certain applications.	N/A

Parameter		Description	Value
Path length constraint		When the value of the path length constraint extension is 0, it indicates that the CA certificate can only issue end entity certificates in the valid certificate path. When the value of the path length constraint extension is greater than 0, it indicates the maximum number of intermediate subordinate CA certificates that may exist in the path from the CA certificate to end entity certificates. If a CA system has n layers, the path length constraint of the top-layer CA certificate is n - 2, and those of the lower-layer certificates is n - 3, n - 4, and so on. The result is greater than or equal to 0. For example, if n is 4, the four-layer structure of the CA is root CA > subordinate CA1 > subordinate CA2 > end entity certificate. That is, the root CA issues the subordinate CA1, subordinate CA1 issues subordinate CA2, and subordinate CA2 issues the end entity certificate. In this case, the path length of the root CA is 2, the path length of subordinate CA1 is 1, and the path length of subordinate CA2 is 0. **NOTE** The path length constraint can be set only when **Certificate level** is set to **Root CA** or **Subordinate CA**.	The path length constraint must range from 0 to 9.
Subject alternative name	Domain name	Domain name contained in the alias of the certificate issuing object.	If **Subject alternative name** is selected, a maximum of 16 domain names and IP addresses in total can be configured at a time when **Subject**

Parameter		Description	Value
	IP address	IP address contained in the alias of the certificate issuing object.	**alternative name** information needs to be set in the profile.
Certificate policy		A certificate policy defines the policy for issuing certificates and the application scenarios of certificates. A certificate policy ID is in the format of object identifier (OID). 2.5.29.32.0 indicates any policy. If you need to customize your own certificate policy, you must create a certificate policy ID, which must be constructed based on the enterprise ID allocated by the IANA. You can obtain the enterprise ID from the IANA free of charge. A certificate policy consists of a certificate policy ID and a qualifier. The certificate policy ID must be unique in the certificate policy extensions of a certificate. The qualifier is used to express the detailed information that depends on the policy. The qualifier includes the following three types: ● No policy qualifier: Indicates that the certificate policy does not contain additional information. ● CPS URI: The CPS qualifier indicates the URI of the certificate practice statement issued by the CA. ● User notice text: Displays certificate information to certificate users.	A maximum of four certificate policies can be created for each certificate profile. The certificate policy ID must be a string of 3 to 256 characters prefixed with 0./1./2. If the period (.) is followed by 0, 0 cannot be followed by other digits. For example, 2.5.29.32.0 is in correct format, but 2.02 is in incorrect format. The CPS URI must contain 1 to 256 characters. The user notice text must contain 1 to 200 characters, including digits, uppercase letters, lowercase letters, spaces, and special characters: (, . ! : ; ?).

Parameter		Description	Value
Key usage	Digital signature	A signature generated using the private key of the issuer. It is used for entity authentication and data source integrity authentication.	If the certificate level of the profile is **End entity**, **Digital signature** is selected by default for **Key usage** and can be deselected.
	Content commitment (non-repudiation)	Verifies digital signature denial services used to provide non-digital signatures, preventing the signing entity from incorrectly denying certain operations. In the case of subsequent conflicts, a reliable third party can determine the authenticity of the signature data.	N/A
	Key encipherment	Encrypts private keys or keys during key transmission.	N/A
	CRL signature	Required when the subject public key is used to verify the signature in the revocation information (such as CRL).	If the certificate level of the profile is **Root CA** or **Subordinate CA**, **CRL signature** is selected by default for **Key usage** and can be deselected.
	Data encipherment	Used to encrypt important user data instead of encoding keys.	N/A
	Certificate signature	Used to verify the signature in the public key certificate.	If the certificate level of the profile is **Root CA** or **Subordinate CA**, **Certificate signature** is selected by default for **Key usage** and can be deselected.
	Key agreement	Key agreement protocol. For example, when the Diffie-Hellman key is used for key management, select this option.	If the certificate level of the profile is **End entity**, **Key agreement** is selected by default for **Key usage** and can be deselected.

Parameter		Description	Value
	Encipher only	Uses a key to encrypt data only when the key protocol agreement is run.	N/A
	Decipher only	Uses a key to decrypt data only when the key protocol agreement is run.	N/A
Extended key usage	TLS web server identity authentication	Authenticates the TLS www server. **Digital signature**, **Key encipherment**, or **Key agreement** may also provide the same function.	N/A
	TLS web client identity authentication	Authenticates the TLS www client. **Digital signature** and/or **Key agreement** may also provide the same function.	N/A
	Sign executable code	Signs the executable code that can be downloaded. **Digital signature** may also provide the same function.	N/A
	Timestamping	Binds the hash of the object to the time. **Digital signature** and/or **Content commitment** may also provide the same function.	N/A
	Email protection	Protects emails. **Digital signature**, **Content commitment**, and/or **Key encipherment** or **Key agreement** may also provide the same function.	N/A
	IPSec end system	IP security terminal system.	N/A
	IPSec user	IP security user.	N/A
	IPSec tunnel	IP security tunnel.	N/A
CRL distribution point		A location where CRLs are published. You can obtain the CRL corresponding to the certificate based on this parameter.	This parameter cannot be set when **Certificate level** is set to **Root CA**.

NOTE

- Critical: The certificate user performs strong verification on the extensions that are marked as critical.
- Required: During certificate request, the packet must contain this extension.
- Permitted in request: During certificate issuing, the value of this extension in the request packet is used.

Step 4 Click **Submit**.

NOTE

You can click **Reset** to clear parameter settings.

----End

Related Tasks

- Viewing a certificate profile

  On the **Certificate Profile** page, click the name of a certificate profile. Then you can view the detailed information about this certificate profile.

- Modifying a certificate profile

  On the **Certificate Profile** page, click **Modify** in the **Operation** column of a certificate profile. Then you can modify the configuration of this certificate profile.

  NOTE

  - The certificate profile name cannot be changed when you modify the certification profile configuration.
  - The predefined certificate profile cannot be modified.
  - If the certificate level of a profile is **Subordinate CA** or **End-entity** and the profile has been associated with a CA, the certificate level of the profile cannot be changed to **Root CA**.

- Copying a certificate profile

  On the **Certificate Profile** page, click **Copy** in the **Operation** column of a certificate profile. Then you can copy this certificate profile and rename it.

- Deleting a certificate profile

  On the **Certificate Profile** page, click **Delete** in the **Operation** column of a certificate profile.

  NOTE

  The predefined certificate profile cannot be deleted.

- Searching for a certificate profile

  On the **Certificate Profile** page, enter a certificate profile name in the search box and click  . The Certificate Authority Service supports fuzzy search by certificate profile name.

4.3.2.4 Configuring a CA

If you do not have a CA or have a CA that does not meet the requirements for issuing certificates, you can configure one on the CA management page to facilitate your subsequent certificate application and use.

Context

The Certificate Authority Service provides a certificate issuance solution to address the problems arising from the unavailability of a CA or an existing CA that does not meet the requirements.

NOTICE

When importing a third-party certificate, ensure that the certificate is issued by a trusted CA. Otherwise, security risks exist.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **PKI Management** > **CA** from the navigation tree on the left.

Step 3 Click **New** and set required parameters.

For detailed parameter descriptions, see **Table 4-13**.

Table 4-13 CA parameters

Parameter	Description	Value
Label	Name of a CA.	• The name is a string of 1 to 45 characters containing letters, digits, underscores (_), and hyphens (-). • The name cannot be **null** or **all** (case insensitive).
Status	You can create an activated, inactive, or pending CA. **NOTE** Before uploading a CA certificate, you cannot apply for a certificate from a CA in the pending state.	By default, the CA created is activated.
Signature algorithm	Signature algorithm used for a CA to issue certificates. **NOTE** RSASSA-PSS is more secure than RSA. Currently, only TLS1.3 supports the certificate signed by RSASSA-PSS. TLS1.2 and earlier versions do not support the certificate signed by RSASSA-PSS. If the certificate issued by the user is used for TLS communication, confirm the TLS version before configuring the CA signature algorithm. Otherwise, the TLS communication may fail.	N/A

Parameter		Description	Value
Certificate SN length		Length of the unique number assigned by a CA to a certificate.	The value is an integer ranging from 18 to 40, in characters.
Max validity period		Maximum validity period of a certificate.	You can set the certificate validity period in units of day, month, or year. The maximum validity period is 18250 days.
New self-signed certificate		A certificate issued by a signing entity to itself, not by an authoritative CA. When creating a CA in self-signed mode, you need to select a certificate profile whose certificate level is **Root CA** and enter the user information configured in the profile.	N/A
Upload certificate file	Certificate file	You can create a CA by uploading a local certificate file. In this mode, you will create a subordinate CA of the organization that issues the certificate file. This subordinate CA is used to issue certificates to lower-level organizations.	• The certificate file must be in .p12, .pfx, or .jks format. • Only one certificate can be uploaded, and the size of a single file cannot exceed 20 KB. • The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space.
	Certificate password	Password set for a certificate during certificate application. The password is contained in the .p12 file. You need to enter this password when uploading the certificate file.	N/A

Parameter		Description	Value
	Upload certificate chain	Upload the corresponding certificate chain. You can select multiple files. For example, if a level-3 CA certificate is imported, upload the corresponding level-1 and level-2 CA certificates.	• The certificate chain file must be in .cer, .crt, or .pem format. • A maximum of 10 files can be upload at a time. And the size of the file to be uploaded at a time cannot exceed 100 KB. • The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space.
New CSR file		When the CA status is **Pending**, **New CSR file** is automatically selected for certificate configuration mode.	N/A
Signed by internal CA	Internal CA	In **Signed by internal CA** mode, a sub-CA is created for a CA. When creating a sub-CA using the internal CA signature, you need to select a CA as the parent CA.	N/A
	Certificate profile	When creating a sub-CA in **Signed by internal CA** mode, you need to select a certificate profile whose certificate level is **Subordinate CA** and enter the user information configured in the profile.	N/A
Key generation mode		You can use **Software** or **HSM** to generate keys.	N/A
CRL generation interval		Interval for generating a CRL.	The value is an integer ranging from 1 to 60, in days.
CRL generation time		Time when the CRL is generated.	N/A

Parameter	Description	Value
CRL overlap time	Period during which a user can obtain a new CRL before the old CRL is considered unavailable.	The value is an integer ranging from 1 to 60, in minutes.
Include revocation reasons	Whether to include the revocation reason.	The default value is **Yes**.
CRL server	Server to which a CRL is published.	N/A
Publication mode	Whether a CRL is published manually or automatically. If you select **Automatic**, you must configure the CRL server and the publication period.	• By default, **Automatic** is not selected, indicating that manual publishing is used. • If you select **Automatic**, the default publishing interval is 60 minutes. • The unit of the publishing interval can be minute, hour, or day. The maximum interval is 180 days.
CRL distribution point	A location where CRLs are published, for example, **http://*IP address*:*Port number*/caname.crl**. You can obtain the CRL corresponding to the certificate based on this parameter. **NOTE** The CRL obtained from the CRL distribution point can be used to verify the validity of the certificate issued by the CA. The Certificate Authority Service does not automatically release the CRL to the CRL distribution point. You need to maintain the validity of the CRL file at the distribution point.	Each CA can be configured with a maximum of four CRL distribution points.

Step 4 Click **Next**.

Step 5 In the profile association list, select the profile to be associated.

NOTE

- Configure an associated profile for the CA to issue certificates. The associated profile must be a sub-CA profile or an end-entity profile.
- A CA must be associated with at least one profile, and a maximum of 16 profiles can be associated.

Step 6 In the default profile list, select an associated profile as the default profile.

NOTE

- During certificate application using CMP or privacy CA protocol, if the request carries the profile name parameter, the specified profile is used; if the request does not carry the profile name parameter, the default profile of the CA is used.
- Only one default profile can be set for a CA.

Step 7 Click **Submit**.

NOTE

- You can click **Reset** to clear parameter settings.
- You can also click **Back** to return to the previous page.

----End

Follow-up Procedure

- Deactivating a CA

  For a created and activated CA, you can access the **CA** page and click **Deactivate CA** in the **Operation** column of the CA to deactivate it.

- Activating a CA

  For a created but inactivated CA, you can access the **CA** page and click **Active CA** in the **Operation** column of the CA to activate it.

- Downloading CSR

  For a created but pending CA, you can download the CSR file directly after creating a CA or click **Download CSR** on the **CA** page to download the CSR file of the CA.

- Uploading a CA certificate

  For a created but pending CA, you can access the **CA** page and click **Upload CA certificate** in the **Operation** column of the CA to upload a CA certificate.

  NOTE

  - The certificate file or certificate chain must be in .cer, .crt, or .pem format. Only one certificate can be uploaded, and the size of a single file cannot exceed 100 KB. The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space.
  - If the certificate issued by the current CA is used to sign the CMP request packet, the CA uses the current CA and CA certificate chain to verify the signature certificate of the request packet.
  - For a CA that has been created and is in the pending state, if the CA certificate is not uploaded within 15 days, the CA will be deleted.

- Updating a Key

  Choose **PKI Management** > **CA**. Click **Rekeying** in the **Operation** column of a CA to update the key. After the key is updated, a new root CA is created and the OldWithNew and NewWithOld certificates are automatically created. You can view or download the associated certificates by referring to **Related Tasks**.

- Downloading a CA certificate

Choose **PKI Management** > **CA**. Click **Download CA Certificate** in the **Operation** column of a CA to download the CA certificate to the local computer.

Choose **PKI Management** > **CA**. Click a CA name. On the page that is displayed, click **Download CA Certificate** to download the CA certificate to the local computer.

NOTE

If the CA status is pending, the CA certificate cannot be downloaded.

Related Tasks

- Querying a CA

  Choose **PKI Management** > **CA**. Click a CA name to view the CA details on the **CA Information** tab page, including the status, Certificate SN length, signature algorithm, associated profile, and default profile.

- Querying a CA certificate

  Choose **PKI Management** > **CA**. Click a CA name to view the CA details on the **CA Certificate** tab page, including the version, SN, subject, and validity period.

  NOTE

  If the CA status is pending, you cannot view the CA certificate information.

- Querying an associate certificate

  Choose **PKI Management** > **CA**. Click a CA name to view the CA details on the **Associate Certificate** tab page, including the version, SN, subject, and validity period.

  NOTE

  - **OldWithNew**: Certificate generated when the CA key is updated. The certificate contains the public key of the old key. The validity period of the certificate is the same as that of the old CA. For the entity that uses the new certificate of the root CA as the trust root, if such an entity is not verified, you need to obtain the **OldWithNew** certificate of the root CA. The verification process is to use the root CA's new key to verify the old key, and then use the old key to verify the end entities that are originally subordinated to the old root CA.
  - **NewWithOld**: Certificate generated when the CA key is updated, including the public key of the new key. The effective date of the certificate is that of the new CA, and the expiration date is that of the old CA. For entities that use the old certificate of the root CA as the trust root, apply for a new certificate as soon as possible. During this period, if entities that use the new certificate of the root CA as the trust root need to be verified, obtain the **NewWithOld** certificate of the root CA first. The verification process is to use the root CA's old key to verify the new key, and then use the new key to verify the end entities that are originally subordinated to the new root CA.

- Downloading an associate certificate

  Choose **PKI Management** > **CA**. Click a CA name, and click **Download** on the **Associated Certificate** tab page to download the CA certificate to the local computer. If you select download multiple certificates, the selected certificates are combined and downloaded to a .pem certificate file.

- Modifying a CA

Choose **PKI Management** > **CA**. Click **Modify** in the **Operation** column of a CA to modify its configuration.

NOTE

- When modifying the CA configuration, you can only modify the **Max validity period**, **Certificate SN length**, **CRL generation interval**, **CRL generation time**, **CRL overlap time**, **Include revocation reasons, CRL server**, **Publication mode**, **CRL distribution point**, associated profile, and default profile of the CA.
- When you create a CA by uploading a file, if a certificate chain file has been uploaded, the **Upload Certificate Chain** option is not displayed when you configure the CA.
- When you create a CA by uploading a file, if the certificate chain file is not uploaded or fails to be uploaded, the **Upload Certificate Chain** option is displayed when you configure the CA.
- If the CA status is pending, the CA configuration information cannot be modified.

- Searching for a CA

  Choose **PKI Management** > **CA**. Enter a CA name in the search box and click to find the specified CA and view its details. The Certificate Authority Service supports fuzzy search by CA name.

- Searching for an associated profile

  When creating or modifying a CA on the **PKI Management** > **CA** page, enter the name of an associated profile in the search box on the page for setting associated profiles, and click to find the specified associated profile. The Certificate Authority Service supports fuzzy search by associated profile name.

- Searching for a default profile

  When creating or modifying a CA on the **PKI Management** > **CA** page, enter the name of a default profile in the search box on the page for setting default profiles, and click to find the specified default profile. The Certificate Authority Service supports fuzzy search by default profile name.

4.3.2.5 Applying for a Certificate

On the **Certificate Application** page, you can apply for a certificate in different modes as required.

4.3.2.5.1 Application Method 1: Entering Basic Information

To meet different requirements for certificate application, the Certificate Authority Service allows you to apply for a certificate by entering basic information.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Certificate Application** > **Certificate Application** from the navigation tree on the left.

Step 3 On the **Apply by Basic Info** tab page, enter certificate application information.

NOTE

- The subject information in the certificate application request must be different from that of the associated CA. Otherwise, certificate application fails.
- When applying for a certificate by configuring basic information, you can select only a profile whose certificate level is **End entity**.
- The validity period of a certificate is the intersection of the following four validity periods: validity period of the CA associated with the certificate, validity period set in the certificate profile, validity period set in the associated CA, and validity period set during certificate application.
- You can click **Reset** to clear parameter settings.

Step 4 Click **Submit**.

----End

Related Tasks

- Viewing a certificate

  On the **PKI Management** > **Certificate** page, click the SN of a certificate to view the certificate details.

  NOTE

  A certificate will be automatically deleted 30 days after it expires. If the number of certificates issued by the Certificate Authority Service exceeds 80% of the maximum number supported by the Certificate Authority Service, all expired certificates are automatically deleted.

- Updating a certificate

  On the **PKI Management** > **Certificate** page, click **Update** in the **Operation** column of a certificate to update it. After the certificate is updated, you can choose whether to download the certificate to the local computer.

  NOTE

  The certificate obtained by using CMP, privacy CA protocol or uploading the CSR file cannot be updated.

- Searching for a certificate

  On the **PKI Management** > **Certificate** page, enter the subject name of the certificate in the search box for a search. You can also specify the SN, validity period, revocation reason, issuer or status of the certificate in **Advanced Search**. The Certificate Authority Service supports fuzzy search by subject name, SN, validity period or issuer.

  On the **Certificate Application** > **Application List** page, enter the applicant, CA name, subject or submitted time of the certificate in the search box for a search. The Certificate Authority Service supports fuzzy search by applicant, CA name, subject or submitted time.

- Revoking a certificate

  On the **PKI Management** > **Certificate** page, click **Revoke** in the **Operation** column of a certificate to revoke it.

NOTICE

Only certificates whose revocation reason is "Certificate is on hold" can have their revocation canceled. Certificates revoked for other reasons can no longer be trusted.

- Canceling certificate revocation

  On the **PKI Management** > **Certificate** page, click **Undo Revoke** in the **Operation** column of a certificate to cancel the certificate revocation.

- Downloading a certificate
  - On the **Certificate Application** > **Application List** page, click **Download Certificate** in the **Operation** column of a certificate to download it to the local computer.

    NOTE

    - When downloading a certificate that is requested by entering basic information, you need to enter a password. The password is a string of 8 to 32 characters containing at least three of the following: digits, uppercase letters, lowercase letters, and special characters. In addition, the password cannot contain two or more of the same characters consecutively.
    - Only successfully obtained certificates can be downloaded.
  - On the **PKI Management** > **Certificate** page, click **Download** in the **Operation** column of a certificate, enter the file name and password, and download the certificate to the local computer.

    NOTE

    - The file name is a string of 1 to 20 characters containing uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_).
    - When downloading a certificate that is requested by entering basic information, you need to enter a password. The password is a string of 8 to 32 characters containing at least three of the following: digits, uppercase letters, lowercase letters, and special characters. In addition, the password cannot contain two or more of the same characters consecutively.

4.3.2.5.2 Application Method 2: Uploading a File

To meet different requirements for certificate application, the Certificate Authority Service allows you to apply for a certificate by uploading a CSR file.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Certificate Application** > **Certificate Application** from the navigation tree on the left.

Step 3 On the **Apply by File Upload** tab page, enter certificate application information.

Step 4 Click **Select** next to **CSR file**.

Step 5 Select a local CSR file and click **Submit**.

NOTE

- The subject information in the CSR file must be different from that of the associated CA. Otherwise, certificate application fails.
- The certificate chain file to be uploaded must be in .csr, .txt, or .req format, and the size of a single file cannot exceed 100 KB. The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space.
- You can click **Reset** to clear parameter settings.

----End

Related Tasks

- Viewing a certificate

  On the **PKI Management** > **Certificate** page, click the SN of a certificate to view the certificate details.

  NOTE

  A certificate will be automatically deleted 30 days after it expires. If the number of certificates issued by the Certificate Authority Service exceeds 80% of the maximum number supported by the Certificate Authority Service, all expired certificates are automatically deleted.

- Updating a certificate

  On the **PKI Management** > **Certificate** page, click **Update** in the **Operation** column of a certificate to update it. After the certificate is updated, you can choose whether to download the certificate to the local computer.

  NOTE

  The certificate obtained by using CMP, privacy CA protocol or uploading the CSR file cannot be updated.

- Searching for a certificate

  On the **PKI Management** > **Certificate** page, enter the subject name of the certificate in the search box for a search. You can also specify the SN, validity period, revocation reason, issuer or status of the certificate in **Advanced Search**. The Certificate Authority Service supports fuzzy search by subject name, SN, validity period or issuer.

  On the **Certificate Application** > **Application List** page, enter the applicant, CA name, subject or submitted time of the certificate in the search box for a search. The Certificate Authority Service supports fuzzy search by applicant, CA name, subject or submitted time.

- Revoking a certificate

  On the **PKI Management** > **Certificate** page, click **Revoke** in the **Operation** column of a certificate to revoke it.

  NOTICE

  Only certificates whose revocation reason is "Certificate is on hold" can have their revocation canceled. Certificates revoked for other reasons can no longer be trusted.

- Canceling certificate revocation

  On the **PKI Management** > **Certificate** page, click **Undo Revoke** in the **Operation** column of a certificate to cancel its revocation.

- Downloading a certificate
  - On the **Certificate Application** > **Application List** page, click **Download Certificate** in the **Operation** column of a certificate to download it to the local computer.

    NOTE

    - When downloading a certificate that is requested by entering basic information, you need to enter a password. The password is a string of 8 to 32 characters containing at least three of the following: digits, uppercase letters, lowercase letters, and special characters. In addition, the password cannot contain two or more of the same characters consecutively.
    - Only successfully obtained certificates can be downloaded.
  - On the **PKI Management** > **Certificate** page, click **Download** in the **Operation** column of a certificate, enter the file name and password, and download the certificate to the local computer.

    NOTE

    - The file name is a string of 1 to 20 characters containing uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_).
    - When downloading a certificate that is requested by entering basic information, you need to enter a password. The password is a string of 8 to 32 characters containing at least three of the following: digits, uppercase letters, lowercase letters, and special characters. In addition, the password cannot contain two or more of the same characters consecutively.

4.3.2.5.3 Application Method 3: Applying Through Dual Certificates

Certificate Authority Service supports dual-certificate certificate application.

Context

Dual certificates refer to the signature certificate and encryption certificate, which are used to establish TLS connections.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Certificate Application** > **Certificate Application** from the navigation tree on the left.

Step 3 On the **Apply by Dual-Certificate** tab page, enter certificate application information.

For detailed parameter descriptions, see **Table 4-14**.

Table 4-14 Dual-certificate parameters

Parameter		Description	Value
Associated CA		Associated CA used to apply for a certificate from the CA.	N/A
Applicant		You can customize the name of a applicant to distinguish different applicants.	N/A
Signature certificate	Signature certificate profile	Signature certificate profile, which is used to issue the signature certificate.	N/A
	CSR file	Certificate signing request.	• The certificate chain file to be uploaded must be in .csr, .txt, or .req format. • Only one file can be uploaded and the file size cannot exceed 100 KB. • The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space. • The subject information in the CSR file must be different from that of the associated CA. Otherwise, certificate application fails.
Encryption certificate	Subject info is consistent with signature certificate's info	• If this option is selected, the subject information is the same as that of the signature certificate. • If this option is not selected, you need to enter the subject information configured in the profile after selecting an encryption certificate profile.	N/A
	Encryption certificate profile	Encryption certificate profile used to issue the encryption certification.	Only the profile of a certificate with the **End entity** level can be selected.

Step 4 Click **Submit.**

----End

Related Tasks

- Viewing a certificate

  On the **PKI Management** > **Certificate** page, click the SN of a certificate to view the certificate details.

  NOTE

  A certificate will be automatically deleted 30 days after it expires. If the number of certificates issued by the Certificate Authority Service exceeds 80% of the maximum number supported by the Certificate Authority Service, all expired certificates are automatically deleted.

- Updating a certificate

  On the **PKI Management** > **Certificate** page, click **Update** in the **Operation** column of a certificate to update it. After the certificate is updated, you can choose whether to download the certificate to the local computer.

  NOTE

  The certificate obtained by using CMP, privacy CA protocol or uploading the CSR file cannot be updated.

- Searching for a certificate

  On the **PKI Management** > **Certificate** page, enter the subject name of the certificate in the search box for a search. You can also specify the SN, validity period, revocation reason, issuer or status of the certificate in **Advanced Search**. The Certificate Authority Service supports fuzzy search by subject name, SN, validity period or issuer.

  On the **Certificate Application** > **Application List** page, enter the applicant, CA name, subject or submitted time of the certificate in the search box for a search. The Certificate Authority Service supports fuzzy search by applicant, CA name, subject or submitted time.

- Revoking a certificate

  On the **PKI Management** > **Certificate** page, click **Revoke** in the **Operation** column of a certificate to revoke it.

  NOTICE

  Only certificates whose revocation reason is "Certificate is on hold" can have their revocation canceled. Certificates revoked for other reasons can no longer be trusted.

- Canceling certificate revocation

  On the **PKI Management** > **Certificate** page, click **Undo Revoke** in the **Operation** column of a certificate to cancel its revocation.

- Downloading a certificate
  - On the **Certificate Application** > **Application List** page, click **Download Certificate** in the **Operation** column of a certificate to download it to the local computer.

NOTE

- When downloading a certificate that is requested by entering basic information or using dual certificates, you need to enter a password. The password is a string of 8 to 32 characters containing at least three of the following: digits, uppercase letters, lowercase letters, and special characters. In addition, the password cannot contain two or more of the same characters consecutively.
- Only successfully obtained certificates can be downloaded.

– On the **PKI Management** > **Certificate** page, click **Download** in the **Operation** column of a certificate, enter the file name and password, and download the certificate to the local computer.

NOTE

- The file name is a string of 1 to 20 characters containing uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_).
- When downloading a certificate that is requested by entering basic information or using dual certificates, you need to enter a password. The password is a string of 8 to 32 characters containing at least three of the following: digits, uppercase letters, lowercase letters, and special characters. In addition, the password cannot contain two or more of the same characters consecutively.

4.3.2.6 Configuring a CRL Server

If you want to publish the CRL corresponding to a CA to a specified CRL server, you can configure information about the CRL server on the CRL management page.

Context

The Certificate Authority Service supports manual and automatic CRL publishing.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **PKI Management** > **CRL** from the navigation tree on the left.

Step 3 On the **CRL Server** tab page, click **New** and set parameters.

For detailed parameter descriptions, see **Table 4-15**.

Table 4-15 CRL server parameters

Parameter	Description	Value
Label	Name of a CRL server.	The name is a string of 1 to 45 characters containing letters, digits, underscores (_), and hyphens (-). The name cannot be **null** or **all** (case insensitive).

Parameter	Description	Value
IP address	IP address of the server.	N/A
Protocol	Type of the CRL server, which can be LDAP or FTP. A maximum of five servers can be added regardless of the server type. **NOTICE** LDAP is recommended because of its higher security than FTP.	N/A
Use TLS	Whether to publish the CRL to the LDAP server or FTP server using TLS. **NOTE** • If you select **Yes**, you can import the CRL corresponding to the trusted certificate chain on the **CRL Server** tab page to check whether the peer server certificate has been revoked. • If you select **No**, you cannot import the CRL on the **CRL Server** tab page. **NOTICE** If you do not use the TLS protocol, a security risk may exist.	The default value is **Yes**.
Port	Port number of the server.	• The port number is an integer ranging from 1 to 65535. • If the LDAP is selected and the TLS protocol is not used, the default port number is 389. • If the LDAP is selected and the TLS protocol is used, the default port number is 636. • When the FTP is selected, the default port number is 21. **NOTICE** LDAP is recommended because of its higher security than FTP.

Parameter	Description	Value
Login name	User name for logging in to the server.	The login name is a string 1 to 128 characters and cannot contain the following special characters: (/\: *?" <>|).
Login password	Password for logging in to the server.	It is recommended that the password contain 6 to 64 characters, including at least three types of the following: digits, uppercase letters, lowercase letters, and special characters. The password cannot be the same as the login name or the reverse of the login name.

Parameter	Description	Value
Publication directory	Directory of the server to which the CRL is published. You can use parameters such as **File path** or **Distinguished name** generated by the system to interconnect with the CRL server of the Certificate Authority Service. ● The publication directory of the FTP server is user-defined, for example, a/b. After a CRL server is created, the system generates a file path in format of *FTP root directory*|*Publication directory*|*CA name associated with the server*|*CRL file name*, where the CRL file name is the CA name and the file name extension is .crl. For example, the file path can be **/home/ftpuser/a/b/caname/caname.crl.** ● The publication directory of the LDAP server is the LDAP path name, for example, **CN=common name, O=organization, OU=organization unit**. After a CRL server is created, the system generates a distinguished name in format of **CN=***CA name associated with the server***,** *Publishing directory*. For example, the distinguished name can be **CN=caname, CN=common name, O=organization, OU=organization unit**.	N/A

Parameter	Description	Value
Trust certificate chain	Local certificate chain file. **NOTICE** If the RSA key length is 1024 or the uploaded trust certificate uses the SHA1withRSA algorithm, security risks exist.	• The certificate file must be in .pem, .cer, or .crt format. • The certificate to be uploaded must be a complete certificate chain. A maximum of 10 files can be uploaded, and the size of a single file cannot exceed 100 KB. • The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space.

Step 4 Click **Submit**.

----End

Related Tasks

- Viewing a CRL server

  On the **CRL Server** tab page under **PKI Management** > **CRL**, click the name of a CRL server to view detailed information about this CRL server.

- Modifying a CRL server

  On the **CRL Server** tab page under **PKI Management** > **CRL**, click **Modify** in the **Operation** column of a CRL server to modify the configuration of this CRL server.

- Deleting a CRL server

  On the **CRL Server** tab page under **PKI Management** > **CRL**, click **Delete** in the **Operation** column of a CRL server to delete this CRL server.

- Importing a CRL

  On the **CRL Server** tab page under **PKI Management** > **CRL**, click **Import CRL** in the **Operation** column of a CRL server to upload the CRL of the trusted certificate chain for checking whether the peer server certificate is revoked.

  NOTE

  The CRL file to be uploaded must be in .crl or .pem format and the file size cannot exceed 2 MB.

- Updating a CRL

  On the **CRL** tab page under **PKI Management** > **CRL**, click **Update** in the **Operation** column of a CRL to manually update the CRL.

- Manually publishing a CRL

  On the **CRL** tab page under **PKI Management** > **CRL**, click **Publish** in the **Operation** column of a CRL to manually publish the CRL.

- Automatically publishing a CRL

  When configuring a CA on the **PKI Management** > **CA** page, you can set an interval for automatically publishing CRLs. Then the system automatically publishes CRLs at the specified interval.

- Searching for a CRL

  On the **CRL** tab page under **PKI Management** > **CRL**, enter a CR name, click  , and view CRL information of the CA that is searched out. The Certificate Authority Service supports fuzzy search by CA name.

- Downloading a CRL

  On the **CRL** tab page under **PKI Management** > **CRL**, click **Download** in the **Operation** column of a CRL to download the CRL in DER or PEM format to the local computer.

4.3.2.7 Configuring a Whitelist

You can configure a whitelist to verify certificate requests. If the common name is in the whitelist, the requests are allowed. Otherwise, the requests are rejected.

Context

If the whitelist verification function is enabled, a certificate can be successfully obtained only when the common name is in the whitelist after a user submits a certificate request.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **PKI Management** > **Whitelist** from the navigation tree on the left.

Step 3 Click **New**. The **Create Whitelist** dialog box is displayed.

Step 4 Enter the whitelist information.

NOTE

- Common name: Mandatory. The common name is a string of 1 to 127 characters containing uppercase letters, lowercase letters, digits, spaces, hyphens (-), colons (:), and dots (.).
- Description: optional. The description is a string of 0 to 128 characters containing digits, uppercase letters, lowercase letters, spaces, and special characters (, . ? ! : ;).
- You can click **Reset** to clear parameter settings.

Step 5 Click **Submit**.

----End

Related Tasks

- Enabling whitelist verification

Choose **Protocol Configuration** > **CMP**. On the **Protocol Configuration** tab page, click **Modify** corresponding to a CA. On the page that is displayed, set **Verify Whitelist** to **Yes**.

NOTE

- By default, the whitelist verification function is disabled.
- The whitelist verification function takes effect only when you apply for a certificate using CMP.

- Modifying a whitelist

  Choose **PKI Management** > **Whitelist**. Click **Modify** corresponding to the desired whitelist and modify it.

- Importing a whitelist

  Choose **PKI Management** > **Whitelist**. Click **Import** to manually import a whitelist.

  NOTE

  - You can download the template file, set parameters following the instructions, and upload the file.
  - The file to be uploaded must be in .csv format and the size of a single file cannot exceed 20 MB. The file can contain a maximum of 4 million data records, but a maximum of 50,000 records can be imported at a time.

- Deleting a whitelist

  Choose **PKI Management** > **Whitelist**. Select the whitelist to be deleted and click **Delete** or click **Delete** corresponding to the whitelist.

- Searching for a whitelist

  Choose **PKI Management** > **Whitelist**. In the search box, enter a common name and click  to search for a specific whitelist. The Certificate Authority Service supports fuzzy search by whitelist name.

4.3.2.8 Configuring CMP

When applying for a certificate using CMP, you need to configure CMP information, request verification, and response protection for data encryption.

4.3.2.8.1 Configuring CMP Information

To apply for a certificate using CMP, you need to first configure CMP information.

Prerequisites

- In the non-multi-tenant deployment scenarios, if the port used by the CMP is not enabled, you need to enable the port on the **Certificate Authority Service** > **Global Configuration** > **Port Management** page.
- In the multi-tenant deployment scenarios, if the port used by the CMP is not enabled, the system administrator needs to enable the port on the **Certificate Authority Service** > **Global Configuration** > **Port Management** page.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Protocol Configuration** > **CMP** from the navigation tree on the left.

Step 3 On the **Protocol Configuration** tab page, click **Modify** corresponding to a CA. On the page that is displayed, set required parameters.

For detailed parameter descriptions, see **Table 4-16**.

Table 4-16 CMP parameters

Parameter	Description	Value
CA	Name of a CA.	The CA name cannot be changed.
Protocol	You can select HTTP, one-way authentication, or two-way authentication. **NOTE** HTTPS is more secure than HTTP. Therefore, you are advised to select HTTPS (**One-way authentication** or **Two-way authentication**) when configuring CMP.	The default value is **two-way authentication**.
Port	Port number. If the selected port is disabled, the message "The port is disabled." is displayed. You cannot apply for a certificate using this port.	• When HTTP is selected, the default port number is 26801 and cannot be changed. • When one-way authentication is selected, the default port number is 26802 and cannot be changed. • When two-way authentication is selected, the default port number is 26803 and cannot be changed.
Version	TLS version corresponding to one-way authentication and two-way authentication.	By default, **TLSv1.2** and **TLSv1.3** are selected and cannot be modified.
Send CA certificate	Whether to send the CA certificate to the terminal.	The default value is **Yes**.
Send responder certificate	Whether to send the response protection certificate to the terminal.	The default value is **Yes**.

Parameter	Description	Value
Return certificate chain	Whether to return the certificate chain to the terminal.	The default value is **Yes**.
Verify whitelist	Whether to enable the whitelist verification function. **NOTE** • If this parameter is set to **Yes**, the Certificate Authority Service enables the whitelist verification function. When you apply for a certificate from the Certificate Authority Service using CMP, the certificate can be successfully applied only when the common name is in the whitelist. • If this parameter is set to **No**, the Certificate Authority Service does not enable the whitelist verification function.	The default value is **No**.
Request time required	Checks whether the time in the certificate application request is the same as the current time. **NOTE** • If this parameter is set to **Yes**, the certificate application request must contain this parameter. The Certificate Authority Service checks whether the value of this parameter is within the **Allowed message time deviation** range. • If this parameter is set to **No**, the certificate application request does not need to contain this parameter. If the certificate application request contains this parameter, the Certificate Authority Service checks whether the value of this parameter is within the **Allowed message time deviation** range.	The default value is **No**.

Parameter	Description	Value
Use the validity period from CMP request	Whether to use the validity period in the CMP request packet when applying for a certificate. **NOTE** • If you select **Yes**, the validity period of a certificate is the intersection of the following four validity periods: validity period of the CA associated with the certificate, validity period set in the certificate profile, validity period set in the associated CA, and validity period set in the CMP request. • If you select **No**, the validity period of a certificate is the intersection of the following three validity periods: validity period of the CA associated with the certificate, validity period set in the certificate profile, and validity period set in the associated CA.	The default value is **No**.
Use CA for responder	Whether to use the CA to protect messages sent to terminals. **NOTE** If this parameter is set to **Yes**, the CA is used for response protection. You do not need to set response protection on the **Responder Configuration** tab page.	The default value is **Yes**.
Allowed message time deviation	The Certificate Authority Service checks whether the deviation between the time in the certificate application request and the current time is within the allowed time deviation range.	The value is an integer ranging from 1 to 3600, in seconds.
Use asynchronous polling	After a terminal sends a certificate application request to the CA, the CA generates a certificate in asynchronous mode. The terminal must periodically and continuously send polling messages to check whether the CA has issued the certificate.	The default value is **No**.

Parameter	Description	Value
Polling interval	Polling interval of the terminal.	The value is an integer ranging from 1 to 3600, in seconds.
Certificate confirmation waiting time	Time after which the CA revokes the certificate if the end entity receiving the certificate does not send a certificate confirmation packet to the CA, when the certificate application request is explicitly acknowledged.	The value is an integer ranging from 1 to 3600, in seconds.
Message protection signature algorithm	Signature algorithm to be used. If the signature algorithm used by the terminal is not selected, the CA rejects the request sent by the terminal.	N/A
POP signature algorithm	Required signature algorithm. It is used to check whether the public key submitted by the terminal has a corresponding private key.	N/A

Parameter	Description	Value
CMP request URI	A user applies for a certificate from the Certificate Authority Service using CMP. The CMP request URI has the following two formats: • The request URI contains the name of the CA that issues the certificate and the name of the used certificate profile, for example, **https://{IP}:26802/cmp/caname?certprofile=profilename**, where **caname** is the name of the CA that issues the certificate, and **profilename** is the name of the used certificate profile. • The request URI contains only the name of a CA that issues the certificate and does not contain the profile name parameter. The default profile of the CA is used for certificate application. An example of this request is **https://{IP}:26802/cmp/caname**, where **caname** is the name of the CA that issues the certificate.	The CMP request URI cannot be modified.

Step 4 Click **Submit**.

----End

Follow-up Procedure

Applying for a certificate based on the CMP request URI

On the **Protocol Configuration** > **CMP** page, click the **Protocol Configuration** tab. On this tab page, click > on the left of a CA name, and copy the CMP request URI corresponding to the CA for use. The CMP request URIs include the following types:

- HTTP
  - http://*IP address*:26801/cmp/*CA name*

  - http://*IP address*:26801/cmp/*CA name*?certprofile=*Certificate profile name*
- One-way authentication
  - https://*IP address*:26802/cmp/*CA name*
  - https://*IP address*:26802/cmp/*CA name*?certprofile=*Certificate profile name*
- Two-way authentication
  - https://*IP address*:26803/cmp/*CA name*
  - https://*IP address*:26803/cmp/*CA name*?certprofile=*Certificate profile name*

For example, http://*IP address*:26801/cmp/caname?certprofile=profilename indicates that a CMP request for applying for a certificate is sent to the Certificate Authority Service through HTTP. In the URL, the IP address indicates the IP address of the Certificate Authority Service.

NOTE

- The **certprofile** parameter specifies the end entity profile used for issuing certificates. This parameter is optional. If this parameter is not specified, the default CA profile is used for certificate application.
- A CA may be associated with multiple profiles. Therefore, the CMP request URI may have multiple values. Select a value based on the site requirements.
- The subject information in the certificate application request must be different from that of the associated CA. Otherwise, certificate application fails.

Related Tasks

- Viewing CMP configuration

  Choose **Protocol Configuration** > **CMP**. On the **Protocol Configuration** tab page, click  on the left of a CA name to access the details page, where you can check the CMP configuration.
- Searching for CMP configuration

  Choose **Protocol Configuration** > **CMP**. On the **Protocol Configuration** tab page, enter a CA name in the search box, and click  to find the specified CA and view the detailed protocol configuration of the CA. The Certificate Authority Service supports fuzzy search by CA name.

4.3.2.8.2 Configuring Request Verification

Request verification protects request messages send by terminals to a CA.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Protocol Configuration** > **CMP** from the navigation tree on the left.

Step 3 On the **Requestor Configuration** tab page, click **Add**. On the **Add Requestor Configuration** page, set required parameters.

For detailed parameter descriptions, see **Table 4-17**.

Table 4-17 Request verification parameters

Parameter	Description	Value
Label	Name of a request verification certificate.	The value can contain only digits, letters, underscores (_), and hyphens (-), but cannot be **null** or **all** (case-insensitive).

Parameter			Description	Value
Authentication mode	Certificate	Certificate configuration mode	• Upload vendor root CA certificate: Uses the vendor root CA certificate to verify the validity of the signature certificate and certificate chain in the CMP packet. In this mode, you need to upload the vendor certificate and select the associated CA. Obtain the vendor root CA certificate by referring to the method provided by the supplier. • New self-signed certificate: If the identity certificate and private key are not available, you can use this method to generate a self-signed certificate using the Certificate Authority Service. Once downloaded, this certificate can be used to sign the CMP request packet. The Certificate Authority Service uses the certificate to verify the validity of the request. In this mode, you need to select the root CA certificate profile, signature algorithm, and associated CA. • Upload obtained identity certificate: If an identity certificate is obtained and the private key of this certificate is used to sign the CMP request packet, you can use this method to upload the identity certificate to the CA server to verify the validity of the request. In this mode, you need to upload the identity	• The vendor root certificate to be uploaded must be in .cer, .crt, .p7b, or .pem format. Only one file can be uploaded and the file size cannot exceed 100 KB. The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space. • The obtained identity certificate to be uploaded must be in .cer or .crt format. Only one file can be uploaded and the file size cannot exceed 10 KB. The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space. • One request verification can be associated with a maximum of 32 CAs.

Parameter			Description	Value
			certificate and select the associated CA.	
	Pre-shared key	Pre-shared key	When a user uses a pre-shared key to protect CMP request messages, the same pre-shared key must be configured on the CA. The CA uses the pre-shared key to authenticate request messages and protect response messages.	The password must be a string of 8 to 128 characters that contain at least three types of the following: digits, uppercase letters, lowercase letters, and special characters. In addition, the password cannot contain three or more of the same characters consecutively.
		Associated CA	Select an associated CA and configure the request verification to verify the validity of the certificate request of the CA.	One request verification can be associated with a maximum of 32 CAs.

Step 4 Click **Submit**.

----End

Related Tasks

- Viewing request verification information

  Choose **Protocol Configuration** > **CMP**. On the **Requestor Configuration** tab page, click a request verification name. On the page that is displayed, you can view the detailed information.

- Searching for request verification information

  Choose **Protocol Configuration** > **CMP**. On the **Requestor Configuration** tab page, enter a request verification name in the name search box and click to find the specified request verification and view the details. The Certificate Authority Service supports fuzzy search by request verification name.

- Modification request verification

  Choose **Protocol Configuration** > **CMP**. On the **Requestor Configuration** tab page, click **Modify** corresponding to the desired request verification. On the page that is displayed, modify request verification information.

  NOTE

  The request verification name cannot be changed.

- Deleting request verification

  Choose **Protocol Configuration** > **CMP**. On the **Requestor Configuration** tab page, click **Delete** corresponding to the desired request verification.

- Downloading a request verification certificate

Choose **Protocol Configuration** > **CMP**. On the **Requestor Configuration** tab page, click **Download** corresponding to the desired request verification to download the request verification certificate.

NOTE

- The password is a string of 8 to 32 characters containing at least three of the following: digits, uppercase letters, lowercase letters, and special characters. In addition, the password cannot contain two or more of the same characters consecutively.
- The downloaded request verification certificate is in .p12 format. The password is contained in the .p12 file. Enter the password for verification when using a certificate file in .p12 format.
- You can download the request verification certificate only when the signature type is self-signed.

4.3.2.8.3 Configuring Response Protection

Response protection protects response messages sent by a CA to terminals.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Protocol Configuration** > **CMP** from the navigation tree on the left.

Step 3 On the **Responder Configuration** tab page, click **Add**. On the **Add Responder Configuration** page, set required parameters.

For detailed parameter descriptions, see **Table 4-18**.

Table 4-18 Response protection parameters

Parameter	Description	Value
Label	Name of a response protection certificate.	The value can contain only digits, letters, underscores (_), and hyphens (-), but cannot be **null** or **all** (case-insensitive).

Parameter		Description	Value
Certificate configuration mode	New self-signed certificate	If no response verification certificate is available, you can use this method to generate a self-signed certificate using the Certificate Authority Service, and the private key of this certificate is used to sign the response. Once downloaded, this certificate can be used to verify the integrity of the CMP response. In this mode, you need to select the root CA certificate profile, signature algorithm, and associated CA.	N/A
	Upload certificate file	If a response signature certificate is obtained, you can use this method to import the certificate and private key to the Certificate Authority Service. The Certificate Authority Service uses the private key to sign the response, and you can use the certificate to verify the integrity of the response. In this mode, you need to upload a certificate file, enter the password of the matching certificate, and select the signature algorithm and associated CA.	• The certificate file to be uploaded must be in .p12 format. Only one file can be uploaded and the file size cannot exceed 20 KB. • The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space.

Step 4 Click **Submit**.

----End

Related Tasks

- Viewing response protection information

  Choose **Protocol Configuration** > **CMP**. On the **Responder Configuration** tab page, click a response protection name. On the page that is displayed, you can view the detailed information.

- Searching for response protection information

Choose **Protocol Configuration** > **CMP**. On the **Responder Configuration** tab page, enter a response protection name in the name search box and click  to find the specified response protection and view the details. The Certificate Authority Service supports fuzzy search by response protection name.

- Modifying response protection information

  Choose **Protocol Configuration** > **CMP**. On the **Responder Configuration** tab page, click **Modify** corresponding to the desired response protection. On the page that is displayed, modify response protection information.

  NOTE

  The response protection name cannot be changed.

- Deleting response protection

  Choose **Protocol Configuration** > **CMP**. On the **Responder Configuration** tab page, click **Delete** corresponding to the desired response protection.

- Downloading a response protection certificate

  Choose **Protocol Configuration** > **CMP**. On the **Responder Configuration** tab page, click **Download** corresponding to the desired response protection to download the response protection certificate.

  NOTE

  The downloaded response protection certificate file is in .pem format.

4.3.2.9 Configuring the Privacy CA Protocol

Before applying for a certificate using the Privacy CA protocol, you need to configure the EK trust certificate or pre-shared password in advance.

4.3.2.9.1 Configuring Privacy CA Protocol Information

To apply for a certificate using the privacy CA protocol, you need to first configure privacy CA protocol information.

Prerequisites

- In the non-multi-tenant deployment scenarios, if the port used by the privacy CA protocol is not enabled, you need to enable the port on the **Certificate Authority Service** > **Global Configuration** > **Port Management** page.
- In the multi-tenant deployment scenarios, if the port used by the privacy CA protocol is not enabled, the system administrator needs to enable the port on the **Certificate Authority Service** > **Global Configuration** > **Port Management** page.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Protocol Configuration > Privacy CA Protocol** from the navigation tree on the left.

Step 3 On the **Protocol Configuration** tab page, click **Modify** corresponding to a CA. On the page that is displayed, set required parameters. For detailed parameter descriptions, see **Table 4-19**.

Table 4-19 Privacy CA protocol parameters

Parameter	Description	Value
CA	Name of a CA.	The CA name cannot be changed.
Port	Port number corresponding to the privacy CA protocol.	The default value is 26805 and cannot be changed.
Use the validity period in the privacy CA request	Whether to use the validity period in the privacy CA request when applying for a certificate. **NOTE** If you select **Yes**, the validity period of a certificate is the intersection of the following four validity periods: validity period of the CA associated with the certificate, validity period set in the certificate profile, validity period set in the associated CA, and validity period set in the CMP request. If you select **No**, the validity period of a certificate is the intersection of the following three validity periods: validity period of the CA associated with the certificate, validity period set in the certificate profile, and validity period set in the associated CA.	The default value is Yes.
Challenge value expiration time	A user sends a challenge value request to the Certificate Authority Service through the privacy CA protocol. If the Certificate Authority Service does not receive the certificate application request within the specified time, the challenge value expires and the verification fails. As a result, the Certificate Authority Service cannot issue the AK certificate.	The default value is 60 and cannot be changed. The unit is minute.

Parameter	Description	Value
Privacy CA protocol request URI	A user applies for a certificate from the Certificate Authority Service using the privacy CA protocol. The privacy CA protocol request URI has the following two formats: • The request URI contains the name of the CA that issues the certificate and the name of the used certificate profile, for example, **https://{IP}:26805/pca/v1/caname?certprofile=profilename**, where **v1** is the API version, **caname** is the name of the CA that issues the certificate, and **profilename** is the name of the used certificate profile. • The request URI contains only the name of a CA that issues the certificate and does not contain the profile name parameter. The default profile of the CA is used for certificate application. An example of this request is **https://{IP}:26805/pca/v1/caname**, where **v1** is the API version and **caname** is the name of the CA that issues the certificate.	The privacy CA protocol request URI cannot be changed.

Step 4 Click Submit.

----End

Follow-up Procedure

Applying for a certificate based on the privacy CA request URI

Choose **Protocol Configuration** > **Privacy CA Protocol**. On the **Protocol**

Configuration tab page, click > on the left of a CA name, and copy the privacy CA request protocol URI of the CA for use.

One-way authentication

- https://*IP address*:26805/pca/v1/*CA name*
- https://*IP address*:26805/pca/v1/*CA name*?certprofile=*Certificate profile name*

For example, https://*IP address*:26805/pca/v1/caname?certprofile=profilename indicates that a privacy CA request for certificate application is sent to the Certificate Authority Service through the one-way TLS authentication protocol. In the URL, the IP address indicates the IP address of the Certificate Authority Service.

NOTE

- The **certprofile** parameter specifies the end entity profile used for issuing certificates. This parameter is optional. If this parameter is not specified, the default CA profile is used for certificate application.
- A CA may be associated with multiple profiles. Therefore, the privacy CA protocol request URI may have multiple values. Select a value based on the site requirements.
- The subject information in the certificate application request must be different from that of the associated CA. Otherwise, certificate application fails.

Related Tasks

- Viewing privacy CA protocol configuration

  Choose **Protocol Configuration** > **Privacy CA Protocol**. On the **Protocol Configuration** tab page, click > on the left of a CA name to view the privacy CA protocol details.
- Searching for privacy CA protocol configuration

  Choose **Protocol Configuration** > **Privacy CA Protocol**. On the **Protocol Configuration** tab page, enter a CA name in the search box, and click to find the specified CA and view the detailed protocol configuration of the CA. The Certificate Authority Service supports fuzzy search by CA name.

4.3.2.9.2 Configuring the EK Trust Certificate

You need to configure the EK trust certificate when applying for an AK certificate.

Context

If the EK certificate is preinstalled on the device, a user uses the RA client to send a challenge value request to the Certificate Authority Service using the privacy CA protocol and import the EK trust certificate chain. The request contains the public AK and EK certificate. After receiving the request, the Certificate Authority Service verifies the public AK information and uses the imported EK trust certificate chain to verify the EK certificate. If the verification is successful, the Certificate Authority Service returns the encrypted challenge value. The user then uses the RA client to send a certificate application request to the Certificate Authority Service using the privacy CA protocol. The request contains the CA name, certificate profile name, subject information, and challenge value. After receiving the request, the Certificate Authority Service checks whether the challenge value has expired and verifies the public AK information. If the verification is successful, the Certificate Authority Service issues the AK certificate.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Protocol Configuration** > **Privacy CA Protocol** from the navigation tree on the left.

Step 3 On the **EK Trust Certificate Configuration** tab page, click **Add** and set the parameters required for the EK trust certificate.

For detailed parameter descriptions, see **Table 4-20**.

Table 4-20 EK trust certificate parameters

Parameter	Description	Value
Label	You can customize the name of the EK trust certificate to distinguish different certificate files.	The value must be a string of 1 to 45 characters, including digits, letters, underscores (_), and hyphens (-). The value cannot be **null** or **all** (case-insensitive).
EK trust certificate	Select the local EK trust certificate file and upload it to verify the request of certificate application through the privacy CA protocol.	• The EK trust certificate file to be uploaded must be in .cer, .crt, or .pem format. A maximum of 10 files can be uploaded at a time, and the total file size cannot exceed 100 KB. • The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space.

Step 4 After the configuration is complete, click **Submit**. On the **EK Trust Certificate Configuration** tab page, you can view the configured EK trust certificate file.

----End

Related Tasks

- Viewing an EK trust certificate

  Choose **Protocol Configuration** > **Privacy CA Protocol**. On the **EK Trust Certificate Configuration** tab page, click > on the left of an EK trust certificate name to view its details.
- Searching for an EK trust certificate

Choose **Protocol Configuration** > **Privacy CA Protocol**. On the **EK Trust Certificate Configuration** tab page, enter the name of an EK trust certificate in the search box, and click to find the specified certificate and view its details. The Certificate Authority Service supports fuzzy search by the name of the EK trust certificate.

- Deleting an EK trust certificate

  Choose **Protocol Configuration** > **Privacy CA Protocol**. On the **EK Trust Certificate Configuration** tab page, click **Delete** on the right of an EK trust certificate to delete it.

4.3.2.9.3 Configuring a Pre-Shared Password

You need to set a pre-shared password when applying for the EK certificate.

Context

If the EK certificate is not preinstalled on the device before delivery, the user uses the privacy CA protocol to send a challenge value request to the Certificate Authority Service through the remote attestation client, and sets a pre-shared password on the Certificate Authority Service and remote attestation client for message authentication. A user logs in to the remote attestation client, and uses the privacy CA protocol to send a certificate application request to the Certificate Authority Service. The request contains information, such as the CA name, certificate profile name, subject information, and challenge value. After obtaining the request, the Certificate Authority Service checks whether the challenge value has expired and verifies the AK public key information. If the verification is successful, the Certificate Authority Service issues the EK certificate.

A user uses the RA client to send a challenge value request to the Certificate Authority Service using the privacy CA protocol and import the EK trust certificate chain. The request contains the public AK and EK certificate. After receiving the request, the Certificate Authority Service verifies the public AK information and uses the imported EK trust certificate chain to verify the EK certificate. If the verification is successful, the Certificate Authority Service returns the encrypted challenge value. The user then uses the RA client to send a certificate application request to the Certificate Authority Service using the privacy CA protocol. The request contains the CA name, certificate profile name, subject information, and challenge value. After receiving the request, the Certificate Authority Service checks whether the challenge value has expired and verifies the public AK information. If the verification is successful, the Certificate Authority Service issues the AK certificate.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Protocol Configuration** > **Privacy CA Protocol** from the navigation tree on the left.

Step 3 On the **Pre-Shared Password Configuration** tab page, click **Add** and set the parameters required for the pre-shared password.

For detailed parameter descriptions, see **Table 4-21**.

Table 4-21 Pre-shared password parameters

Parameter	Description	Value
Label	You can customize the name of a pre-shared password to distinguish different passwords.	The name is a string of 1 to 45 characters containing letters, digits, underscores (_), and hyphens (-).The name cannot be null or all (case insensitive).
Pre-shared password	Customize a pre-shared password for message integrity protection and identity authentication during message authentication.	• The password must be a string of 12 to 128 characters that contain at least three types of the following: digits, uppercase letters, lowercase letters, and special characters. In addition, the password cannot contain three or more of the same characters consecutively. • A maximum of 16 pre-shared passwords can be configured.
Associated CA	Select an associated CA and configure the pre-shared password for verifying the challenge request.	N/A

Step 4 After the configuration is complete, click **Submit**.

----End

Related Tasks

- Searching for the pre-shared password

  Choose **Protocol Configuration** > **Privacy CA Protocol**. On the **Pre-Shared Password Configuration** tab page, enter a pre-shared password name in the search box and click to find the pre-shared password. The Certificate Authority Service supports fuzzy search by pre-shared password name.

- Modifying the pre-shared password

  Choose **Protocol Configuration** > **Privacy CA Protocol**. On the **Pre-Shared Password Configuration** tab page, click **Modify** on the right of the pre-shared password to change the pre-shared password.

- Deleting the pre-shared password

  Choose **Protocol Configuration** > **Privacy CA Protocol**. On the **Pre-Shared Password Configuration** tab page, click **Delete** on the right of the pre-shared password to delete the pre-shared password.

4.3.2.10 Global Configuration

On the **Global Configuration** page, you can configure the CMP port status or privacy CA protocol port status and TLS certificate.

4.3.2.10.1 Configuring a Port

On the **Port Management** page, you can view the current port status and manually enable or disable the HTTP port, TLS one-way authentication port, TLS two-way authentication port or privacy CA protocol port.

Context

- In the multi-tenant deployment scenario, you need to contact the administrator to configure a port.
- For details about the port description, see **Table 4-22**.

Table 4-22 Port parameters

Protocol	Port	Description
CMP	26801	HTTP port. After the port is enabled, you can use the CMP to apply for a certificate. **NOTE** HTTPS is more secure than HTTP. Therefore, you are advised to select HTTPS (**One-way authentication** or **Two-way authentication**) when configuring CMP.
	26802	One-way TLS authentication port. When the CMP is used to apply for a certificate, the client needs to authenticate the CA server.
	26803	Two-way TLS authentication port. When the CMP is used to apply for a certificate, the client and CA server must authenticate each other.
Privacy CA protocol	26805	One-way TLS authentication port. When the privacy CA protocol is used to apply for a certificate through this port, the client needs to authenticate the CA server.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Global Configuration** > **Port Management** from the navigation tree on the left.

Step 3 Enable or disable a port as required.

- Click **Enable** to enable the port.
- Click **Disable** to disable the port.

NOTE

- After the port is disabled and the HiSecLiteCA service is restarted, the certificate cannot be applied for through the port. Exercise caution when performing this operation.
- Actual status indicates the real status of the port on the CA server. If **Enable** is displayed, the port is enabled and can be used to apply for a certificate. If **Disable** is displayed, the port is disabled and cannot be used to apply for a certificate.
- Configured status indicates the required status of the port. If **Enable** is displayed, the port needs to be enabled. If **Disable** is displayed, the port needs to be disabled. After the service is restarted, the system port of the CA server is enabled or disabled based on the port's configured status and TLS certificate configuration.

----End

Follow-up Procedure

Restarting the Certificate Authority Service

After enabling or disabling a port, you need to restart the HiSecLiteCA service on the PowerEcho for the port configuration to take effect. For detailed operations, see "Stopping Product Services" and "Starting Product Services" in the *Administrator Guide*.

NOTE

After enabling the TLS one-way or two-way authentication port, you need to configure the corresponding TLS certificate and restart the HiSecLiteCA service on the PowerEcho for the port configuration to take effect.

Related Tasks

Querying the port status

On the **Global Configuration** > **Port Management** page, you can view the current status of a port in the **Actual Status** column.

4.3.2.10.2 Configuring TLS

When applying for a certificate using CMP or Privacy CA protocol, you can configure a TLS certificate to encrypt messages exchanged.

Context

- TLS is designed to ensure data confidentiality and integrity between two communication application programs.
- In the multi-tenant deployment scenario, you need to contact the system administrator to configure the TLS certificate.

Procedure

Step 1 Choose **System** > **About** > **Certificate Authority Service** from the main menu.

Step 2 Choose **Global Configuration** > **TLS Configuration** from the navigation tree on the left.

Step 3 Click **Certificate Configuration**. On the page that is displayed, set required parameters.

For detailed parameter descriptions, see **Table 4-23**.

Table 4-23 TLS certificate parameters

Parameter		Description	Value
Trust certificate chain	Trust certificate chain	Used by the server to check whether the client certificate is trusted during communication.	• The trust certificate chain file to be uploaded must be in .pem, .cer, or .crt format. • The certificate to be uploaded must be a complete certificate chain. A maximum of 16 files can be uploaded, and the size of the file to be uploaded at a time cannot exceed 100 KB. • The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space.
Identity certificate	Application protocol	The CMP or privacy CA protocol can be used for the identity certificate. Each application protocol corresponds to only one identity certificate.	N/A
	Identity certificate	Identity certificate of the server, which is verified by the client to determine whether the server is trusted during communication.	• The identity certificate file to be uploaded must be in .p12 format. Only one file can be uploaded and the file size cannot exceed 20 KB. • The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space.

Parameter		Description	Value
	Certificate password	Password set for a certificate during certificate application. The password is contained in the .p12 file. You need to enter this password when uploading the certificate file.	N/A
	Upload certificate chain	Upload the corresponding certificate chain. You can select multiple files. For example, if a level-3 CA certificate is imported, upload the corresponding level-1 and level-2 CA certificates.	• The identity certificate chain file to be uploaded must be a .cer, .crt, or .pem file smaller than 100 KB. A maximum of 10 files can be uploaded. • The certificate file name is a string of 1 to 256 characters containing Chinese characters, digits, letters, underscores (_), and hyphens (-), spaces, dots (.) and round brackets. It cannot start with a dots (.) or space.

NOTE

If the TLS identity certificate exists, a dialog box is displayed when you select **Identity Certificate** or change the application protocol.

- If you click **OK**, the current identity certificate will be replaced. If an identity certificate issued by another CA is uploaded, the trust certificate of the device must be updated accordingly. Otherwise, the TLS connection between the device and the Certificate Authority Service fails to be established.
- If you click **Cancel**, the identity certificate will not be replaced.

Step 4 Upload the trust certificate chain or identity certificate and click **Submit**.

NOTE

When one-way TLS is selected, you only need to upload the identity certificate. When two-way TLS is selected, you need to upload both the trust certificate chain and identity certificate.

----End

Follow-up Procedure

Restarting the Certificate Authority Service

After the TLS certificate is uploaded or deleted, restart HiSecLiteCA on the PowerEcho for the TLS configuration to take effect. For detailed operations, see

"Stopping Product Services" and "Starting Product Services" in the *Administrator Guide*.

Related Tasks

- Viewing a TLS certificate

  On the **Global Configuration** > **TLS Configuration** page, click the SN of the TLS certificate to view the certificate details.

- Deleting a TLS certificate

  On the **Global Configuration** > **TLS Configuration** page, click **Delete** on the right of the TLS certificate to delete the TLS certificate.

- Importing a CRL

  On the **Global Configuration** > **TLS Configuration** page, click **Import CRL** on the right of the TLS certificate to upload the CRL of the trusted certificate chain for checking whether the peer server certificate is revoked.

  NOTE

  The CRL file to be uploaded must be in .crl or .pem format and the file size cannot exceed 2 MB.

- Uploading a TLS certificate chain

  On the **Global Configuration** > **TLS Configuration** page, click **Upload Certificate Chain** on the right of the TLS certificate to upload the certificate chain file. You can perform this operation only for TLS identity certificates that are not configured with a certificate chain.

5 Operations on the App Client

This section describes the operations on the NetEco app.

5.1 Viewing Device Alarms

You can view the current alarms, historical alarms, and alarm details.

Prerequisites

You have logged in to the NetEco app.

Procedure

If You Need To...	Then...
View current alarms	1. In the lower part of the home screen, tap **Alarm**. By default, all alarms reported by NEs and systems are displayed. 2. On the **Current Alarms** tab, view details about the current alarm. • In the **Alarms** area, the total number of current alarms and the number of alarms of each severity are displayed. • Click an alarm to view alarm details. **NOTE** If the **Push notifications** function is enabled, you can tap an alarm in the message push area on the mobile phone to view the alarm details. For details about how to enable the **Push notifications** function, see **6.6 How Do I Enable or Disable the Message Push Function**.
View historical alarms	1. In the lower part of the home screen, tap **Alarm** and select **Historical Alarms**. 2. On the **Historical Alarms** tab, tap an alarm to view the alarm details.
Viewing the pushed alarm list	Tap  on a screen.

5.2 Viewing Site Monitoring Details

You can view the environment, key devices, alarms, and security protection monitoring details of each site.

Prerequisites

You have logged in to the NetEco app.

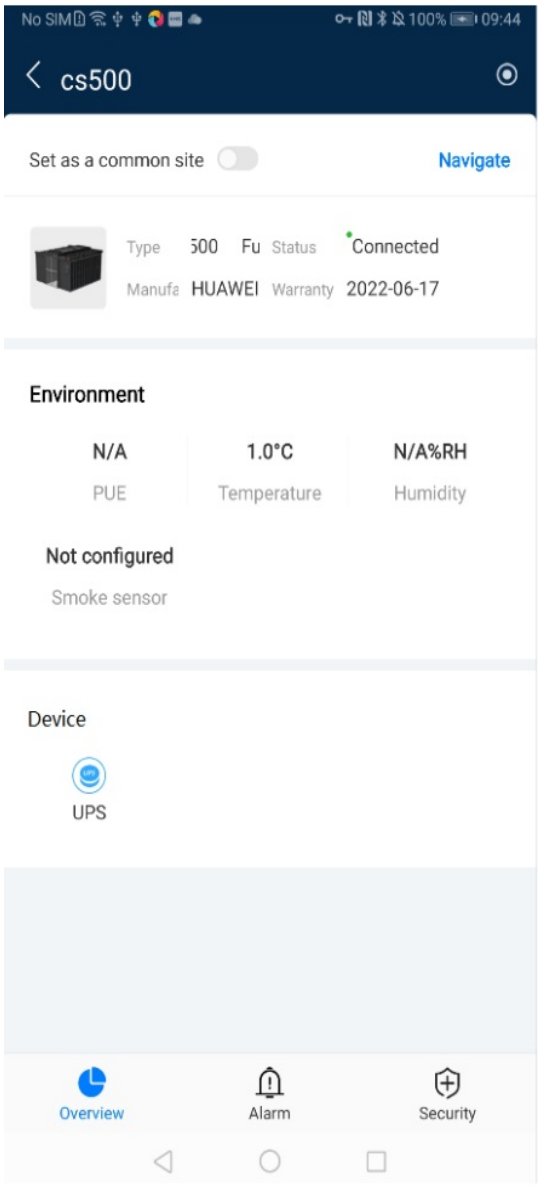
Procedure

Step 1 On the home screen, tap a site icon.

NOTE

On the home screen, tap  to view the site list. To return to the home screen, tap  on the **Site List** screen.

Figure 5-1 Site monitoring details



Step 2 On the site screen, perform the following operations as required.

Table 5-1 Viewing site monitoring details

Task	Operation
Viewing site overview	On the **Overview** tab, view the basic information about the site and the temperature, humidity, water, and smoke status of the devices in the **Environment** area.
Viewing device monitoring details	In the **Device** area, tap a device model to view the real-time monitoring data of the device.

Task	Operation
Viewing alarm monitoring details	In the lower area, tap the **Alarm** tab to view the alarm details of the site.
Viewing security monitoring details	In the lower part of the screen, tap the **Security** tab to view the door status and video surveillance information of the cabinets in the site. **NOTE** • To play a video, tap  . • To play a video in full screen mode, tap  .

----End

5.3 Custom Settings

You can set the **Push notifications** function or upgrade the app version as required.

Prerequisites

You have logged in to the NetEco app.

Procedure

Step 1 On the home screen of the NetEco app, tap **Me**.

Step 2 On the **Me** screen, perform the following operations as required.

Table 5-2 Custom settings

Operation	Description	Procedure
Setting the **Push notifications** function	You can enable or disable the **Push notifications** function as required.	For details, see **6.6 How Do I Enable or Disable the Message Push Function**.
Upgrading the app version	If a new version is detected, you can determine whether to upgrade the app to the new version based on the site requirements.	• Automatic upgrade: If a new version is available, the app displays a dialog box to remind you to upgrade the app. • Manual upgrade: Tap **Update check** to check whether an upgrade is required.

----End

6 FAQs

This section describes the common faults of the NetEco client, analyzes the possible causes, and provides the solutions.

6.1 How Do I Handle the Problem of Certificate Error or Security Alarm Displayed in the Web Browser

Symptom

- When the Google Chrome is used to log in to NetEco the system displays a connection error message as shown in **Figure 6-1**.
- When the Mozilla Firefox is used to log in to NetEco, the system displays a connection error message as shown in **Figure 6-2**.

Figure 6-1 A connection error prompted by the Chrome

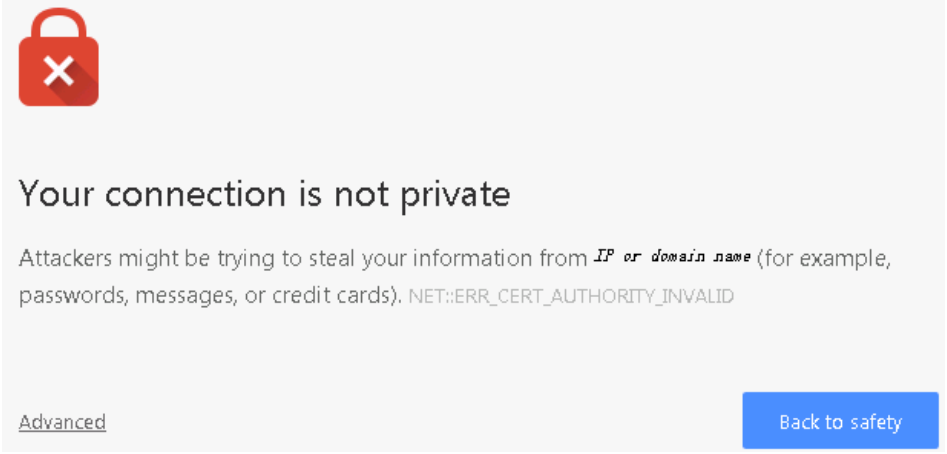
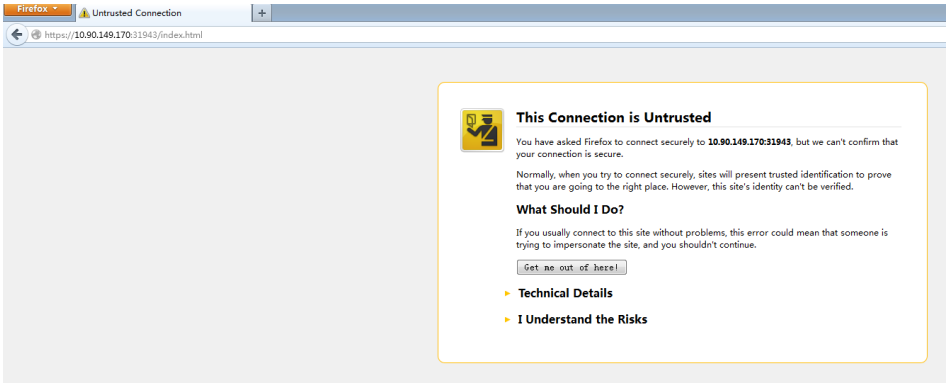


Figure 6-2 A connection error prompted by the Firefox



Procedure

NOTE

Operations on the browser may vary depending on browser versions but are similar to the examples in the following steps. You are advised to perform the operations based on actual situations.

- Install the security certificate in Google Chrome.

  Please select whether to execute the subsequent operations according to the following scenarios.

  a. Obtaining the Trust Certificate from the NetEco Server.

     Use FileZilla to download the **trust.cer** certificate file from the **/opt/oss/NetEco/etc/ssl/er** directory on the NetEco server as user **ossuser** to the local PC.

  b. Installing the Trust Certificate on the Browser:

i. Open Google Chrome and click in the upper right corner of the browser Icon Go to **Customise and control Google Chrome** Interface.

ii. Click **Settings**.

iii. Click **Show advanced settings**, Click again **Manage certificates**.

iv. Importing Steps in a Trusted Root Certification Authorities **a** Certificates that have been saved to the local computer, click **Import**.

v. Click **Next step** Browse **Selecting a certificate**.

vi. Click **Next step**.

vii. Click **Next step**.

viii. Click **Completed**.

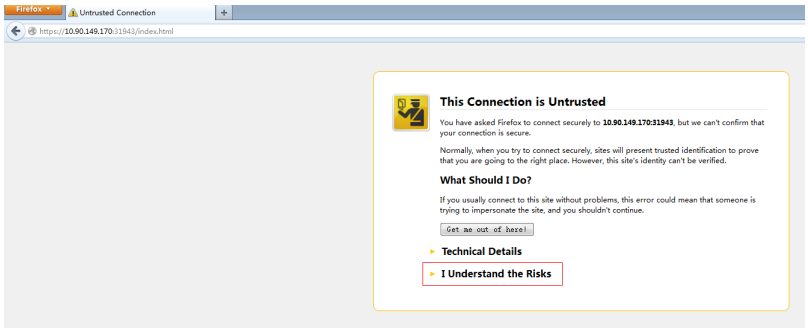
ix. The **Security Warning** dialog box is displayed. Select **Yes(Y)**.

x. Click **Yes** Restart the browser.

- Add the exception in Mozilla Firefox.

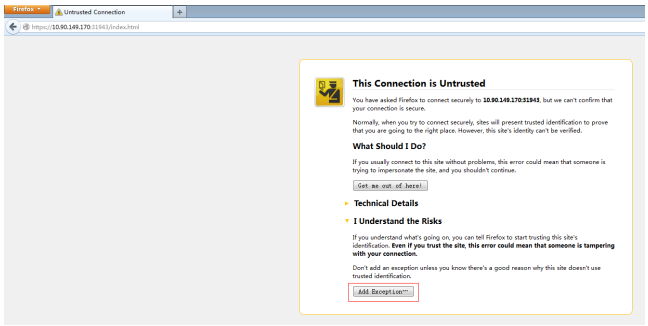
  a. Click **I Understand the Risks** as shown in **Figure 6-3**.

  Figure 6-3 Clicking I Understand the Risks

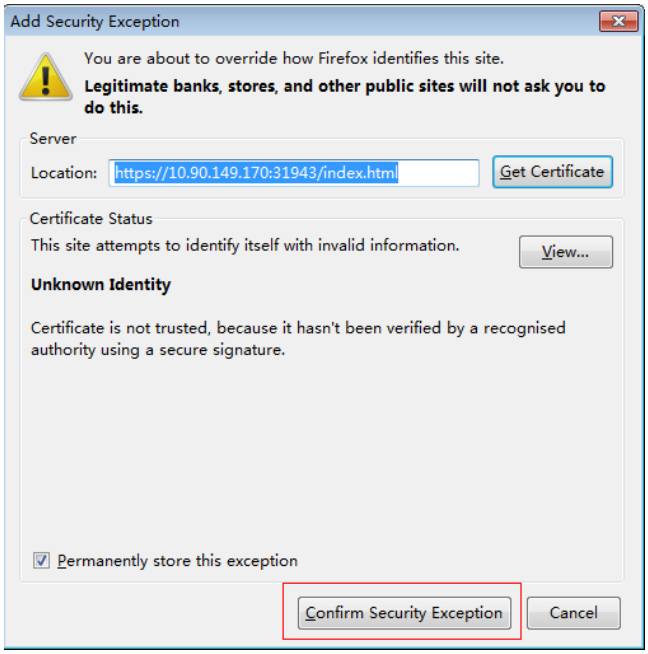
  b. In the expanded area, click **Add Exception** as shown in **Figure 6-4**.

  Figure 6-4 Adding exception.

  c. Click **Confirm Security Exception** as shown in **Figure 6-5**.

Figure 6-5 Confirming security exception



6.2 How Do I Rectify a NetEco-NE Intermittent Disconnection Alarm?

This section describes how to rectify an intermittent disconnection alarm between the NetEco and an NE.

Symptom

Intermittent disconnection occurs due to unstable links between the NetEco and NEs, triggering disconnection alarms.

Possible Cause

The preset duration for alarm masking rules is too short, leading to the fact that lots of disconnection alarms are reported.

Procedure

1. Choose **Device Management** > **Alarm Management** > **Alarm Settings**.
2. In the navigation tree on the left, choose **Masking Rule**.
3. Create an alarm masking rule, set the alarm retention time, and mask intermittent disconnection alarms.
   a. Click **+** to create a masking rule for intermittent disconnection alarms.
   b. Select **Custom alarm sources** in the alarm source area and add communication alarms to be masked in **Add Alarm Sources**.

c. Set **Duration (s)** to ≤ **600** in **Advanced Setting**.

This is to mask disconnection alarms that are automatically cleared within 10 min after their generation.

d. Click **OK** to save the alarm masking rule.

6.3 How Do I Install the Video Surveillance Subsystem Client?

This section describes how to install the video surveillance subsystem client.

Prerequisites

The network communication between the VCN/IVS1800 and the camera is normal.

Procedure

- If the video surveillance subsystem is VCN
  a. Download the VCN Client.
     i. Log in to Huawei technical support website and download the following software package. The download method is as follows:
        - For enterprise users:
          1) Log in to Huawei enterprise technical support website **https://support.huawei.com/enterprise**.
          2) Browse or search for **VCN** and select a product from the drop-down list box.
        - For carriers:
          1) Log in to Huawei technical support website **https://support.huawei.com**.
          2) Browse or search for **VCN** and select a product from the drop-down list box.
     ii. On the **Software** or **Product Software** tab page, download the software package as required.
  b. Decompress the software package, double-click the installation program, and complete the installation as prompted.
- If the video surveillance subsystem is IVS1800
  a. Download the iClient.

  You can obtain the iClient in either of the following ways:

Method 1:	Obtain the iClient installation program from the OMU portal. Log in to the OMU portal, click **Client Download**  in the upper right corner, and save the installation program to a local directory.

Method 2:	1. Log in to the OMU portal, choose **Local Configuration** > **Basic Configuration**, and view **Current version**. 2. Log in to Huawei technical support website and download the following software package. The download method is as follows: • For enterprise users: a. Log in to Huawei enterprise technical support website **https://support.huawei.com/enterprise**. b. Browse or search for **iClient**. • For carriers: a. Log in to Huawei technical support website **https://support.huawei.com**. b. Browse or search for **iClient** and select a product from the drop-down list box. 3. On the **Software** or **Product Software** tab page, click the version and patch number corresponding to the current version, and download the software package as required.

b. Decompress the software package, double-click the installation program, and complete the installation as prompted.

----End

6.4 How Do I Add a Camera on the Video Surveillance Subsystem?

Before creating a camera on the NetEco, you need to add the camera to the video surveillance subsystem.

Prerequisites

- The video surveillance subsystem and camera are powered on and connected through a switch.
- The IP addresses of the video surveillance subsystem and camera are in the same network segment.
- The video surveillance subsystem client has been installed. For details, see **6.3 How Do I Install the Video Surveillance Subsystem Client?**
- You have obtained the user name and password of a camera.

Procedure

- Adding a camera on the VCN
  a. Log in to the VCN IVS client as the **Admin** user.

NOTE

- The default **User name** is **Admin**, and **Password** is **Change_Me**. When a user logs in to the VCN IVS client for the first time, a password change dialog box is displayed, requiring the user to change the password.
- Set **Server IP address** to the IP address of the VCN.
- The default value of **Port** is **9900**. The default value is recommended.

b. In the **Quick Setup** area, double-click **Add Camera**.

c. Set search criteria.

i. Set the value of the **Drive**.

NOTE

- The default **Drive** is **ONVIF**. If an IPC6325 camera is added, select **HWSKD** for **Drive**.
- If there are multiple VCNs, set **Access server** to the VCN which the camera needs to be connected.

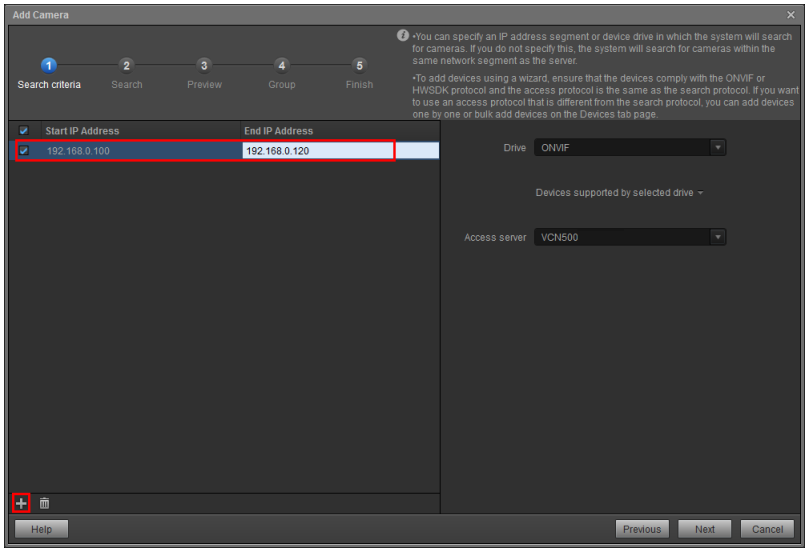
ii. Click  at the lower left corner, and enter **Start IP Addresses** and **End IP Addresses** for the camera, then click **Next**.

Set **Start IP Addresses** and **End IP Addresses** to an appropriate IP address range. If the range is too large, the search process may take a long time.

NOTE

In the scenario where smart ETH gateways are networked, the camera has an internal IP address and an external IP address, ECC800-Pro searches for the internal IP address of camera.

Figure 6-6 Setting the start and end IP addresses



d. Search for and verify the camera.

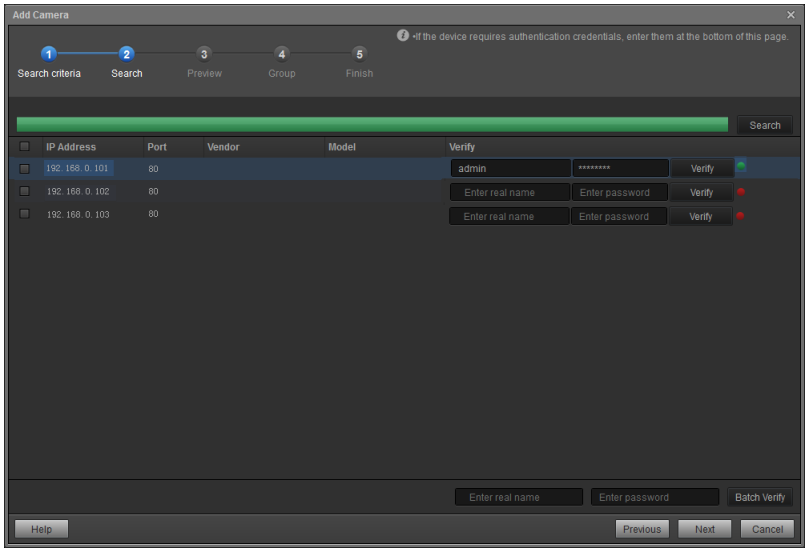
i. Click **Search**.

The system displays the IP address of the camera that is found.

ii. In the **Verify** area, enter user name and password of a camera, click **Verify**.

If the verification succeeds, the camera icon color changes to green.

Figure 6-7 Verifying the camera user name and password



NOTICE

- Cameras already added to the VCN will not be displayed on the search result page.
- Please confirm that the user name and password are correct. If you enter the incorrect password, and click **Verify** for three times, the user account will be locked.

e. Select the camera to be added, and click **Next**.

The camera preview page appears.

f. Preview the monitored area, and modify parameters such as **Camera name**, **Location**, and **Brightness** as necessary, click **Next**.

The camera grouping page appears.

g. Click **Next**.

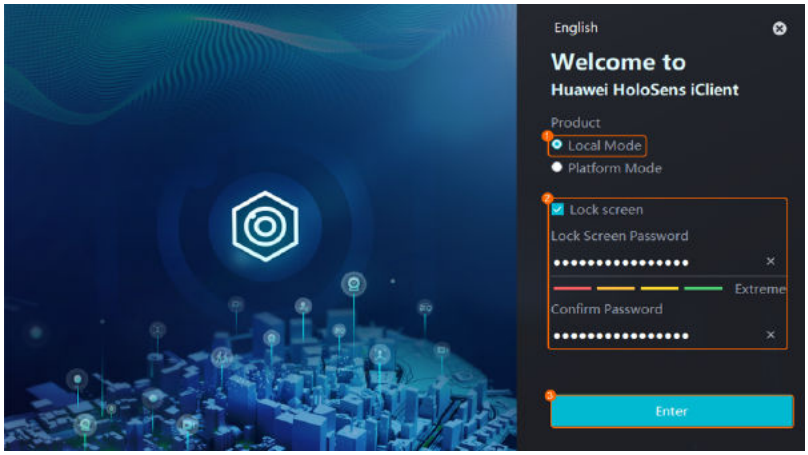
If the **Status** bar displays ., the camera is successfully added.

h. Click **Finish**.

- Adding a camera on the IVS1800

a. Log in to the iClient client as the **administrator** user.

Figure 6-8 Logging in to the iClient



b. On the home page of the iClient, choose **System Management > DeviceManagement > Device Management > Micro Edge**.

c. Right-click an IVS1800 and choose **Camera Access**.

d. Select **Auto Batch Access** and click **Start**.

e. Set the IP address segment.

Figure 6-9 Setting an IP network segment

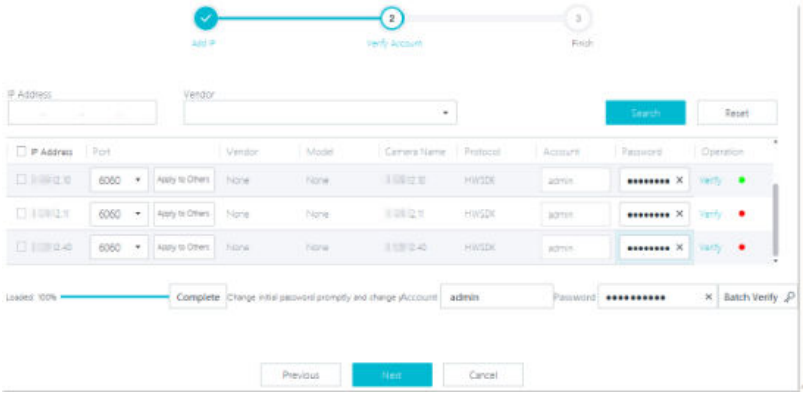
NOTE

- The driver protocol of IPC6325 and C3220 cameras is HWSDK.
- The IP address segment indicates the start and end IP addresses of cameras.

f. You can use **IP Address** and **Vendor** to filter the required cameras in thecamera search result and select the required cameras. Alternatively,

you can directly select the required cameras in the camera list. Then verify accounts.The default password of the HWSDK protocol is **HuaWei123**.

Figure 6-10 Verifying accounts



NOTE

If there are multiple IVS1800s for multiple smart modules, you are advised to evenly distribute the cameras to each IVS1800.

g. Select the cameras to be added and click **Next**.

h. Click **Finish**.

i. Preview live video. On the iClient home page, click **Live** and drag a camera to the live video pane. If the live video can be properly played, the camera is successfully connected.

----End

6.5 How Do I Set Video Playback Parameters on the Video Surveillance Subsystem?

A camera can play videos only after video playback parameters are set on the video surveillance subsystem.

Prerequisites

You have installed and logged in to the video surveillance subsystem client.

Procedure

- If the video surveillance subsystem is VCN
  a. On the home page, choose **Maintenance** > **Unified Configuration**.
  b. In the **System Domain List** area, select an object, set **Module Name** to **MU**, and click **Query**.
  c. In the **Parameters** area, click **Edit** next to **IsConstantUrl** and set the parameter value to **1**.
- If the video surveillance subsystem is IVS1800

a. On the home page, choose **Maintenance**.
b. In the navigation pane on the left, choose **Unified Configuration**, set **Module Name** to **MU**, and click **Search**.
c. In the **Parameters** area, click **Edit** next to **IsConstantUrl** and set the parameter value to **1**.

----End

6.6 How Do I Enable or Disable the Message Push Function

You can enable or disable the real-time alarm notification function as required.

Prerequisites

You have logged in to the NetEco app.

Procedure

Step 1 Enable or disable the **Push notifications** function as required.

Table 6-1 Setting the **Push notifications** function

Operation	Description	Procedure
Enabling the **Push notifications** function	If the **Push notifications** function is disabled and you need to view the real-time alarm information pushed by the NetEco app on the mobile phone, perform this operation.	• Method 1 1. When the system displays a message asking you whether to enable the **Push notifications** function, tap **OK**. 2. Follow the onscreen instructions to enable the **Push notifications** function. • Method 2 1. On the home screen of the NetEco app, tap **Me**. 2. On the **Me** screen, tap **Push notifications**. 3. Follow the onscreen instructions to enable the **Push notifications** function. **NOTE** If a Huawei mobile phone is used, the **Push notifications** function is enabled for the NetEco app by default.

Operation	Description	Procedure
Disabling the **Push notifications** function	If you do not need to view the real-time alarms pushed by the NetEco app on a mobile phone, perform this operation.	• Method 1 When the system displays a message asking you whether to enable the **Push notifications** function, tap **Cancel**. • Method 2 1. On the home screen of the NetEco app, tap **Me**. 2. On the **Me** screen, tap **Push notifications**. 3. Follow the onscreen instructions to disable the **Push notifications** function.

Table 6-2 Obtaining addresses involved in the **Push notifications** function online

Address	Description
https://oauth-login.cloud.huawei.com	Huawei access token address
https://push-api.cloud.huawei.com	Push message address

----End