2-Wire Controller

User's Manual

V1.0.4

Foreword

General

This manual introduces the structure, functions, and operations of the 2-wire controller (hereinafter referred to as "the 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.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.4	Revise network diagram.	February 2025
V1.0.3	• Revise RS-485 configuration. • Revise module. • Add audio.	January 2025
V1.0.2	Revise network diagram.	December 2024
V1.0.1	Revise network diagram.	September 2024
V1.0.0	First Release.	July 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 Safeguard and Warnings

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

Installation Requirements

WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Please follow the electrical requirements to power the device.
  - 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 device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device 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 device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- Install the device 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 device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Operation Requirements

DANGER

Battery Pack Precautions

Preventive measures (including but not limited to):

- Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
- Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.

- Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

⚠

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Transport, use and store the device under allowed humidity and temperature conditions.
- If the device is powered off for longer than a month, it should be placed in its original package and sealed. Make sure to keep it away from moisture, and store it under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.

Table of Contents

Foreword I
Important Safeguard and Warnings III
1 Overview 1
1.1 Introduction 1
1.2 Structure 1
2 Network Diagram 3
3 Webpage Operations 7
3.1 Home Page 7
3.2 Admin Center 8
3.2.1 Resetting the Password 8
3.2.2 Changing the User Message 9
3.2.3 Restoring the Factory Default Settings 9
3.2.4 Restarting the Device 9
3.2.5 Logging Out 10
3.3 Security Center 10
3.3.1 Security Status 10
3.3.2 Configuring HTTPS 11
3.3.3 Attack Defense 11
3.3.4 Installing Device Certificate 14
3.3.5 Installing the Trusted CA Certificate 17
3.3.6 Security Warning 18
3.3.7 Security Authentication 18
3.4 VTO Configuration 19
3.4.1 Personnel Management 19
3.4.2 VTH Room Number Mapping 21
3.4.3 Access Control 22
3.4.4 Module 25
3.4.5 Maintenance 26
3.4.6 Audio 26
3.5 Adding Person 27
3.6 Importing Persons in Batches 29
3.7 Network Settings 29
3.7.1 Configuring TCP/IP 29
3.7.2 Configuring Basic Services 30
3.8 Maintenance Center 32
3.8.1 One-click Diagnosis 32
3.8.2 System Information 32

3.8.3 Exporting and Importing Configuration Files.....32
3.8.4 Updating the System.....33
3.8.5 Advanced Maintenance.....34
Appendix 1 Security Recommendation.....35

1 Overview

1.1 Introduction

The 2-wire controller uses the plastic material and supports slide rail installation. Up to 100 analog VTHs or 22 VTHs with Wi-Fi function can be connected to one 2-wire controller. The 2-wire controller can connect to other 2-wire controllers in the cascading mode (up to 10 levels of cascading are supported). You can log in to the webpage of the Controller to manage the devices.

- In the cascading mode, please configure the devices through one webpage of the 2-wire controller at the same time.
- Please use the recommended power supply.

1.2 Structure

Figure 1-1 Front panel

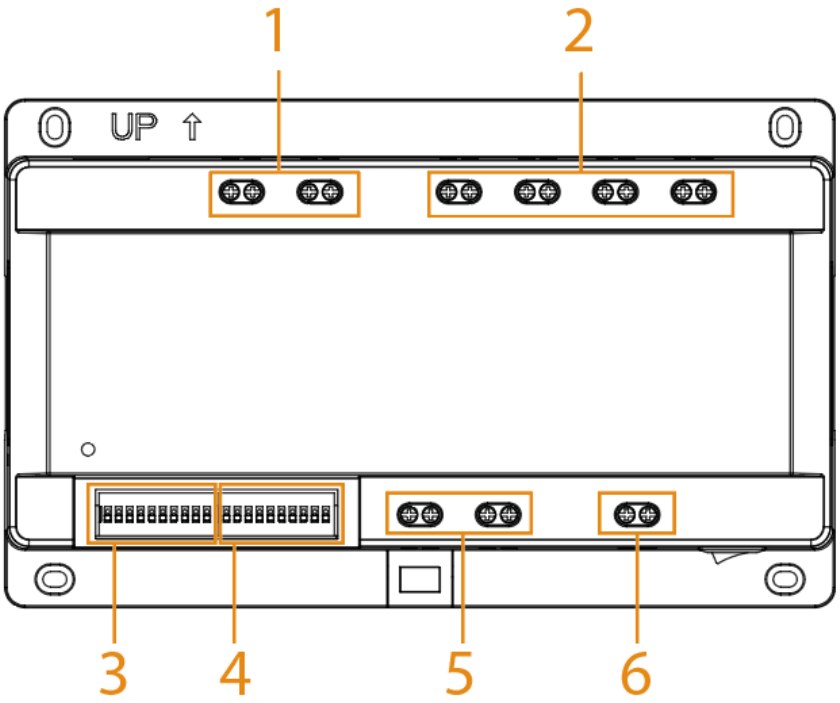
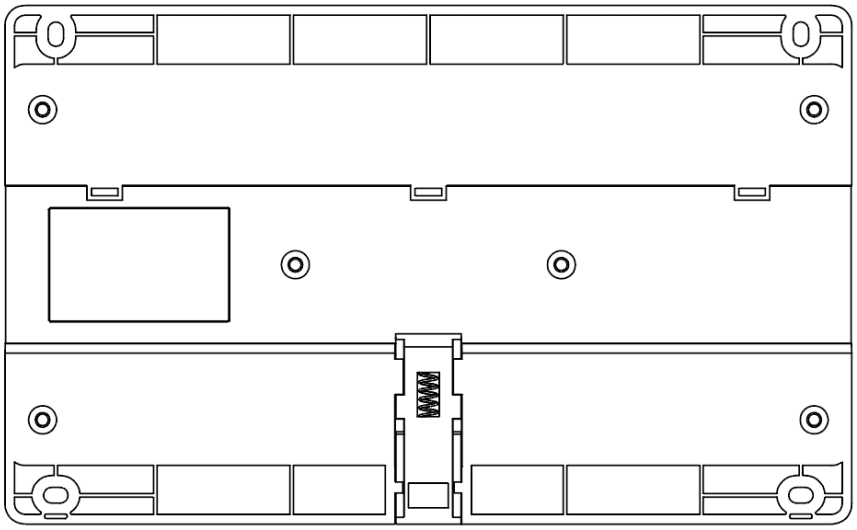


Table 1-1 Front panel description

No.	Description
1	Connect to VTO.
2	Connect to VTH.

No.	Description
3	After connecting to VTHs, set the DIP to the minimum ID of all the VTH IDs. Move the actuator completely to the top or bottom position. If the actuator is in the middle position, it is considered to be in the top position.
4	After connecting to VTHs, set the DIP to the maximum ID of all the VTH ID. Move the actuator completely to the top or bottom position. If the actuator is in the middle position, it is considered to be in the top position.
5	Connect to other 2-wire controllers. The **UP** port can only be connected to the **Down** port on another controller. The **Down** port can only be connected to the **Up** port on another controller. For details, see the wiring diagram.
6	Connect to power supply.

Figure 1-2 Rear panel



2 Network Diagram

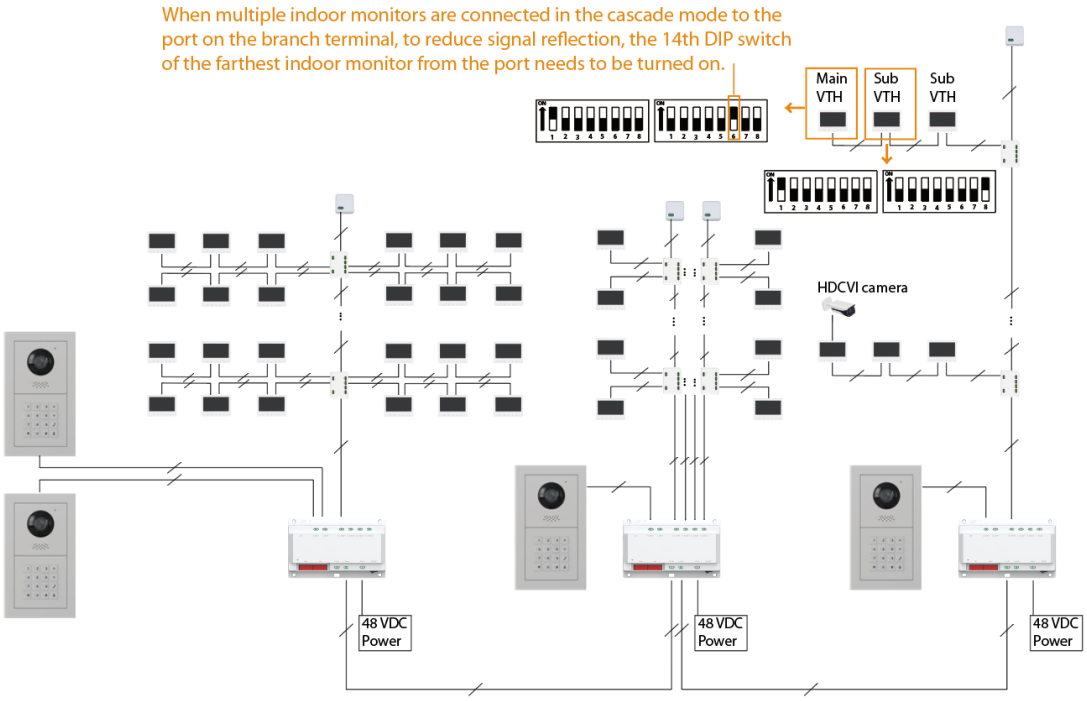
When multiple indoor monitors are connected in the cascade mode to the port on the branch terminal, to reduce signal reflection, the 14th DIP switch of the farthest indoor monitor from the port needs to be turned on.

Refer to the following image to configure the DIP switch of the device in the cascade. The DIP switch of ID should be configured according to the actual situation.

- The power supply of HDCVI camera cannot be grounded.
- The product appearance is for reference only.

Network Diagram

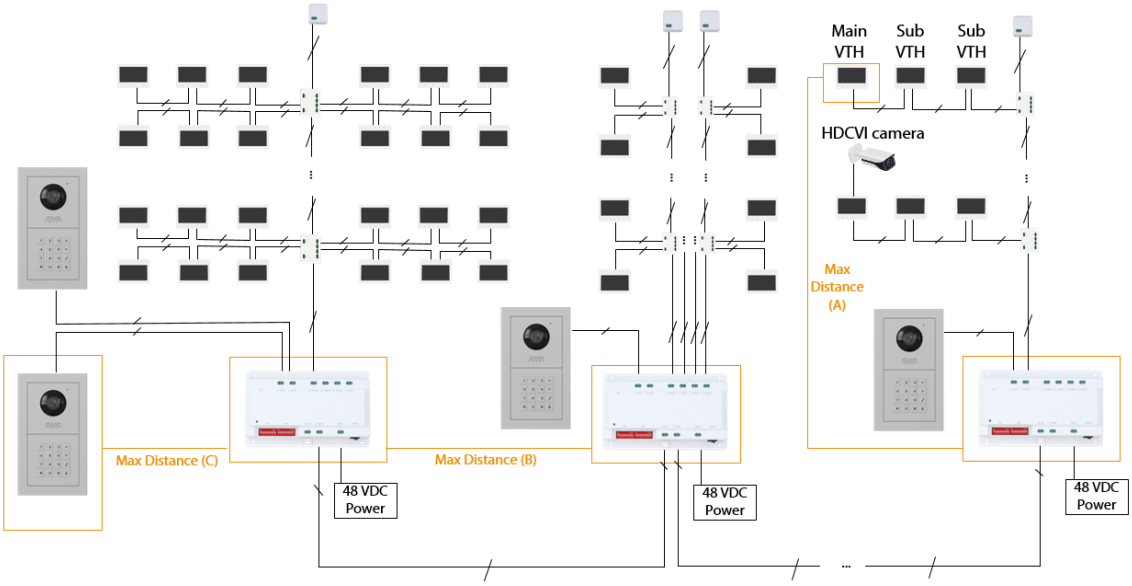
Figure 2-1 Network diagram



Wiring Distance between the Controller, VTH and the VTO

- Max distance (A) refers to the distance between the 2-wire controller and the VTH. A≤100 m.
- Max distance (B) refers to the distance between the cascading 2-wire controllers. B≤100 m.
- Max distance (C) refers to the distance between the 2-wire controller and the VTO. C≤100 m.
- The number of cascading controllers must be less than or equal to 10.
- For systems with multiple VTHs in a cascade, the number of devices must be less than or equal to 10 in each branch.

Figure 2-2 Max distance



Network Capacity for VTH

The capacity for the VTH indicates the maximum number of VTHs that can be connected to one indoor monitor port on the 2-wire controller.

Each controller can connect up to 22 VTHs with Wi-Fi function or up to 100 VTHs without Wi-Fi function.

- The 2-wire VTHs with the Wi-Fi function can work at the same time. The number of 2-wire VTHs without the Wi-Fi function that work at the same time is 5% of the maximum capacity according to different cable specifications and distances.
- The capacity values are based on the default settings for voice and screen brightness, and standard cables that are mentioned in the following table.
- In the network, if you want to replace the VTH with Wi-Fi function to the VTH without Wi-Fi function, the conversion ratio is 1:8.

  For example, if you want to reduce 1 VTH with Wi-Fi function in the network, you can connect to 8 VTHs without Wi-Fi function.

  The maximum number of VTHs with Wi-Fi function cannot exceed 22.

  The maximum number of VTHs without Wi-Fi function cannot exceed 100.

Table 2-1 Network capacity for VTH (240 W power supply as an example)

Cable Type	Cable Specification	AWG	Device Type	A=0–25 m	A=26–50 m	A=51–75 m	A=76–100 m
Regular cable	RVV 2 × 1.5 mm^2 (Recommend)	AWG 15	With Wi-Fi	22	22	22	17
			Without Wi-Fi	100	100	100	100
	RVV 2 × 1 mm^2	AWG 17	With Wi-Fi	22	22	18	13

Cable Type	Cable Specification	AWG	Device Type	A=0–25 m	A=26–50 m	A=51–75 m	A=76–100 m
			Without Wi-Fi	100	100	100	100
	RVV 2 × 0.5 mm^2	AWG 20	With Wi-Fi	22	17	11	8
			Without Wi-Fi	100	100	91	68
Network cable	Double-pair network cable	AWG 21	With Wi-Fi	22	14	9	7
			Without Wi-Fi	100	100	75	56
	Single-pair network cable	AWG 24	With Wi-Fi	14	7	4	3
			Without Wi-Fi	100	56	37	28

Network Capacity for 2-Wire Controller

The capacity for the 2-wire controller indicates the maximum number of controllers that can be connected to one corresponding port on the controller.

The capacity values are based on standard cables that are mentioned in the following table.

Table 2-2 Network capacity for the controller

Cable Type	Cable Specification	AWG	B=0–100 m
Regular cable	RVV 2 × 1.5 mm^2	AWG 15	8
	RVV 2 × 1 mm^2	AWG 17	10
	RVV 2 × 0.5 mm^2 (Recommend)	AWG 20	10
Network cable	Double-pair network cable	AWG 21	10
	Single-pair network cable	AWG 24	10

Network Capacity for VTO

The capacity for the VTO indicates the maximum number of VTOs that can be connected to one 2-wire controller.

Up to 2 VTOs can be connected to one 2-wire controller.

The capacity values are based on standard cables that are mentioned in the following table.

Table 2-3 Network capacity for the VTO

Cable Type	Cable Specification	AWG	C=0–25 m	C=26–50 m	C=51–75 m	C=76–100 m
Regular cable	RVV 2 × 1.5 mm^2 (Recommend)	AWG 15	2	2	2	2
	RVV 2 × 1 mm^2	AWG 17	2	2	2	2
	RVV 2 × 0.5 mm^2	AWG 20	2	2	2	2

Cable Type	Cable Specification	AWG	C=0–25 m	C=26–50 m	C=51–75 m	C=76–100 m
Network cable	Double-pair network cable	AWG 21	2	2	2	2
	Single-pair network cable	AWG 24	2	2	1	1

3 Webpage Operations

For first-time login, you need to initialize the device on the webpage.

Log in to the webpage to configure the parameters of the Controller and manage the VTO connected to the current controller and the VTO connected to cascading controllers.

3.1 Home Page

The system automatically goes to the home page after you log in.

Figure 3-1 Home page

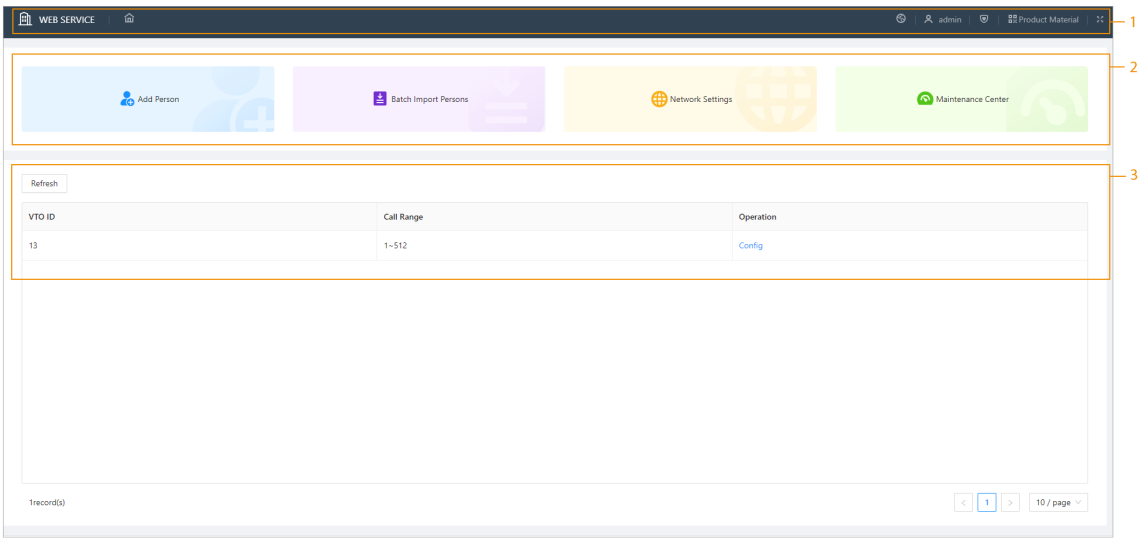


Table 3-1 Home page introduction

No.	Icon	Function	Description	Reference
1		Home button	Go back to the home page.	—
		Language	Change language of the webpage of the device.	—
	admin	Admin center	Change password, log out of the current device, restart the system, and restore the device to factory settings.	"3.2 Admin Center"
		Security center	View and configure the security settings.	"3.3 Security Center"
	Product Material	Product material	Scan the QR code to view the product material, such as the user's manual.	—
		Full screen	View the webpage in the full screen mode. Click again or press the Exit key to exit the full screen mode.	—

No.	Icon	Function	Description	Reference
2	—	Add person	Add the person and send the information to VTOs.	"3.5 Adding Person"
	—	Batch import persons	After exporting person information from the VTO, import persons in batches to other VTOs.	"3.6 Importing Persons in Batches"
	—	Network settings	Configure the network parameters such as TCP/IP, and basic services.	"3.7 Network Settings"
	—	Maintenance center	View the system information. Export and import configuration files. Update the device and more.	"3.8 Maintenance Center"
3	—	VTO configuration	Manage person information on the VTO. Configure the VTO parameters, including access control parameters, module parameters and more.	"3.4 VTO Configuration"

3.2 Admin Center

Change password, logout, restart the device, restore the device to factory default settings and other operations on the home page.

3.2.1 Resetting the Password

If you forget the login password of the admin account, scan the QR code to reset it.

Prerequisites

Make sure that you have enabled **Password Reset** through **Network Settings** > **Basic Services**.

If you did not configure the email address during the initialization, the system will report an error. Please contact the local dealer or the technical support for help.

Procedure

Step 1 Click **Forget Password?** on the login page, and then click **Next**.

Step 2 Get the **Security Code** according to the instructions.

- You can get up to 2 security codes with the same QR code. If you need more security codes, you need to refresh the QR code and scan it again.
- The security code will be sent to your email address. You must use it in 24 hours. Otherwise, the security code will be invalid.
- The account will be locked for 5 minutes if you enter the wrong security code 5 times in a row.

Step 3 Enter the security code you received, and then click **Next**.

Step 4 Enter new password, confirm the new password, and then click **OK**.

3.2.2 Changing the User Message

Change the login password and the email address of the user.

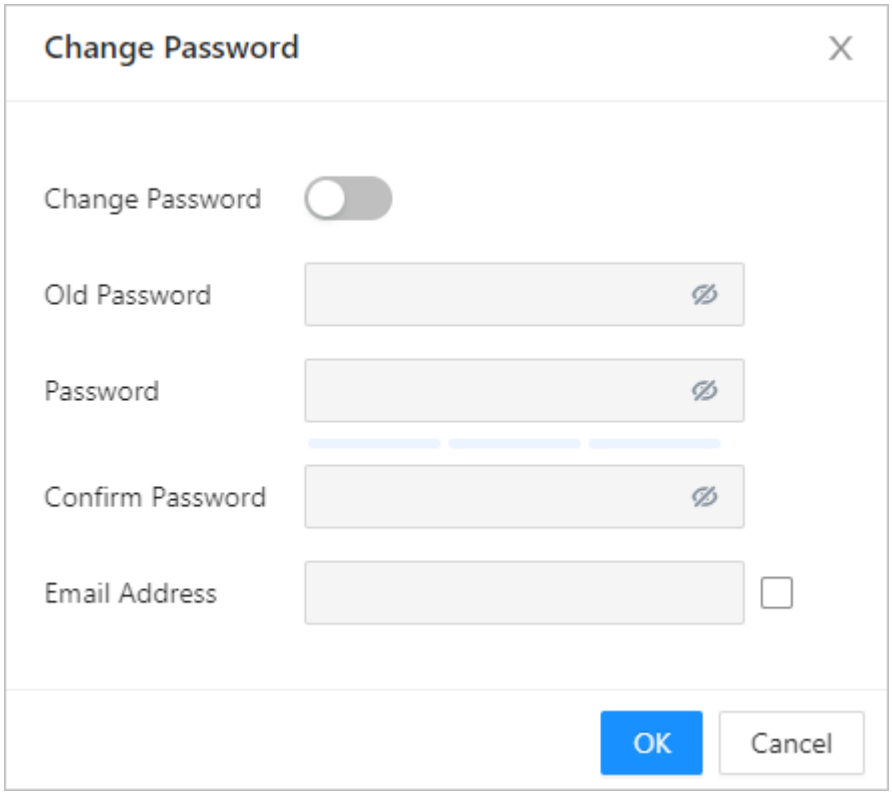
Procedure

Step 1 Click admin on the home page.

Step 2 Click **Change Password**.

Step 3 Enable the function, configure the parameters, and then click **OK**.

Figure 3-2 Changing the user message



3.2.3 Restoring the Factory Default Settings

Procedure

Step 1 Select admin > **Factory Default**.

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

Step 2 Enter the login password, and then click **OK**.

Step 3 Restore to the factory default settings if necessary.

3.2.4 Restarting the Device

Select admin > **Restart**, and then click **OK** in the pop-up window. The device automatically restarts, and the webpage goes to the login page.

3.2.5 Logging Out

Select admin > **Logout**. The webpage goes to the login page.

3.3 Security Center

3.3.1 Security Status

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

Background Information

- User and service detection: Check whether the current configurations conform to recommendation.
- Security modules scanning: Scan the running status of security modules, such as trusted protection, firmware encryption and attack defense.

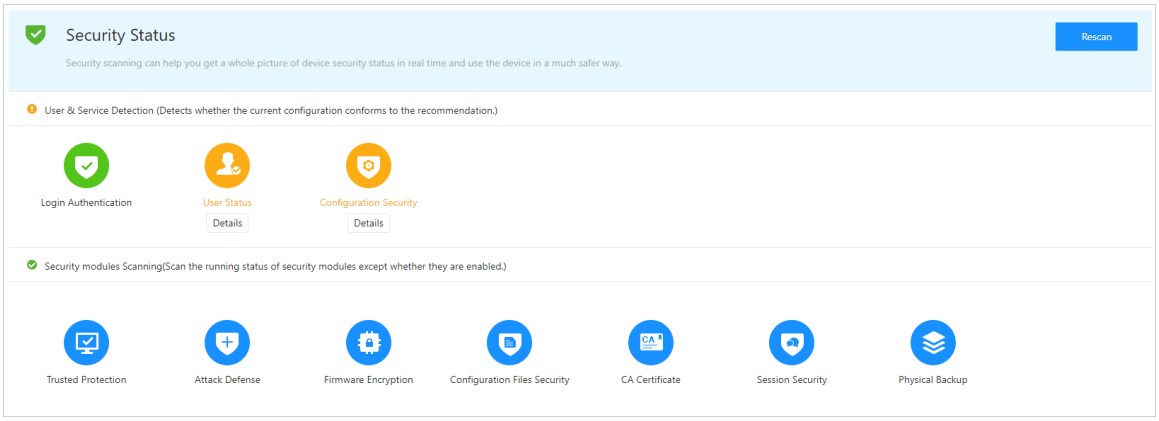
Procedure

Step 1 Select > **Security Status**.

Step 2 Click **Scan** to perform a security scan of the device.

- Hover over the icons of the security modules to see their running status.
- If you want to check the status after the first scanning, click **Rescan**.

Figure 3-3 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.

3.3.2 Configuring HTTPS

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 Select > **System Service** > **HTTPS**.

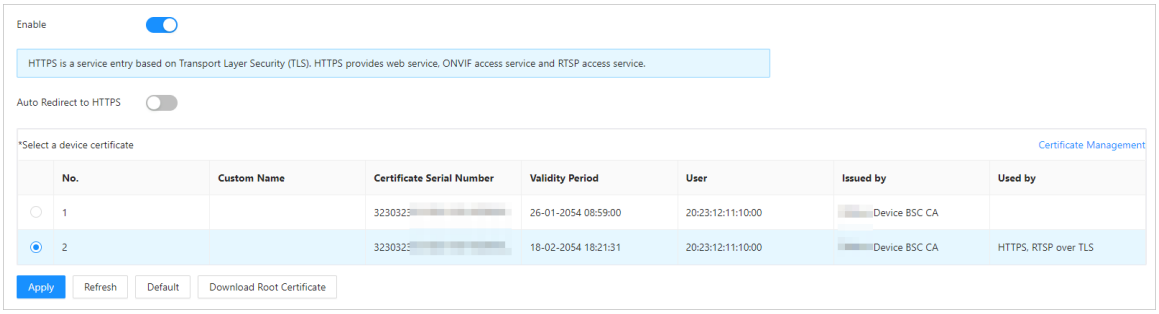
Step 2 Enable the HTTPS service.

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 3-4 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.

3.3.3 Attack Defense

3.3.3.1 Configuring Firewall

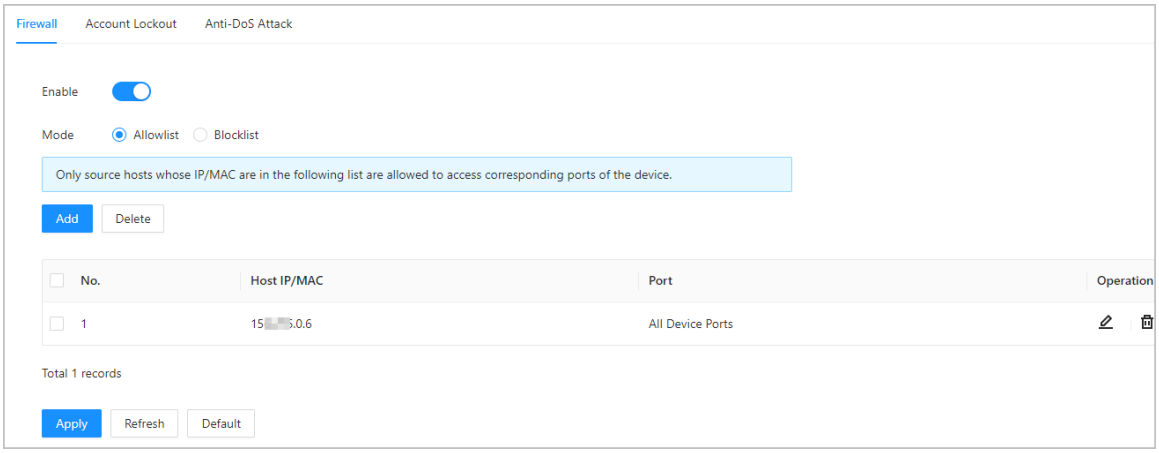
Configure firewall to limit access to the Device.

Procedure

Step 1 Select > **Attack Defense** > **Firewall**.

Step 2 Click to enable the firewall function.

Figure 3-5 Firewall

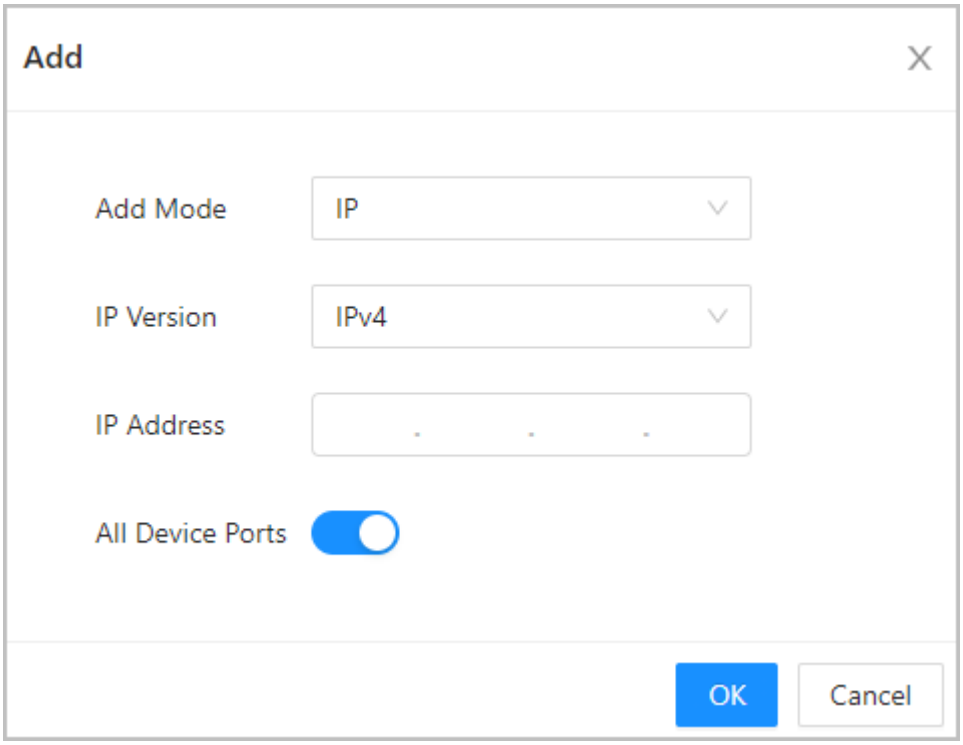


Step 3 Select the mode: **Allowlist** and **Blocklist**.

- **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 3-6 Add IP information



Step 5 Click **OK**.

Related Operations

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

3.3.3.2 Configuring Account Lockout

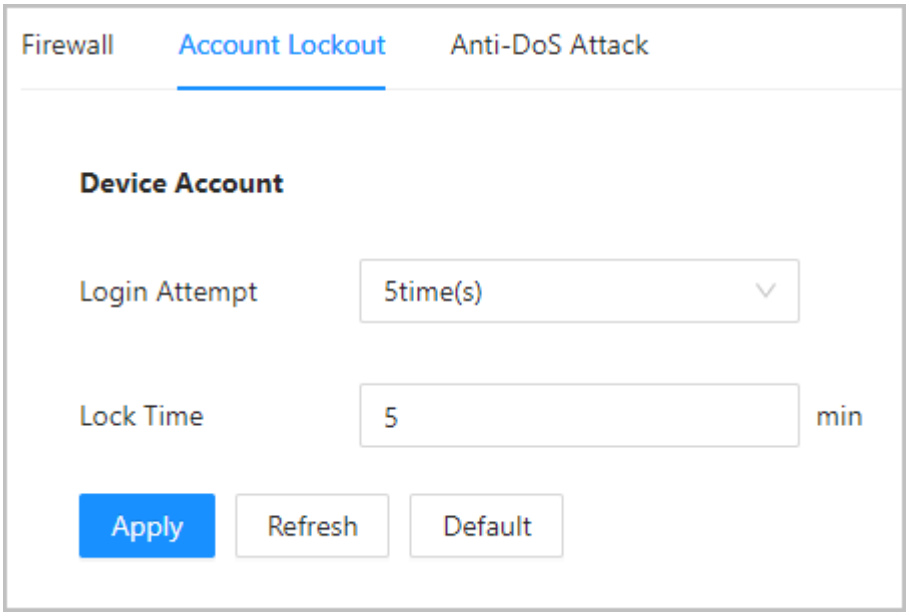
If the incorrect password is entered for a defined number of times, the account will be locked.

Procedure

Step 1 Select > **Attack Defense** > **Account Lockout**.

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

Figure 3-7 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**.

3.3.3.3 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 Select > **Attack Defense** > **Anti-DoS Attack**.

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

Figure 3-8 Anti-DoS attack

Step 3 Click **Apply**.

3.3.4 Installing Device Certificate

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

3.3.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

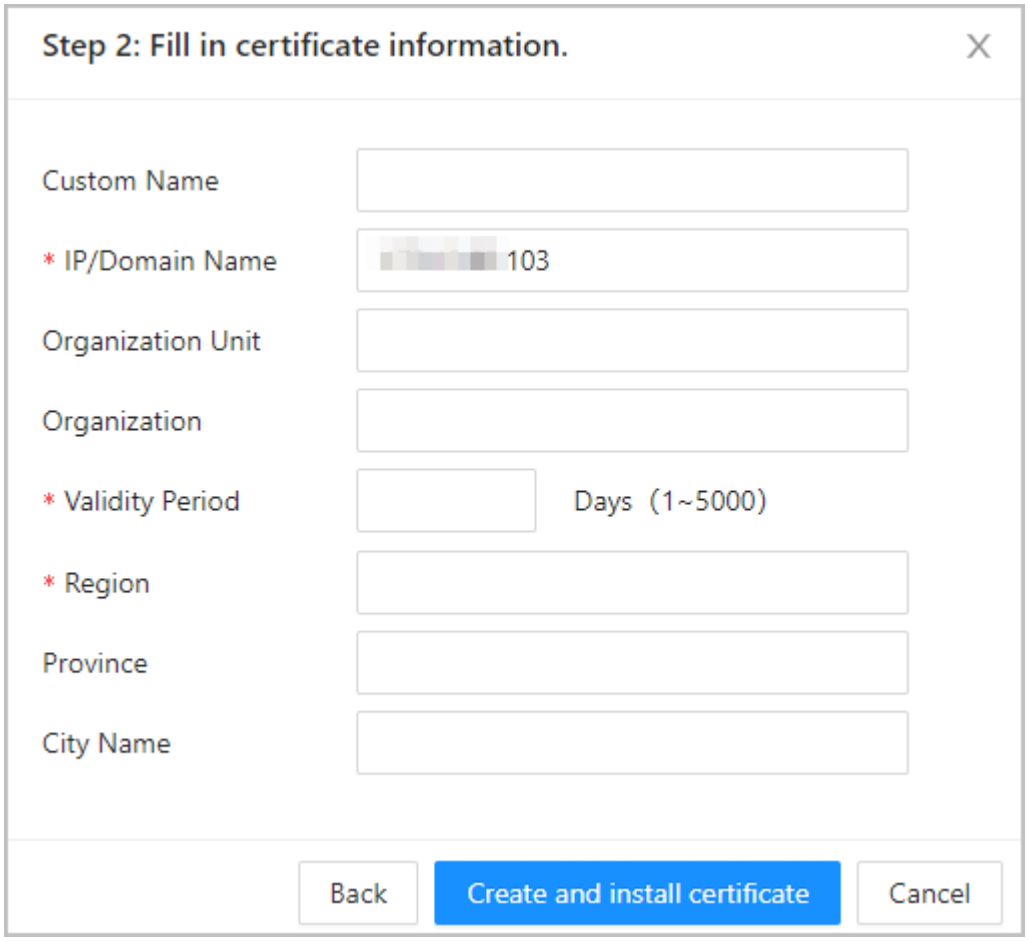
Step 1 Select > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Device Certificate**.

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

Step 4 Enter the certificate information.

Figure 3-9 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.

3.3.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Device.

Procedure

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

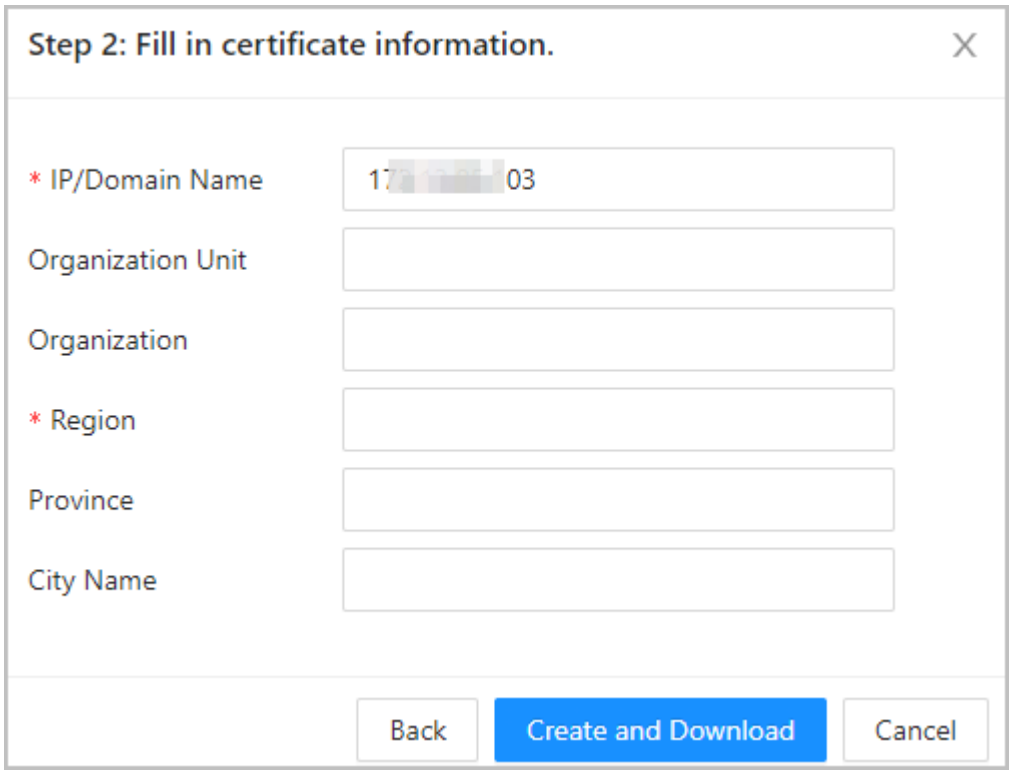
Step 2 Click **Install Device Certificate**.

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 3-10 Certificate information



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 other 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.

3.3.4.3 Installing Existing Certificate

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

Procedure

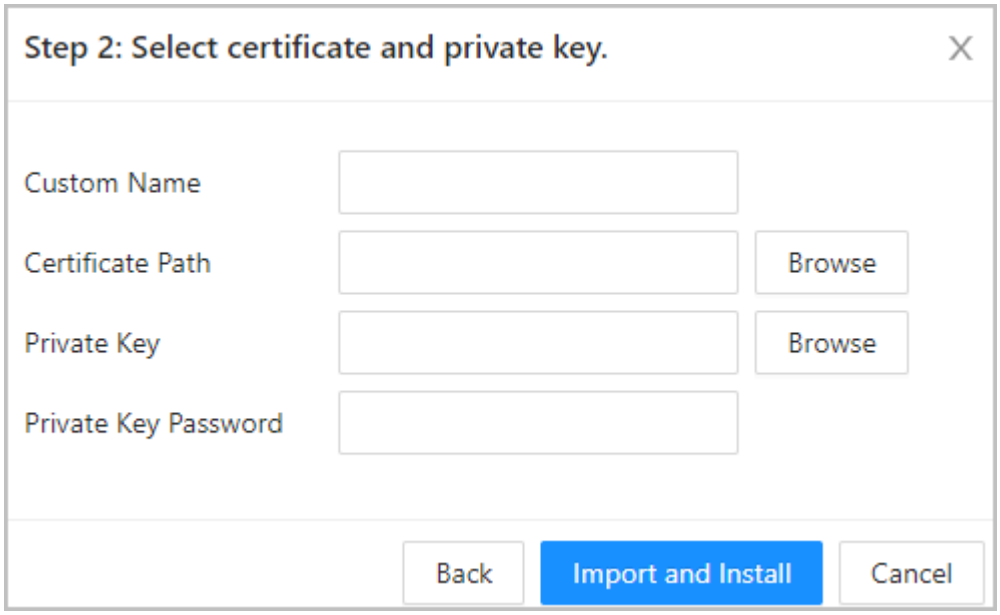
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

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 3-11 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.

3.3.5 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 the user access to the network.

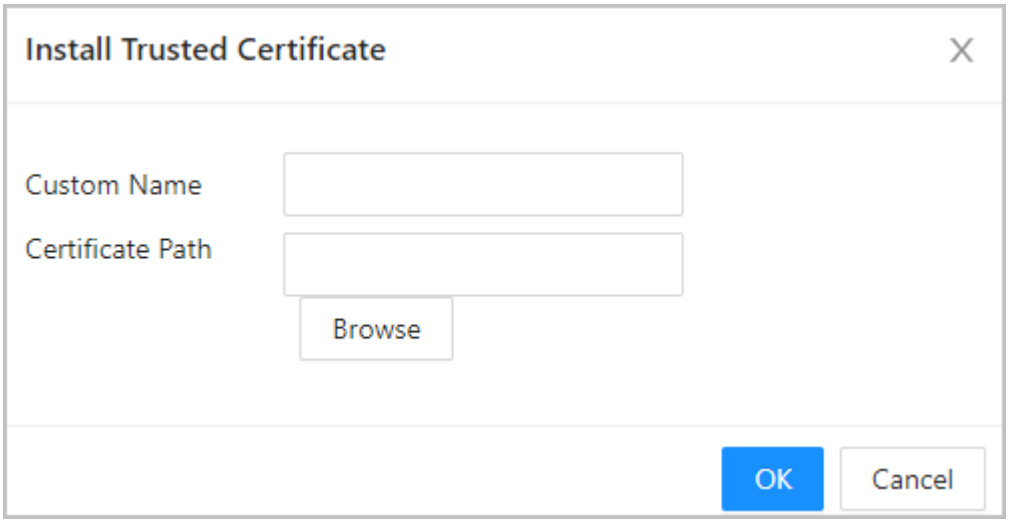
Procedure

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

Step 2 Select **Install Trusted Certificate**.

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

Figure 3-12 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.

3.3.6 Security Warning

Procedure

Step 1 Select > **Security Warning**.

Step 2 Enable the security warning function.

Step 3 Click **Apply**.

3.3.7 Security Authentication

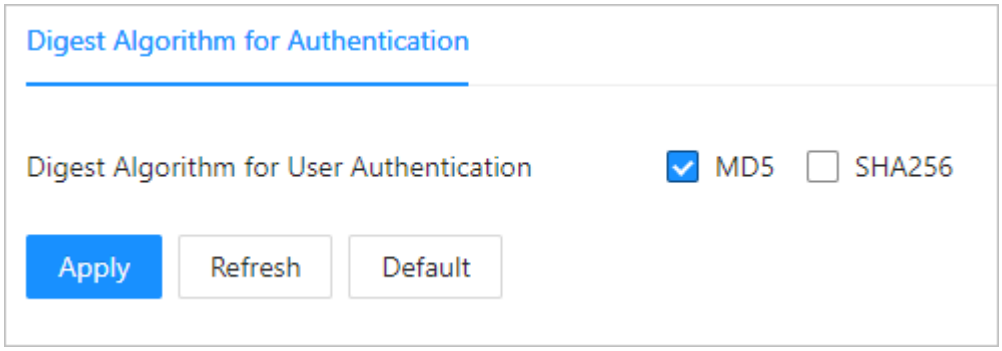
Procedure

Step 1 Select > **Security Authentication**.

Step 2 Select a message digest algorithm.

Step 3 Click **Apply**.

Figure 3-13 Security Authentication

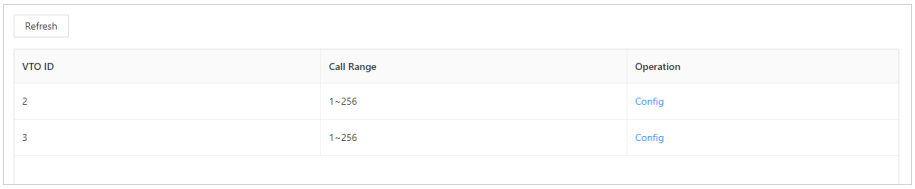


3.4 VTO Configuration

Log in to the webpage of the 2-wire controller. The system displays the VTO connected to the current controller and the VTO connected to cascading controllers.

- Click **Config** to finish the detailed configuration of the VTO.
- **Call Range** : The number range that the VTO can call. You cannot call the number that beyond this call range. The range is generated according to the configured DIP on the 2-wire controller. If the call range fails to be generated and displays red -, please configure the DIP on the 2-wire controller again.

Figure 3-14 VTO



3.4.1 Personnel Management

Manage and view the information of the people, cards, passwords and fingerprints.

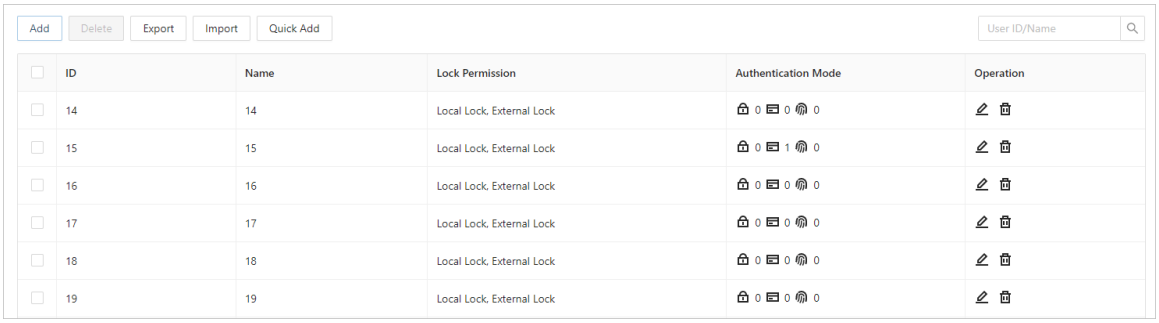
Procedure

Step 1 Log in to the webpage.

Step 2 Click **Config** next to the corresponding VTO.

Step 3 Select **Person Management**.

Figure 3-15 Person management



Step 4 Click **Add**.

Step 5 Configure the parameters, and then click **Add**.

Figure 3-16 Add the person

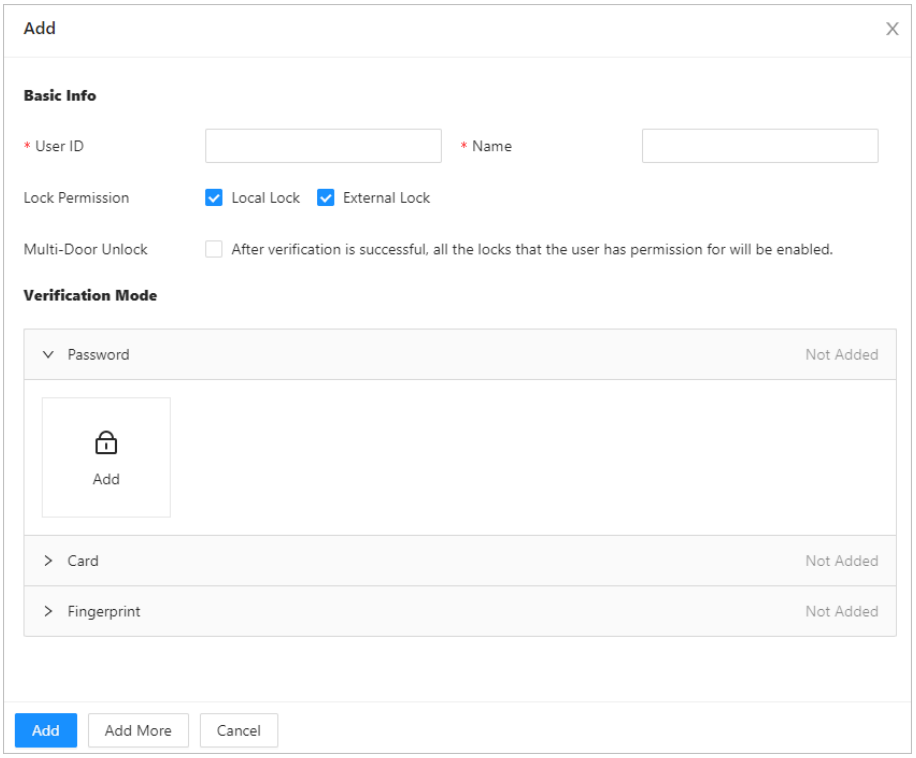


Table 3-2 Parameters description of adding person

Parameter	Description
User ID	Enter the user ID and the name. The user ID cannot be the same as the existing ID.
Name	
Lock Permission	Select the lock permission. ● Local Lock: Local lock. ● External Lock: RS-485 lock.
Multi-Door Unlock	If enabled, after verification is successful, all the locks that the user has permission for will be enabled.

Parameter	Description
Verification Mode	Add the password, card or fingerprint. ● Password: Select **Password** > **Add**, enter the password, confirm the password, and then click **OK**. ● Card: Select **Card** > **Add**, swipe the card or enter the card number, and then click **Add**. Click **Modify** to change the card reading device. If you select **Enrollment Reader**, you need to select the card type from IC card and ID card. ● Fingerprint: Select **Fingerprint** > **Add**, press your finger on the scanner 3 times continuously, and then click **Add**. Click **Modify** to change the recognition device.

Related Operations

- Add person quickly.
  1. Click **Quick Add**.
  2. Configure the user ID number that you want to start from, enter the total quantity.
  3. Configure the lock permission and multi-door unlock.
  4. Select **Card** > **Add**, swipe the card or enter the card number, and then click **Add**.

     Click **Modify** to change the card reading device. If you select **Enrollment Reader**, you need to select the card type from IC card and ID card.
  5. Click **Add**.
- Delete, export or import the people information.

  When exporting the people information, you can configure the file password. Enter the password when you import the information file to other VTOs.

3.4.2 VTH Room Number Mapping

You can set the dial-up number for the corresponding VTH ID. After mapping, call the VTH only through the configured number.

The VTH room number mapping function is only valid when the keyboard module is connected.

Procedure

Step 1 Log in to the webpage.

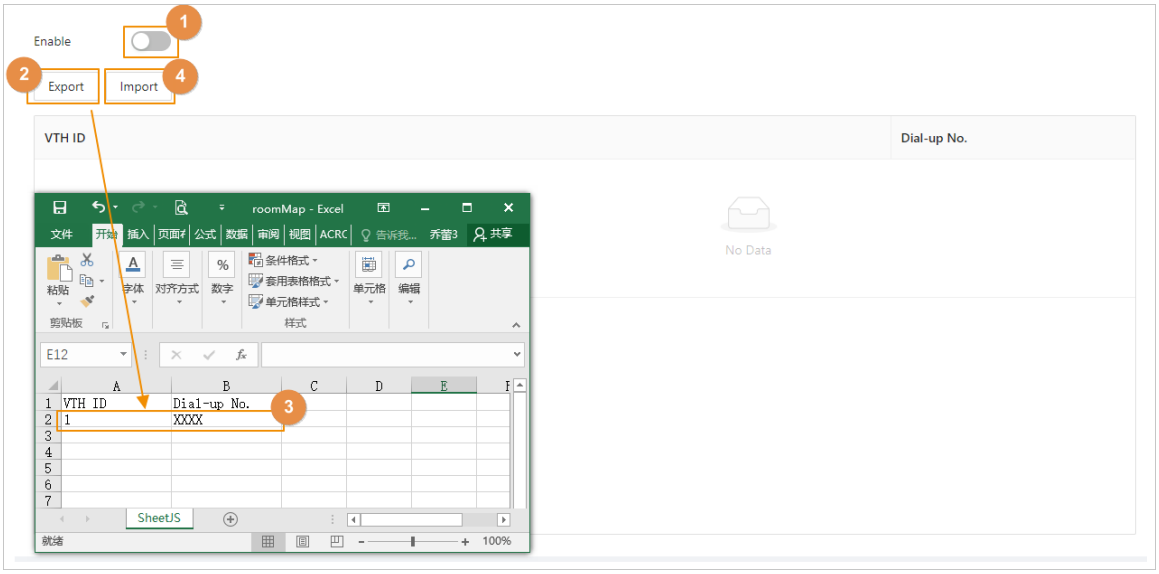
Step 2 Click **Config** next to the corresponding VTO.

Step 3 Select **Room No. Mapping**, and then configure the mapping.

1. Enable the function.
2. Click **Export** to download the template.
3. Enter the VTH ID and configure the corresponding dial-up number, and then save the template.
4. Click **Import** to upload the file.

The configured dial-up numbers will be displayed on the system.

Figure 3-17 Mapping



3.4.3 Access Control

3.4.3.1 Config

Procedure

Step 1 Log in to the webpage.

Step 2 Click **Config** next to the corresponding VTO.

Step 3 Select **Access Control** > **Config**.

Step 4 Configure the parameters.

Figure 3-18 Access control

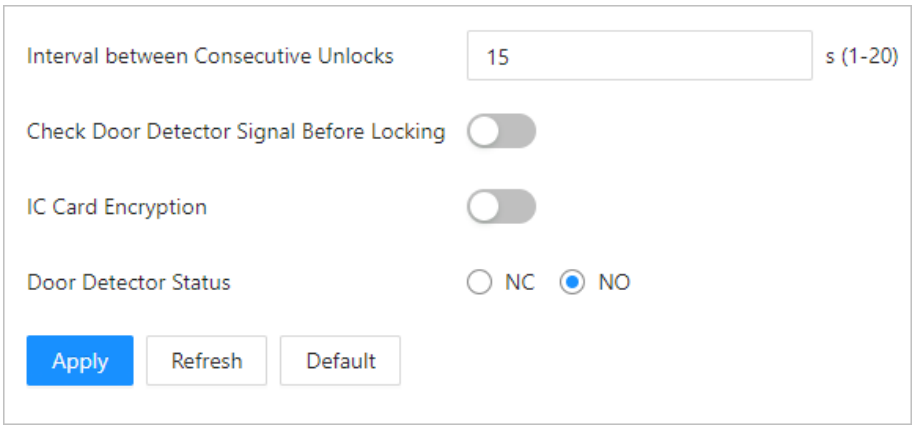


Table 3-3 Access control parameter description

Parameter	Description
Interval between Consecutive Unlocks	The door can only be unlocked again after the interval.

Parameter	Description
Check Door Detector Signal Before Locking	Enable the function as needed. If enabled, the door detector status will be detected before locking to avoid the opening door.
IC Card Encryption	Enable the function so that the IC card encryption takes effect.
Door Detector Status	• **NC** : Normally closed. • **NO** : Normally open.

Step 5 Click **Apply**.

3.4.3.2 RS-485

Procedure

Step 1 Log in to the webpage.

Step 2 Click **Config** next to the corresponding VTO.

Step 3 Select **Access Control** > **RS-485**.

Step 4 Configure the parameters of the lock connected through the RS-485 port.

Figure 3-19 RS-485

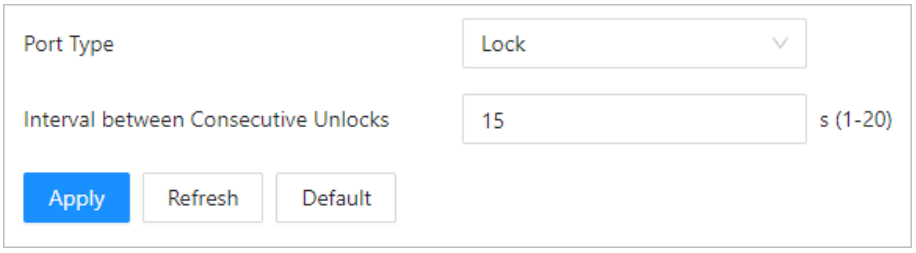


Table 3-4 RS-485 description

Parameter	Description
Port Type	• **Lock** : Connects to external lock. It is selected by default. • **Card Reader** : Connects to external card reader. • **Alarm** : Connects to 485_IO module.
Interval between Consecutive Unlocks	The door can only be unlocked again after the interval.

Here uses **Alarm** as the port type as an example.

Enable **Expand Call Buttons**, and then configure the parameters.

Figure 3-20 Port type: alarm

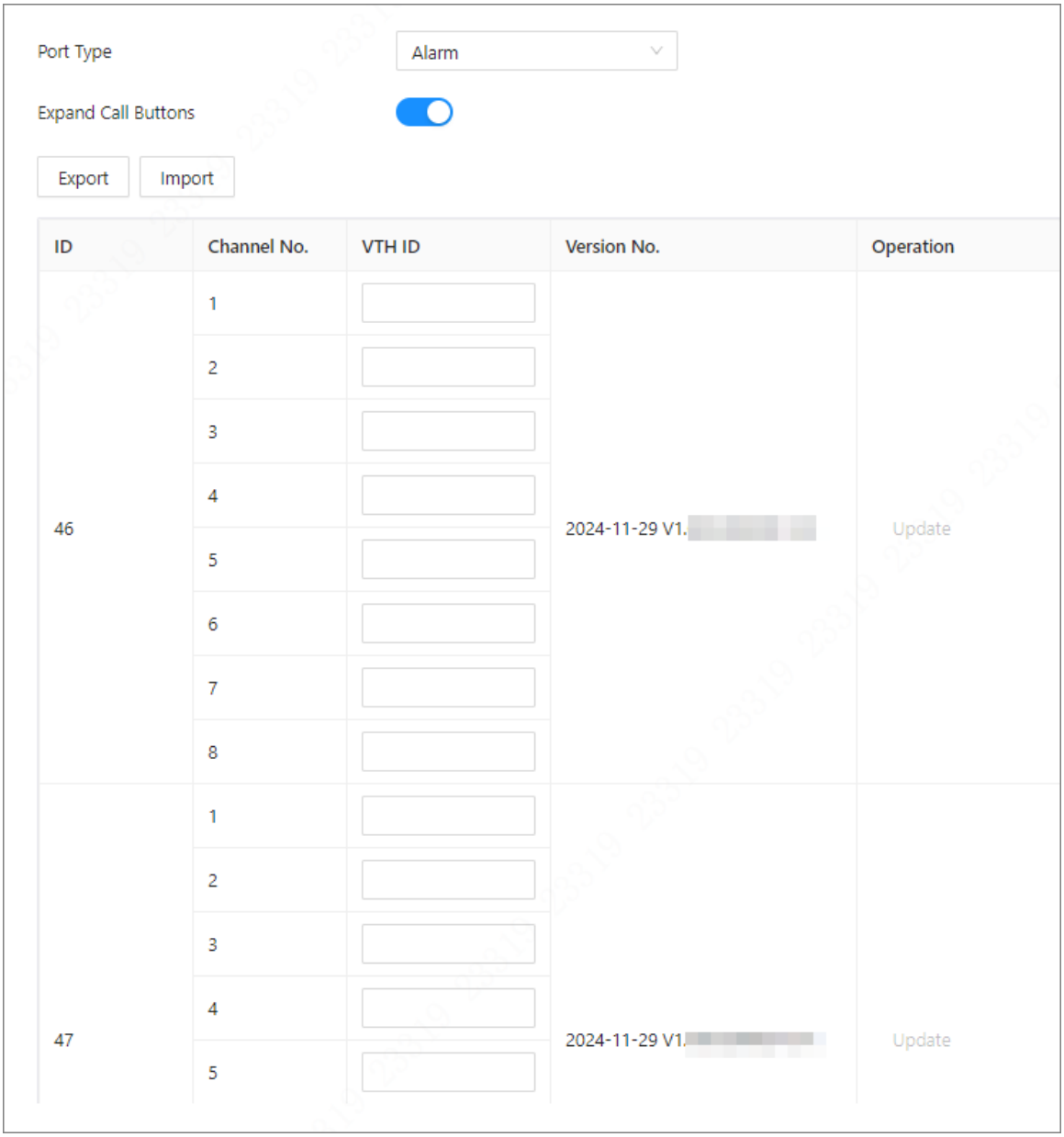


Table 3-5 RS-485 description

Parameter	Description
Export/Import	Click **Export** /**Import** to export/import the configurations in batches.
ID	The ID number of module.
Channel No.	The number of alarm input channel module.
VTH ID	The ID number of VTH. After the VTH ID is configured, if the alarm input of the channel is triggered, the VTO will call the VTH with the corresponding ID.
Version No.	The software version number of module.

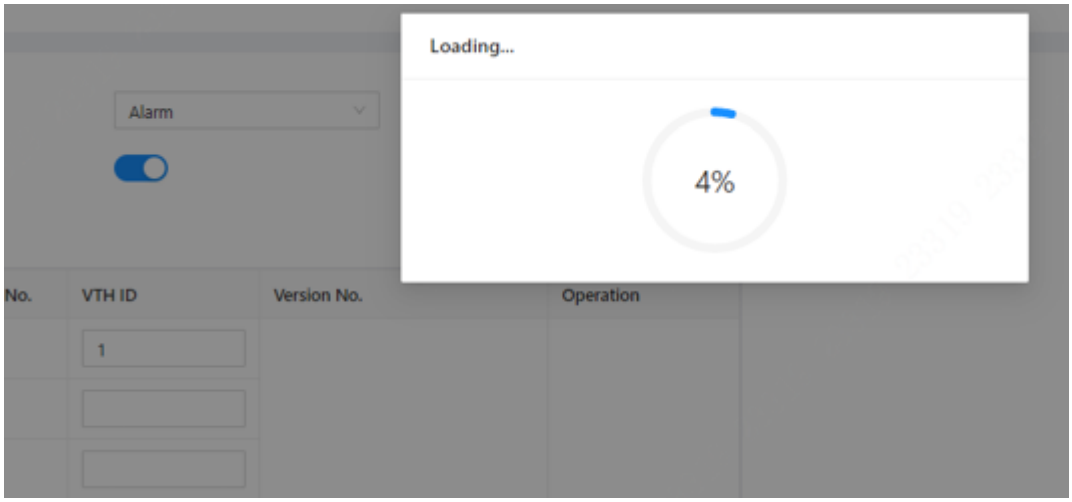
Parameter	Description
Operation	• If the software version is not latest, click **Update** to update the software version to the latest. • If the software version is latest, the button of **Update** is in grey and cannot be selected.

- The VTO supports cascading up to twenty 485_IO modules.
- 485_IO modules need to be configured as input mode. For details, see its user's manual.

Step 5 Click **Apply**.

When you select **Alarm** as the port type, you need to wait for a while until the 485_IO modules are automatically configured. The wait time is related to the number of connected modules.

Figure 3-21 Loading



3.4.4 Module

View the VTO, all the cascading modules and version information. Update the VTO and the modules. Customize the calling number.

Procedure

Step 1 Log in to the webpage.

Step 2 Click **Config** next to the corresponding VTO.

Step 3 Select **Module**, and then you can view the VTO and all the cascading modules.

Figure 3-22 Module

- 1: Click to view the current version information. If the current version is not the latest, click **Browse** to select the updating file, and then click **Update** to update the version to latest.
- 2: The number on the module is the ID number of target VTH, which is editable. The numbers are increasing from the top to the bottom according to the cascading order by default.

3.4.5 Maintenance

Procedure

Step 1 Log in to the webpage.

Step 2 Click **Config** next to the corresponding VTO.

Step 3 Select **Maintenance**.

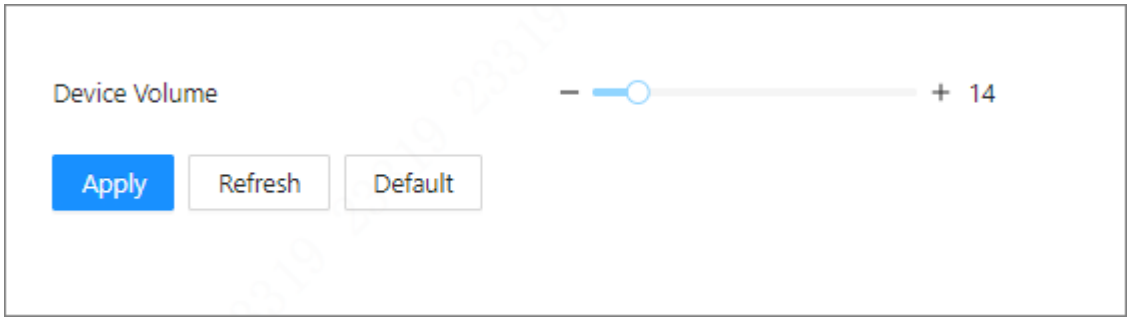
- Click **Factory Default** to restore to default settings.
- Click **Restart** to restart the controller.

3.4.6 Audio

Configure the device volume of VTO (excluding intercom volume).

Move the slider left and right to adjust the volume, with 0 indicating silence while 100 the largest volume.

Figure 3-23 Device volume



3.5 Adding Person

Add the person and send the information to VTO.

Procedure

Step 1 Log in to the webpage.

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

Figure 3-24 Adding person

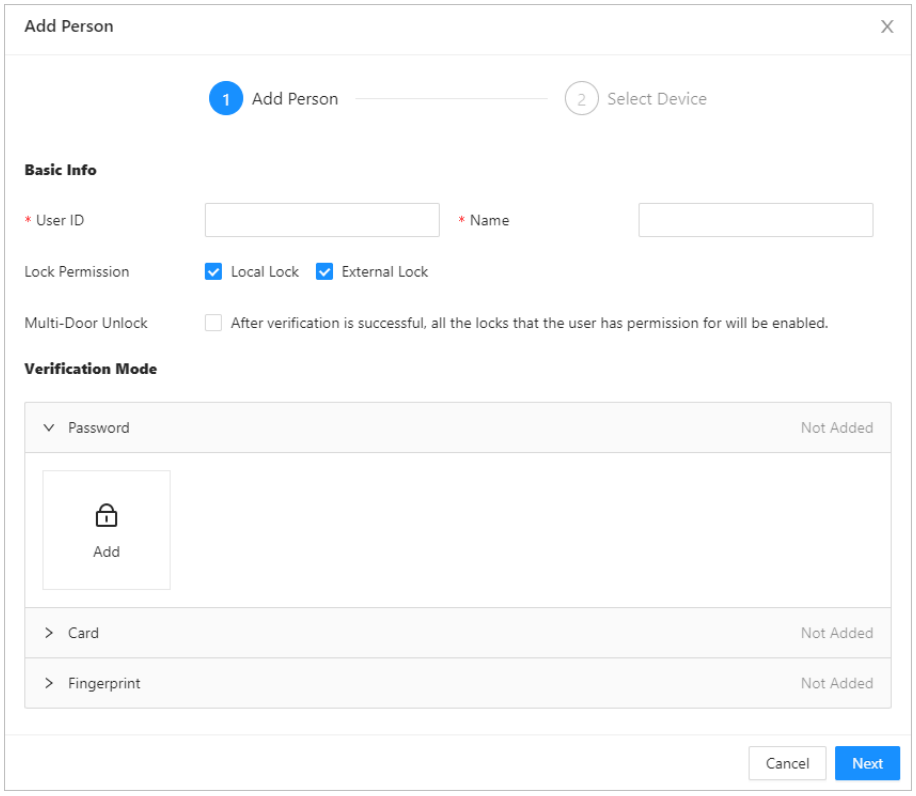


Table 3-6 Parameters description of adding person

Parameter	Description
User ID	Enter the User ID and the name.
Name	The user ID cannot be the same as the existing ID.

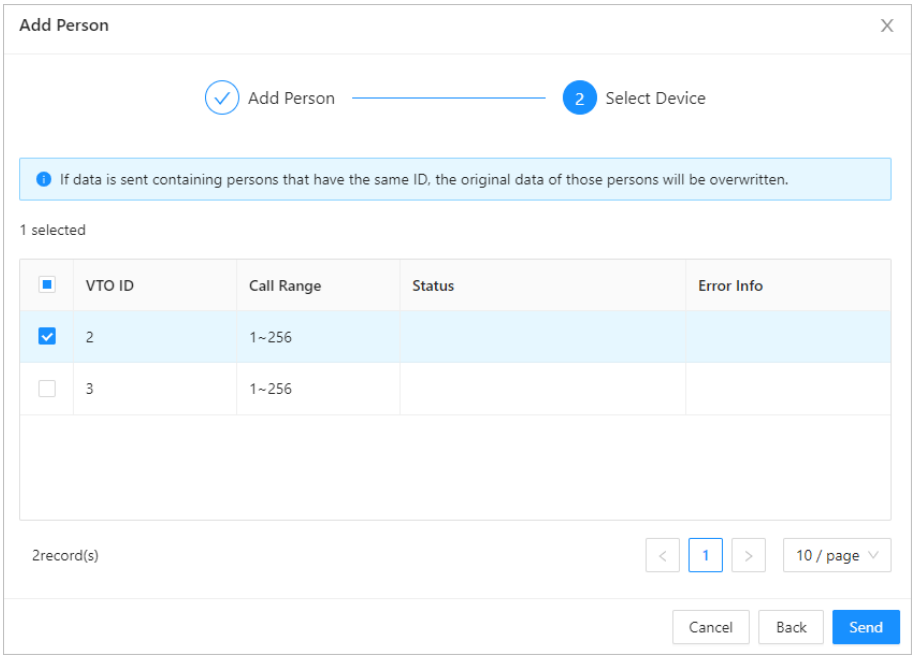
Parameter	Description
Lock Permission	Select the lock permission. ● Local Lock: Local lock. ● External Lock: RS-485 lock.
Multi-Door Unlock	If enabled, after verification is successful, all the locks that the user has permission for will be enabled.
Verification Mode	Add the password, card or fingerprint. ● Password: Select **Password** > **Add**, enter the password, confirm the password, and then click **OK**. ● Card: Select **Card** > **Add**, swipe the card or enter the card number, and then click **Add**. Click **Modify** to change the card reading device and the card type. ● Fingerprint: Select **Fingerprint** > **Add**, press your finger on the scanner 3 times continuously, and then click **Add**. Click **Modify** to change the recognition device.

Step 3 Click **Next**.

Step 4 Select the device, and then click **Send**.

The person information will be sent to the VTO that you selected.

Figure 3-25 Select the VTO



3.6 Importing Persons in Batches

After exporting the person information from the VTO, you can upload the file to import persons in batches to other VTOs.

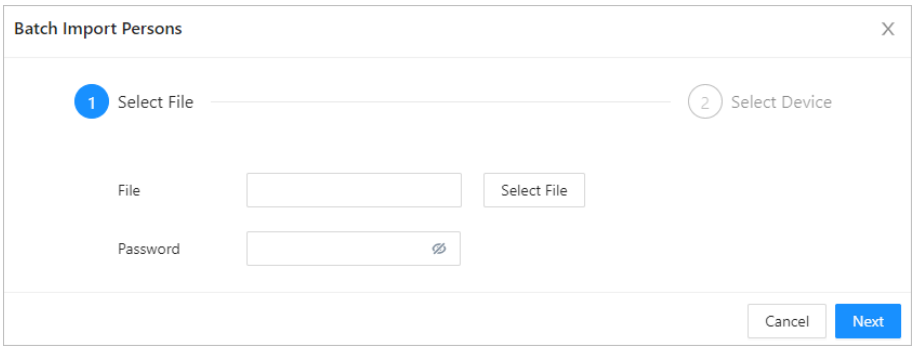
Procedure

Step 1 Log in to the webpage.

Step 2 Click **Batch Import Persons**.

Step 3 Select the file, enter the password that is configured when exporting the information, and then click **Next**.

Figure 3-26 Import people



Step 4 Select the device, and then click **Send**.

The person information will be sent to the VTO that you selected.

3.7 Network Settings

3.7.1 Configuring TCP/IP

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

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Network Settings** > **TCP/IP**.

Step 3 Configure the parameters.

Figure 3-27 TCP/IP

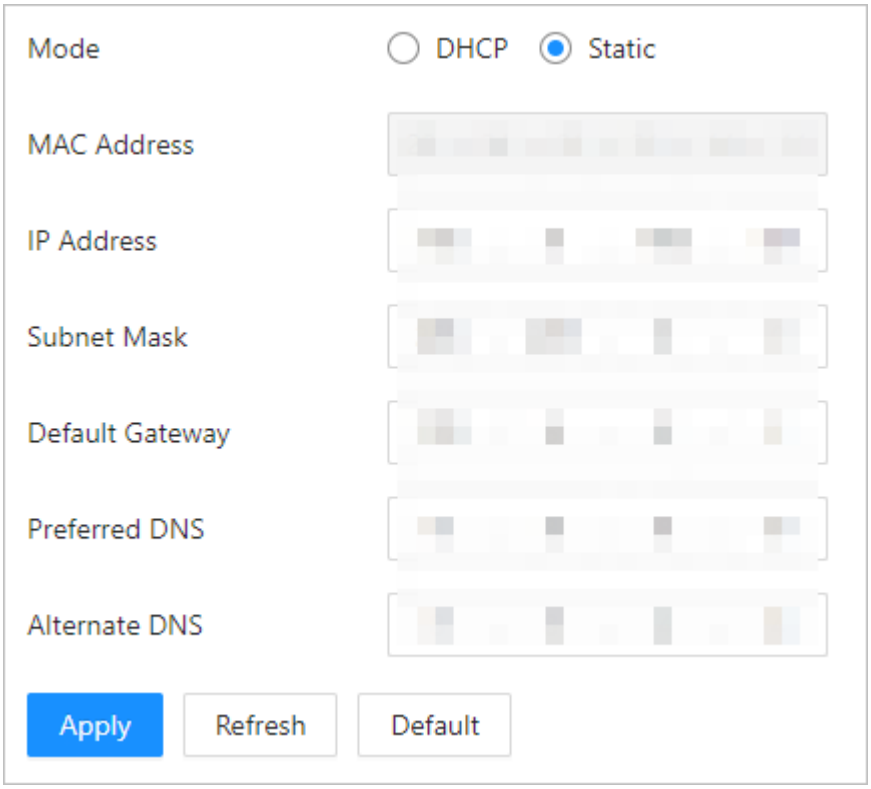


Table 3-7 Description of TCP/IP parameters

Parameter	Description
Mode	• **DHCP** (Dynamic Host Configuration Protocol): The Device will automatically be assigned with IP address, subnet mask, and gateway. • **Static** : Manually enter IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
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.

Step 4 Click **Apply**.

3.7.2 Configuring Basic Services

Log in to the webpage, and then select **Network Settings** > **Basic Services**.

Enable the protocol as needed, and then click **Apply**.

Figure 3-28 Basic services

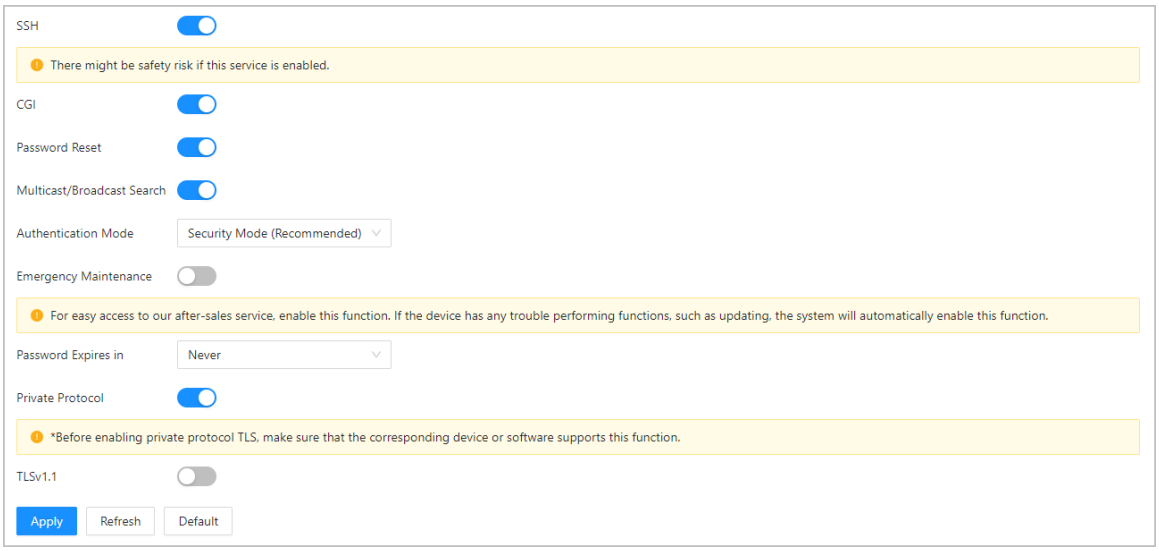


Table 3-8 Description of basic services

Service	Description
SSH	If enabled, you can log in to the VTO through SSH.
CGI	Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similarly to console applications running on a server that dynamically generates web pages. If enabled, CGI commands can be used. The CGI is enabled by default.
Password Reset	Enabled by default. Enable the function, and then configure the email address. After configuration, you can click **Forget Password?** on the login page to reset the password.
Multicast/Broadcast Search	Enable this function, and then when multiple users are previewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
Authentication Mode	• **Security Mode (Recommended)** : The mode does not support logging in with Digest, DES and plain text authentication. • **Compatibility Mode** : The mode supports logging in with Digest, DES and plain text authentication.
Emergency Maintenance	When this function is enabled, if the device fails to restart 5 times in a row, it will automatically turn on a service port used by technical support to perform upgrades and recovery.
Password Expires in	Select the time that the password will expire in.
Private Protocol	If enabled, the platform can access to the device with private protocol.
TLSv1.1	⚠ There is security risk if you enable **TLSv1.1**.

3.8 Maintenance Center

3.8.1 One-click Diagnosis

The system automatically diagnoses the configurations and the status of the device to improve its performance.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **One-click Diagnosis**.

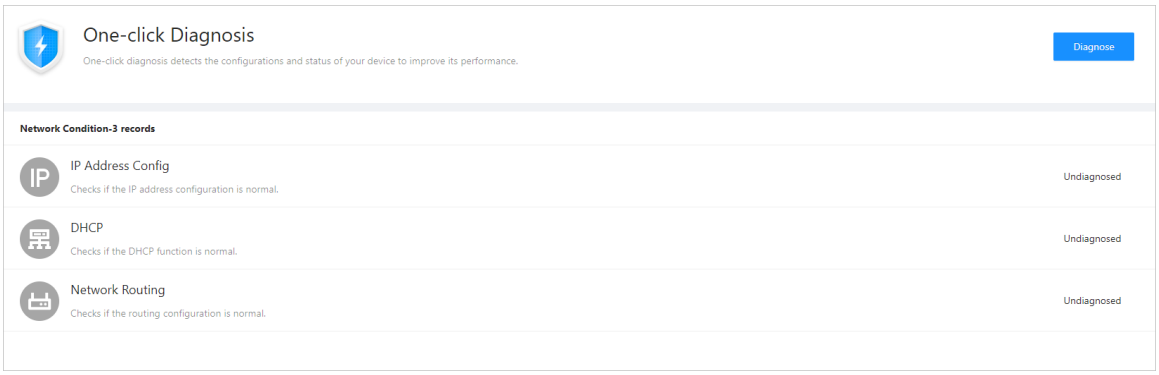
Step 3 Click **Diagnose**.

The system automatically diagnoses the configurations and the status of the device and displays diagnosis results after it completes.

Step 4 (Optional) Click **Details** to view details of abnormal items.

You can ignore the abnormality or optimize it. You can also click **Diagnose Again** to perform automatic diagnosis again.

Figure 3-29 One-click diagnosis



3.8.2 System Information

Log in to the webpage, select **Maintenance Center** > **System Info**, and you can view the open source software notice.

Select **Legal Info** to view the open source software notice.

Select **System Info** to view the version information of the controller.

3.8.3 Exporting and Importing Configuration Files

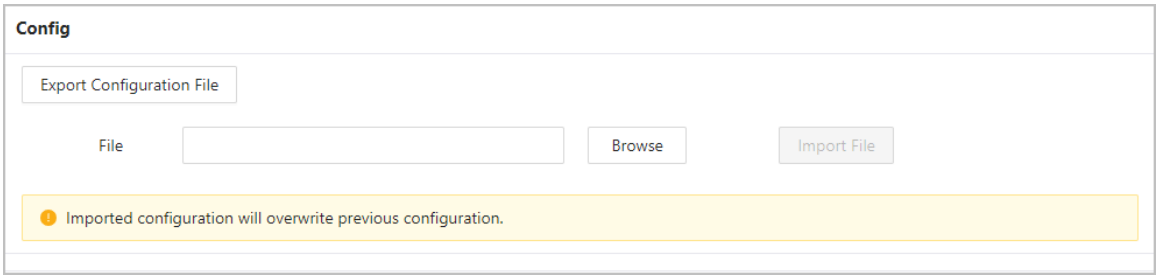
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Config**.

Figure 3-30 Configuration management



Step 3 Export or import configuration files.

- 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.

3.8.4 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.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Update**.

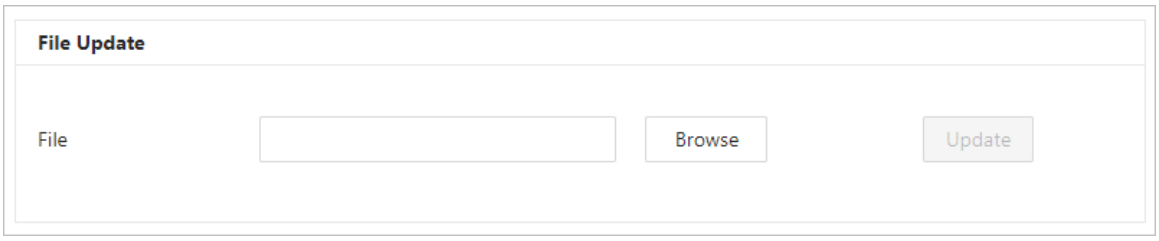
Step 3 In the **File Update** area, click **Browse**, and then upload the update file.

The update file should be a .bin file.

Step 4 Click **Update**.

The 2-wire controller will restart after the update finishes.

Figure 3-31 File update



3.8.5 Advanced Maintenance

Acquire device information and capture packet to make it easier for maintenance personnel to perform troubleshooting.

3.8.5.1 Exporting

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Advanced Maintenance** > **Export**.

Step 3 Click **Export** to export the serial number, firmware version, device operation logs and configuration information.

3.8.5.2 Packet Capture

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Figure 3-32 Packet Capture

Step 3 Enter the IP address, click ▶.

▶ changes to ⏸.

Step 4 After you acquired enough data, click ⏸.

Captured packets are automatically downloaded to your local computer.

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 Allowlist**

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