Elevator Controller

User's Manual

V1.0.0

Foreword

General

This manual introduces the functions and operations of the Elevator Controller (hereinafter referred to as the Device or the Elevator Controller). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	August 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or

visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Elevator Controller, hazard prevention, and prevention of property damage. Read carefully before using the Elevator Controller, and comply with the guidelines when using it.

Transportation Requirement

Transport, use and store the Elevator Controller under allowed humidity and temperature conditions.

Storage Requirement

Store the Elevator Controller under allowed humidity and temperature conditions.

Installation Requirements

- Do not connect the power adapter to the Elevator Controller while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Elevator Controller.
- Do not connect the Elevator Controller to two or more kinds of power supplies, to avoid damage to the Elevator Controller.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the Elevator Controller.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the Elevator Controller.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the Elevator Controller label.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Elevator Controller in a place exposed to sunlight or near heat sources.
- Keep the Elevator Controller away from dampness, dust, and soot.
- Install the Elevator Controller on a stable surface to prevent it from falling.

- Install the Elevator Controller in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The Elevator Controller is a class I electrical appliance. Make sure that the power supply of the Elevator Controller is connected to a power socket with protective earthing.

Operation Requirements

- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the Elevator Controller while the adapter is powered on.
- Operate the Elevator Controller within the rated range of power input and output.
- Use the Elevator Controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Elevator Controller, and make sure that there is no object filled with liquid on the Elevator Controller to prevent liquid from flowing into it.
- Do not disassemble the Elevator Controller without professional instruction.
- This product is professional equipment.
- The Elevator Controller is not suitable for use in locations where children are likely to be present.

Table of Contents

1 Overview

The Elevator Controller supports the platform mode and the standalone mode. Different people can have different access permissions to the elevator through the configurations on the DSS Pro or the Elevator Controller.

You can only change the mode during the initialization. If you want to change the mode while using the Device, you need to restore it to the factory default settings, and then select the mode during the initialization. Please be advised.

Platform Mode

If you select the platform mode, add and manage person on DSS Pro. Configure the time template, floor permissions on DSS Pro. For details, see *DSS User's Manual*.

Standalone Mode

If you select the standalone mode, add and manage person on the Elevator Controller. Configure the time template, floor permissions on the Elevator Controller. For details, see "2.4.4 Adding Users".

2 Webpage Operations

2.1 Initialization

Initialize the Elevator Controller when you log in to the webpage for the first time or after it is restored to its factory defaults.

Prerequisites

Make sure that the computer used to log in to the webpage is on the same LAN as the elevator controller.

Procedure

Step 1 Open a browser, go to the IP address (the IP address is 192.168.1.108 by default) of the elevator controller.

We recommend you use the latest version of Chrome or Firefox.

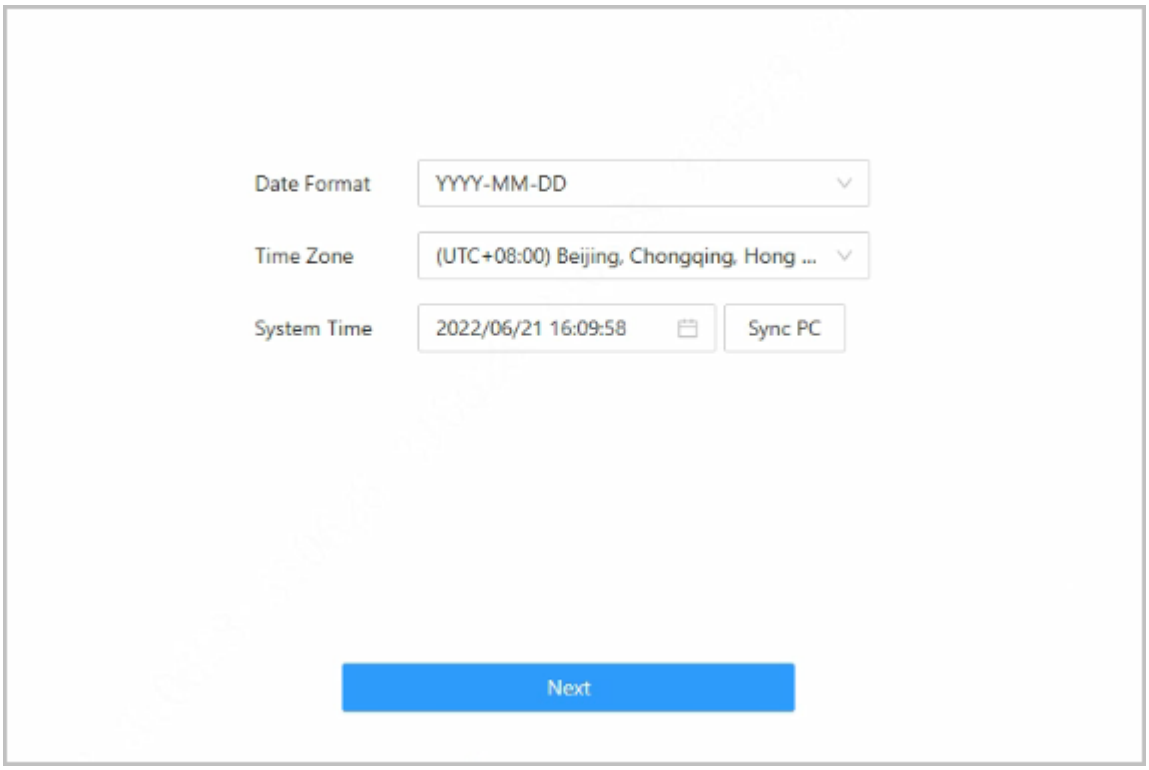
Step 2 Select a language, and then click **Next**.

Step 3 If there are the software license agreement and privacy policy, read them carefully, select **I have read and agree to the terms of the Software License Agreement and Privacy Policy.** , and then click **Next**.

The software license agreement and privacy policy are available on select models.

Step 4 Configure the system time, and then click **Next**.

Figure 2-1 Configure the time



Step 5 Set the password and email address.

- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case and lower case letters, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.

Step 6 (Optional) Select **Auto Check for Updates** , and then click **Completed**.

The system automatically checks that if there is any higher version available, and informs the user to update the system.

Step 7 Click **Completed**.

The system automatically goes to the login page after initialization is successful.

2.2 Logging in

For first-time login after the initialization, you need to configure the mode. The elevator controller supports the platform mode and the standalone mode.

Procedure

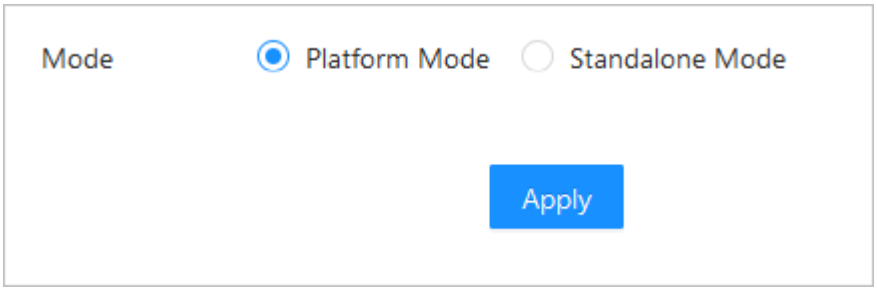
Step 1 On the login page, enter the username and password.

- The default administrator name is admin, and the password is the one you set during initialization. We recommend you change the administrator password regularly to increase the security of the platform.
- If you forget the administrator login password, you can click **Forgot password?**.

Step 2 Select the mode, and then click **Apply**.

- Platform mode: The platform sends the people information, the time template and the floor permissions.
- Standalone mode: Manage the people information, configure the time template and the floor on the Elevator Controller.

Figure 2-2 Select the mode



2.3 Resetting the Password

Reset the password through the linked e-mail when you forget the admin password.

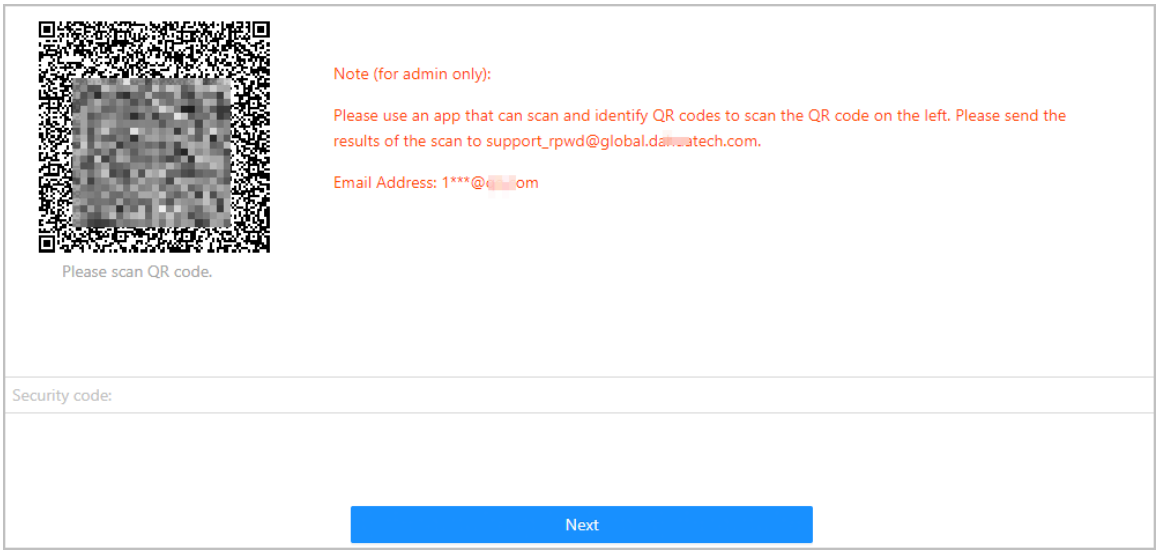
Procedure

Step 1 On the login page, click **Forgot password**.

Step 2 Read the on-screen prompt carefully, and then click **OK**.

Step 3 Scan the QR code, and you will receive a security code.

Figure 2-3 Reset password



- Up to two security codes will be generated when the same QR code is scanned. If the security code becomes invalid, refresh the QR code and scan again.
- After you scan the QR code, you will receive a security code in your linked e-mail address. Use the security code within 24 hours after you receive it. Otherwise, it will become invalid.
- If the wrong security code is entered 5 times in a row, the administrator account will be frozen for 5 minutes.

Step 4 Enter the security code.

Step 5 Click **Next**.

Step 6 Reset and confirm the password.

The password should consist of 8 to 32 non-blank characters and contain at least two of the following types of characters: upper case, lower case, number, and special character (excluding ' " ; : &).

Step 7 Click **OK**.

2.4 Local Device Configurations

After logging in, the **Local Device Config** page is displayed. Configure the time plan, alarm linkage, network and other basic parameters.

The parameters may differ according to the selected mode.

2.4.1 Configuring Module

We recommend you use one elevator controller for one elevator.

2.4.1.1 Configuring Elevator Control Module

You can add the elevator control module to the elevator controller.

Prerequisites

Before adding the module, make sure that the elevator controller and the elevator control module are in the same network and can be connected through the network.

Procedure

Step 1 On the home page, select **Elevator Control Module** > **Elevator Control Module**.

Step 2 Click , and then configure the module.

Figure 2-4 Elevator control module

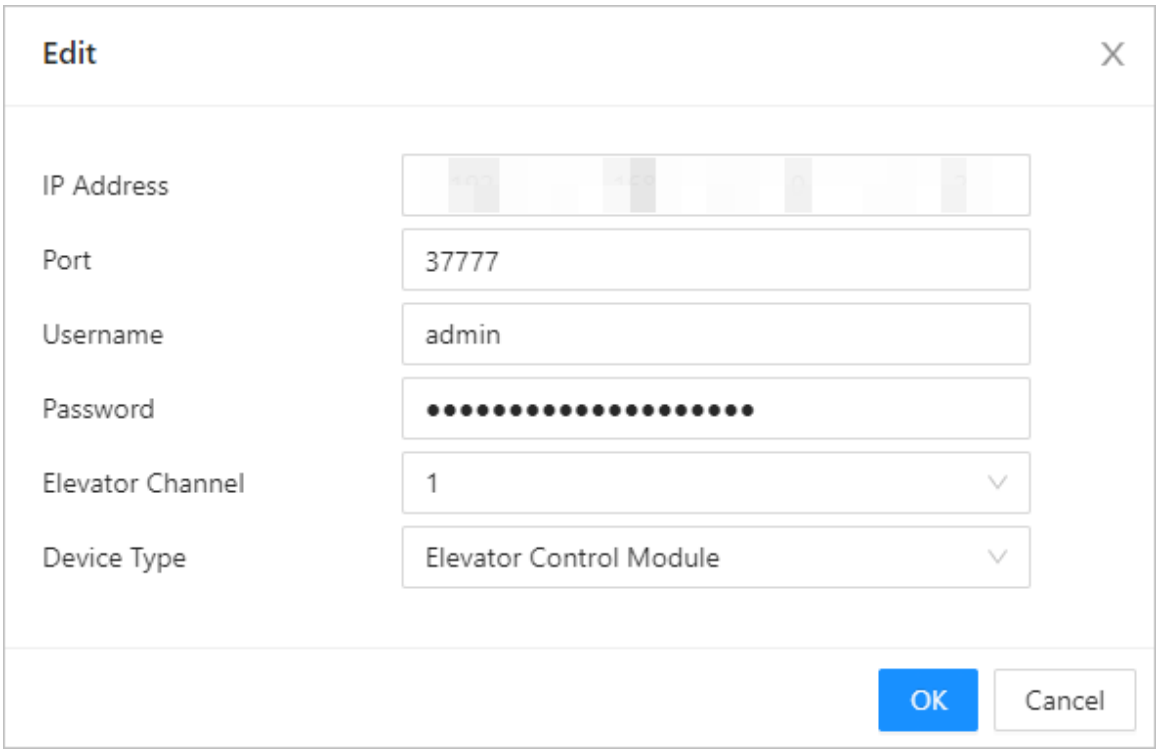


Table 2-1 Device parameters description

Parameter	Description
IP Address	Enter the IP address of the elevator control module.
Port	The port number is 37777 by default.
Username/Password	Enter the username and password of the elevator control module.
Elevator Channel	Select from **1** and **2**.
Device Type	Select from **Elevator Control Module** and **Elevator Call Module**.

Step 3 Click **OK**.

2.4.1.2 Configuring Elevator Control Parameters

Configure basic parameters for the elevator channel 1 and channel 2.

On the home page, select **Elevator Control Module** > **Elevator Control Config**. Configure the parameters, and then click **Apply**.

Figure 2-5 Elevator control configuration

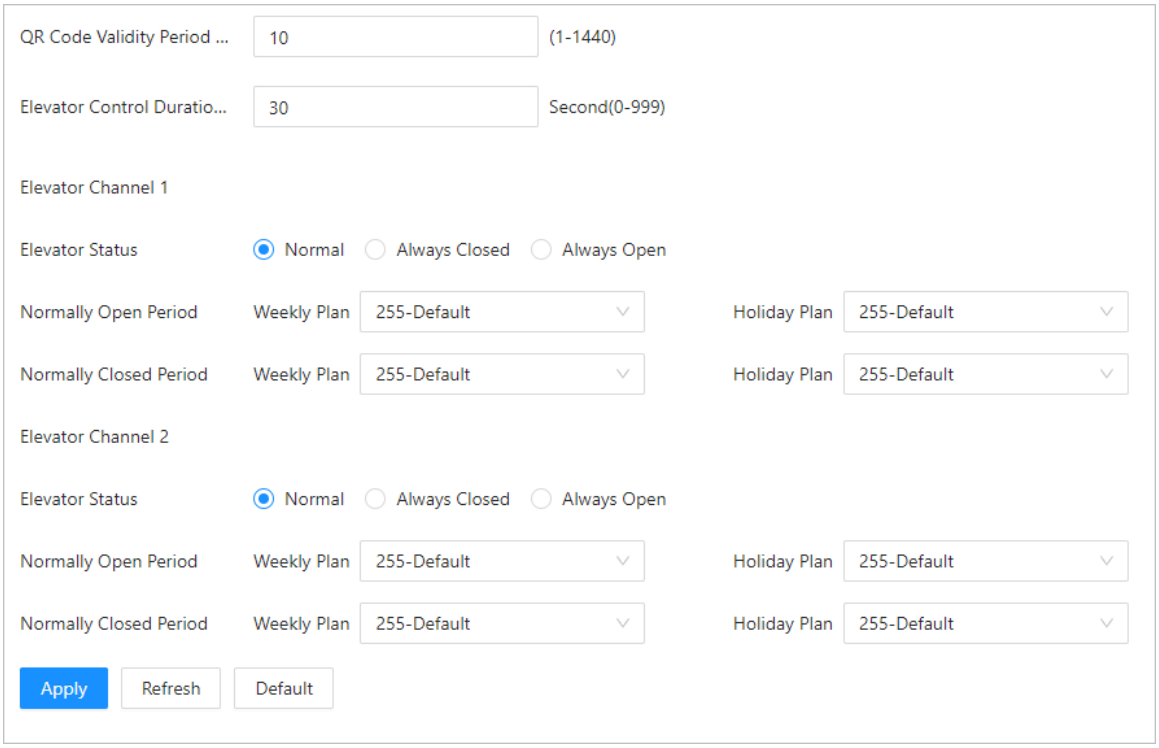


Table 2-2 Description of elevator control parameters

Parameter		Description
QR Code Validity Period (min)		Configure the validity period for the QR code that is generated for the host. Hosts can access to the elevator using the QR code within the configured period.
Elevator Control Duration		Configure the elevator control duration. It is 10 seconds by default. The value ranges from 0 second to 999 seconds.
Elevator Channel 1/Elevator Channel 2	Elevator Status	Configure the elevator status for the elevator channel 1 or elevator channel 2. ● Normal: Authentication mode. After configuring weekly plan and holiday plan, the elevator can be accessed within the configured period. The holiday plan has the priority over the weekly plan. ● Always closed: The elevator is not running. ● Always open: You can access to the elevator without verification.

Parameter		Description
	Normally Open Period	If you select **Normal** as the elevator status, configure the normally open period for weekly pan and holiday plan. The elevator can be accessed within the configured period. The holiday plan has the priority over the weekly plan. Normally open period has priority over the normally closed period. For example, if you select the same weekly plan for normally open period and the normally closed period, during the period, the elevator normally opens.
	Normally Closed Period	If you select **Normal** as the elevator status, configure the normally closed period for weekly plan and holiday plan. The elevator cannot be accessed within the configured period. The holiday plan has the priority over the weekly plan.

2.4.1.3 Configuring Floor Name

Procedure

Step 1 On the home page, select **Elevator Control Module** > **Floor Config**.

Step 2 Add the floor.

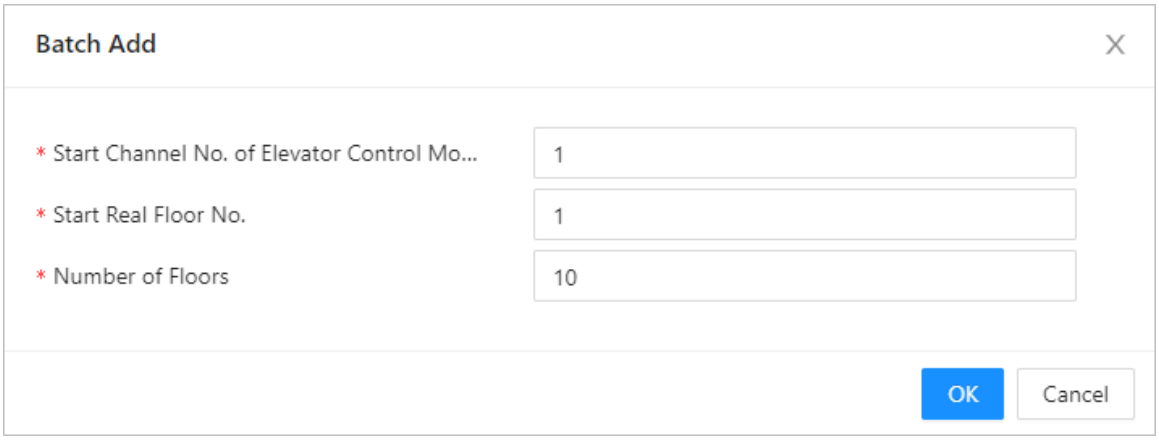
You can add up to 128 elevator control module channels.

- Click **Add**, and then enter the elevator control module channel number and the real floor name.

Figure 2-6 Add the floor

- Click **Batch Add**, and then enter the start channel number of the elevator control module, the start real floor number and the number of floors.

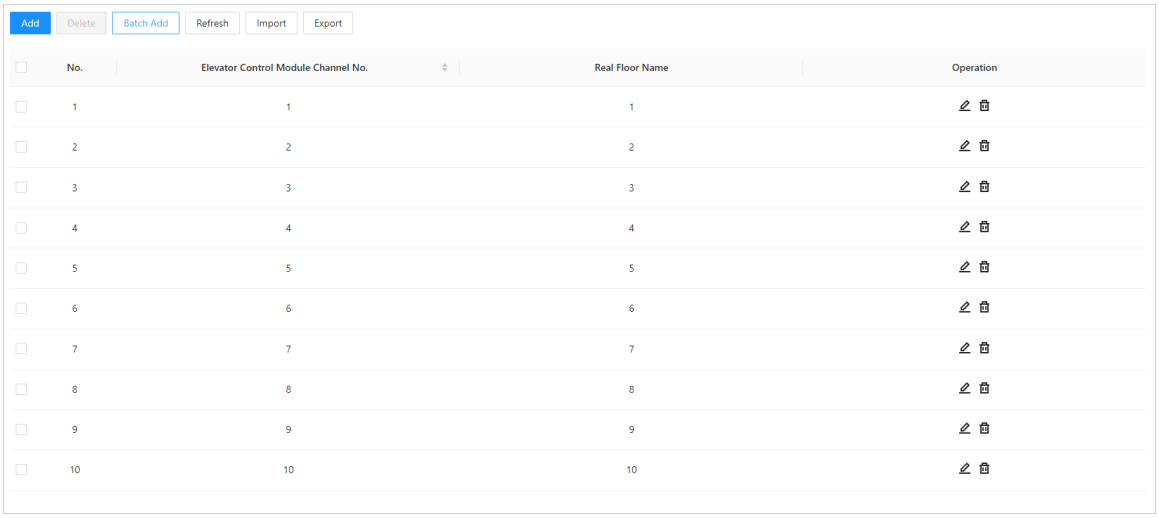
Figure 2-7 Add the floor in batches



Step 3 Click **OK**.

View the floor number and the real floor name in the list. Click the channel number of the elevator control module to sort in ascending or descending order.

Figure 2-8 Floor list



2.4.2 Adding Weekly Plans

The weekly plan is used to set the elevator control schedule for the week. You can also create your own templates.

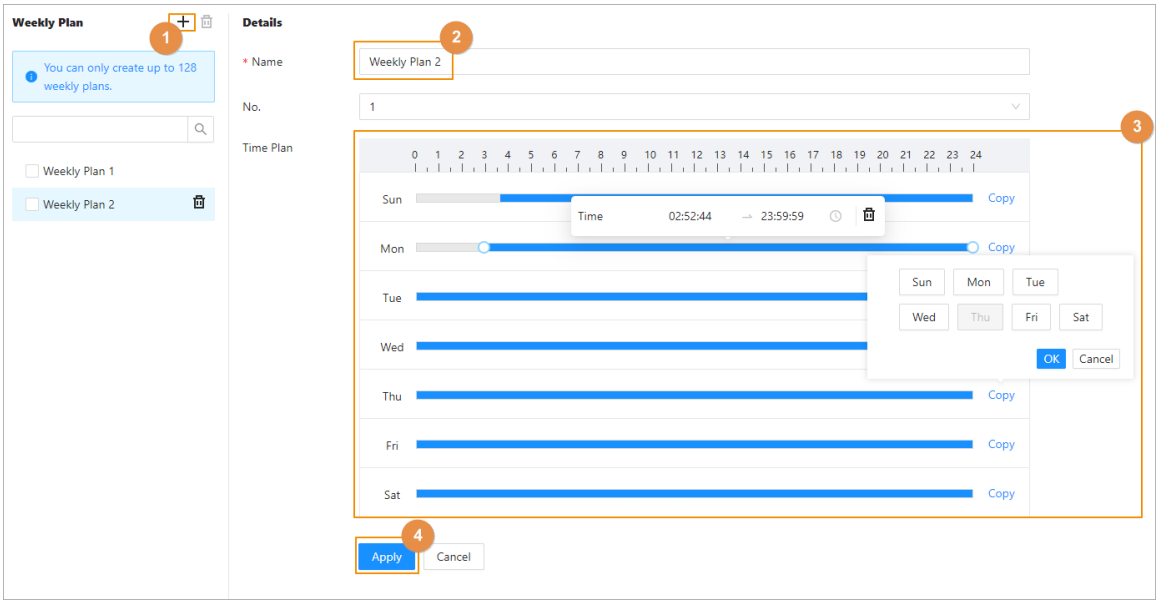
Procedure

Step 1 On the home page, select **Weekly Plan**, and then click +.

You can create up to 128 weekly plans.

Step 2 Enter the name of the time template.

Figure 2-9 Create the weekly plan



Step 3 Drag the slider to adjust the time period for each day.

You can also click **Copy** to apply the configured time period to other days.

You can only configure up to 4 time sections for each day.

Step 4 Click **Apply**.

2.4.3 Adding Holiday Plans

This function is only available for the standalone mode.

Procedure

Step 1 On the home page, select **Holiday Plan** , and then click **+**.

You can create up to 128 holiday plans.

Step 2 Enter the name of the time template.

Step 3 Select the time period.

You can also click to apply the configured time period to other plans.

Step 4 Click **Apply**.

2.4.4 Adding Users

Procedure

Step 1 On the home page, select **Person Management**.

Step 2 Add users.

- Add users one by one.

1. Click **Add**, and then enter the basic information on the user.

Figure 2-10 Basic information on the user

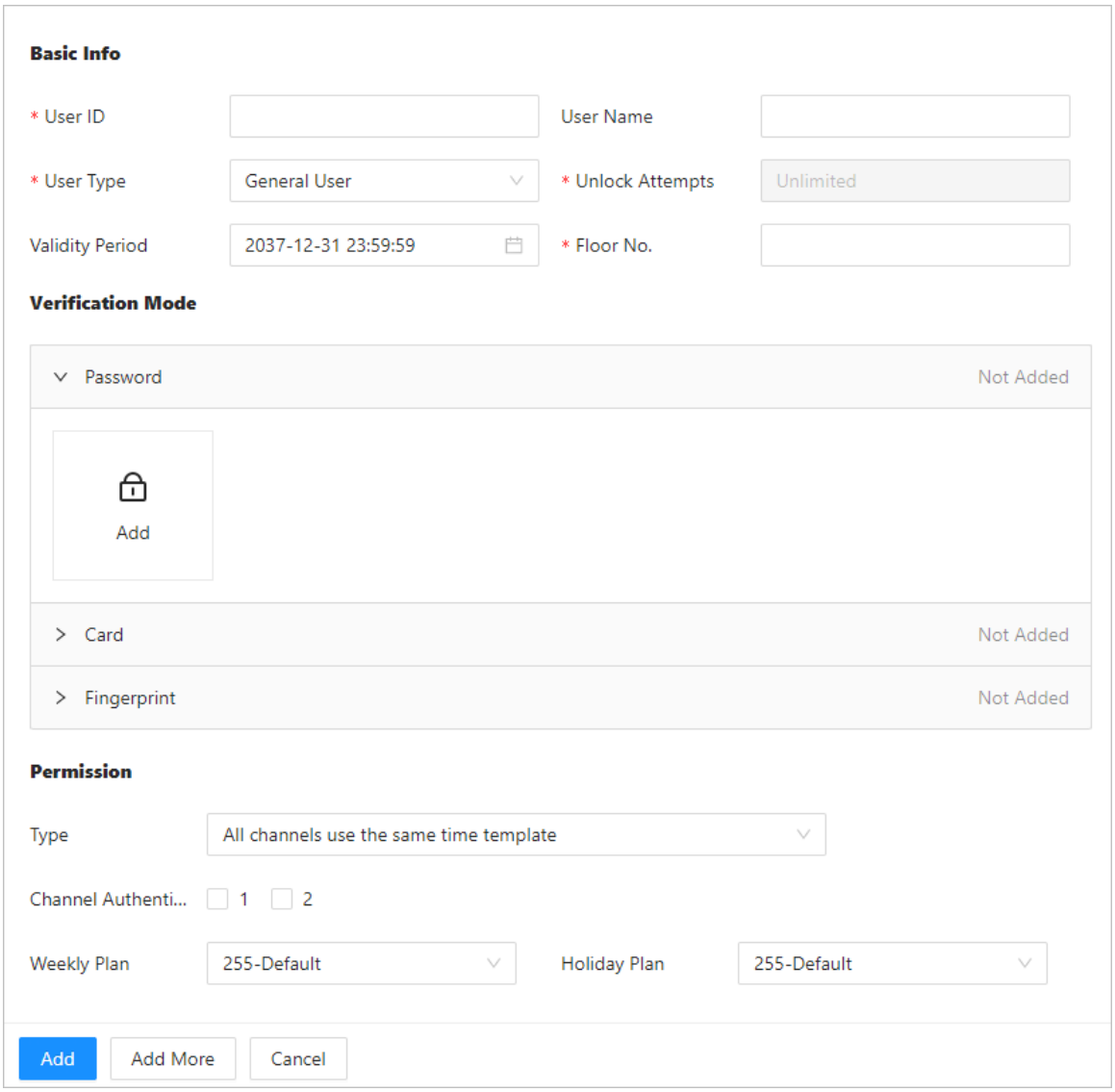


Table 2-3 Parameters description

Parameter	Description
User ID	The ID of the user.
User Name	Enter the name of the user.
User Type	◇ **General User** , **VIP User**, **Patrol User**, **Other User**, and **Custom User 1/Custom User 2**: Can access floors that they were granted permission for within the configured validity period. ◇ **Guest User** : Can access floors within a defined period or for a set number of times. After the period expires or they reach the limit for the number of accessing to the elevator, they cannot access the floor anymore. ◇ **Blocklist User** : The users in the blocklist cannot access floors.

Parameter	Description
Unlock Attempts	The number of times a guest user can access floors. This parameter can be configured when the user type is **Guest User**.
Validity Period	Set a date on which the access permissions of the person will become effective.
Floor No.	Select the floors, and the person has access to the selected floors. If there is no floor to be selected, please configure the floors first.

2. Configure the verification method for the user.

   Add password, cards, or fingerprints to users, so that users can access floors through authentication. Each user can have up to 1 password, 5 IC/ID cards and 3 fingerprints.

Figure 2-11 Add the password (example)

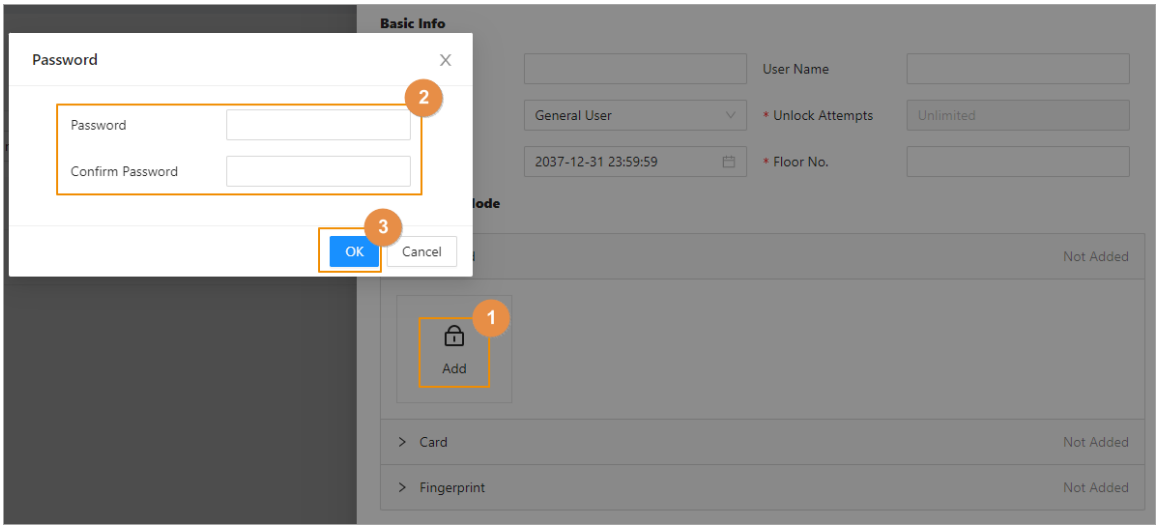


Table 2-4 Parameters description

Parameter	Description
Password	a. Click **Add**. b. Enter and confirm the password. The password must include 6 numbers. The length of user ID and password should not exceed 18. c. Click **OK**. People can access floors by entering ***user ID#Password#*** on face recognition access controller, door station or card reader. For example, the user ID is 2, and the password is 123456. You can enter 2#123456# to be recognized and access floors in the elevator.
Card	a. Click **Add**. b. Swipe the card or enter the card number to add the card. ◇ Click **Modify** to select the card reader device that connecter to the Elevator Controller or the USB scanner that connected to the computer, and then swipe the card on the corresponding device. The card number will be displayed on the platform. ◇ Enter the card number. c. Click **Add**. ◇ : Change the number of the card. ◇ : Set the card to duress card. An alarm is triggered when people use the duress card to unlock the door. ◇ : Delete the card.
Fingerprint	a. Click **Add**. b. Follow the on-screen instructions to register the fingerprint. Click **Modify** to select the card reader device that is connected to the elevator controller or the USB scanner that connected to the computer, and then register the fingerprint on the corresponding device according to the instructions. c. Click **Add**.

3. Configure the permission for the user.

   Select the type that whether all the channels use the same template, select channel authentication, and then select the weekly plan and the holiday plan.
4. Click **Add**.

   You can click **Add More** to add more users.

- Add users through importing the template.
  1. Click **Import** > **Download Template** to download the user template.
  2. Enter user information in the template, and then save it.

3. Click **Import**, and upload the template to the Elevator Controller.

   The users are added to the Elevator Controller automatically.

2.4.5 Configuring Alarm Linkages

You can configure alarm linkages.

Procedure

Step 1 On the home page, select **Local Alarm Linkage**.

Step 2 Click to configure alarm.

Figure 2-12 Alarm linkage

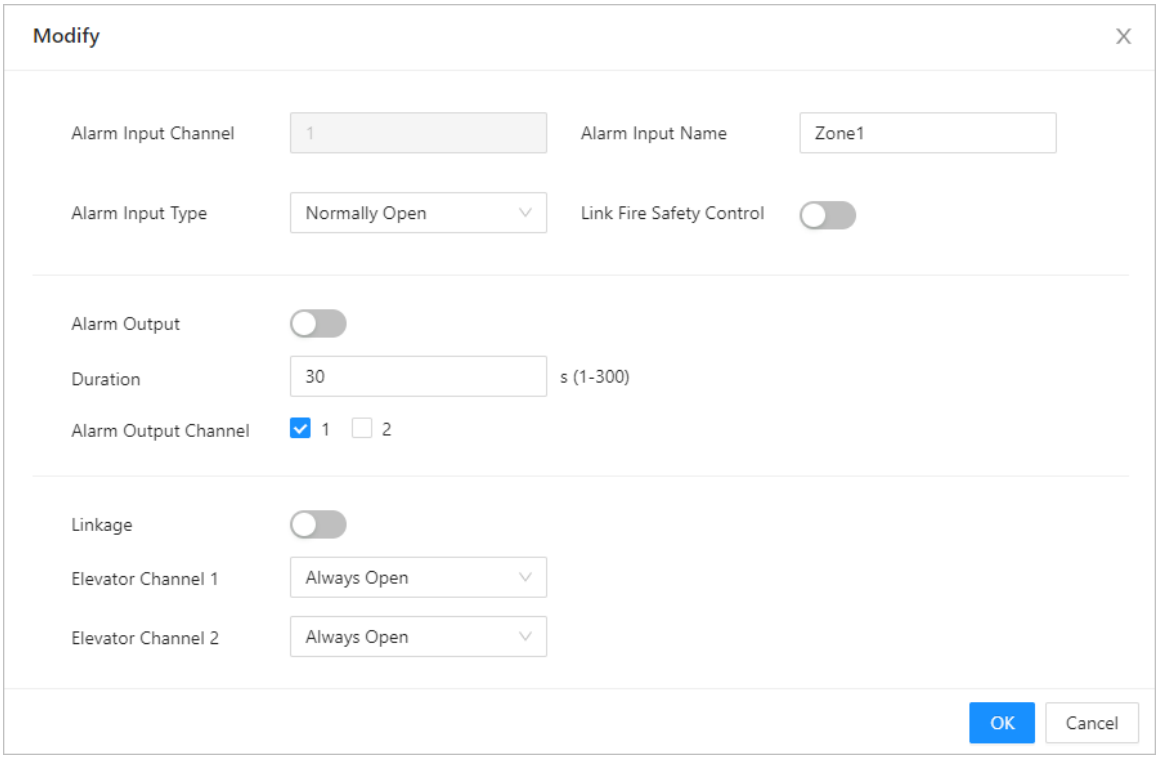


Table 2-5 Description of alarm linkage parameters

Parameter	Description
Alarm Input Channel	The number of the alarm input channel. Each elevator controller has 2 alarm inputs and 2 alarm outputs.
Alarm Input Name	The name of the alarm input.
Alarm Input Type	The type of the alarm input. • **Normally Closed** • **Normally Open**

Parameter	Description
Link Fire Safety Control	After the function is enabled, when the fire alarm is triggered, the Device links alarm output and elevator channels. If the function is enabled, the alarm-out port and elevator channels linkage are enabled by default.
Alarm Output	After the function is enabled, when the alarm is triggered, the alarm information will be sent. Configure the duration and select the alarm out channel according to the actual situation.
Duration	
Alarm Output Channel	
Linkage	After the function is enabled, if there is alarm signal input, the Device links to the elevator channel of always open or always closed.
Elevator Channel 1	• Always open: You can access to the elevator without verification. • Always closed: The elevator is not running.
Elevator Channel 2	

Step 3 Click **OK**.

2.4.6 Viewing System Logs

View and search for system logs.

Procedure

Step 1 On the home page, Select **System Logs**.

Step 2 Select the time range and the log type, and then click  .

Related Operations

- Click **Export** to export the searched logs to your local computer.
- Click **Encrypt Log Backup**, and then enter a password. The exported file can be opened only after entering the password.
- Click  to view details of a log.

2.4.7 Network Settings

2.4.7.1 Configuring TCP/IP

You need to configure IP address of Device to make sure that it can communicate with other devices.

Procedure

Step 1 On the home page, select **Network Settings** > **TCP/IP**.

Step 2 Configure the parameters.

Figure 2-13 TCP/IP

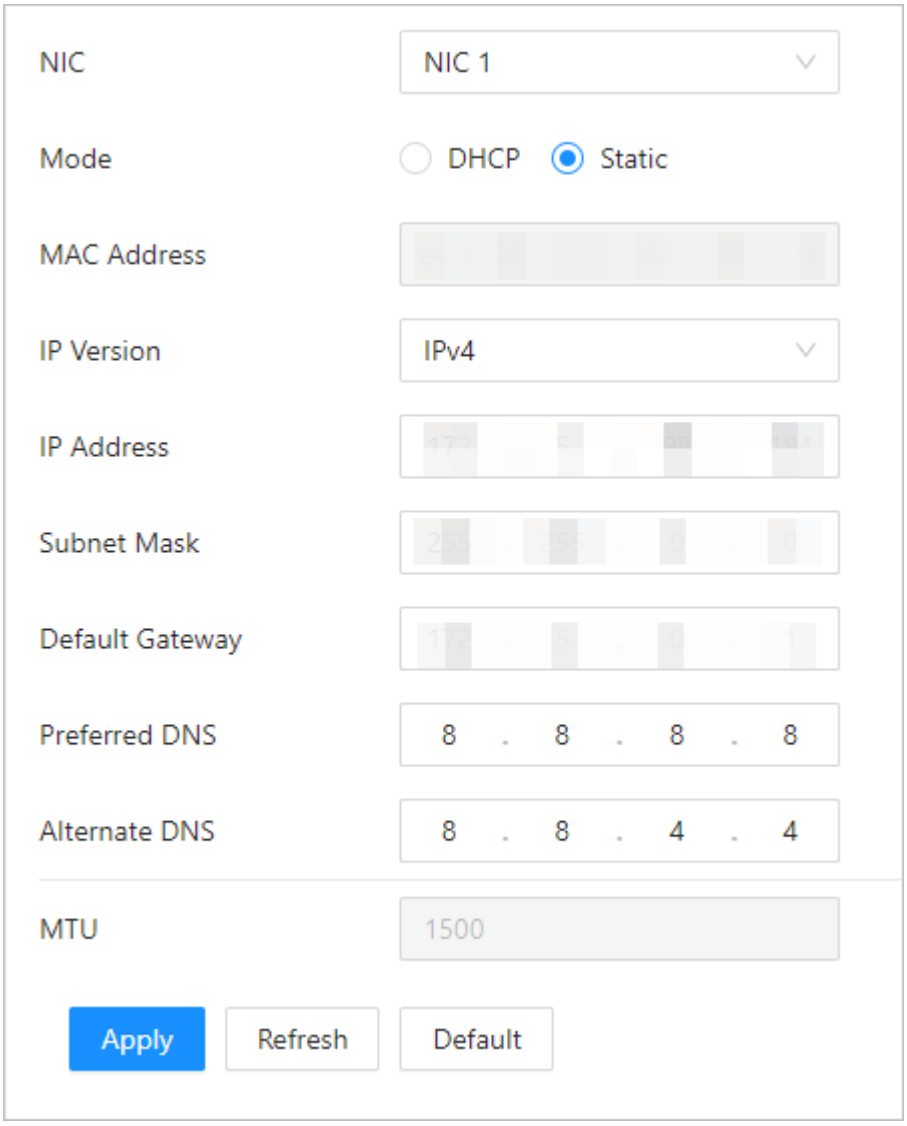


Table 2-6 Description of TCP/IP

Parameter	Description
Mode	• Static: Manually enter IP address, subnet mask, and gateway. • DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.

Parameter	Description
IP Address	If you set the mode to **Static**, configure the IP address, subnet mask and gateway.  • IPv6 address is represented in hexadecimal. • IPv6 version do not require setting subnet masks. • The IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
MTU	MTU (Maximum Transmission Unit) refers to the maximum size of data that can be transmitted in a single network packet in computer networks. A larger MTU value can improve network transmission efficiency by reducing the number of packets and associated network overhead. If a device along the network path is unable to handle packets of a specific size, it can result in packet fragmentation or transmission errors. In Ethernet networks, the common MTU value is 1500 bytes. However, in certain cases such as using PPPoE or VPN, smaller MTU values may be required to accommodate the requirements of specific network protocols or services. The following are recommended MTU values for reference: • 1500: Maximum value for Ethernet packets, also the default value. This is a typical setting for network connections without PPPoE and VPN, some routers, network adapters, and switches. • 1492: Optimal value for PPPoE • 1468: Optimal value for DHCP. • 1450: Optimal value for VPN.

Step 3 Click **Apply**.

2.4.7.2 Configuring Port

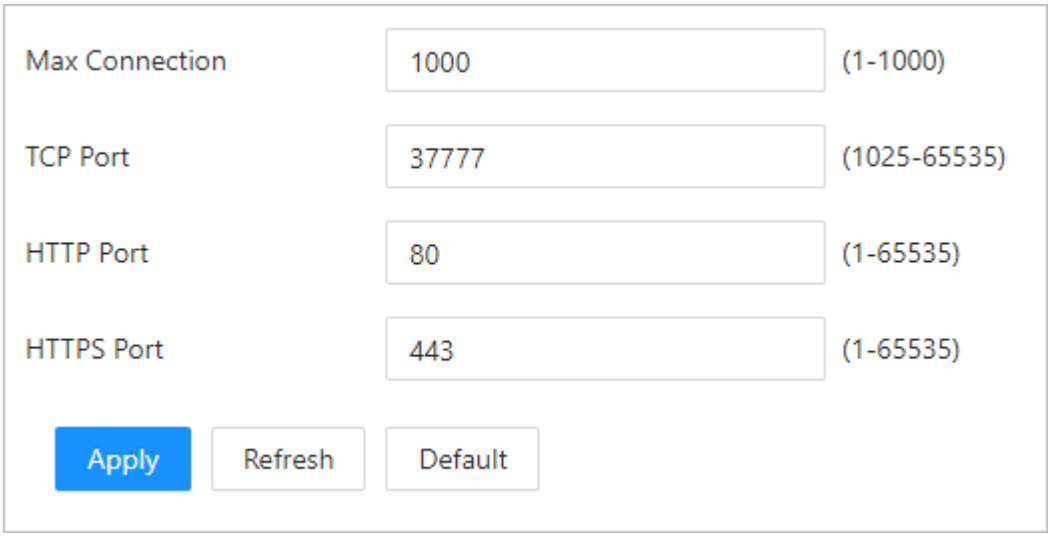
You can limit access to the Device at the same time through webpage, desktop client and mobile client.

Procedure

Step 1 On the home page, select **Network Settings** > **Port**.

Step 2 Configure the ports.

Figure 2-14 Configure ports



- Except for **Max Connection** and **RTSP Port**, you need to restart the Device to make the configurations effective after you change other parameters.
- Make sure the port is unique.

Table 2-7 Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients (such as webpage, desktop client and mobile client) that can access the Device at the same time.
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If you have changed the port number, add the port number after the IP address when access the webpage.
HTTPS Port	Default value is 443.

Step 3 Click **Apply**.

2.4.7.3 Configuring Auto Registration

The auto registration enables the devices to be added to the management platform without manual input of device information such as IP address and port.

Background Information

The auto registration only supports SDK.

Procedure

Step 1 On the home page, select **Network Setting** > **Auto Registration**.

Step 2 Enable the auto registration function and configure the parameters.

Figure 2-15 Auto Registration

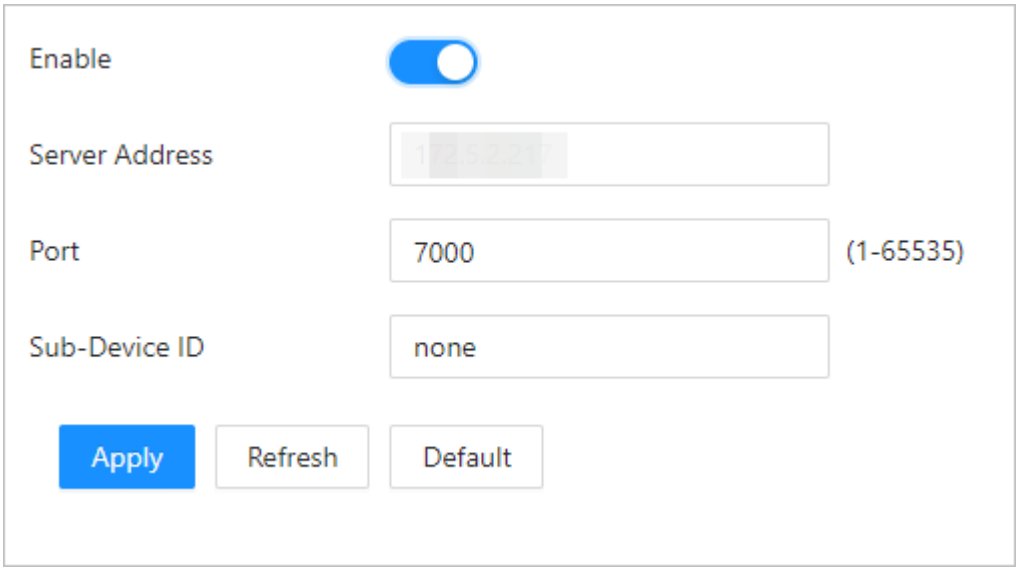


Table 2-8 Automatic registration description

Parameter	Description
Server Address	The IP address or the domain name of the server.
Port	The port of the server that is used for automatic registration.
Sub-Device ID	The ID (user defined) of the device. Adding the device to the management by entering the sub-device ID on the platform. Make sure the ID is unique.

Step 3 Click **Apply**.

2.4.7.4 Configuring Basic Service

When you want to connect the Device to a third-party platform, turn on the CGI and ONVIF functions.

Procedure

Step 1 On the home page, select **Network Settings** > **Basic Services**.

Step 2 Configure the basic service.

Figure 2-16 Basic service

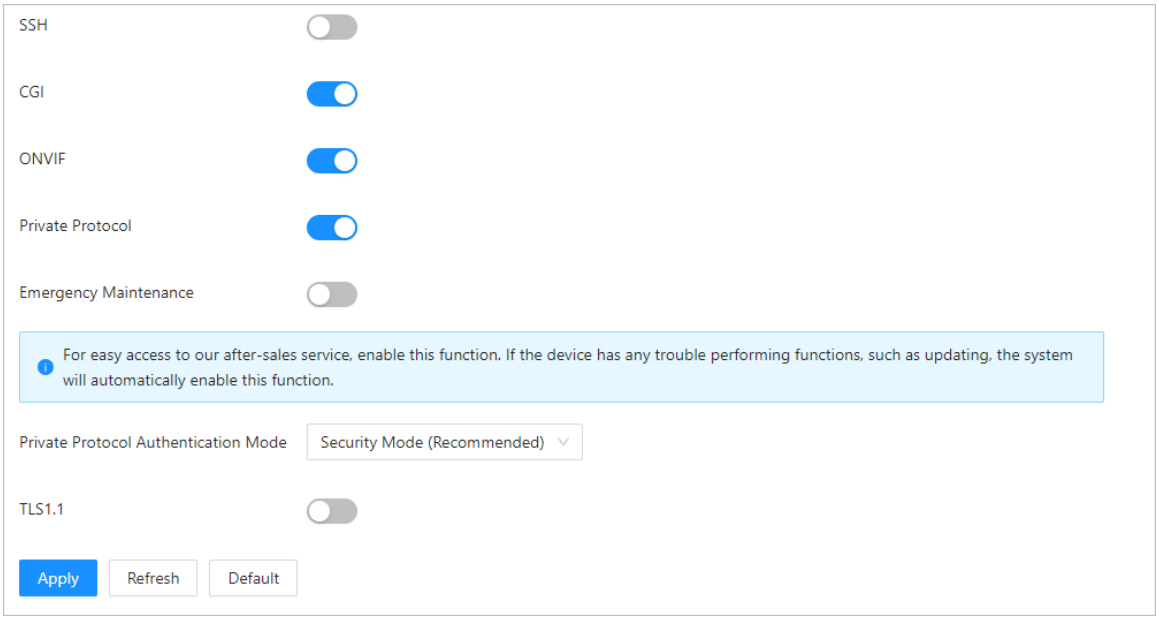


Table 2-9 Basic service parameter description

Parameter	Description
SSH	After the function is enabled, you can access the Device through SSH.
CGI	The Common Gateway Interface (CGI) is an intersection between web servers through which the standardized data exchange between external applications and servers is possible.
ONVIF	ONVIF stands for Open Network Video Interface Forum. Its aim is to provide a standard for the interface between different IP-based security devices. These standardized ONVIF specifications are like a common language that all devices can use to communicate.
Private Protocol	The platform adds devices through private protocol.
Emergency Maintenance	For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.
Private Protocol Authentication Mode	Set the authentication mode, including safe mode and compatibility mode. It is recommended to choose **Security Mode**. ● Security Mode (recommended): Does not support accessing the device through Digest, DES, and plaintext authentication methods, improving device security. ● Compatible Mode: Supports accessing the device through Digest, DES, and plaintext authentication methods, with reduced security.

Parameter	Description
TLS1.1	TLS1.1 refers to Transport Layer Security version 1.1. TLS is a cryptographic protocol designed to provide secure and authenticated communication over a computer network.  Security risks might present when TLSv1.1 is enabled. Please be advised.

Step 3 Click **Apply**.

2.4.8 Configuring Time

Procedure

Step 1 On the home page, select **System** > **Time**.

Step 2 Configure the time of the Platform.

Figure 2-17 Date settings

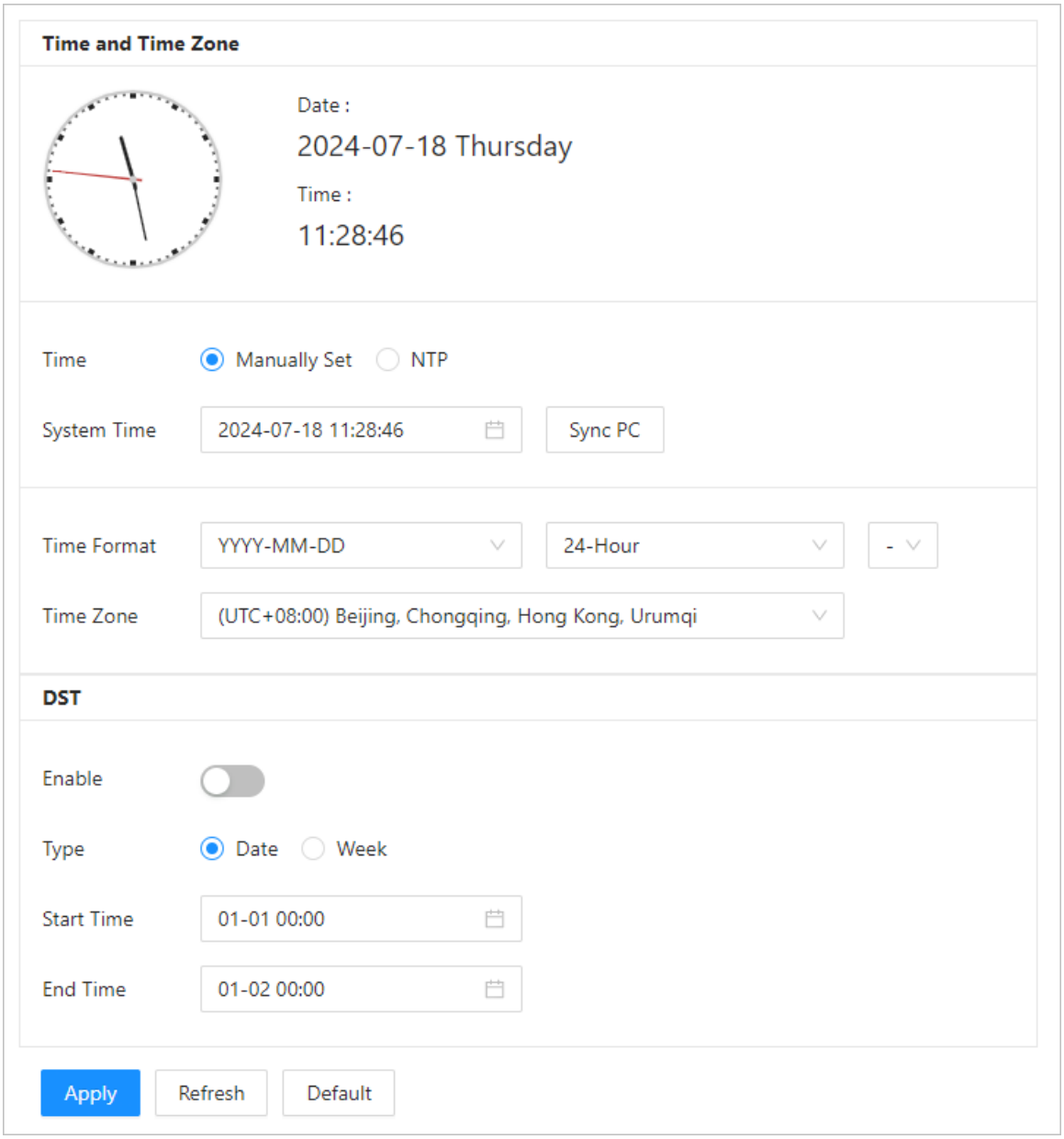


Table 2-10 Time settings description

Parameter	Description
Time	• Manual Set: Manually enter the time or you can click **Sync Time** to sync time with computer. • NTP: The Device will automatically sync the time with the NTP server. ◇ **Server** : Enter the domain of the NTP server. ◇ **Port** : Enter the port of the NTP server. ◇ **Interval** : Enter its time with the synchronization interval.
Time format	Select the time format.
Time Zone	Enter the time zone.

Parameter	Description
DST	1. (Optional) Enable DST. 2. Select **Date** or **Week** from the **Type**. 3. Configure the start time and end time of the DST.

Step 3 Click **Apply**.

2.4.9 User Management

You can add or delete users, change users' passwords, and enter an email address for resetting the password when you forget your password.

2.4.9.1 Adding Administrators

You can add new administrator accounts, and then they can log in to the webpage of the Device.

Procedure

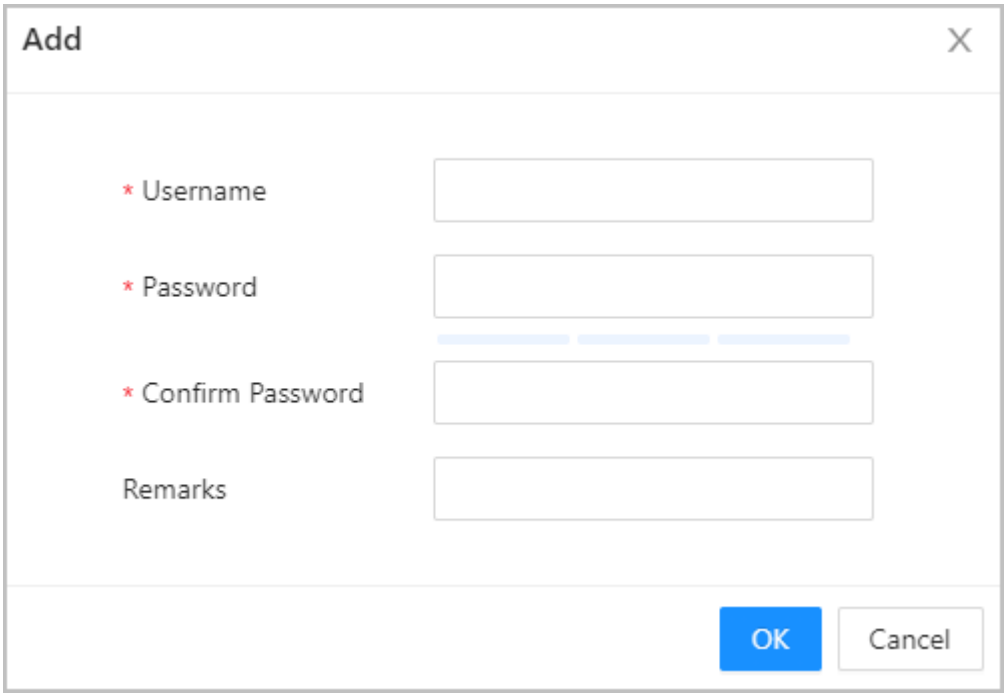
Step 1 On the home page, select **Account Management** > **Account**.

Step 2 Click **Add**, and enter the user information.

- The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &).

  Set a high-security password by following the password strength prompt.

Figure 2-18 Add administrators



Step 3 Click **OK**.

Only admin account can change password and admin account cannot be deleted.

2.4.9.2 Resetting the Password

Reset the password through the linked e-mail when you forget your password.

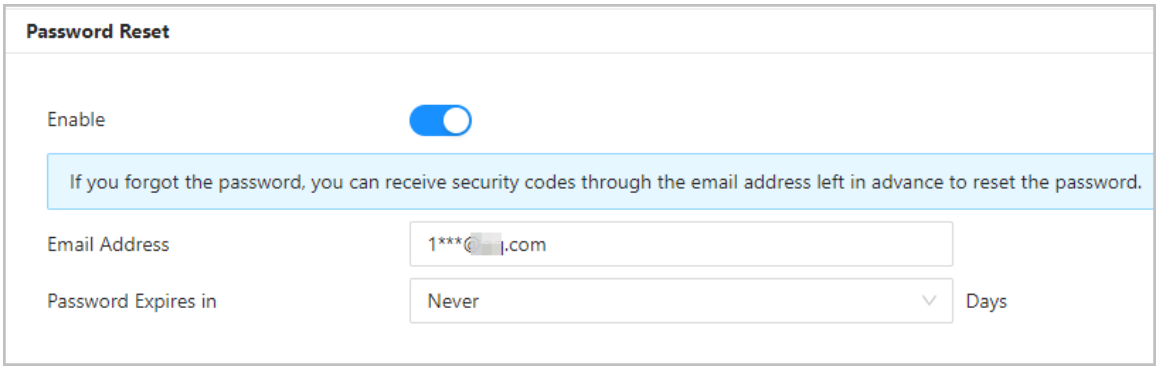
Procedure

Step 1 Select **Account Management** > **Account**.

Step 2 Enter the email address, and set the password expiration time.

Step 3 Turn on the password reset function.

Figure 2-19 Reset Password



If you forgot the password, you can receive security codes through the linked email address to reset the password.

Step 4 Click **Apply**.

2.4.9.3 Adding ONVIF Users

Background Information

Open Network Video Interface Forum (ONVIF), a global and open industry forum that is established for the development of a global open standard for the interface of physical IP-based security products, which allows the compatibility from different manufactures. ONVIF users have their identities verified through ONVIF protocol. The default ONVIF user is admin.

Procedure

Step 1 On the home page, select **Account Management** > **ONVIF User**.

Step 2 Click **Add**, and then configure parameters.

Figure 2-20 Add ONVIF user

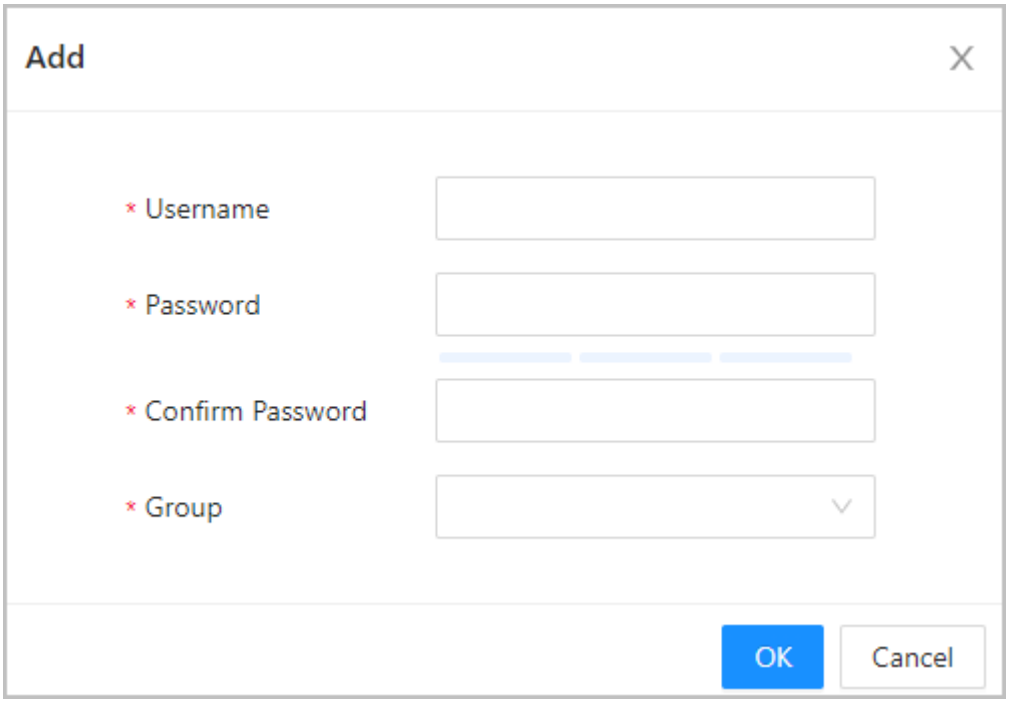


Table 2-11 ONVIF user description

Parameter	Description
Username	The username cannot be the same with existing account. The username consists of up to 31 characters and only allows for numbers, letters, underscores, midlines, dots, or @.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &).
Group	There three permission groups which represents different permission levels. ● admin: You can view and manage other user accounts on the ONVIF Device Manager. ● Operator: You cannot view or manage other user accounts on the ONVIF Device Manager. ● User: You cannot view or manage other user accounts and system logs on the ONVIF Device Manager.

Step 3 Click **OK**.

2.4.10 Maintenance

Regularly restart the Device during its idle time to improve its performance.

Procedure

Step 1 Log in to the webpage.

Step 2 On the home page, select **Maintenance**.

Step 3 Set the time, and then click **Apply**.

The Device will restart at the scheduled time, or you can click **Restart** to restart it immediately.

2.4.11 Advanced Settings

On the home page, select **Advanced Settings**, export and import configuration files, configure card reader parameters, fingerprint parameter and restore the device to default settings.

Configurations Management

You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

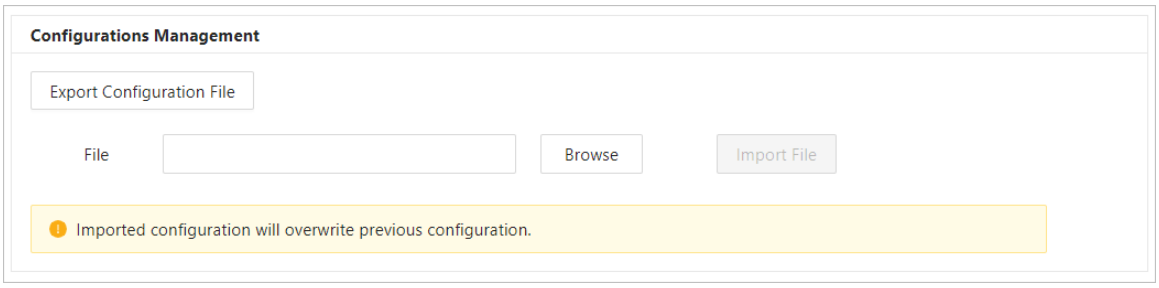
- Export the configuration file.

  Click **Export Configuration File** to download the file to the local computer.

  The IP will not be exported.
- Import the configuration file.
  1. Click **Browse** to select the configuration file.
  2. Click **Import configuration**.

     Configuration files can only be imported to devices that have the same model.

Figure 2-21 Configuration management



Card Reader Settings

Configure the card reader parameters, and then click **Apply**.

Figure 2-22 Card reader settings

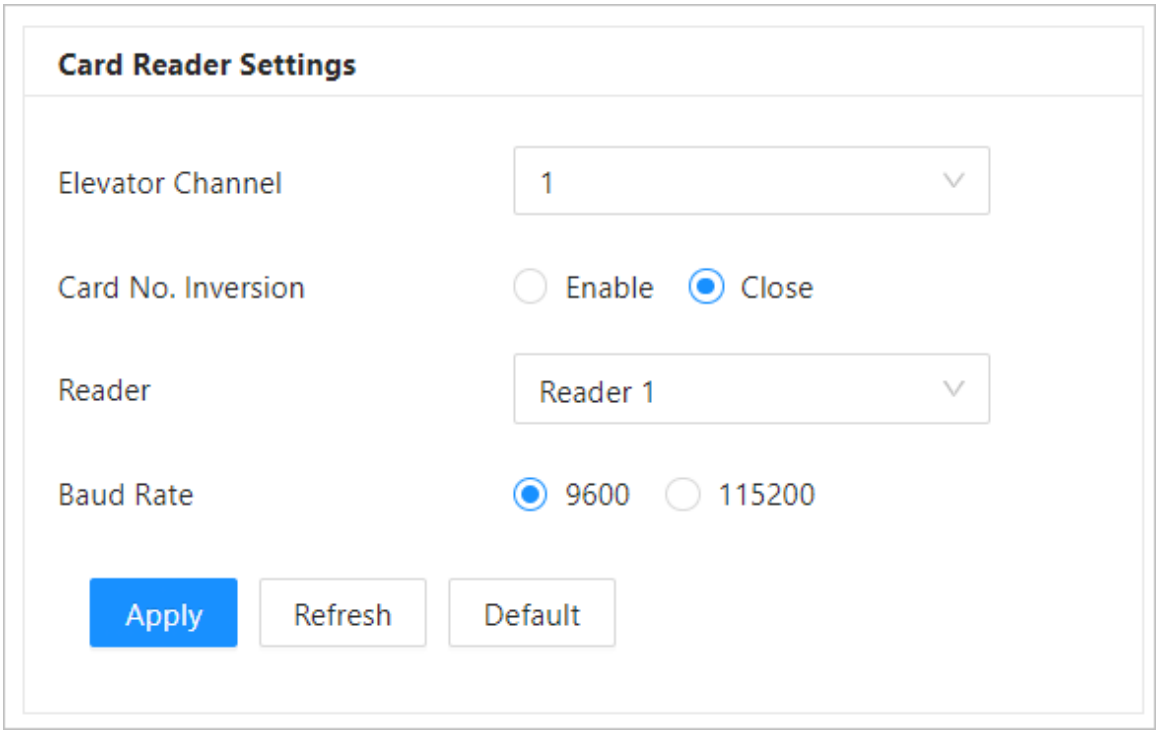


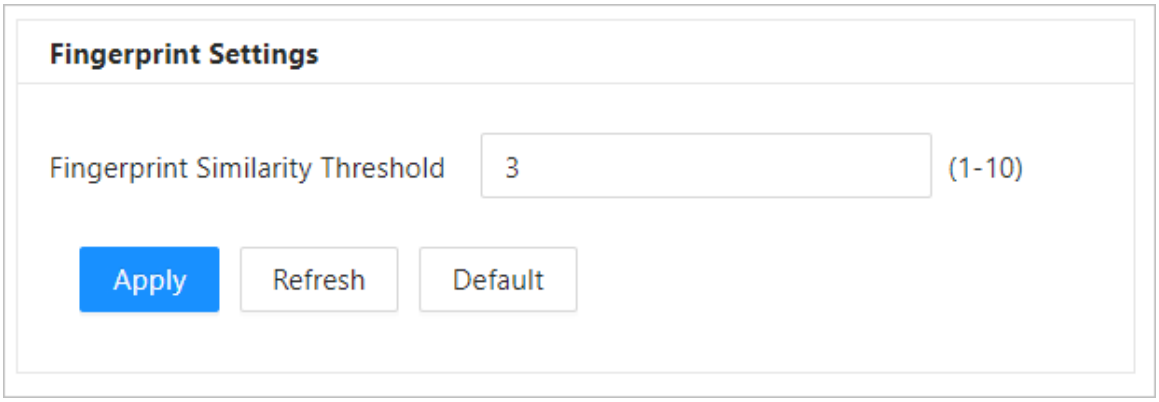
Table 2-12 Description of card reader parameters

Parameter	Description
Elevator Channel	Select the channel according to the actual card reader location.
Card No. Inversion	When the Device connects to a third-party device through the Wiegand input port, and the card number read by the Device is in the reverse order from the actual card number. In this case, you can turn on **Card No. Inversion** function.
Reader	Select the reader.
Baud Rate	Select the baud rate for the card reader.

Fingerprint Settings

Configure the fingerprint similarity threshold, and then click **Apply**.

Figure 2-23 Fingerprint settings



Default

Restoring the **Device** to its default configurations will result in data loss. Please be advised.

- **Factory Defaults** : Resets all the configurations of the Device and delete all the data.
- **Restore to Default (Except for User Info)** : Resets the configurations of the Device and deletes all the data except for user information.

2.4.12 Updating the System

- Use the correct update file. Make sure that you get the correct update file from technical support.
- Do not disconnect the power supply or network, and do not restart or shutdown the Device during the update.

2.4.12.1 File Update

Procedure

Step 1 On the home page, select **System Update**.

Step 2 In **File Update** , click **Browse**, and then upload the update file.

The update file should be a .bin file.

Step 3 Click **Update**.

The Device will restart after the update finishes.

2.4.12.2 Online Update

Procedure

Step 1 On the home page, select **System Update**.

Step 2 In the **Online Update** area, select an update method.

- Enable **Auto Check for Updates**, and the Device will automatically check for the latest version update.
- Click **Manual Check**, and you can immediately check whether the latest version is available.

Step 3 (Optional) Click **Update Now** to update the Device immediately.

2.4.13 Viewing Version Information

On the webpage, select **Version Info**, and you can view version information of the Device.

2.4.14 Viewing Legal Information

On the home page, select **Legal Info**, and you can view open source software notice.

2.5 Reporting

2.5.1 Viewing Alarm Records

Procedure

Step 1 On the home page, select **Reporting** > **Alarm Records**.

Step 2 Select the type and the time range, and then click **Search**.

You can view the records of duress alarm, tamper alarm, blocklist, offline alarm for elevator control module or all the alarm records.

2.5.2 Viewing Elevator Control Records

Procedure

Step 1 On the home page, select **Reporting** > **Elevator Control Records**.

Step 2 Select the authentication type and the time range, and then click **Search**.

You can view the records of the following authentication types: **All** , **Unknown**, **Elevator Control by VTO**, **Elevator Control by Platform**, **Elevator Control by Elevator Controller** and **Elevator Control by ASI**.

2.6 Security

2.6.1 Security Status

Scan the users, service, and security modules to check the security status of the Device.

Background Information

- User and service detection: Check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio and video transmission, trusted protection, securing warning and attack defense, not detect whether they are enabled.

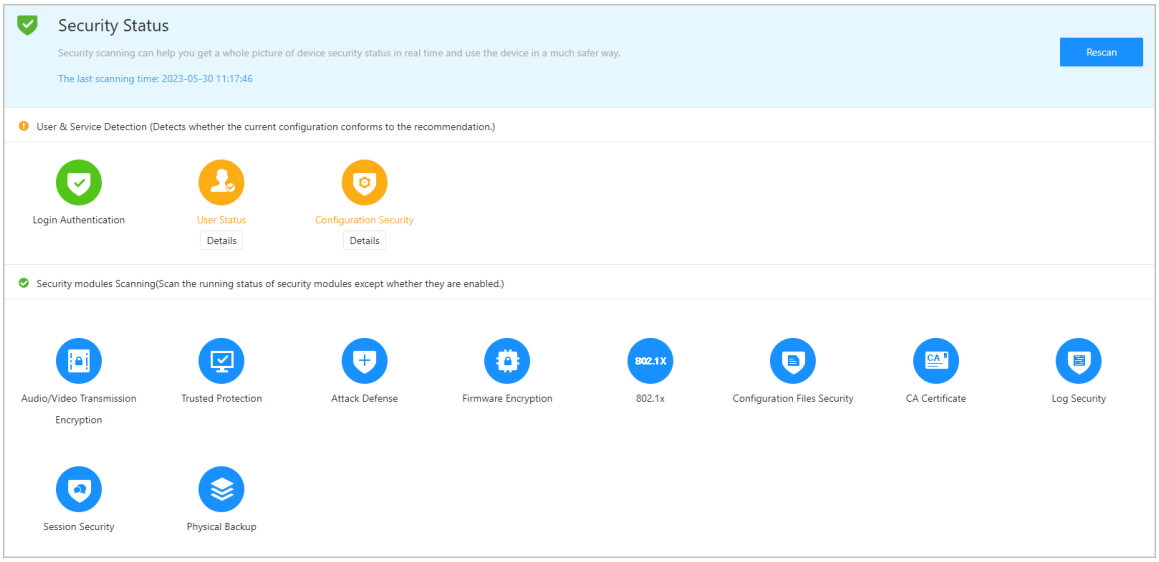
Procedure

Step 1 On the home page, select **Security** > **Security Status**.

Step 2 Click **Rescan** to perform a security scan of the Device.

Hover over the icons of the security modules to see their running status.

Figure 2-24 Security Status



Related Operations

After you perform the scan, the results will be displayed in different colors. Yellow indicates that the security modules are abnormal, and green indicates that the security modules are normal.

- Click **Details** to view the details on the results of the scan.
- Click **Ignore** to ignore the abnormality, and it will not be scanned. The abnormality that was ignored will be highlighted in grey.
- Click **Optimize** to troubleshoot the abnormality.

2.6.2 Configuring System Service

Create a certificate or upload an authenticated certificate, and then you can log in to the webpage through HTTPS on your computer. HTTPS secures communication over a computer network.

Procedure

Step 1 On the home page, select **Security** > **System Service**.

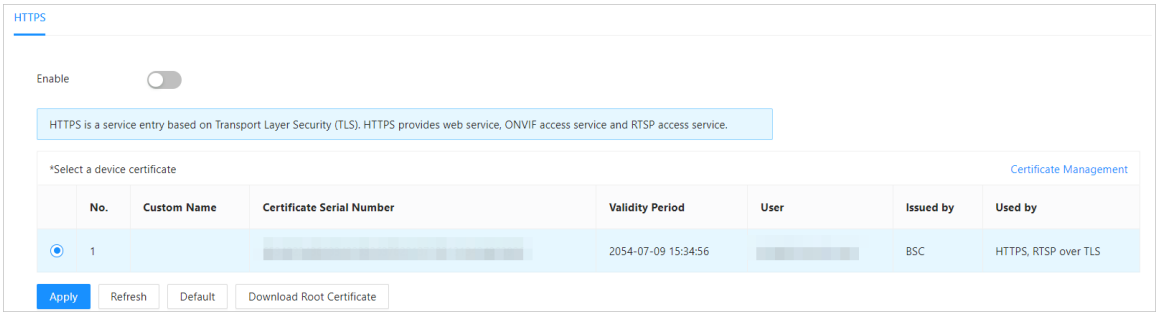
Step 2 Turn on the HTTPS service.

If you turn on the compatible with TLS v1.1 and earlier versions, security risks might occur. Please be advised.

Step 3 Select the certificate.

If there are no certificates in the list, click **Certificate Management** to upload a certificate.

Figure 2-25 HTTPS



Step 4 Click **Apply**.

Enter "https://*IP address*:*httpsport*" in a web browser. If the certificate is installed, you can log in to the webpage successfully. If not, the webpage will display the certificate as wrong or untrusted.

2.6.3 Attack Defense

2.6.3.1 Configuring Firewall

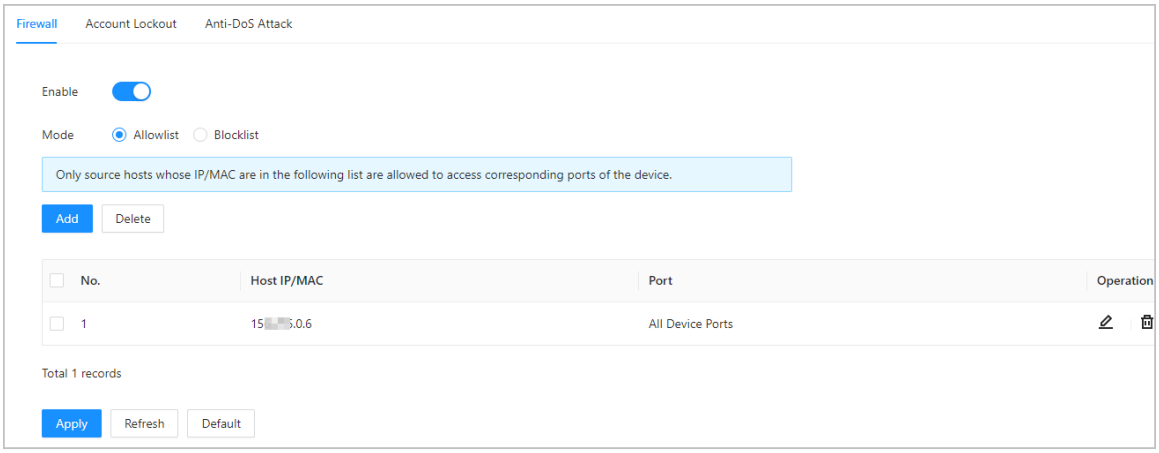
Configure firewall to limit access to the Device.

Procedure

Step 1 On the home page, select **Security** > **Attack Defense** > **Firewall**.

Step 2 Click to enable the firewall function.

Figure 2-26 Firewall

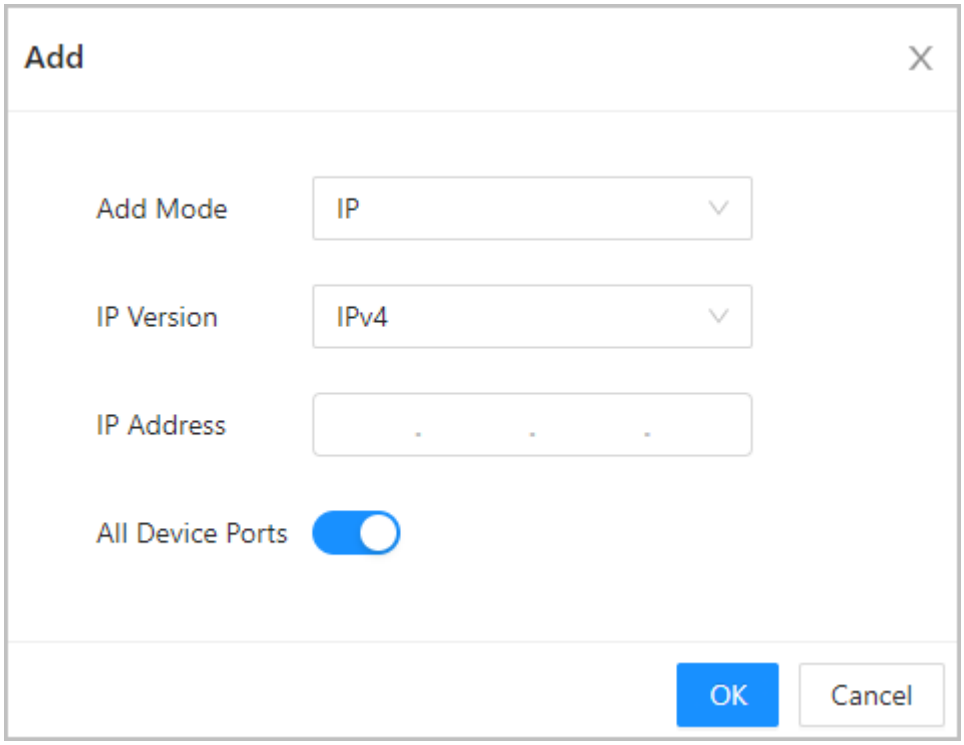


Step 3 Select the mode: **Allowlist** and **Blocklist**.

- **Allowlist** : Only IP/MAC addresses on the allowlist can access the Device.
- **Blocklist** : The IP/MAC addresses on the blocklist cannot access the Device.

Step 4 Click **Add** to enter the IP information.

Figure 2-27 Add IP information



Step 5 Click **OK**.

Related Operations

- Click to edit the IP information.
- Click to delete the IP address.

2.6.3.2 Configuring Account Lockout

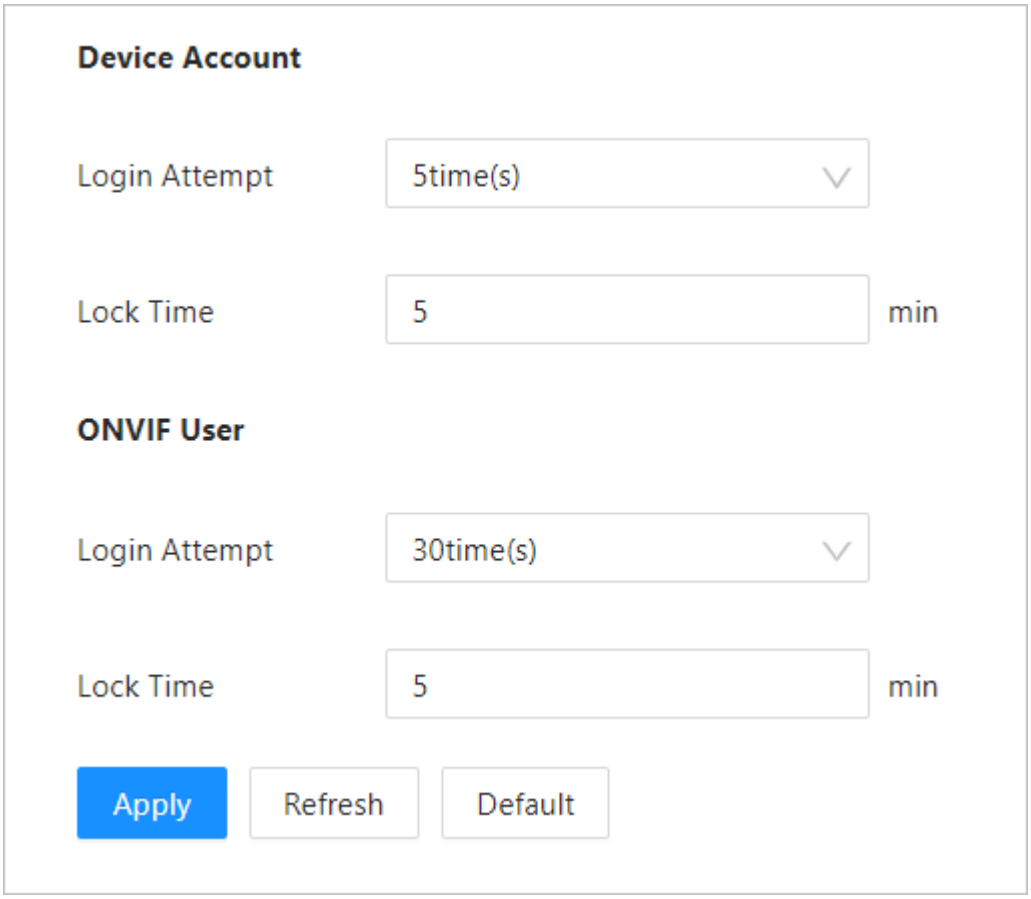
If the incorrect password is entered for a defined number of times, the account will be locked.

Procedure

Step 1 On the home page, select **Security** > **Attack Defense** > **Account Lockout**.

Step 2 Enter the number of login attempts and the time the administrator account and ONVIF user will be locked for.

Figure 2-28 Account lockout



- Login Attempt: The limit of login attempts. If the incorrect password is entered for a defined number of times, the account will be locked.
- Lock Time: The duration during which you cannot log in after the account is locked.

Step 3 Click **Apply**.

2.6.3.3 Configuring Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attacks.

Procedure

Step 1 On the home page, select **Security** > **Attack Defense** > **Anti-DoS Attack**.

Step 2 Turn on **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to protect the Device against Dos attack.

Figure 2-29 Anti-DoS attack

Step 3 Click **Apply**.

2.6.4 Installing Device Certificate

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS on your computer.

2.6.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

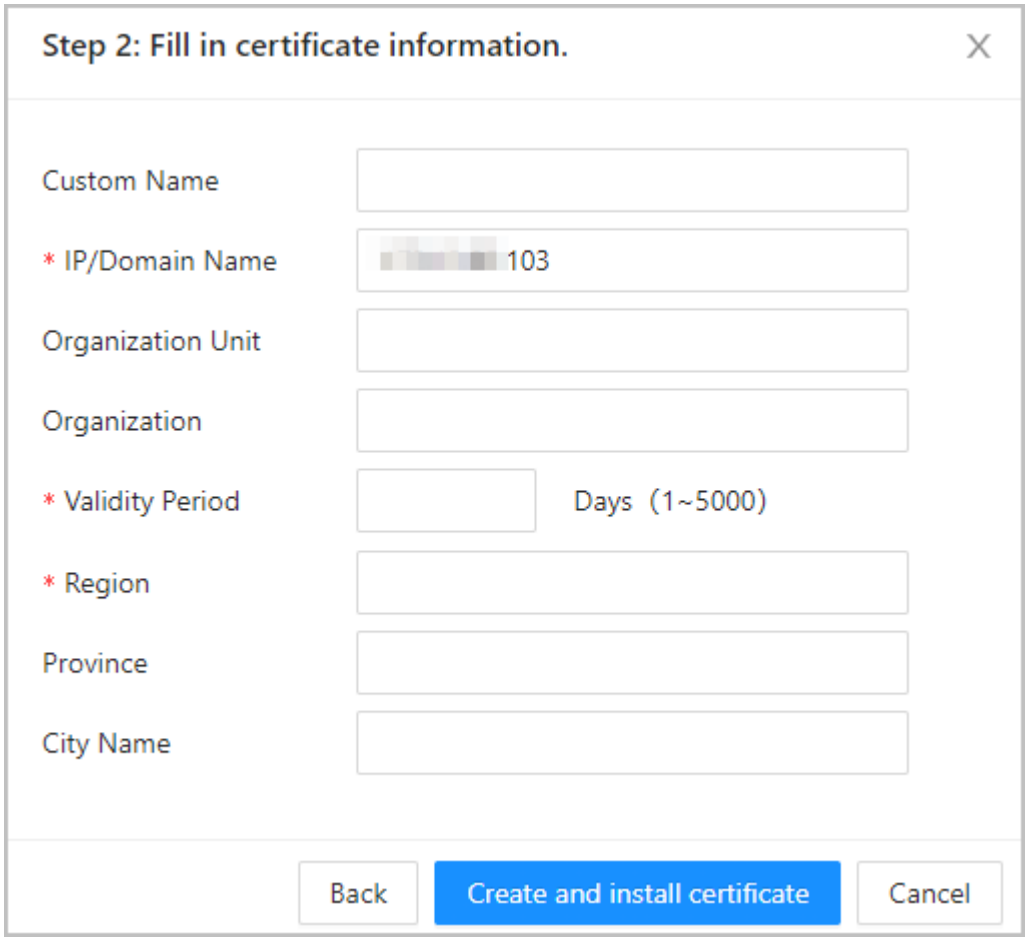
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Device Certificate**.

Step 3 Select **Create Certificate** , and click **Next**.

Step 4 Enter the certificate information.

Figure 2-30 Certificate information



The name of region cannot exceed 2 characters. We recommend entering the abbreviation of the name of the region.

Step 5 Click **Create and install certificate**.

The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

2.6.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Device.

Procedure

Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Click **Install Device Certificate**.

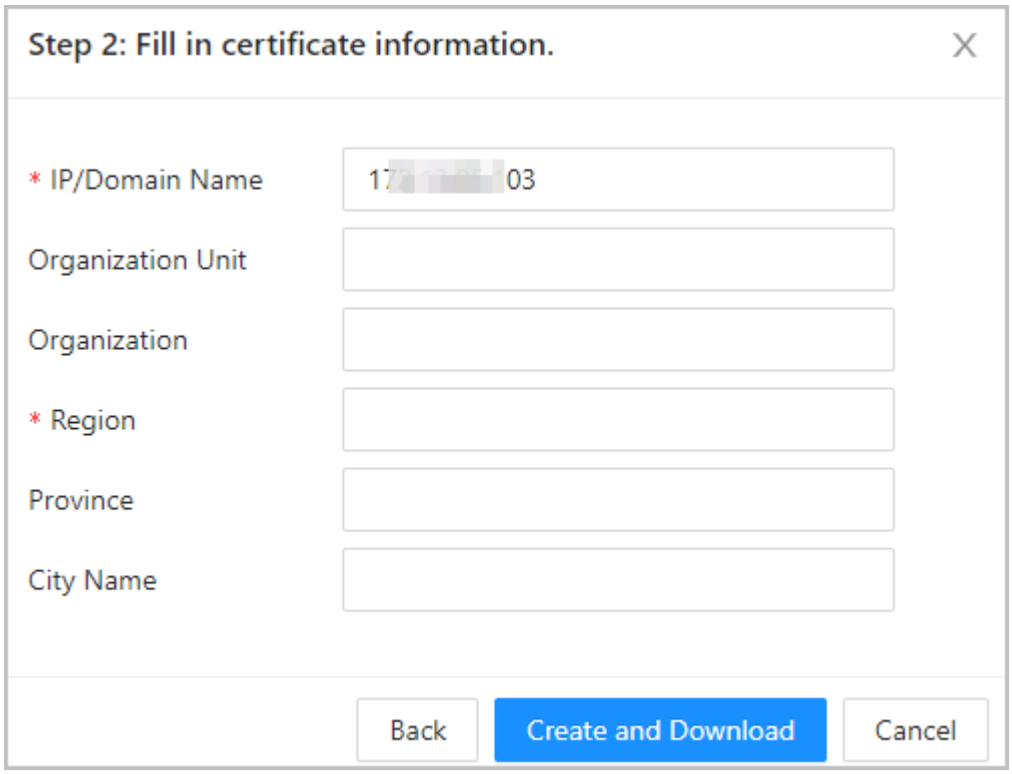
Step 3 Select **Apply for CA Certificate and Import (Recommended)** , and click **Next**.

Step 4 Enter the certificate information.

- IP/Domain name: the IP address or domain name of the Device.

- Region: The name of region must not exceed 3 characters. We recommend you enter the abbreviation of region name.

Figure 2-31 Certificate information (2)



Step 5 Click **Create and Download**.

Save the request file to your computer.

Step 6 Apply to a third-party CA authority for the certificate by using the request file.

Step 7 Import the signed CA certificate.

1. Save the CA certificate to your computer.
2. Click **Installing Device Certificate**.
3. Click **Browse** to select the CA certificate.
4. Click **Import and Install**.

   The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

   - Click **Recreate** to create the request file again.
   - Click **Import Later** to import the certificate at another time.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

2.6.4.3 Installing Existing Certificate

If you already have a certificate and private key file, import the certificate and private key file.

Procedure

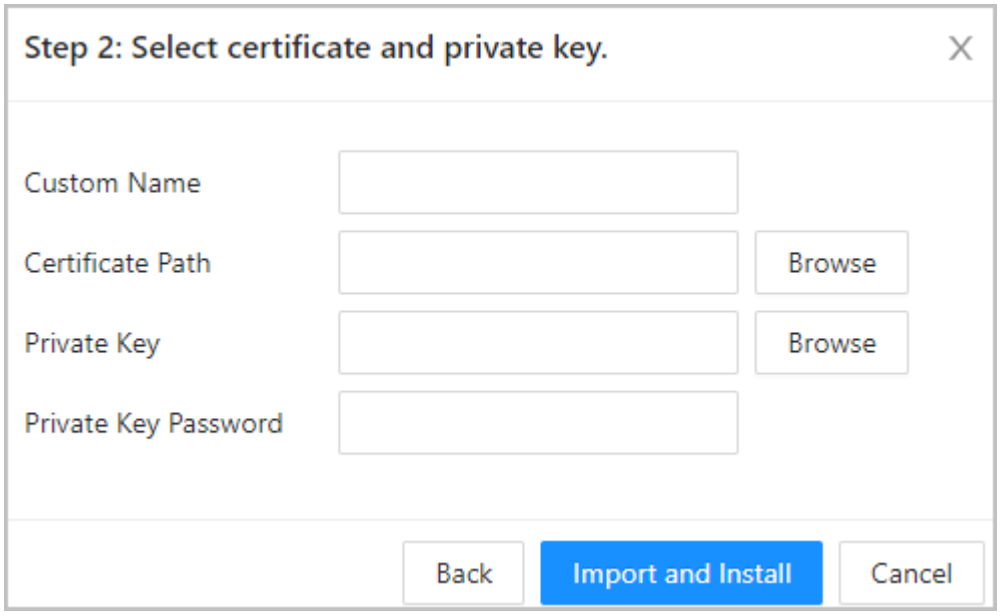
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Click **Install Device Certificate**.

Step 3 Select **Install Existing Certificate** , and click **Next**.

Step 4 Click **Browse** to select the certificate and private key file, and enter the private key password.

Figure 2-32 Certificate and private key



Step 5 Click **Import and Install**.

The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

2.6.5 Installing the Trusted CA Certificate

A trusted CA certificate is a digital certificate that is used for validating the identities of websites and servers. For example, when 802.1x protocol is used, the CA certificate for switches is required to authenticate its identity.

Background Information

802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them access to the network.

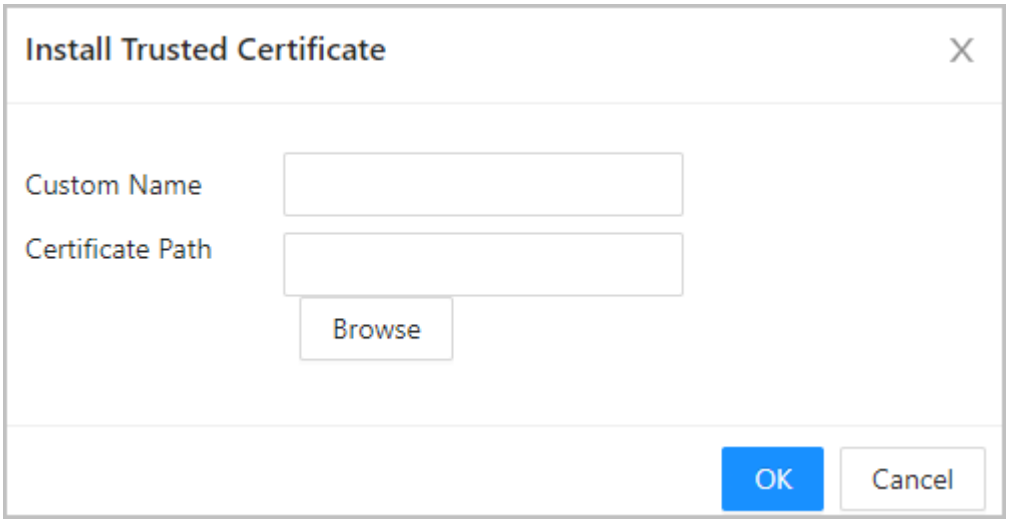
Procedure

Step 1 Select **Security** > **CA Certificate** > **Trusted CA Certificates**.

Step 2 Select **Install Trusted Certificate**.

Step 3 Click **Browse** to select the trusted certificate.

Figure 2-33 Install the trusted certificate



Step 4 Click **OK**.

The newly installed certificate is displayed on the **Trusted CA Certificates** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

2.6.6 Security Warning

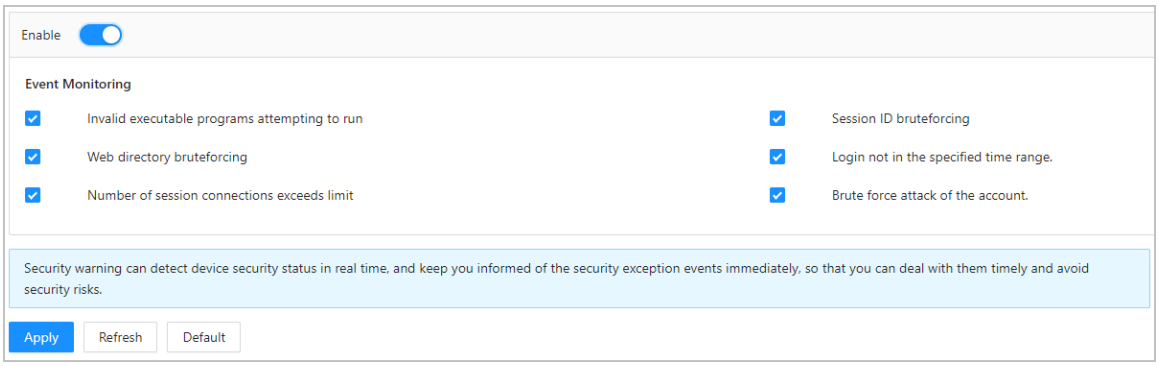
Procedure

Step 1 On the home page, select **Security** > **Security Warning**.

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 2-34 Security warning



Step 4 Click **Apply**.

Appendix 1 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).