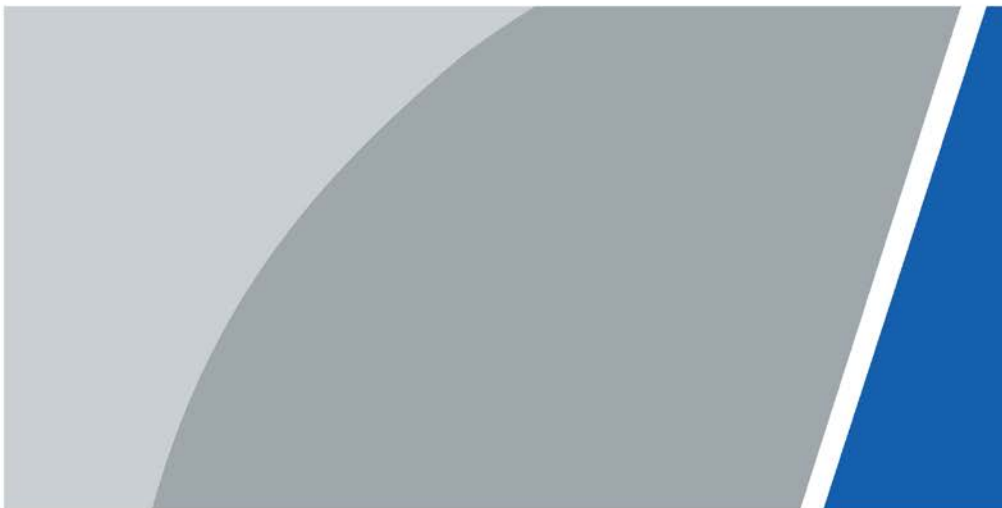


Web Access Controller

User's Manual



V1.0.0






Foreword

General

This manual introduces the functions and operations of the Access 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.
 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 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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 Access Controller, hazard prevention, and prevention of property damage. Read carefully before using the Access Controller, and comply with the guidelines when using it.

Transportation Requirement



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

Storage Requirement



Store the Access Controller under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the Access 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 Access Controller.
- Do not connect the Access Controller to two or more kinds of power supplies, to avoid damage to the Access Controller.
- Improper use of the battery might result in a fire or explosion.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Access Controller in a place exposed to sunlight or near heat sources.
- Keep the Access Controller away from dampness, dust, and soot.
- Install the Access Controller on a stable surface to prevent it from falling.
- Install the Access 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 power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Access Controller label.
- The Access Controller is a class I electrical appliance. Make sure that the power supply of the Access Controller is connected to a power socket with protective earthing.

Operation Requirements



- Check whether the power supply is correct before use.

- Do not unplug the power cord on the side of the Access Controller while the adapter is powered on.
- Operate the Access Controller within the rated range of power input and output.
- Use the Access Controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Access Controller, and make sure that there is no object filled with liquid on the Access Controller to prevent liquid from flowing into it.
- Do not disassemble the Access Controller without professional instruction.

Table of Contents

Foreword	I
Important Safeguards and Warnings.....	III
1 Product Overview	1
1.1 Product Introduction.....	1
1.2 Main Features.....	1
1.3 Application Scenarios	1
2 Main Controller-Sub Controller.....	3
2.1 Networking Diagram	3
2.2 Configurations on Main Controller	3
2.2.1 Configuration Flowchart.....	3
2.2.2 Initialization.....	3
2.2.3 Logging In	5
2.2.4 Dashboard	9
2.2.5 Homepage	10
2.2.6 Adding Devices.....	11
2.2.6.1 Adding Individually	11
2.2.6.2 Adding in Batches	13
2.2.7 Adding Users.....	13
2.2.8 Adding Time Templates	16
2.2.9 Adding Area Permissions	18
2.2.10 Assigning Access Permissions	19
2.2.10.1 Assigning Permissions Individually.....	19
2.2.10.2 Assigning Permissions in Batches.....	20
2.2.11 Viewing Authorization Progress	21
2.2.12 (Optional) Configuring Access Control.....	22
2.2.12.1 Configuring Basic Parameters.....	22
2.2.12.2 Configuring Unlock Methods	23
2.2.12.3 Configuring Alarms	25
2.2.13 (Optional) Configuring Global Alarm linkages	25
2.2.14 (Optional) Local Device Configurations	27
2.2.14.1 Configure Local Alarm Linkages	27
2.2.14.2 Configuring Card Rules.....	28
2.2.14.3 Backing up System Logs	29
2.2.14.4 Configuring Network	30
2.2.14.4.1 Configuring TCP/IP	30
2.2.14.4.2 Configuring Port	31

2.2.14.4.3	Configuring Cloud Service	32
2.2.14.4.4	Configuring Automatic Registration	33
2.2.14.4.5	Configuring Basic Service	33
2.2.14.5	Configuring Time	34
2.2.14.6	Account Management	36
2.2.14.6.1	Adding Users	36
2.2.14.6.2	Resetting Password	37
2.2.14.6.3	Adding ONVIF Users	37
2.2.14.7	Maintenance	38
2.2.14.8	Advanced Management	39
2.2.14.8.1	Exporting/Importing Configuration Files	39
2.2.14.8.2	Configuring Card reader	40
2.2.14.8.3	Configuring Fingerprint Level	40
2.2.14.8.4	Restoring Factory Defaults	40
2.2.14.9	Updating System	41
2.2.14.9.1	File Update	41
2.2.14.9.2	Online Update	41
2.2.14.10	Configuring Hardware	41
2.2.14.11	Viewing Version Information	42
2.2.14.12	Viewing Legal Information	42
2.2.15	Viewing Records	42
2.2.15.1	Viewing Alarm Records	42
2.2.15.2	Viewing Unlock Records	43
2.2.16	Security	43
2.2.16.1	Security Status	43
2.2.16.2	Configuring HTTPS	44
2.2.16.3	Attack Defense	45
2.2.16.3.1	Configuring Firewall	45
2.2.16.3.2	Configuring Account Lockout	46
2.2.16.3.3	Configuring Anti-DoS Attack	47
2.2.16.4	CA Certificate	48
2.2.16.4.1	Installing Device Certificate	48
2.2.16.4.2	Installing Trusted CA Certificate	51
2.2.16.5	Security Warning	52
2.2.17	Access Monitoring	52
2.2.17.1	Remotely Opening and Closing Door	52
2.2.17.2	Setting Always Open and Always Close	53
2.3	Configurations on Sub Controller	53
2.3.1	Initialization	53

2.3.2 Logging In 54

2.3.3 Home Page 54

3 Smart PSS Lite-Sub Controllers 55

3.1 Networking Diagram 55

3.2 Configurations on SmartPSS Lite 55

3.3 Configurations on Sub Controller 55

Appendix 1 Cybersecurity Recommendations 56

1 Product Overview

Flexible and convenient, ASC3 Series Access Controller has a user friendly system that allows you to access controllers on the webpage through IP address. It comes with a professional access management system, and makes the networking of main and sub control modes quick and easy, meeting the needs of small and advanced systems.

1.1 Product Introduction

Flexible and convenient, Access Controller has a user friendly system that allows you to access controllers on the webpage through IP address. It comes with a professional access management system, and makes the networking of main and sub control modes quick and easy, meeting the needs of small and advanced systems.

1.2 Main Features

- Built of flame-retardant PC and ABS material, it is both sturdy and elegant with an IK06 rating.
- Supports TCP and IP connection, and standard PoE.
- Accesses card readers through Wiegand and RS-485 (OSDP) protocols.
- Supplies power to the lock through its 12 VDC output power supply, which has a maximum output current of 1000 mA.
- Supports 1000 users, 5000 cards, 3000 fingerprints, and 300,000 records.
- Multiple unlock methods including IC card, password, fingerprint and more. You can also combine these methods to create your own personal unlock methods.
- Multiple types of alarms events are supported, such as duress, tampering, intrusion, unlock timeout, and illegal card.
- Supports a wide range of users including general, patrol, VIP, guest, blocklisted, and more users.
- Manual and automatic time synchronization.
- Retains stored data even while powered off.
- Offers a variety functions and the system can be configured. Devices can also be updated through the webpage.
- Features main and sub control modes. The main control mode offers user management, access control device management and configuration, and more options. Devices under sub-control modes can be added to multiple platforms.
- A main controller can connect with and manage up to 19 sub controllers.
- Watchdog protects the system to allow the device to be stable and perform efficiently.
- Sub controllers can be added to SmartpssLite, DSS Pro and DMSS.

1.3 Application Scenarios

It is widely used in parks, communities, business centers and factories, and ideal for places such as

office buildings, government buildings, schools and stadiums.

There are two different networking methods available for the web access controller. You can select a networking method based on your needs.

Table 1-1 Networking methods of access controller

Networking methods	Description
Main Controller—Sub Controller	The main controller comes with a management platform. Sub controllers need to be added to the management platform of the main controller. The main controller can manage up to 19 sub controllers. For details, see "2 Main Controller-Sub Controller".
SmartPSS Lite—Sub Controller	Sub controllers needs to be added to a standalone management platform (SmartPSS Lite). The platform can manage up to 32 sub controllers. For details, see "3 Smart PSS Lite-Sub Controllers".

Controller is restored to the factory defaults.

Prerequisites

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

Background Information

Set a password and an email address before logging in to the webpage for the first time.

Step 1 Open a browser, go to the IP address (the default address is 192.168.1.108) of the Access Controller.



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

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

Step 3 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, lower case, 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 4 Configure the system time, and then click **Next**.

Figure 2-3 Configure time

Date Format	YYYY-MM-DD
Time Zone	(UTC+08:00) Beijing, Chongqing, Hong ...
System Time	2022/06/21 16:09:58 Sync PC

Next

Step 5 (Optional) Select **Auto Check for Updates**, and then click **Completed**.

The system automatically check is there any higher version available, and inform the user to update the system.

Step 6 Click **Completed**

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

2.2.3 Logging In

For the first-time login after successful initialization, you need to follow the login wizard to configure the type and hardware of the main controller.

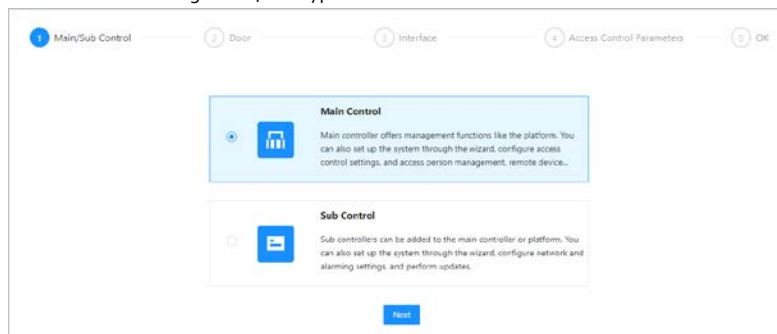
Step 1 On the login page, enter the username and password.



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

Step 2 Select **Main Control**, and then click **Next**.

Figure 2-4 The type of the access controller



- Main control: The main controller comes with a management platform. You can manage all sub controllers, configure access control, and access personal management on the platform, and more.
- Sub Control: Sub controller needs to be added to the management platform of the main controller or other management platforms such as DSS Pro or SmartPss Lite. You can only perform the local configurations on the webpage of the sub controller.

Step 3 Select the number of doors, and then enter the name of the door.

Step 4 Configure the parameters of doors.

Figure 2-5 Configure door parameters

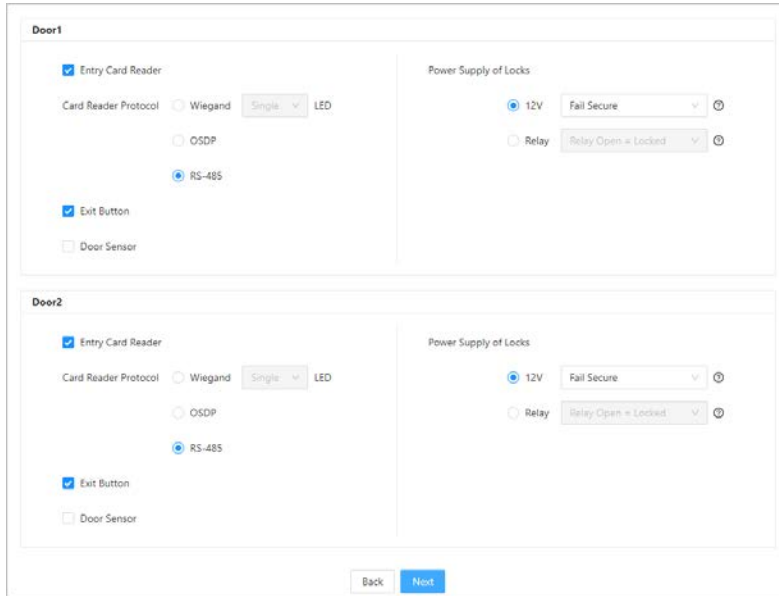


Table 2-1 Parameter descriptions

Parameter	Description
Entry Card Reader	<p>Card Reader Protocol.</p> <ul style="list-style-type: none"> Wiegand: Connects to a Wiegand reader. You can connect the LED wire to the LED port of the controller, and the reader will beep and flash when the door unlocks. OSDP: Connects to a OSDP reader. RS-485: Connects to a OSDP reader.
Exit Button	Connects to a exit button.
Door Sensor	Connects to a door sensor.
Power Supply of Locks	<ul style="list-style-type: none"> 12 V: The controller provides power for the lock. <ul style="list-style-type: none"> Fail secure: When the power is interrupted or fails, the door stays locked Fail safe: When the power be interrupted or fail, the door automatically unlocks or releases to let people out of the space. Relay: The relay supplies power for the lock. <ul style="list-style-type: none"> Relay open=locked: Sets the lock to remain locked when the relay is open. Relay open=locked: Sets the lock to unlock when

Step 5 Configure access control parameters.

Step 6 In the **Unlock Settings** area, select an unlock mode.

- Combination Unlock
 - Select **Combination Unlock** form the **Unlock Method** list.

2. Select **Or** or **And**

- ◊ Or: Verify one of the selected unlocking methods to open the door.
- ◊ And: Verify all the selected unlocking methods to open the door.

The Controller supports unlock through card, fingerprint or password.

3. Select unlock methods, and then configure other parameters.

Figure 2-6 Element (multiple choice)

Unlock Settings

Unlock Mode Combination Unlock ▾

Combination Method Or And

Unlock Method (Multi-select) Card Fingerprint Password

Door Unlocked Duration s (0.2-600)

Unlock Timeout s (1-9999)

Table 2-2 Unlock settings description

Parameter	Description
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 s to 600 s.
Unlock Timeout	A timeout alarm can be triggered if the door remains unlocked for longer time than this value.

- Unlock by period

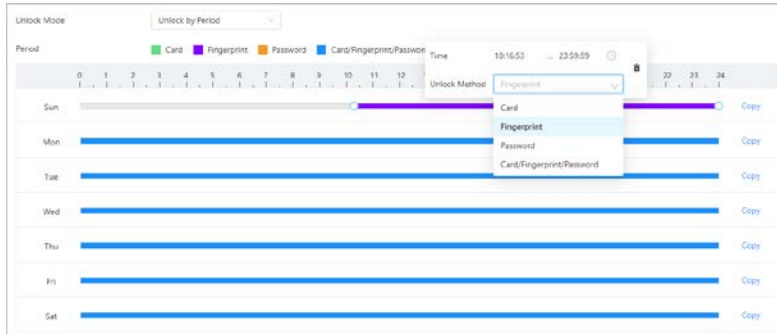
1. In the **Unlock Method** list, select **Unlock by Period**,
2. Drag the slider to adjust time period for each day.



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

3. Select an unlock method for the time period, and then configure other parameters.

Figure 2-7 Unlock by period



Step 7 In the **Alarm Settings** area, configure the alarm parameters.

Figure 2-8 Alarm

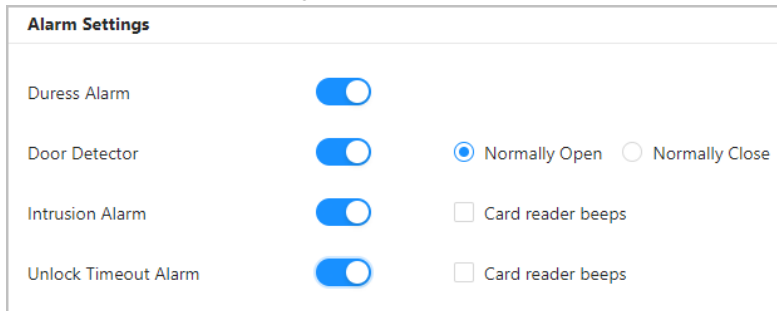


Table 2-3 Description of alarm parameters

Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Detector	Select the type of the door detector.
Intrusion Alarm	<ul style="list-style-type: none"> When door detector is enabled, an intrusion alarm will be triggered if the door is opened abnormally. A timeout alarm will be triggered if the door remains unlocked longer than the defined unlock time. When Card reader beeps is enabled, the card reader beeps when intrusion alarm or timeout alarm is triggered.
Unlock Timeout Alarm	

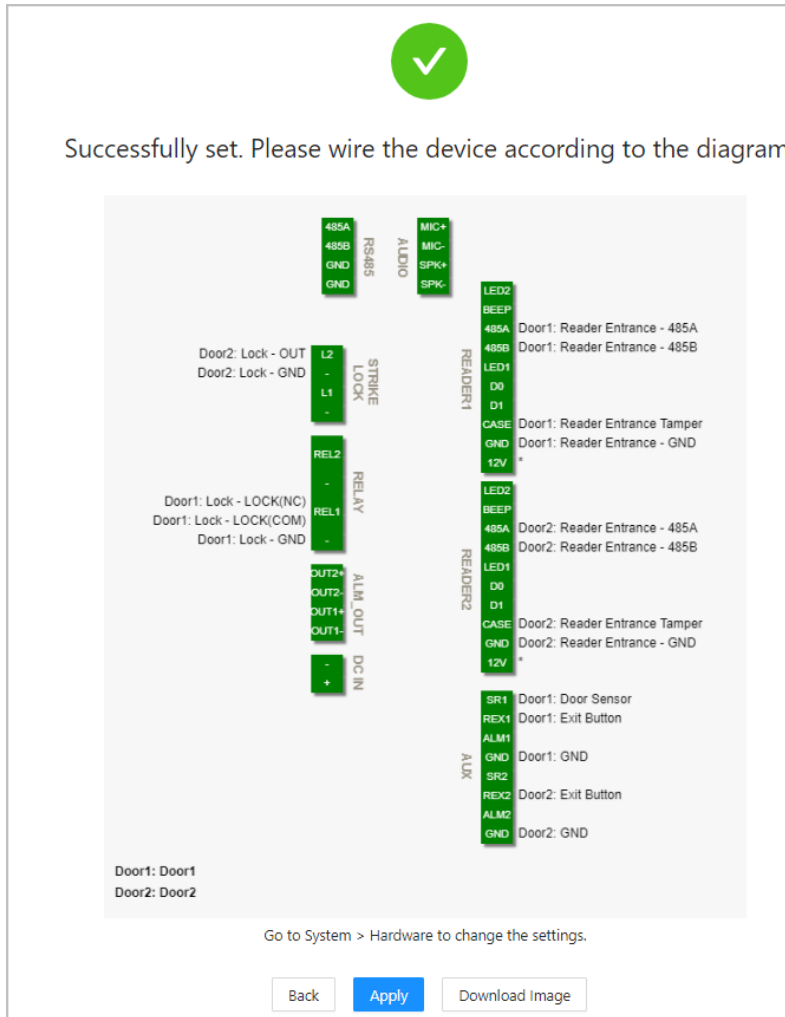
Step 8 Click **Next**.

A wiring diagram is generated base on your above settings. You can wire the device according to the diagram.



The image below is for reference only.

Figure 2-9 Wiring diagram



Step 9 Click **Apply**.

- You can go to **Local Device Config** to change the settings after you successfully log in to the platform.
- Click **Download Image** to download the diagram to your computer.

2.2.4 Dashboard

After you successfully log in, the dashboard page of the platform is displayed. the dashboard is

displayed to show visualized data.

Figure 2-10 Dashboard



Table 2-4 Home page description

No.	Description
1	Displays daily unlocks. Hover over a day, you can see all types of unlocks on that day.
2	Displays the number of total alarms.
3	<ul style="list-style-type: none"> Click to go to the dashboard page. Click to go to the home page of the platform.
4	Displays the status of devices, including offline devices and online devices.
5	Displays the data capacity of cards, fingerprint and users.
6	<ul style="list-style-type: none"> : The number of doors of the controller. <ul style="list-style-type: none"> ◇ Double door ◇ Single door The type of the controller. <ul style="list-style-type: none"> ◇ : Main controller. ◇ : Sub controller. : Select the language on the platform. : Goes to the Security page directly. : Restarts or log out of the platform. : Display the webpage in full screen.

2.2.5 Homepage

After you successfully log in, the home page of the main controller is displayed.

Figure 2-11 Home page

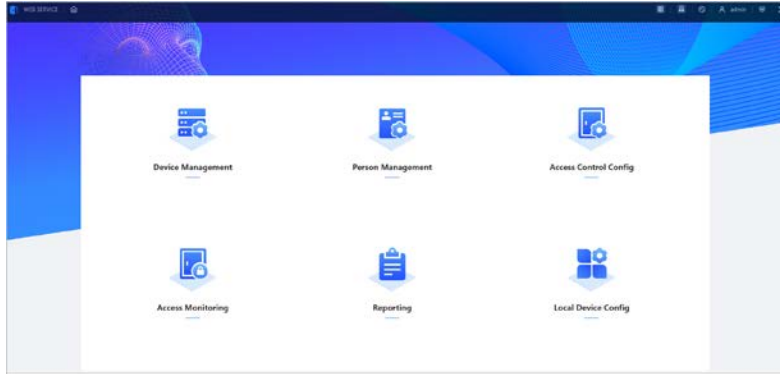


Table 2-5 Home page description

Menu	Description
Device Management	Add devices to the platform of the main controller.
Person Management	Add personnel and assign area permissions to them.
Access Control Config	Add time templates, create and assign area permissions, configure door parameters and global alarm linkages, and view authorization progress.
Access Monitoring	Remotely control door status and view event log.
Reporting	View or export alarm records/unlock records.
Local Device Config	Configure local device, such as network, local alarm linkage, and more.

2.2.6 Adding Devices

You can add devices to the management platform of the main controller in batches or individually. If the controller is set to the main controller during the logging-in wizard, you can add other sub controllers to the platform, and then you can manage sub controllers through the platform.



Only the main controller comes with a management platform.

2.2.6.1 Adding Individually

You can add sub controllers individually by entering their IP addresses or domain names.

Procedure

Step 1 On the home page, Click **Device Management**, and then click **Add**.

Step 2 Enter the device information.

Figure 2-12 Device information

Table 2-6 Device parameters Description

Parameter	Description
Device Name	Enter the name of the Controller. We recommend you name it after its installation area.
Add Mode	Select IP to add the Access Controller by entering its IP Address.
IP Address	Enter IP address of the Controller.
Port	The port number is 37777 by default.
User Name/Password	Enter the username and password of the Controller.

Step 3 Click **OK**.

The added controllers are displayed on the **Device Management** page.

Figure 2-13 Successfully add devices

No.	Device Name	IP Address	Device Type	Device Model	Connection Status	DR	Operation
1	W2_LAL_MLR	192.168.1.104	Access Controller	ASC3008	Online	901241808488	ⓘ ⚙ ⌵ ⌵ ⌵
2	192.168.1.100	192.168.1.100	Access Controller	Sub-w212028	Offline	8889870478000	ⓘ ⚙ ⌵ ⌵ ⌵



If the access controller is set to the main controller during the log-in wizard, the controller will be added to the management platform automatically and functions as both the main controller and sub controller.

Related Operations

- ✎ : Edit the information of the device.



Only sub controllers support the below operations.

- 🌐 : Go to the webpage of the sub controller.
- 🔑 : Log out of the device.
- 🗑️ : Delete the device.

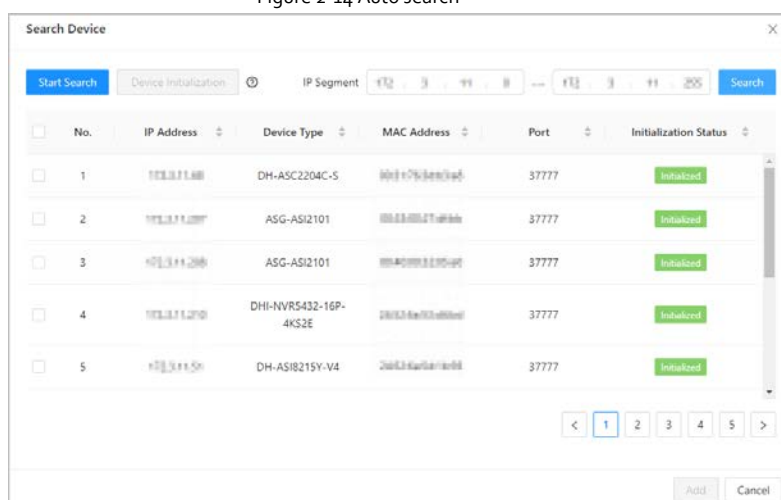
2.2.6.2 Adding in Batches

We recommend you use the auto-search function when you add want to Access Controllers in batches. Make sure the Access Controllers you want to add are on the same network segment.

Procedure

- Step 1** On the home page, Click **Device Management**, and then click **Search Device**.
- Click **Start Search** to search for devices on the same LAN.
 - Enter a range of the network segment, and then click **Search**.

Figure 2-14 Auto search



All searched devices will be displayed.



You can select devices in the list, and click **Device Initialization** to initialize them in batches.



To ensure the security of devices, initialization is not supported for devices on different segments.

Step 2 Select the Controllers that you want to add to the Platform, and then click **Add**.

Step 3 Enter the username and password of the Controller.

The added Controller displays on the **Device Management** page.

Related Operations

- **Modify IP:** Select added devices, and then click **Modify IP** to change their IP addresses.
- **Sync Time:** Select added devices, and then click **Sync Time** to sync the time of the devices with NTP server.
- **Delete:** Select added devices, and then click **Delete** to delete them.

2.2.7 Adding Users

Add users to departments, enter the basic information of users and authentication methods to verify

their identities.

Procedure

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

Step 2 Create departments.

1. Click **+**.
2. Enter the name of the department, and then click **Add**.



The default company cannot be deleted.

Figure 2-15 Add department

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first is labeled "Upper Level Department" and has a dropdown menu with "Default Company" selected. The second is labeled "* Department Name" and has a text input field containing "human resources". At the bottom right of the dialog, there are two buttons: "Add" (blue) and "Cancel" (white).

Step 3 (Optional) before you assign cards to users, set the card type and the type of the card number.

1. On the **Person Management** page, select **More > Card Type**.
2. Select ID or IC Card, and then click **OK**.



Make sure that the card type is same to the actually assigned card; otherwise, the card number cannot be read. For example, if the assigned card is an ID card, set card type to ID card.

3. Select **More > Card No. System**.
4. Select decimal format or hexadecimal format for the card number.

Step 4 Add users.

- Add users individually



When you want to assign access permissions to a single person, you can add users individually. For details on how to assign access permissions, see "2.2.10.1 Assigning Permissions Individually".

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

Figure 2-16 Basic information of user

The screenshot shows a window titled 'Add' with three tabs: 'Basic Info', 'Authentication', and 'Permission'. The 'Basic Info' tab is active. It contains the following fields:

- * User ID: Text input with value '001'
- * User Name: Text input with value 'Tom'
- * Department: Dropdown menu with value 'Default Company'
- * User Type: Dropdown menu with value 'General User'
- Validity Period: Two date-time pickers. The first has value '2022-08-16 00:00:00' and the second has value '2037-12-31 23:59:59', separated by 'To'.
- * Unlock Attempts: Text input with value 'Unlimited'

At the bottom right, there are three buttons: 'Add' (highlighted in blue), 'Add More', and 'Cancel'.

Table 2-7 parameters description

Parameter	Description
User ID	The ID of the user.
Department	The department that the user belongs to.
Validity Period	Set a date on which the access permissions of the person will become effective.
To	Set a date on which the access permissions of the person will be expired.
User Name	The name of the user.
User Type	<p>The type of the user.</p> <ul style="list-style-type: none"> ● General User: General users can unlock the door. ● VIP User: When VIP unlock the door, service personnel will receive a notice. ● Guest User: Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● Patrol User: Patrol users will have their attendance tracked, but they have no unlocking permissions. ● Blocklist User: When users in the blocklist unlock the door, service personnel will receive a notification. ● Other User: When they unlock the door, the door will stay unlocked for 5 more seconds.
Unlock Attempts	The times of unlock attempts for guest users.

2. Click **Add**.

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

- Add users in batches.
 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 Platform.

The users are added to the Platform automatically.

Step 5 Click **Authentication** tab, set authentication methods for identity verification.



Each user supports 1 password, 5 cards, and 3 fingerprints.

- Password: Enter and confirm the password.
- Card: Enter the card number manually or connect a card issuer to the computer to read the number automatically.
- Fingerprint: Connect a fingerprint scanner to the computer and register the fingerprint according to the on-screen instructions.

Figure 2-17 Authentication method

The screenshot shows a software interface for editing user authentication methods. It features three tabs: 'Basic Info', 'Authentication', and 'Permission'. The 'Authentication' tab is active. Under the 'Password' section, there is a '+ Add' button. The 'Card' section includes a '+ Add' button and four card entries, each with a card number and a timestamp of '2022-08-15'. The 'Fingerprint' section has a '+ Add' button and three entries labeled 'Fingerprint 1', 'Fingerprint 2', and 'Fingerprint 3'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Step 6 Click OK.

Related Operations

- On the **Person Management** page, click **Export** to export all users in the excel format.
- On the **Person Management** page, click **More > Extract**, and select a device to extract all users on the sub controller to the Platform of the main controller.
- On the **Person Management** page, click **More > Card Type**, set the card type before you assign cards to users. For example, if the assigned card is an ID card, set card type to ID card.
- On the **Person Management** page, click **More > Card No. System**, set the card system to decimal or hexadecimal format.

2.2.8 Adding Time Templates

Time template defines the unlock schedules of the Controller. The platform offers 4 time templates

by default. The template is also customizable.

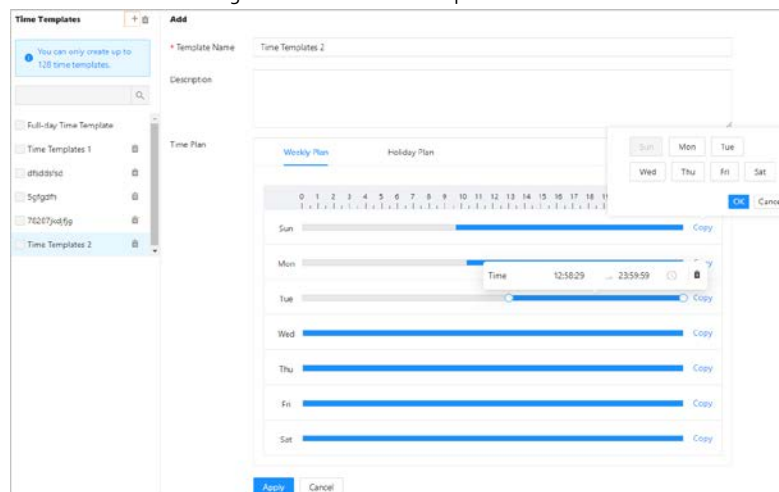


The default templates cannot be changed.

Step 1 On the homepage, select **Access Control Config > Time Template**, and then click **+**.

Step 2 Enter the name of the time template.

Figure 2-18 Create time templates



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

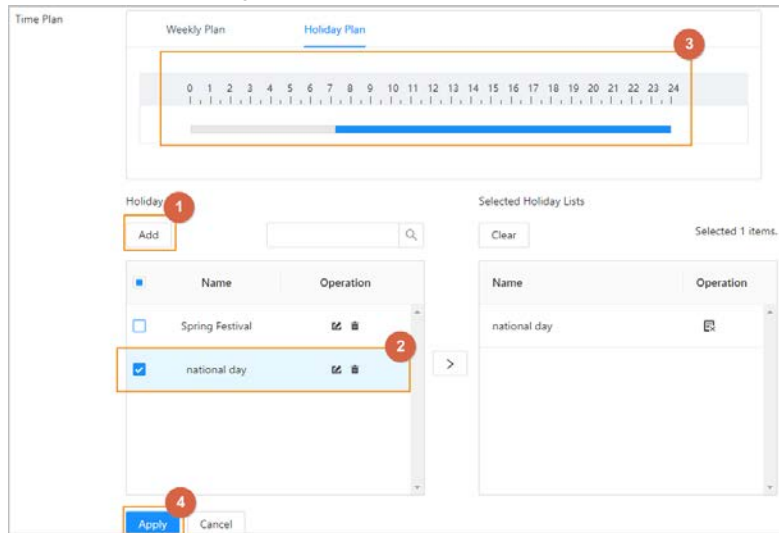
You can also click **Copy** to apply the configured time period to other days.

Step 4 Click **Apply**.

Step 5 Configure holiday plans.

1. Click **Holiday Plan** tab, and then click **Add** to add holidays.
2. Select a holiday.
3. Drag the slider to adjust time period for the holiday.
4. Click **Apply**.

Figure 2-19 Create holiday plan



2.2.9 Adding Area Permissions

An area permission is a collection of door access permissions in a defined time. Create a permission group, and then associate users with the group so that users will be assigned with access permissions defined in the group.

Step 1 Click **Access Control Config > Permission Settings**.

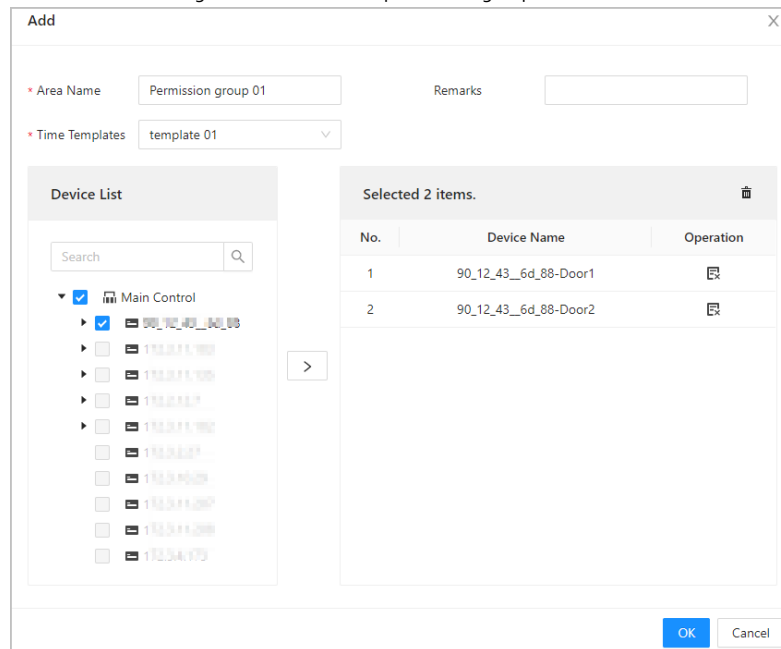
Step 2 Click + .

Step 3 Enter the name of the area permission group, remarks (optional), and select a time template.

Step 4 Select doors.

Step 5 Click OK.

Figure 2-20 Create area permission groups



2.2.10 Assigning Access Permissions

Assign access permissions to users by associating users with the defined permission groups, and then users can gain access to a secured area after valid identity verification.

2.2.10.1 Assigning Permissions Individually

When you want to assign permission to a new person or change access permissions of a existing person. You can assign access permissions to people individually.

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

Step 2 Select the department, and then select an existing user.



If the user has not been added, you click **Add** to add the user. For details on creating users, see "2.2.7 Adding Users" for details.

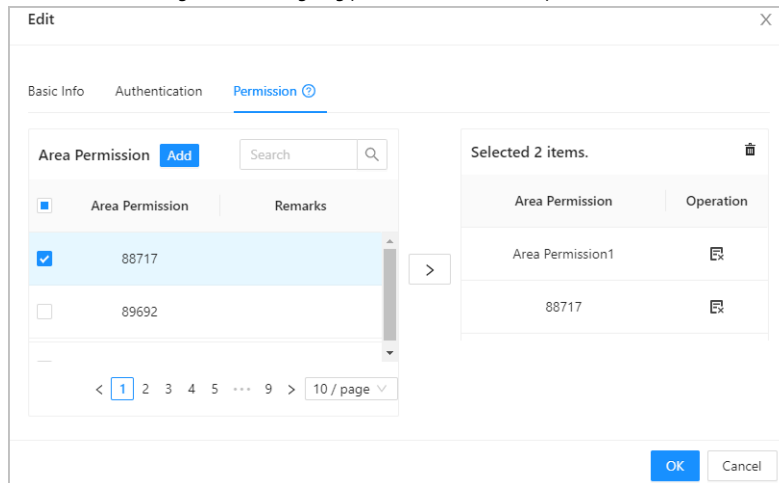
Step 3 Click corresponding to the user.

Step 4 On the **Permission** tab, select existing permission groups.



- You can click **Add** to create new area permissions. For details on creating area permissions, see "2.2.9 Adding Area Permissions" for details..
- You can associate multiple area permissions to a user.

Figure 2-21 Assigning permissions individually




Step 5 Click OK.

2.2.10.2 Assigning Permissions in Batches

You can assign access permissions to users in batches.

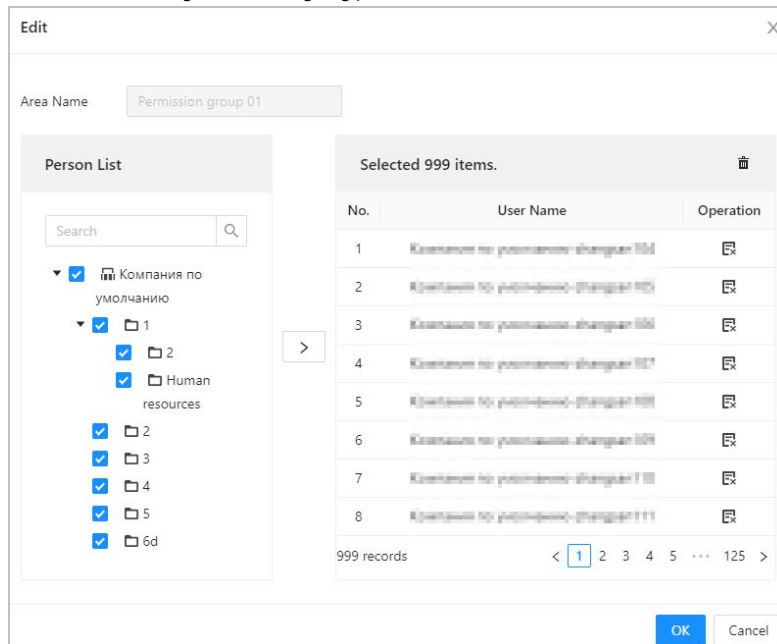
Step 1 On the home page, select **Access Control Config > Permission Settings**.

Step 2 Click  of an existing permission group, and then select users in departments. You can select the whole department.



You can click **+** to create new permission groups. For details on creating permission groups, see "2.2.9 Adding Area Permissions" for details.

Figure 2-22 Assigning permissions in batches



Step 3 Click OK.

2.2.11 Viewing Authorization Progress

After you assign access permissions to users, you can view the authorization process.

Step 1 On the home page, select **Access Control Config > Authorization Progress**.

Step 2 View the authorization progress.

- Sync SubControl Person: Sync personnel on the main controller to the sub controller.
- Sync Local Person: Sync personnel on the management platform of the main controller to the its server.

Figure 2-23 Authorization progress

Area Permission	Device Name	Type	Progress	Results	Time	Operation
	1752.0-18.182	Sync SubControl Person		Success: 1, Failed: 0	2023-06-12 20:04:58	
	1752.0-18.182	Sync SubControl Person		Success: 0, Failed: 1	2023-06-12 20:04:55	
	1756	Sync Local Person		Success: 1, Failed: 0	2023-06-12 20:04:55	

Step 3 If authorization failed, click to try again.

You can click to view details of the failed authorization task.

2.2.12 (Optional) Configuring Access Control

2.2.12.1 Configuring Basic Parameters

Step 1 Select **Access Control Config > Door Parameters**.

Step 2 In the **Basic Settings** area, configure basic parameters of access control.

Figure 2-24 Basic parameters

Basic Settings

Name

Unlock Type Fail Secure ? Fail Safe ?

Door Status Normal Always Open Always Closed

Normally Open Period

Normally Closed Period

Admin Unlock Password

Table 2-9 Basic parameters description

Parameter	Description
Name	The name of the door.
Unlock mode	<ul style="list-style-type: none"> • Fail Secure: The door locks in the event of a power outage or emergency. • Fail Safe: The door is unlocked in the event of a power outage or emergency.
Door Status	Set the door status. <ul style="list-style-type: none"> • Normal: If Normal is selected, the door will be unlocked and locked according to your settings. • Always Open: The door remains unlocked all the time. • Always Closed: The door remains locked all the time.
Normally Open Period	When you select Normal , you can select a time template from the drop-down list. The door remains open or closed during the defined time.
Normally Closed Period	
Admin Unlock Password	Turn on the admin unlock function, and then enter the password of the administrator. Administrator can unlock the door by only entering the admin password.

2.2.12.2 Configuring Unlock Methods

Use card, fingerprint, password or their combinations to unlock the door.

Step 1 Select **Access Control Config > Door Parameters**.

Step 2 In the **Unlock Settings** area, select an unlock mode.

- Combination Unlock
 1. Select **Combination Unlock** form the **Unlock Method** list.
 2. Select **Or** or **And**
 - ◇ **Or**: Verify one of the selected unlocking methods to open the door.

- ◊ And: Verify all the selected unlocking methods to open the door.
The Controller supports unlock through card, fingerprint or password.
- 3. Select unlock methods, and then configure other parameters.

Figure 2-25 Element (multiple choice)

Unlock Settings

Unlock Mode: Combination Unlock ▾

Combination Method: Or And

Unlock Method (Multi-select): Card Fingerprint Password

Door Unlocked Duration: 3.0 s (0.2-600)

Unlock Timeout: 60 s (1-9999)

Table 2-10 Unlock settings description

Parameter	Description
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 s to 600 s.
Unlock Timeout	A timeout alarm can be triggered if the door remains unlocked for longer time than this value.


- Unlock by period
 1. In the **Unlock Method** list, select **Unlock by Period**,
 2. Drag the slider to adjust time period for each day.
-  You can also click **Copy** to apply the configured time period to other days.
3. Select an unlock method for the time period, and then configure other parameters.

Figure 2-26 Unlock by period

Unlock Mode: Unlock by Period ▾

Period: Card Fingerprint Password Card/Fingerprint/Password

Time: 19:16:53 → 23:59:59

Unlock Method: Fingerprint ▾

Sun: Copy

Mon: Copy

Tue: Copy

Wed: Copy

Thu: Copy

Fri: Copy

Sat: Copy

Step 3 Click **Apply**.

2.2.12.3 Configuring Alarms

An alarm will be triggered when abnormal access events occur.

Step 1 Select **Access Control Config > Door Parameters**

Step 2 Select **Access > Alarm**.

Step 3 Enable the alarm type.

Figure 2-27 Alarm

The screenshot shows the 'Alarm Settings' interface. It contains the following elements:

- Duress Alarm:** A blue toggle switch is turned on.
- Door Detector:** A blue toggle switch is turned on. To its right are two radio buttons: 'Normally Open' (selected with a blue dot) and 'Normally Close' (unselected).
- Intrusion Alarm:** A blue toggle switch is turned on. To its right is a checkbox labeled 'Card reader beeps', which is currently unchecked.
- Unlock Timeout Alarm:** A blue toggle switch is turned on. To its right is a checkbox labeled 'Card reader beeps', which is currently unchecked.

Table 2-11 Description of alarm parameters

Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Detector	Select the type of the door detector.
Intrusion Alarm	<ul style="list-style-type: none"> When door detector is enabled, an intrusion alarm will be triggered if the door is opened abnormally. A timeout alarm will be triggered if the door remains unlocked longer than the defined unlock time. When Card reader beeps is enabled, the card reader beeps when intrusion alarm or timeout alarm is triggered.
Unlock Timeout Alarm	

2.2.13 (Optional) Configuring Global Alarm linkages

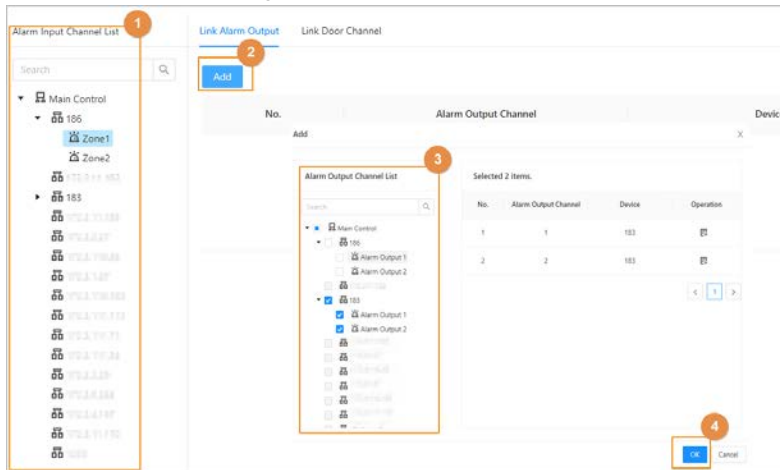
You can configure global alarm linkages across different access controllers.

Step 1 Select **Access Control Config > Global Alarm Linkage**.

Step 2 Configure the alarm output.

1. Select an alarm input from the alarm input channel list, and then click **Link Alarm Output**.
2. Click **Add**, select an alarm output channel, and then click **OK**.

Figure 2-28 Alarm output

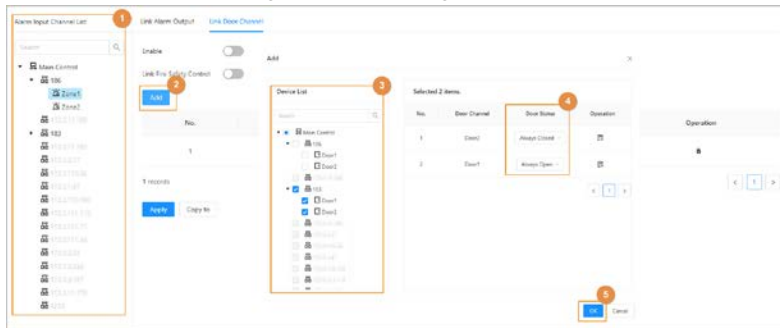


3. Turn on the alarm output function and then enter the alarm duration.
4. Click **Apply**.

Step 3 Configure the door linkage.

1. Select an alarm input form the channel list, and then click **Add**.
2. Select the linkage door, select the door status, and then click **OK**.
 - Always Closed: The door automatically locks when an alarm is triggered.
 - Always Open: The door automatically unlocks when an alarm is triggered.

Figure 2-29 Door linkage



3. Turn on the door linkage function.



If you turn on the link fire safety control, all doors will open when the fire alarm is triggered.

4. Click **Apply**.
You can click **Copy to** to apply the pre-configured alarm linkages to other alarm input channel.

2.2.14 (Optional) Local Device Configurations

Local device configurations can only be applied to the local controller.

2.2.14.1 Configure Local Alarm Linkages

You can only configure local alarm linkages on the same access controller.

Each controller has 2 alarm inputs and 2 alarm outputs.

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


Step 2 Click  to configure local alarm linkage.


Figure 2-30 Local alarm linkage

The screenshot shows a 'Modify' dialog box with the following settings:

- Alarm Input Channel: 1
- Alarm Input Name: Zone1
- Alarm Input Type: Normally Open
- Link Fire Safety Control: Disabled
- Alarm Output: Enabled
- Duration: 5 s (1-300)
- Alarm Output Channel: 1 and 2 (checked)
- AC Linkage: Enabled
- Door1: Always Open
- Door2: Always Closed

Table 2-12 Local alarm linkage

Parameter	Description
Alarm input channel	The number of the alarm input channel.  Each 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. <ul style="list-style-type: none"> • Normally Open • Normally Close
Link Fire Safety Control	If you turn on the link fire safety control, all doors will open when the fire alarm is triggered.
Alarm Output	Turn on the alarm output function.
Duration	When an alarm is triggered, the alarm remains for a defined time.

Parameter	Description
Alarm Output Channel	Select the alarm output channel.  Each controller has 2 alarm inputs and 2 alarm outputs.
AC Linkage	Turn on AC Linkage to configure the door linkage.
Door1/Door2	Set the door to always open or always closed status. When an alarm is triggered, the door will automatically open or close.

Step 3 Click **OK**.

2.2.14.2 Configuring Card Rules

The platform supports 5 types of Wiegand formats by defaults. You can also add custom Wiegand formats.

Step 1 On the home page, select **Local Device Config > Access Card Rule Config**.

Step 2 Click **Add**, and then configure new Wiegand formats.

Figure 2-31 Add new Wiegand formats

Table 2-13 Configure wiegand format

Parameter	Description
Wiegand format	The name of the Wiegand format.
Total bits	Enter the total number of bits.
Facility Code	Enter the start bit and the end bit for the facility code.
Card number	Enter the start bit and the end bit for the card number.
Parity Code	<ol style="list-style-type: none"> Enter the even parity start bit and even parity end bit. Enter the odd parity start bit and odd parity end bit.

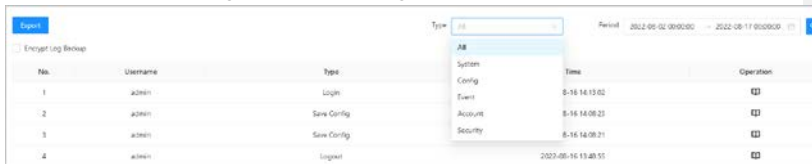
Step 3 Click OK.

2.2.14.3 Backing up System Logs

Step 1 On the home page, select **Local Device Config > System Logs**.

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

Figure 2-32 Back up logs



Step 3 Click **Encrypt Log Backup** to back up encrypted logs.
You can also click **Export** to export logs.

2.2.14.4 Configuring Network

2.2.14.4.1 Configuring TCP/IP

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

Step 1 Select **Network Setting > TCP/IP**.

Step 2 Configure parameters.

Figure 2-33 TCP/IP

NIC: NIC 1

Mode: DHCP Static

MAC Address: 90 : 12 : 43 : 65 : 6d : 88

IP Version: IPv4

IP Address: [. . .]

Subnet Mask: [. . .]

Default Gateway: [. . .]


Preferred DNS: 8 . 8 . 8 . 8

Alternate DNS: 8 . 8 . 4 . 4

MTU: 1500

Buttons: Apply, Refresh, Default

Table 2-14 Description of TCP/IP

Parameter	Description
IP Version	IPv4
MAC Address	MAC address of the Access Controller.
Mode	<ul style="list-style-type: none"> • Static: Manually enter IP address, subnet mask, and gateway. • DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Access Controller will automatically be assigned with IP address, subnet mask, and gateway.
IP Address	If you select static mode, configure the IP address, subnet mask and gateway.  IP address and gateway must be on 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 3 Click OK.

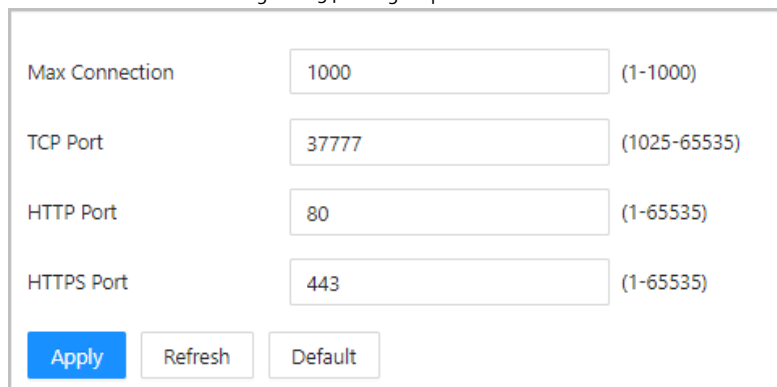
2.2.14.4.2 Configuring Port

You can limit access to the Access Controller at the same through web, desktop client and phone.

Step 1 Select **Network Setting > Port**.

Step 2 Configure port numbers.

Figure 2-34 Configure ports




Except **Max Connection** and **RTSP Port**, you need to restart the Access Controller to make the configurations effective after you change other parameters.

Table 2-15 Description of ports

Parameter	Description
Max Connection	You can set the maximum number of clients (such as web, desktop client and phone) that can access the Access Controller at the same time.
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If you want to change the port number, add the new port number after the IP address when you log in to the webpage.
HTTPS Port	Default value is 443.
RTSP Port	Default value is 554.

Step 3 Click OK.

2.2.14.4.3 Configuring Cloud Service

The cloud service provides a NAT penetration service. Users can manage multiple devices through DMSS. You do not have to apply for dynamic domain name, configuring port mapping or deploying server.

Step 1 On the home page, select **Network Setting > Cloud Service**.

Step 2 Turn on the cloud service function.

Figure 2-35 Cloud service

Step 3 Click OK.

Step 4 Download DMSS and sign up, you can scan the QR code through DMSS to add the Access Controller to it.

2.2.14.4.4 Configuring Automatic Registration


The Access Controller reports its address to the designated server so that you can get access to the Access Controller through the management platform.

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

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

Figure 2-36 Register

Table 2-16 Automatic registration description

Parameter	Description
Host IP	The IP address or the domain name of the server.
Port	The port of the server used for automatic registration.
Sub-Device ID	Enter the sub-device ID (user defined).  When you add the Access Controller to the management platform, the sub-device ID on the management platform must conform to the defined sub-device ID on the Access Controller.

Step 3 Click **Apply**.

2.2.14.4.5 Configuring Basic Service

When you want to connect the Access Controller to a third-party platform, turn on the CGI and ONVIF function.

Step 1 Select **Network Settings > Basic Service**.

Step 2 Configure the basic service.

Figure 2-37 Basic service

Enable

The Imou will be enabled to assist you in remotely managing your device. We need to collect your IP address, MAC address, device name, device SN after enabling Imou and connecting to the Internet. All collected info is used only for the purpose of remote access. Please un-select the check box if you do not agree to enable the Imou function.

Status

SN




Table 2-17 Basic service parameter description

Parameter	Description
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. When CGI is enabled, CGI commands can be used. The CGI is enabled by default.
ONVIF	Enable other devices to acquire video stream of the VTO through the ONVIF protocol.
Private Protocol Authentication Mode	<ul style="list-style-type: none"> Security Mode (recommended) Compatible Mode

Step 3 Click **Apply**.

2.2.14.5 Configuring Time

Step 1 On the home page, select **Local Device Config > Time**.

Step 2 Configure the time of the Platform.

Figure 2-38 Date setting

Time and Time Zone

Date :
2022-07-07 Thursday

Time :
10:21:35

Time Manual Settings NTP

Time

Time Format

Time Zone

DST

Enable

Type Date Week

Start Time

End Time

Table 2-18 Data setting description

Parameter	Description
Time	<ul style="list-style-type: none"> • Manual Settings: manually enter the time or you can click Sync PC to sync time with computer. • NTP: The Access Controller will automatically sync time with NTP server. <ul style="list-style-type: none"> ◇ Server: Enter the domain of the NTP server. ◇ Port: Enter the port of the NTP server. ◇ Interval: Enter time synchronization interval.
Time format	Select the time format for the Platform.
Time Zone	Enter the time zone of the Access Controller.

Parameter	Description
DST	<ol style="list-style-type: none"> (Optional) Enable DST. Select Date or Week from the Type. Configure start time and end time.

Step 3 Click **Apply**.

2.2.14.6 Account Management

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

2.2.14.6.1 Adding Users

You can add new users and then they can log in to the webpage of the Access Controller.

Procedure

Step 1 On the home page, select **Local Device Config > 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 2-39 Add user

Add
✕

* Username

* Password

Confirm Password

Remarks

Step 3 Click **OK**.



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

2.2.14.6.2 Resetting Password

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

Step 1 Select **Local Device Config > Account Management > Account**.

Step 2 In the Enter the email address, and set the password expiration time, Scan the QR code, and you will get the security code.

Step 3 Turn on the password reset function.

Figure 2-40 Reset Password

Figure 2-40 shows the Password Reset configuration interface. It includes a toggle for 'Enable', an informational message, input fields for 'Email Address' and 'Password Expires in' (set to 'Never'), and buttons for 'Apply', 'Refresh', and 'Default'.



- Two methods are available for you to reset password. For option 1, you will receive a security code to set password after you scan DMSS. 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.
- For option 2, after you scan the QR code, send the encryption strings that you received to the designated email address, and then 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 in a row, the administrator account will be frozen for five minutes.

Step 4 Enter the security code.

Step 5 Click **Next**.

Step 6 Enter and confirm the new 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**.

2.2.14.6.3 Adding ONVIF Users

Open Network Video Interface Forum (ONVIF), a global and open industry forum that is established

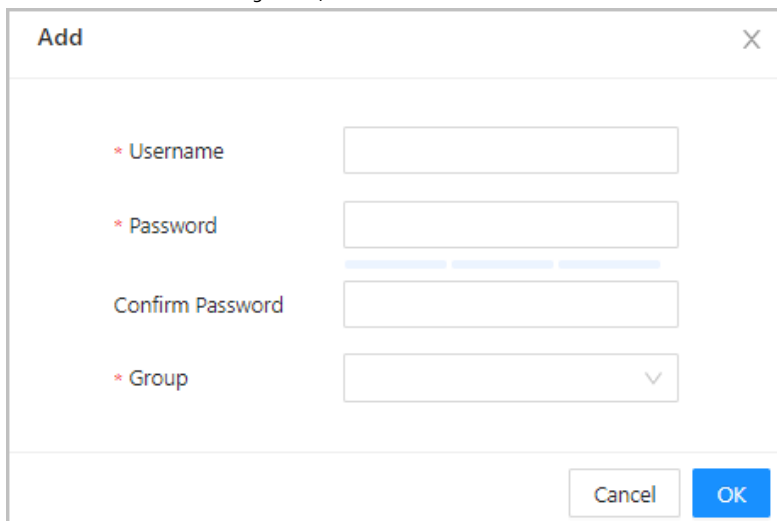
for the development of a global open standard for the interface of physical IP-based security products, which allows the compatibility from different manufactures. ONVIF users have their identities verified through ONVIF protocol. The default ONVIF user is admin.

Procedure

Step 1 On the home page, select **Local Device Config > Account Management > ONVIF Account**.

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

Figure 2-41 Add ONVIF user



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields:

- * Username**: A text input field.
- * Password**: A text input field with a strength indicator below it.
- Confirm Password**: A text input field.
- * Group**: A dropdown menu with a downward arrow.

At the bottom right of the dialog, there are two buttons: "Cancel" and "OK".

Step 3 Click **OK**.

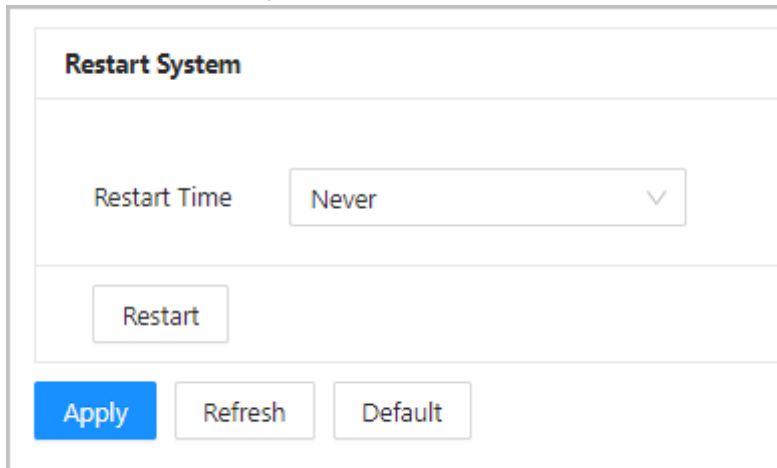
2.2.14.7 Maintenance

You can regularly restart the Access Controller during its idle time to improve its performance.

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config > Maintenance**.

Figure 2-42 Maintenance



Step 3 Set the restart time, and then click **OK**.

Step 4 (Optional) Click **Restart**, the Access Controller will restart immediately.

2.2.14.8 Advanced Management

When more than one Access Controller require the same configurations, you can configure them quickly by importing or exporting configuration files.

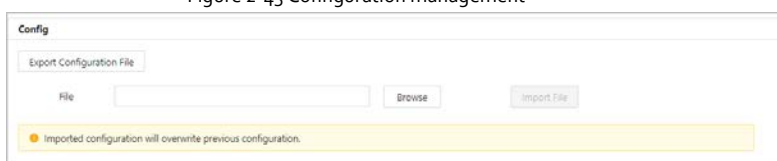
2.2.14.8.1 Exporting/Importing Configuration Files

You can import or export the configuration file of the Access Controller. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config > Advanced Settings**.

Figure 2-43 Configuration management



Step 3 Export or import configuration files.

- Export configuration file.
Click **Export Configuration File** to download the file to the local.



IP will not be exported.

- Import configuration file.
 1. Click **Browse** to select the configuration file.
 2. Click **Import configuration**.



Configuration file can only be imported to the device with the same model.

2.2.14.8.2 Configuring Card reader

Step 1 On the home page, select **Local Device Config > Advanced Settings**.

Step 2 Configure card reader.

Figure 2-44 Configure card reader

The screenshot shows the 'Card Reader Settings' interface. It includes the following fields and controls:

- Door Channel:** A dropdown menu with the value '1' selected.
- Card No. Inversion:** Radio buttons for 'Enable' and 'Close', with 'Close' selected.
- Reader:** A dropdown menu with the value 'Reader 1' selected.
- Baud Rate:** Radio buttons for '9600' and '115200', with '9600' selected.
- Buttons:** 'Apply' (blue), 'Refresh', and 'Default' (grey).

2.2.14.8.3 Configuring Fingerprint Level

On the home page, select **Local Device Config > Advanced Settings**.

Figure 2-45 Fingerprint Level

The screenshot shows the 'Configurations Management' interface for fingerprint settings. It includes the following field and controls:

- Fingerprint Similarity Threshold:** A text input field with the value '3' and a range indicator '(1-10)' to its right.
- Buttons:** 'Apply' (blue), 'Refresh', and 'Default' (grey).

2.2.14.8.4 Restoring Factory Defaults



Restoring the **Access Controller** to default configurations will cause data loss. Please be advised.

Step 1 Select **Local Device Config > Advanced Settings**

Step 2 Restore factory defaults if necessary.

- **Factory Defaults:** Resets configurations of the Access Controller and delete all data.
- **Restore to Default (Except for User Info and Logs):** Resets configurations of the

Access Controller and deletes all data except for user information and logs.

2.2.14.9 Updating System



- Use the correct update file. Make sure you get the correct update file from the technical support.
- Do not disconnect the power supply or network, or restart or shut down the Access Controller during the update.

2.2.14.9.1 File Update

- Step 1** On the home page, select **Local Device Config > System Update**.
- Step 2** In the **File Update** area, click **Browse**, and then upload the update file.



The update file should be a .bin file.

- Step 3** Click **Update**.
- The Access Controller will restart after update completes.

2.2.14.9.2 Online Update

- Step 1** On the home page, select **Local Device Config > System Update**.
- Step 2** In the **Online Update** area, select an update method.
- Select **Auto Check for Updates**, the Access Controller will automatically check whether the its latest version is available.
 - Select **Manual Check**, and you can immediately check whether the latest version is available.
- Step 3** Click **Manual Check** to update the Access Controller when the latest version is available.

2.2.14.10 Configuring Hardware

On the home page, select **Local Device Config > Hardware**. You can view the hardware you have configured during you log in to the platform for the first time. You can also re-configure the hardware. For details, see "Parameter descriptions".

The wiring diagram is generated based for your reference. You can download it to your computer.

Figure 2-46 Hardware



2.2.14.11 Viewing Version Information

On the home page, select **Local Device Config > Version Info**, and you can view version information, such as device model, serial number, hardware version, legal information and more.

2.2.14.12 Viewing Legal Information

On the home page, select **Local Device Config > Legal Info**, and you can view the software license agreement, privacy policy and open source software notice.

2.2.15 Viewing Records

You can alarm logs and unlock logs.

2.2.15.1 Viewing Alarm Records

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

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

Figure 2-47 Alarm records

No.	Time	Device	Door	Event Type
1	2022-08-15 17:03:52	186	Door1	Unlock Timeout Alarm
2	2022-08-15 17:03:52	186	Door1	Intrusion Alarm

- **Export:** Exports unlock logs on main controller to a local place.
- **Extract Device Records:** When logs on sub controller are generated when they go online, you extract logs on the sub controller to the main controller.

2.2.15.2 Viewing Unlock Records

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

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

Figure 2-48 Unlock logs



The screenshot shows a web interface for viewing unlock logs. At the top, there are filters for 'Device' (set to 'All'), 'Department', and 'Period' (set to '2022-08-01 00:00:00' to '2022-08-17 00:00:00'). A 'Search' button is visible. Below the filters, there is a table with the following columns: No., Time, User ID, Username, Card, Department, Device, Door, and Status. Two entries are shown in the table.

No.	Time	User ID	Username	Card	Department	Device	Door	Status
1	2022-08-15 08:55:37			84E9E54		186	Door2	Failed
2	2022-08-15 08:55:45			8228730		186	Door1	Failed

- **Export:** Exports unlock logs.
- **Extract Device Records:** When logs on sub controller are generated when they go online, you extract logs on the sub controller to the main controller.

2.2.16 Security

2.2.16.1 Security Status

Background Information

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

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

Procedure

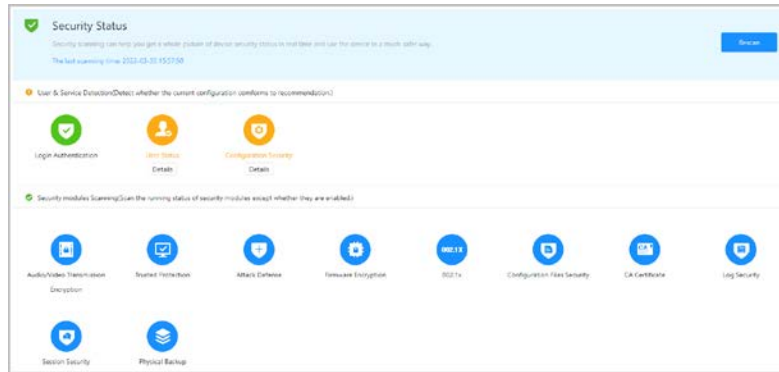
Step 1 Select **Security > Security Status**.

Step 2 Click **Rescan** to scan the security status of the Access Terminal.



Hover on the icons of the security modules, you can view their running status.

Figure 2-49 Security Status



Related Operations

After scanning, different results will be displayed with different color. Yellow indicates that the security modules are abnormal, and Green indicates that the security modules are normal.

- Click **Details** to view the details of scanning results.
- Click **Ignore** to ignore the abnormality, and it will not be scanned; the ignored abnormality is highlighted in grey.
Click **Rejoin Detection**, and the ignored abnormality will be scanned again.
- Click **Optimize** to troubleshoot the abnormality.

2.2.16.2 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 **Security > System Service > HTTPS**.

Step 2 Click to turn on the HTTPS service.



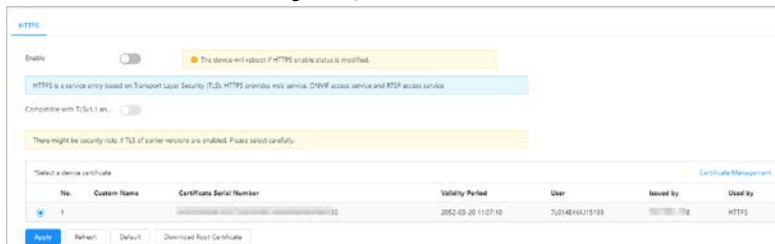
If you turn on **Compatible with TLSv1.1** and earlier versions, security risks might occur.
Please be advised.

Step 3 Select the certificate.



If there is no certificate in the list, click **Certificate Management** to upload certificate. For details, see "2.2.16.4.1 Installing Device Certificate".

Figure 2-50 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 web page will display the certificate is wrong or untrusted.

2.2.16.3 Attack Defense

2.2.16.3.1 Configuring Firewall

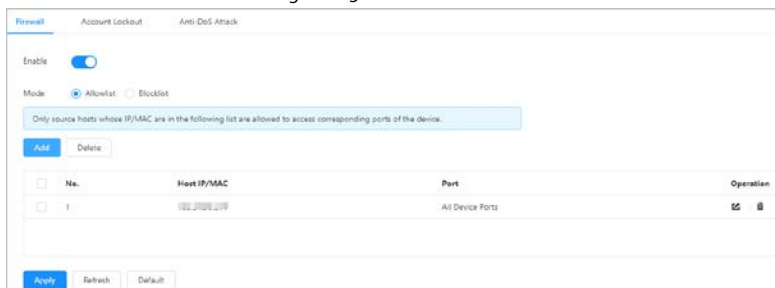
Configure firewall to limit access to the Access Terminal.

Procedure

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

Step 2 Click to enable the firewall function.

Figure 2-51 Firewall



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

- **Allowlist**: Only IP/MAC address in the allowlist can access the Access Controller.
- **Blocklist**: The IP/MAC addresses in the blocklist cannot access the Access Controller.

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



Figure 2-52 Add

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following elements:

- Add Mode:** A dropdown menu with "IP" selected.
- IP Version:** A dropdown menu with "IPv4" selected.
- IP Address:** A text input field with four placeholder boxes and a delete icon.
- All Device Po...:** A toggle switch that is currently turned on (blue).
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Step 5 Click OK.

Related Operations

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

2.2.16.3.2 Configuring Account Lockout

If wrong password is entered in a row for defined times, the account will be locked.

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

Step 2 Enter the login attempts and lock time for administrator account and ONVIF user.

- **Login attempt:** The upper limit of login attempts. If wrong password is entered in a row for the defined times, the account will be locked.
- **Lock time:** The duration during which you cannot log in after the account is locked.

Figure 2-53 Account lockout

Device Account

Login Attempt

Lock Time min

ONVIF User

Login Attempt

Lock Time min

Step 3 Click **Apply**.

2.2.16.3.3 Configuring Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Access Controller against Dos attack.

Step 1 Select **Security > Attack Defense > Anti-DoS Attack**.

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

Figure 2-54 Anti-DoS attack

SYN Flood Attack Defense

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack Defense

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

Apply Refresh Default

Step 3 Click **Apply**.

2.2.16.4 CA Certificate

2.2.16.4.1 Installing Device Certificate

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

Creating Certificate

Creating certificate for the Access Controller.

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 2-55 Certificate information

Step 2: Fill in certificate information. X

Custom Name

* IP/Domain Name

Organization Unit

Organization

* Validity Period Days (1~5000)

* Country

Province

City Name

Back Create and install certificate Cancel




The country name cannot exceed two characters. We recommend you enter the abbreviation of country name.

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

The newly installed certificate displays on the **Device Certificate** page after successful installation.

Related Operations

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

Applying for and Importing CA Certificate

Import the third-party CA certificate to the Access Controller.

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 Click **Browse** to select

Step 5 Enter the certificate information.

- IP/Domain name: the IP address or domain name of the Access Terminal.
- Country: The country name must not exceed three characters. We recommend you enter the abbreviation of country name.

Figure 2-56 Certificate information (2)

The screenshot shows a dialog box titled "Step 2: Fill in certificate information." with a close button (X) in the top right corner. The form contains the following fields:

- * IP/Domain Name:
- Organization Unit:
- Organization:
- * Validity Period: Days (1~5000)
- * Country:
- Province:
- City Name:

At the bottom of the dialog, there are three buttons: "Back", "Create and Download" (highlighted in blue), and "Cancel".

Step 6 Click **Create and Download**.

Save the request file to your computer.

Step 7 Apply to a third-party CA authority for the certificate by using the request file.


Step 8 Import the signed CA certificate.

- 1) Save the CA certificate to your computer.
- 2) Click **Installing Device Certificate**.
- 3) Follow [Step 2](#) to [Step 4](#), and then select the certificate.
- 4) Click **Install and Import**.

The newly installed certificate displays on the **Device Certificate** page after successful installation.

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

Related Operations

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

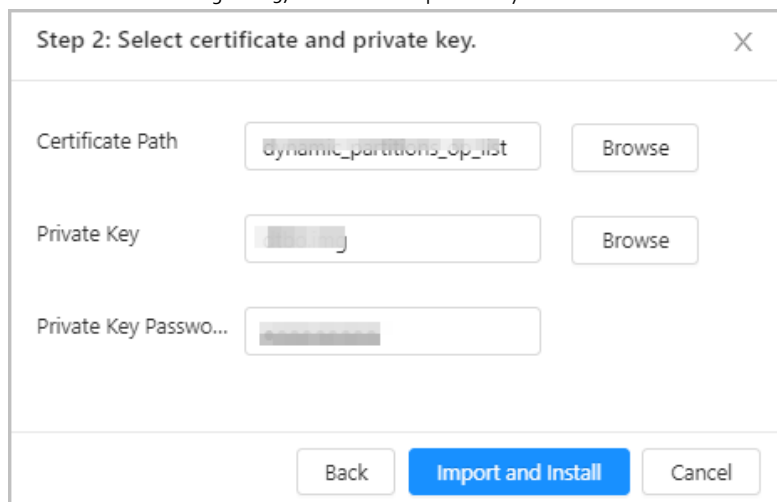
Installing Existing Certificate

If you already have a certificate and private key file, please 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 2-57 Certificate and private key



- Step 5** Click **Import and Install**.
The newly installed certificate displays on the **Device Certificate** page after successful installation.

Related Operations

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

2.2.16.4.2 Installing Trusted CA Certificate

A trusted CA certificate is a digital certificate to validate the identities of websites or server. For example, when 802.1x protocol is used, CA certificate for switch is required to authenticate its identity.

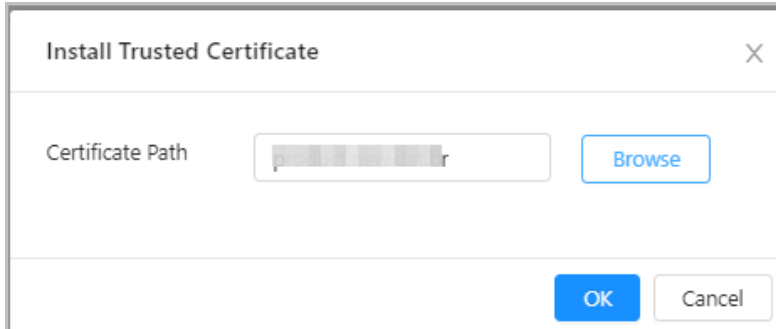
802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network.

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 2-58 Install trusted certificate



Step 4 Click **OK**.

The newly installed certificate displays on the **Trusted CA Certificates** page after successful installation.

Related Operations

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

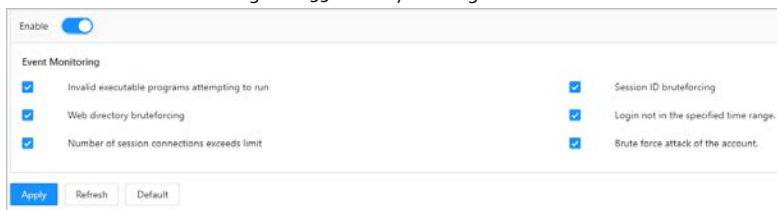
2.2.16.5 Security Warning

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

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 2-59 Security warning



Step 4 Click **Apply**.

2.2.17 Access Monitoring

2.2.17.1 Remotely Opening and Closing Door

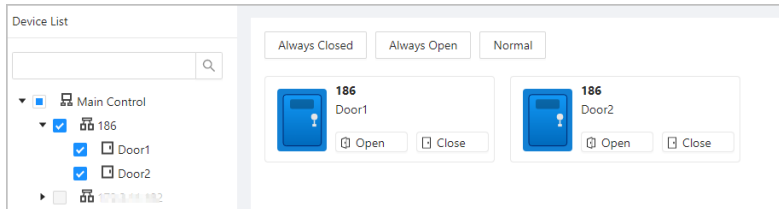
You can remotely monitor and control door through Smart PSS Lite. For example, you can remotely open or close the door.

Procedure


Step 1 Click **Access Monitoring** on the home page.

Step 2 Select the door, and then click **Open** or **Close** to remotely control the door.

Figure 2-60 Remotely control the door



Related Operations

- Event filtering: Select the event type in the **Event Info**, and the event list displays the selected event type, such as alarm events and abnormal events.
- Event deleting: Click  to clear all events in the event list.

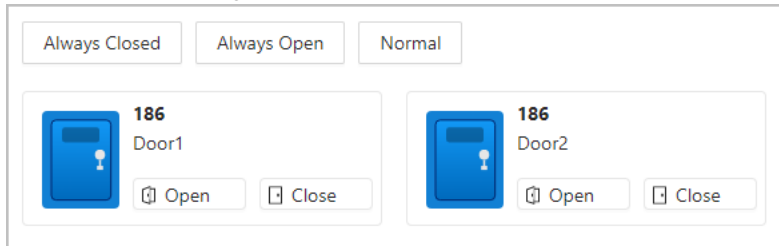
2.2.17.2 Setting Always Open and Always Close

After setting always open or always close, the door remains open or closed all the time.

Step 1 Click **Access Monitoring** on the home page.

Step 2 Click **Always Open** or **Always Close** to open or close the door.

Figure 2-61 Always open or close



The door will remain open or closed all the time. You can click **Normal** to restore the access control to normal status, and the door will be open or closed based on the configured verification methods.

2.3 Configurations on Sub Controller

You can log in to the webpage of the sub controller to configure it locally.

2.3.1 Initialization

Initialize the sub controller when you log in to the webpage for the first time or after the sub controller is restored to the factory defaults. For details on how to initialize the sub controller, see "2.2.2 Initialization".

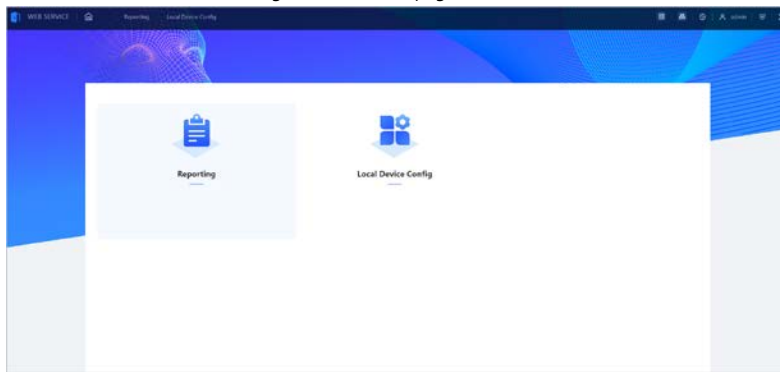
2.3.2 Logging In

Set the access control to sub control during the log in wizard. For details, see "2.2.3 Logging In"

2.3.3 Home Page

The webpage of the sub controller only includes **Local Device Config** and **Reporting** menu. For details, see "2.2.14 (Optional) Local Device Configurations" and "2.2.15 Viewing Records".

Figure 2-62 Home page



3 Smart PSS Lite-Sub Controllers

3.1 Networking Diagram

The sub controllers are added to a standalone management platform, which is SmartPSS Lite. You can manage all sub controllers through the SmartPSS Lite.

Figure 3-1 Networking Diagram



3.2 Configurations on SmartPSS Lite

Add sub controllers to SmartPSS Lite and configure them on the platform. For details, see the user's manual of the SmartPSS Lite.

3.3 Configurations on Sub Controller

For details, see "2.3 Configurations on Sub Controller".

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic equipment network security:

1. Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024-65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

- **SNMP:** Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- **SMTP:** Choose TLS to access mailbox server.
- **FTP:** Choose SFTP, and set up strong passwords.
- **AP hotspot:** Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

- **Check online users:** we suggest that you check online users regularly to see if the device is logged in without authorization.
- **Check equipment log:** By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- **Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.**
- **The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.**
- **Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.**
- **Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.**