ARMATURA

User Manual

ARMATURA ONE

Armatura One 4.1.0

Date: December 2024

Doc Version: 3.0

Copyright © 2024 ARMATURA LLC. All rights reserved.

Without the prior written consent of ARMATURA, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ARMATURA and its subsidiaries (hereinafter the "Company" or "ARMATURA").

Trademark

ARMATURA is a registered trademark of ARMATURA. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

The copyright in all the documents, drawings, etc. in relation to the ARMATURA supplied equipment vests in and is the property of ARMATURA. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ARMATURA.

The contents of this manual must be read before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ARMATURA before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel have read, understood, and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/ documents shall prevail. The contract specific conditions/documents shall apply in priority.

ARMATURA offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ARMATURA does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability, or fitness for a particular purpose.

ARMATURA does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ARMATURA in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ARMATURA has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ARMATURA periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ARMATURA reserves the right to add, delete, amend, or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc.

 Copyright © 2024 ARMATURA LLC. All rights reserved

for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement/better operations of the machine/unit/ equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ARMATURA shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available at https://armatura.us/

If there is any issue related to the product, please contact us.

ARMATURA Headquarters

Address 190 Bluegrass Valley Parkway Alpharetta, GA 30005

Phone +1-650-4556863

Email: info@zktecousa.com

Website: www.zktecousa.com

About the Manual

This manual introduces the operations of Armatura One

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Copyright © 2024 ARMATURA LLC. All rights reserved

Table of Contents

1. OVERVIEW 8
1.1. PERSONNEL MODULE 9
1.2. ACCESS MODULE 9
1.3. ELEVATOR MODULE 9
1.4. VIDEO MODULE 9
1.5. ENTRANCE CONTROL 9
1.6. DATA MONITOR MODULE 9
1.7. SYSTEM MODULE 9
2. SYSTEM OPERATIONS 10
2.1. LOGIN TO THE SYSTEM 10
2.2. ALARM CENTER 12
2.3. MODIFYING PASSWORD 12
2.4. MODIFYING APPEARANCE 13
2.5. EXITING THE SYSTEM 13
3. ALARM CENTER 14
3.1. PERSONNEL TRACKING 16
3.2. VEHICLE TRACKING 17
3.3. BATCH DOOR OPERATIONS 18
3.4. BATCH CAMERA OPERATIONS 19
3.5. DEVICE SEARCH 20
3.6. BROWSER NOTIFICATIONS 20
4. SYSTEM MESSAGES 24
4.1. MESSAGE NOTIFICATION BAR 24
4.2. MESSAGE MANAGEMENT 26
4.3. SYSTEM MESSAGES 28
5. PERSONNEL MANAGEMENT 29
5.1. PERSONNEL 30
5.1.1. PERSONNEL 31
5.1.2. ORGANIZATION 60
5.1.3. POSITION 65
5.1.4. DISMISSED PERSONNEL 69
5.1.5. PENDING REVIEW 71
5.1.6. BLOCK LIST 73
5.1.7. CUSTOM ATTRIBUTES 74
5.1.8. PARAMETERS 77
5.1.9. DUPLICATE PERSONNEL 80
5.2. CARD MANAGEMENT 82
5.2.1. CARD MANAGEMENT 82
5.2.2. WIEGAND FORMATS 84
5.2.3. ISSUED CARD RECORDS 90
5.2.4. CARD PARAMETERS 91
6. ACCESS CONTROL MANAGEMENT 92
6.1. DEVICE 92
6.1.1. DEVICE FUNCTION 93
6.1.2. I/O BOARD 154

Copyright © 2024 ARMATURA LLC. All rights reserved

6.1.3. DOOR 161
6.1.4. READER 175
6.1.5. AUXILIARY INPUT 181
6.1.6. AUXILIARY OUTPUT 185
6.1.7. EVENT TYPE 190
6.1.8. DAYLIGHT SAVING TIME (DST) 192
6.2. MONITORING 196
6.2.1. DEVICE MONITORING 196
6.2.2. REAL-TIME MONITORING 199
6.2.3. TOPOLOGY MANAGEMENT 211
6.3. ACCESS CONTROL 214
6.3.1. TIME ZONES 215
6.3.2. HOLIDAY MANAGEMENT 218
6.3.3. ACCESS LEVELS 221
6.3.4. SET ACCESS BY LEVELS 242
6.3.5. SET ACCESS BY PERSON 247
6.3.6. SET ACCESS BY ORGANIZATION 251
6.3.7. INTERLOCK 253
6.3.8 LINKAGE 258
6.3.9 ANTI-PASSBACK 269
6.3.10 FIRST-PERSON NORMALLY OPEN 280
6.3.11 MULTI-PERSON GROUP 285
6.3.12 MULTI-PERSON OPENING DOOR 289
6.3.13 VERIFICATION MODE 292
6.3.14 VERIFICATION MODE GROUP 298
6.3.15 PARAMETERS 300
6.4 ADVANCED FUNCTIONS 304
6.4.1 ZONE 304
6.4.2 READER DEFINE 309
6.4.3 WHO IS INSIDE 314
6.4.4 GLOBAL LINKAGE 315
6.4.5 GLOBAL INTERLOCK GROUP 321
6.4.6 GLOBAL INTERLOCK 324
6.4.7 PERSON AVAILABILITY 328
6.4.8 OCCUPANCY CONTROL 334
6.4.9 MUSTER POINT 337
6.4.10 MUSTER POINT REPORT 340
6.5 REPORTS 343
6.5.1 ALL TRANSACTIONS 344
6.5.2 EVENTS FROM TODAY 346
6.5.3 ALL EXCEPTION EVENTS 347
6.5.4 ACCESS RIGHTS BY DOOR 349
6.5.5 ACCESS RIGHTS BY PERSONNEL 350
6.5.6 FIRST IN AND LAST OUT 352
6.5.7 DEVICE LOG 354
6.5.8 DEVICE FACE EXTRACTION FAILURE LOG 355
6.5.9 ACCESS ALARM RECORDS 356
7 ENTRANCE CONTROL 358
7.1 CHANNEL DEVICE 358
7.1.1 PASSAGE 358
7.1.2 DEVICE 361
7.1.3 GATES 374
7.1.4 READER 377
7.1.5 AUXILIARY INPUT MANAGEMENT 379
7.1.6 EVENT TYPE MANAGEMENT 381
7.1.7 DAYLIGHT SAVING TIME 383

Copyright © 2024 ARMATURA LLC. All rights reserved

7.2 MONITORING 385
7.2.1 DEVICE MONITORING 385
7.2.2 REAL-TIME MONITORING 387
7.3 ENTRANCE CONTROL 390
7.3.1 BARRIER GATE PERMISSION GROUP 390
7.3.2 SET ACCESS BY LEVELS 394
7.3.3 ANTI-PASSBACK 397
7.3.4 LINKAGE 399
7.3.5 PARAMETERS 402
7.4 PASSAGE SETTINGS 404
7.4.1 BARRIER GATE PASSING RULES 404
7.4.2 SWING BARRIER 406
7.5 CHANNEL REPORTS 408
7.5.1 ALL TRANSACTIONS 408
7.5.2 EVENTS FROM TODAY 410
7.5.3 PERSONNEL LAST ACCESS LOCATION 411
7.5.4 ALL EXCEPTION EVENTS 412
8 ELEVATOR CONTROL MANAGEMENT 415
8.1 ELEVATOR SETTINGS 415
8.1.1 BUILDINGS 416
8.1.2 FLOORS 419
8.1.3 ELEVATOR GROUPS 425
8.1.4 ELEVATOR CARS 431
8.1.5 DEVICES 432
8.1.6 I/O BOARD 454
8.1.7 READERS 456
8.1.8 AUXILIARY INPUTS 458
8.1.9 EVENT TYPES 459
8.1.10 DAYLIGHT SAVINGS TIME 460
8.2 MONITORING 462
8.2.1 DEVICE MONITORING 462
8.2.2 REAL-TIME MONITORING 464
8.3 ELEVATOR CONTROL 468
8.3.1 TIME ZONES 468
8.3.2 HOLIDAYS 471
8.3.3 ELEVATOR LEVELS 474
8.3.4 SET ACCESS BY LEVELS 480
8.3.5 SET ACCESS BY PERSON 485
8.3.6 SET ACCESS BY ORGANIZATION 487
8.3.7 DEFAULT FLOOR 489
8.3.8 GLOBAL LINKAGES 490
8.3.9 PARAMETERS 495
8.4 REPORT 497
8.4.1 ALL TRANSACTIONS 497
8.4.2 ALL EXCEPTION EVENTS 499
8.4.3 ACCESS RIGHTS BY FLOOR 501
8.4.4 ACCESS RIGHTS BY PERSONNEL 502
8.5 DCS SETTINGS 504
8.5.1 INTEGRATED DEVICE 504
8.5.2 EXTERNAL READERS 506
8.5.3 INTERNAL READERS 510
8.5.4 OPERATION LOGS 514
9 VIDEO 515
9.1 VIDEO MANAGEMENT 515

Copyright © 2024 ARMATURA LLC. All rights reserved

9.1.1 DEVICE 515
9.1.2 PREVIEW 518
9.1.3 PLAYBACK 524
9.2 SETTINGS 528
9.2.1 ARTECO CONNECTOR 528
9.3 REPORTS 531
9.3.1 VIDEO EVENT RECORD 531
10 DATA MONITOR 534
10.1 DATA CHART 534
10.1.1 BASE CHART 534
10.2 FUNCTION CHART 546
10.2.1 ALARM MANAGEMENT 547
11 SYSTEM 569
11.1 GENERAL SETTINGS 569
11.1.1 AREA SETTINGS 569
11.1.2 ORGANIZATIONS 572
11.1.3 CERTIFICATE TYPES 578
11.1.4 MEDIA FILES 580
11.1.5 CARD TEMPLATES 583
11.2 DATA MANAGEMENT 586
11.2.1 OPERATION LOGS 587
11.2.2 DICTIONARY MANAGEMENT 588
11.2.3 DATABASE MANAGEMENT 588
11.2.4 DATA CLEANING 593
11.2.5 SYSTEM MONITORING 593
11.2.6 EVENT TYPES 595
11.3 AUTHORITY 595
11.3.1 USERS 596
11.3.2 USERS ONLINE 599
11.3.3 ROLES 600
11.3.4 APP MANAGEMENT 603
11.3.5 SECURITY PARAMETERS 605
11.3.6 THREAT LEVELS 606
11.4 PRIVACY SECURITY 610
11.4.1 PRIVACY AGREEMENT 610
11.5 COMMUNICATION 611
11.5.1 DEVICE COMMANDS 612
11.5.2 COMMUNICATION STATUS 613
11.5.3 PRODUCT DEFINITIONS 614
11.5.4 AUTHORIZED MANAGEMENT 617
11.5.5 COMMUNICATION SERVICES 619
11.6 INTEGRATION 620
11.6.1 PLATFORM CONNECTIONS 620
11.6.2 E-MAIL MANAGEMENT 630
11.6.3 MESSAGES MANAGEMENT 632
11.6.4 AD MANAGEMENT 634
11.6.5 SYSTEM MESSAGE 635
11.6.6 MAP CONFIGURATION 636
11.6.7 API AUTHORIZATION 641

Copyright © 2024 ARMATURA LLC. All rights reserved

1. Overview

The ARMATURA One software provides a unified management platform, enabling efficient, streamlined management and integration of security operations with minimal efforts. Its robust data processing capabilities support up to 300,000 personnel records simultaneously, ensuring high performance and data security. The platform employs role-based, multi-level management to protect user information and delivers real-time event and operation tracking with timely notifications for system users.

Key Features

- High-Capacity Data Management: Manages up to 300,000 personnel records efficiently with powerful data processing capabilities.
- Enhanced Data Security: Utilizes role-based, multi-level access management to safeguard user information.
- Real-Time Tracking and Notifications: Monitors events and operations in real-time, providing prompt feedback to system administrators.

System Requirements

- Processor: Quad-core, 2.5 GHz or higher.
- Memory: 16GB DDR4 or above.
- Storage: 500GB of available space; NTFS partition recommended for installation directory.
- Display: Monitor with 1920*1080 resolution or higher.

Supported Platforms and Software

Operating Systems	Windows 11 Windows Server 2012/2016/2019/2022
Supported Databases	PostgreSQL (Default), SQL Server & Oracle (Optional).
Recommended Browser Version	Chrome 33+ Microsoft Edge 88+ Firefox 27+

Copyright © 2024 ARMATURA LLC. All rights reserved

Modules

The system includes 7 distinct modules, structured to support comprehensive management and operational functions.

1.1. Personnel Module

The Personnel Module manages employee information and organizational structure through two main components: Department Management, which allows configuration of the company's organizational hierarchy, and Personnel Management, which handles employee data entry, departmental assignments, and staff administration.

1.2. Access Module

The Access Module is a web-based management system for access control, facilitating the management of networked access control panels and unified personnel access. It enables functions such as setting door access schedules and access levels for registered users, ensuring secure and organized entry control.

1.3. Elevator Module

The Elevator Module configures elevator parameters (e.g., swiping interval and elevator key duration), manages personnel access rights to specific floors, and supervises elevator-related events. Permissions can be set so that only authorized users may access certain floors for a defined period post-authentication. The system is compatible with third-party elevators, including brands such KONE, Mitsubishi, and Hitachi.

1.4. Video Module

The Video Module is integrated with Hanwha Wave, DW Spectrum, and Arteco's Omnia Video Management Systems, supporting functions such as live preview, playback, and recording. Additional applications, such as video patrols, enhance monitoring capabilities.

1.5. Entrance Control

The Entrance Control module connects to the gate control board through channel devices (e.g., TDA integrated machines), enabling software-based configuration of gate parameters. This setup controls entry and exit at gates, facilitating automated gate management.

1.6. Data Monitor Module

The Data Monitor Module consolidates and analyzes system data, providing intuitive security insights. It tailors data displays for different roles, offering targeted guidance to help users assess security levels and make informed decisions to enhance system security.

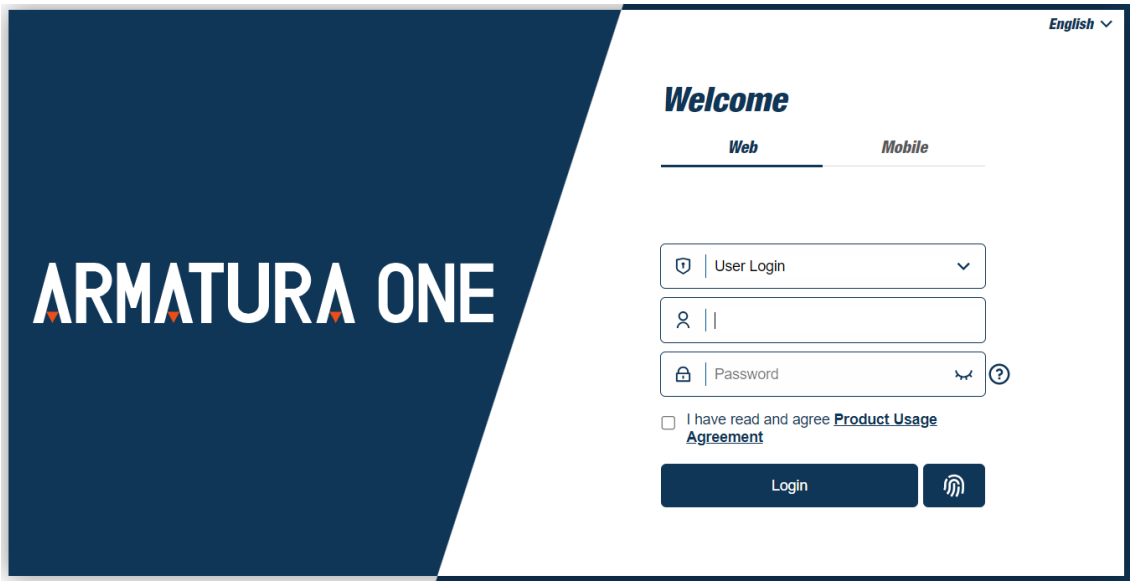
1.7. System Module

The System Module allows for the assignment of system users and role-based module access configurations. It includes database management functions, such as backup, initialization, and recovery, as well as system parameter settings and operational log management.

Copyright © 2024 ARMATURA LLC. All rights reserved

2. System Operations

2.1. Login to the System



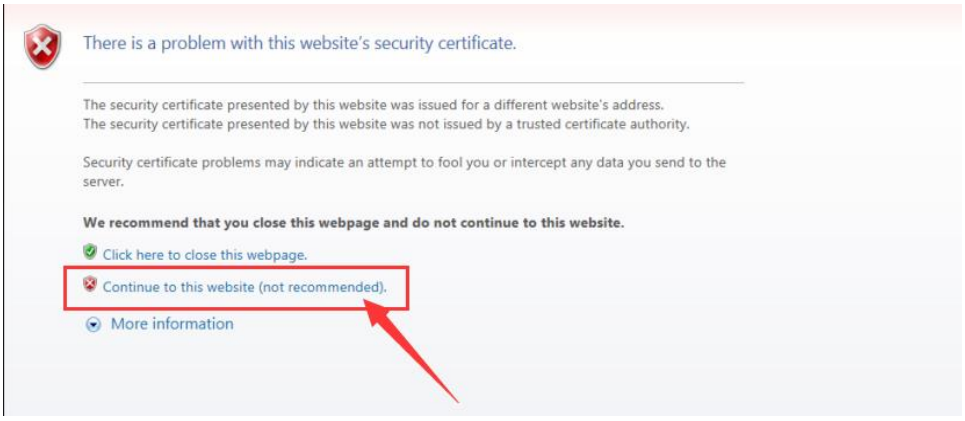
After installing the software, you can access the system in the following ways:

- Option 1: double-click the ARMATURA One icon to access the system.
- Option 2: Open the recommended browser and enter the IP address and server port in the address bar. By default, the IP address is set to https://127.0.0.1:8098

Note:

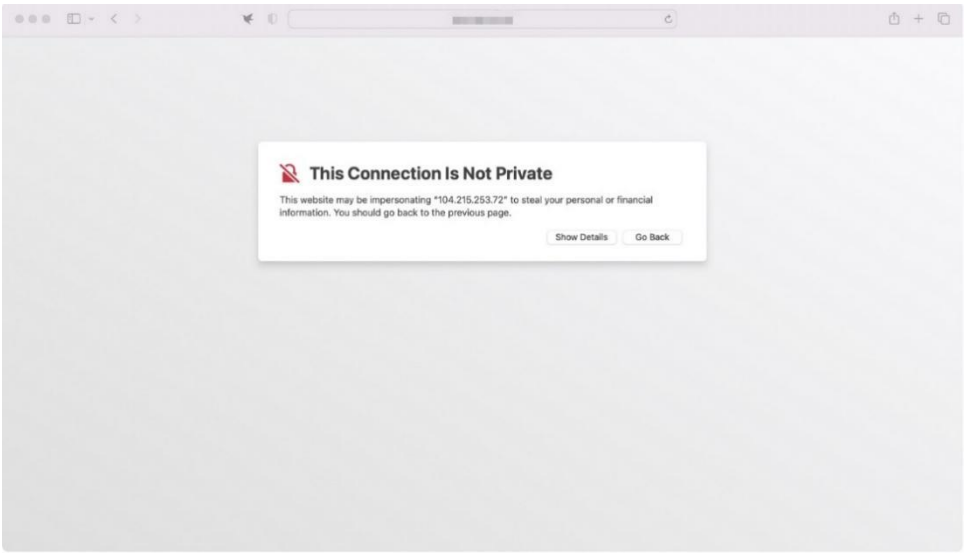
The username of the super user is **[admin]**, and the password is **[admin]**. After the first login to the system, please reset the password.

If you have selected the HTTPS port during software installation, input the server IP address and port number (for example, https://127.0.0.1:8098) in the address bar and press Enter. The following prompt may be displayed:

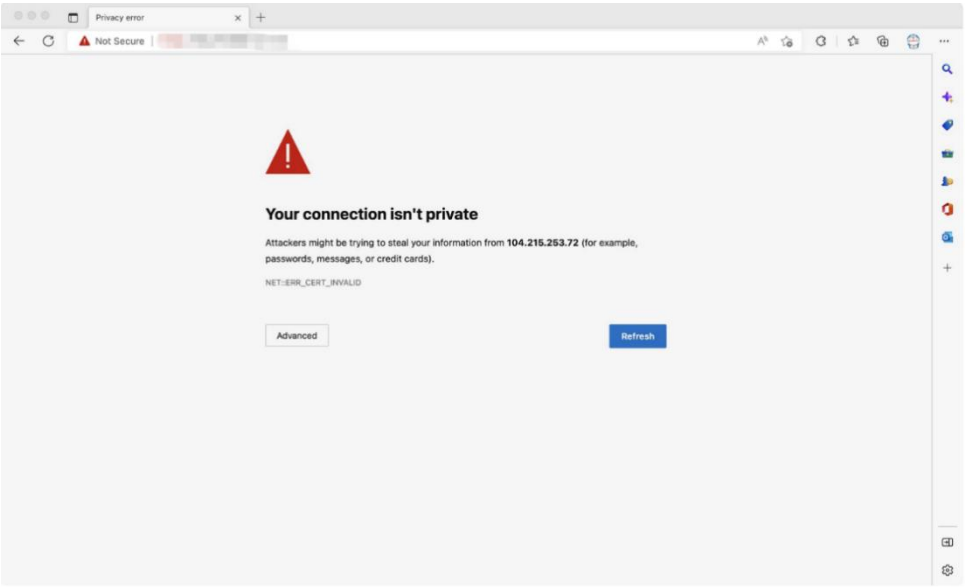


- Windows Users**:** Click "Continue to this website" as shown. Note that the exact steps may vary by browsers.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Mac Users (Safari): In the security prompt window, click “Show Details” and “Visit the Website”.

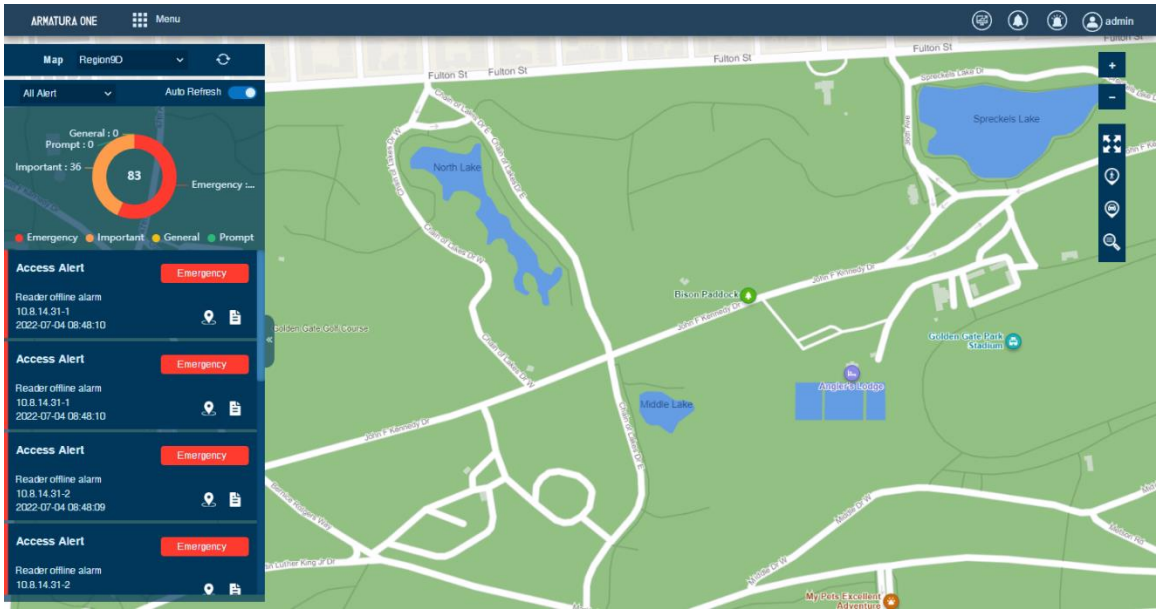


- Microsoft Edge Users: When this page appears, click “Advanced” and continue to **[Server address]**.

Copyright © 2024 ARMATURA LLC. All rights reserved

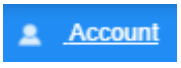
2.2. Alarm Center

After logging in, the home page will be displayed as shown below. To return to the home page from any screen, click the home icon located in the upper left corner of the interface.

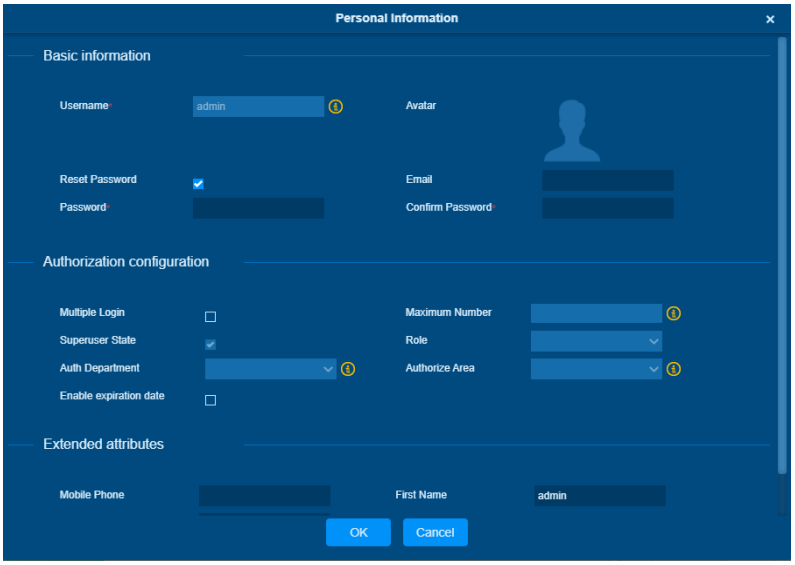


System Activation: Please refer to the license document for details on system activation.

2.3. Modifying Password

To modify your login password, go to **[Account]** 

and then check the **[Reset Password]** to modify the password.

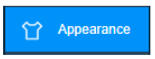


Note:

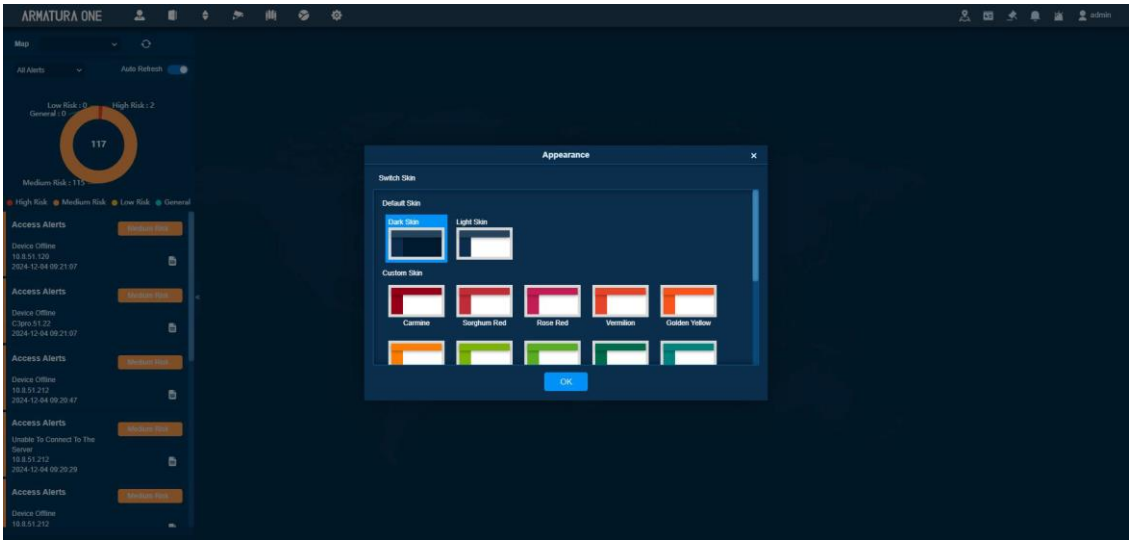
- Both the super user and any new users are created by the super user.
- Usernames are not case-insensitive, but the password is case-sensitive.

Copyright © 2024 ARMATURA LLC. All rights reserved

2.4. Modifying Appearance

To change the appearance of the interface, click the **[Appearance]** button 

and select your preferred theme.



2.5. Exiting the System

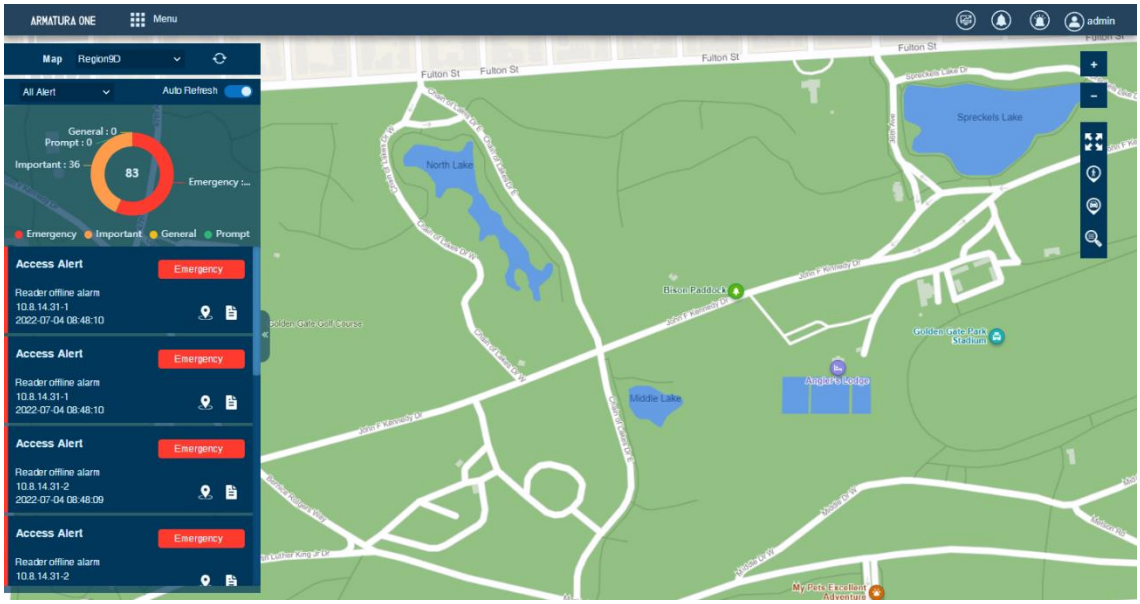
To log out, click the **[Logout]** button

on the upper right corner of the interface.

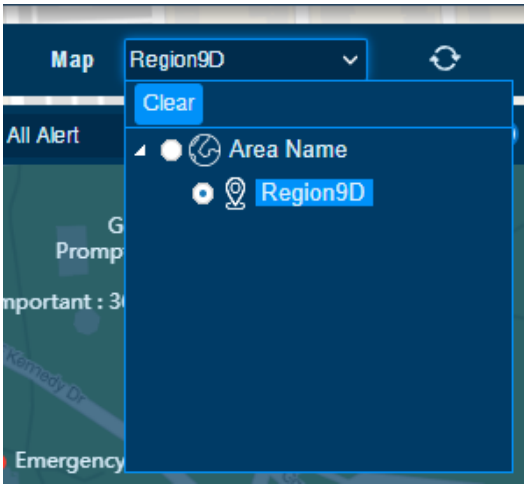
Copyright © 2024 ARMATURA LLC. All rights reserved

3. Alarm Center

The Alarm Center displays alerts triggered when a device detects abnormal conditions that meet the specified alarm criteria. Users can view, filter, and manage these alarms as follows:



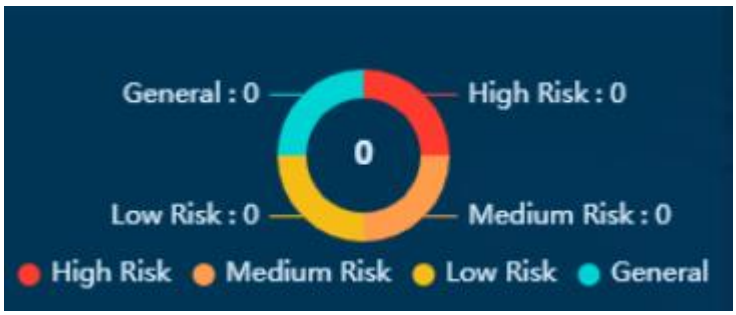
1. Map Navigation: Use the drop-down menu to switch between maps in different areas.



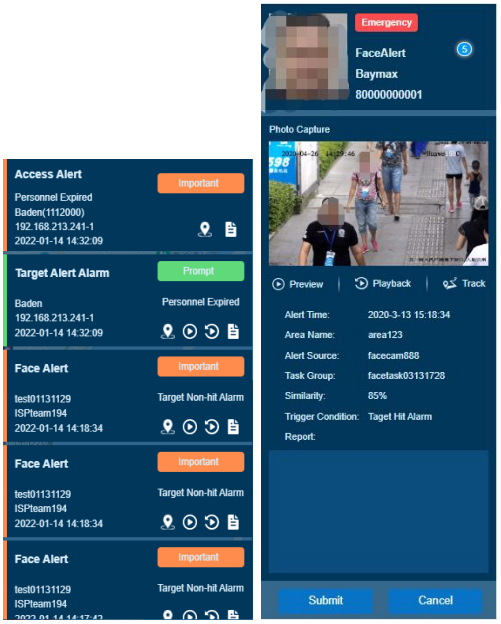
2. Use the drop-down menu to view different types of alerts, including Access Alerts. These alarms are configured in the Access and Video modules.

3. Auto Refresh: Toggle the Auto Refresh feature on or off to focus on specific alarms or to view real-team alarm data as it updates.

Copyright © 2024 ARMATURA LLC. All rights reserved



4. Dashboard Filters: The dashboard not only displays alerts counts but also offers filtering options to help you quickly locate relevant alerts.

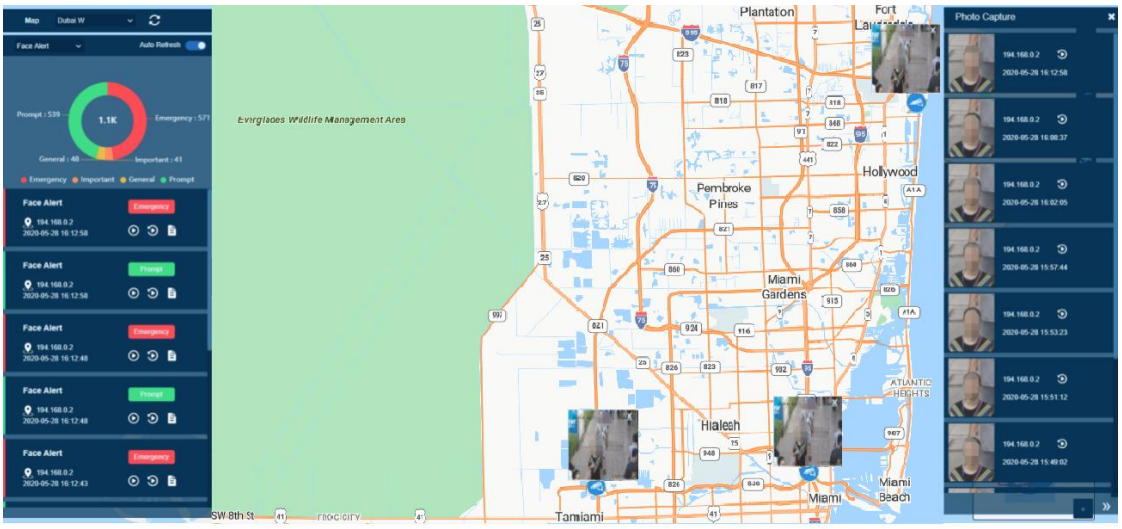


5. Alarm list: The alarm list allows you to locate devices associated with alerts, view previews and playback, and access detailed alarm information for resolution.

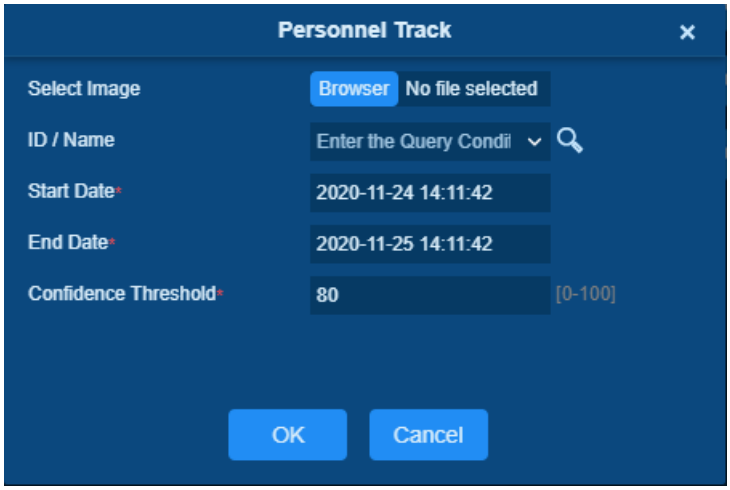
Copyright © 2024 ARMATURA LLC. All rights reserved

3.1. Personnel Tracking

The Personnel Track feature maps the trajectory of individuals' movements using data captured by cameras.



- Instructions: Click "Personal Track", then upload a photo of the person or select an employee/guest and set the desired parameters.

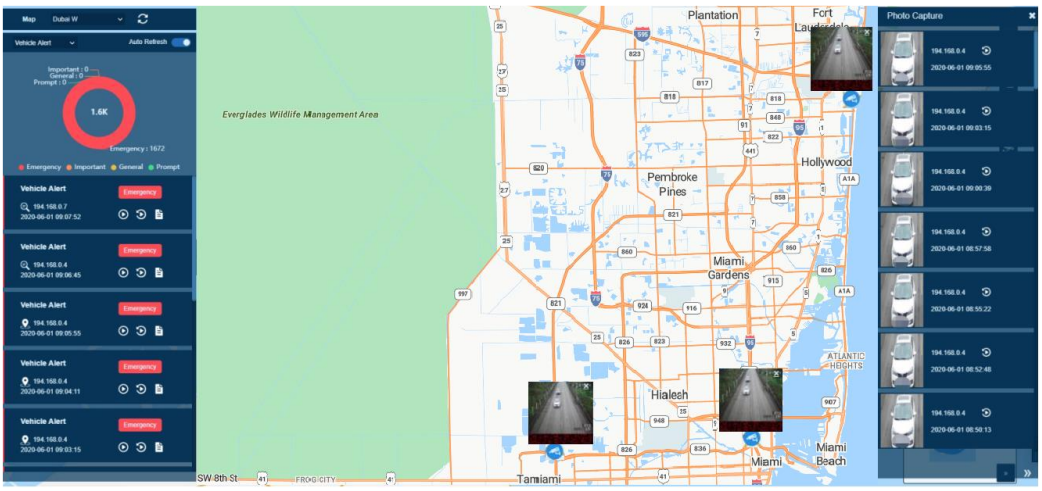


- Playback: Users can view playback of captured images from the list on the right side of the screen.

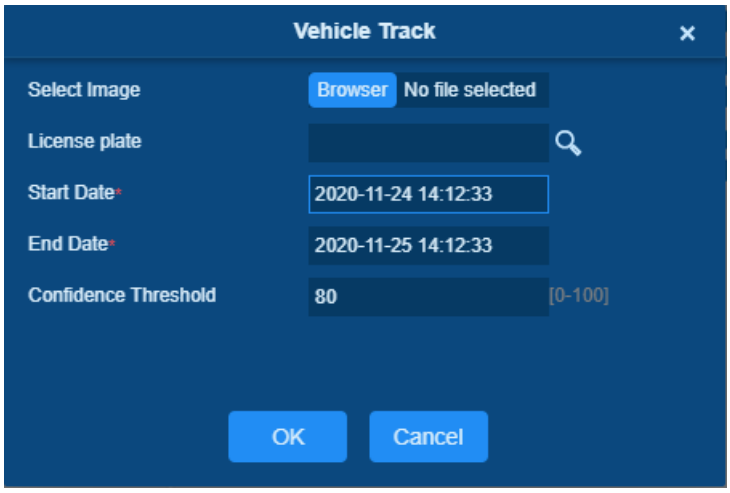
Copyright © 2024 ARMATURA LLC. All rights reserved

3.2. Vehicle Tracking

The Vehicle Tracking feature simulates vehicle movements on a map using data captured by cameras.



- Instructions: Click “Vehicle Tracking”, then upload a photo of the vehicle of select a license plate from the Parking module and set parameters.

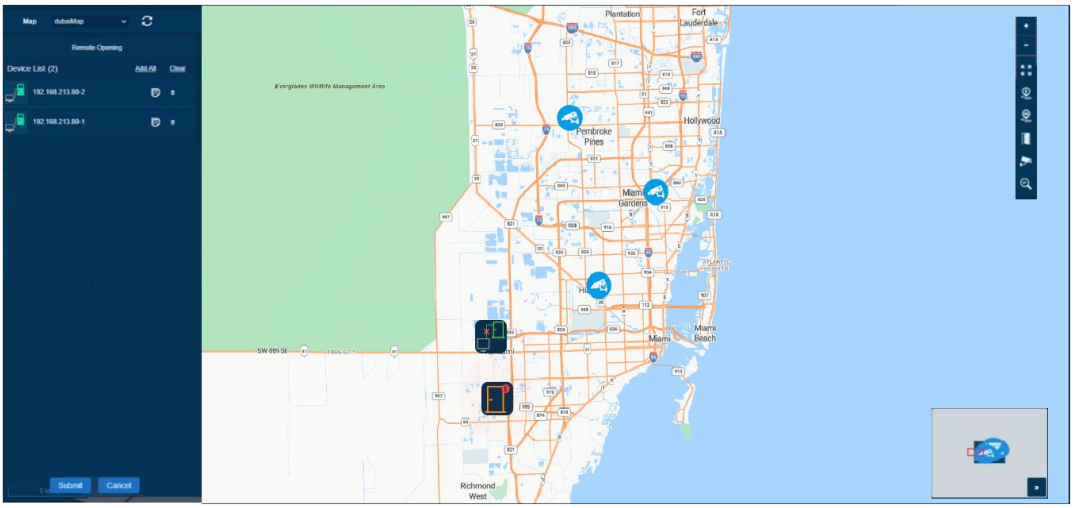


- Playback: Users can access playback of captured images from the list on the right.

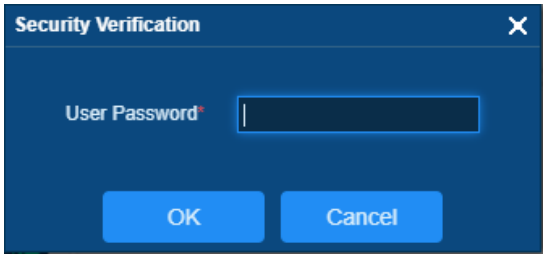
Copyright © 2024 ARMATURA LLC. All rights reserved

3.3. Batch Door Operations

Batch Door Operations allow users to perform quick actions on multiple doors, including remote open/close, lockdown activation/deactivation, cancelling alarms, and setting doors to “Normally Open”.



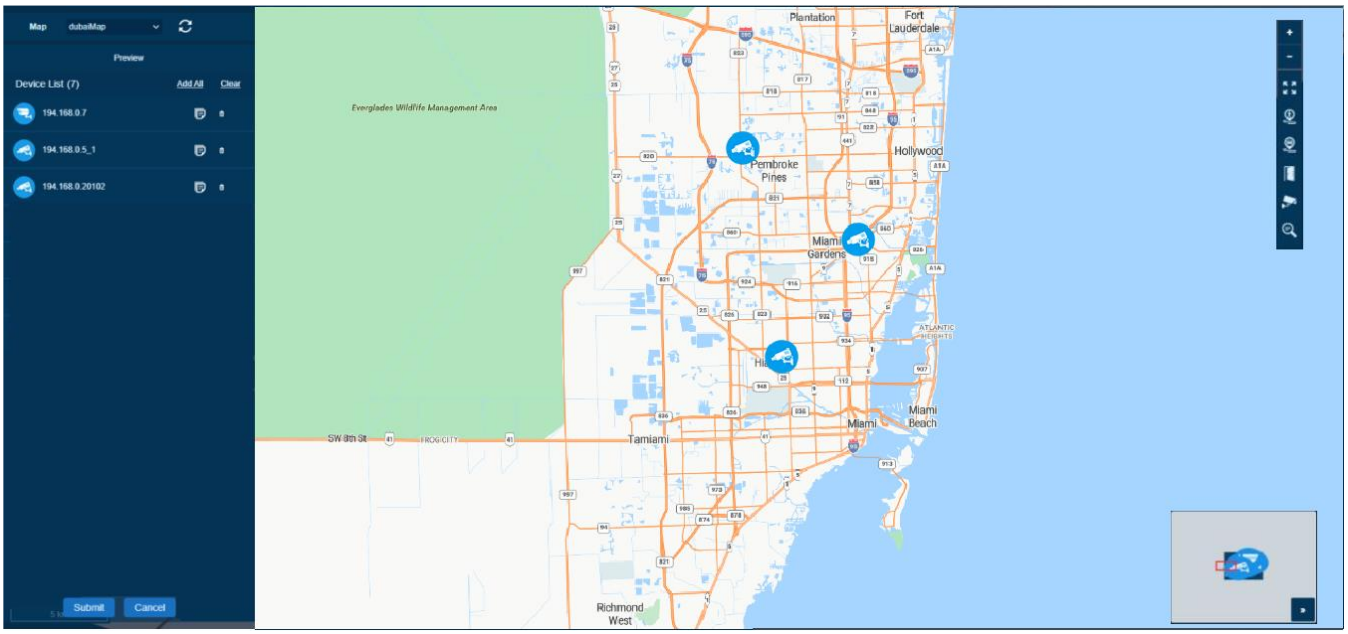
- Instructions: Use the selection tool to choose specific doors or click “Add All” to select all doors. Submit the action and enter the user password to proceed.



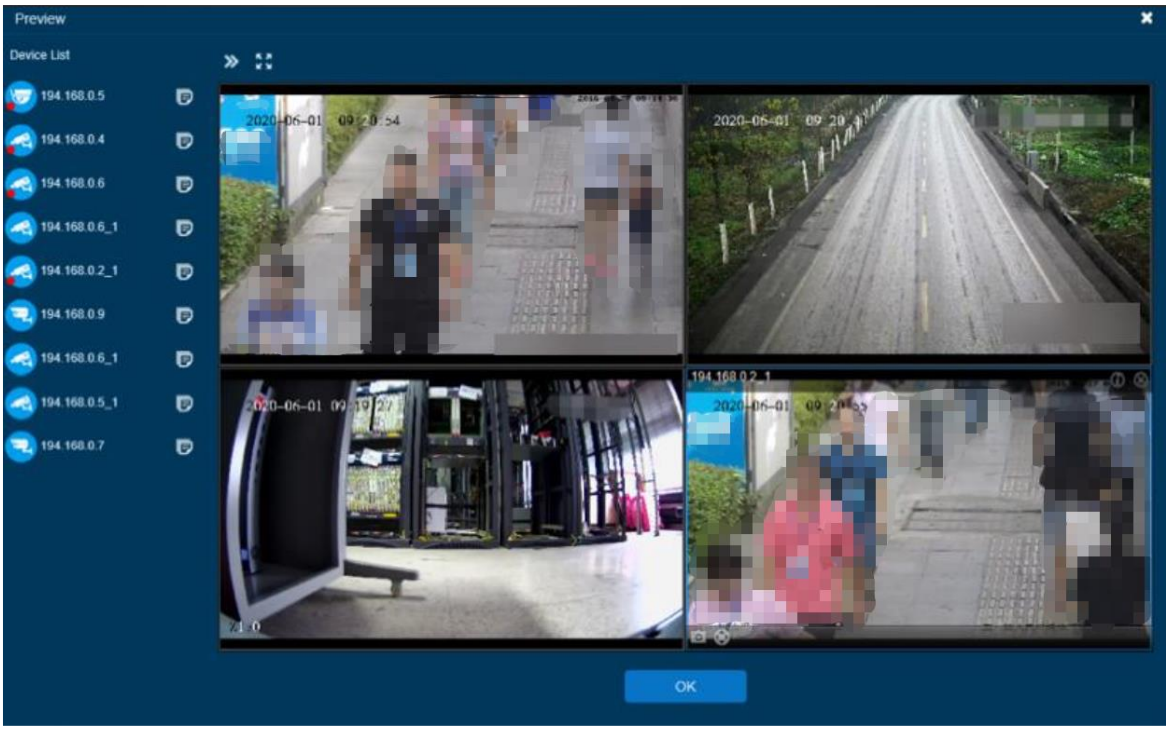
Copyright © 2024 ARMATURA LLC. All rights reserved

3.4. Batch Camera Operations

This feature allows users to perform batch operations on camera previews.



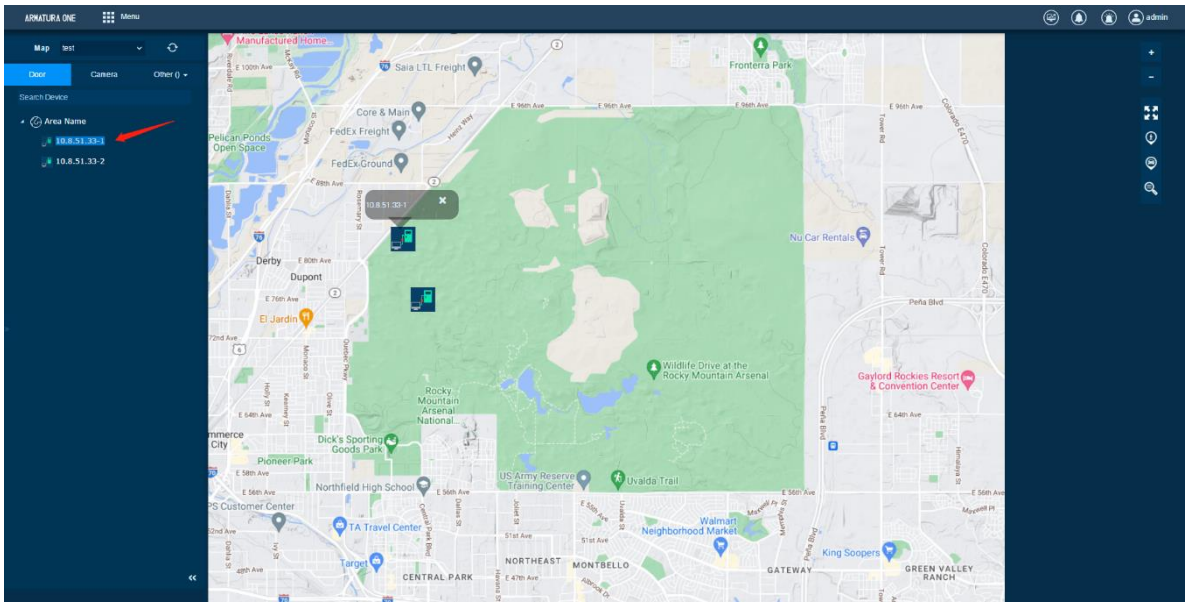
- Instructions: Select individual cameras using the frame selection tool or click “Add All” to choose all cameras, then submit to proceed.



Copyright © 2024 ARMATURA LLC. All rights reserved

3.5. Device Search

The Device Search function allows users to locate devices on the map easily.



- Instructions: Click “Search Device” and center the device name of select if from the list. The map will automatically adjust to center on the selected device.

3.6. Browser Notifications

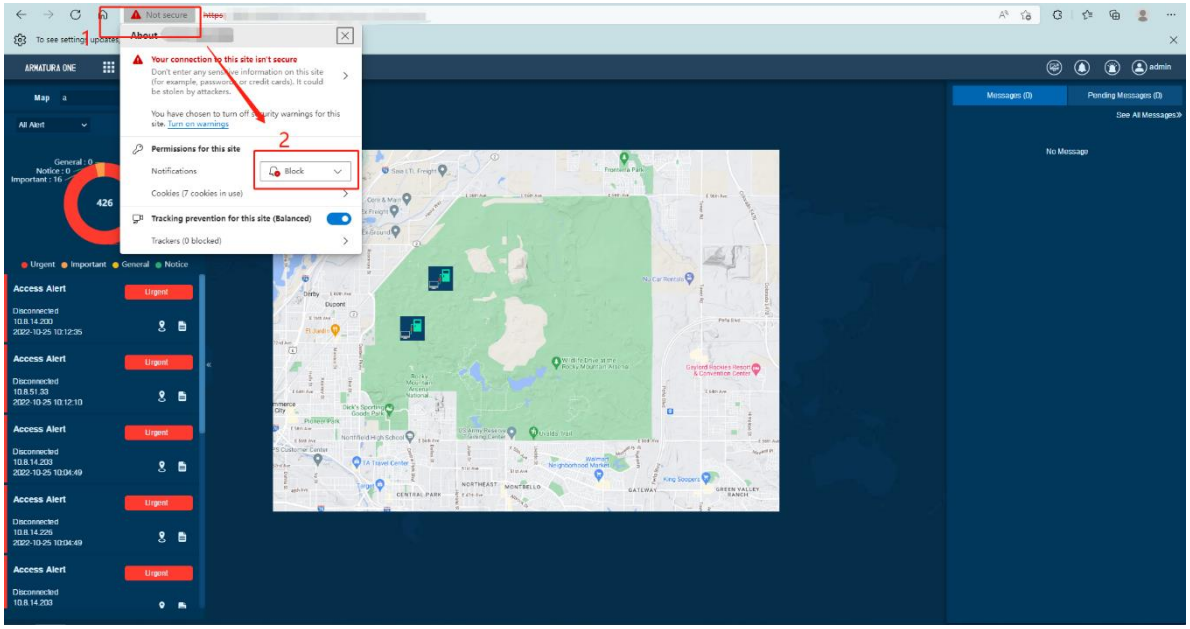
The Browser Notification feature prevents users from missing important software messages by enabling pop-up alerts even when the application runs in the background.

Enable Browser Notifications

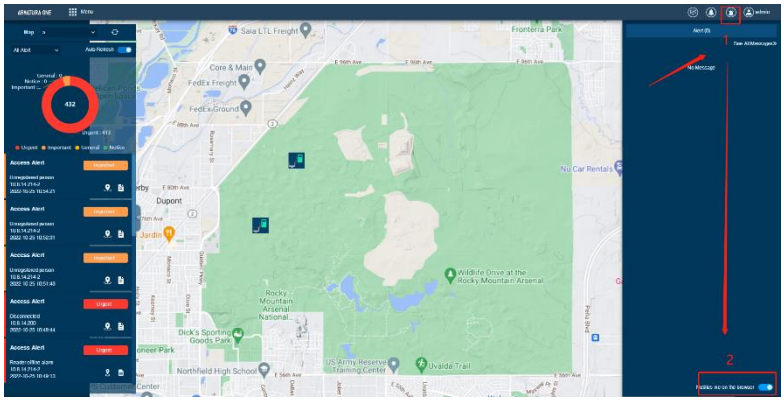
There are two ways to enable browser notifications:

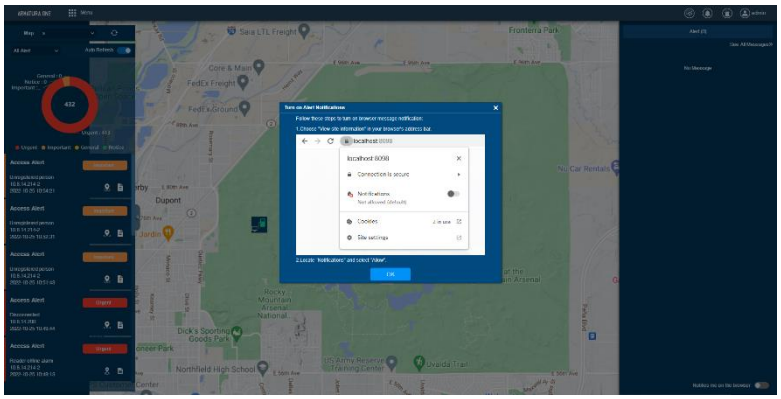
1. After successfully logging into the system, a pop-up window for browser authorization will appear. Click the **[Allow]** button to enable notifications, as shown in the figure below.

Copyright © 2024 ARMATURA LLC. All rights reserved



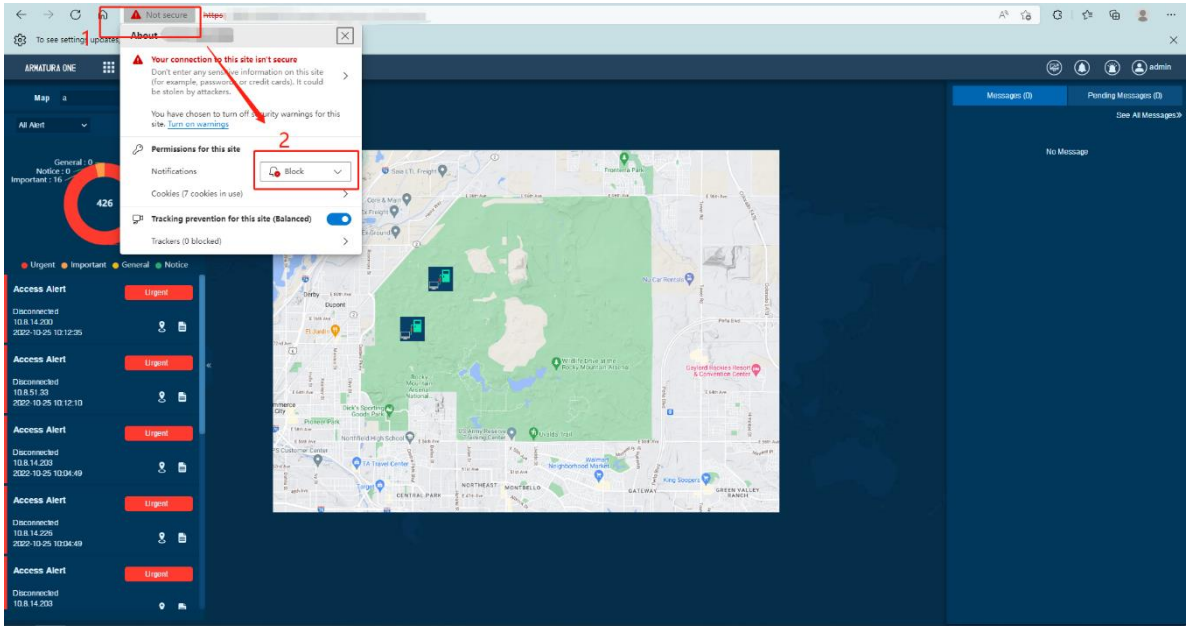
2. If users have already clicked **[Block]** and need to restart message notifications, click the button on the application's home page, then click the notifications button. A corresponding operation prompt will appear—follow the prompt to enable browser notifications.





Copyright © 2024 ARMATURA LLC. All rights reserved

3. Follow steps ① and ② to change message notification authorization, as shown in the figure below.

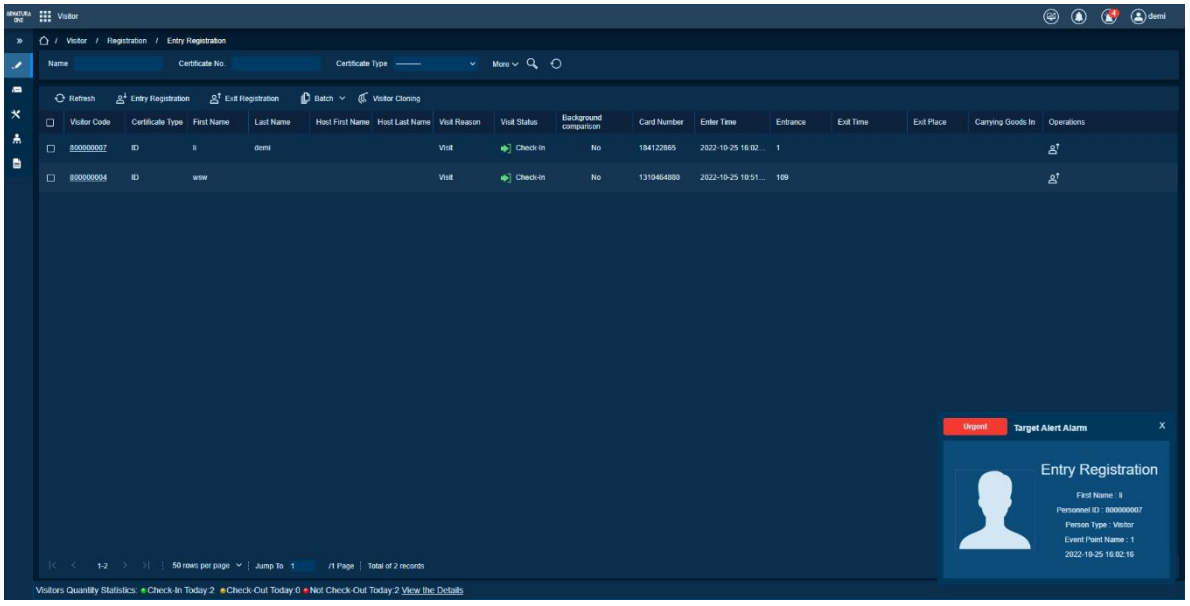


Viewing Notification Details

Note: Users may need to configure their computers to receive notifications from the application.

Viewing Notification Details below:

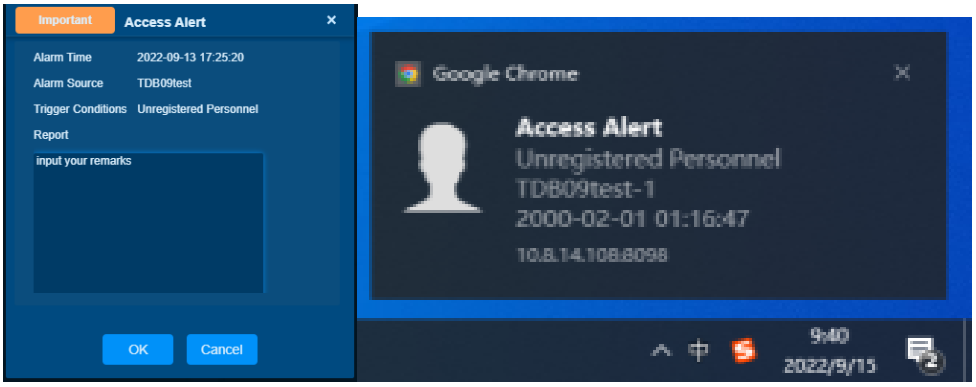
- Notification Pop-up: Double-click a notification pop-up to view detailed event information.



- Unread Messages: Click the Alert Button to view a list of unread messages.

Copyright © 2024 ARMATURA LLC. All rights reserved

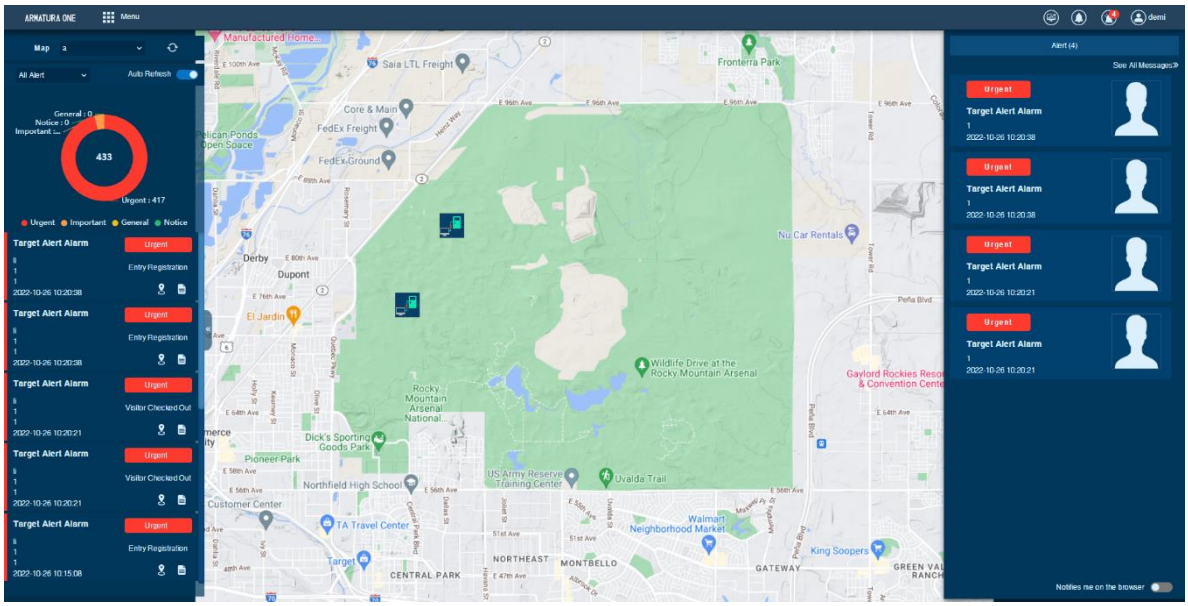
- If a pop-up notification appears, user can double-click the message interface to view the event details.



- When the software is running in the background, the browser can also send pop-up messages.

Note:

Users may need to configure their servers to receive notifications from the application. Once configured, user can view a list of unread messages by clicking the **[Alert]** button .



Copyright © 2024 ARMATURA LLC. All rights reserved

4. System Messages

System Messages provide notifications based on event types generated by each module, such as a successful Visitor Module reservation approval, an Office Module meeting room repair report, or a meeting room booking. Relevant system personnel receive message statuses and detailed lists, enabling users to log in and view updates.

4.1. Message Notification Bar

Function Description

Each event generated by the system is sent to the designated handler. After logging in, the handler can click the message button (the notification bar shows all unread messages) to review and process notifications. The bell icon displays the total number of unread messages awaiting the user's attention.

Prerequisites for Use

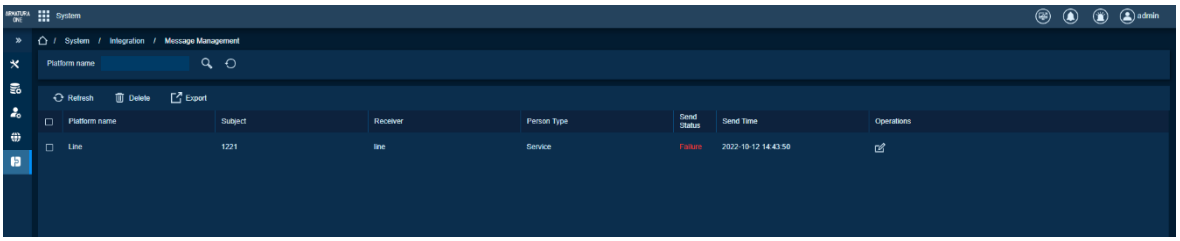
Log into the system using an account with the required permissions.

Usage Scenarios

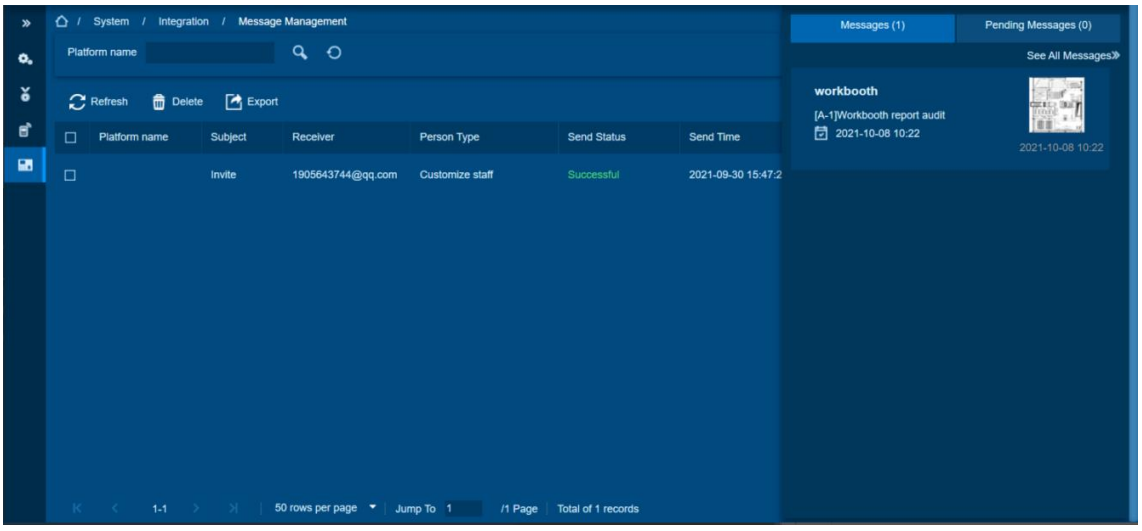
When users need to view or process certain messages to progress with tasks or actions.

Steps:

- The total number of unread and pending messages appears in the upper right corner.

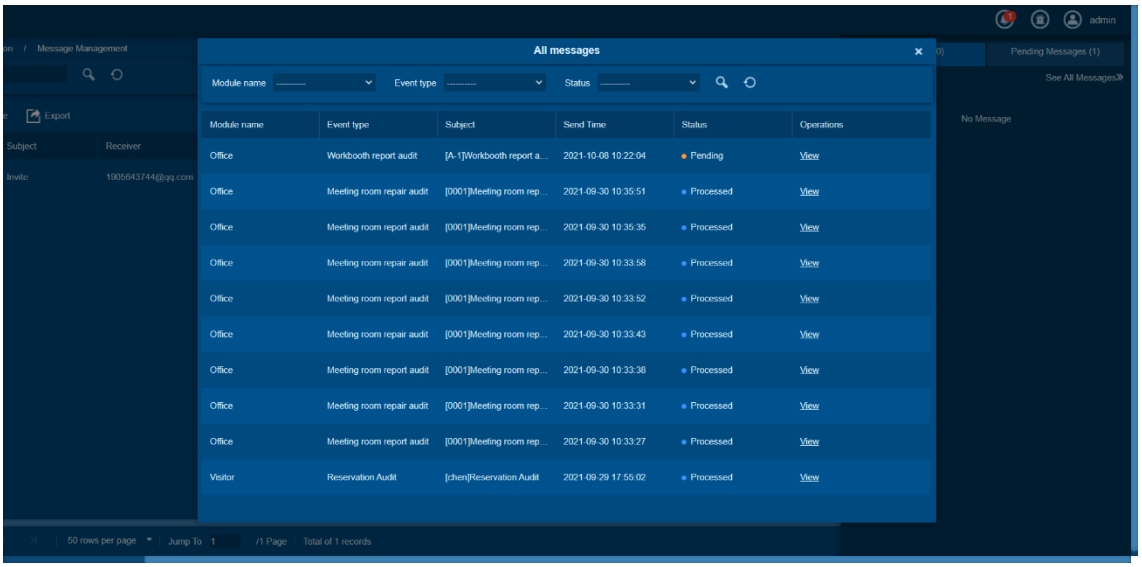


- Click the bell icon to open the message bar. The left side displays unread messages, while the right-side shows read messages pending further action.

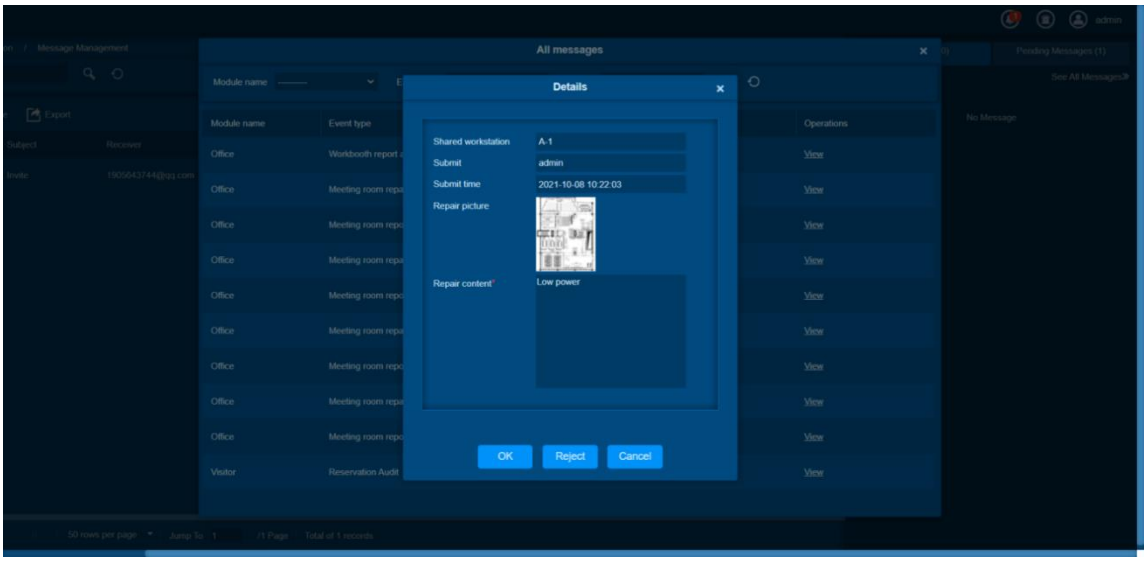


Copyright © 2024 ARMATURA LLC. All rights reserved

- Click **[See all messages]** to view the message history.



- In the history section, click **[View]** to check the message details.



Copyright © 2024 ARMATURA LLC. All rights reserved

4.2. Message Management

Function Description

Integrated messaging through third-party messaging platforms.

Delete

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

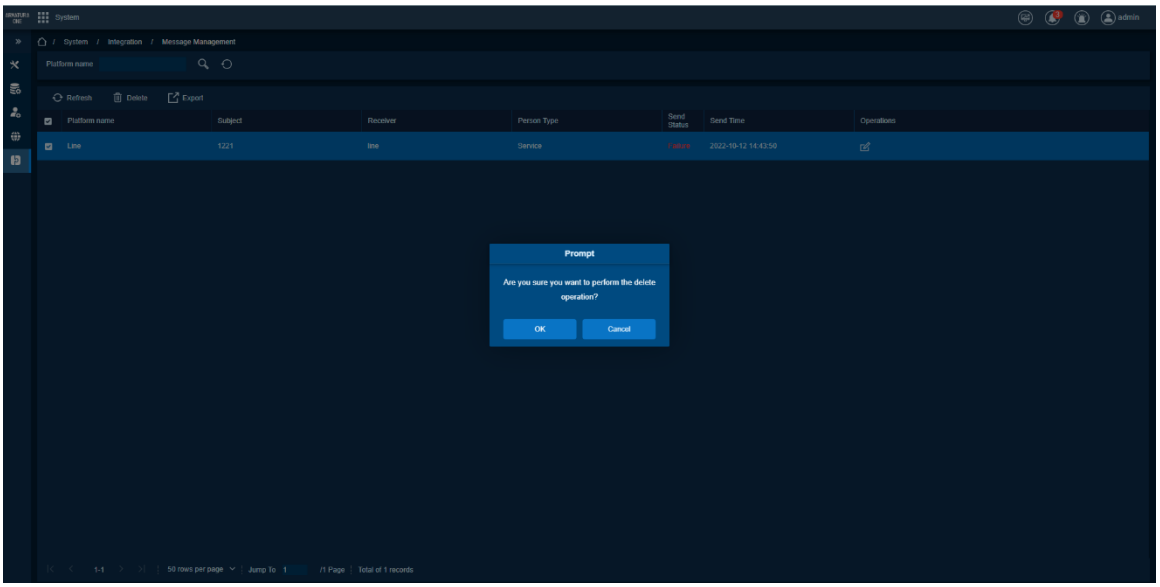
Delete unnecessary or expired message data.

Expected Trigger Results

The selected data is removed from the system.

Steps:

- Select the messages to be deleted.
- Click the **[Delete]** button, and a confirmation window will appear.



- Click **[OK]** in the prompt to confirm and complete the deletion.

Export

Prerequisites for Use

Data export is restricted to administrators only.

Usage Scenarios

Export message information from the software to user's PC.

Copyright © 2024 ARMATURA LLC. All rights reserved

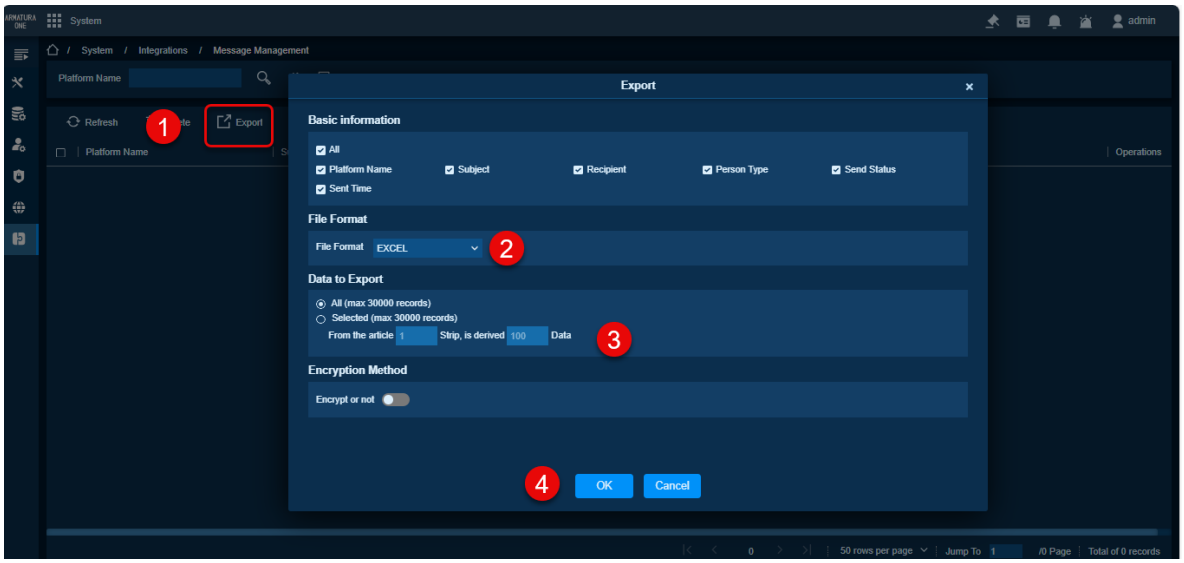
Trigger Results

The message data is exported in the chosen format.

Operations	Description
Select Excel	Export the message to EXCEL format
Select PDF	Export the message to PDF format
Select CSV	Export the message to CSV format
Select All Data	Export all message data
Select Partial Data	Export only selected message data.

Steps:

- Click **[Export]** to open the Export dialog box.
- Select the desired file format for export in the pop-up window.
- Choose the data scope to export (all or partial data).
- Click **[OK]** to complete the export operation.



Copyright © 2024 ARMATURA LLC. All rights reserved

4.3. System Messages

Function Description

Stores all system messages.

Export

Prerequisites for Use

The export function is available to administrators when data is present in the list.

Usage Scenarios

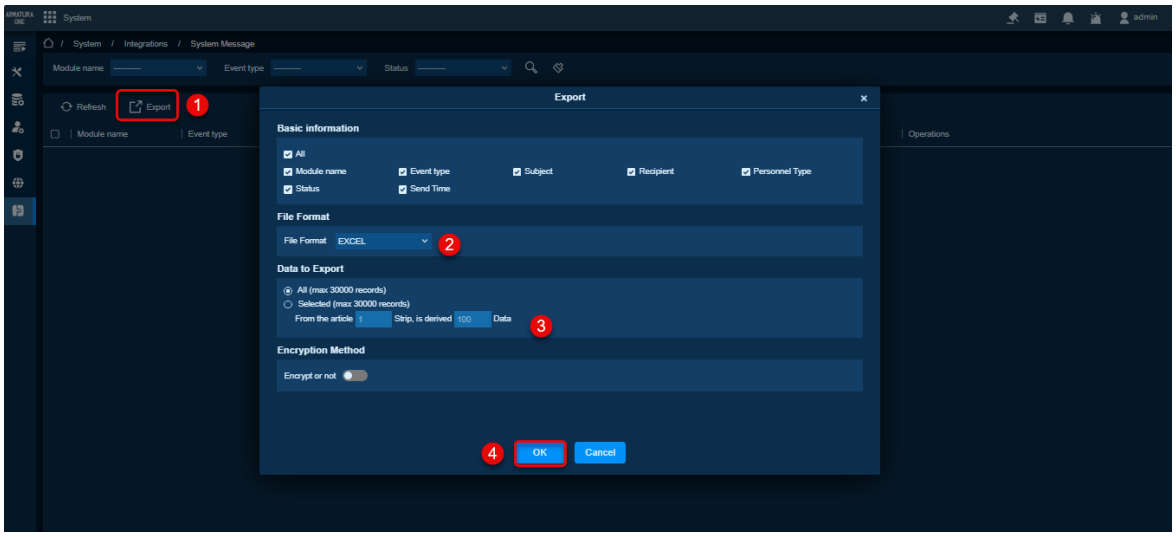
Export the data from the software to user pc.

Trigger Results

Operations	Description
Select Excel	Export system messages to Excel format
Select PDF	Export system messages to PDF format
Select CSV	Export system messages to CSV format
Export all system message data.	Export all system message data
Export partial system message data	Export only selected system message data

Steps:

- Click **[Export]** to open the Export dialog box.
- Select the file format for export in the pop-up window.
- Choose the scope of data to export (all or partial).
- Click **[OK]** to complete the export process.



Copyright © 2024 ARMATURA LLC. All rights reserved

5. Personnel Management

Personnel Management module includes the following components: Personnel, Organization, Position, Dismissed Personnel, Pending Review, Block List, Custom Attributes, Parameters, Duplicated Personnel Card, Wiegand Format, Issued Card Record, and Card Parameters.

Module Function List

Functions	Descriptions
Personnel	Manage essential personnel data by adding, deleting, editin and searching records. Supports synchronization, as well a importing and exporting personnel information.
Organization	Manage organizational structures with options to add, edit, viev delete, import, and export records.
Position	Manage position data by adding, editing, viewing, deleting, and supporting the import and export of records.
Dismissed Personnel	Access records of resigned personnel with options to restore them as needed.
Pending Review	Access and review items flagged as pending for assessment.
Block List	View a list of individuals blocked across various departments.
Custom Attributes	Add detailed custom attributes for personnel, allowing for enhanced record customization.
Parameters	Configure parameters for personnel management, selecting the most suitable options for operation.
Duplicated personnel	Identify and manage duplicate personnel records.
Card	Access all issued personnel cards, with options for reporting los cards.
Wiegand Format	Manage Wiegand format settings by adding, editing, deleting, and viewing configurations for Wiegand cards.
Issued Card Record	Access issued card records, report lost cards, reactivate lost cards, manage card writing, return cards, and modify card details.
Card Parameters	View and configure settings for card parameters.

Copyright © 2024 ARMATURA LLC. All rights reserved

5.1. Personnel

Usage Scenarios

Create new personnel records, edit existing personnel information, and modify the organizational structure and permissions associated with each person.

Trigger Results

Operation	Description
Check SMS Notification	**Scenario 1:** If prompted with "Please add SMS notification platform," it indicates that the SMS platform has not been configured. To resolve this, go to the System Integration module, set it up, and check again. **Scenario 2:** After setup, when this individual triggers an Access Control or Elevator Control event, a notification will be sent to their registered mobile number via SMS.
Check The Email Information	**Scenario 1**: Use the pop-up window to configure email settings. Enter the required parameters to set up the sender's mailbox, then verify the configuration. **Scenario 2:** After verification, event notifications (Access Control or Elevator Control) will be sent to the registered email.
Controller Issuance	Select the reader for the controller in the pop-up window. After selection, swipe the individual's card at the corresponding reader, and the system will automatically populate the card number in the text box.
Biometric Template-Fingerprint	Access the Fingerprint Registration interface via the pop-up window, where you can select the finger for registration. Ensure that the Fingerprint Collector or Access Control device is connected, and select it for fingerprint registration.
Biometric Template-Finger Vein	Access the Finger Vein Registration interface through the pop-up window, and choose the appropriate finger for registration. Ensure the Finger Vein Collector or Access Control device is connected for vein registration.
Person Avatar-Browse	Click "**Browse**" to upload a profile picture from the local computer.
Person Avatar-Snapshot	Click "**Capture**" to access the real-time avatar capture interface. Ensure a USB camera is connected to the server. Some browsers, like Chrome, may require permission to access the camera.

Copyright © 2024 ARMATURA LLC. All rights reserved

Access Control Settings-Permission Group Check	Add personnel to selected Access Levels. When Access Levels are linked to a device, personnel information is sent to the corresponding devices.
Access Control Settings-Personnel Database Check	Push personnel information to the selected personnel list database. Ensure you're connected to the system and have created the personnel database.
Access Control Settings-Super User	The super user is exempt from access control restrictions, possessing high-level permissions to open doors.
Access Control Settings-Extended Access	For individuals with disabilities, the device's opening time can be extended to allow more time for access.
Access Control Setting-Banned List	Revokes access permissions for individuals on the banned list.
Set Access Control Setting-Effective Time	Set a time limit for an individual's access control permissions. After this period expires, access rights are permanently revoked, ideal for temporary personnel.
Elevator Control Settings-Check the Elevator Control Permission Group	Assign specific elevator access levels for the individual.
Detailed Information	Stores additional details as a supplementary record for personnel information.

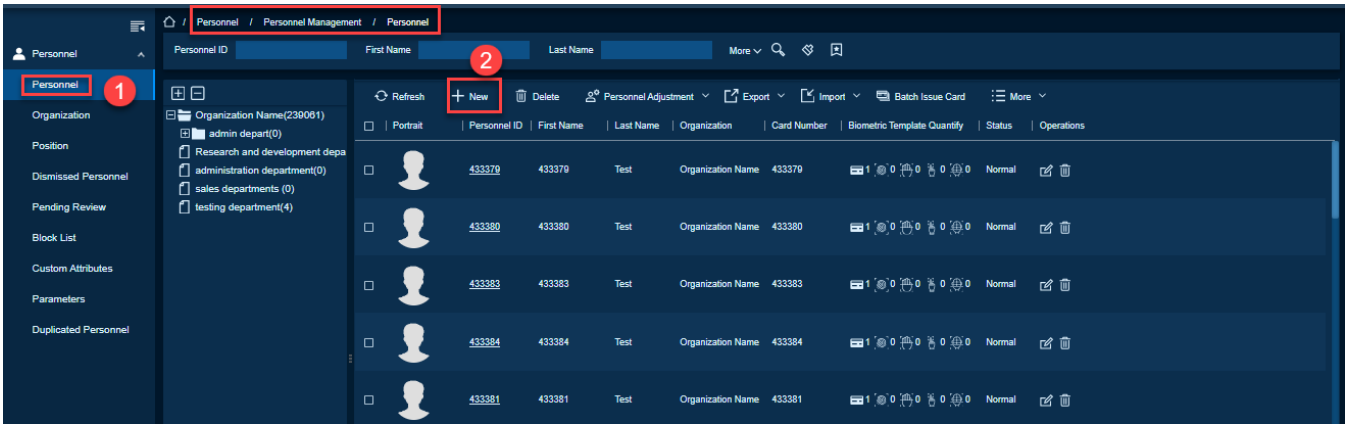
5.1.1. Personnel

When using the Personnel Management module, users must register personnel directly within the system or import personnel data from other software or documents. For detailed steps on importing, refer to the Common Operations section. Personnel Management functions include adding, editing, deleting, exporting, and importing personnel records, as well as adjusting departmental assignments.

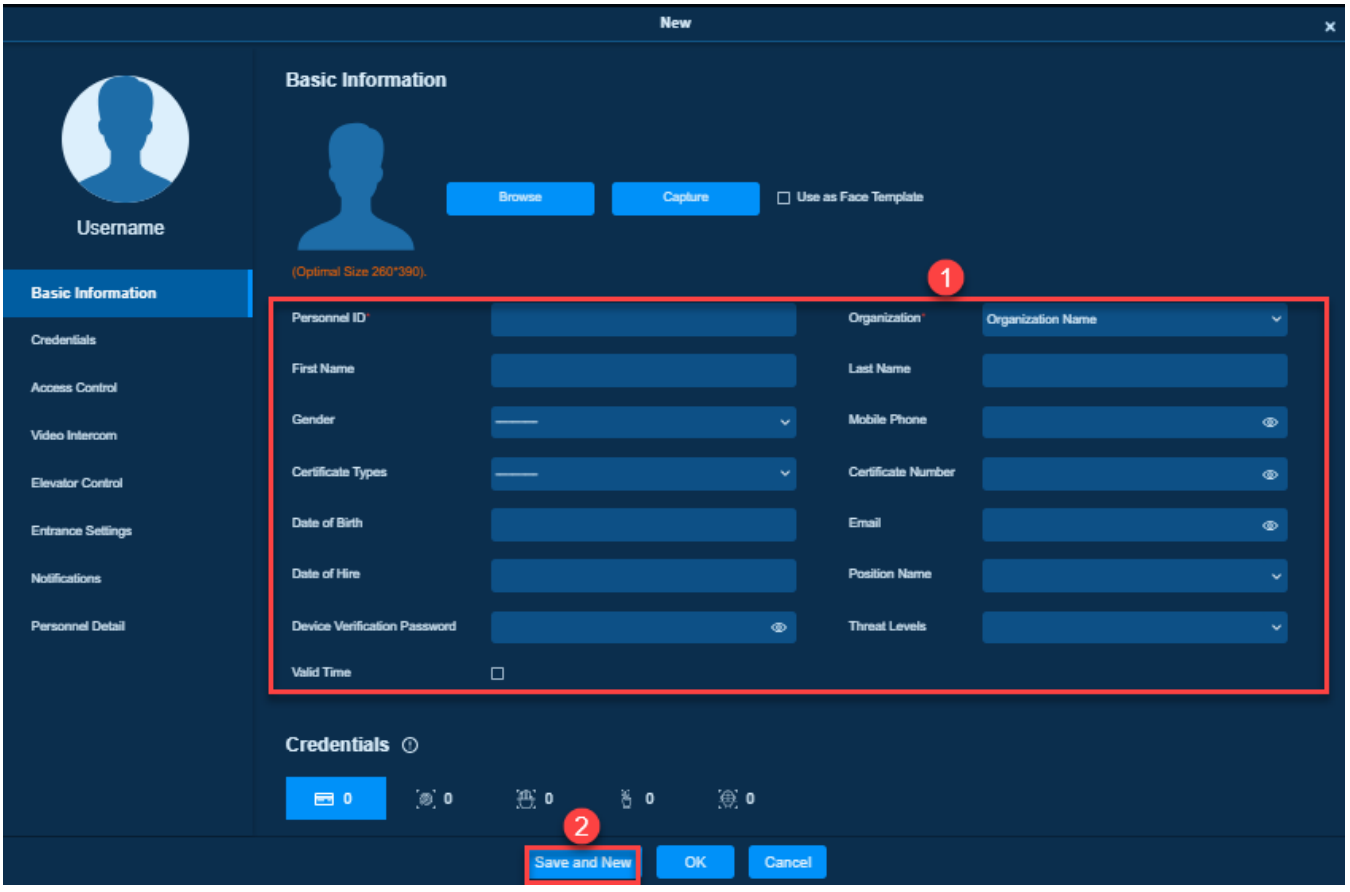
Adding Personnel

- Navigate to **[Personnel]** > **[Personnel Management]** > **[Personnel]** > **[New]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



- In the New Personnel interface, enter the Personnel ID, Department, First Name, Last Name, and other details as prompted.
- For Personnel Permission Settings, click **[Access Control]**, select General, and set values for Personnel Library, Superuser, Device Operation Role, Delay Passage, Block All Access, and Auto Block Access.
- Click **[OK]** to save the settings.



Field Description

Personnel Photo: Includes an image preview function supporting **JPG, JPEG, BMP, PNG**, and **GIF**. The recommended size for optimal display is 120×140 pixels.

Copyright © 2024 ARMATURA LLC. All rights reserved

- **Browse:** Click **[Browse]** to upload a local photo.
- **Capture:** Take a photo with a connected camera, if available.

Personnel ID: A unique identifier of up to 9 characters, ranging from 1 to 79,999,999, customizable per requirements.

Note:

Verify the device's maximum character length for Personnel IDs, as well as letter compatibility. To adjust these settings, go to **[Personnel]** > **[Parameters]**.

Organization: Select an organization from the drop-down list. If no prior organization has been set, only **[Company Name]** will be displayed**.**

First Name/Last Name: Each field accepts up to 50 characters.

Gender: Specify the personnel's gender**.**

Mobile Phone: Optional, with a maximum length of 20 characters.

Certificate Type: Choose from ID, Passport, Driver's License, or Others.

Certificate Number: Enter the certificate number corresponding to the selected type.

Date of Birth Date: Enter the birthdate of the employee.

Email: Specify the personnel's email address (maximum 30 characters). Allowed punctuation: "-", "_", and ".". If Event Notification is selected, an email is required.

E-mail Notification: When enabled, the system sends notifications for Access Control and Elevator events to this email. If the email server is not configured, a setup window will appear. See **Email Management** for configuration details.

Date of Hire: Record the personnel's start date by selecting a date.

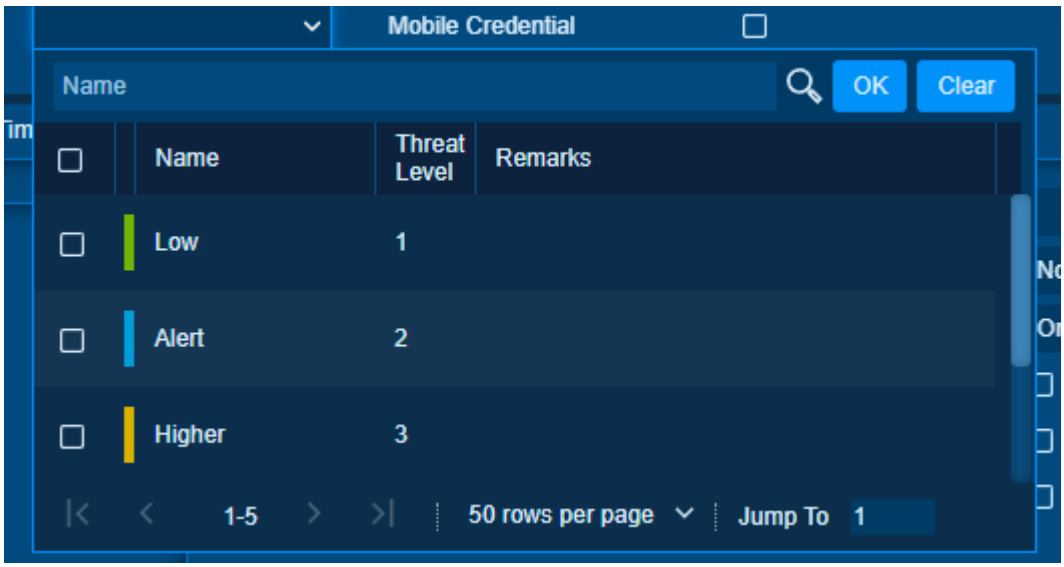
Position Name: Enter the personnel's job designation.

Device Verification Password: Password used on readers for identity verification.

Personnel Threat Level

Assigns a threat level to the personnel. The system checks whether this level matches the current system threat level. If not, access is restricted.

Copyright © 2024 ARMATURA LLC. All rights reserved



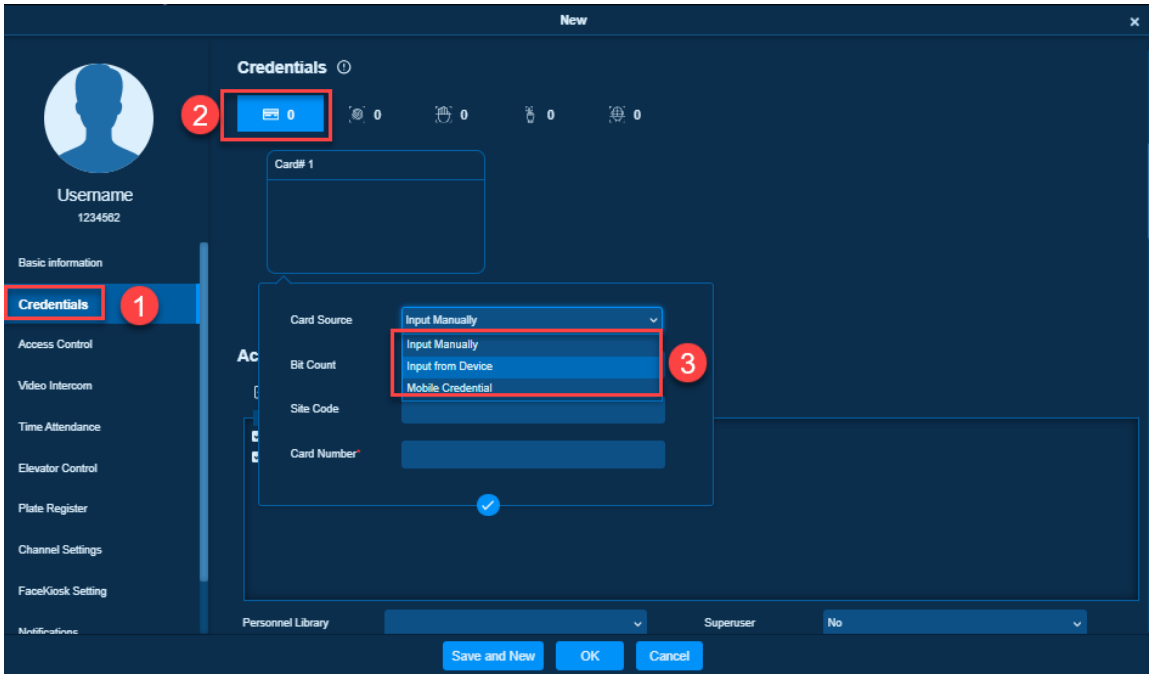
Related Function: Check the Threat Level.

Personnel Validity: Set the validity period for personnel access. If enabled, specify start and end dates.

Card Number: Maximum 10 characters, must be unique. Click the 0 button to capture the card number directly from the reader.

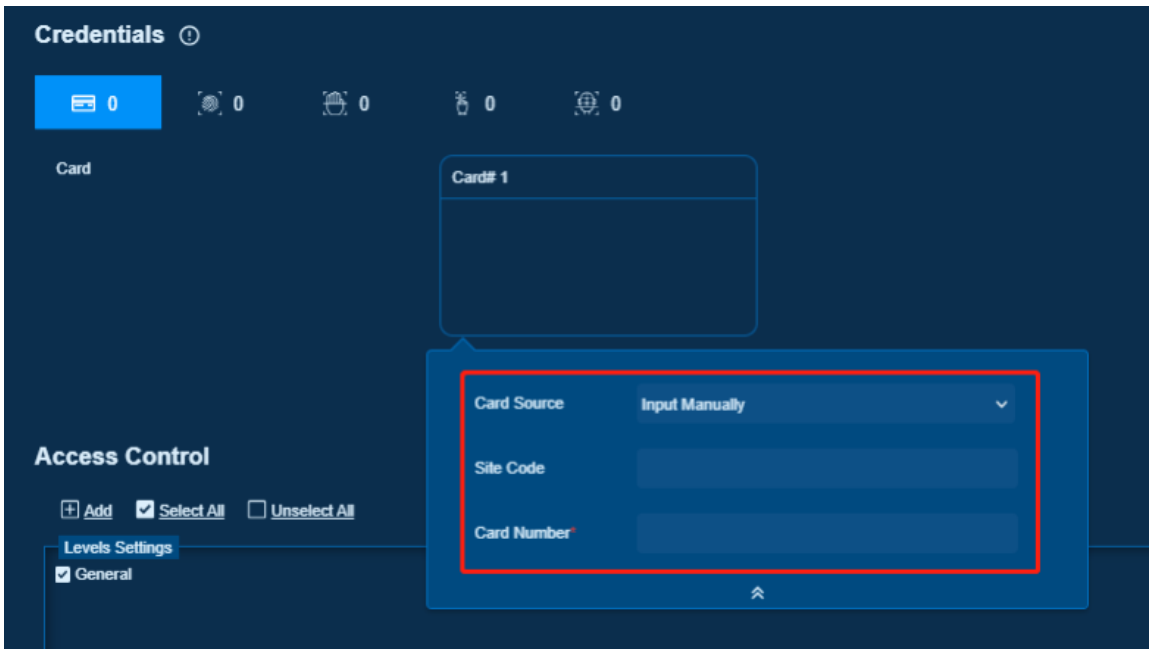
- Multi-Site Code Support: The Wiegand card system can include a site code with the card number for unique identification, distinguishing similar card numbers across sites (e.g., 100-1234 vs. 200-1234).

Card Sources: There are three card sources available for use.

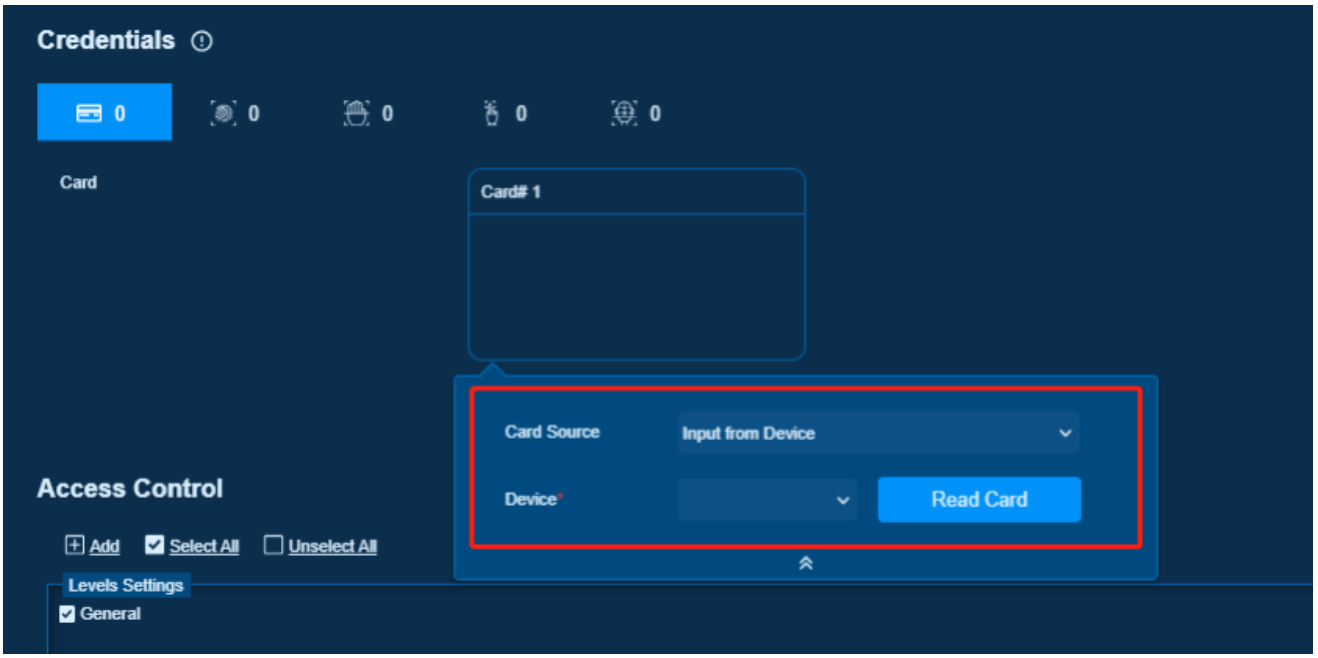


- **Manual Entry**: Allows entry of bit count and site code.

Copyright © 2024 ARMATURA LLC. All rights reserved

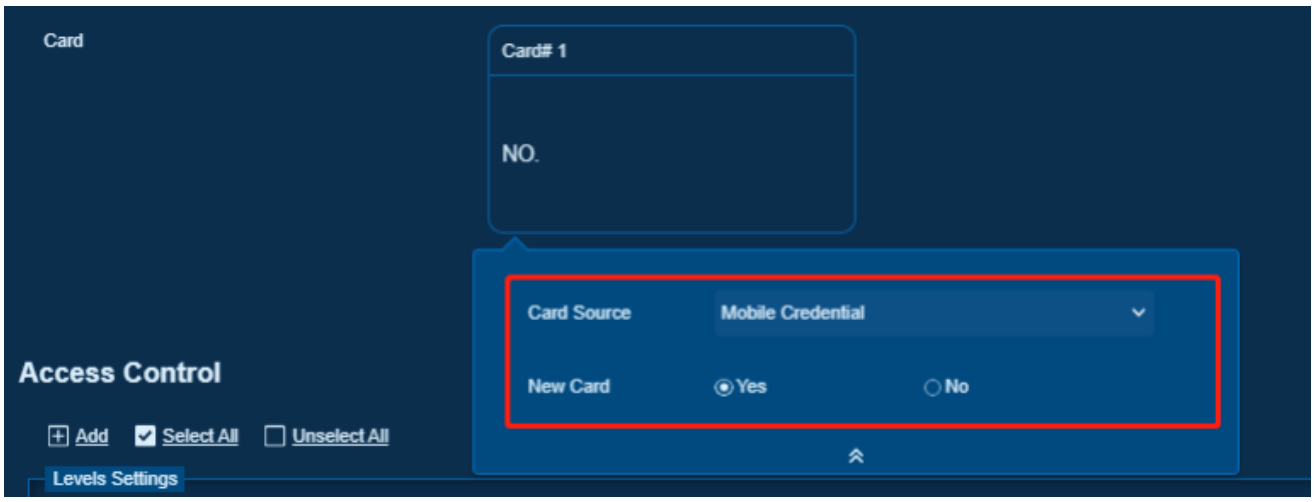


- **Device Entry**: Select the corresponding device to register the card number.



- **Mobile Credential**: Option to issue a new mobile credential or enter an existing ACMS credential manually.

Copyright © 2024 ARMATURA LLC. All rights reserved



Person Type: Specify as Employee or Visitor

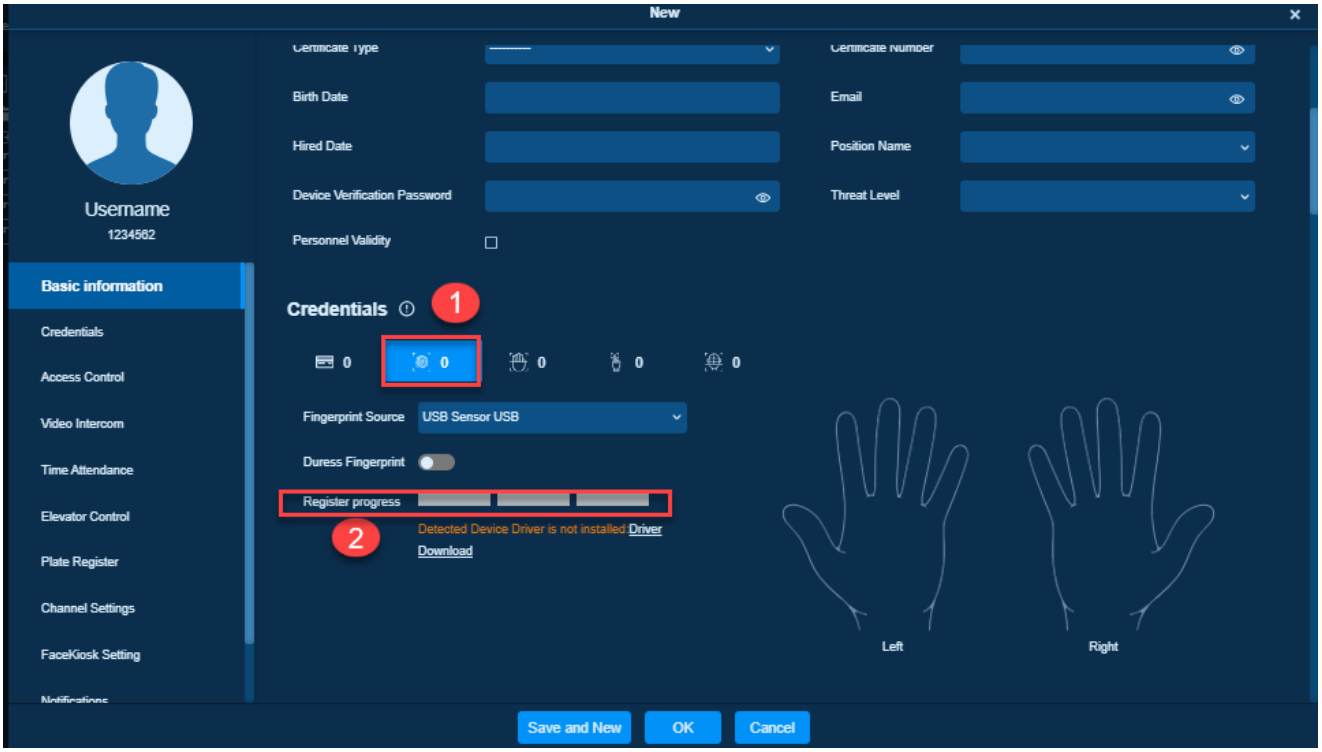
Biometric Template Quantity: Displays the number of biometric credentials associated with the user.

Biometric Registration

Register Fingerprint/Finger Vein: Enroll personnel's fingerprint, finger vein, or duress fingerprint. The duress fingerprint triggers an alarm in emergencies.

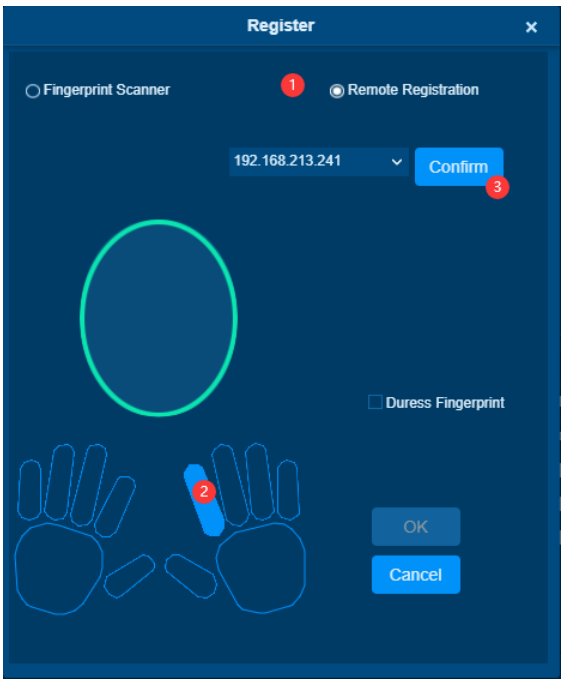
Fingerprint Registration Steps:

- Hover over the fingerprint icon to open the registration prompt. Click **[Register]** to proceed.

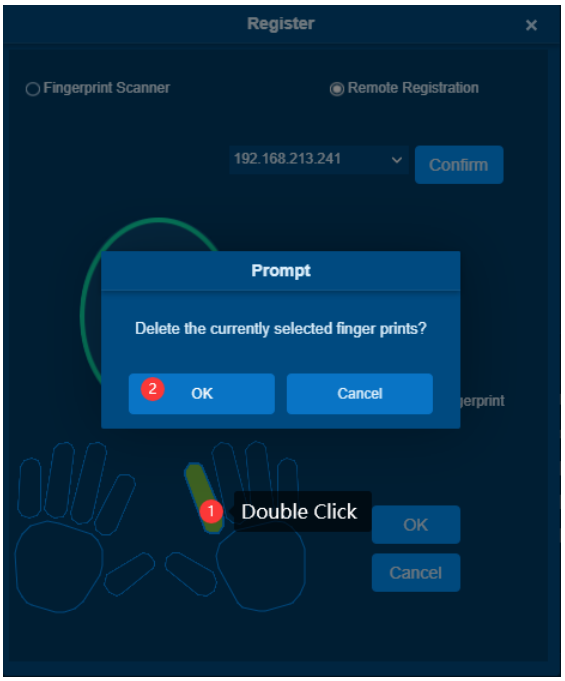


- Choose Fingerprint Scanner for direct scanning or Remote Registration for remote devices.

Copyright © 2024 ARMATURA LLC. All rights reserved

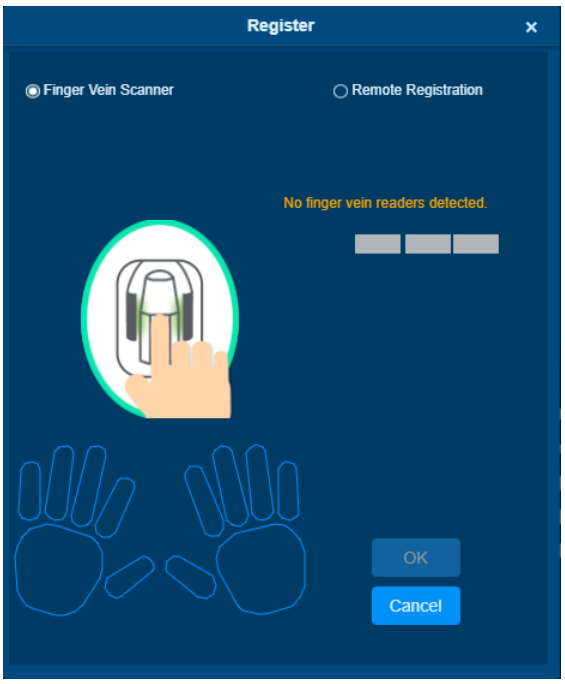


- Select a finger and press it on the sensor three times. Once registered, a confirmation message ("Fingerprint registered successfully") will appear.



- Click **[OK]** to complete registration.

Copyright © 2024 ARMATURA LLC. All rights reserved



- To delete a fingerprint, double-click the entry. To register a duress fingerprint, ensure "**Duress Fingerprint**" is selected.

Note:

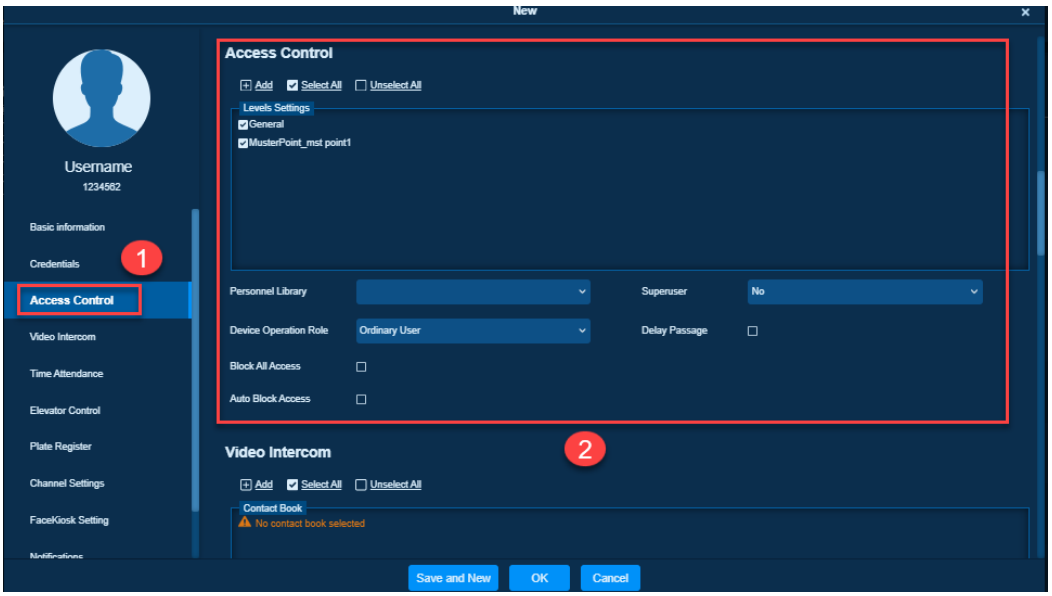
If duplicate fingerprints are detected, a message will appear stating, “Don’t repeat the fingerprint entry”.

If the fingerprint sensor driver is not installed, click **“Install driver”** and the system will prompt you to download and install it.

Access Control

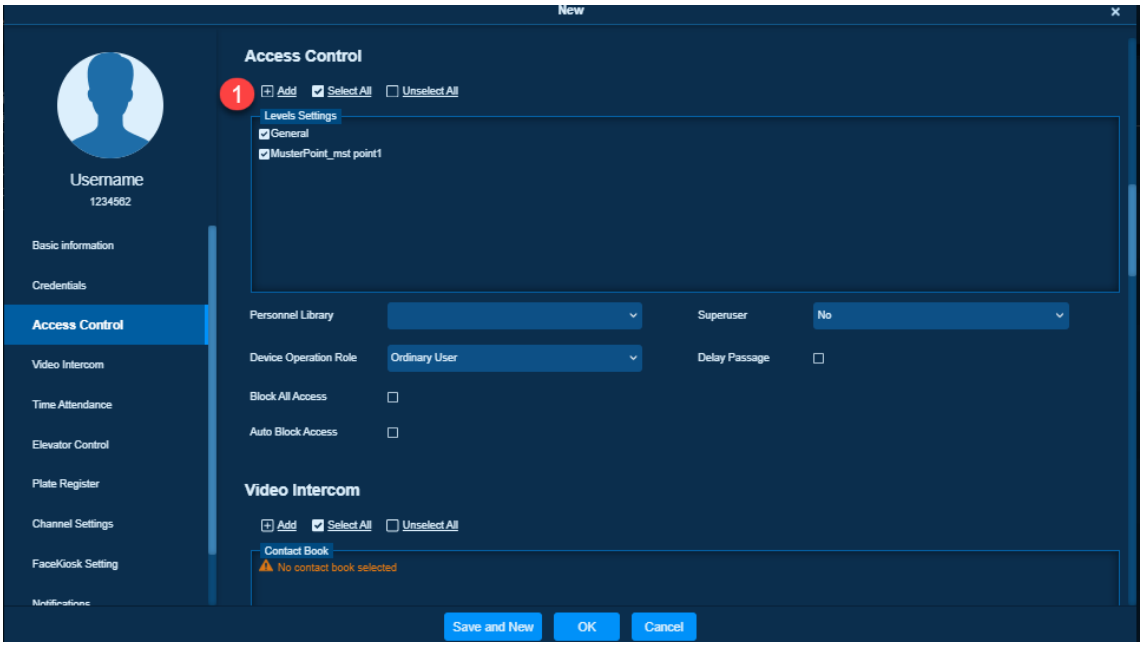
Set the Access Control parameters for the user by selecting **[Access Control]**.

Copyright © 2024 ARMATURA LLC. All rights reserved

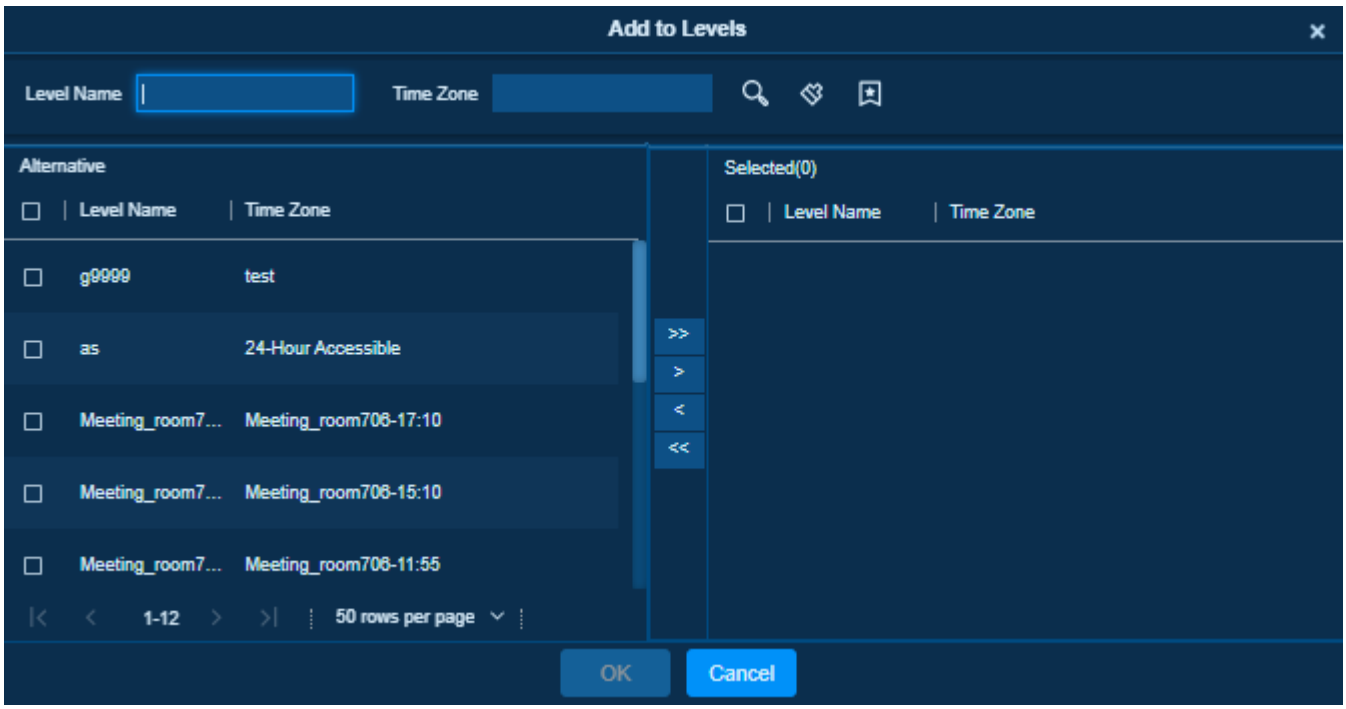


The following fields and options are available:

- **Level Settings**: Click **[Add]** and choose the access levels for the user. Access levels define the specific areas and times personnel are permitted to enter.



Copyright © 2024 ARMATURA LLC. All rights reserved



Superuser: A privileged account that bypasses standard access restrictions including time zones, antipassback, and interlock controls. Superusers receive highest priority for door access permissions.

Device Operation Role: Defines user authorization levels on standalone terminals with three permission tiers: Ordinary User, Administrator, and Enroller.

Delay Passage: Extends the standard access point response time to accommodate individuals requiring additional time to transit, such as persons with mobility limitations or disabilities.

Block All Access: When activated, prevents execution of all access-related functions across the system.

Auto Block Access: Automatically restricts access privileges based on predefined security parameters and conditions.

Note:

During verification, the system will search for corresponding records in the departure library as part of the access check.

By default, the Personnel Information List is displayed as a table. Selecting Graphic Display will show photos and personnel numbers; Hovering over a photo will reveal additional details.

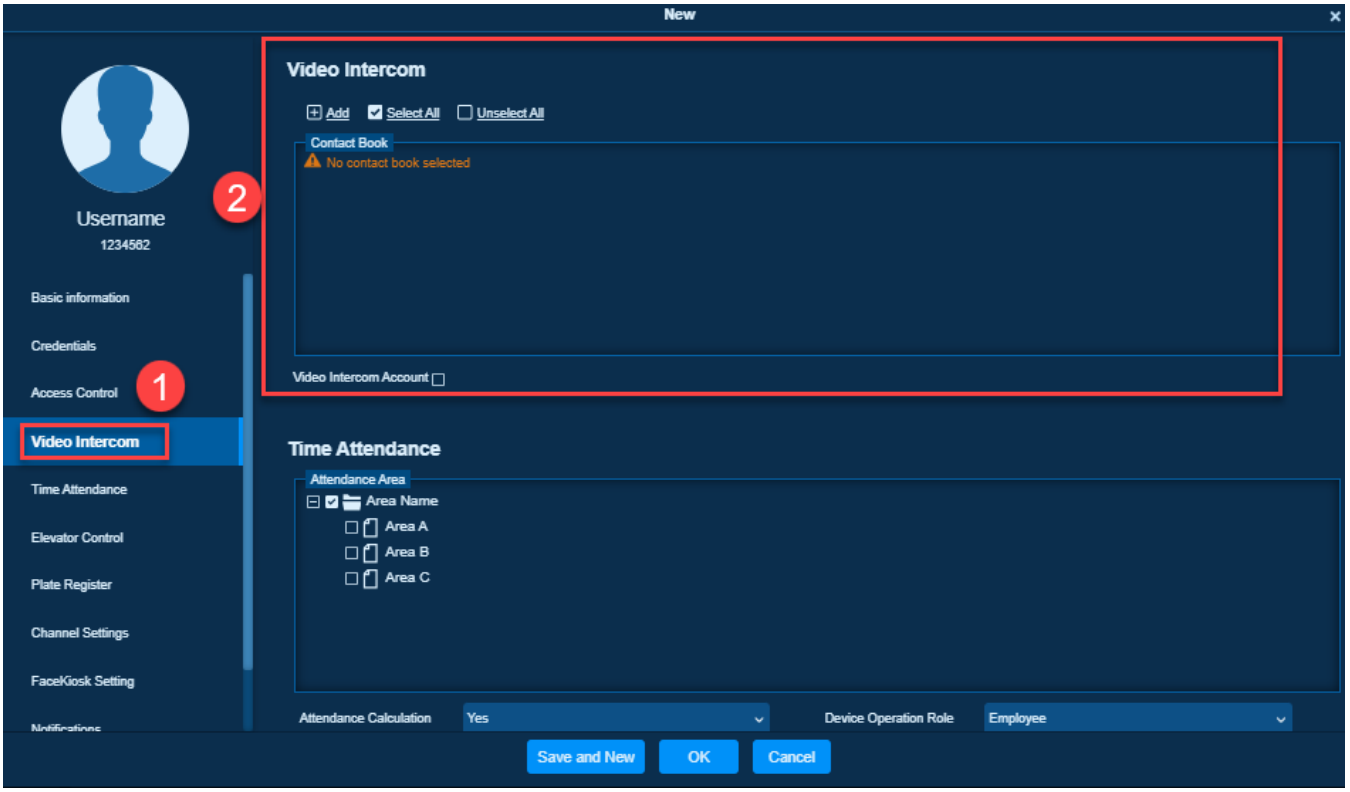
Note:

The Personnel Background Comparison Verification feature is supported in the Video module, allowing personnel to be verified against lists created in the personnel library.

Copyright © 2024 ARMATURA LLC. All rights reserved

Video Intercom

Set the Video Intercom parameters for the personnel by clicking on **[Video Intercom].**



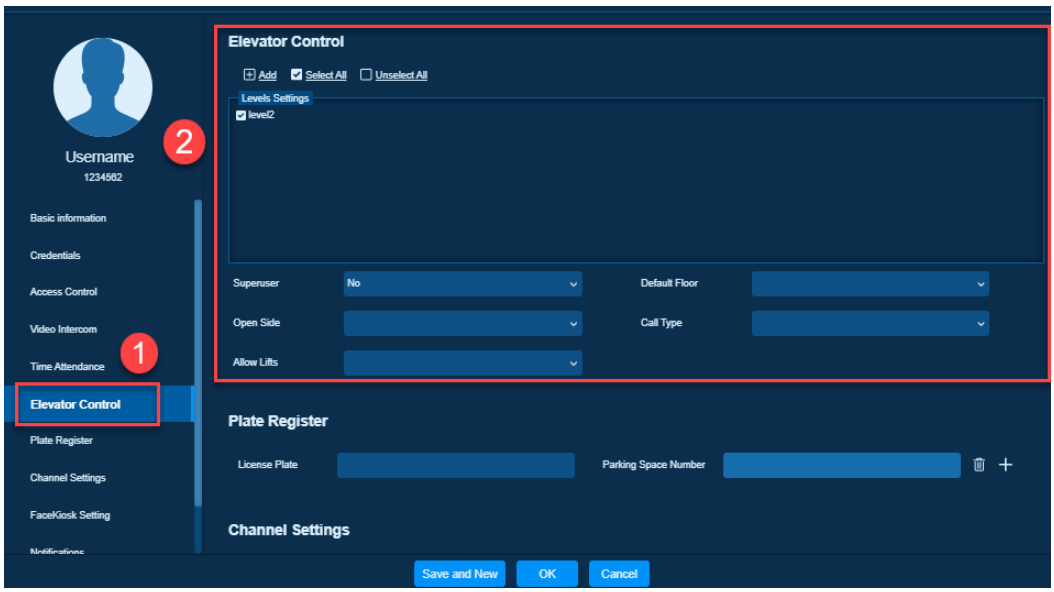
Contact Book: Click **[Add]** to set the name of the contact book and add any relevant remarks.

Video Intercom Account: Configure the video intercom account to enable both video and audio intercommunication.

Elevator Control

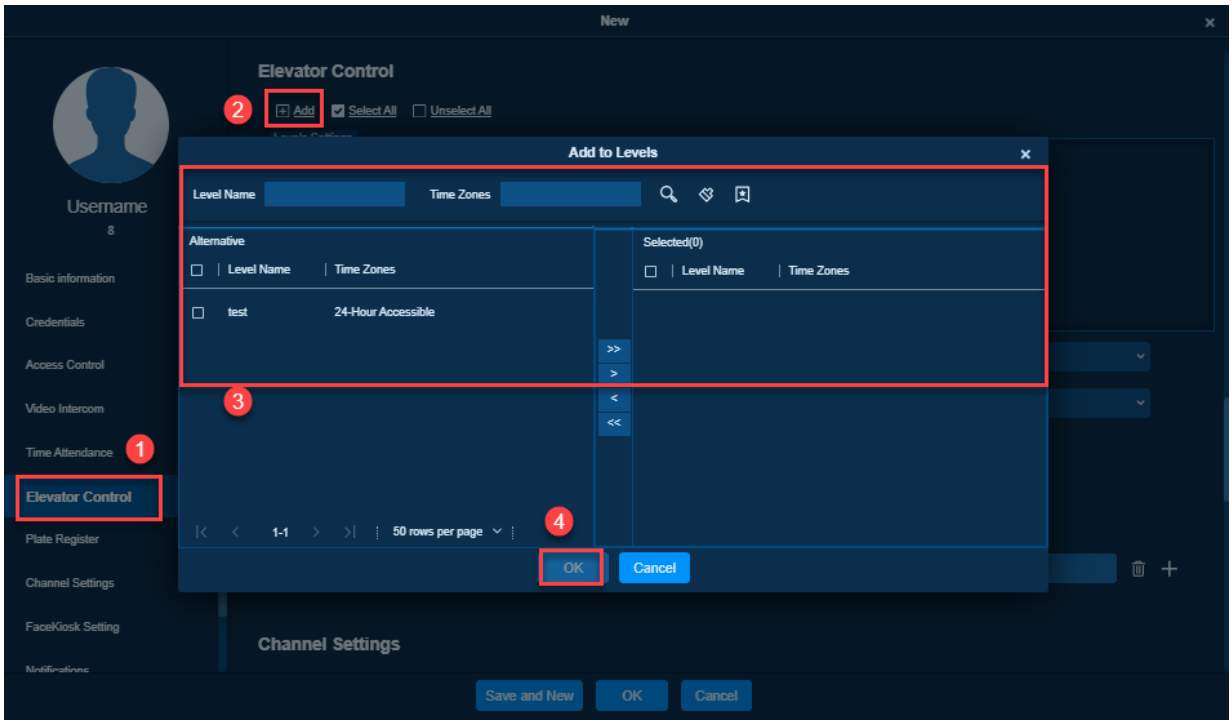
Configure elevator control settings by selecting **[Elevator Control].**

Copyright © 2024 ARMATURA LLC. All rights reserved



The available fields are:

Level Settings: Click **[Add]** and select the desired access level for elevator use.



Superuser: A superuser in the elevator control system is exempt from time zone and holiday restrictions and holds top priority for elevator access.

Default Floor: Set a default floor for check-ins, allowing only one default floor per building.

Open Side: Set the front and back door switches for the elevator when it arrives at the default floor. Choose from three modes: Front Door Open, Back Door Open, or Both Doors Open.

Call Type: Configure the call type based on the elevator control device used in each building.

Copyright © 2024 ARMATURA LLC. All rights reserved

Elevator Type	Type of Call
Kone	Normal Call
	Handicapped Call
	Priority Call
	Empty Car Call
	Space Allocation Call
Mitsubishi	General
	Handicapped Person
	VIP
Hitachi	General
	Handicapped Person
	VIP

Allow Lifts: Specify which elevators are accessible to the user.

Note:

The elevator level settings must be configured in advance.

Parking Settings

Configure parking information by registering the following details.

License Plate: Register the user's license plate number.

Parking Space Number: Assign a specific space corresponding to the vehicle.

Note:

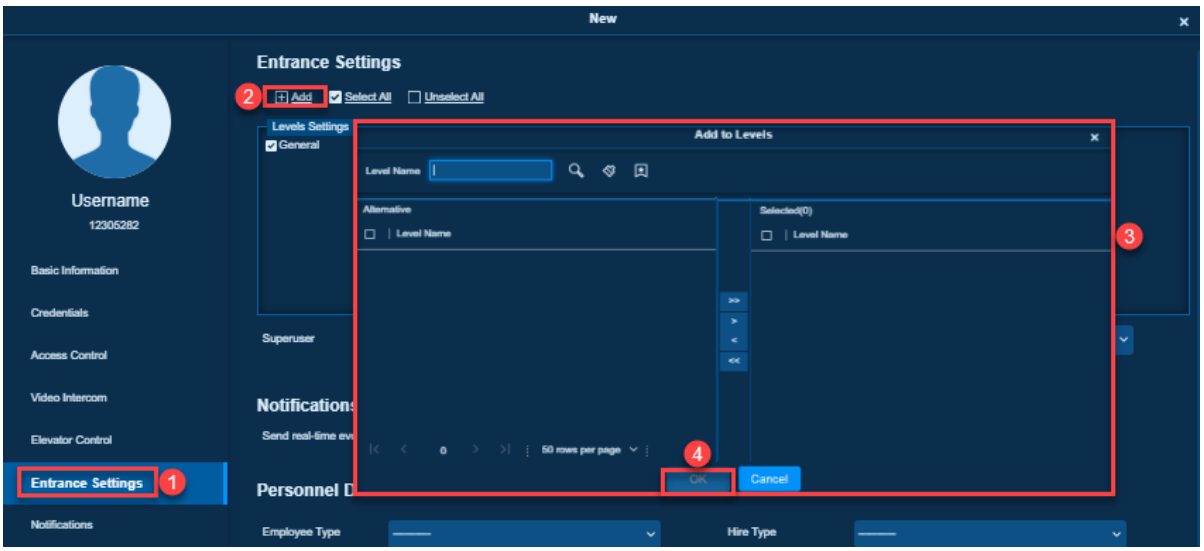
Each user may register up to 6 license plates.

Entrance Settings

To configure entrance parameters, Select **[Entrance Settings]**. The available fields are:

Level Settings: Click **[Add]** and select the appropriate access level.

Copyright © 2024 ARMATURA LLC. All rights reserved

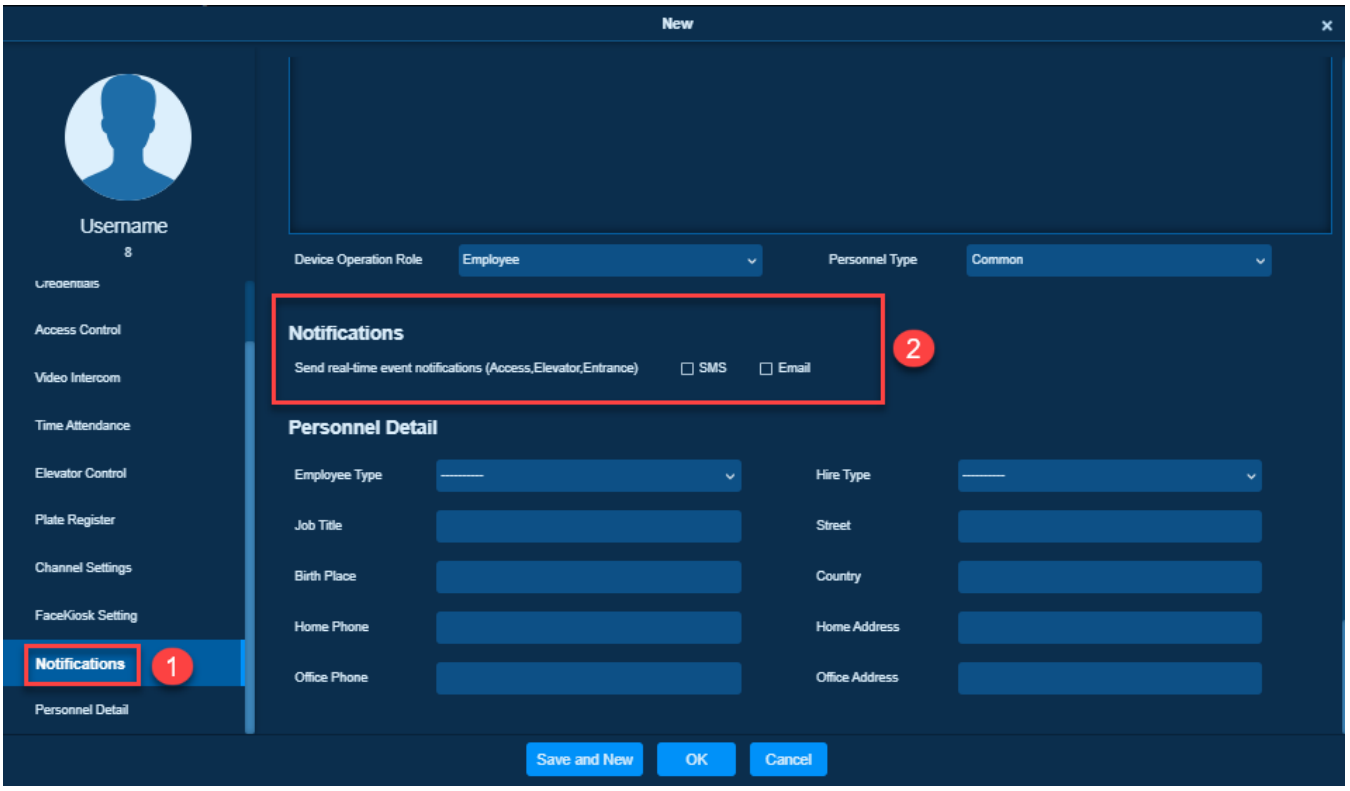


Superuser: A superuser in the entrance control system is exempt from time zone and holiday restrictions, providing them with prioritized access.

Device Operation Role: Set the user's authority level for device operations.

Notifications

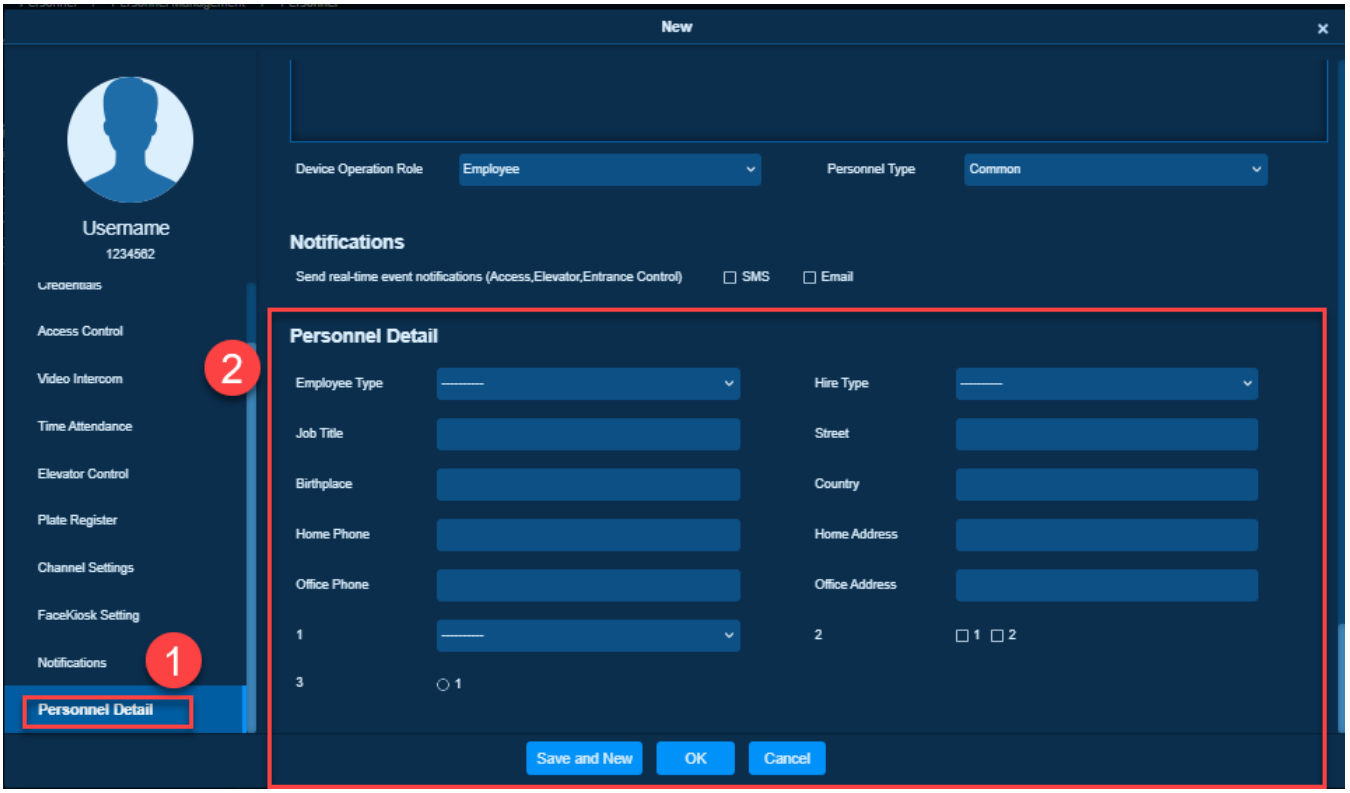
To send notifications, click **[Notifications]** and select preferred method – either **Email** or **SMS**.



Personnel Detail

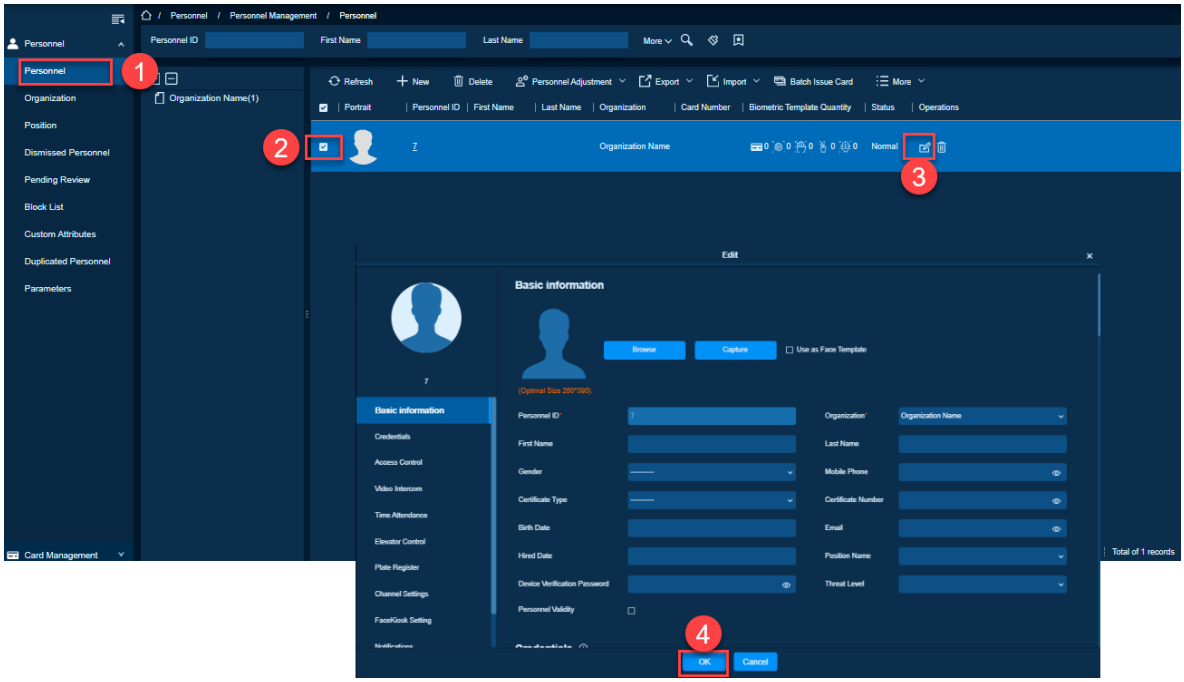
- Click **[Personnel Detail]** to enter the detail information for the user. After entering the information, click **[OK]** to save and exit.

Copyright © 2024 ARMATURA LLC. All rights reserved



Edit Personnel

- Go to **[Personnel]** > **[Person]**. Select the desired person and click **[Edit]**.

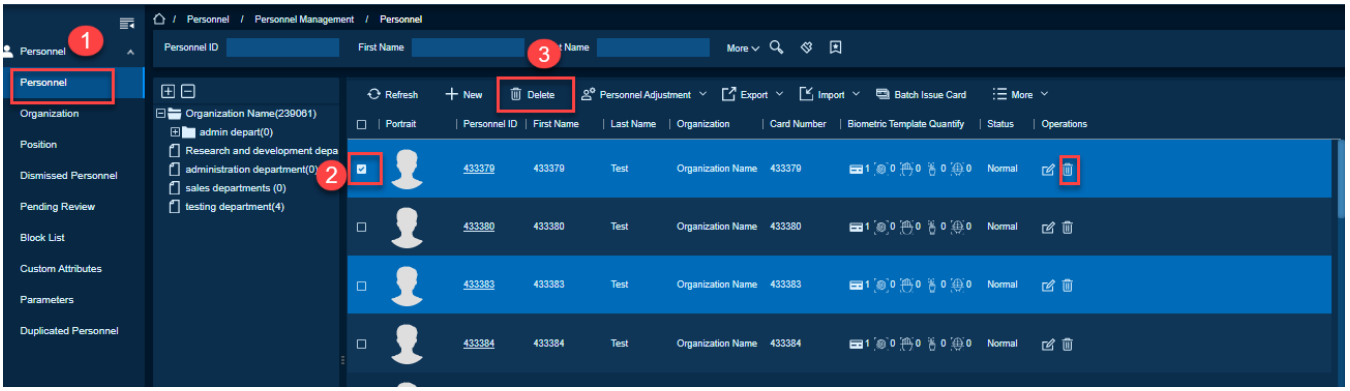


- After entering the necessary details, click **[OK]** to save changes.

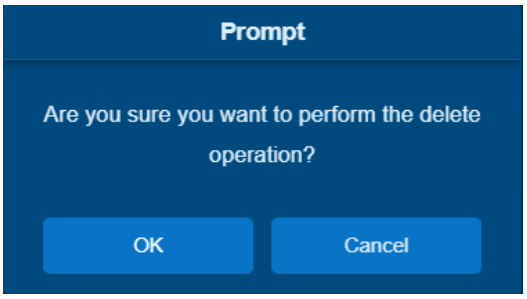
Delete Personnel

- Navigate to **[Personnel Management]** > **[Personnel]** and select the person.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Click **[Delete]**, **[OK]** to confirm deletion.

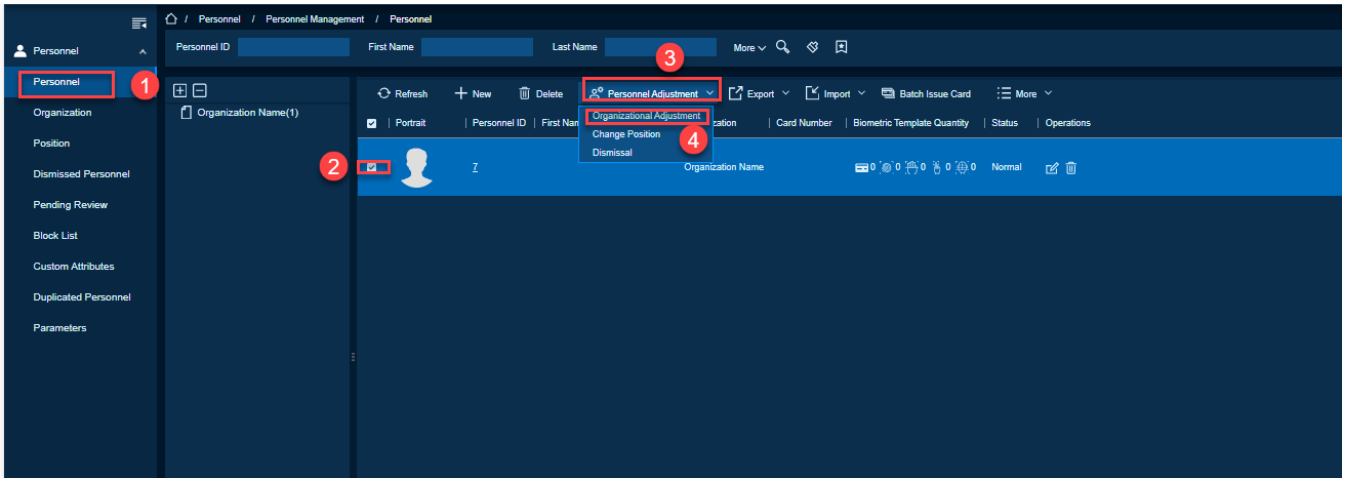


Note:

All relevant information about the person will be deleted.

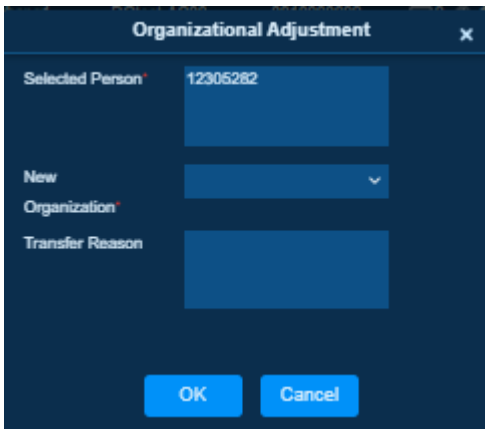
Organizational Adjustment

- Go to **[Personnel Management]** > **[Personnel]**. Select the person, then click **[Personnel Adjustment] > [Organizational Adjustment].**



In the Adjust Department interface, enter the Selected Person, New Organization, and Transfer Reason.

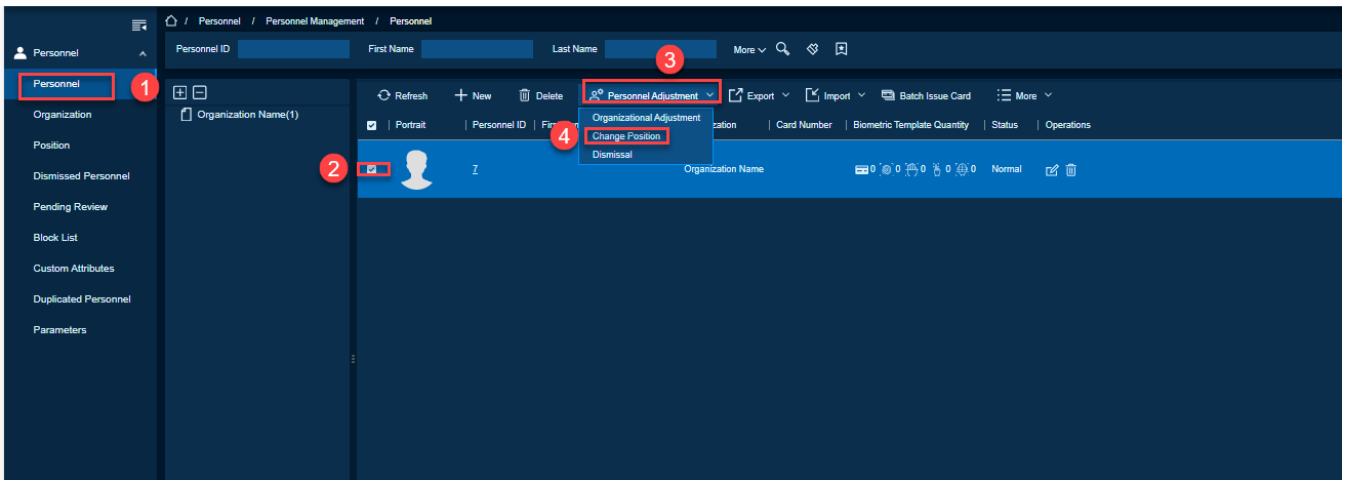
Copyright © 2024 ARMATURA LLC. All rights reserved



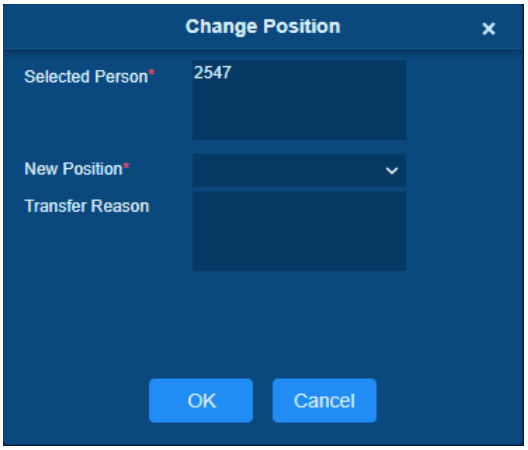
- Click **[OK]** to save and exit.

Change Position

- Navigate to **[Personnel Management]** > **[Personnel]**. Select the person, then click **[personnel adjustment] > [Change Position]**.



In the Change Position interface, enter the Selected Person, New Position, and Transfer Reason.

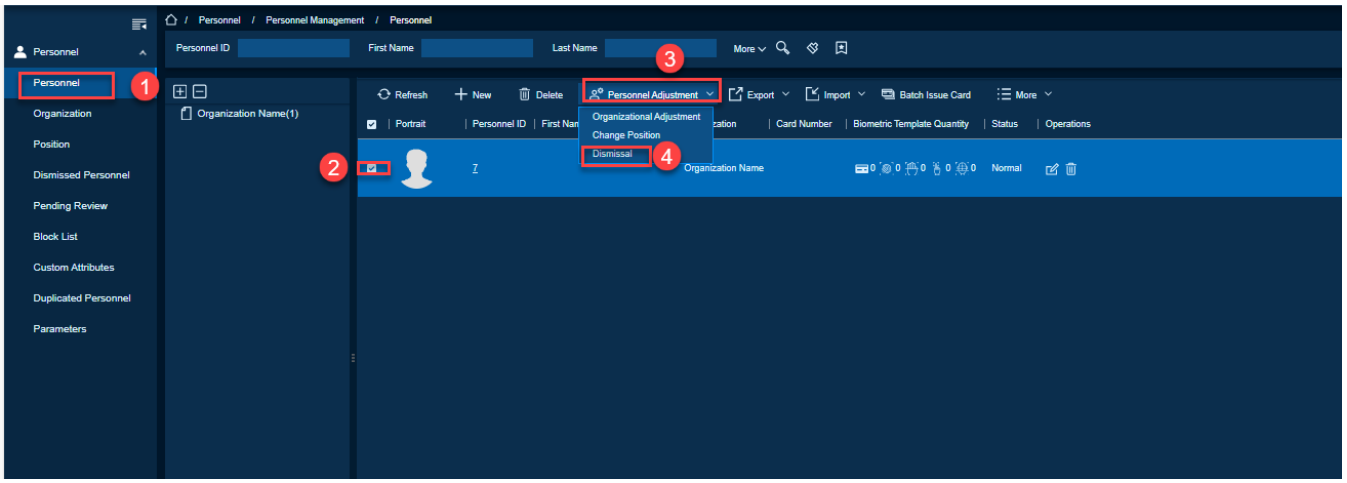


- Click **[OK]** to save and exit.

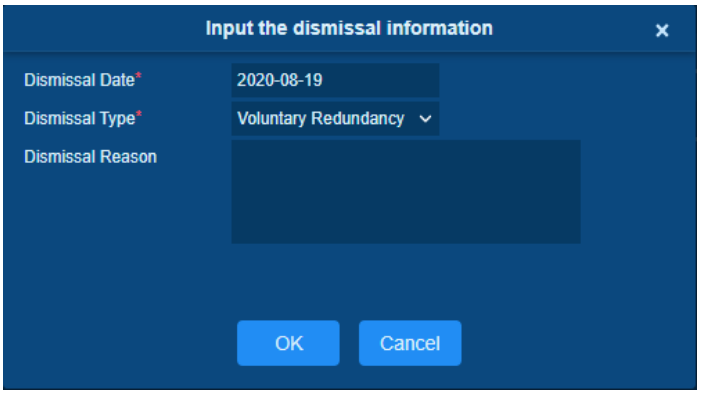
Copyright © 2024 ARMATURA LLC. All rights reserved

Dismissal

- Go to **[Personnel Management]** > **[Personnel]**. Select the person, then click **[Personal adjustment]** > **[Dismissal]**.



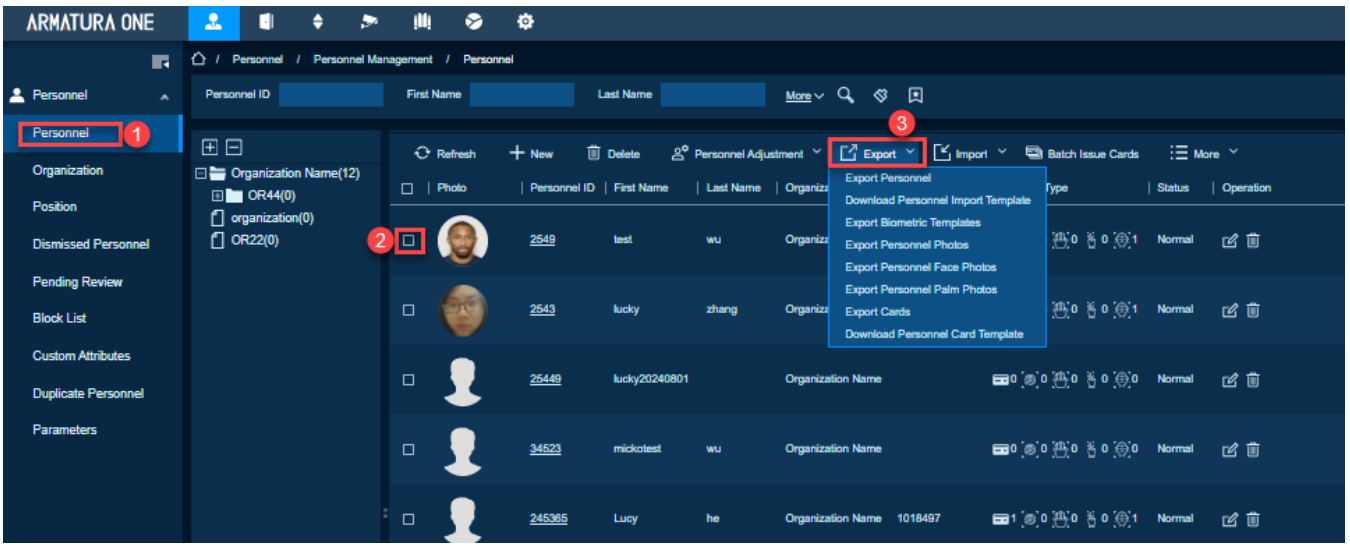
- Choose the Date, Type, and Reason for dismissal, then click **[OK]**.



Export

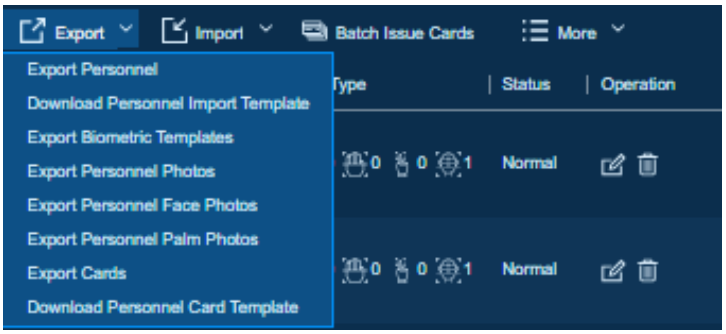
- To export personnel information and biometric templates, navigate **[Personnel Management] > [Personnel] > [Export]**.

Copyright © 2024 ARMATURA LLC. All rights reserved

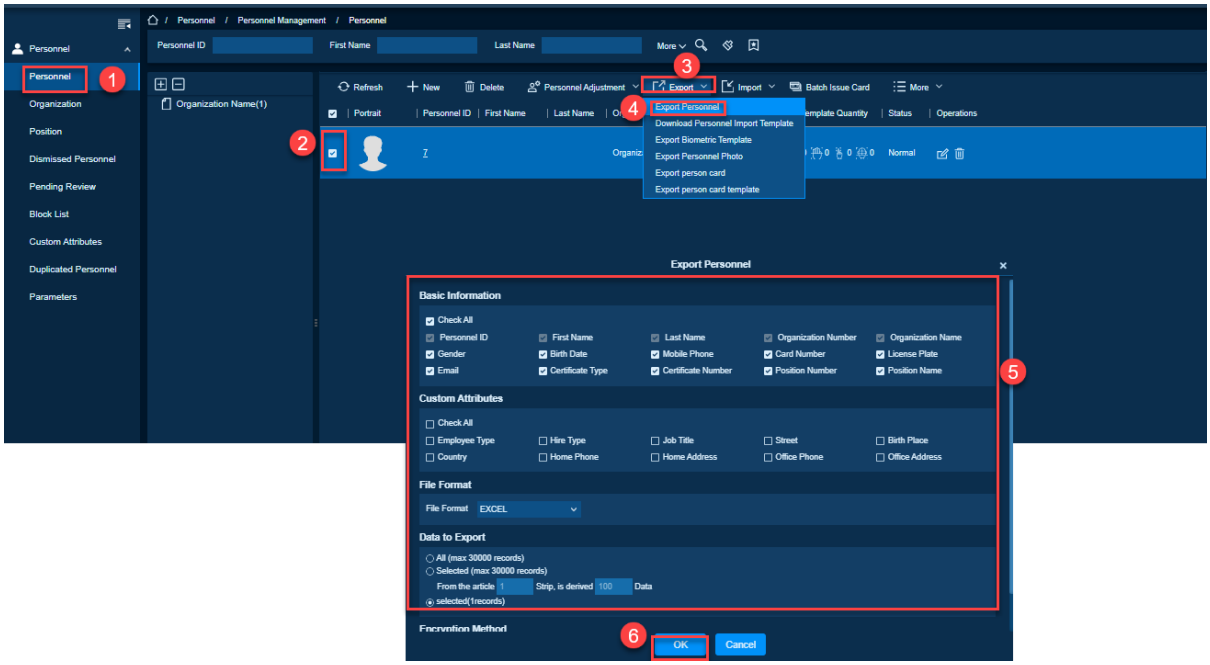


Export Personnel

Choose to export either all personnel data or specify a particular range.



In the Export Personnel interface, select the desired personnel details and any custom attributes to include.



Copyright © 2024 ARMATURA LLC. All rights reserved

Choose the report fields flexibly, assembling various reports according to business needs.

Note:

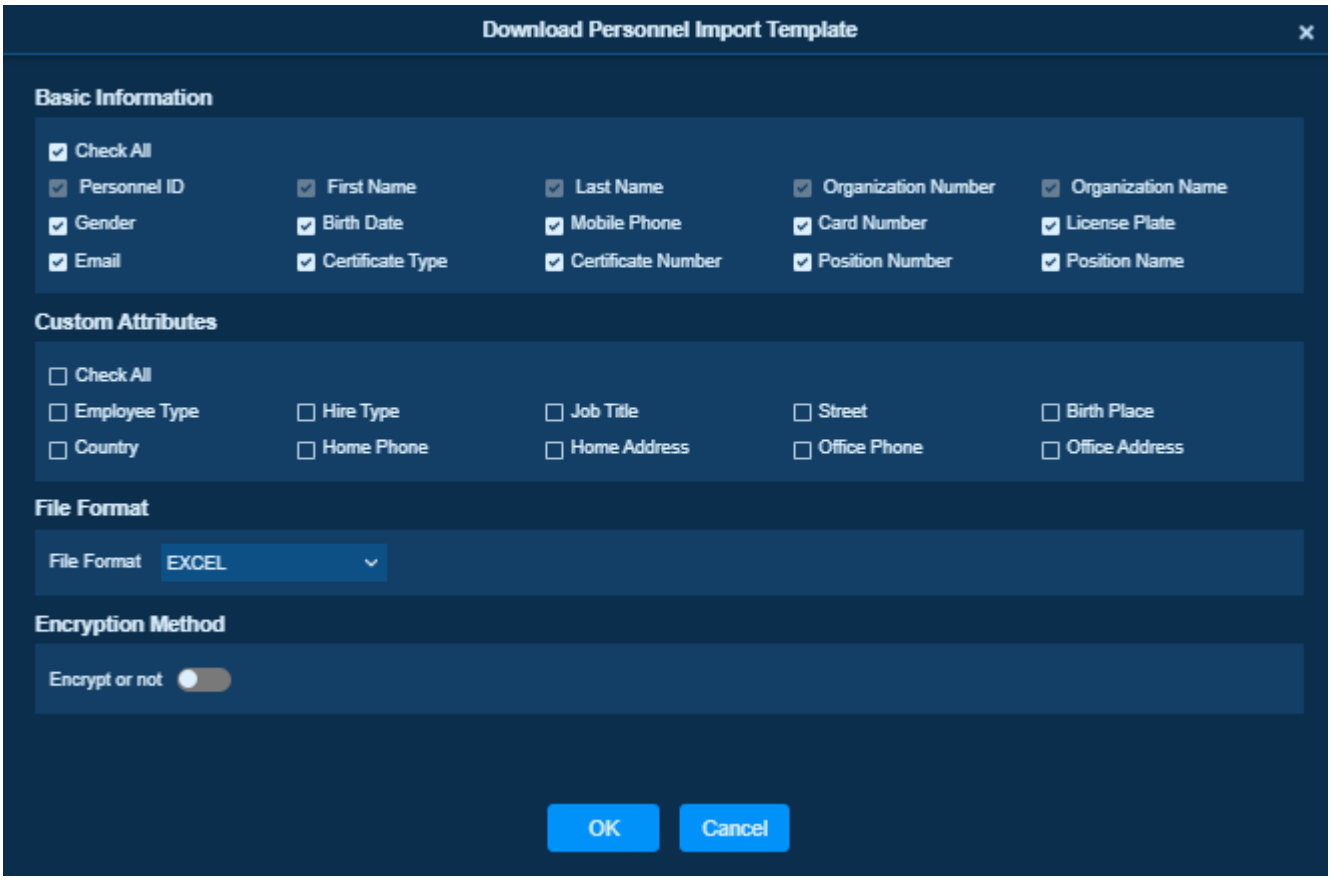
Exported information will be in XLSX format as shown in below image.

Person

Personnel ID	First Name	Last Name	Department Number	Department Name	Gender	Birthday	Password	Certificate Type	Certificate Number	Card Number	Email	Reservation Code	Mobile Phone
1	Jerry	Wang	1	General	Male	1980-04-23	1	1	TP443566	4461253	abwe@qwe.com	123456	59496464
2	Lucky	Tan	3	Development Department	Female	1992-12-08	2	3	784515	6155266	778@abc.com	123456	4425521
2940	Sherry	Yang	hotel	Hotel	Female	1997-12-01	2940	1	741741	1411237	555@qq.com	123456	145145145
3	Leo	Hou	4	Financial Department	Male	1998-12-22	3	1	23687	13271770	3232@qq.com	123456	34342543
4	Berry	Cao	1	General	Female	2007-12-05	4	4	745688QQWA	13592341	QWA@zzz.com	123456	74755466
5	Necol	Ye	2	Marketing Department	Male	2017-01-10	5	1	32242311	13260079	3322@qq.com	123456	6645454
6	Amber	Lin	4	Financial Department	Female	2017-07-04	6	1	784525004	4628036	787878@eru.com	123456	44620545
7	Jacky	Xiang	1	General		2016-01-05	7	8	ees1213232	6323994	434@qq.com	123456	54243231
8	Glori	Liu	2	Marketing Department	Female	1995-12-05	8	1	433114354	6189166	987@abcd.com	123456	77545353
9	Lilian	Mei	3	Development Department	Female	1992-12-23	9	1	XS22030	9505930	8989@pp.com	123456	221112121

Download Personnel Import Template

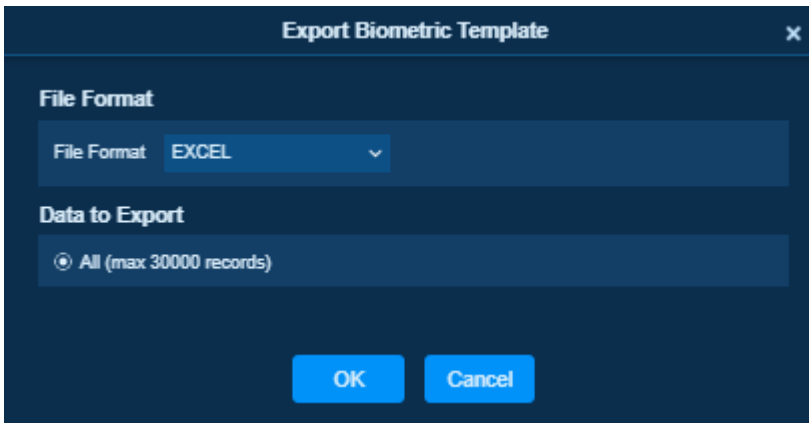
Before exporting the template, configure the necessary fields, including custom attribute fields. Note that required fields—Personnel ID, Name, Department ID, and Department Name—cannot be modified.



Export Biometric Templates

Exports registered biometric information for users.

Copyright © 2024 ARMATURA LLC. All rights reserved

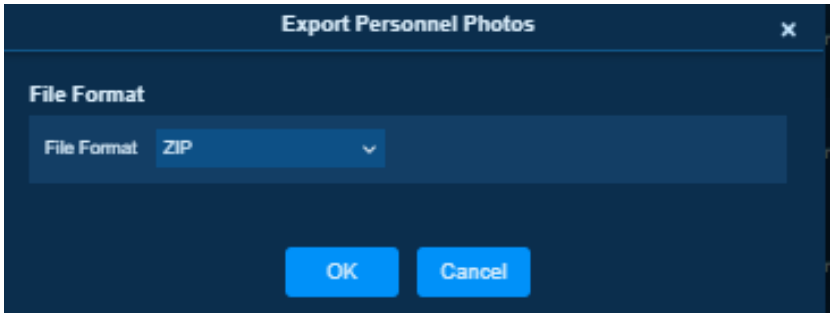


Personnel Biometric Template

Personnel ID	First Name	Last Name	Biometric	Biometric	Biometric	Biometric	Biometric	Biometric Template
1	Jerry	Wang	1	Fingerprint	10	4	1	TExTUzkAAAFDxEECAUHCc7QAAAdDmkBAAAAhDlvmg/fADwLvgANACkAyQCzAB4PFwD2DzoM1g ACAX4H9A/gACgP5QBOABUE8QCHAI4LhACJD+MMNQCfAJ8MSQ8gAVgM0ACQAIMAAAEsAVoJpQ AyD+4PKgA6ARwGtw8aAAEPkAB+AOMFjwDhAFILqACwD+QPrgCHANQP6g+5ACAPTAAXAFcAQQ CpAN4MNwCDD5IL+wAQAYMFTw8eAVYM0wDyAdQA5gBdABMPiAA/DtUPDAD+ABQK7Q8wAI8IlA CBAFsOiQDCAAQLuwCqD/QLagDjABoP3w/vAD4M5gAzADoI9wCpAJkEBwBsDw8P8AASAfoEeA82 AdMP9QDYAbsKNAADAc8PNgA1Ds8K9gBFAZ8MDA8FAcAK2ADiABYFvOzqOS4S7BK7/X7wtfZqAp 6ENfF8gE39fYBafY/hyrOrF78tbpYdkc5954P1kg+v1B0gB7//RXw4elFyQVphs8KzHZQddf7nYzNnbwD DpyG8+MPqgVLh4uMjfKTd69/0ecw/SMBKRjgUGt1P6v4KYBSgVe9XNMIjmBqL6g3XjeBNvQYRlx+PW QpghCr9tAtiHTgTQFlh9KJbwTHdZcX/Y7iBmODaHFogy79BBJzBtr0iH1KCzZ/3nNWcFoHYCMpEdcg+B6 48aUSOo1njYfQrQZdAl2FHACsisgFOXWlWcNSfXP/Wb+OPu1g/MPLgBDfkN+fYOQdwjk2nnaev8CrHt4 Ee114Y08A7OFIfLC8+vrQlX/GbaM5qb9d7sPJU4AArcnJwrFdAVrQ/9+/gQAnAFuZAkAaAFrwTppxR0 B2wWJi8GaevvOccETAOYNRlkz4XAcFYGAHAYBTLBFQDyGly7e3nOcWpaEACt2YB7zX/Ac2cHAH AeA1hLCwDmM48Fwm/MZhcBCEiTvnTEzsNpcWvAwAQXBAdQkHNyhnROwMRVwAwAz1WJqnyO8 BkBC1yQwKhngc1uwMFJwFvBAO9RFl0RAQtmVXL7zorCwMKEwMlAwWgH/UvDFgB5aYZgwMJ4w MLCOv9vfMEAMRsD4MHBU14YG1ZEgHlepZKw3dxfG8bUZ+WMH//8FaB8WygwNB/8lRAKpCg8fNw8 F2dn5W1QD1il39g4CAwQWEAQ/nihM7CAB3jBXwwf7BVx0B042nzFh6eG93wDrFxfH+wcLAgQjFNK RfXUtNcGAD1YJzFcYjCwsHCwLXBkWR6DgCCsPA7/S3xOcA4CADEdZfEzMCkHAEQeYAIHTB/8 M6XMWEDwBtsf7+6SnE8f5FCADMstL+R1wJAJS3A/84/TUFAcu3HC//jP4OD26XHf/wTpFDw+NvHDEw cEHVvoAAaS/D/spO/1GTsEOAKPEHjr8+vH8/lvAMQ3Fvskm/io+/8A/1ABVwtL+wP/+wDj/+SROwAUAS NSfw/rNBABO1VPAB/4OD5DhNPsywQf8QAoB8eE/sEFCwWv4zT9+1tFOhlFYeLewPz7/Dn9+PD6wf7 BwP46wAMP3/l6/v5RwwDg9DsqwAgQ2MBJR/JUGRDvDbpRwl2Cjld+//x+xhD7HTb5CBEWEpX/x/LDP wcQ7RWD/vvwSgUQRyBaBVQBH00iUCwFEccuW898ERB9M9M6c8DNzcjDwsH/BVkBH+40WkoXEIk2 1InBPP77+vw+l1ZLAhDQPVrAzxA7V+XBb2TACsWN6bXVEQ=

Export Personnel Photos

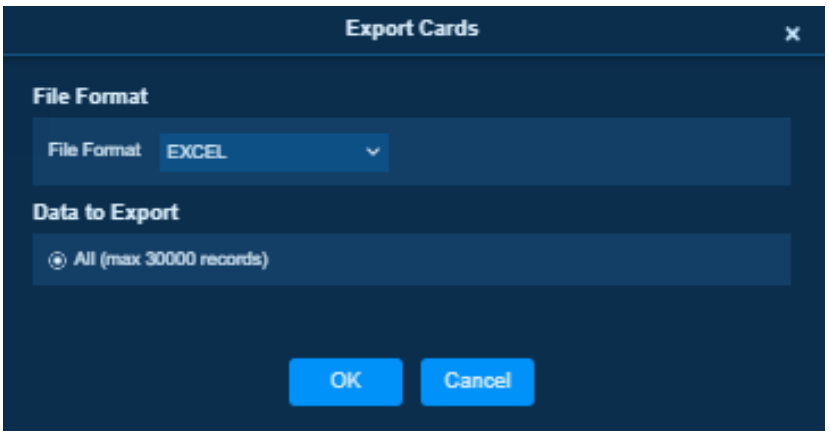
- Select the file type and click **OK.**



Export Cards

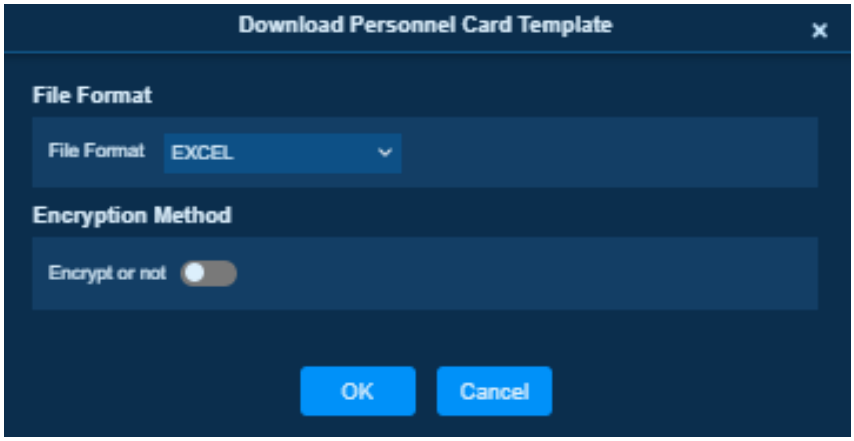
Exports details of registered cards.

Copyright © 2024 ARMATURA LLC. All rights reserved



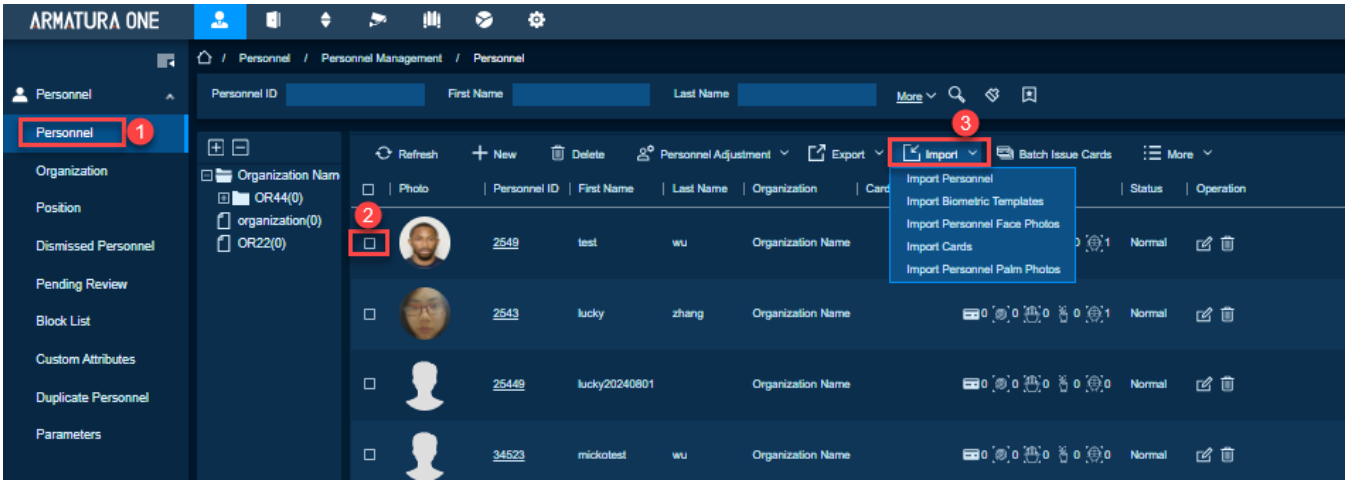
Download Personnel Card Template

Downloads the template for registered card details.



Import

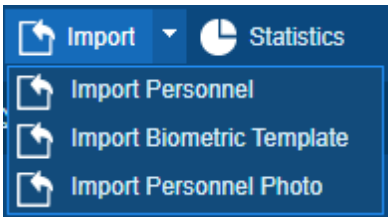
To import personnel information, biometric templates, photo, and related data, navigate to **[Personnel Management] > [Personnel] > [Import]**



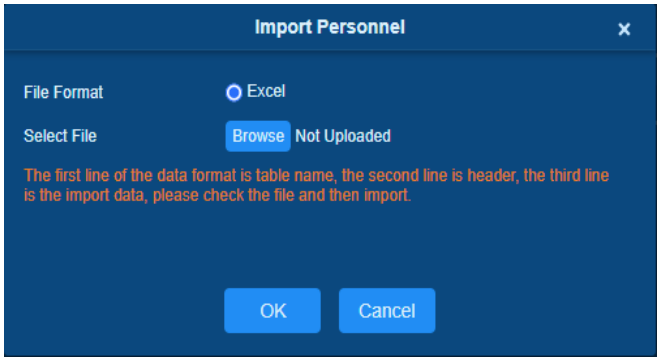
Copyright © 2024 ARMATURA LLC. All rights reserved

Import Personnel

Click **[Import] > [Import Personnel].**

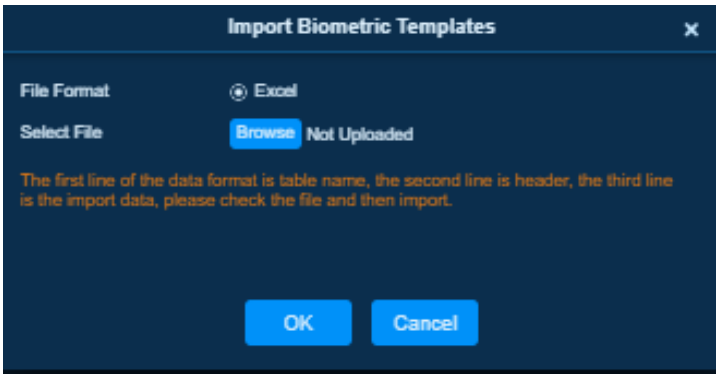


In the Import Personnel interface, click **[Browse]** to select the desired Excel file.



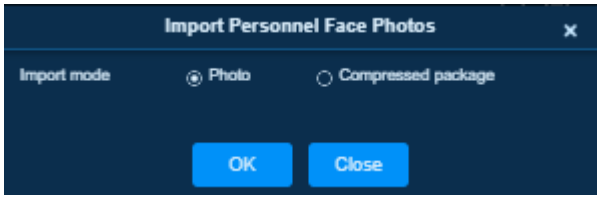
Import Biometric Templates

- Click **[Import]** > **[Browse]**
- In the interface, click **[Browse]** to select and upload the desired Excel file.

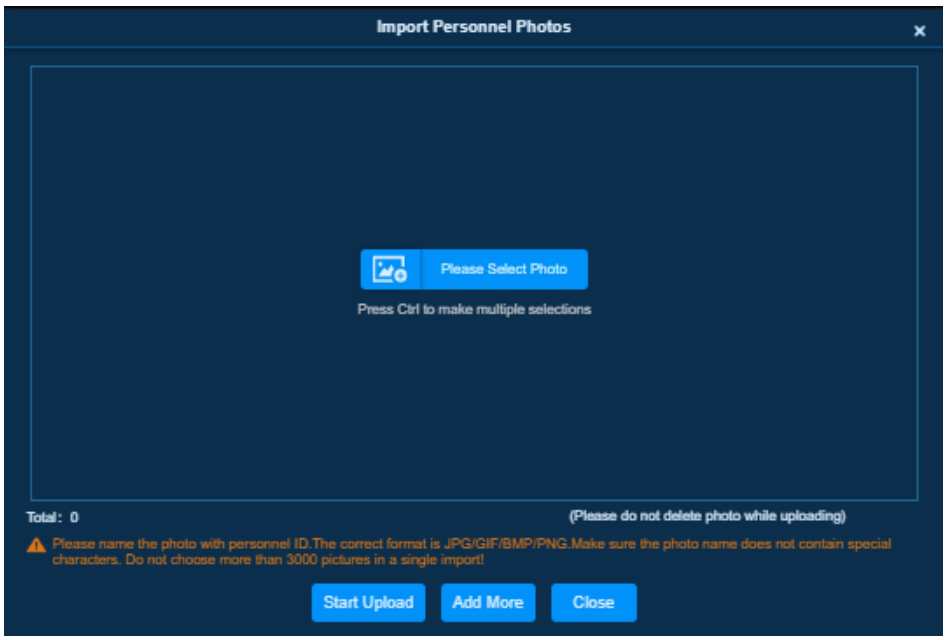


Import Personnel Face Photos

Personnel photos must be names according to the personnel ID for proper association. Supported image formats include **JPG, JPEG, PNG, and GIF.**

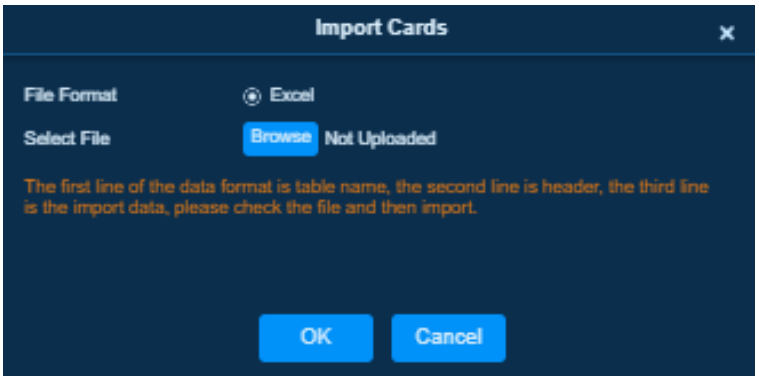


Copyright © 2024 ARMATURA LLC. All rights reserved



Import Card

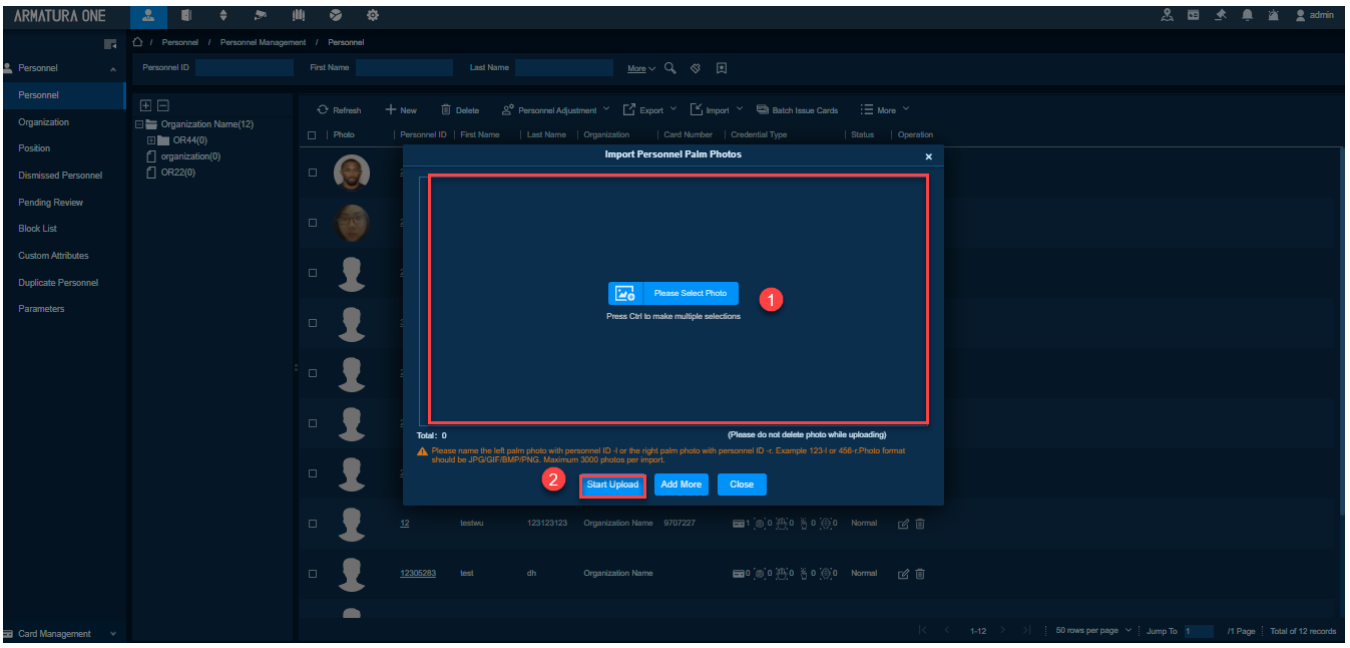
- Click **[Browse]** to select the Excel file and upload.



Import Personnel Palm Photo

This function is to import palm photos, which will be sent to the device, and the software will not generate biological templates. Click **[Please Select Photo]**, choose the photo, and then click **[Start Upload]** to begin.

Copyright © 2024 ARMATURA LLC. All rights reserved



Note:

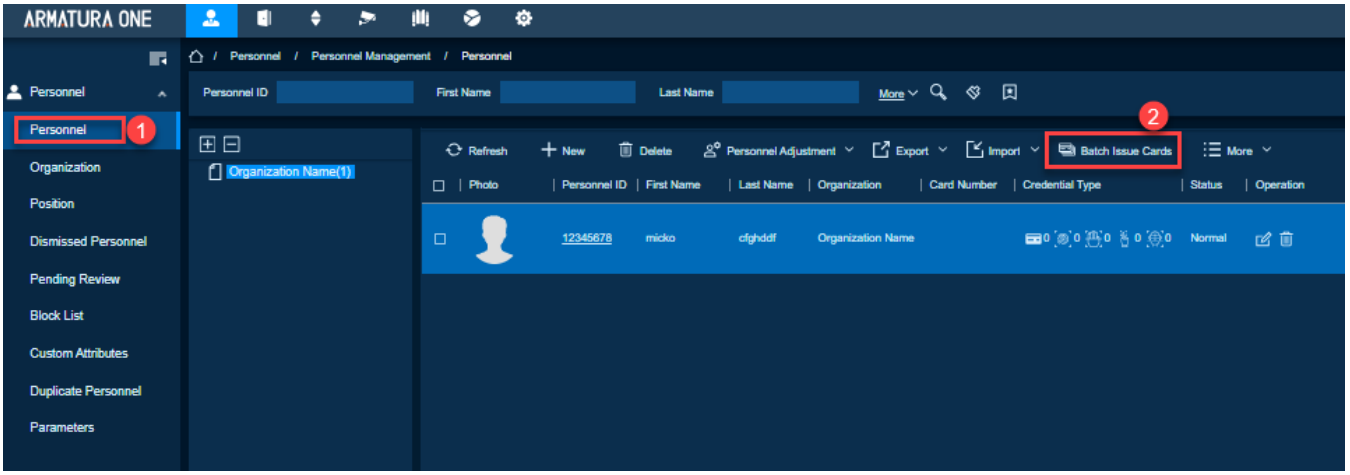
Personnel photos can be imported in two ways:

1. Import Distinctive Photos: Batch import up to 3,000 individual photo files simultaneously.

2. Import Compressed Package: Upload a single ZIP archive with a maximum size of 500MB.

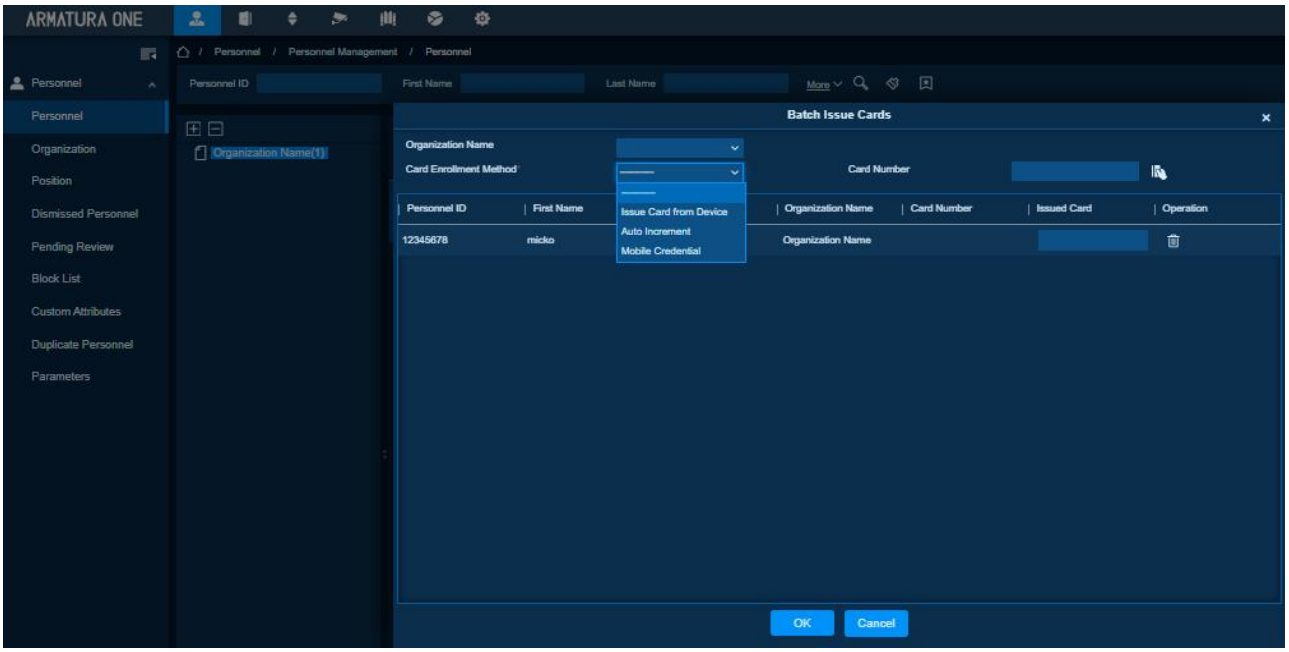
Batch Issue Cards

Navigate to **[Personnel Management]** > **[Personnel] > [Batch Issue Cards].**



Copyright © 2024 ARMATURA LLC. All rights reserved

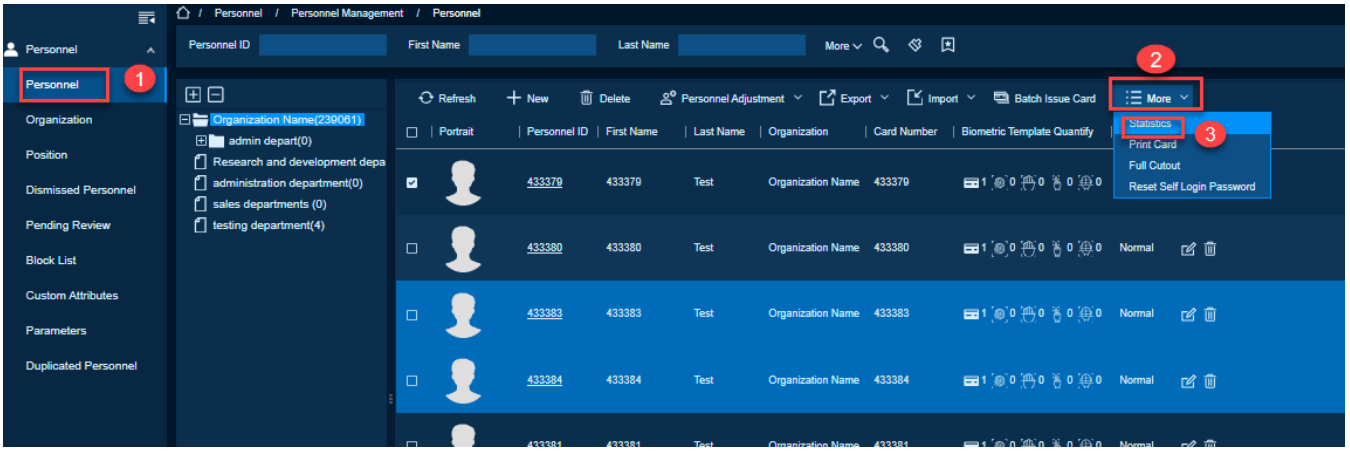
The Batch Issue Cards interface is shown below.



Use the Batch Issue Cards interface to issue multiple credentials on a single page, streamlining the process by eliminating the ned to issue cards one by one.

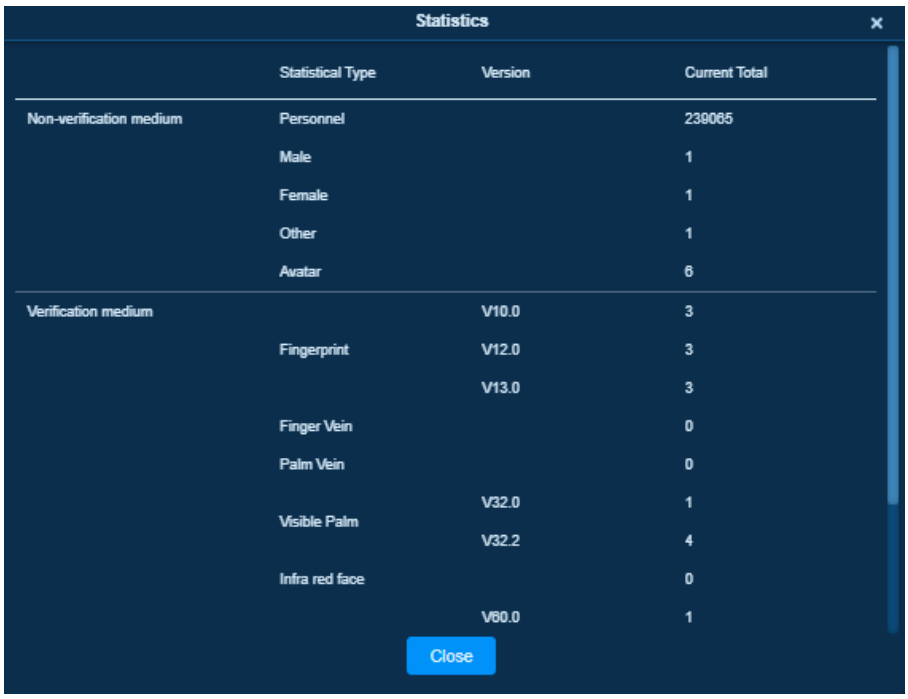
Statistics

To view detailed statistical information about personnel and their credentials, navigate to **[Personnel Management] > [Personnel] > [Statistics].** This includes the number of personnel, fingerprints, face templates, finger veins, card numbers, gender distribution, and other related data.



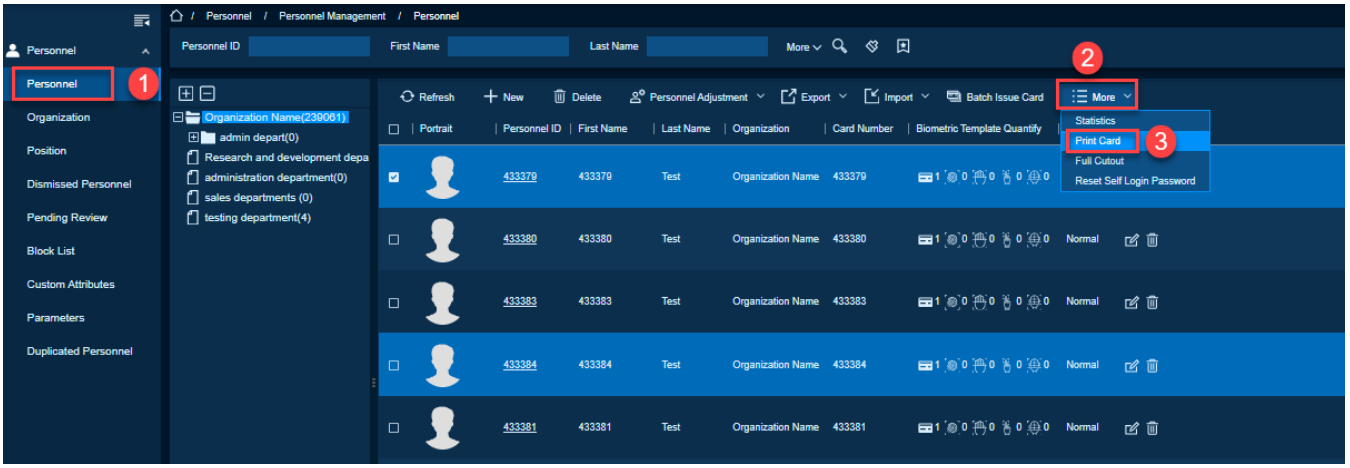
The Statistics interface is shown below.

Copyright © 2024 ARMATURA LLC. All rights reserved



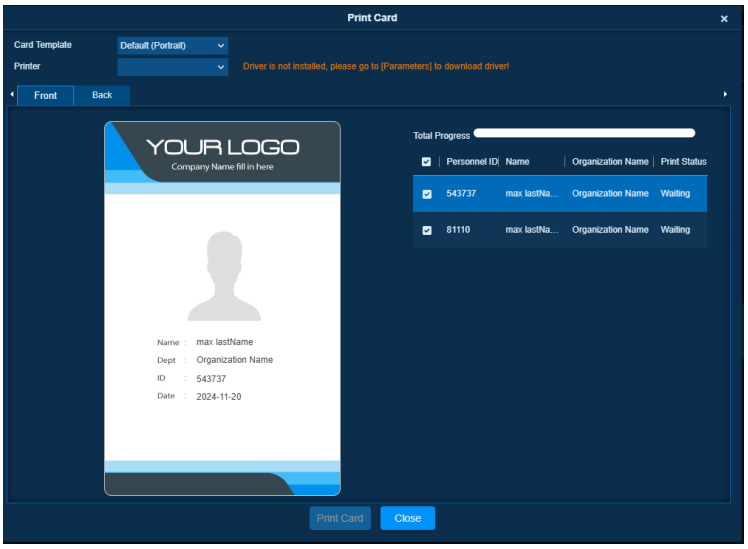
Print Card

- Navigate to **[Personnel Management]** > **[Personnel]** > **[Import]** to access the card printing interface.
- Select the desired Personnel ID and click **Print Card**.



Copyright © 2024 ARMATURA LLC. All rights reserved

The Print Card interface is shown below.



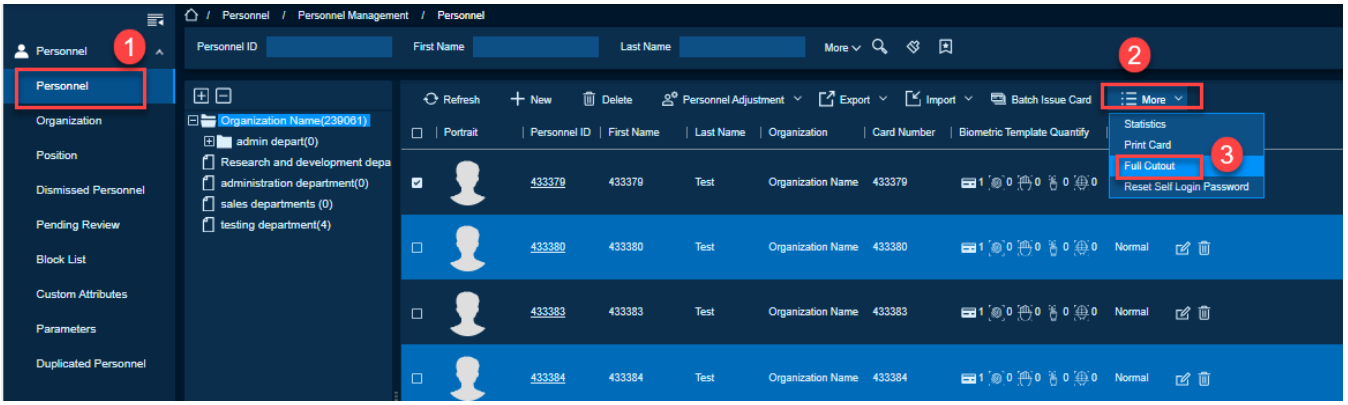
Note:

Card templates can be defined under **[System] > [Basic Management] > [Print Template]**.

Ensure the card printer driver is downloaded and installed properly through **[Personnel Management] > [Personnel] > [Parameters] > [Registration Client].** The registration code can be added via **[System] > [Authority Management] > [Client Register].**

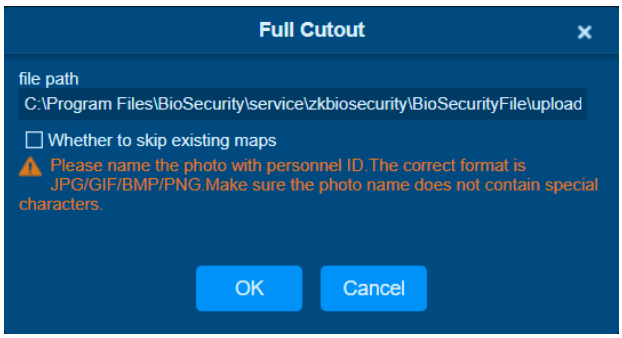
Full Cutout

- Navigate to **[Personnel Management]** > **[Personnel]**, select a person, and click **[Full Cutout]**.



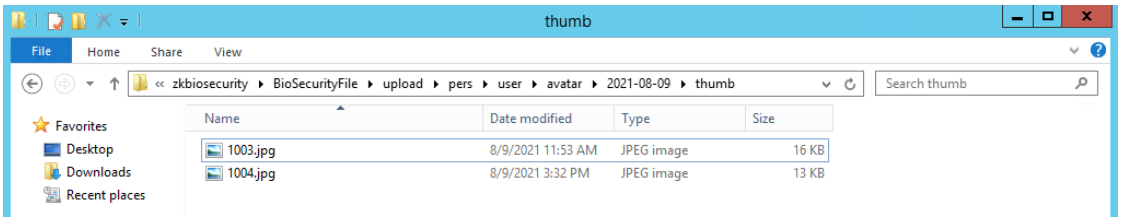
- In the **Full Cutout** interface, enter the file path and click **OK.**

Copyright © 2024 ARMATURA LLC. All rights reserved



Choose whether to skip existing maps when creating a new folder.

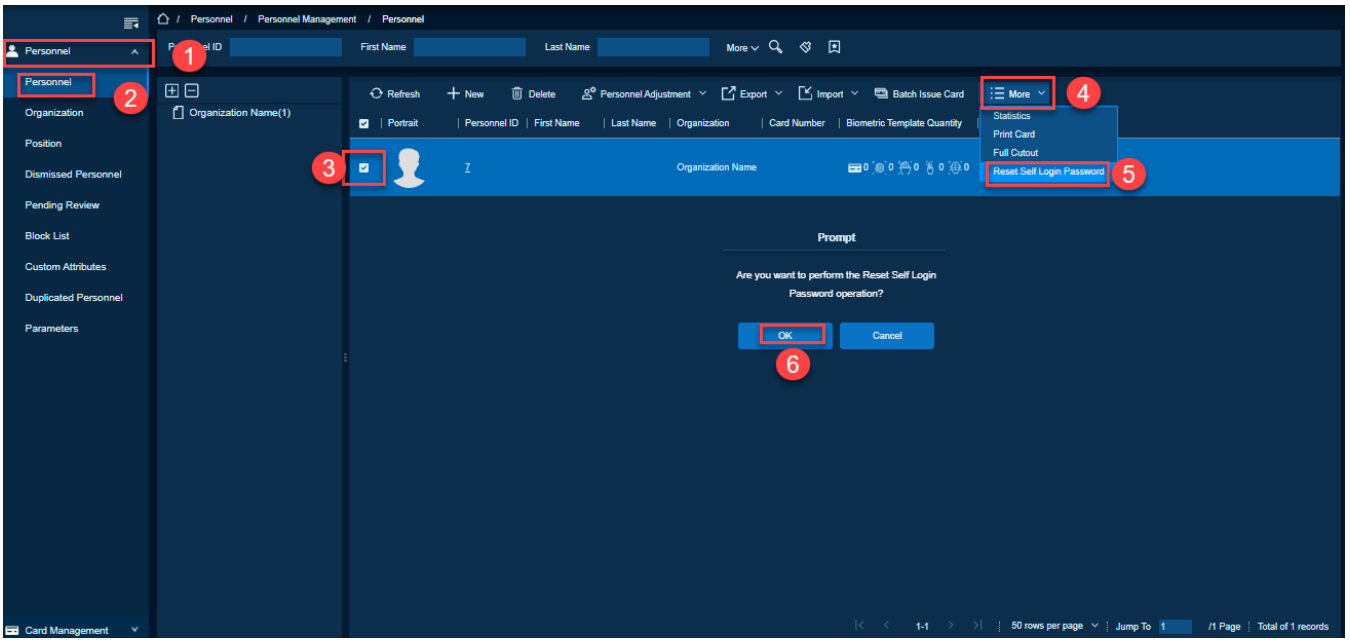
Once the process is complete, all personnel photos will be saved locally and names according to the personnel ID.



All photos will be encrypted and cannot be opened directly. This ensures their secure use for future imports into the system.

Reset Self-Login Password

- Go to **[Personnel Management]** > **[Personnel]**, then select a person, and click **[Reset self-login password]**.
- Choose the desired Personnel ID and click **Reset Self-Login Password**.



Copyright © 2024 ARMATURA LLC. All rights reserved

5.1.2. Organization

Before managing employees, it is necessary to establish the company's departmental organization chart within the system. By default, the system includes a primary department named **[General]**, numbered **[1]**. This organization can be edited but cannot be deleted. The key functions of Organization Management include adding, editing, deleting, exporting, and importing organizations.

Usage Scenario

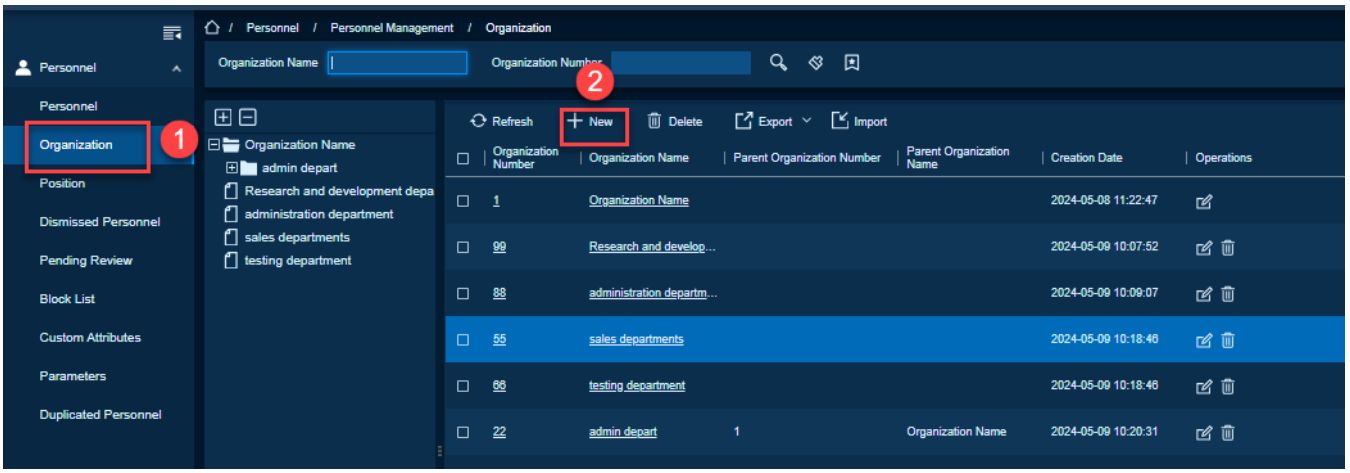
The Organization module allows users to create a new organization, define its structure, and manage relationships between various departments.

Trigger Results

Operation	Description
Check the parent organization	Set the newly added organization as a sub-organization of an existing organization. Personnel authority and structure are integrated with the parent organization.

Add Organization

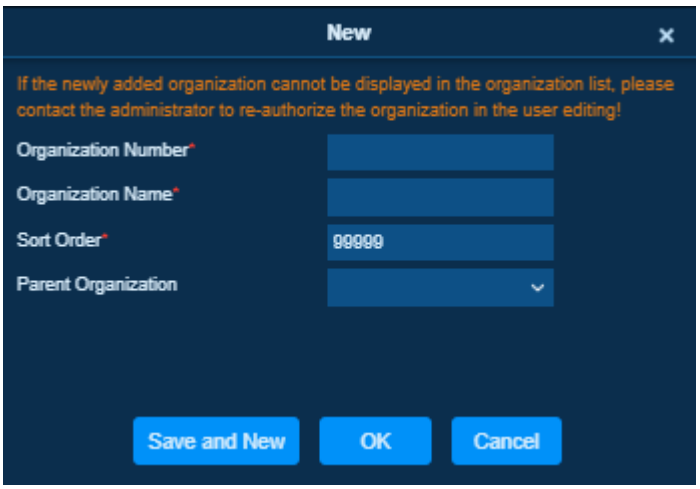
- Navigate **[Personnel]** > **[Personnel Management]** > **[Organization]** > **[New]**.



- On the New Organization Interface, complete the following fields:

Organization Number: Must be alphanumeric, unique, and no longer than 30 characters.

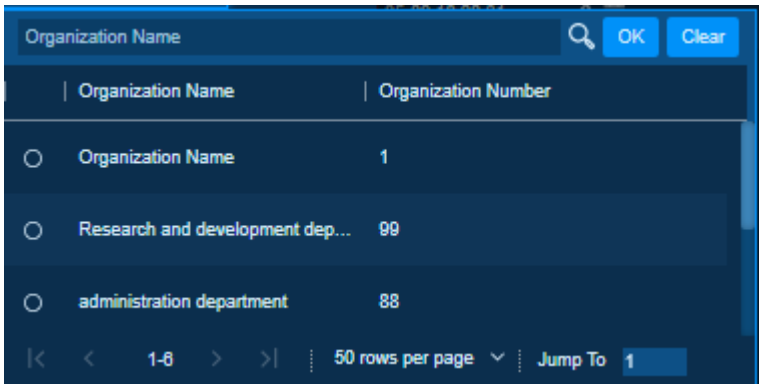
Copyright © 2024 ARMATURA LLC. All rights reserved



Organization Name: Can include any characters, with a maximum length of 100 characters. Names may be repeated at different hierarchy levels.

Rank: Specify a number between 1 and 999,999,999. Smaller numbers denote higher ranks within the same level. If left empty, departments are sorted in ascending order by default.

Parent Organization: Choose a parent organization from the drop-down menu. This establishes the organization's position in the company hierarchy, which is displayed as an organization tree on the left side of the interface.



After completing the fields:

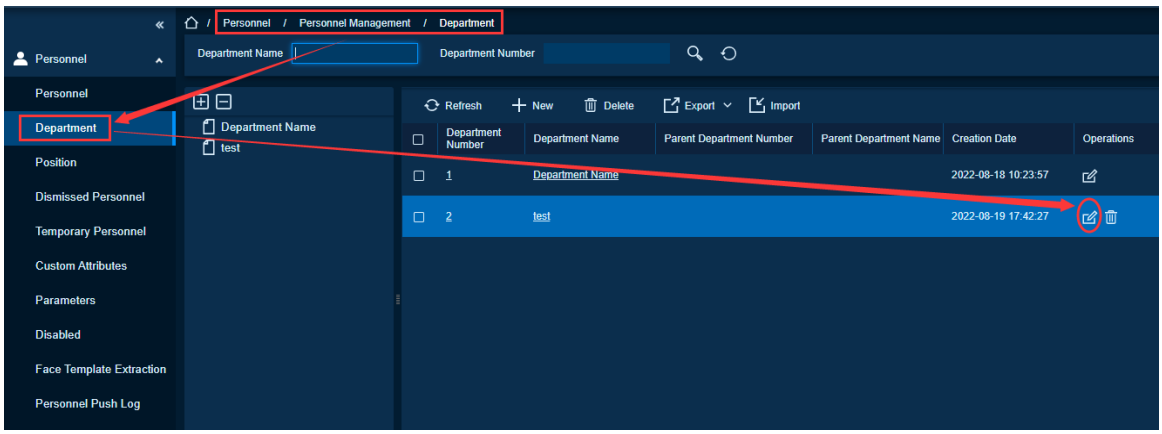
1. Click **[OK]** to save the changes.
2. Click **[Cancel]** to discard changes.
3. Click **[Save and New]** to save the current organization and add another.

Alternatively, use the **[Import]** feature to upload organizational information from external software of documents. For details, refer to the Common Operations section.

Edit An Organization

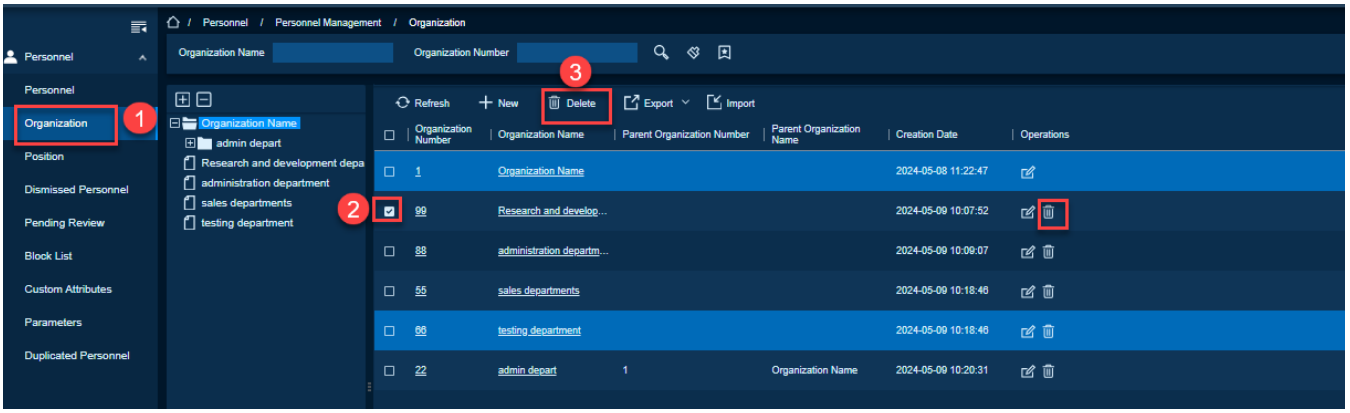
- Navigate to **[Personnel]** > **[Personnel Management]** > **[Organization]** > **[Edit]**.
- Select the organization to modify, make the required changes, and click **[OK]** to save.

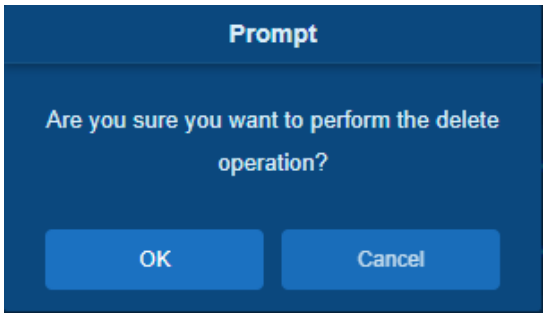
Copyright © 2024 ARMATURA LLC. All rights reserved



Delete An Organization

- Navigate to **[Personnel]** > **[Personnel Management]** > **[Organization]** > **[Delete]**.
- Select the organization to delete and click **[OK]** to confirm.





Note:

Organizations with sub-organizations or personnel assigned cannot be deleted.

Export

To export organizational data, follow these steps:

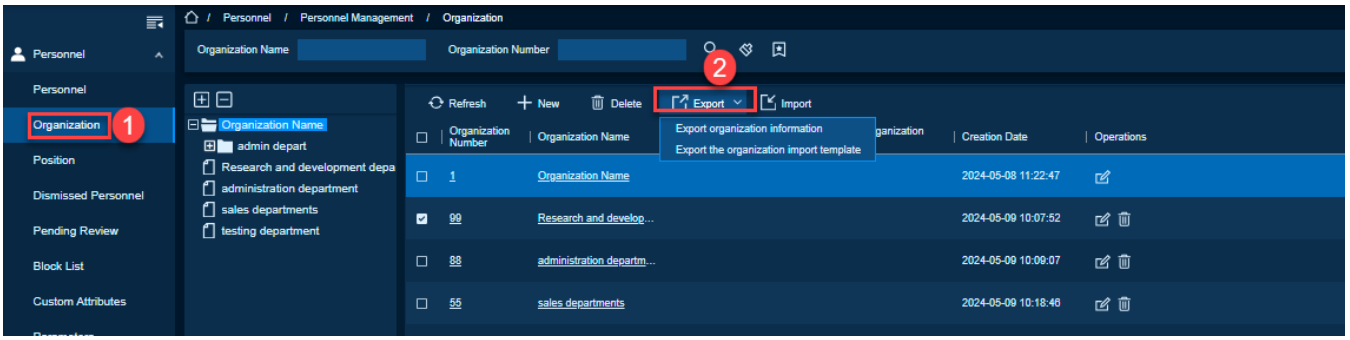
- Navigate to **[Personnel Management] > [Organization] > [Export].**

Choose from the available export options:

Export Organization: Export detailed organizational information.

Copyright © 2024 ARMATURA LLC. All rights reserved

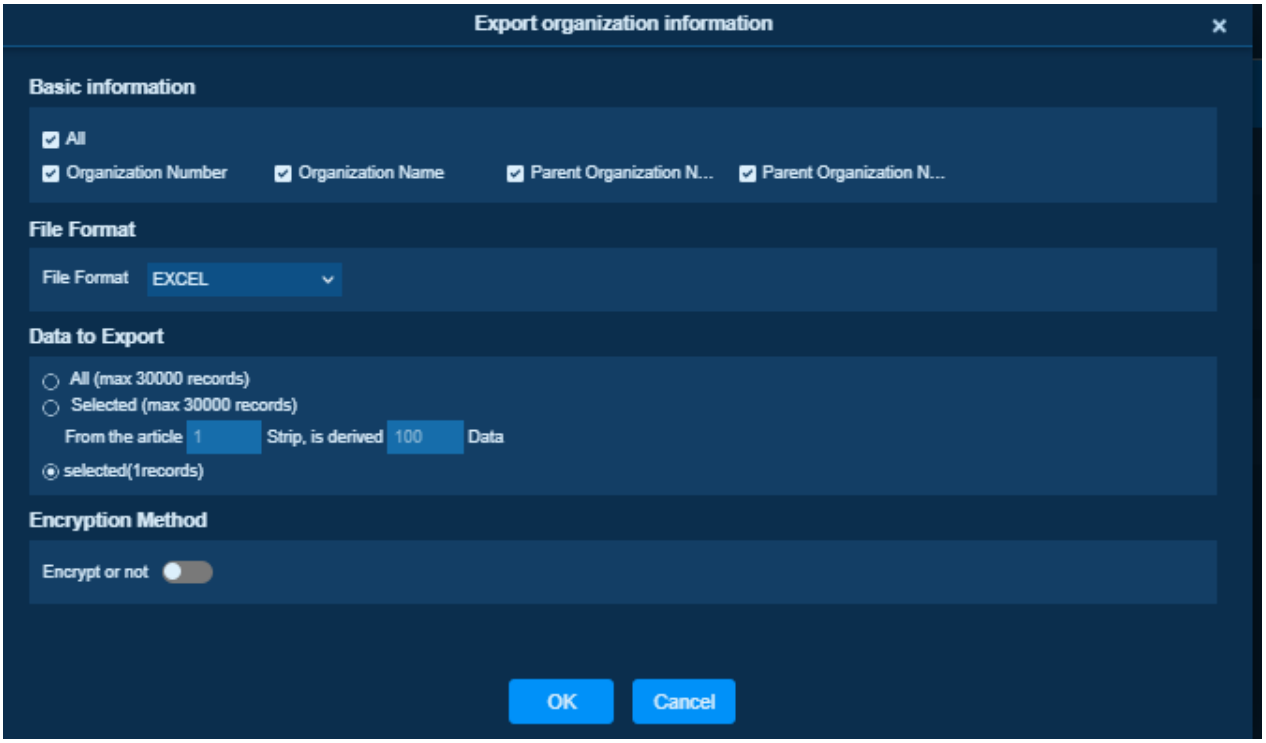
Download Organization Import Template: The export options include **Export Organization** and **Download Organization** Import Template.



On the Export Organization interface:

Select the File Type (EXCEL, PDF, or CSV) and the desired Export Mode

- Click **[OK]** to proceed.



Department

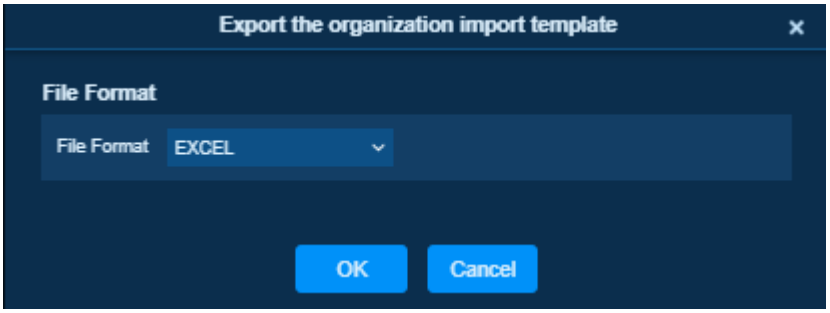
Department Number	Department Name	Parent Department Number	Parent Department	Created Date
hotel	Hotel			2017-12-15 09:06:51
4	Financial Department	1	General	2017-12-15 09:06:48
3	Development Department	1	General	2017-12-15 09:06:48
2	Marketing Department	1	General	2017-12-15 09:06:48
1	General			2017-12-15 09:06:48

Copyright © 2024 ARMATURA LLC. All rights reserved

For the Download Organization Import Template option:

Select the **EXCEL** File format to download template.

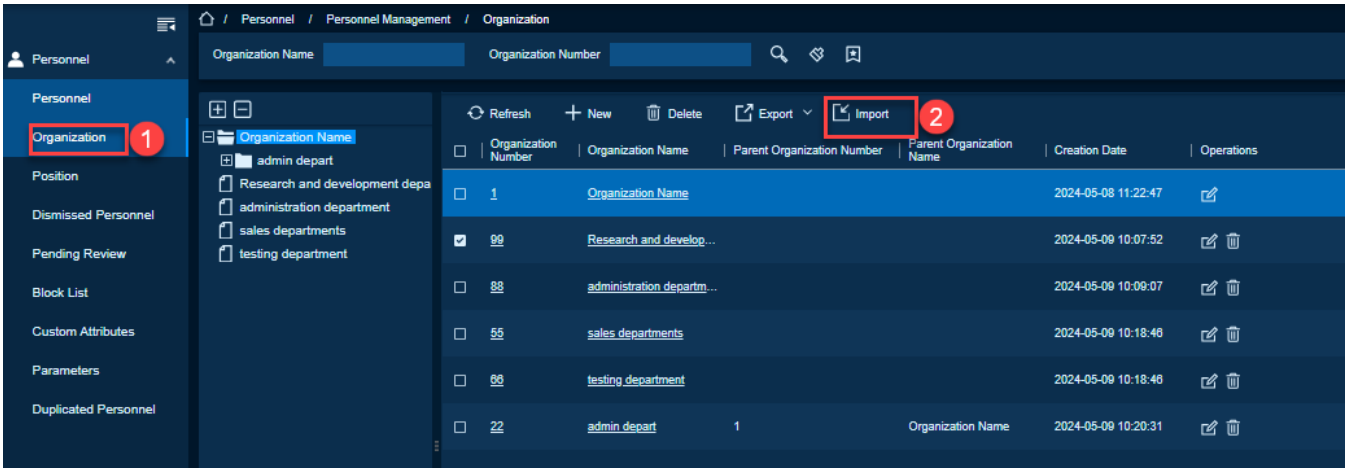
This template provides a structured format for importing organizational data into the system.



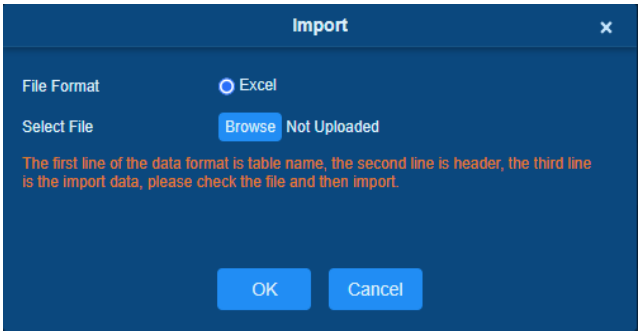
Import

To import organizational data:

- Go to **[Personnel Management]** > **[Organization]** > **[Import]**.



- Select the file format as Excel and upload the corresponding file.



- Click **[OK]** to complete the import process.

Copyright © 2024 ARMATURA LLC. All rights reserved

5.1.3. Position

The Position module allows operators with appropriate authority to organize personnel based on their roles, competencies, and skills. Users can define designations to streamline personnel management and facilitate easier sorting.

Usage Scenario

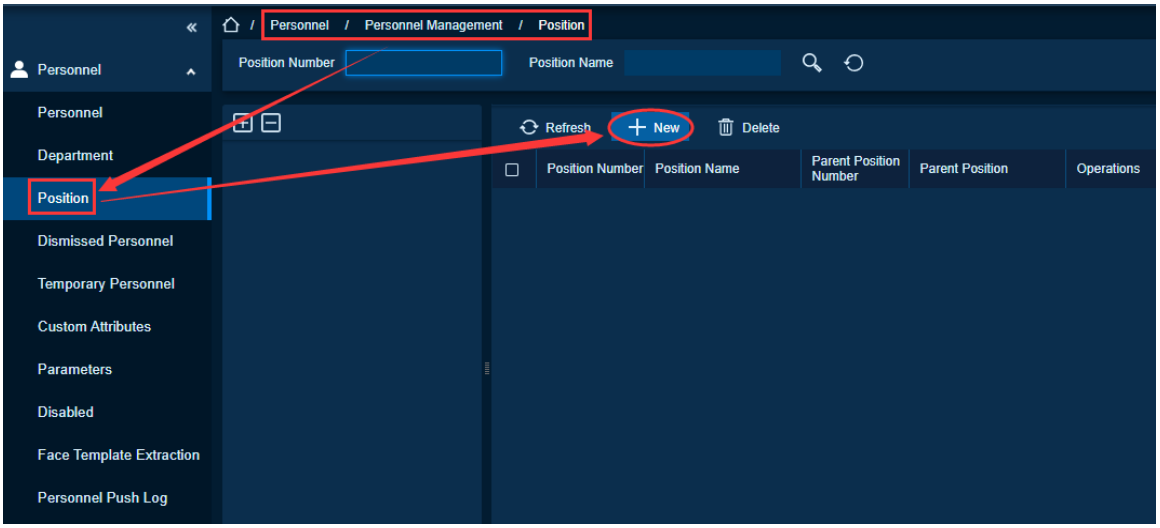
Create and manage position information for personnel, define hierarchical connections, and establish roles necessary for operations such as attendance approval.

Trigger Result

Operation	Description
Check the Superior Position	Set the newly added position as a sub-position of an existing one, ensuring its personnel attendance aligns with the superior position.

Add Position

- Navigate **[Personnel]** > **[Personnel Management]** > **[Position]** > **[New]**.



- On the New interface, complete the following fields:

a) Position Number: Enter a unique alphanumeric value (up to 30 characters). Special characters are not allowed.

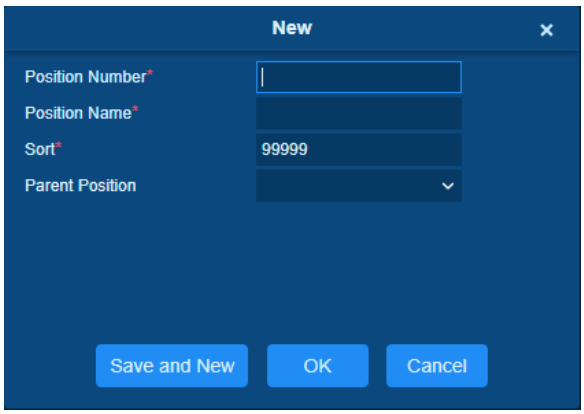
b) Position Name: Provide a unique name for the position (up to 100 characters).

c) Sort: Enter a numeric value (1–999,999,999). Positions with smaller sort numbers are ranked higher within the same level. If left empty, positions are ordered by their creation sequence.

d) Parent Position: Select a parent position to define the hierarchy. This parameter helps organize personnel based on skills and competencies.

- Click **[OK]** to save the changes.

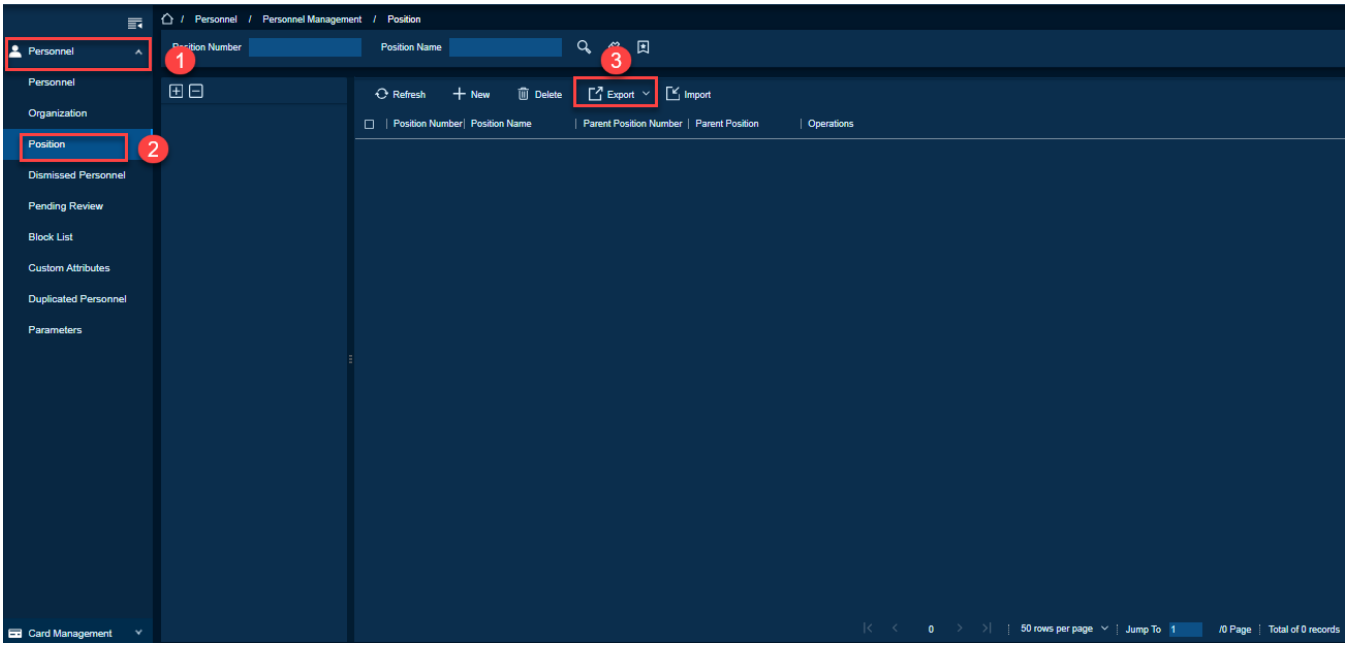
Copyright © 2024 ARMATURA LLC. All rights reserved



Export

To export position data :

- Navigate to **[Personnel]** > **[Personnel Management]** > **[position]** > **[Export]**.

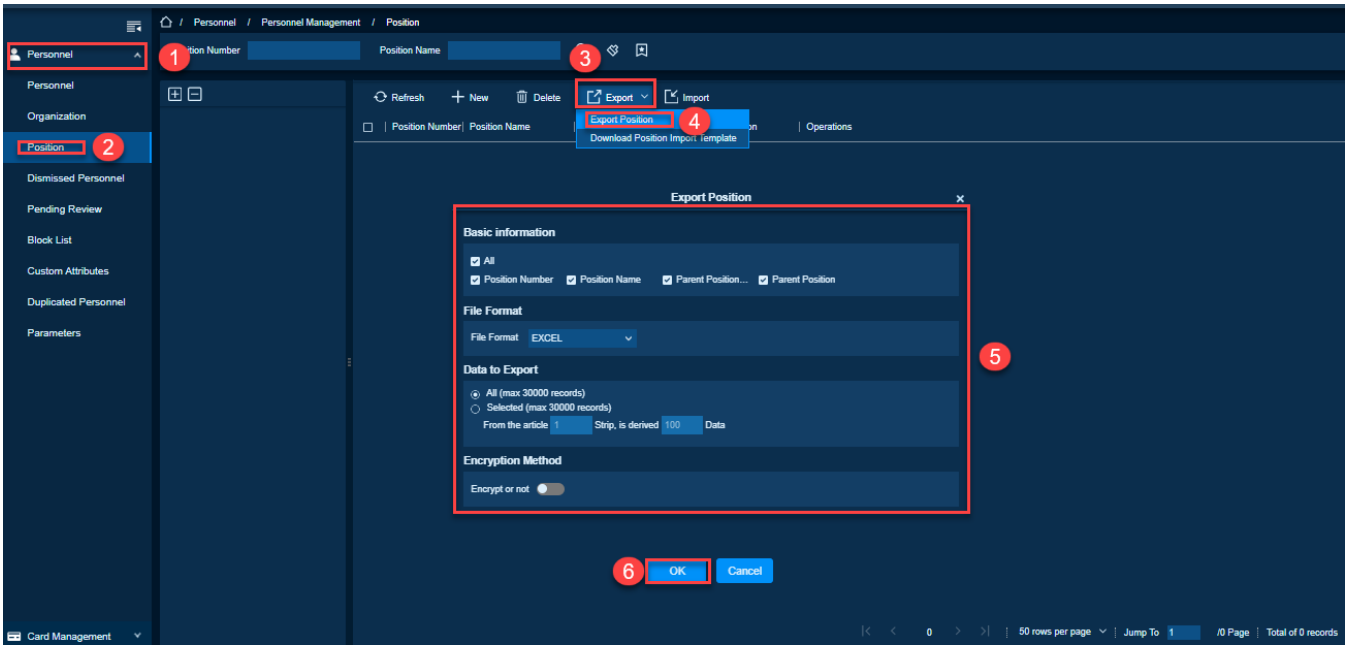


- Choose one of the following options:

  Export Position: Export the details of positions in the system.

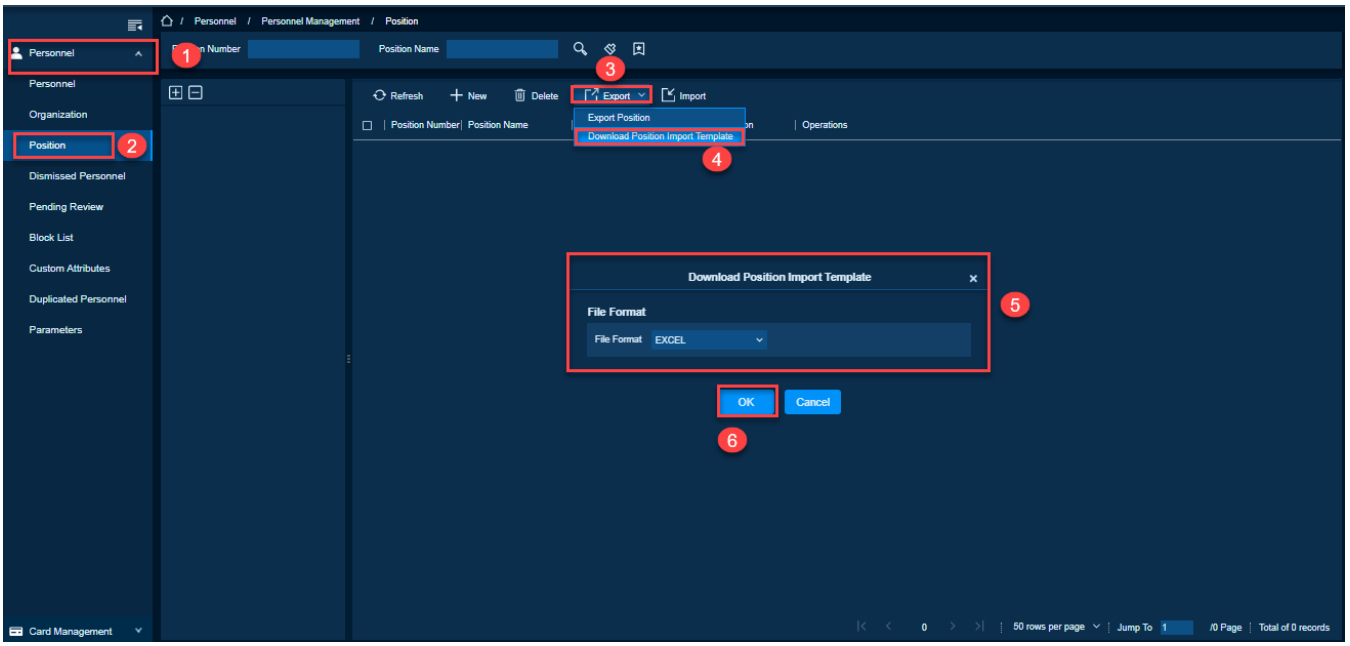
  Download Position Import Template: Download a predefined template to assist with importing position data.

Copyright © 2024 ARMATURA LLC. All rights reserved



On the export Interface: Select the file format (e.g., EXCEL, PDF, CSV).

- Click **[OK]** to proceed.

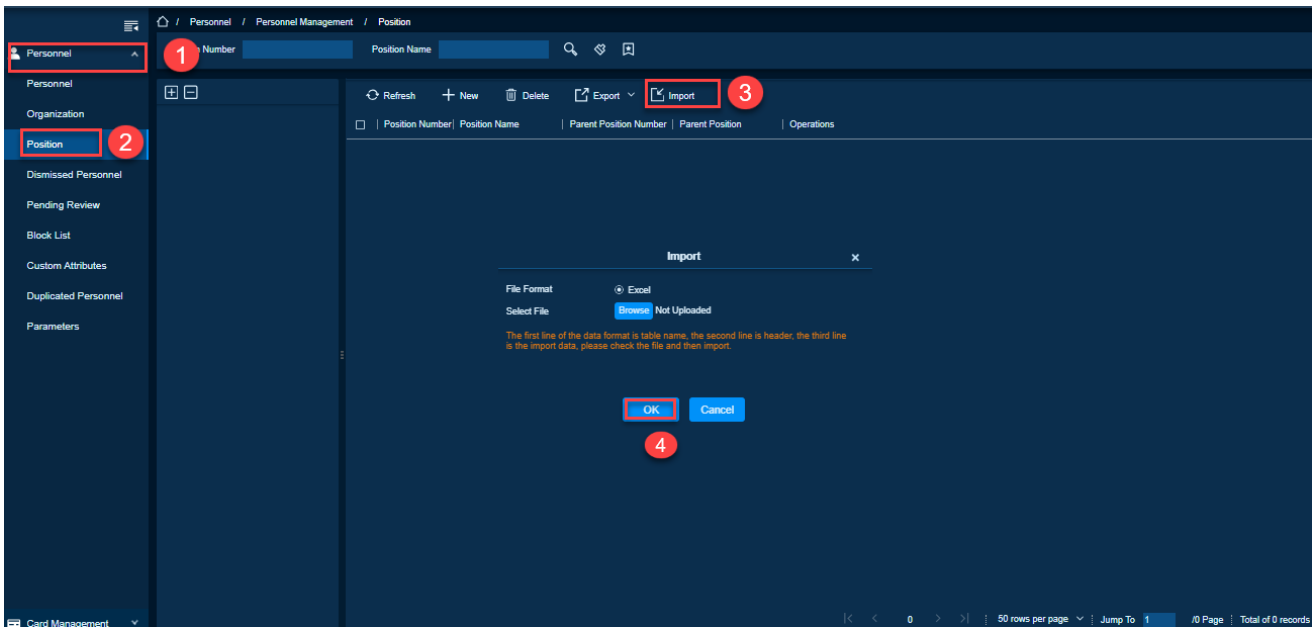


Import

To import position data:

- Navigate to **[Personnel]** > **[Personnel Management]** > **[position]** > **[Import]**.

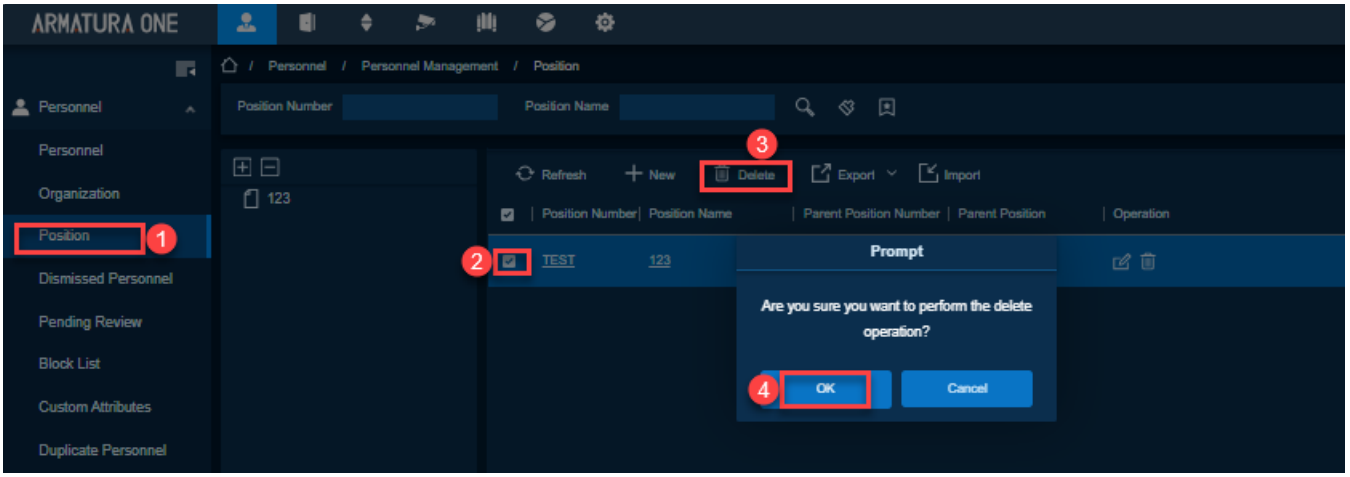
Copyright © 2024 ARMATURA LLC. All rights reserved



- Select the file format and click browse to upload the file
- Click **[OK]** to complete the import process.

Delete Position

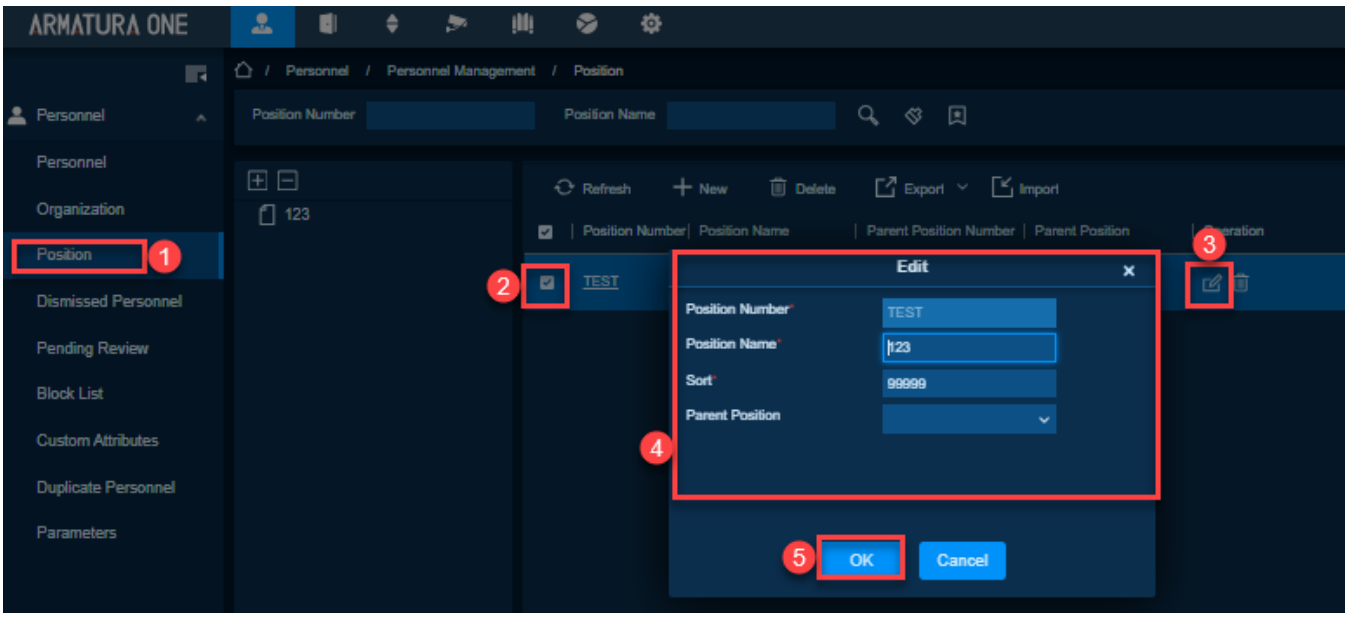
- Navigate to **[Personnel]** > **[Personnel Management]** > **[position]** > **[Delete]**
- Select the position to delete and Click **[OK]** to confirm.



Edit Position

- Navigate to **[Personnel]** > **[Personnel Management]** > **[position]** > **[Edit]**
- Select the desired position, update its details, and click **[OK]** to save.

Copyright © 2024 ARMATURA LLC. All rights reserved



5.1.4. Dismissed Personnel

The Dismissed Personnel module allows operators to manage records of personnel who have resigned, including saving their identity information, exporting their details, and reinstating them if necessary.

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Save and manage the identity information of resigned personnel.

Export the details of dismissed personnel for record-keeping.

Reinstate personnel who have left the organization.

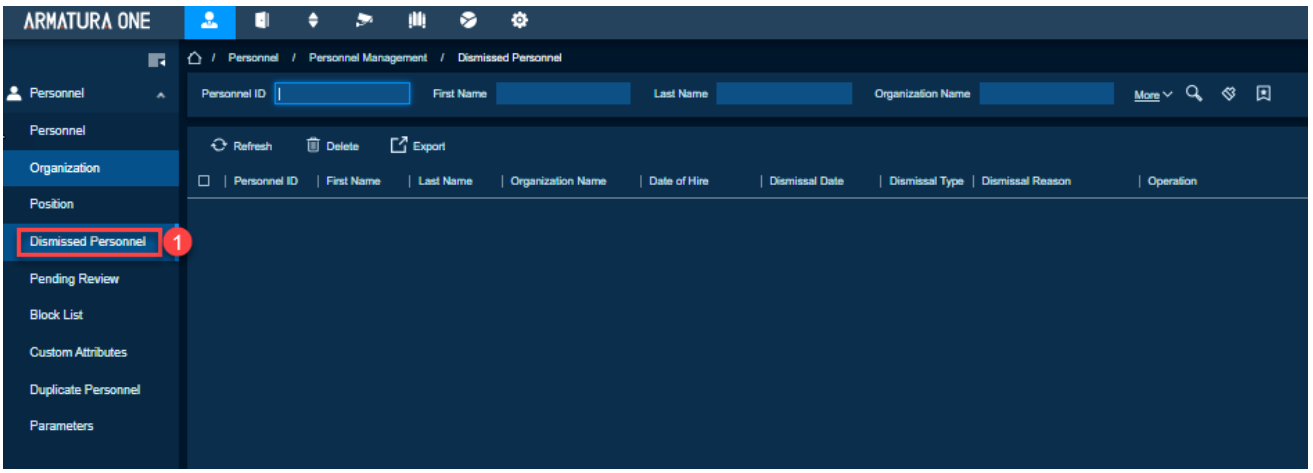
Trigger Result

Operation	Description
Check the recor dismissed perso	View details of dismissed personnel, including th dismissal date, type, and reason.

Steps to Check Dismissed Personnel Records

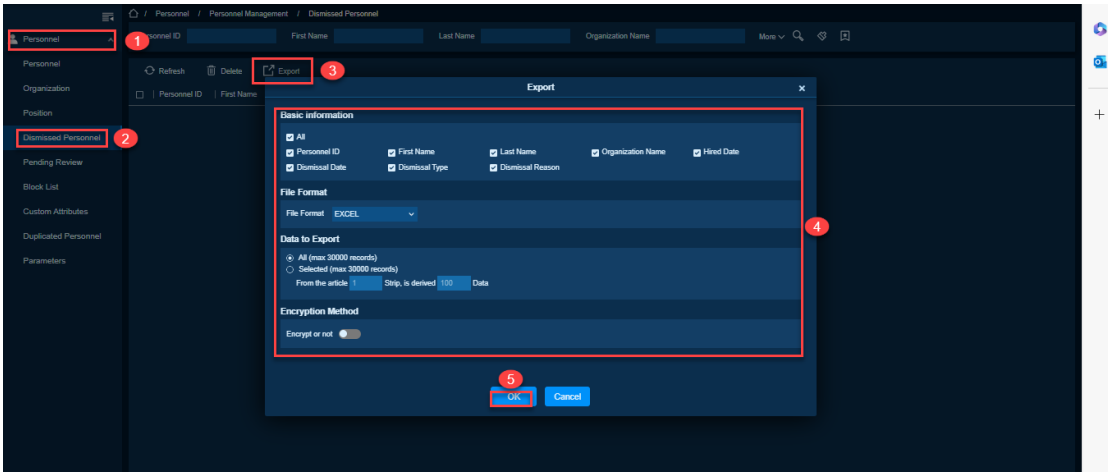
- Navigate to **[Personnel] > [Personnel Management] > [Dismissed Personnel].**
- Review the list of dismissed personnel and view their details.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export Dismissed Personnel Records

- Go to **[Personnel]** > **[Personnel Management]** > **[Dismissed Personnel]** > **[Export]**.

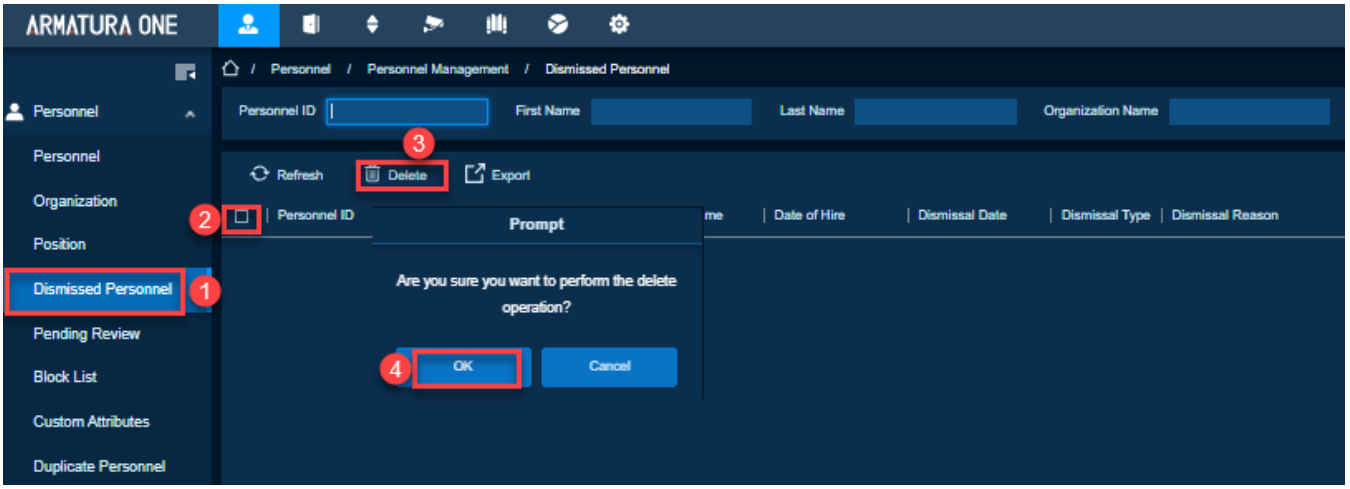


- Enter the required details in the export interface and click **[OK]** to download the records.

Delete Dismissed Personnel

- Navigate to **[Personnel]** > **[Personnel Management]** > **[Dismissed Personnel]** Select the required personnel ID, click **[Delete]**, then confirm by clicking **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



5.1.5. Pending Review

The Pending Review module allows operators to manage and review temporary personnel records, enabling them to approve access or make necessary adjustments.

Prerequisites for Use

Log into the system using an account with the required permissions, ensuring the 'Personnel Self-Service Appointment' function enabled and the 'Automatic Review' function disabled.

Usage Scenario

This module displays a list of personnel added via QR code scanning from a device. Temporary personnel listed here can be granted access to specific areas based on the operator's review.

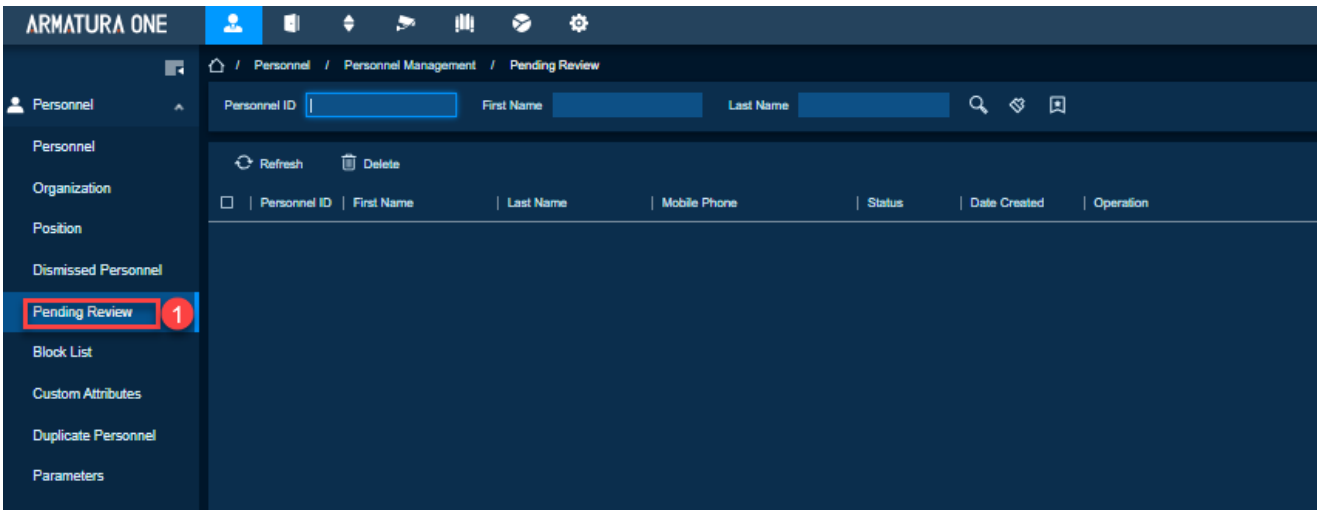
Trigger Result

Operation	Description
Review Operation	Review the information of temporary personnel assign necessary permissions.

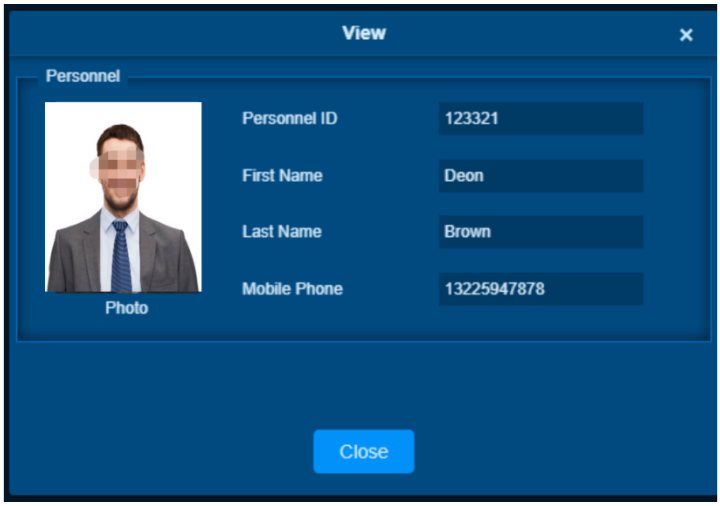
Steps to Review Pending Personnel:

- Navigate to **[Personnel]** > **[Personnel Management]** > **[Pending Review]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Select the personnel and click **[view]**, the review interface will display the personnel's information.



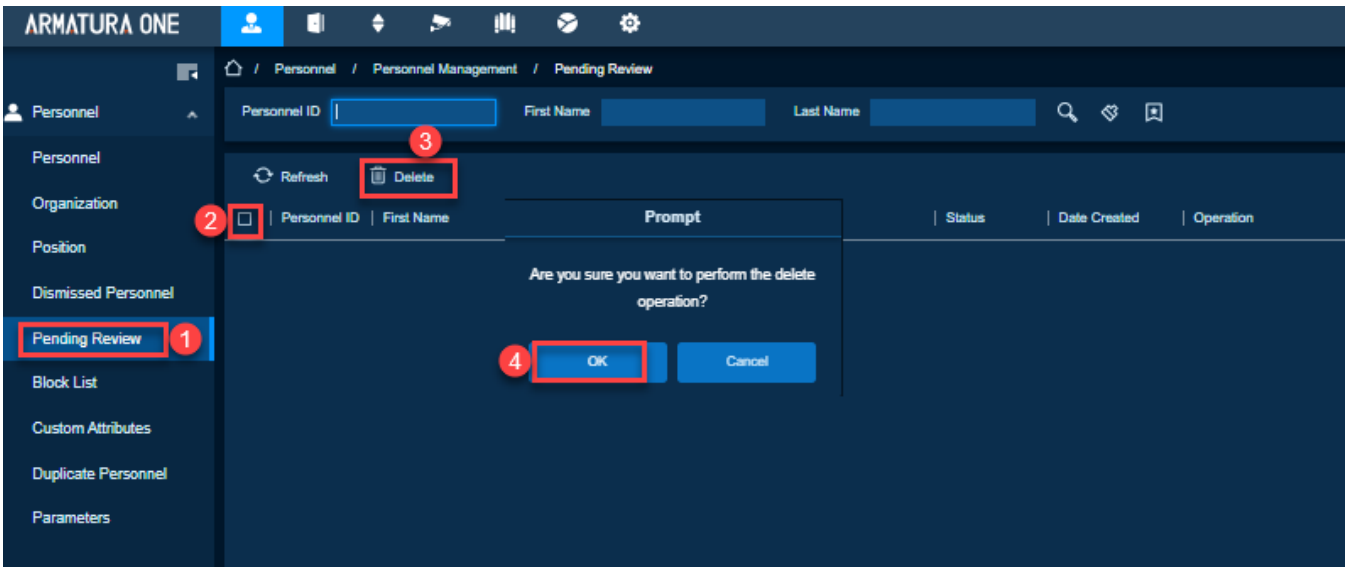
- Make any required changes and click **[OK]** to save, once approved, the personnel will be automatically added to the Personnel List.

Delete Pending Review

It is used for deleting the selected temporary personnel.

- Go to **[Personnel]** > **[Personnel Management]** > **[Pending Review]** > **[Delete]** and confirm the action by selecting the required personnel ID and click **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



5.1.6. Block List

The Block List module is used to manage individuals whose access rights have been revoked. When a person is added to this list, all associated access permissions are automatically blocked.

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Add personnel to the Block List to immediately revoke all of their access rights across the system.

Trigger Results

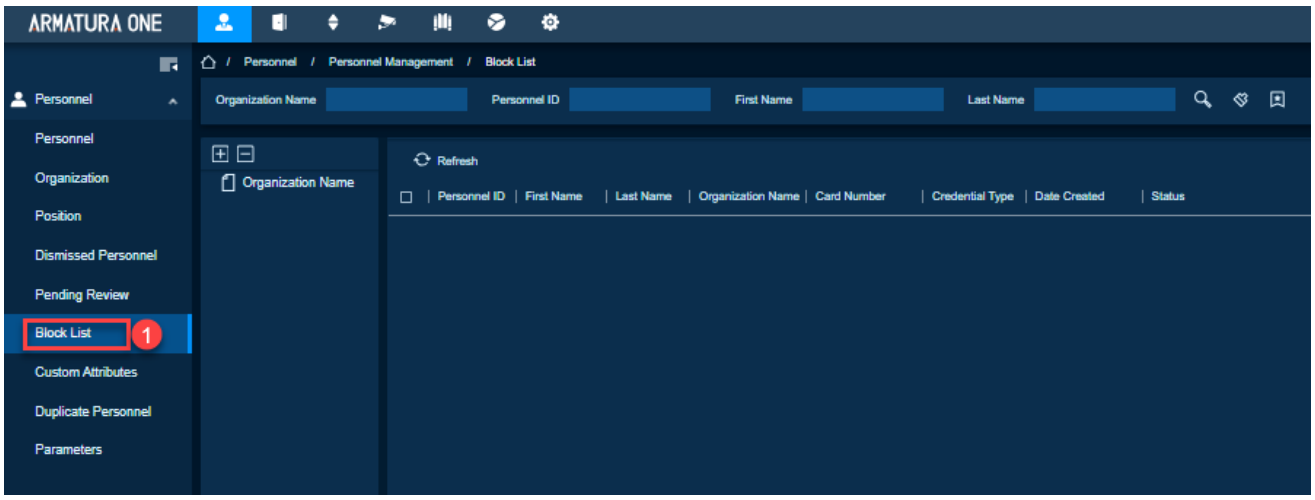
Operation	Description
In the Staff Editing section check the Block List.	Add a person to the Block List, which automatic blocks all their access rights.

Viewing the Block List

- Navigate to **[Personnel]** > **[Personnel Management]** > **[Block List]**, the interface displays all personnel who have been added to the Block List.

Note: Ensure proper authorization and documentation before adding or removing individuals from the Block List.

Copyright © 2024 ARMATURA LLC. All rights reserved



5.1.7. Custom Attributes

The Custom Attributes module allows the customization and management of personal attributes to meet specific customer requirements. These attributes can be added, modified, or deleted based on project-specific needs. By default, some attributes are pre-initialized upon the first use of the system.

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Use this module to add special fields, such as Emergency Contact or other non-default personnel information, to meet specific project requirements.

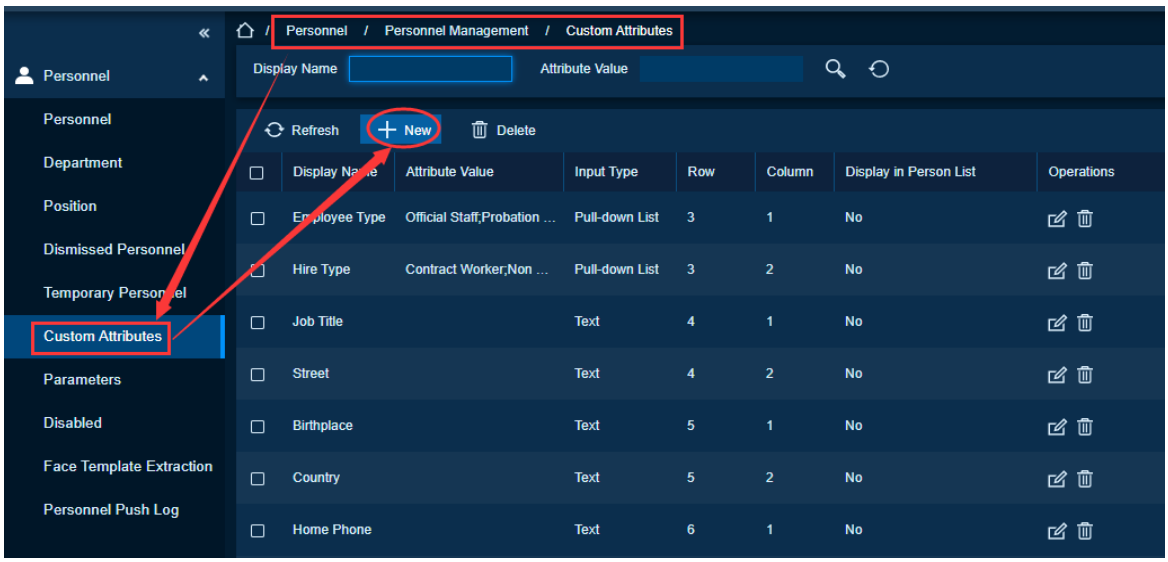
Trigger Result

Operation	Description
Display in the Personnel Li	If set to "Yes," the selected field will be display in the personnel list.

Steps to Create a New Custom Attribute:

- Navigate to **[Personnel]** > **[Personnel Management]** > **[Custom Attributes]** > **[New]**.

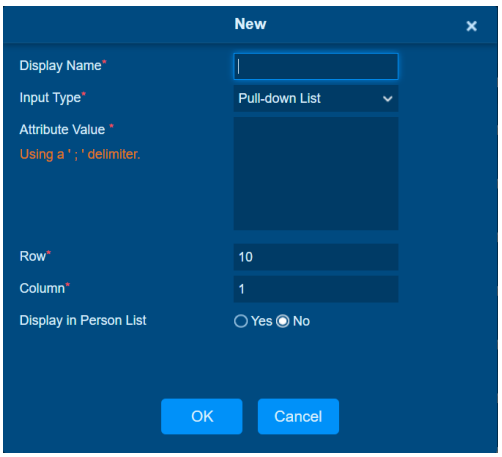
Copyright © 2024 ARMATURA LLC. All rights reserved



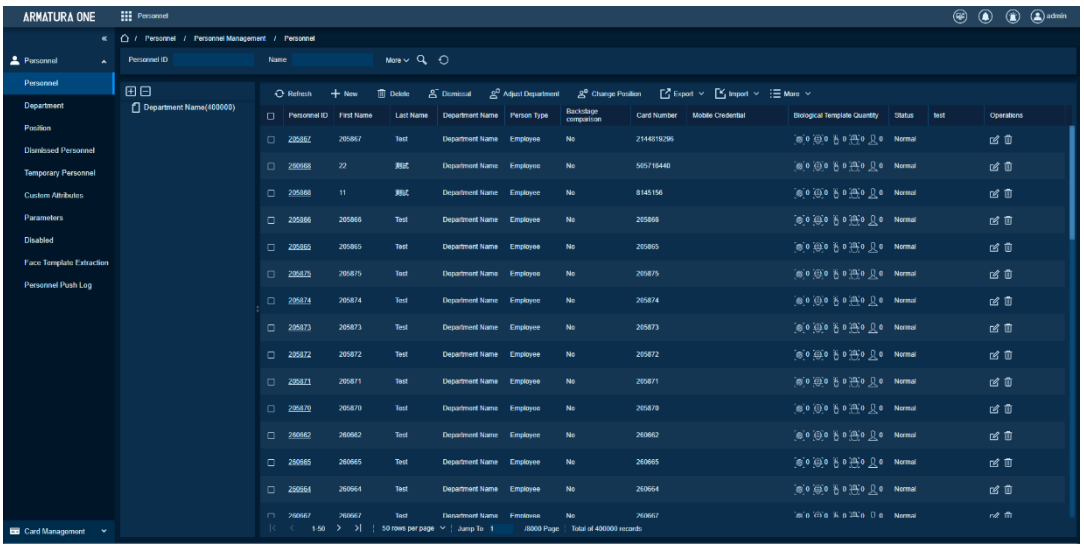
- On the New Custom Attribute interface, complete the following fields:

a) Display Name: Must be unique and no longer than 30 characters.
b) Input type: Choose from the following options:
   Drop-down List
   Multiple Choice
   Single Choice
   Text
c) Attribute Value: Relevant for input types like Drop-down List, Multiple Choice, or Single Choice. Separate multiple values using a semicolon (;). For Text, this field is not applicable.
d) Row/Column: These determine the display position of the attribute on the interface. Values must be numeric:
   Column: Up to 99.
   Row: Either 1 or 2.
   Ensure that the combination of column and row is unique.
e) Display in Personnel List: Set to "Yes" if the attribute should appear in the personnel list.

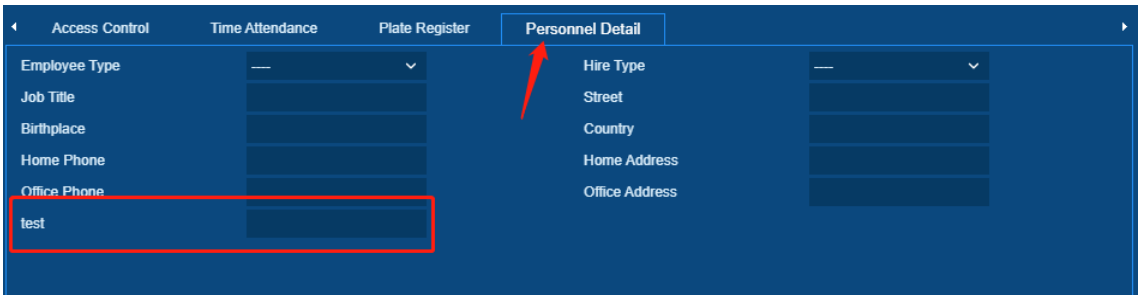
- Click **[OK]** to save the custom attribute and exit.



Copyright © 2024 ARMATURA LLC. All rights reserved

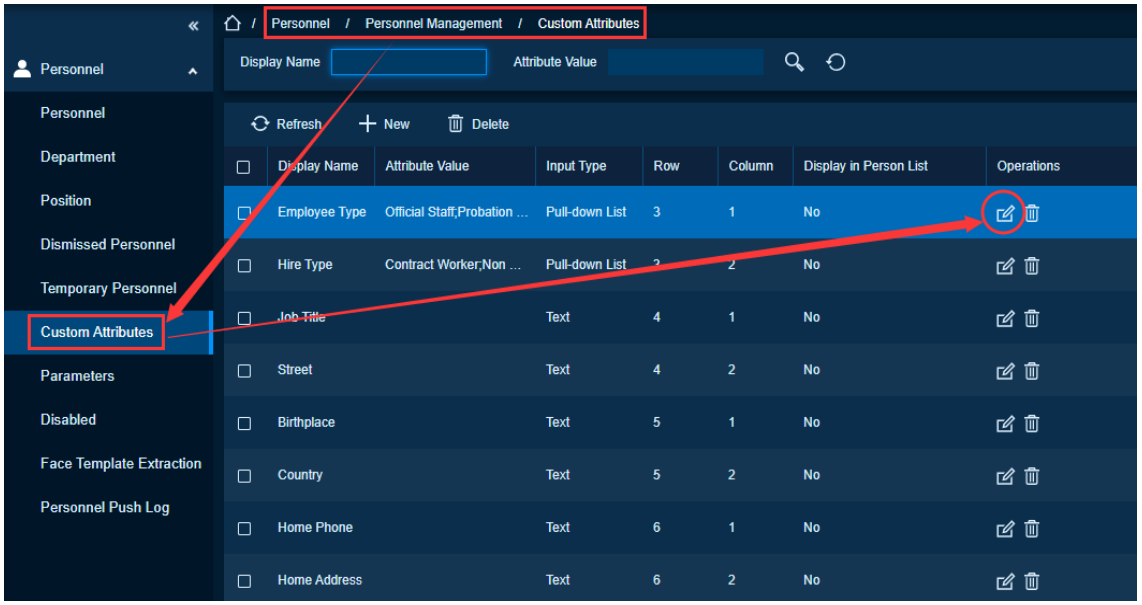


As shown in the following figure, "**Employee Type**" is displayed in the first column and first row, while "**Hire Type**" is in the same column but in the second row.



Edit a Custom Attribute

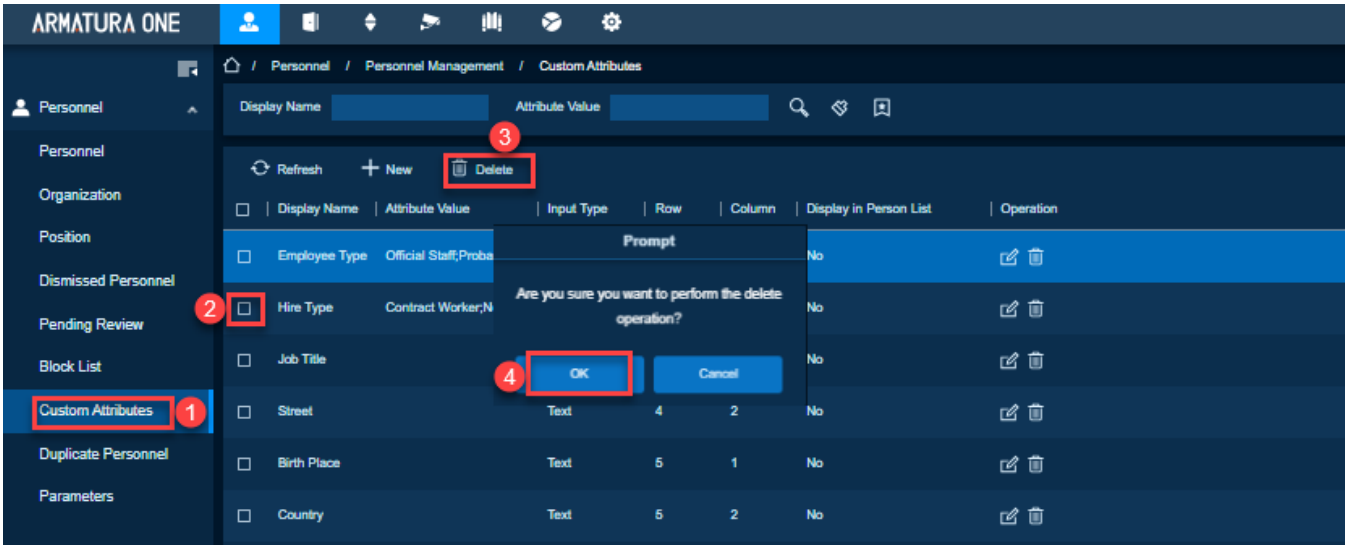
Click **[Edit]** to modify the corresponding attributes.



Copyright © 2024 ARMATURA LLC. All rights reserved

Delete a Custom Attribute

Click **[Delete]** to remove an unused attribute. If the attribute is currently in use, the system will display a confirmation prompt. Review the details and confirm the deletion.



Note:

Once a custom attribute is deleted, it cannot be recovered. Ensure that the attribute is no longer required before proceeding with the deletion.

5.1.8. Parameters

The Parameters module allows operators to configure preferences and settings related to personnel management, including Personnel ID, card settings, and additional operational parameters.

Prerequisites for Use

Log into the system using an account with the required permissions. Access to the document identification and card issuing features requires a valid software license.

Usage Scenario

Configure personnel management preferences, such as Personnel Number, Card Number, and Certificate Identification, to align with operational needs and usage habits.

Trigger Result

Personnel ID Setting

Operation	Description
Maximum ID Length	Set the maximum length for a Personnel ID.
Support Alphanumeric characters	Select **Yes** to allow alphanumeric Personnel IDs.
Auto Increment ID Nur	Automatically increments Personnel IDs by 1 for entries. Cannot be enabled if letters are supported.

Copyright © 2024 ARMATURA LLC. All rights reserved

Override duplicate ID number when enrolling devices	Select **Yes** to override duplicate ID numbers during enrollment, or **No** to retain existing IDs.

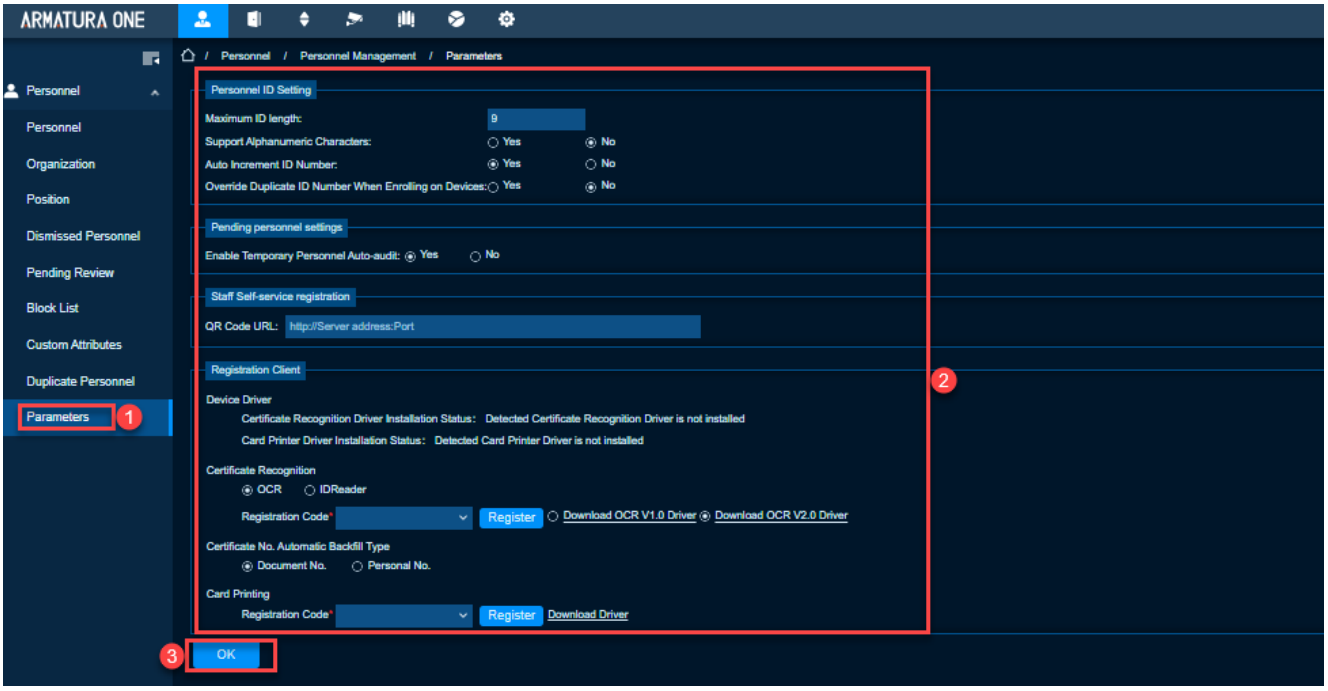
Card Setting

Operation	Description
Multiple Cards per per	Enable to allow personnel to have up to 16 cards assigned.

Steps:

Personnel ID Settings:

- Click **[Personnel]** > **[Personnel Management]** > **[Parameters]**.



- Configure the following options:
  a. Set the maximum length for the Personnel ID.
  b. Enable Support Alphanumeric Characters if desired.
  c. Enable Auto Increment ID Number to automate the assignment of IDs.

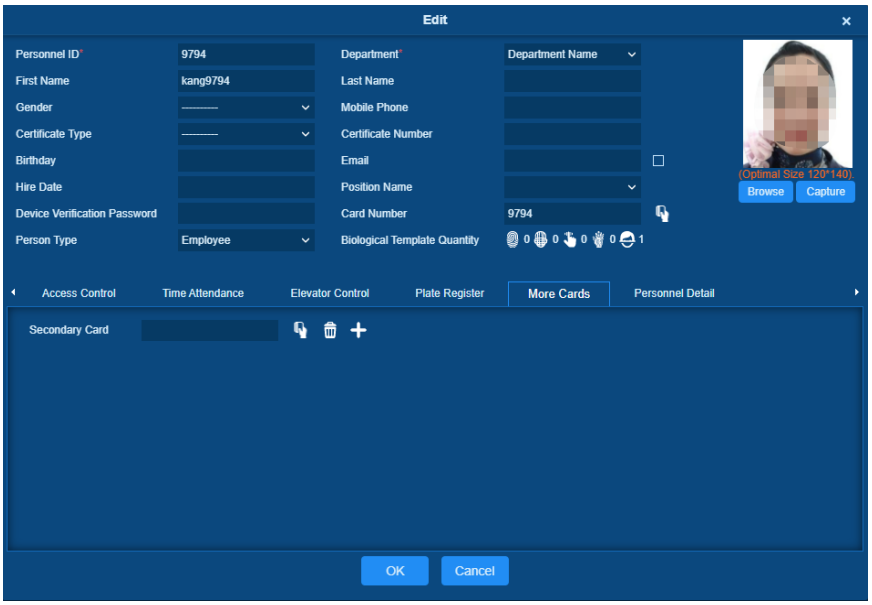
Copyright © 2024 ARMATURA LLC. All rights reserved

Card Settings

Set whether multiple cards are allowed for a single person by enabling “**Multiple Cards per Person**”.

More Cards

Enable the "**Multiple Cards per Person**" function, you can set multiple cards on the personal info page.



Note: Not all devices support this function. Consult with your sales representative for compatibility.

Copyright © 2024 ARMATURA LLC. All rights reserved

Additional Settings

Temporary Staff Setting: Configure whether temporary personnel registered via QR code require manual review.

Synchronize VCM Settings: Define the concurrency of push operations for personnel synchronization.

Set Face Cropping: Enable the Face Cropping function to enhance clarity by removing non-facial image areas for accurate access verification.

Self-Service Registration: Use a QR code for personnel to self-register and update their information.

Registration Client: Use this function for service registration, such as OCR document recognition.

If the required driver is not installed, click the **[Download Driver]** link to download and install it**.**

Select the corresponding Registration Code and click **[Register].**

Save the configuration by clicking **[OK]**.

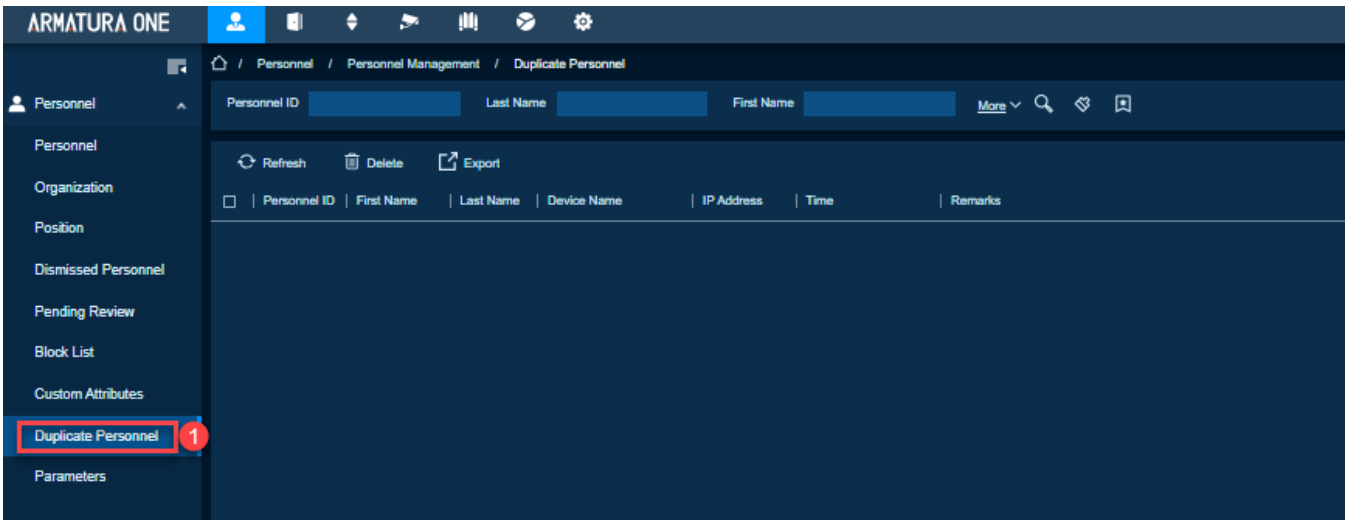
Note:

The registration code can be viewed under **[System] > [Authority Management] > [Client Register].**

5.1.9. Duplicate Personnel

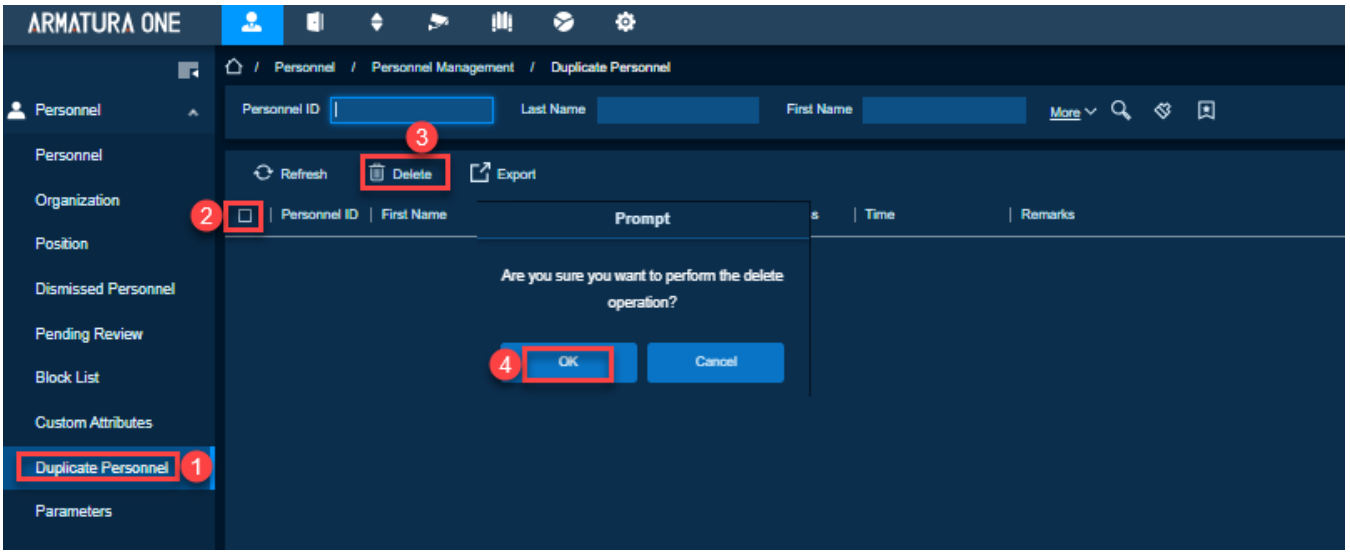
The Duplicate Personnel module allows users to manage instances of duplicated Personnel IDs within the system. This feature ensures that duplicate records are tracked and managed appropriately, with results stored in the personnel database.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Duplicate Personnel

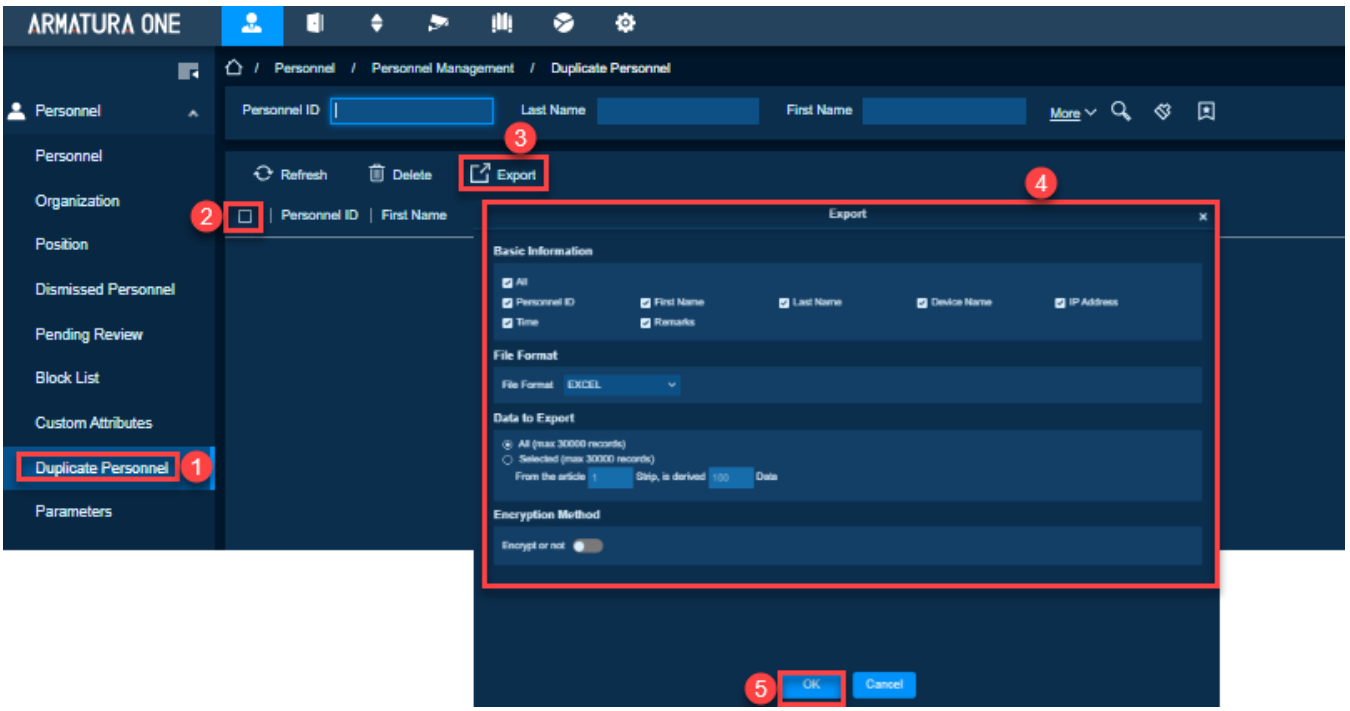
- Navigate to **[Personnel]** > **[Personnel Management]** > **[Duplicate Personnel]** > **[Delete]**
- Select the duplicate record(s) you with to delete.
- Click **[Delete]** and confirm the deletion.



Export Duplicate Personnel

- Navigate to **[Personnel]** > **[Personnel Management]** > **[Duplicate Personnel]** > **[Export]**
- Select the desired file format (PDF, Excel or CSV) and click **[OK]** to export the data.

Copyright © 2024 ARMATURA LLC. All rights reserved



5.2. Card Management

Card Management is a critical module that facilitates the management of issued cards, their statuses, and Wiegand formats to meet high-security requirements. Users can perform actions such as issuing, revoking, or reactivating cards, as well as viewing historical card operations and configuring card-related parameters.

There are three functions in Card Management: **Card, Wiegand Format, and Issue Card Record.**

5.2.1. Card Management

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Manage card statuses, including reporting and reactivating lost cards.

Associate personnel information with issued cards.

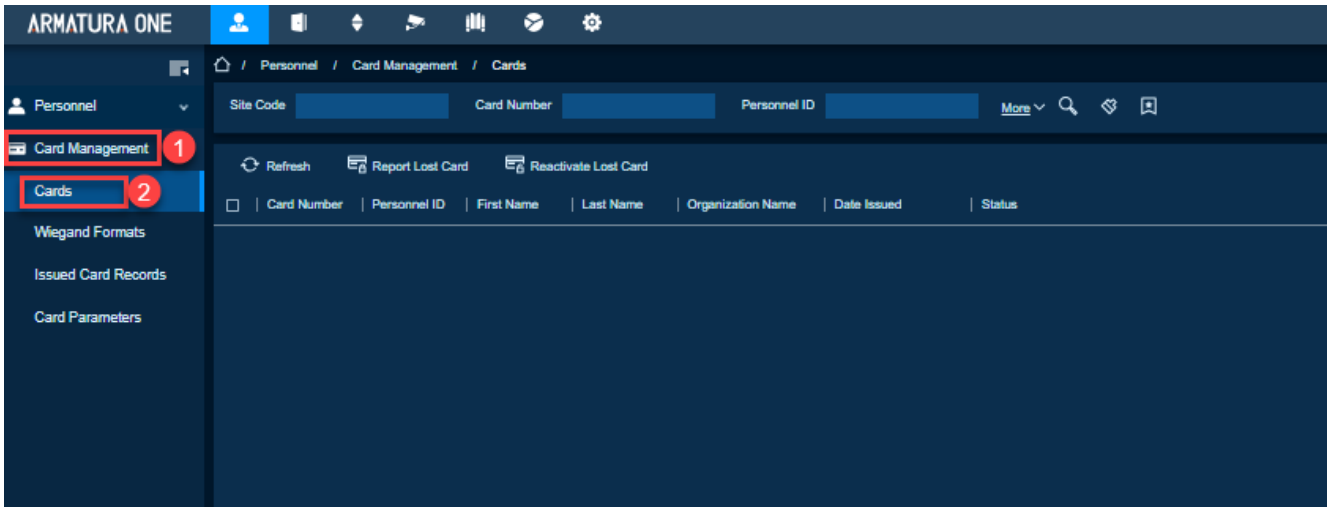
Trigger Result

Operation	Description
Check Card Number/Report Lost	When a card is reported as lost, it will lose th original access control authority.
Resolve Report	Once the lost report is resolved, the card number gains the original access control authority.

Copyright © 2024 ARMATURA LLC. All rights reserved

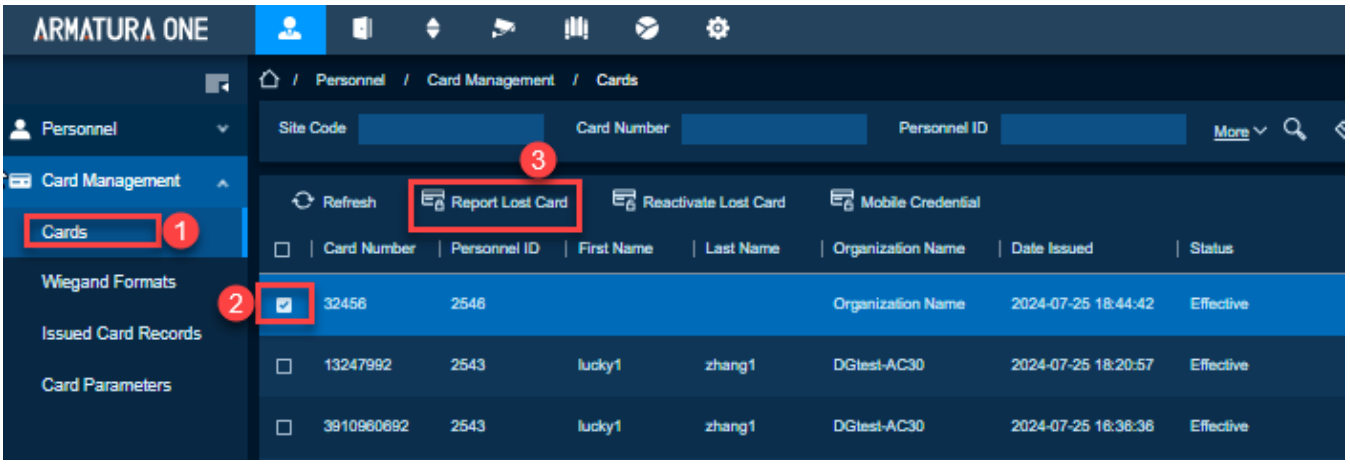
Steps:

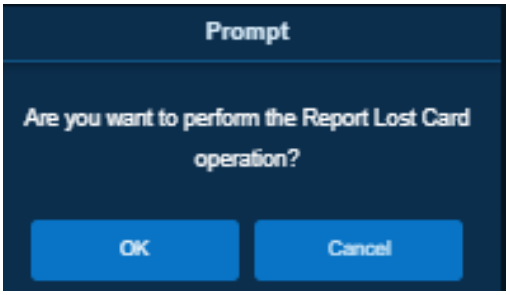
- Navigate to **[Personnel]** > **[Card Management]** > **[Card]** to view issued cards and their statuses.



Report Lost Card

- Go to **[Card Management]** > **[Card]**.
- Select the Card Number and click **[Report Card as Lost]**.



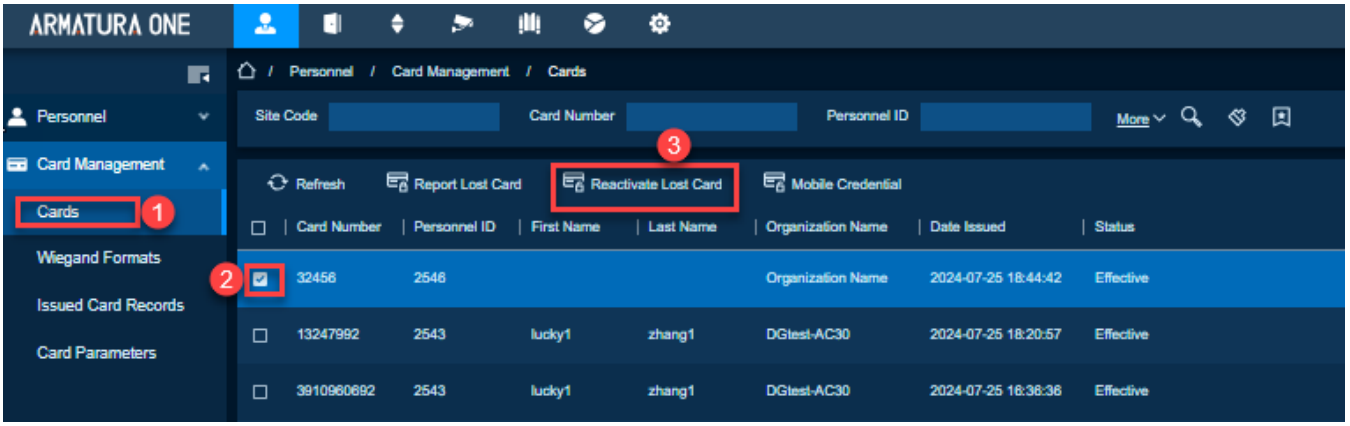


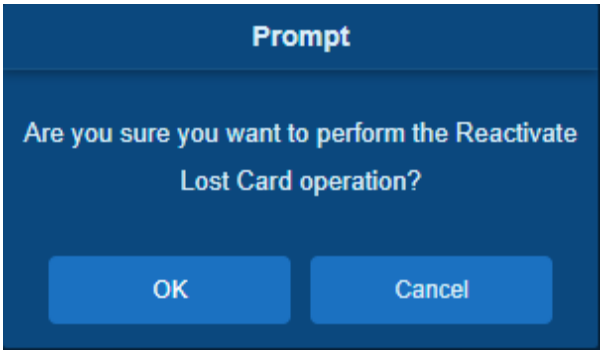
Copyright © 2024 ARMATURA LLC. All rights reserved

- Confirm the action by clicking **[OK]** and the card's permission will be revoked.

Reactivate Lost Card

- Go to **[Card Management]** > **[Card]**.
- Select the card number and click Reactivate Lost Card.





- Confirm the action by clicking **[OK]** and the card's permission will be restored.

5.2.2. Wiegand Formats

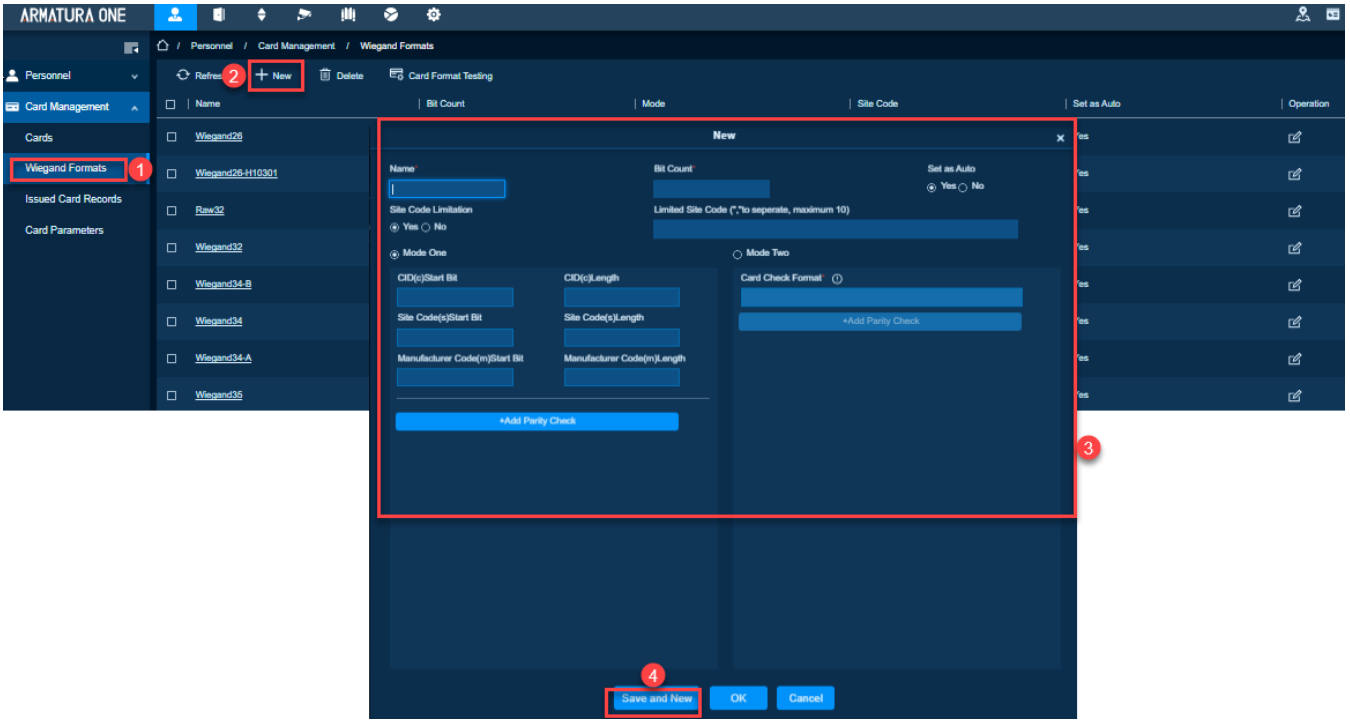
The Wiegand Format determines how card data is read by Wiegand-compatible devices. This module allows users to configure and auto detect Wiegand formats.

Steps:

Copyright © 2024 ARMATURA LLC. All rights reserved

Adding Wiegand Formats

- Navigate to **[Card management]** > **[Wiegand Formats]** > **[new]**.
- Enter the required format details in the provided fields.
- Enter format details and click **[OK]** to save.



Copyright © 2024 ARMATURA LLC. All rights reserved

Format Explanation

The Wiegand format is defined using the following symbols:

- **p**: Parity Position
- **s**: Site Code
- **c**: Cardholder ID
- **m**: Manufacturer Code
- **e**: Even Parity Check
- **o**: Odd Parity Check
- **b**: Both Odd and Even Parity Check
- **x**: Ignored Bits

Note:

Card Check Format can only include the symbols: “p, x, m, c, s”.
Parity Check Format can only include the symbols: “x, b, o, e”.

Copyright © 2024 ARMATURA LLC. All rights reserved

Example: 26-Bit Format Wiegand26a

A **Wiegand26a 26-bit format** consists of:

- **1 parity bit (even)** at the start
- **8-bit Site Code**
- **16-bit Card Number**
- **1 parity bit (odd)** at the end

Example Data:

- **Site Code**: 10101011 (binary for 171 in decimal)
- **Card Number**: 0011100101010110 (binary for 14646 in decimal)
- **Even Parity (e)**: 1 (Calculated from bits 2–13)
- **Odd Parity (o)**: 1 (Calculated from bits 14–25)

Final Bit Representation

1 10101011 00111001 01010110 1

Card Check Format Setting:

pssssssssccccccccccccccccp

eeeeeeeeeeeeeeoooooooooooooo

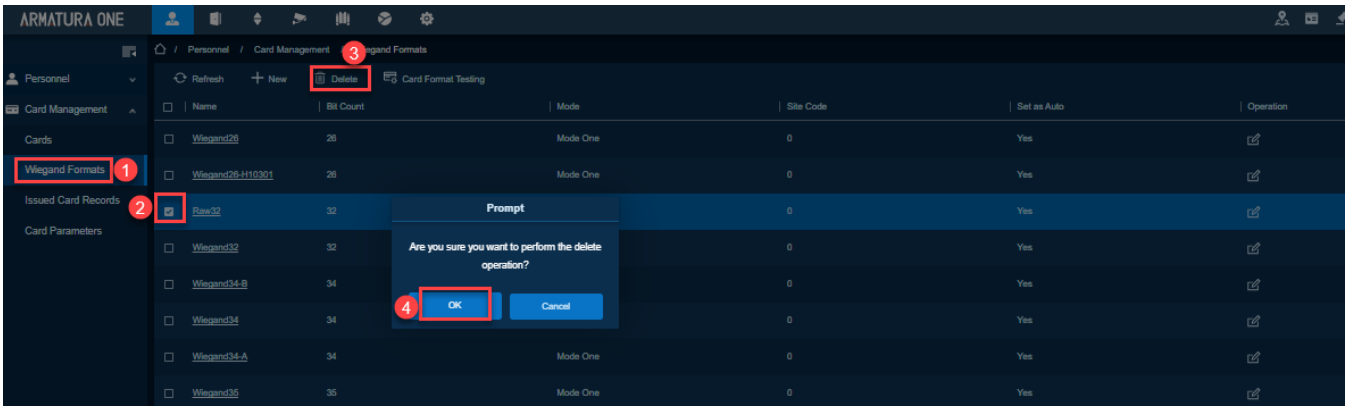
Explanation:

1. **Even Parity (e)**: The total number of 1s in bits 1–13 is counted. If even, the even parity check passed; otherwise, it fails.
    - For 1 10101011 0011, the number of 1s is **8** (even), so even parity check passed.
2. **Odd Parity (o)**: The total number of 1s in bits 14–26 is counted. If odd, the odd parity check passed; otherwise, it fails.
    - For 1001 01010110 1, the number of 1s is **7** (odd), so odd parity check passed.
3. **Site Code**: Calculated for bits 2–9. The binary sequence 10101011 represents 171 in decimal.
4. **Card Number**: Calculated for bits 10–25. The binary sequence 00111001 01010110 represents 14646 in decimal.

Copyright © 2024 ARMATURA LLC. All rights reserved

Deleting Wiegand Formats

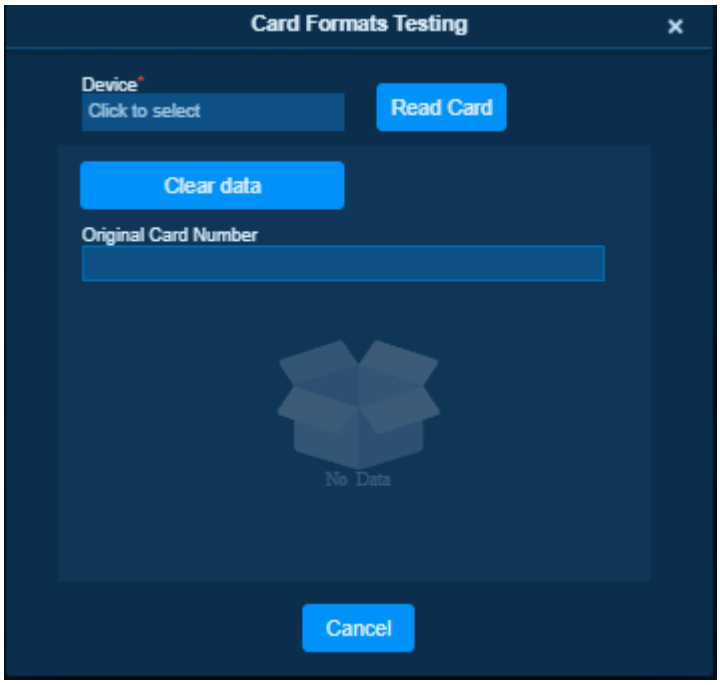
- Go to **[card management]** > **[Wiegand formats]**
- Select the format and click **[Delete]** to confirm the action.



Card Format Testing

Card Format Testing is a feature used to automatically detect the Wiegand format of a card. This process involves swiping the card at a reader and entering its known card number. The system will then automatically calculate the Wiegand format for the card that was just swiped.

This tool simplifies the process of identifying card formats, ensuring accuracy and reducing manual configuration errors.



Steps:

- Select a compatible device and input the card number and site code into the designated fields.
- Click **[Read Card]** and swipe the card on the reader.
- Click **[Recommended Card Format]** and the recommended Wiegand card format will be displayed on the screen.

Copyright © 2024 ARMATURA LLC. All rights reserved

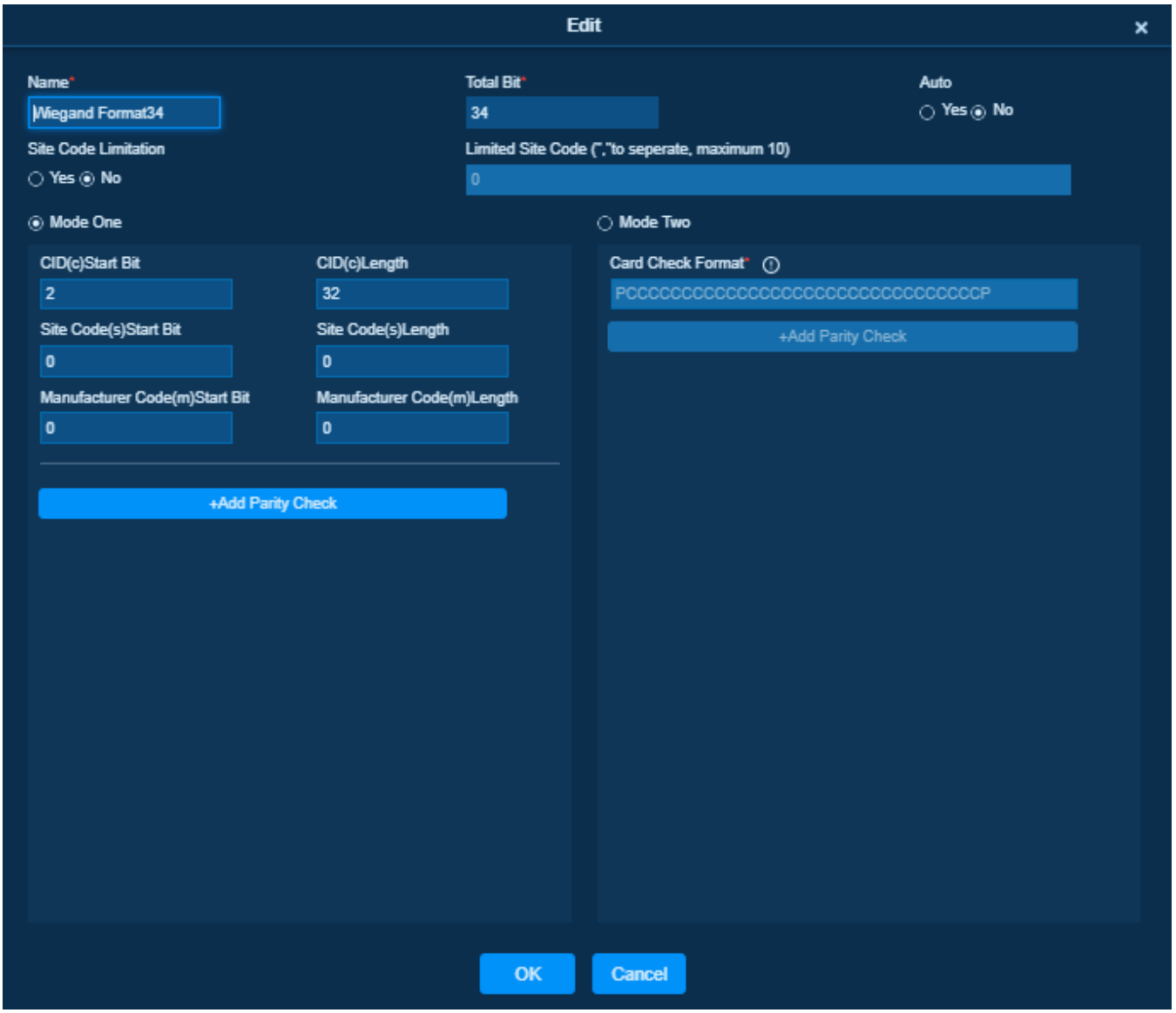
- Click **[Auto calculate site code while the site code is left bank]** and the software will calculate the site code according to the card format and card number.
- Click **[OK]** and the page will jump to the Wiegand format page to save the new Wiegand format.

Note:

The card format testing function is only supported by access control panels.

Edit Wiegand Formats

- Go to **[Personnel]** > **[Card Management]** > **[Wiegand Format]** select the name and click **[Edit]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

5.2.3. Issued Card Records

This function displays the history of issued cards, including all operations performed on each card, such as issuance, loss reporting, reactivation, and other changes.

Prerequisite for use

Log into the system using an account with the required permissions.

Usage Scenario

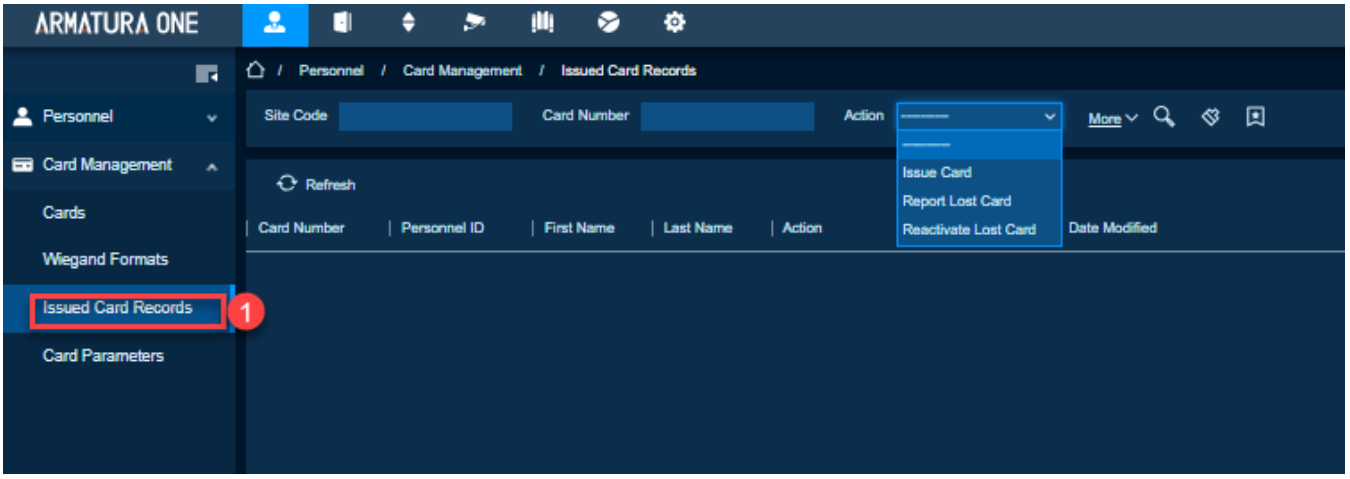
View historical data for card-related activities to ensure comprehensive tracking of all card operations.

Trigger Result

Operation	Description
Switch Operation Type	It displays records results of different operation types.

Steps:

- Navigate to **[Personnel]> [Card Management]> [Issued Card Records]**. Then use the drop-down menu to filter records by specific operation types, such as issuance or loss reporting.



Note:

If an employee's account is deleted, all associated card records will also be removed.

Copyright © 2024 ARMATURA LLC. All rights reserved

5.2.4. Card Parameters

This section allows users to configure and manage general card settings and parameters to align with organizational policies.

Prerequisite for use

Log into the system using an account with the required permissions.

Usage Scenarios

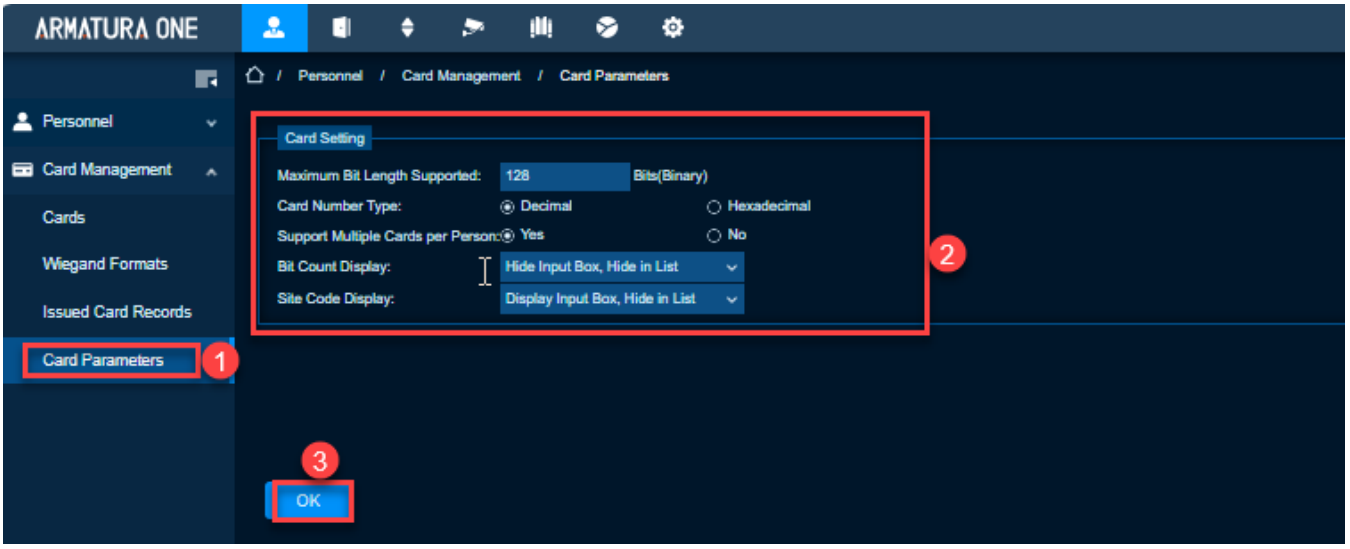
Adjust and review card-related settings to ensure compatibility with organizational access control requirements.

Trigger Result

Operation	Description
Card parameters	Configure and update card settings.

Steps:

- Navigate to **[Personnel]** > **[Card Management]** > **[Card parameters].**
- Modify the card parameters as per organizational requirements.
- Click **[OK]** to save the updated settings.



Copyright © 2024 ARMATURA LLC. All rights reserved

6. Access Control Management

Access Control Management is a critical component for enterprises to implement secure and efficient digital access solutions. To activate access control functions, the system must be connected to the relevant access control devices. Users are required to install and configure these devices to ensure proper functionality, including device management, data synchronization, and report generation.

6.1. Device

Function List

Functions	Operation Instructions
Device	Add, delete, edit, and search devices. Clear administrator credentials. Set login user passwords. Upgrade firmware. Restart devices. Synchronize time. Enable or disable devices. Synchronize all data. Reset device data. Configure background verification parameters. Set device time zones. Configure registration machines. Set daylight saving time. Modify fingerprint comparison thresholds. Adjust machine access status. Configure echo parameters. Set authentication server parameters. Configure access control parameters. Set date and time. Manage access control records. Adjust face recognition parameters. Configure temperature management settings. Set timing sleep durations. Configure temperature measurement parameters. Adjust extended parameters. Retrieve device parameters, personnel information, eve records, and logs. View medium access control rules. Download device logs. Query device capacity and information. View firmware details. Manage system time, data, and temperature settings. Modify IP addresses, communication passwords, and RS485 addresses. Switch network connections.
Door	Edit door configurations. Perform remote operations: open, close, enable, disabl cancel alarm, normally open, lock, unlock.

Copyright © 2024 ARMATURA LLC. All rights reserved

	Enable/disable the day's normally open time.
Reader	Edit reader settings. Bind/unbind cameras.
Daylight Saving Ti	Add, edit, delete, and set daylight saving time.
Auxiliary Input	Edit auxiliary input settings. Bind/unbind cameras.
Event Type	Edit and configure event types.
Auxiliary Output	Edit auxiliary outputs. Perform remote operations: open, close, normally open
I/O Expansion Boa	Add, edit, view, and delete I/O expansion boards.

6.1.1. Device Function

The Device module in Access Control Management provides comprehensive functionality for adding, configuring, and managing devices. Users can perform advanced operations such as parameter configuration, data synchronization, firmware upgrades, remote monitoring, and system control, ensuring seamless device management.

Adding a New Device

Prerequisites for Use

Log into the system using an account with the required permissions. Access Control devices valid within the software's designated publication region are required.

Usage Scenarios

This feature allows users to integrate devices into the software. Once a device is added, users can configure its parameters, update firmware for enhanced functionality, enroll personnel for access control, and manage access levels efficiently within the software.

Trigger Result

Once a device is added, its device is automatically synchronized with the software, including personnel records, access control configurations, and device settings.

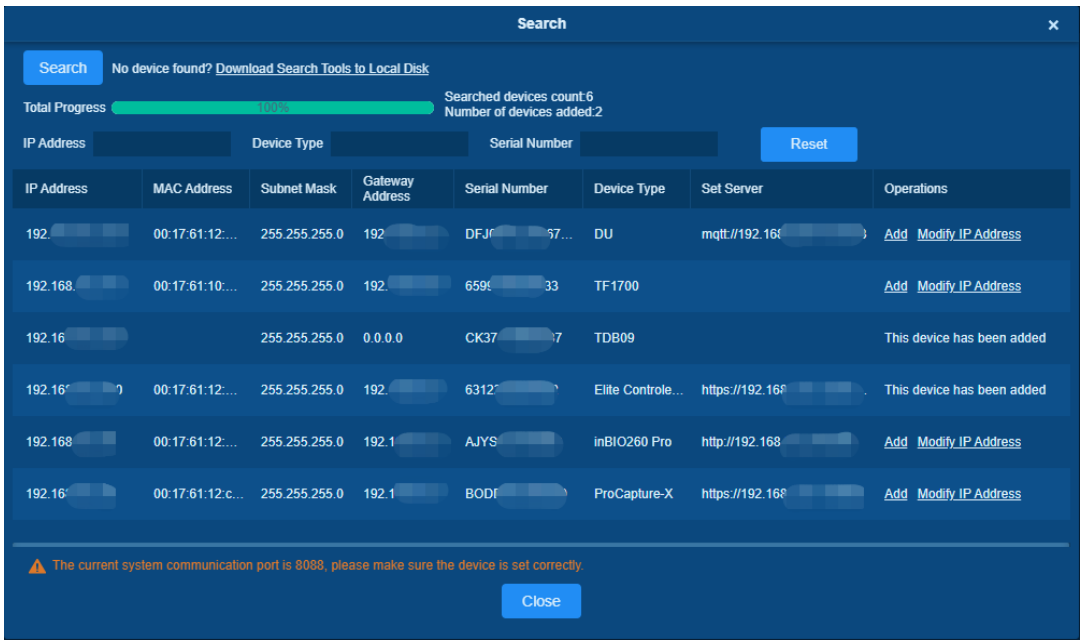
How to Add Access Devices

OmniAC Series Standalone Terminal

Search for access controllers within the Ethernet network:

- Navigate to **[Device] > [Device] > [Search Device]**.
- Click **Search**; the system will display a list of discovered access controllers.
- Select a device and click **Add**.

Copyright © 2024 ARMATURA LLC. All rights reserved



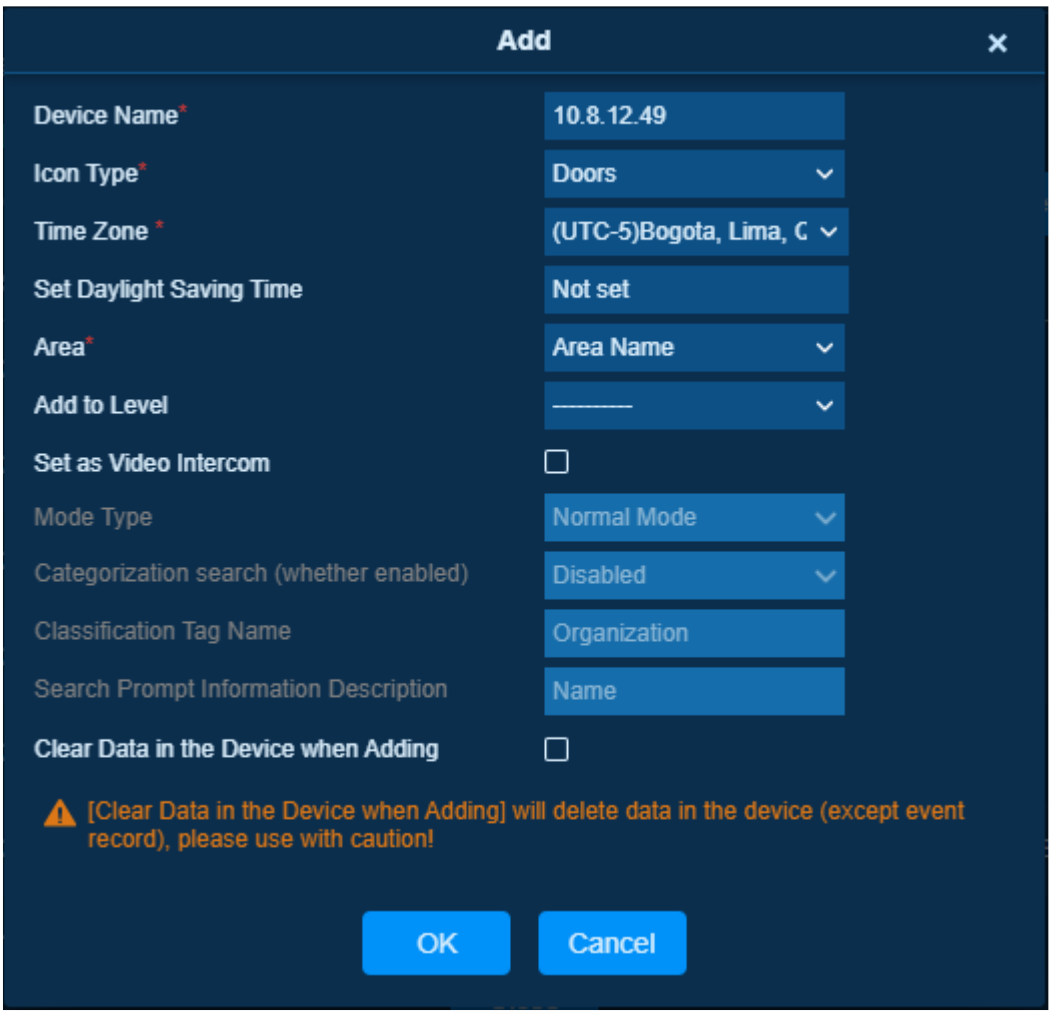
Note:

UDP broadcast mode will be used to search access device. This mode cannot perform Cross-Router function. IP address can provide cross-net segment, but it must be in the same subnet, and needs to be configured the gateway and IP address in the same net segment.

- Click on **[Add]** in the search list.

If the device is a pull device, user can enter a device name and click **[OK]** to complete device adding.

Copyright © 2024 ARMATURA LLC. All rights reserved



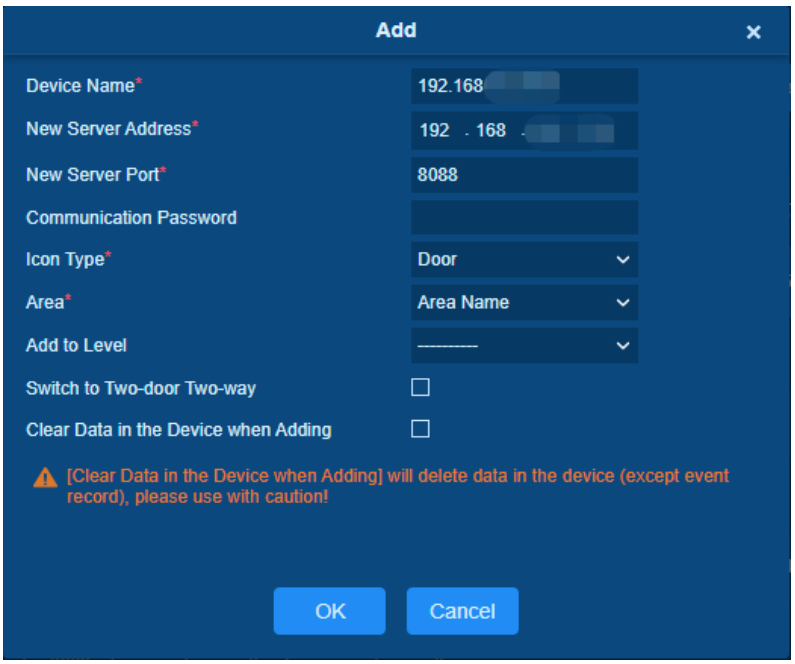
Clear Data on Adding

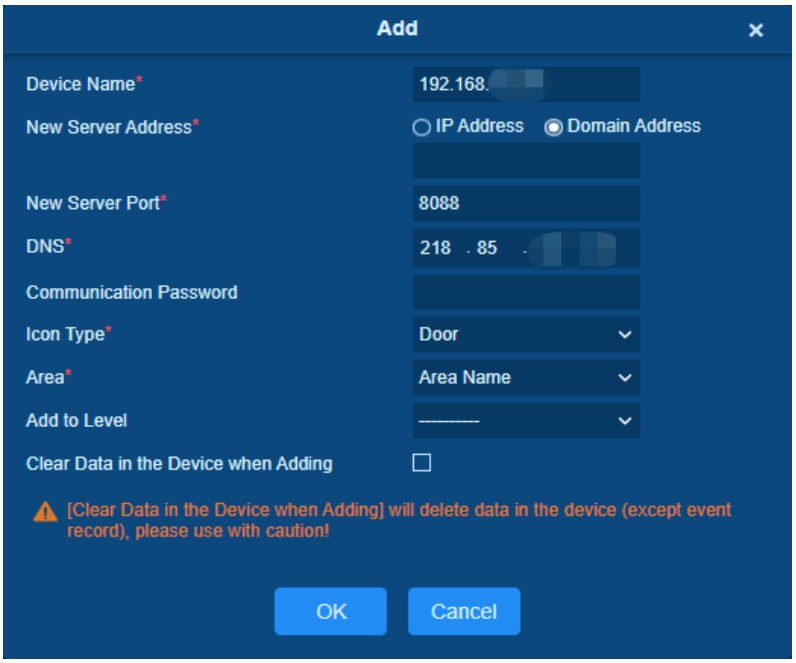
- Optionally, select Clear Data in Device when Adding to delete existing data (except logs) from the device.

Configuration Options

- New Server Address: Enter domain or IP address.
- New Server Port: Set the system's access port.
- DNS: Configure the DNS server address.

Copyright © 2024 ARMATURA LLC. All rights reserved





New Server Address: Devices can be added to the software by entering the domain address or IP address.

New Server Port: Set the access point of system.

DNS: Set the DNS address of the server.

Clear Data In The Device When Adding: If this option is selected, the system will clear all data on the device (except for the event logs) after adding it. If user are adding the device only for demonstration or testing purposes, there is no need to select this option.

Copyright © 2024 ARMATURA LLC. All rights reserved

Note:

- When using either of the above three device adding methods, if there exist residual data in the original device, please sync original data to it after adding a new device to the software by clicking **[Device]** > **[Synchronize All Data to Devices]**, otherwise these original data may conflict with normal usage.
- The default IP address of the access device may conflict with the IP of a device on the Local network.
- You can modify its IP address: click **[Modify IP Address]** beside the **[Add]** and a dialog box will pop up in the interface. Enter the new IP address and other parameters (Note: Configure the gateway and IP address in the same net segment).

Note:

Some OmniAC Series devices support SSL. To use this function, select the HTTPS port during software installation and ensure that the device firmware supports SSL.

Adding Horizon Series Controllers

Horizon Series Controllers include the following models:

- AHSC-1000: **Primary Controller**
- AHDU-1160, AHDU-1260, AHDU-1460: Distributed Controllers

Security Level

1. **Security Levels**

The system supports three levels of security for adding Horizon Series Controllers:

2. **Low Security Level**:
    - Uses MQTT without SSL authentication.
    - Relies solely on pre-shared keys and does not utilize certificates.
3. **Normal Security Level** (Default):
    - Utilizes MQTTs with one-way SSL authentication.
    - In this configuration:
        - The client connects to the server (broker), which provides its certificate to the client.
        - The client verifies the certificate is signed by a trusted Certificate Authority (CA), confirming the server's identity.
        - An encrypted tunnel is established for secure communication.
4. **High Security Level**:
    - Employs MQTTs with two-way SSL authentication (Mutual Authentication).
    - In addition to verifying the server's certificate, the client sends its unique certificate to the server.
    - The server validates the client's certificate against a trusted CA, using the CN field as the client’s user ID.

Copyright © 2024 ARMATURA LLC. All rights reserved

Note:

The system defaults to the **Normal Security Level**.

Low Security Level and **High Security Level** require adjustments to software settings. Contact technical support for assistance.

The information below is specific to the **Normal Security Level** setup.

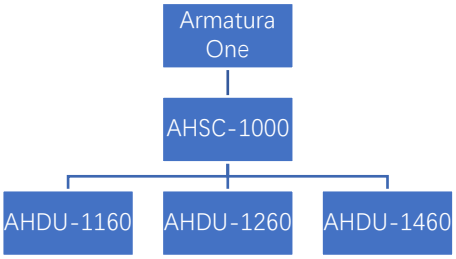
Device Models

- AHSC-1000: **Primary Controller**
- AHDU-1X60: Distributed Controller

Management Models

Horizon Series Controllers support **Master-Slave Mode** with two types of connections:

- TCP/IP
- RS-485.



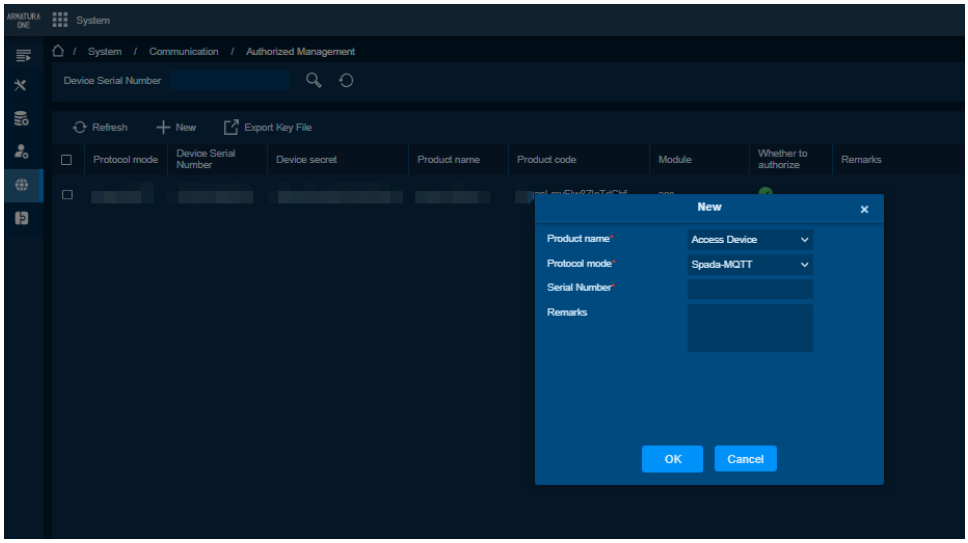
Connecting AHDU-1X60 to AHSC-1000 via TCP/IP

Step 1 Add the Primary Controller

1. Add a Device:

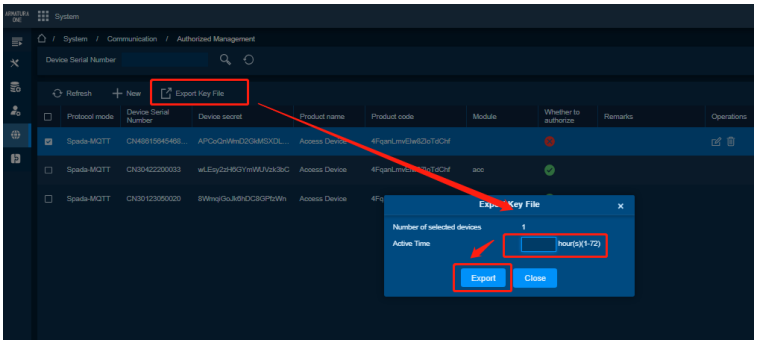
- Navigate to **[System]** > **[Communication]** > **[Authorized Management]**.
- Click New and input the product details, including the serial number.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export the Key File:

- Go to **[System]** > **[Communication]** > **[Authorized Management]**.
- Click Export Key File and set the key validity time (1-72 hours).
- Save the .zip file containing the controller certificates and server certificates.



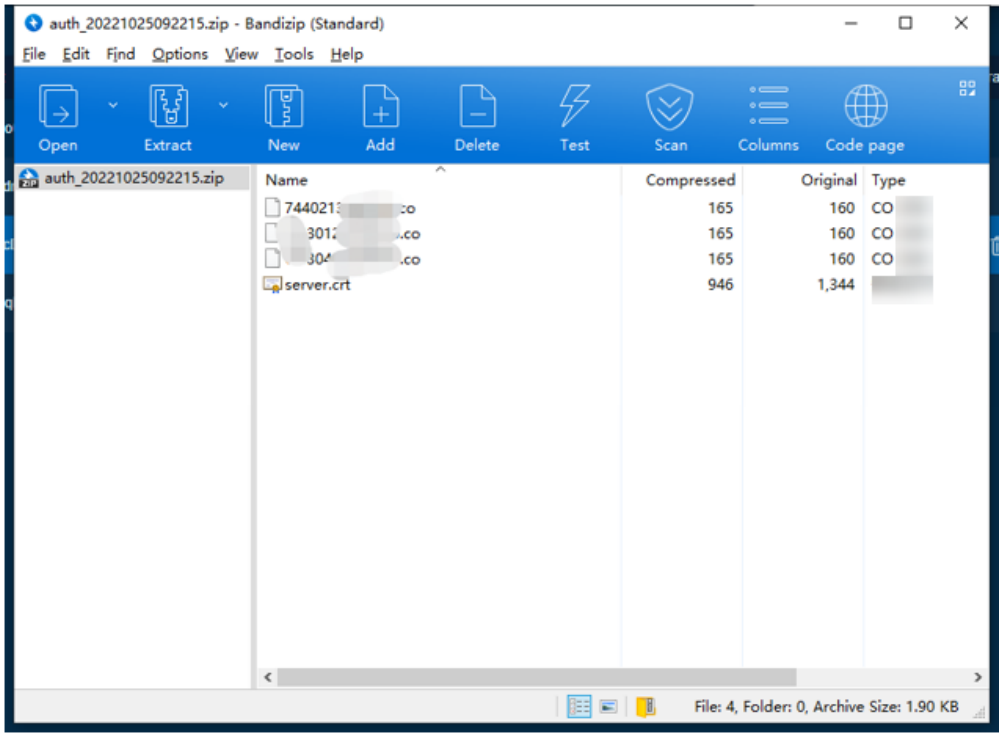
Active Time Key file validity, the value can range from 1-72 Hours.

After clicking Export Button, the browser will download a .zip file.

Note:

This function supports selecting multiple devices. By clicking the icon, it generates .co files for all controllers and a server certificate, packaged into a .zip file. Simply upload this .zip file to the controller's web server.

Copyright © 2024 ARMATURA LLC. All rights reserved



Import the Key File to the Controller.

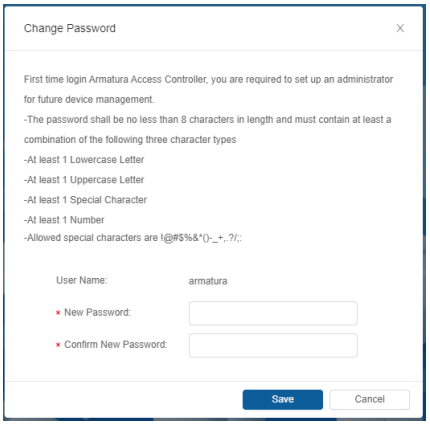
Open the controller's web interface via a browser: https://**[controller IP address]**.

Default login credentials:

- **Username**: armatura
- **Password**: armatura

Copyright © 2024 ARMATURA LLC. All rights reserved

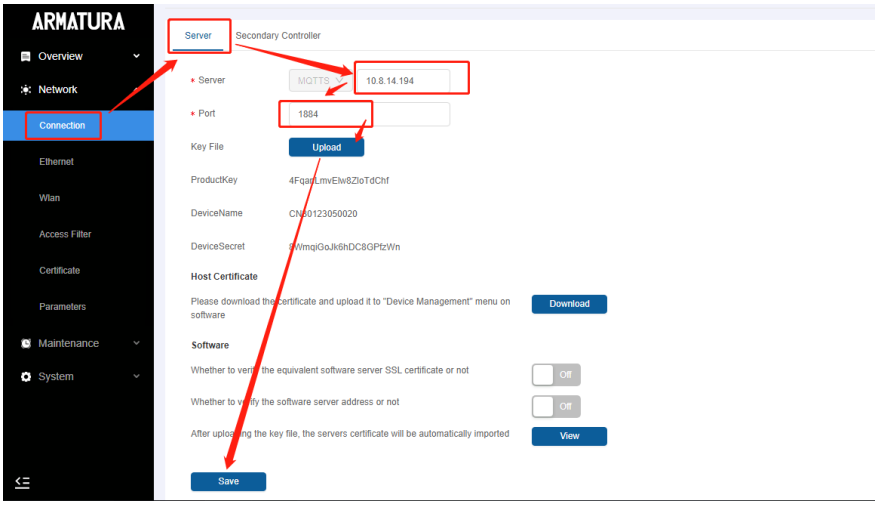
Upon the first login, the system prompts you to change the admin password.



Server Configuration

Navigate to the Server Settings

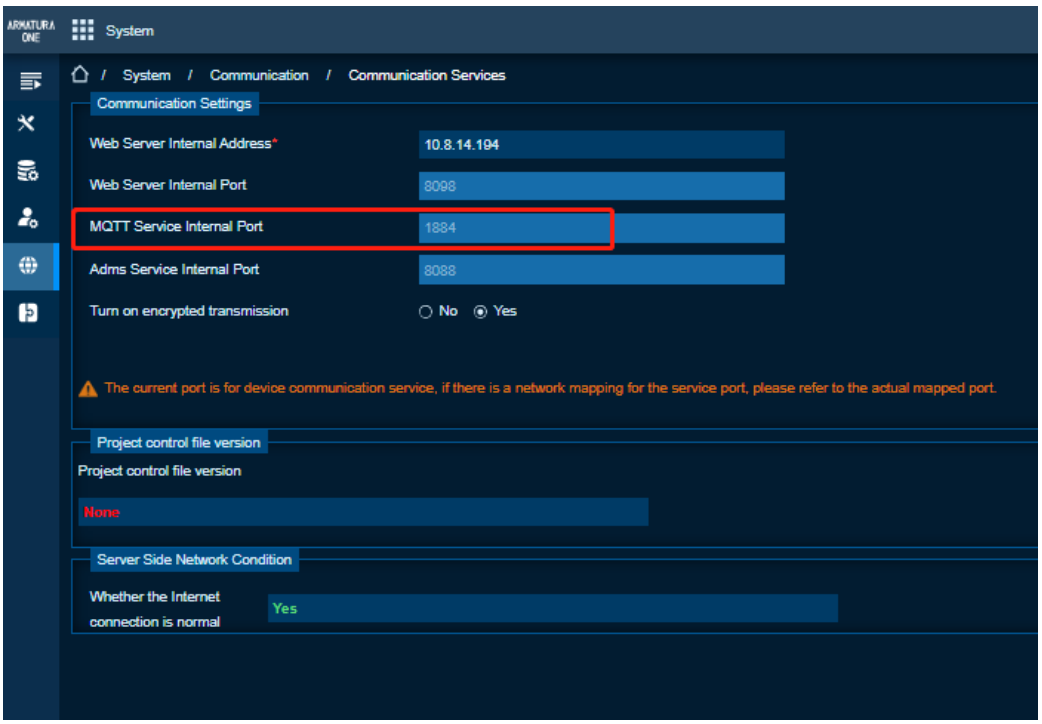
- Go to **[Network]** > **[Connection]** in the controller's web interface.
- Open the Server tab.



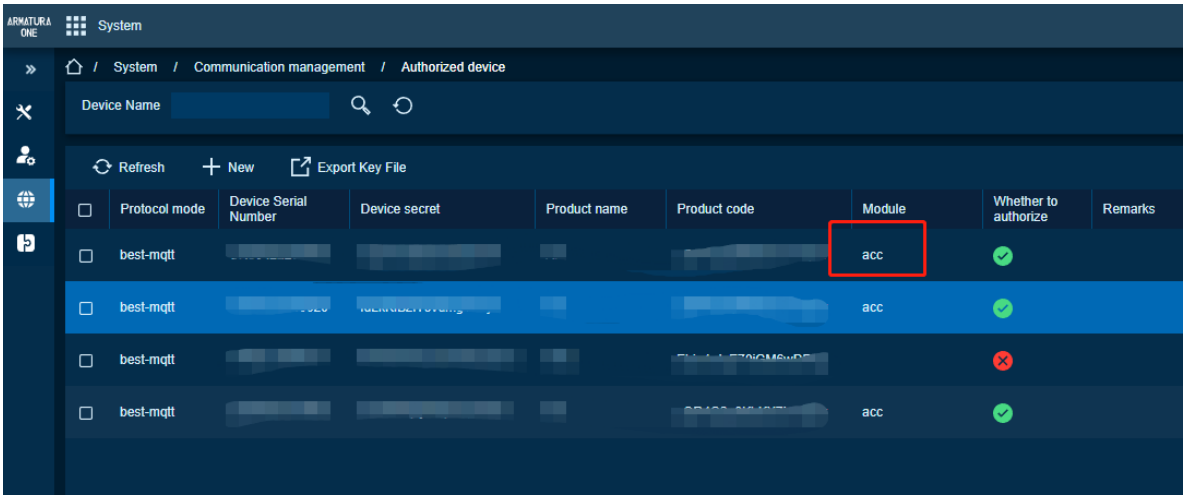
Set the Following Parameters:

- **Protocol**: Select **MQTTs**.
- **Server Address**: Enter the systems server address.

Copyright © 2024 ARMATURA LLC. All rights reserved



Key File: Upload the key file exported from **[System] > [Communication] > [Authorized Management]** in the software.



Verify MQTT Connection:

- After a successful connection, the Column **Module** will display **'acc'**.
- If the device has not yet been authorized in the Access Module, it will show .

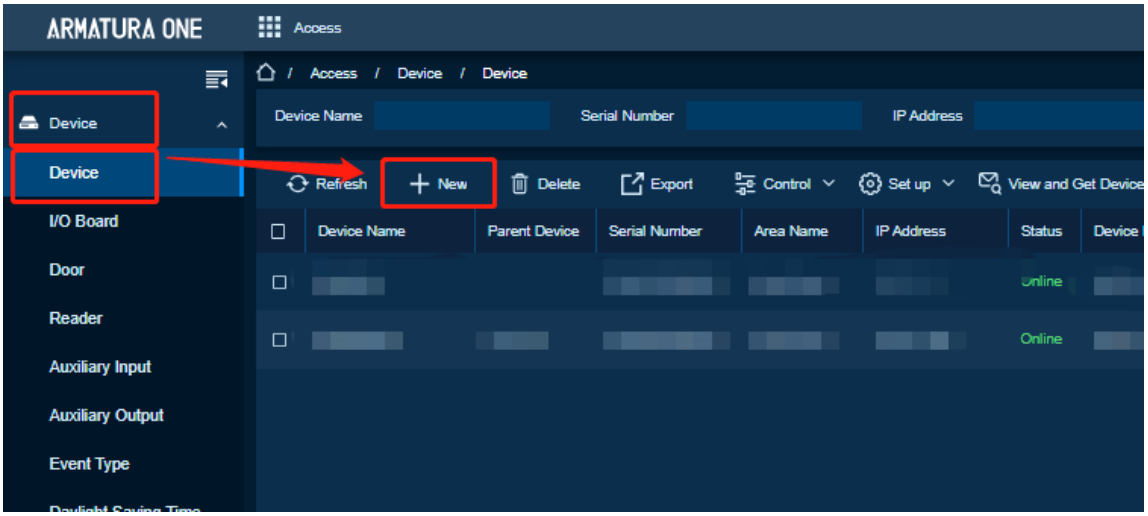
Adding the Controller in the Access Module

Open the Access Module

- Navigate to **[Access]** > **[Device]** > **[Device]** in the software.

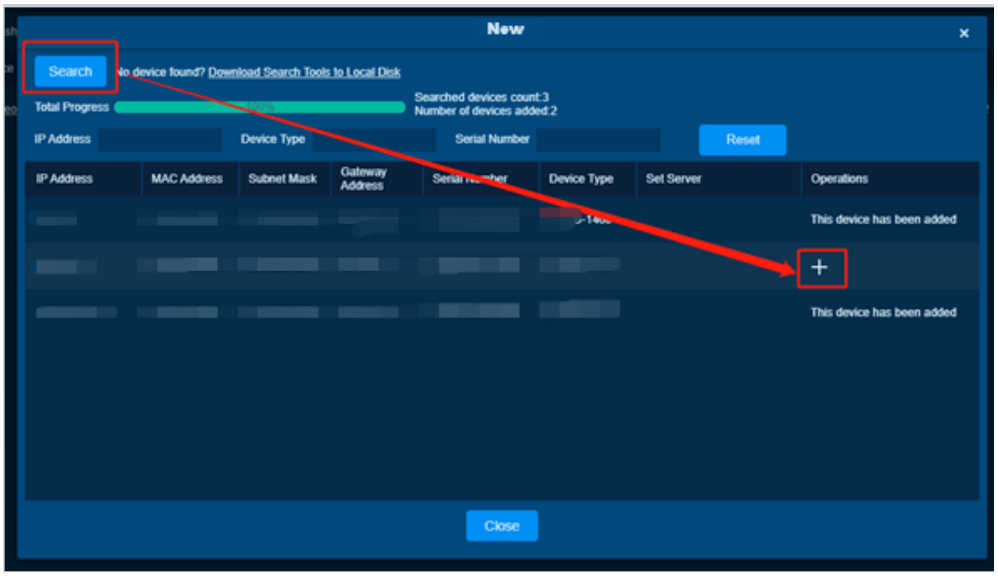
Copyright © 2024 ARMATURA LLC. All rights reserved

- Click the New button to add a device.



Search for the Device

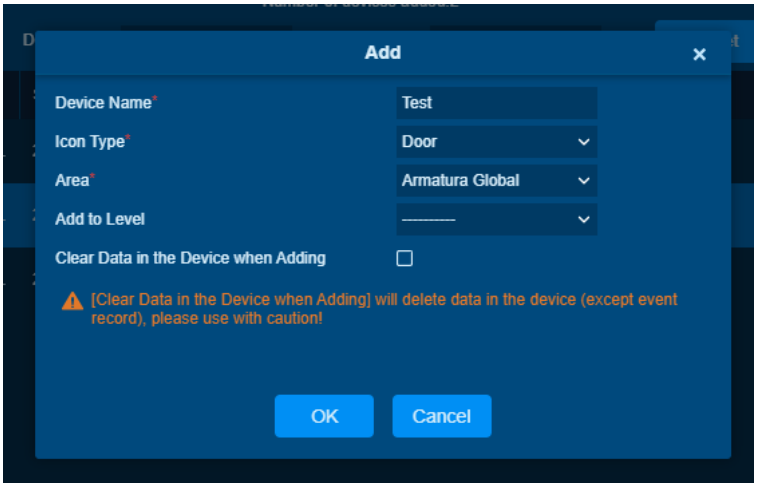
- In the **New Device** window, click the **Search** button.



Add the Device

- In the **Add Device** window, input the device details as prompted.
- **Recommended Option**: Select **[Clear Data in Device When Adding]** to erase any existing data on the device and ensure a clean integration with the software.

Copyright © 2024 ARMATURA LLC. All rights reserved



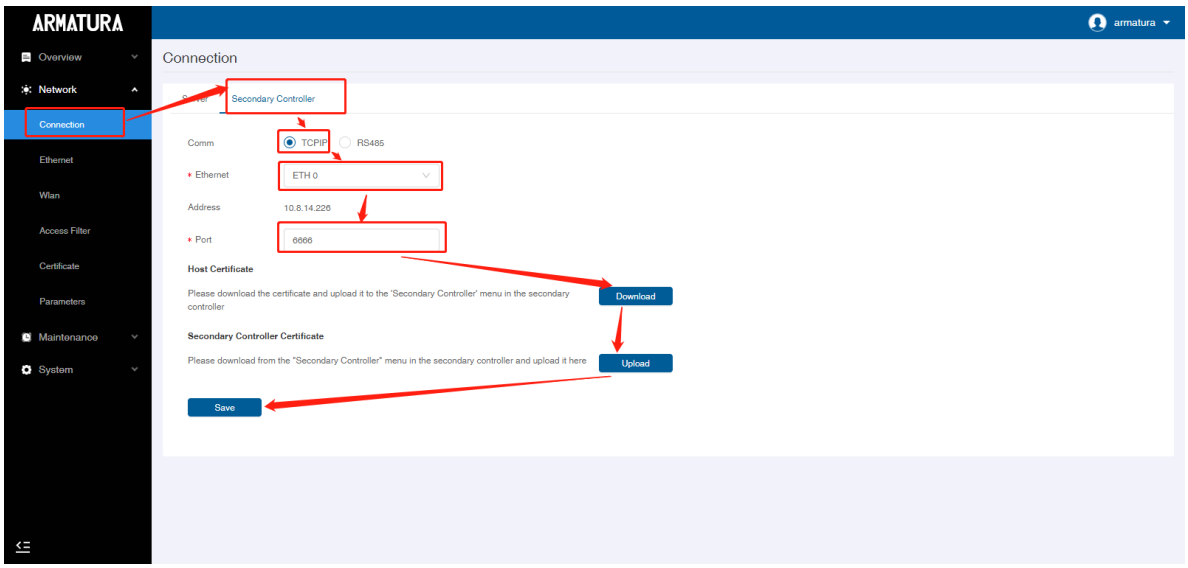
Note:

Clearing device data prevents conflicts with residual information and ensures seamless synchronization with the system.

Step 2: Configure the **Secondary Controller** Communication Port.

Access Communication Settings

- Navigate to **[Network]** > **[Connection]** in the controller's web interface.



Select Communication Type

- Choose the **TCPIP** radio button under **Comm**.

Configure Ethernet Settings

- Ethernet: Select either '**ETH 1**' or '**ETH 2**' based on the connection in use.
- Address: Confirm the displayed IP address to ensure accuracy.

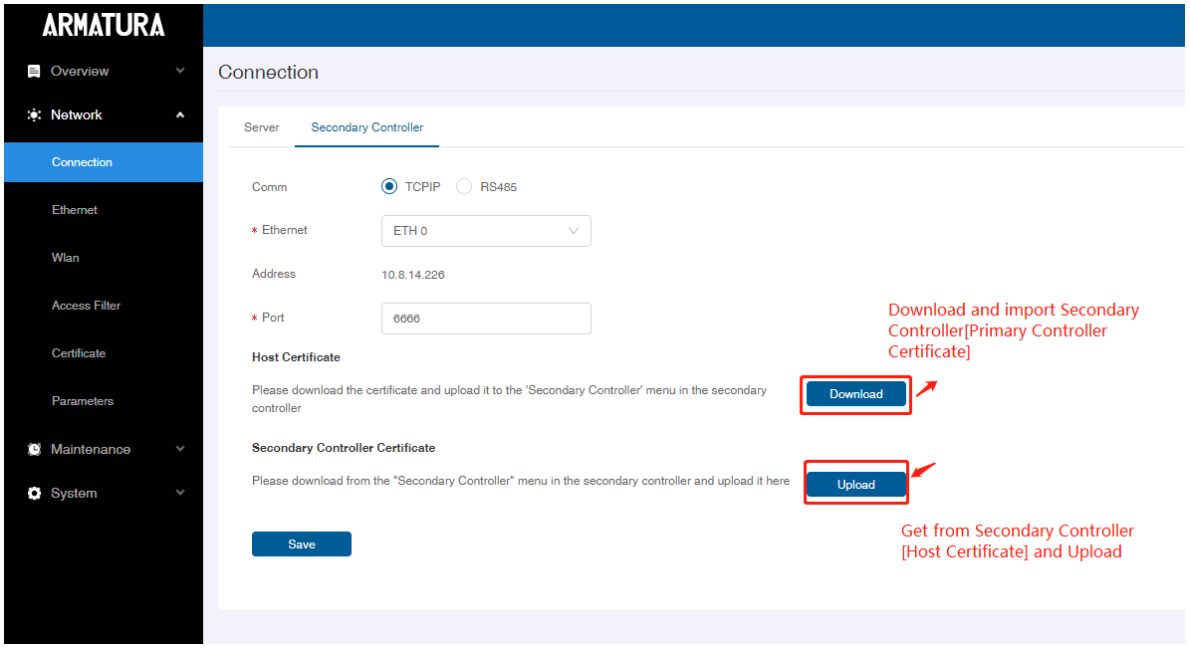
Copyright © 2024 ARMATURA LLC. All rights reserved

Set Port

- Specify the port for the **Secondary Controller** to connect using the WSS protocol.

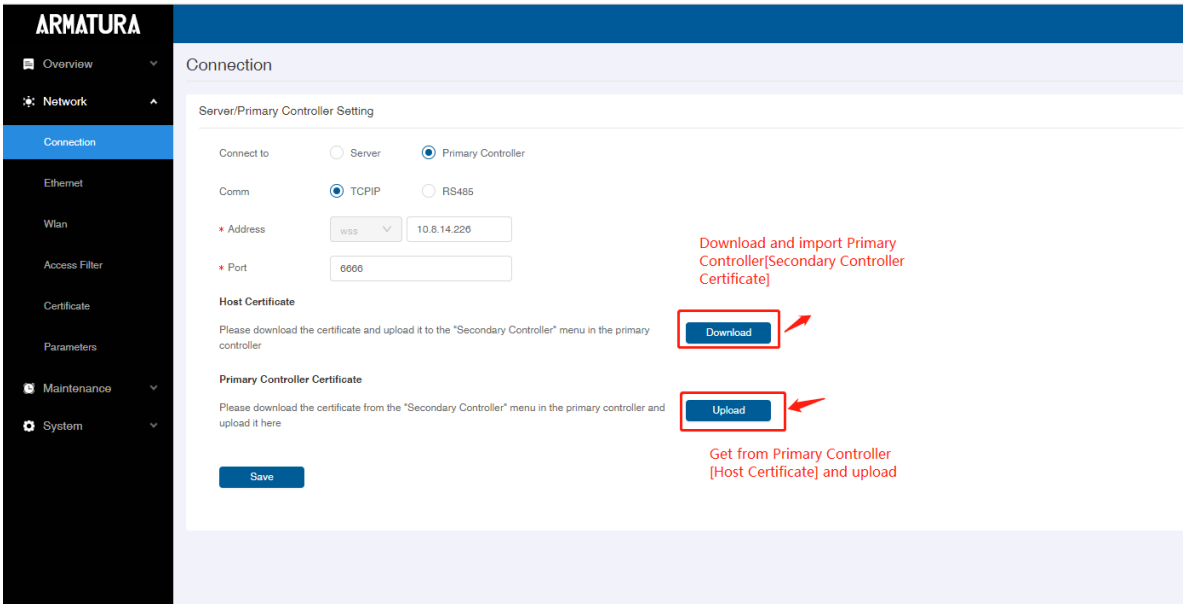
Primary Controller:

- Download the **[Host Certificate]** from the **Primary Controller**.
- Upload it to the **Secondary Controller** Page under **[Primary Controller Certificate].**

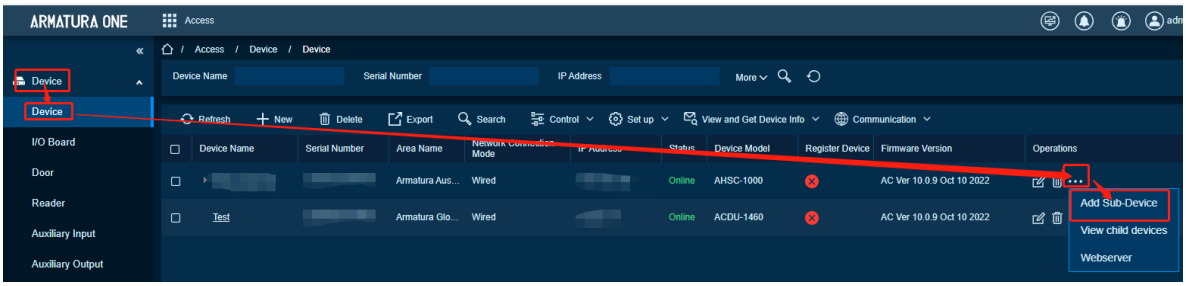


Secondary Controller:

- Download the **[Host Certificate]** from the **Secondary Controller**.
- Upload it to the **Primary Controller** Page under **[Secondary Controller Certificate]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

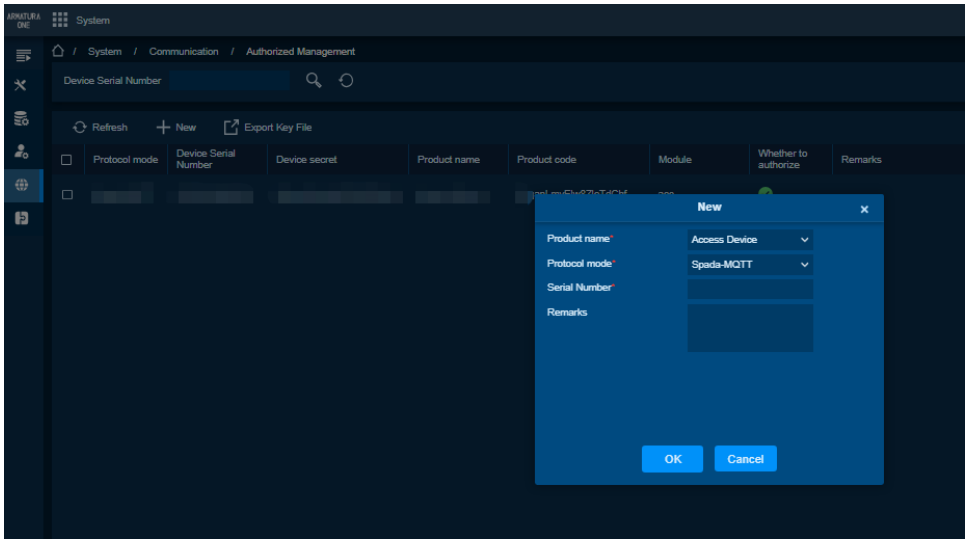


➢ Connect AHDU-1X60 to AHSC1000 via RS-485

Step 1 Add Primary Controller

- Add a device

Navigate to **[System] > [Communication] > [Authorized Management]** and click the **New** button.

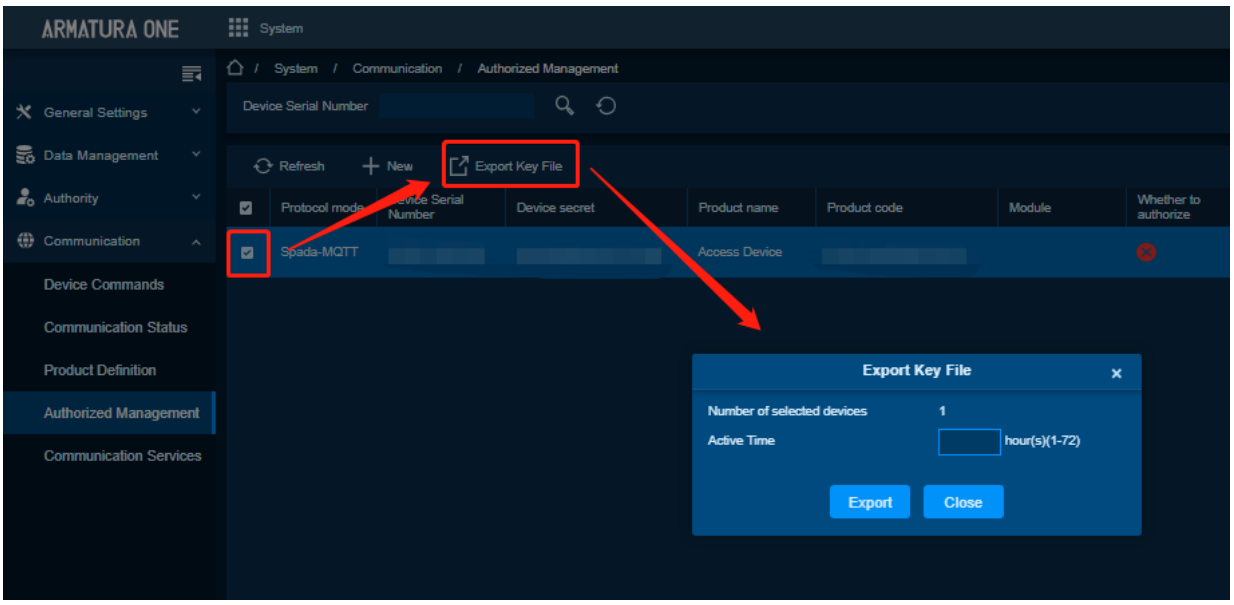


Select the **Product Name**, **Product Mode**, and enter the **Serial Number** of the controller.

- Export Key File

Go to **[System] > [Communication Management] > [Authorized Device]** and click the **Export Key File** button.

Copyright © 2024 ARMATURA LLC. All rights reserved

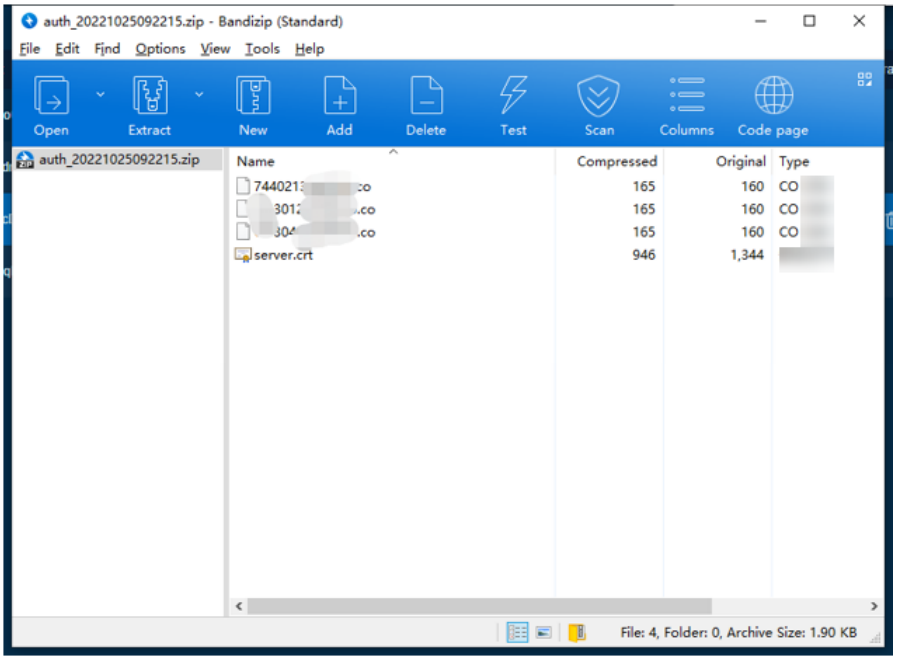


Set the Active Time for the Key File validity (1–72 hours).

Click the **Export** button to download a .zip file containing the .co file for each controller and the server certificate.

Note:

This function supports batch exporting for multiple devices. Ensure the .zip package is uploaded to the controller's web server.



- Import Key file to controller.

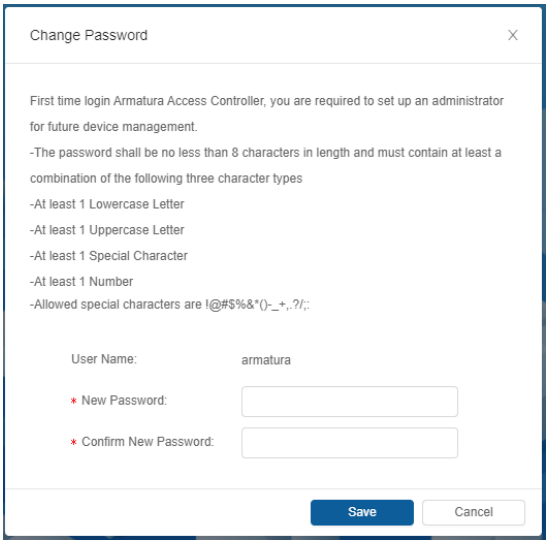
Open a browser and enter the controller's web interface URL: https://**[controller IP address]**.

Copyright © 2024 ARMATURA LLC. All rights reserved

Login credentials for the first-time login:

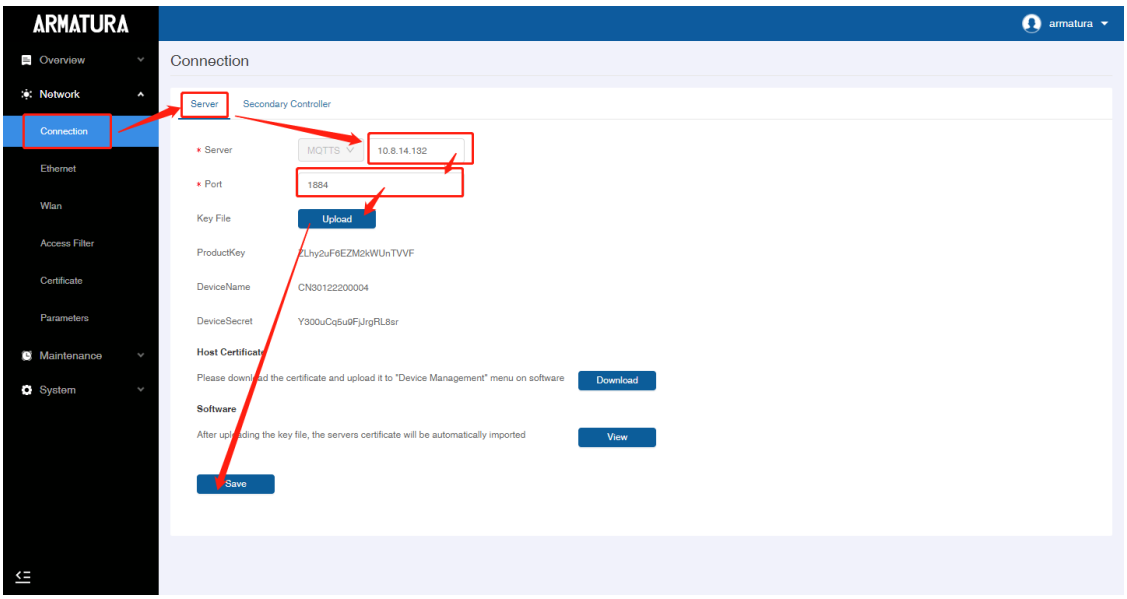
- **Username**: armatura
- **Password**: armatura

After logging in, change the admin password as prompted.



- Navigate to **[Network]** > **[Connection]** and open the Server tab

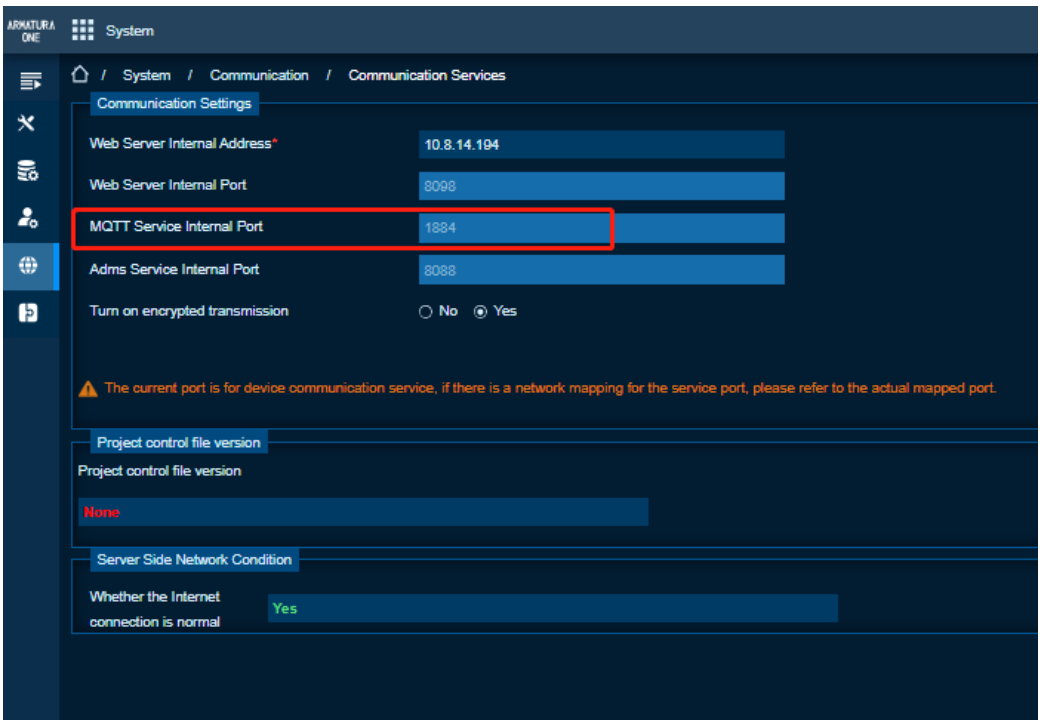
Copyright © 2024 ARMATURA LLC. All rights reserved



Protocol: MQTTs

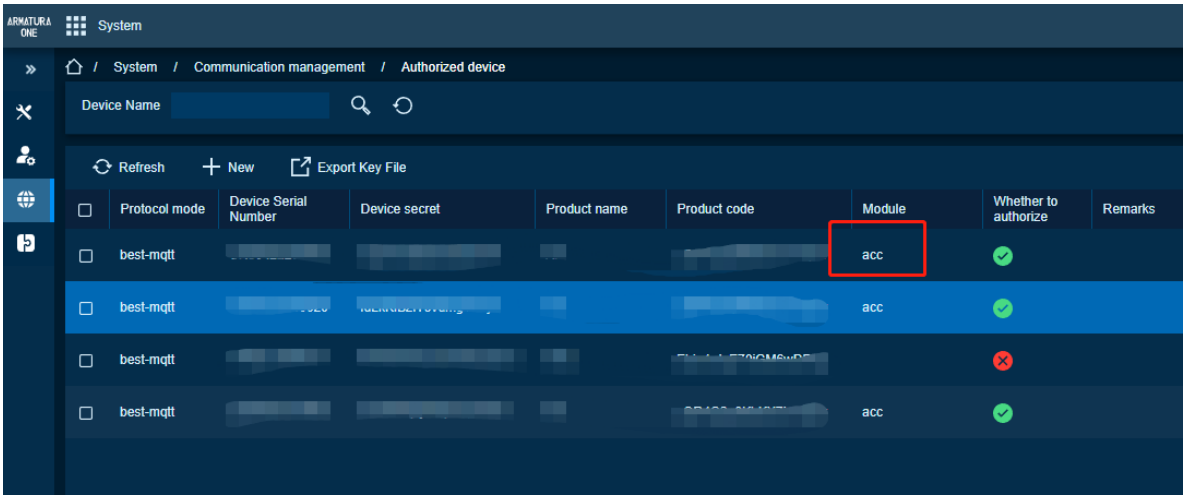
Server Address: Enter the appropriate server address.

Port: Default is 1884. Verify this via **[System] > [Communication Management] > [Communication Services] > [MQTT Service Internal Port]**. Set as Registration Device.



Key File: Upload the file exported from **[System] > [Communication] > [Authorized Management]**.

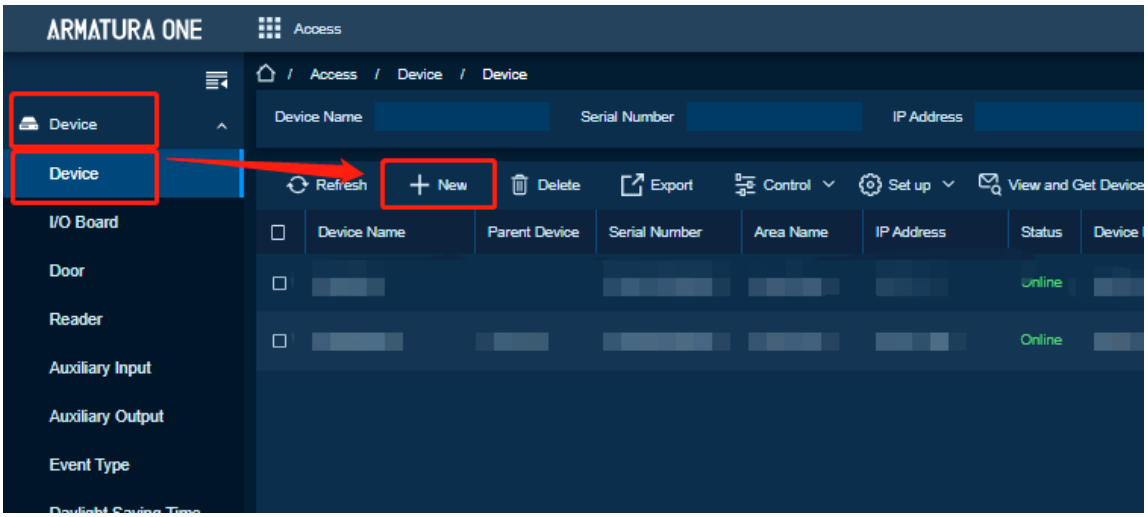
Copyright © 2024 ARMATURA LLC. All rights reserved



Upon successful connection to MQTT, the Column **Module** will show acc. If the device is not yet authorized in the **Access Module**, it will display a .

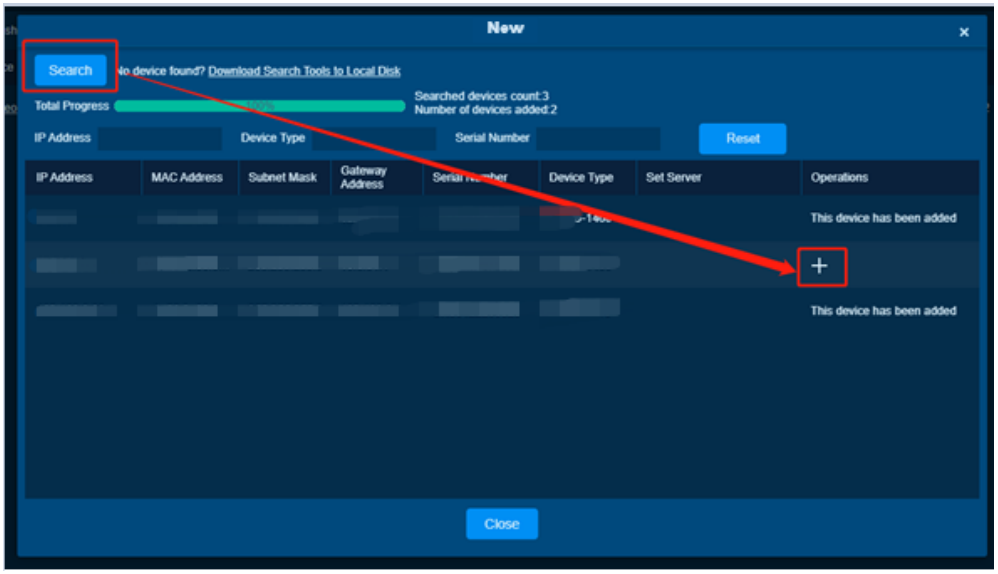
Add Controller in [Access] Module.

- Go to **[Access]** > **[Device]** > **[Device]** and click the New button.

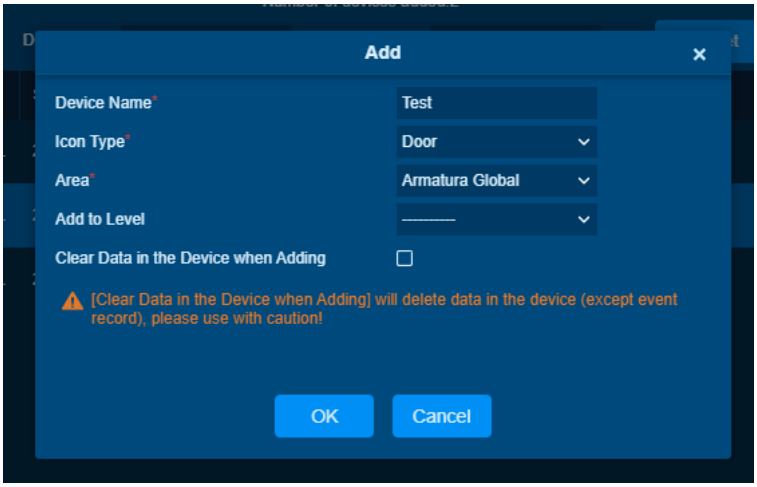


In the **New** window, click the **Search** button to locate the controller.

Copyright © 2024 ARMATURA LLC. All rights reserved



In the **Add** window, select the controller and click **Add**.



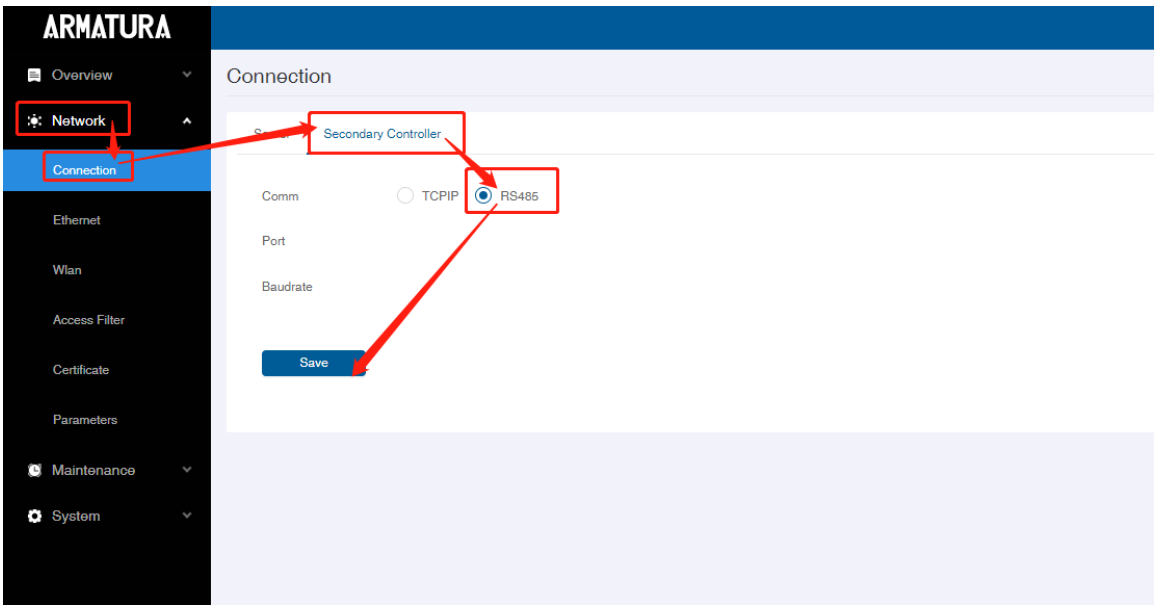
Note:

Enable the "**Clear Data in Device when Adding**" option to ensure no previous data remains on the device that could lead to unauthorized access.

Step 2: Set Secondary Controller Communication Port.

- Navigate to **[Network]** > **[Connection]** and select the Secondary Controller tab.

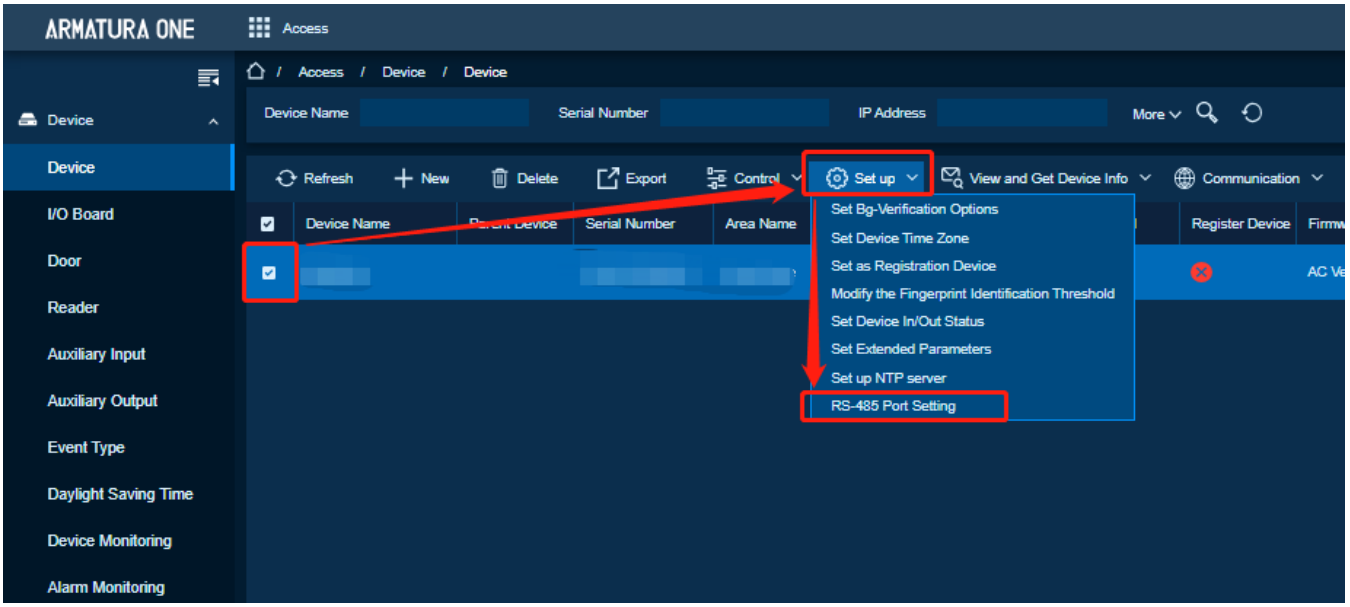
Copyright © 2024 ARMATURA LLC. All rights reserved



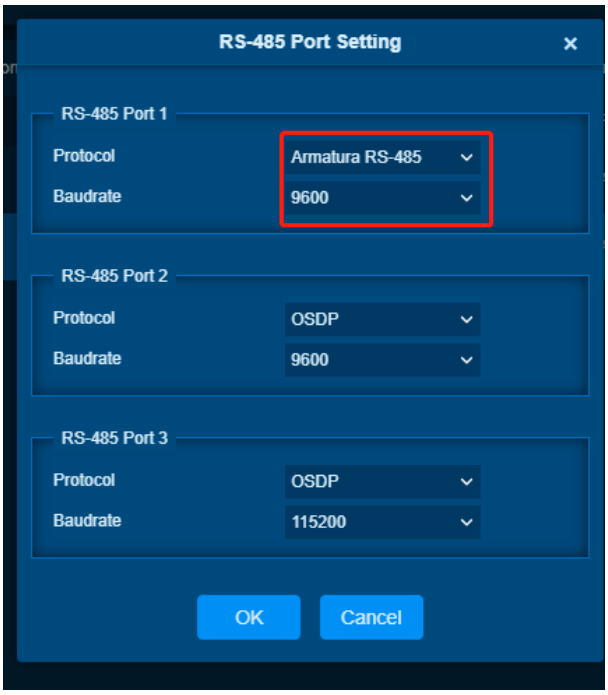
Configure the RS-485 settings:

- **Connection**: Select the **RS-485** radio button.
- **Port**: Choose the RS-485 port for the **Secondary Controller** connection. This depends on the RS-485 settings configured in the software (**[Access] > [Device] > [Device] > [Set up] > [RS-485 Port Settings]**).
- **Baudrate**: Set the appropriate RS-485 baud rate, matching the settings configured in the software.

Save the configuration.



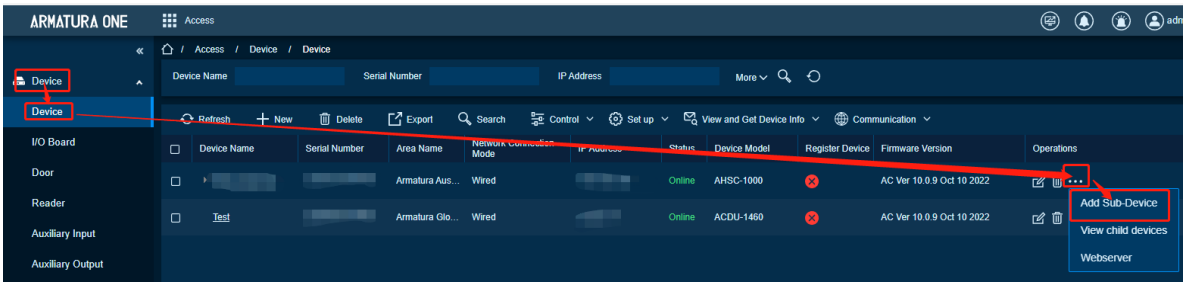
Copyright © 2024 ARMATURA LLC. All rights reserved



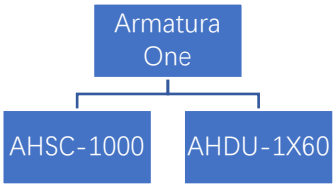
Device has three inputs, RS-485 Port 1/Port 2/Port 3.

Armatura RS-485 is the protocol used for primary-secondary connection.

Step 3: Add Secondary Controller.



- Master Mode

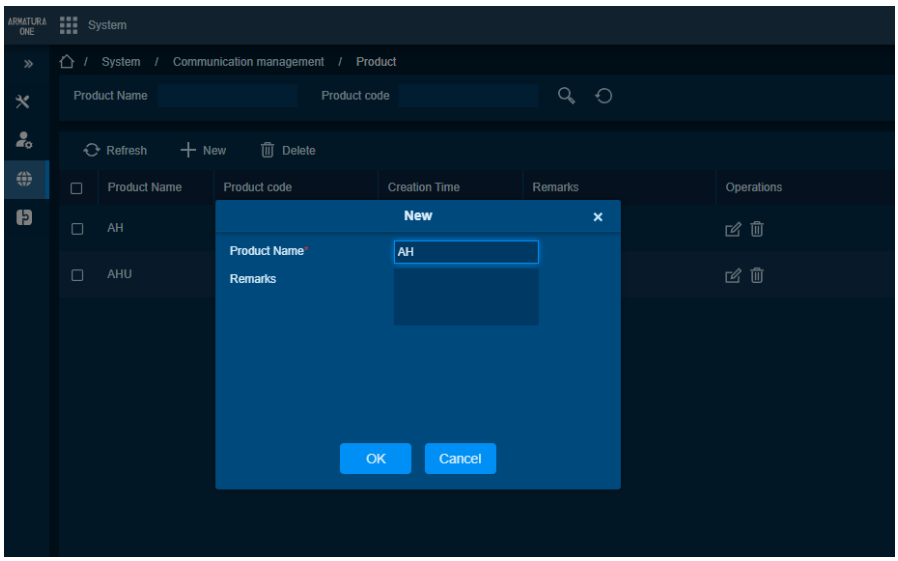


Step 1: Add **Primary Controller**

Add a product

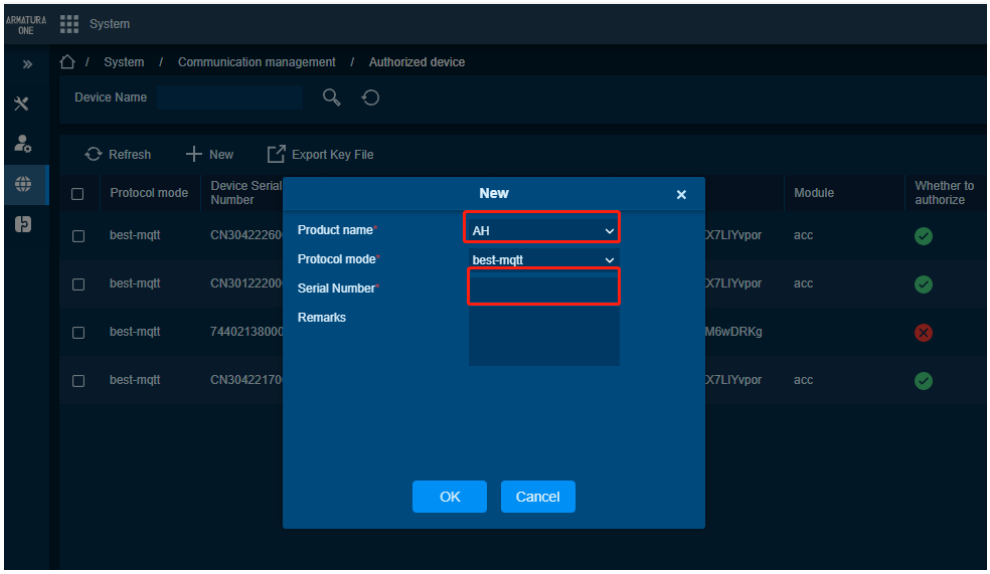
- In **[System]** > **[Communication Management]** > **[Product]**, Click New Button.

Copyright © 2024 ARMATURA LLC. All rights reserved



Add a device

- In **[System]** > **[Communication Management]** > **[Authorized Device]**, Click New Button.

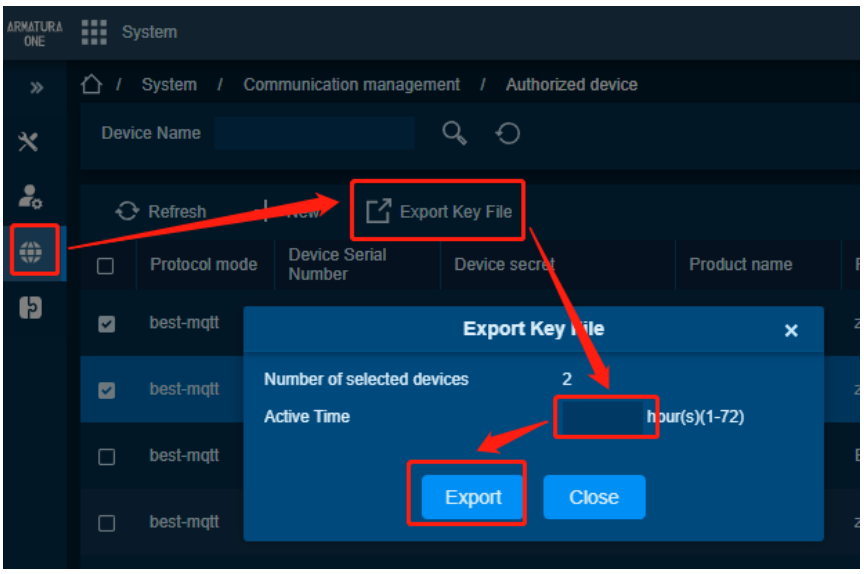


Select the product you just created, then enter the serial number.

Export Key File

- Go to **[System]** > **[Communication Management]** > **[Authorized Device]** and click New to add the device.

Copyright © 2024 ARMATURA LLC. All rights reserved

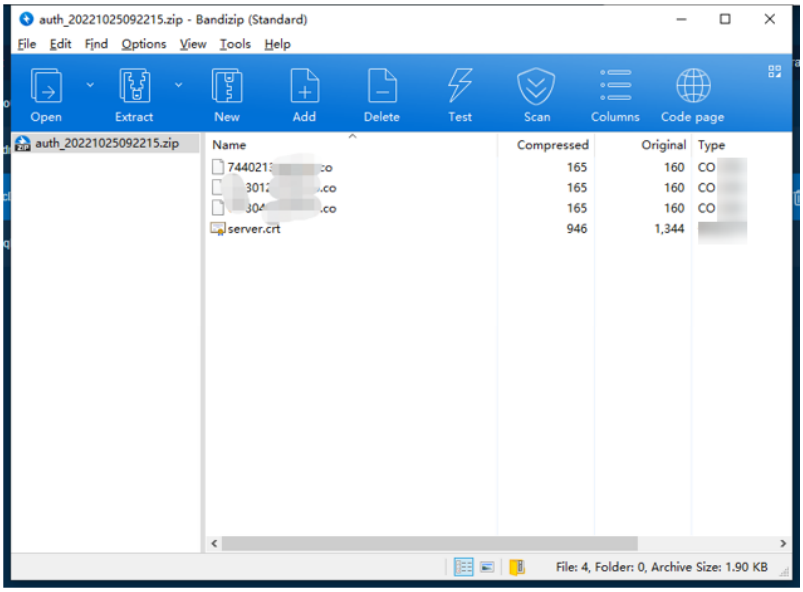


Active time Key file validity, the value ranges from 1-72 Hours.

After clicking the **Export Button**, the browser will download a .zip file.

Note:

This function supports selecting multiple devices. By clicking the icon, it generates .co files for all controllers and a server certificate, packaged into a .zip file. Simply upload this .zip file to the controller's web server.



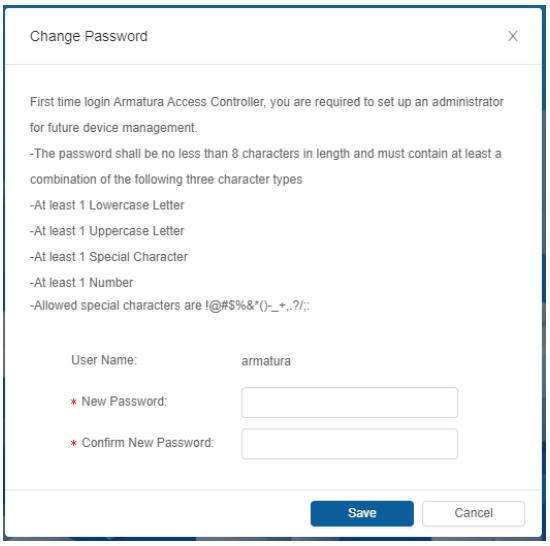
Import Key File to Controller

Step 1: Access the Controller Web Interface

- Open a browser and navigate to the controller's web interface using the URL: https://**[controller IP address]**.

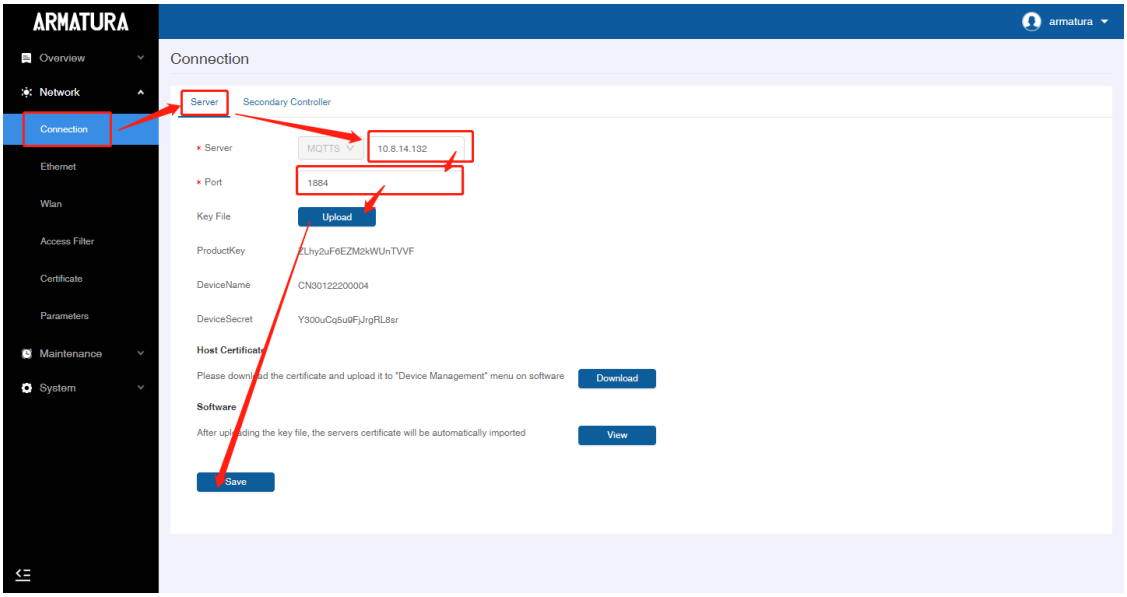
Copyright © 2024 ARMATURA LLC. All rights reserved

- Login credentials for the first-time login:



- **Username**: armatura
- **Password**: armatura

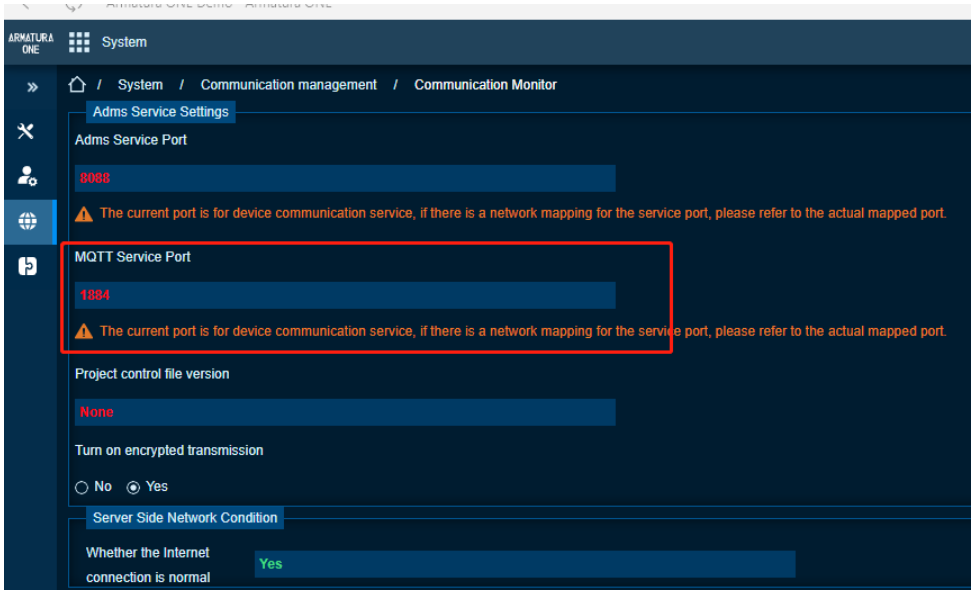
Upon logging in for the first time, you will be prompted to change the admin account password.



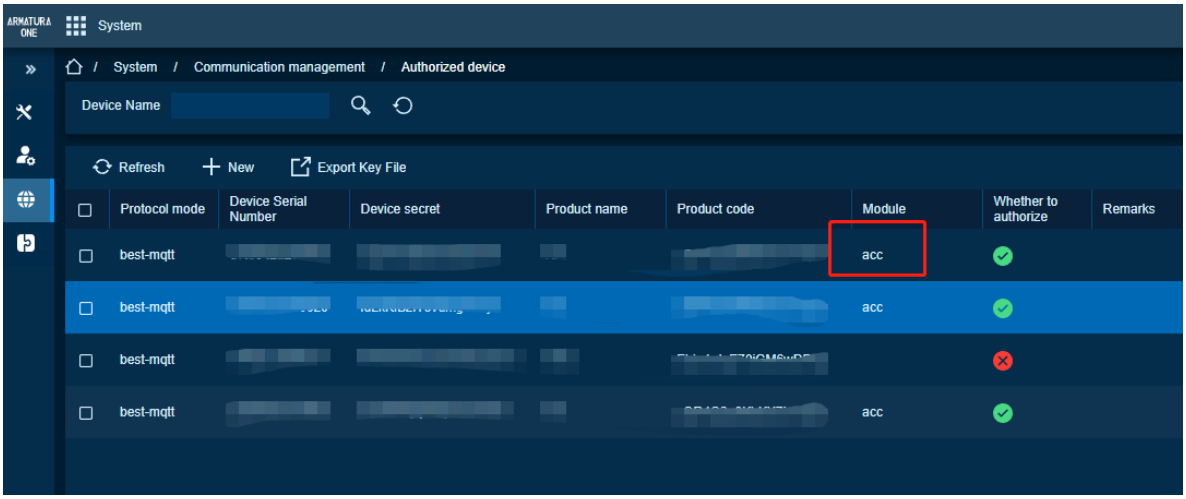
Copyright © 2024 ARMATURA LLC. All rights reserved

Step 2: Configure the Server Settings

- Navigate to **[Network] > [Connection]**.
- Open the **Server** tab and configure the following parameters:
  - **Protocol**: MQTTs (default).
  - **Server Address**: Enter the appropriate server address.
  - **Port**: Default is 1884. Verify this in the software via **[System] > [Communication Management] > [Communication Monitor] > [ADMS Service Settings] > [MQTT Service Port]**.



Key File: Upload the key file exported from **[System] > [Communication Management] > [Authorized Device].**



Step 3: Verify MQTT Connection

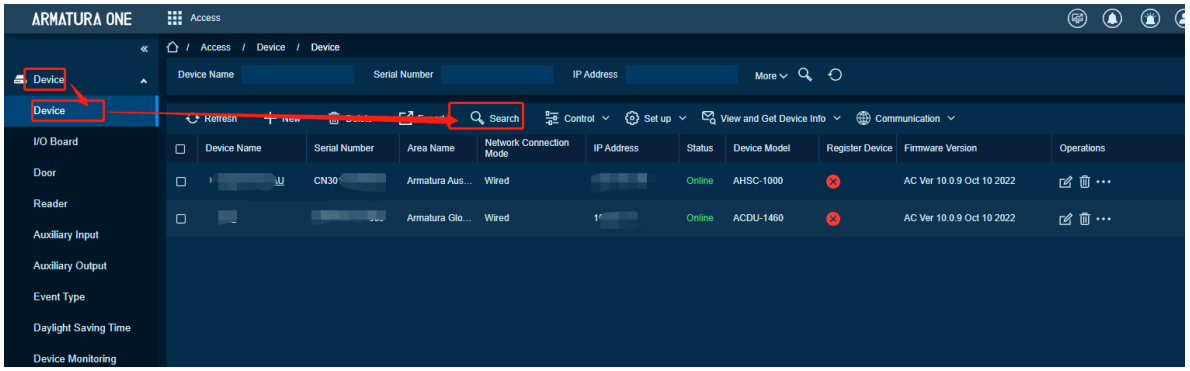
- After the controller successfully connects to MQTT, the Column Module will display acc.

Copyright © 2024 ARMATURA LLC. All rights reserved

- If the device is not yet authorized in the **Access Module**, it will display a .

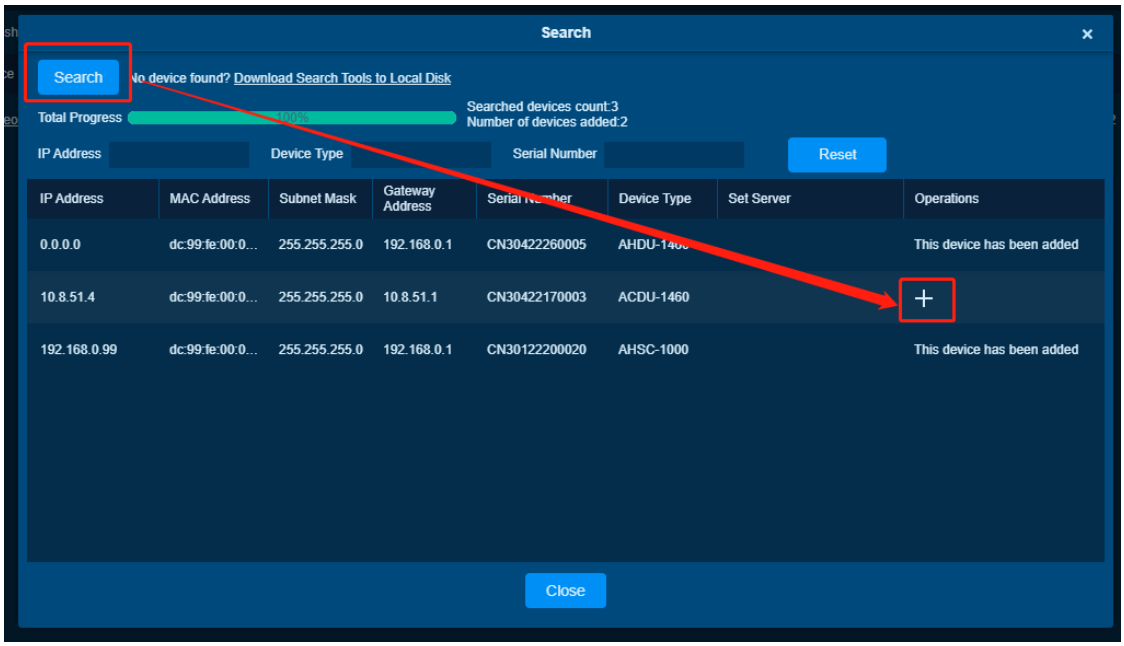
Step 4: Add the Controller to the Access Module

- Navigate to **[Access]** > **[Device]** > **[Device]** in the software.



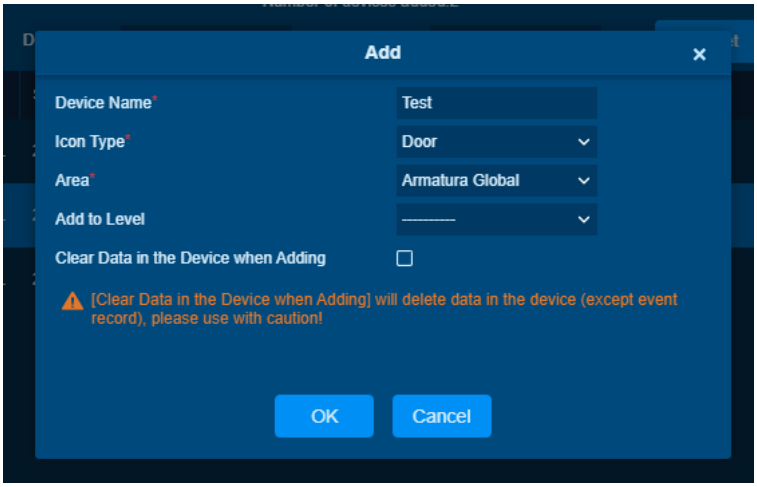
Click the **Search** button to locate the controller.

- In the **Search** window, click **Search** to display a list of available devices.



- Select the desired controller from the list and click Add

Copyright © 2024 ARMATURA LLC. All rights reserved



Note:

Enable the "**Clear Data in Device when Adding**" option to ensure no previous data remains on the device that could lead to unauthorized access.

Delete Device

Prerequisites for Use

Log into a valid account that has the required permissions to delete devices. Devices with **Global Anti-Passback** or **Global Interlock** rules cannot be deleted. Deleting such device requires first deleting the associated **Global Anti-Passback** or **Global Interlock** rules.

Usage Scenarios

The device requires re-registration, or the device is no longer in use.

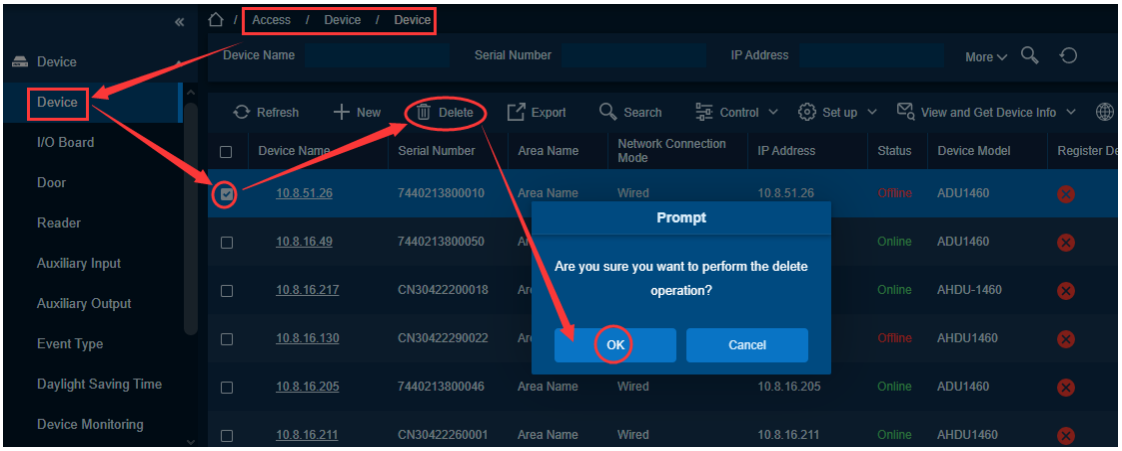
Trigger Results

When a device is removed, it is successfully deleted from the system. If the **Primary Controller** is deleted from **[Access] > [Device]**, any **Secondary Controller**s linked to it will also be removed. Furthermore, if the device uses the Spada Protocol, deleting it will automatically remove it from **[System] > [Authorized Device]**.

Steps to Delete a Device:

- Navigate to **[Access] > [Device] > [Device] > [Delete]**.
- Select the desired device to delete, and the system will display the delete page.
- Confirm the deletion by clicking **OK**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export Device

Prerequisites for Use

Log into with a valid account that has the required permissions.

Usage Scenarios

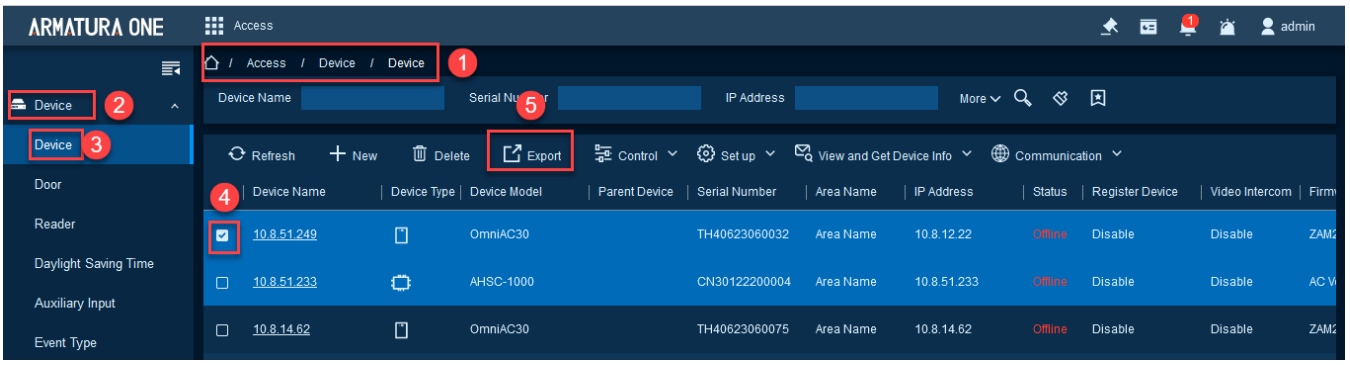
Export device information for reference or documentation purposes.

Trigger Results

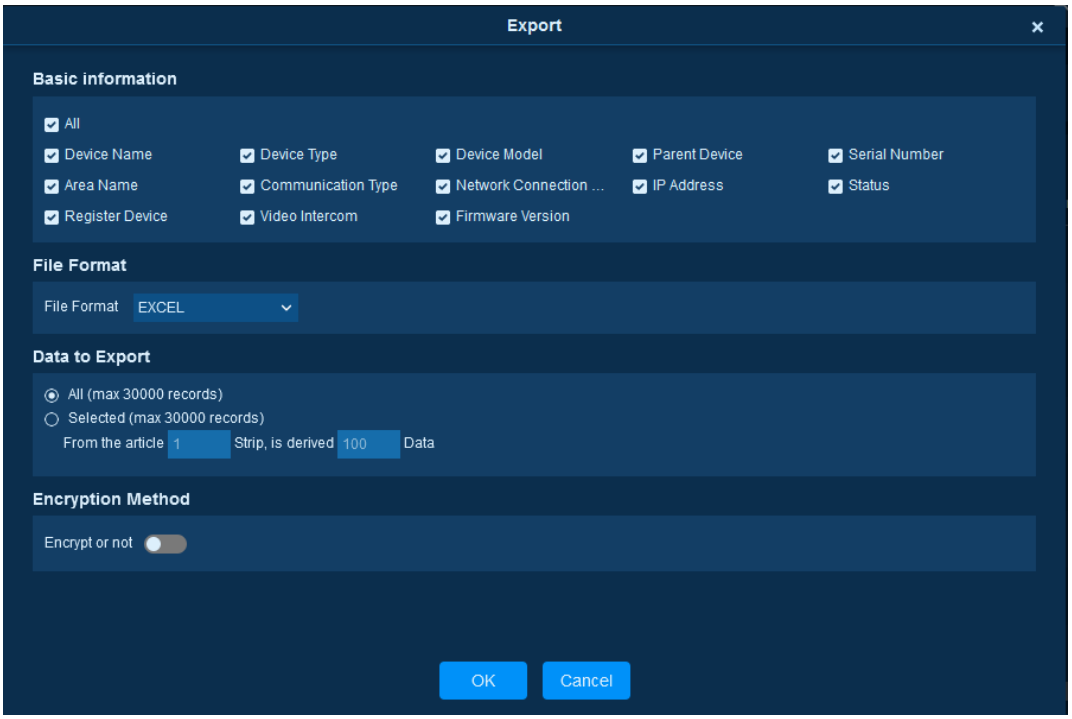
Export files in Excel/PDF/CSV format. The exported data includes device name, serial number, area name, network connection mode, IP address, status, device model.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [Export]**.
- Select the desired file format (Excel, PDF, or CSV) and click **OK**.
- The system will generate and download the export file with the specified details.



Copyright © 2024 ARMATURA LLC. All rights reserved



Device

Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Enable	Device Model	Register device	Firmware Version
192.168.218.60	20100501999	Area Name	HTTP	Wired	192.168.218.60		Enable	C3-400Pro		AC Ver 4.7.7.3033 Jun 16 2017

Control: Clear Administrator Permission

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

The device no longer requires an administrator permission.

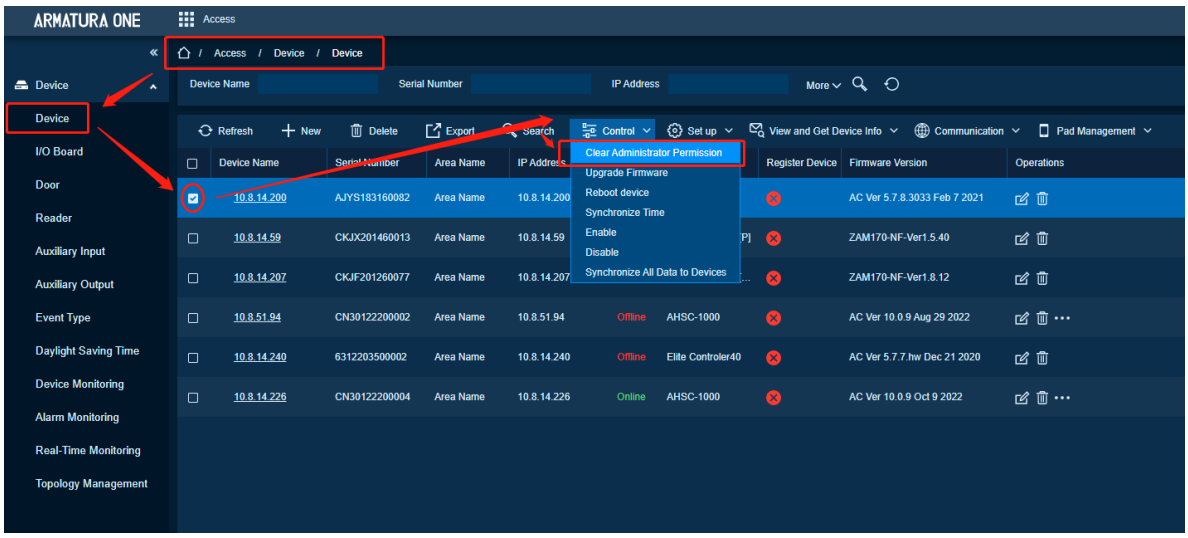
Trigger Result

The administrator account is removed from the device.

Steps:

- Navigate to **[Access]** > **[Device]** > **[Device]** > **[Control]** to access the control page.
- Select the desired device from the list.
- Click **[Clear Administrator Permission]**.
- Confirm the action, and the administrator account will be cleared from the device.

Copyright © 2024 ARMATURA LLC. All rights reserved



Upgrade Firmware

Prerequisites for Use

Log into the system using an account with the required permissions to upgrade firmware.

A valid firmware release from authorized resources is required.

Usage Scenarios

The device requires a new feature that is not supported by its current firmware.

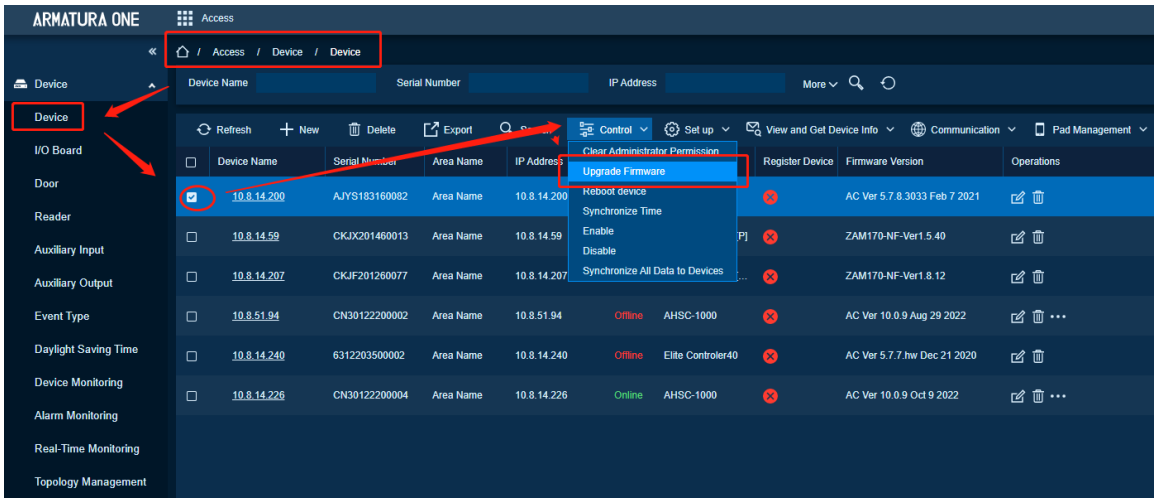
Trigger Result

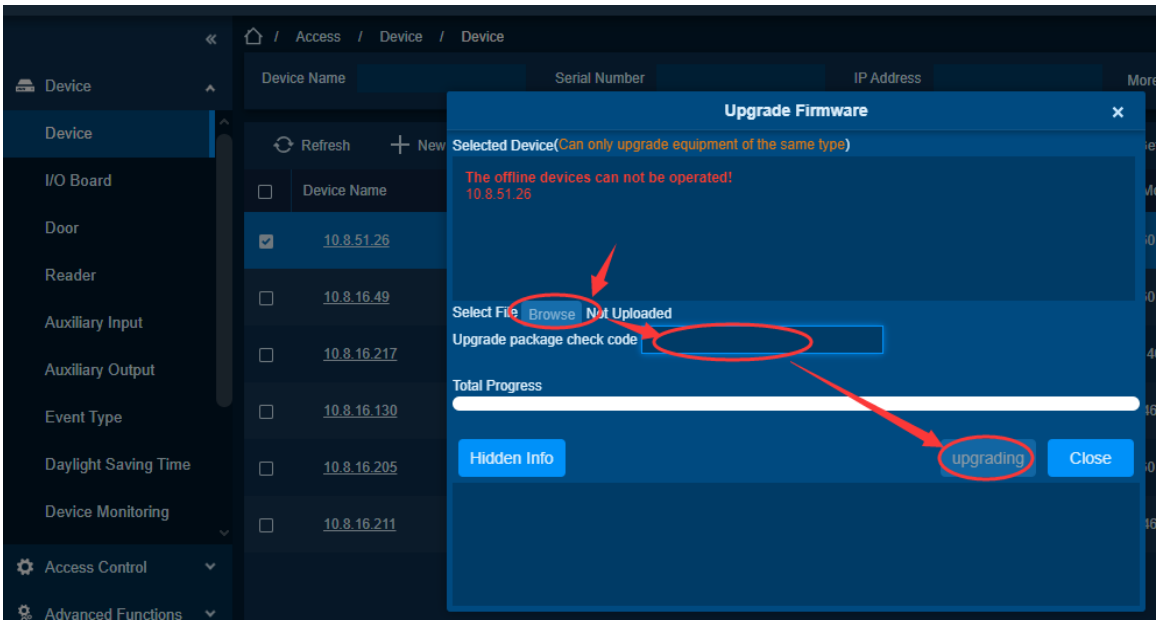
After a successful firmware upgrade, the device's firmware version is updated in the system's device list, and the device gains support for the required software functionality.

Steps to Upgrade Firmware:

- Navigate to **[Access]** > **[Device]** > **[Device]** > **[Control]** to access the control page.
- Click **[Upgrade Firmware]** to open the firmware upgrade window.
- Click **[Browse]** to locate and select the firmware upgrade package.
- Rename the firmware package file name as “crtlfw.ar”.
- Enter the **Upgrade Package Check Code** in the designated field (Only applies when firmware is required).
- Click **[Upgrade]** to initiate the firmware upgrade process.
- Monitor the progress bar. Wait until the process is completed successfully.

Copyright © 2024 ARMATURA LLC. All rights reserved





Note:

Do not upgrade firmware without proper authorization. Contact the systems integrator before performing a firmware upgrade or proceed only as instructed by the system integrator. Unauthorized upgrades may void the device warranty or disrupt device operation.

Reboot Device

Prerequisites for Use

Log into the system using an account with the required permissions and confirm the device is online.

Usage Scenarios

Address device data errors, prepare the device for a firmware re-upgrade, or reset it to restore proper functionality.

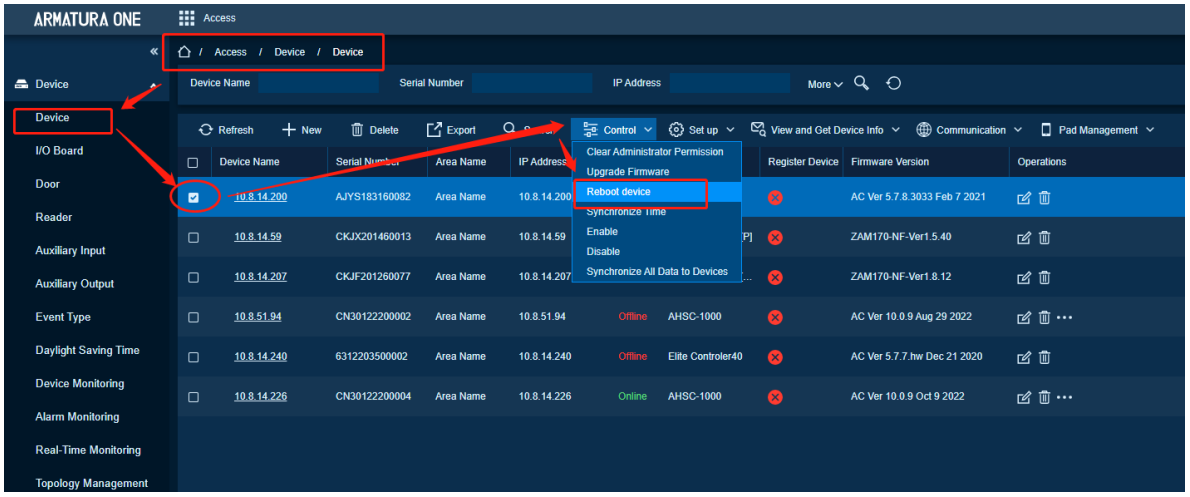
Copyright © 2024 ARMATURA LLC. All rights reserved

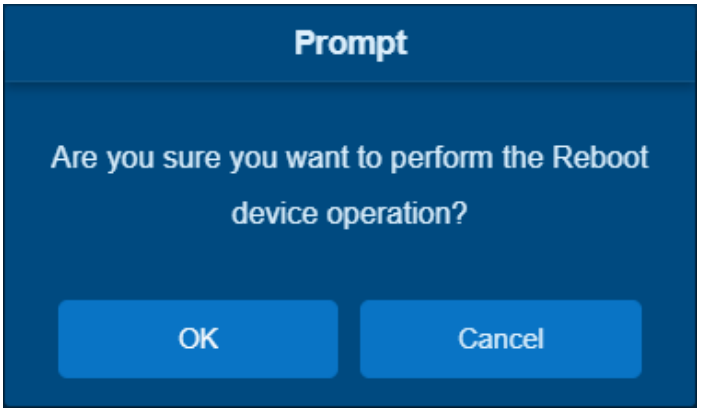
Trigger Results

The device will reboot, temporarily interrupting communication with the software. After the reboot is complete, the device will automatically reconnect to the software and return to an online status, typically within 1-2 minutes.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [Control]** to access the control page.
- Click **[Reboot Device]** to open the reboot interface.
- Confirm the action by clicking **[OK]**.
- Allow the reboot process to complete.
- The device will automatically reconnect to the software upon successful reboot.





Synchronize Time

Prerequisites for Use

Log into the system using an account with the required permissions and confirm the device is online.

Usage Scenarios

When the time settings between the software and the connected device are inconsistent.

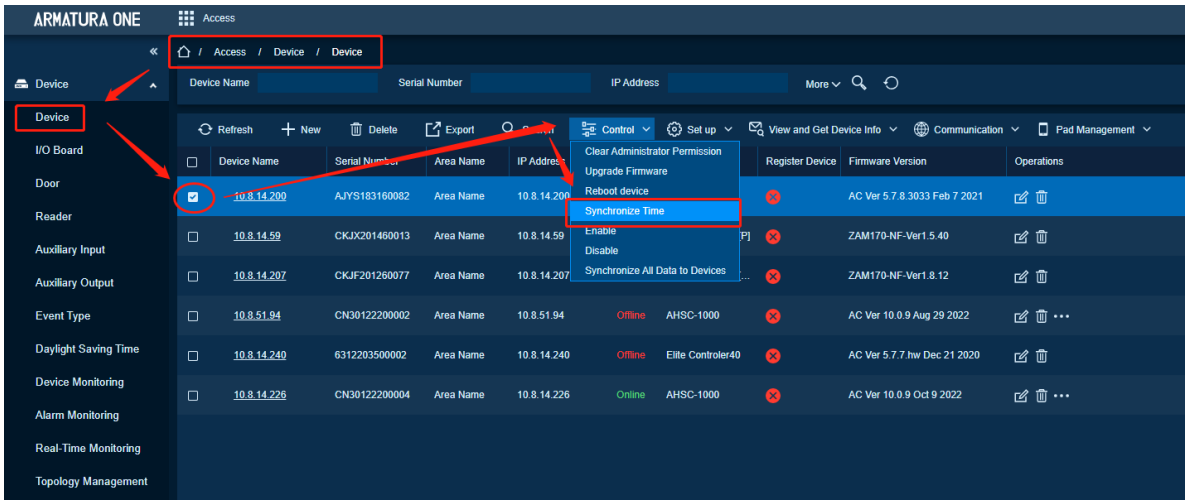
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Results

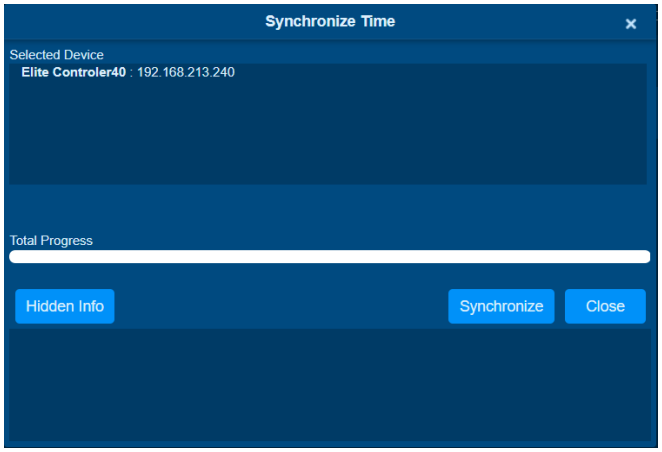
The software synchronizes the time with the connected device to ensure consistency.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [Control]** to access the control page.
- Click **[Synchronize Time]** to open the time synchronization interface.



- On the **Synchronize Time** interface, click **[Synchronize]** and wait for the process to complete.



Note:

If **[NTP Server Time Sync]** is enabled, the device will synchronize its time directly from the NTP server rather than the software.

Secondary Controller will not receive time synchronization directly from the software or NTP server. Instead, they will synchronize their time settings from the **Primary Controller**.

Enable

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device is ready to be connected and operated.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

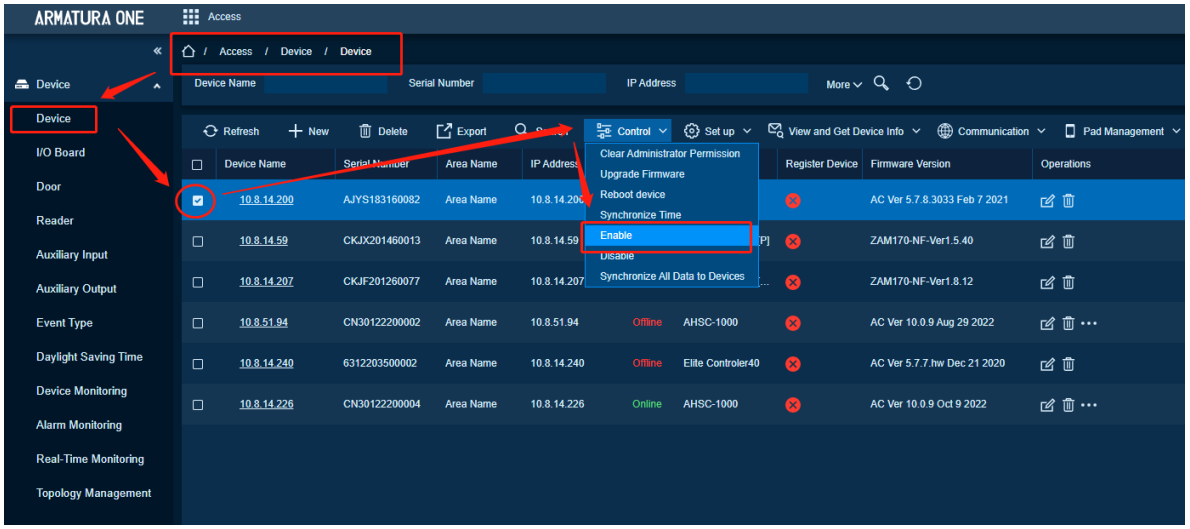
To re-establish communication with a device and enable its operation through the software.

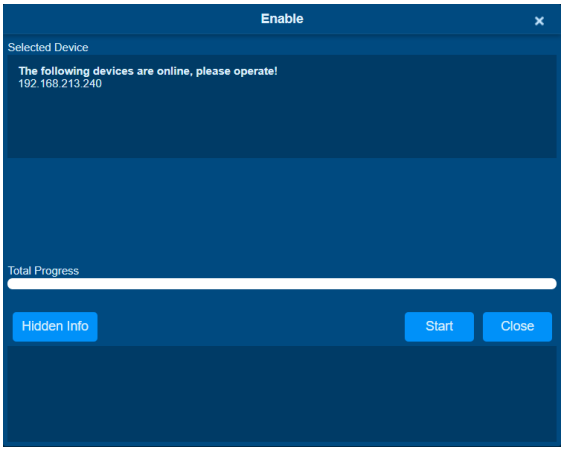
Trigger Results

Restores communication with the device, allowing it to function and perform operations listed in the device menu.

Steps:

- Navigate to **[Access]** > **[Device]** > **[Device]** > **[Control]** to access the control page.
- Click **[Enable]** to open the device enabling interface.
- Click **[Start]** to activate the device.





Disable

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function is used when communication between the device and the system is interrupted, the device encounters an error, or the device is temporarily not in use.

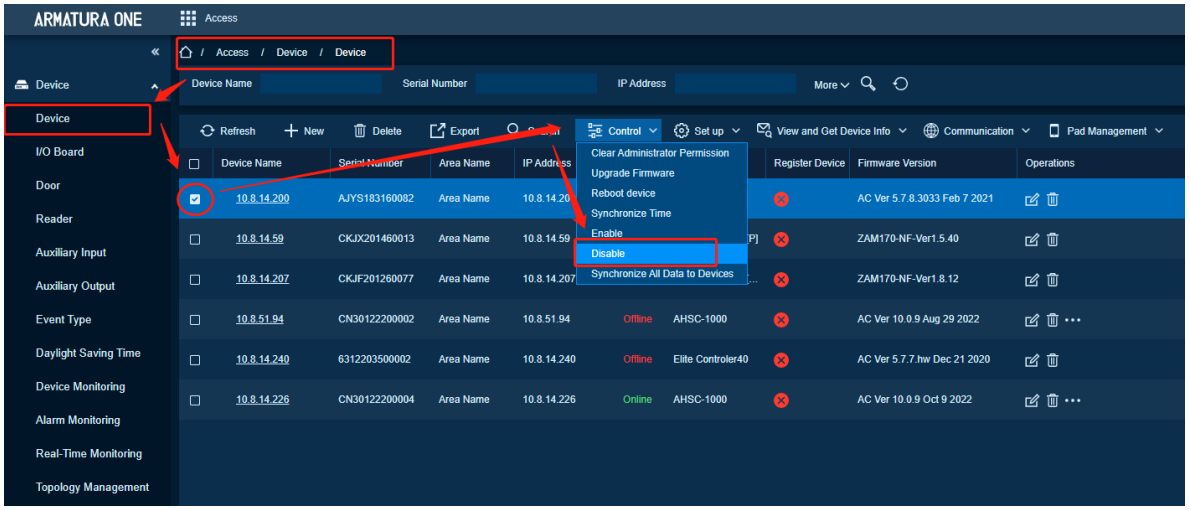
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Results

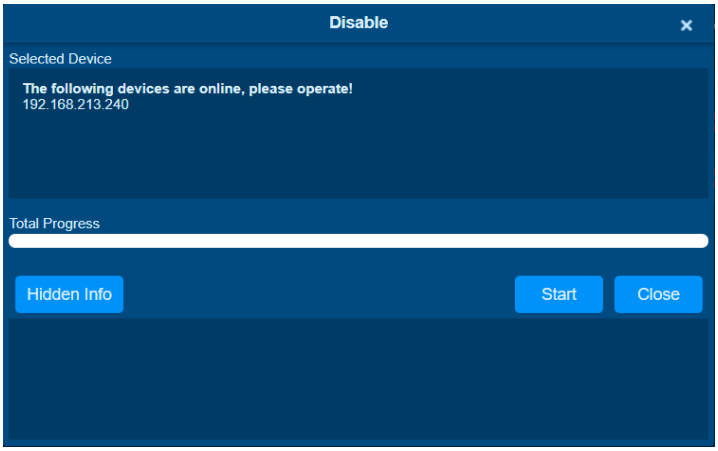
Terminate communication between the software and the device, updating the device status to "Disabled".

Steps:

- Navigate to **[Access] > [Device] > [Device] > [Control]** to access the control page.
- Select **[Disable]** to open the disabling interface.



- Click **[Start]** to disable the selected device.



Synchronize All Data

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device is online and properly connected.

Usage Scenarios

This function is used to manually transfer all data and configuration parameters from the software to the connected device.

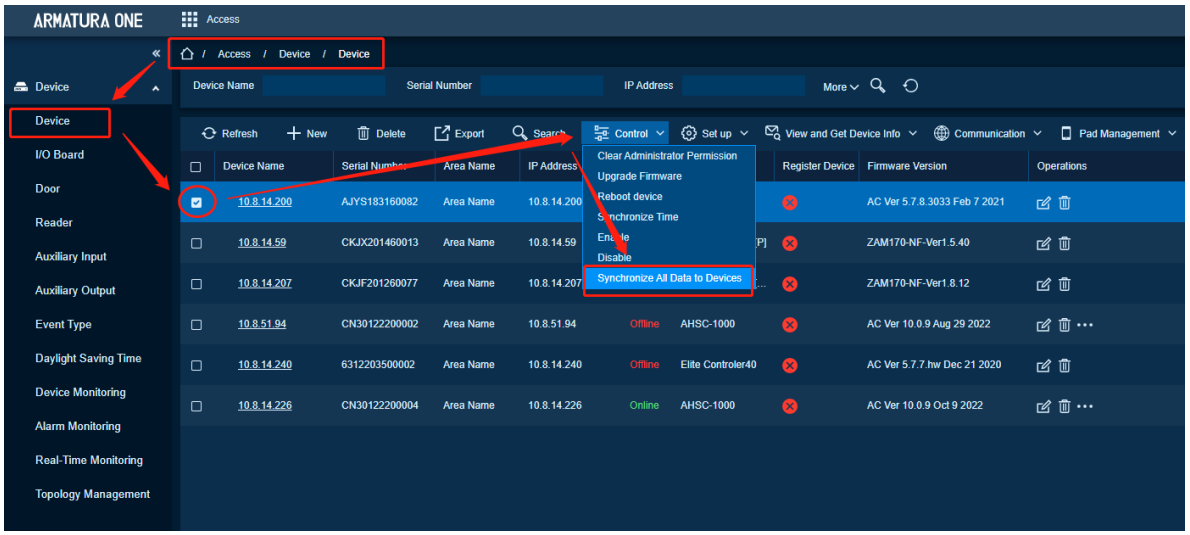
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Results

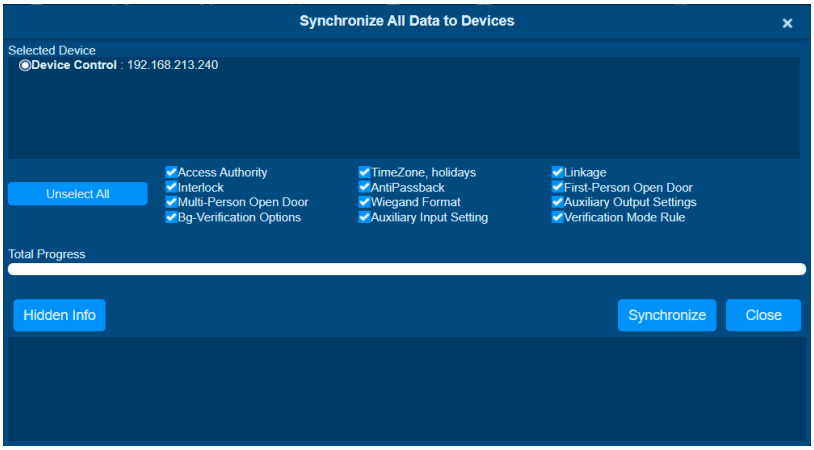
All data, including personnel records, access control settings, and other configurations from the software, are transferred and synchronized to the connected device.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [Control]** to access the control page.
- Click **[Synchronize All Data to Devices]** to open the synchronization interface.



- Click **[Synchronize]** to begin the synchronization process.
- Wait for the process to complete, ensuring all data is successfully transferred to the device.



Set Up: Background Verification Parameters

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device is online and connected. The device must support standard access permissions or have the ability to deny user

Copyright © 2024 ARMATURA LLC. All rights reserved

access when offline. This feature is only available when the device is online, and modifications cannot be made while the device is offline.

Usage Scenarios

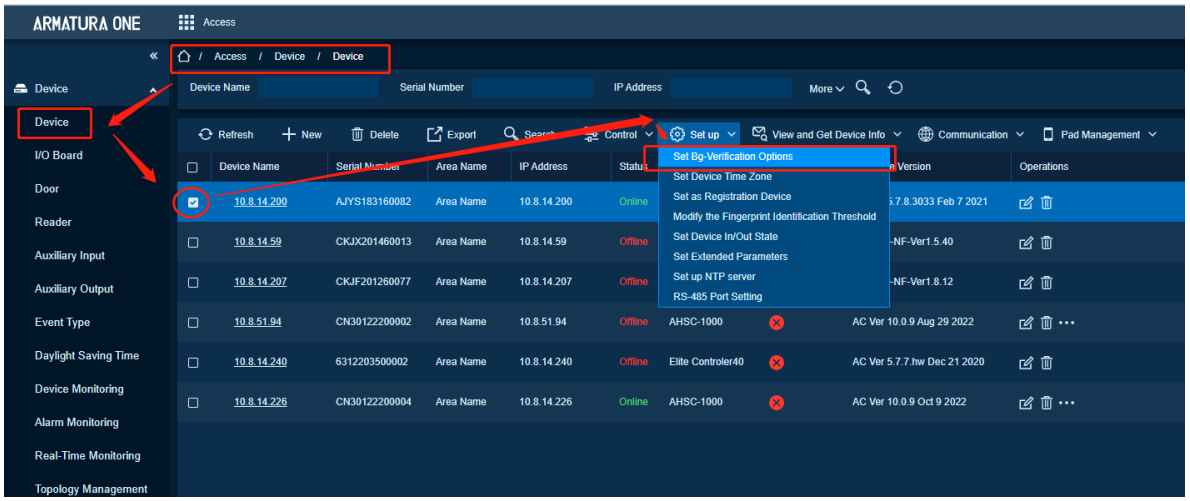
This function is used when the device requires verification through the software for enhanced access control or when configuring permissions for offline access scenarios.

Trigger Results

Enabling this function activates or deactivates the background verification feature on the device. It also updates the permissions applied when the controller is offline.

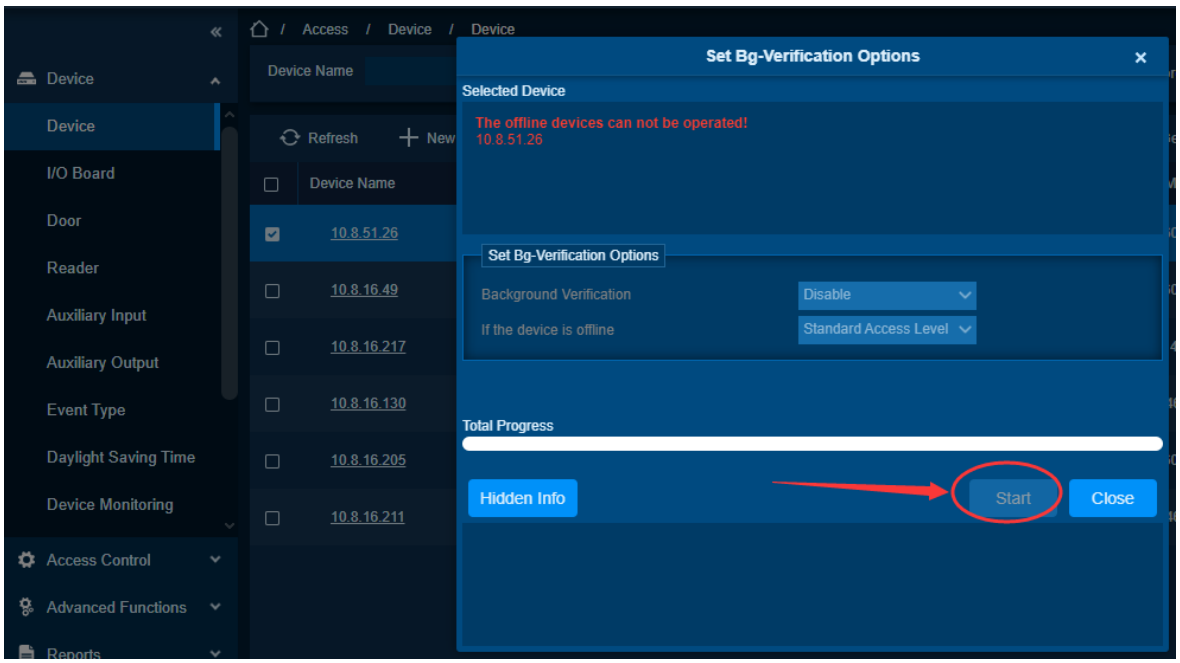
Steps:

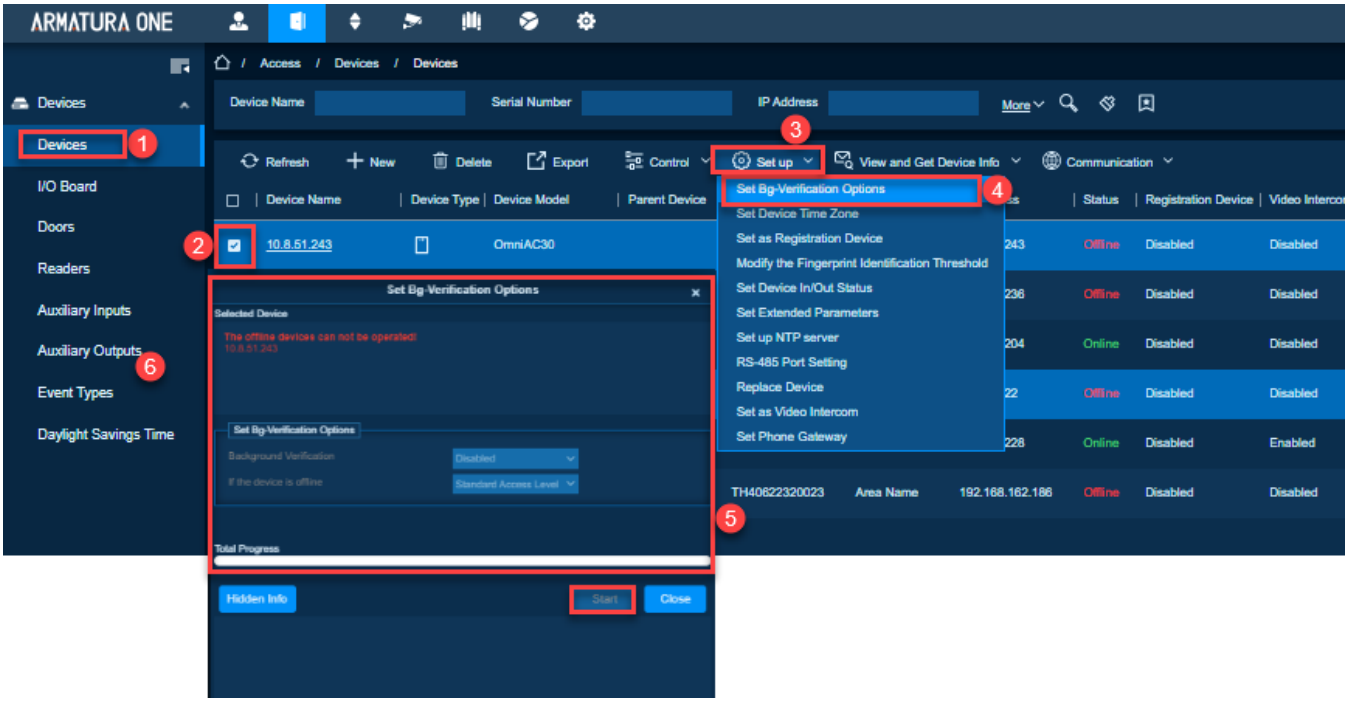
- Navigate to **[Access]** > **[Device]** > **[Device]** > **[Set Up Settings]** to access the settings page.
- Select the online device for which you want to configure the background verification options.
- Click **[Set BG-Verification Options]** and fill in the required parameters in the displayed form.



- After completing the configuration, click **[Start]** to apply the settings.
- Wait for the process to complete. The new settings will be synchronized with the device.

Copyright © 2024 ARMATURA LLC. All rights reserved





Set Device Time Zone

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function is used when the device's time zone configuration is incorrect or when the device's time zone differs from the server's time zone and requires synchronization.

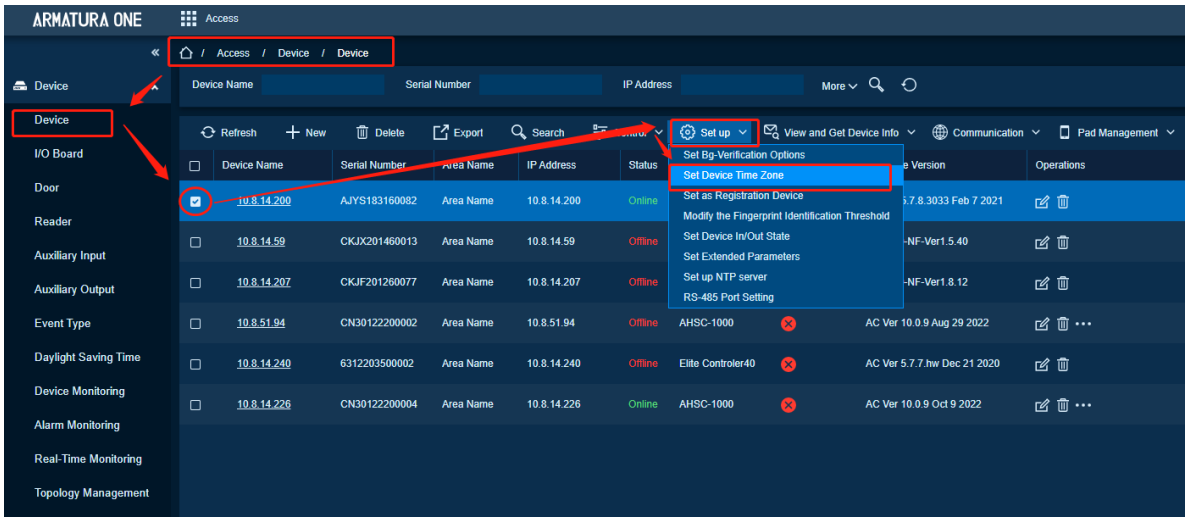
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

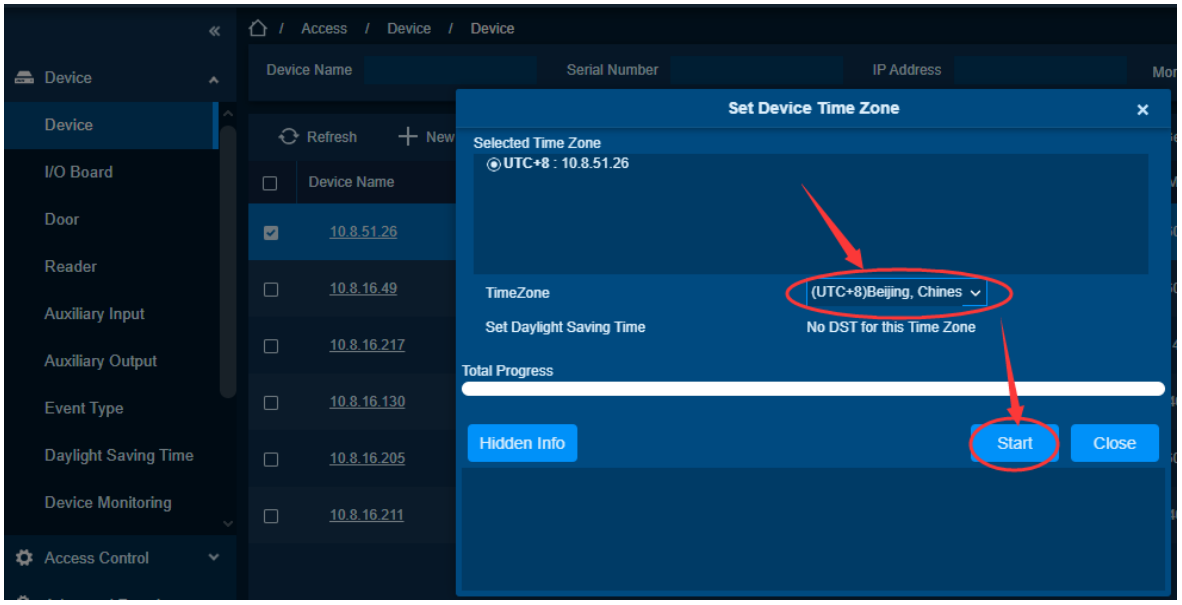
The modified time zone is synchronized with the device to ensure consistent time settings.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [Set Up]** to open the settings page.

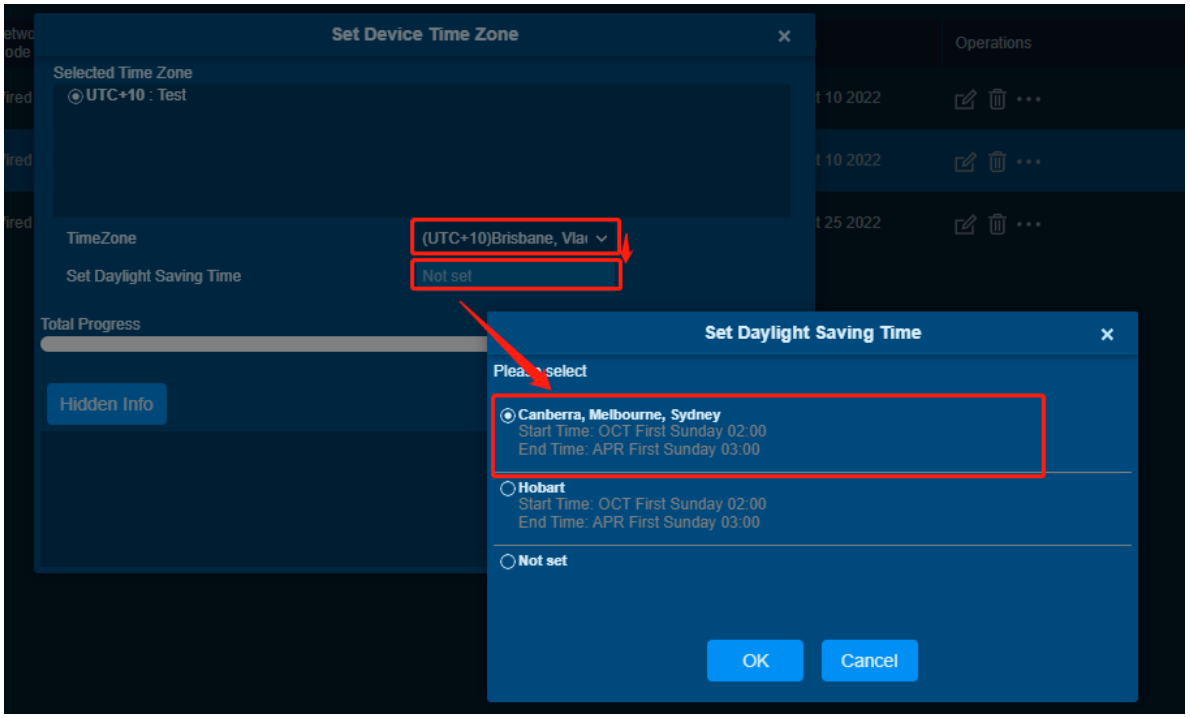


- Click **[Set Device Time Zone]** to display the time zone configuration interface.



- Select the desired time zone from the available options.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Click **[Start]** to apply the selected time zone and synchronize it with the device.

Set as Registration Device

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the connected device supports the registration function.

Usage Scenarios

This function is used when a user is enrolled on the device, and the user's data will be automatically uploaded to the software with all personnel entries.

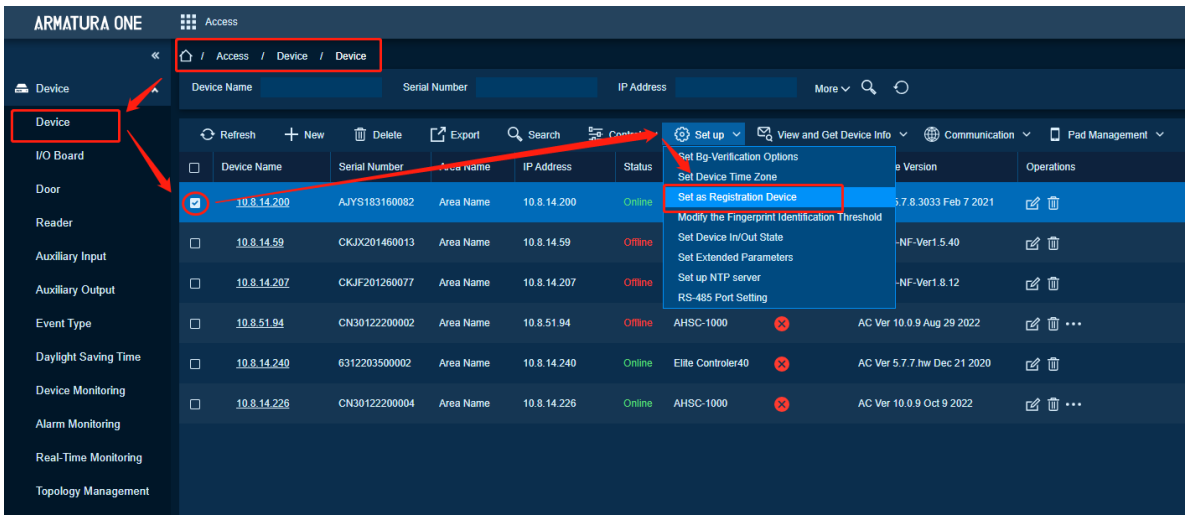
Trigger Result

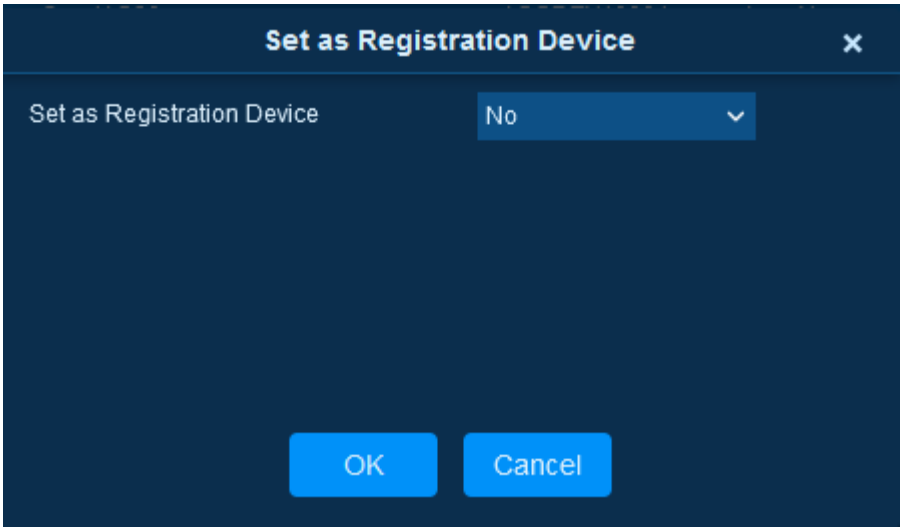
Any personnel added from that device, including their data and set parameters, will be automatically uploaded to the software.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [Set Up]** to access the settings page.
- Click **[Set Up Registration Device]** to open the registration device configuration interface.
- Review the settings and click **[OK]** to finalize the configuration.

Copyright © 2024 ARMATURA LLC. All rights reserved





Modify Fingerprint Comparison Threshold

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function is used to adjust the fingerprint comparison threshold. A higher threshold means more verification is required, while a lower threshold makes verification easier.

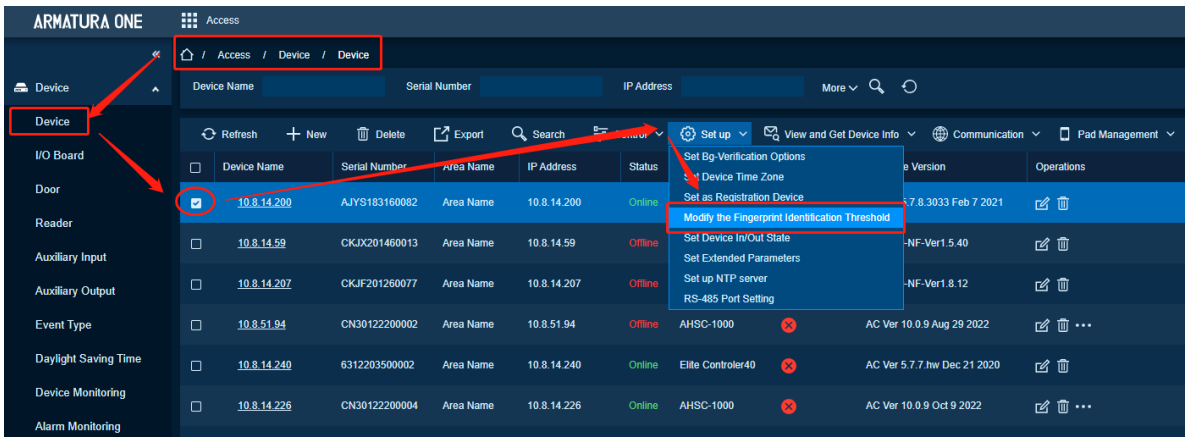
Trigger Results

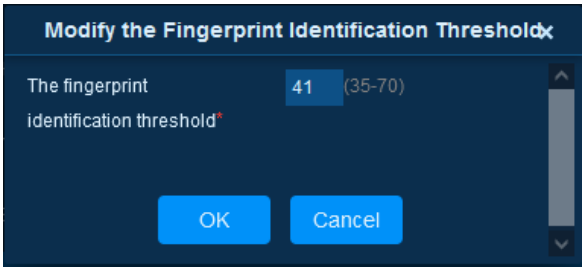
The fingerprint comparison threshold is modified, and the system will use the new threshold for fingerprint verification.

Steps:

- Click **[Access] > [Device] > [Device] > [Set up]** to display the setting page.
- Click **[Modify the Fingerprint Identification Threshold]** to exit the setting interface.

Copyright © 2024 ARMATURA LLC. All rights reserved





- Set the fingerprint identification threshold, then click **[OK]** to update the comparison threshold and synchronize it with the device.

Set Device In/Out Status

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function is used when configuring the device's access status for the anti-passback function.

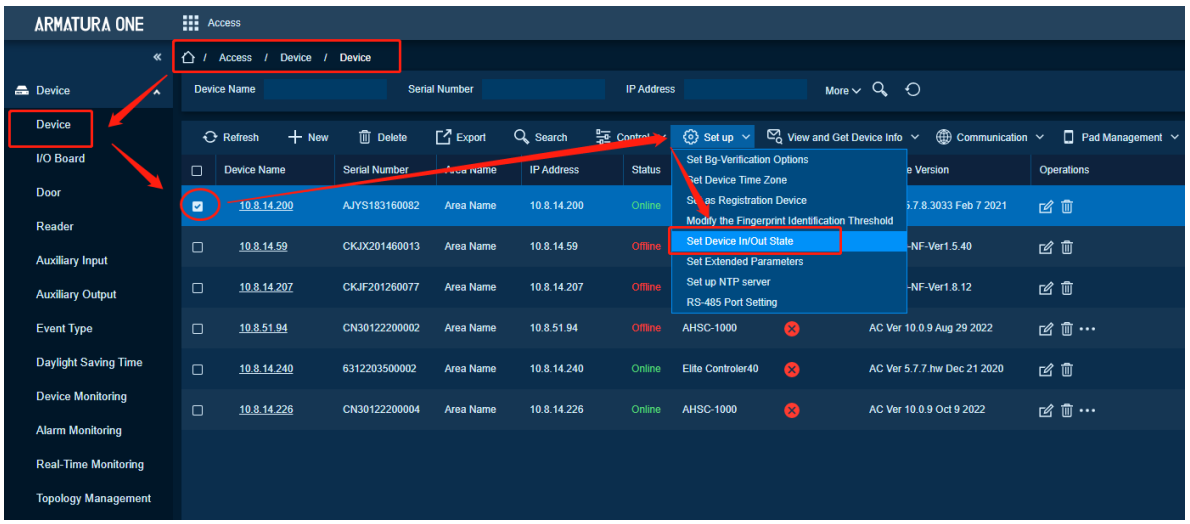
Trigger Results

The device will be marked as an in/out device. If the anti-passback function is enabled, the system will apply the anti-passback rule based on the device direction. For detailed settings, refer to the anti-passback function.

Steps:

- Click **[Access] > [Device] > [Device] > [Set up]** to open the settings page.
- Click **[Set Device In/Out State]** to exit the setting interface.

Copyright © 2024 ARMATURA LLC. All rights reserved



Set Extended Parameters

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenario

This function is used to configure extended parameters for face and access control features, including options for temperature detection, mask detection, access for unregistered people, triggering external alarms, and QR code settings.

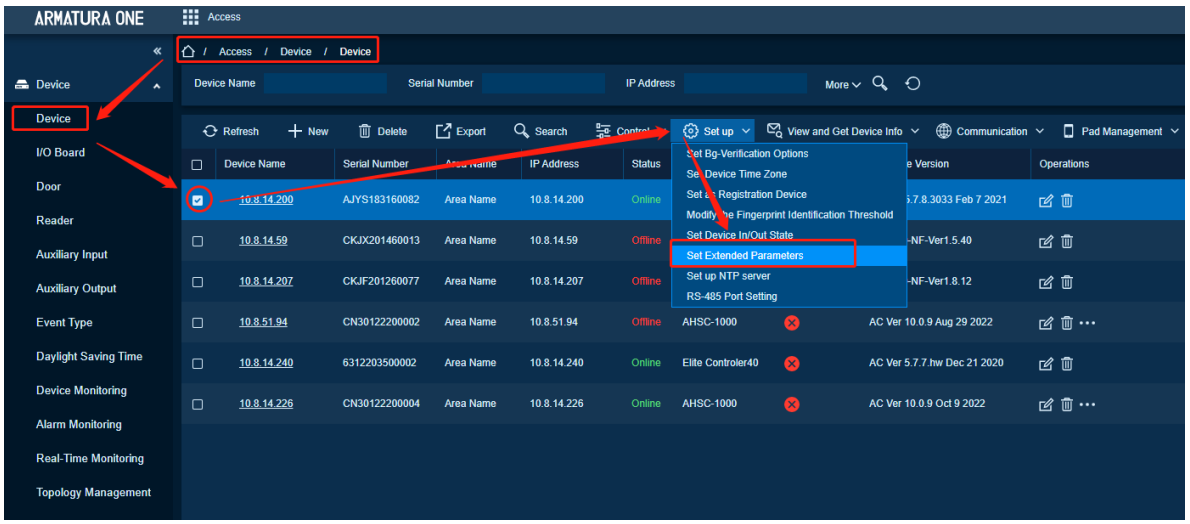
Trigger Results

The selected extended parameters will be applied to the system, enabling or disabling the respective features based on the configuration.

Steps:

- Navigate to **[Access]** > **[Device]** > **[Device]** > **[Set up]** to open the device settings page.
- Click **[Set Extended Parameters]** to open the extended parameters configuration interface.
- Modify the desired parameters.
- Click **[OK]** to apply the changes.

Copyright © 2024 ARMATURA LLC. All rights reserved



Set Up NTP Server

Prerequisites for Use

Log into the system using an account with the required permissions. Ensure that you have **AHSC-1000** and **AHDU-1X60** devices, as only these devices support this feature.

Usage Scenario

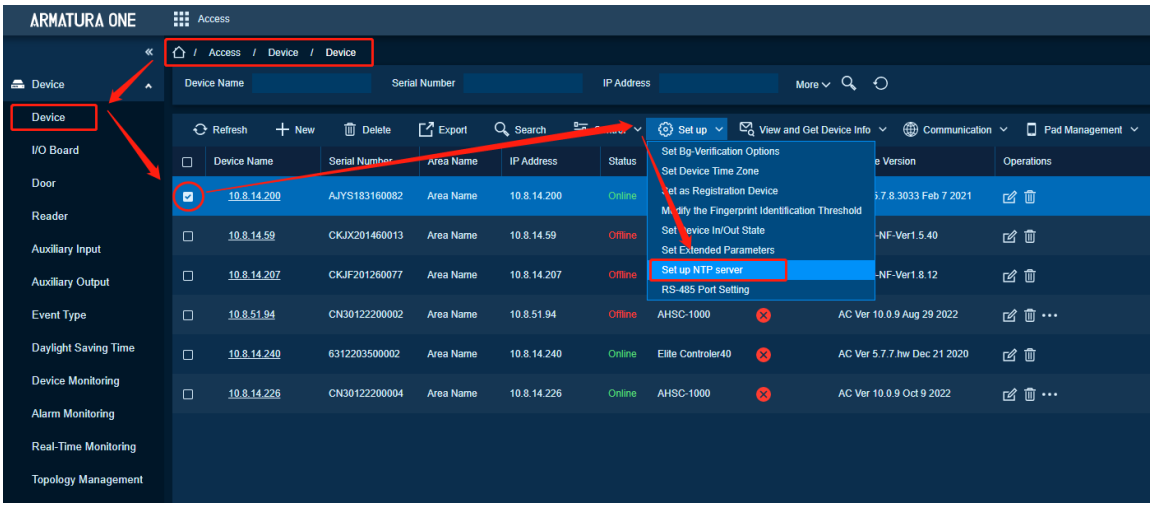
This function is used to configure the time server for the device, ensuring synchronized time settings.

Trigger Result

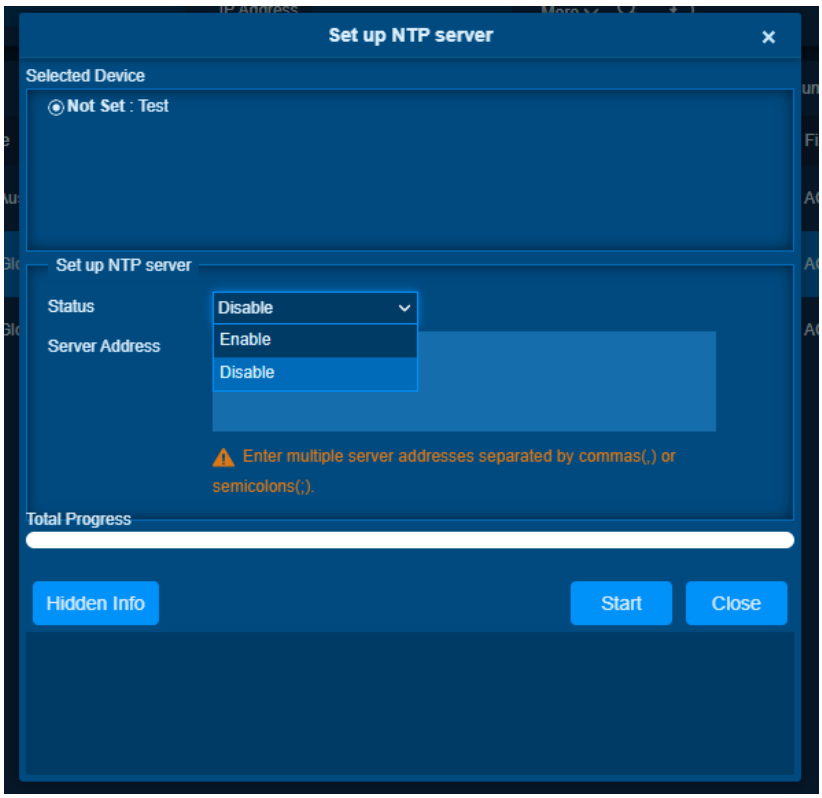
The device will retrieve the time from the specified NTP server and update its time accordingly.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [Set up]** to open the device settings page.
- Click **[Set up NTP Server]** to display the NTP server configuration interface.



Copyright © 2024 ARMATURA LLC. All rights reserved



- If the device settings in the selected window display **'Not Set',** it indicates the device (e.g., named 'Test') has not yet been configured with an NTP server.
- **Enable NTP Server:** Set the **[Status]** to **Enable.**
- **Enter Server Address:** Provide one or more NTP server addresses. Use commas (,) or semicolons (;) to separate multiple addresses.
- Click **[Start]** to save the configuration and apply it to the device.

Set RS-485 Port Setting

Prerequisites for Use

Log into the system using an account with the required permissions. Ensure that you have **AHSC-1000** and **AHDU-1X60** devices, as only these devices support this feature.

Usage Scenario

This function is used to configure the RS-485 port parameters for connecting devices via RS-485.

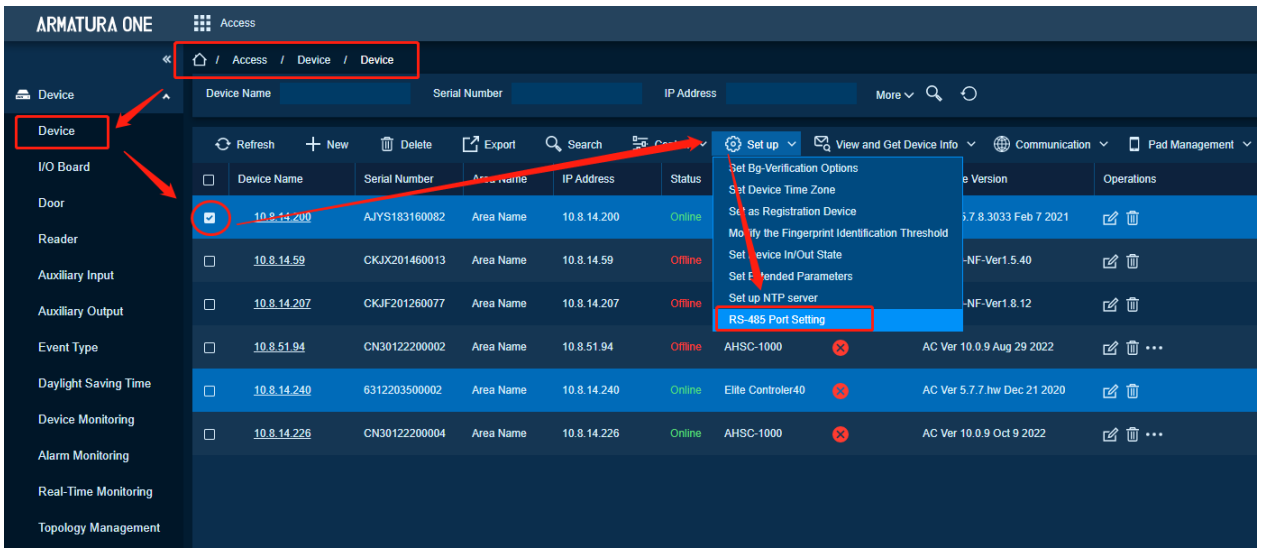
Trigger Results

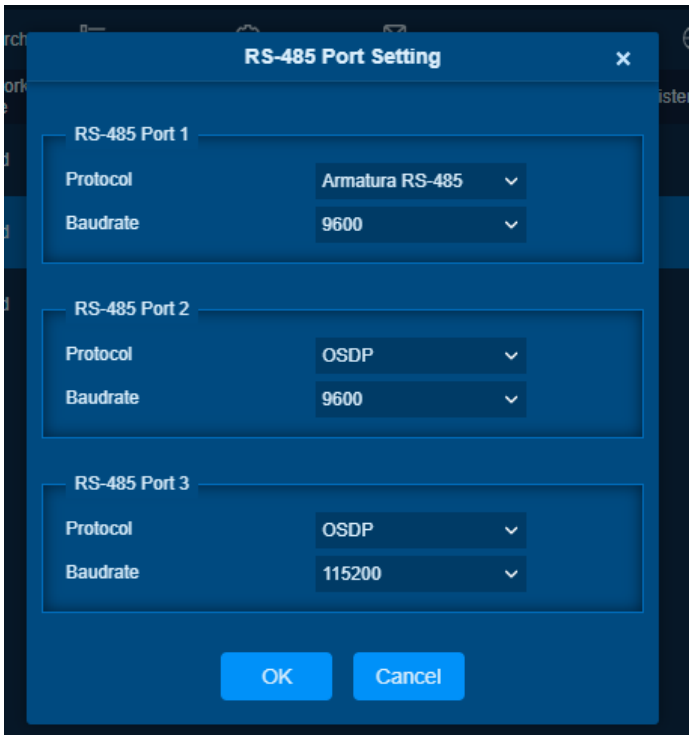
The device will enable the connection of **Secondary Controller**s, readers, or expansion boards via RS-485, using the specified protocol and baud rate.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [Set up]** to open the settings page.
- Click **[RS-485 Port Setting]** to open the configuration window.
- Set the appropriate protocol and baud rate for the desired RS-485 port based on the connection requirements.

Copyright © 2024 ARMATURA LLC. All rights reserved





Port Introduction

Parameter		Introduction
RS-485 Port	Protocol	Armatura RS-485/OSDP/Aperio
	Baudrate	4800/9600/19200/38400/57600/115200
RS-485 Port	Protocol	Armatura RS-485/OSDP/Aperio
	Baudrate	4800/9600/19200/38400/57600/115200
RS-485 Port	Protocol	Armatura RS-485/OSDP/Aperio
	Baudrate	4800/9600/19200/38400/57600/115200

Copyright © 2024 ARMATURA LLC. All rights reserved

Protocol Introduction

Protocol	Usage	Supported Devices
OSDP	For Reader/Expansion Board	AHSC1000, AHDU1X6(
Armatura RS 485	For primary and **Secondary Controller**s	AHSC1000, AHDU1X6(
Aperio	For ASSA ABLOY Aperio AH3(	AHSC1000

- Click **[OK]** to save and apply the configurations to the device.

Replace Device

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenario

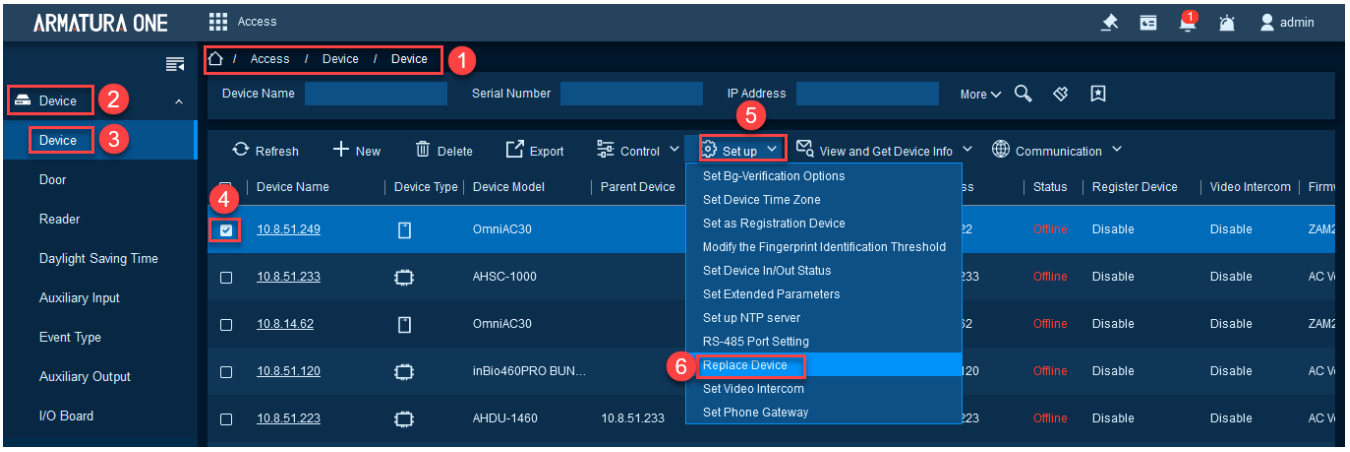
This function allows for the replacement of an old device with a new one, ensuring a seamless transition.

Trigger Result

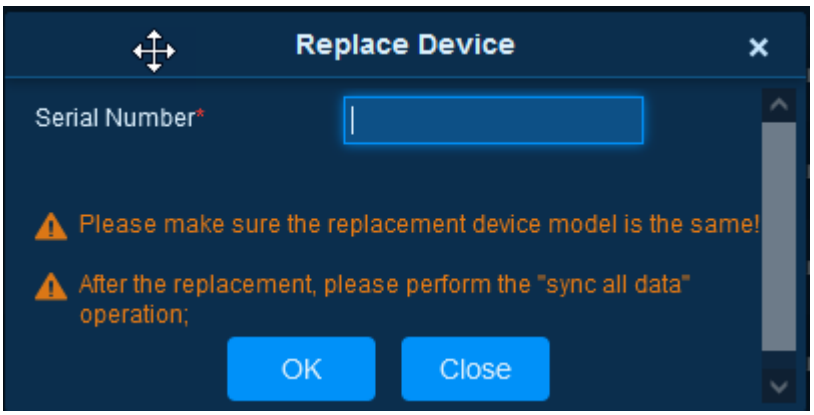
After entering the new device's serial number and completing the operation, the selected device will be successfully replaced.

Steps:

- Go to **[Access] > [Device] > [Device] > [Set up]** to access the settings page.
- Click **[Replace Device]** to open the pop-up window for device replacement settings.
- Enter the **serial number** of the replacement device in the designated field.
- Click **[OK]** to confirm and complete the replacement process.



Copyright © 2024 ARMATURA LLC. All rights reserved



Set Video Intercom

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenario

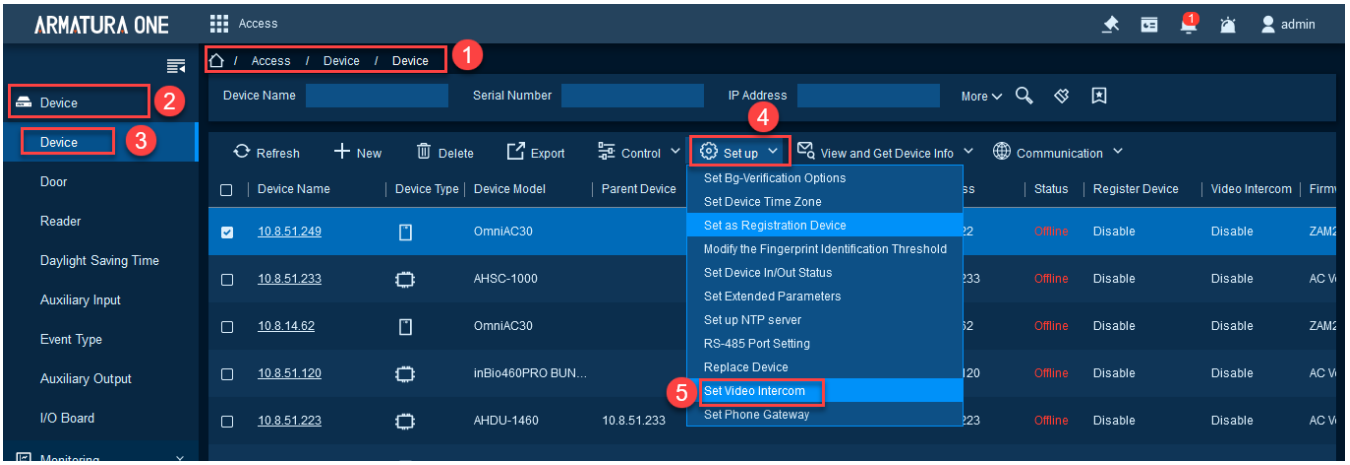
The Set Video Intercom function is used to configure video intercom functionality and mode type for the selected device.

Trigger Results

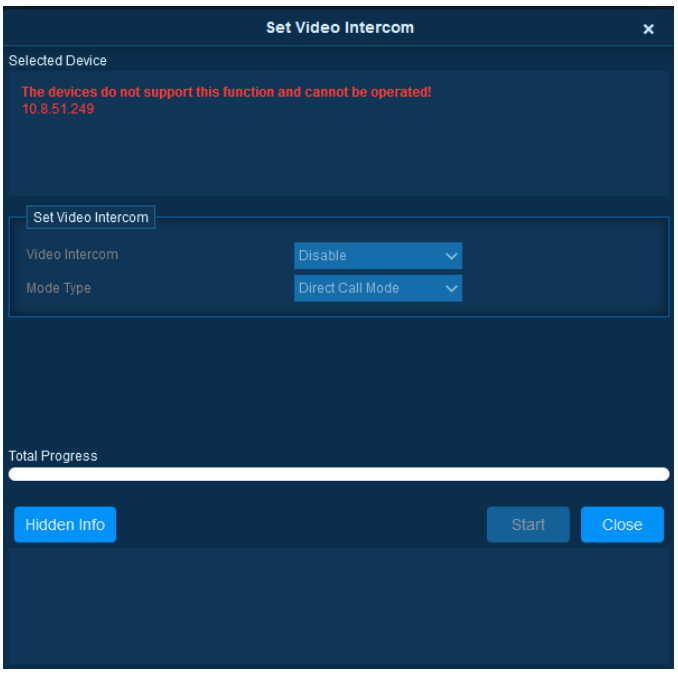
The configured device will support video intercom functionality based on the defined settings.

Steps:

- Go to **[Access] > [Device] > [Device] > [Set up]** to access the device settings page.
- Click **[Set Video Intercom]** to open the configuration pop-up window.
- Define the necessary parameters for the video intercom and select the appropriate mode type for the device.
- Click **[OK]** to save the configuration and apply the video intercom settings to the device.



Copyright © 2024 ARMATURA LLC. All rights reserved



Set Phone Gateway

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenario

The Set Phone Gateway function is used to configure and set up phone gateway parameters for the selected device.

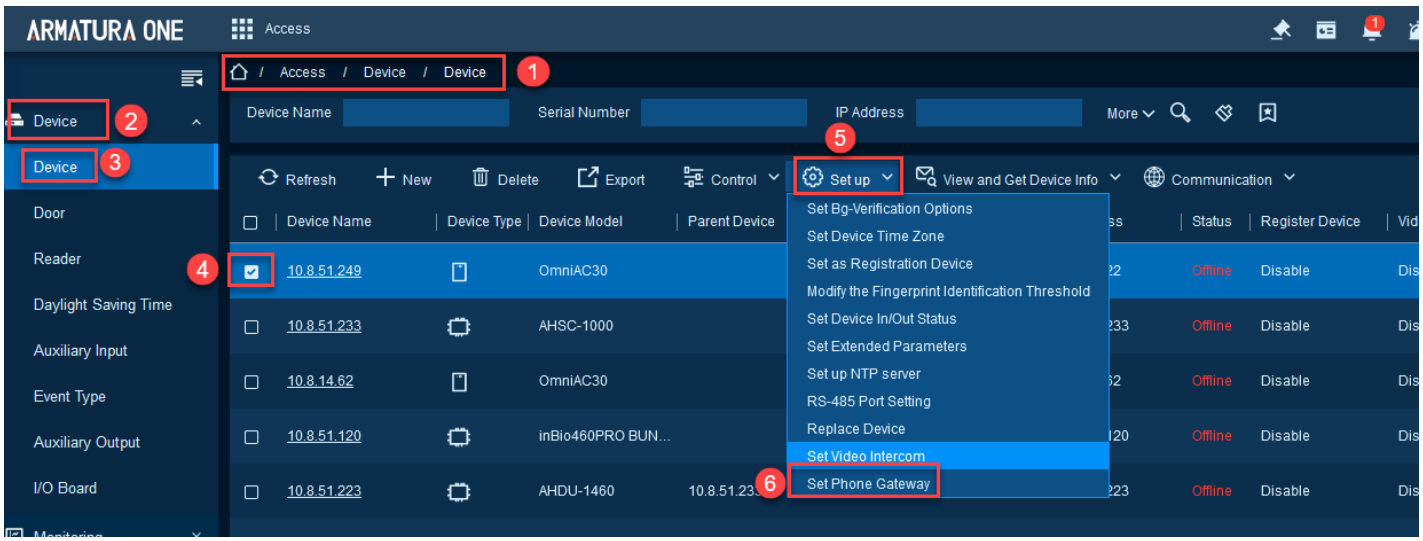
Trigger Result

The selected device will be configured with the phone gateway settings.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [Set up]** to access the device settings page.
- Click **[Get Phone Gateway]** to open the configuration pop-up window.
- Enter the required parameters for the phone gateway setup in the pop-up window.
- Click **[OK]** to save the settings and apply the phone gateway configuration to the device.

Copyright © 2024 ARMATURA LLC. All rights reserved



View and Get Device Info: Get Device Option

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

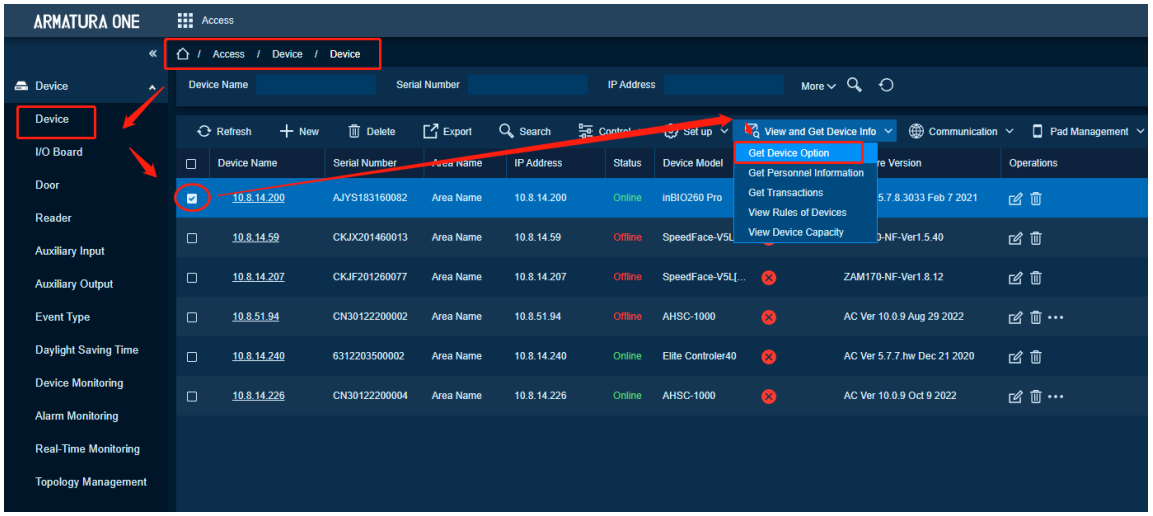
This function is used to retrieve updated device parameters and configurations. For example, after firmware updates, this function will update the firmware version and other parameters in the software.

Trigger Results

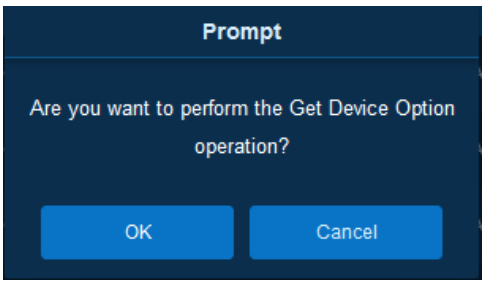
Retrieves the device's parameters, ensuring that the software has the latest device information.

Steps:

- Go to **[Access] > [Device] > [Device] > [View and Get Device Info]** to access the device information page.
- Click **[Get Device Option]**. A pop-up window will appear displaying the device's parameters.
- Click **[OK]** to retrieve and synchronize the parameters from the device to the software.



Copyright © 2024 ARMATURA LLC. All rights reserved



Get Personnel Information

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

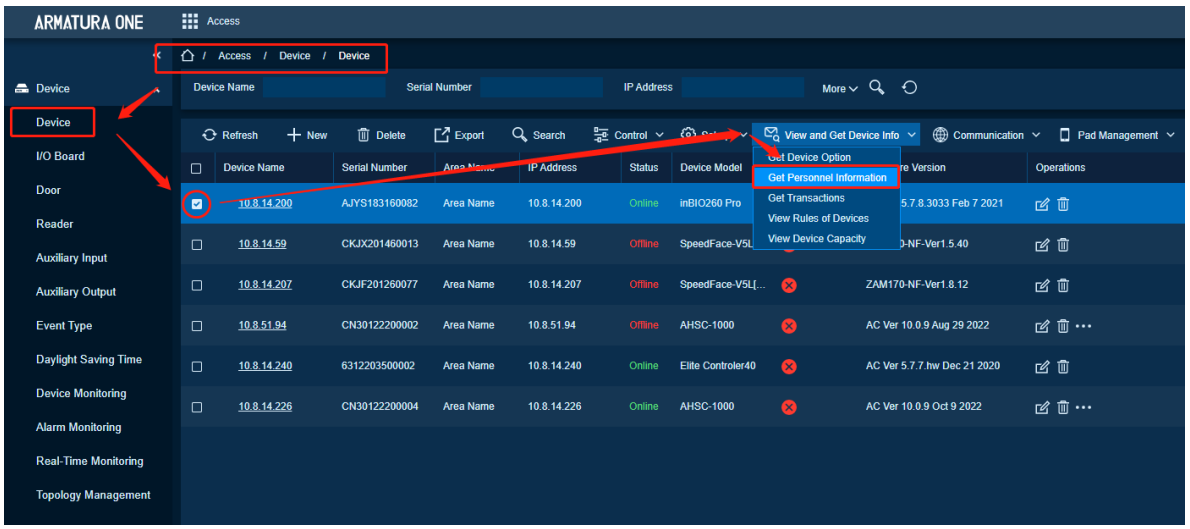
This function gets personnel information stored in the device, including personal biometric data such as fingerprints, finger veins, and facial data, and transfers it to the software. Use this function when you need to retrieve personnel data into the software.

Trigger Results

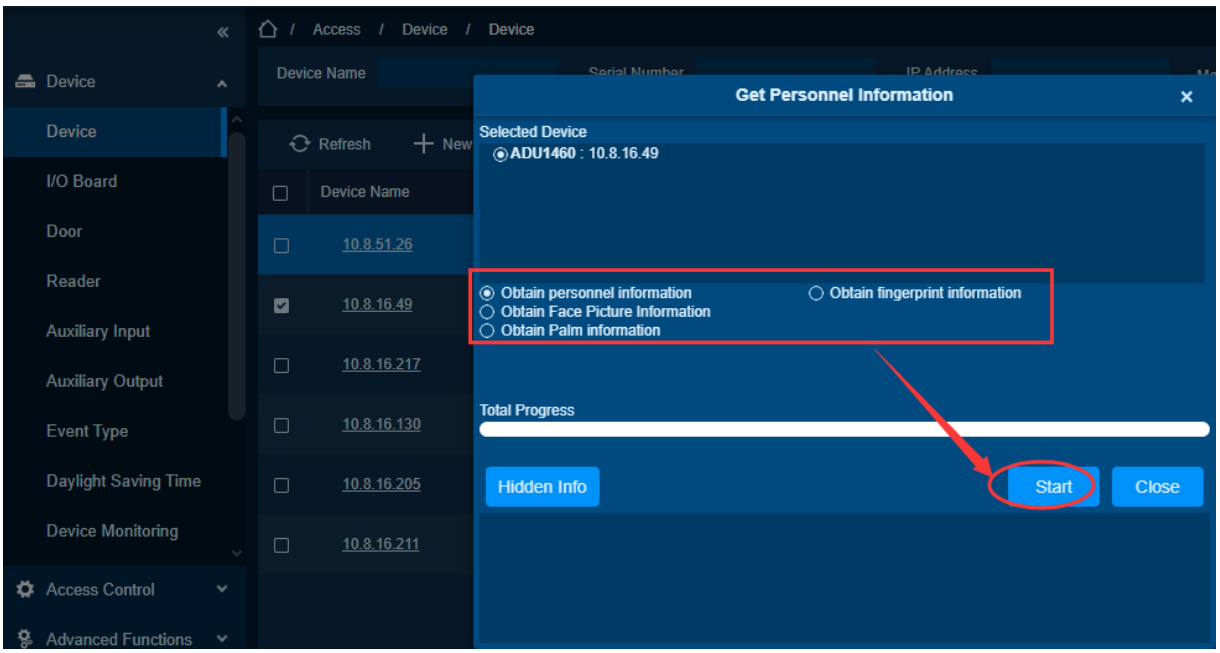
The system retrieves personnel data from the device and stores it in the software.

Steps:

- Go to **[Access] > [Device] > [Device] > [View and Get Device Info]** to access the device information page.
- Click **[Get Personnel Information]**. The system will display an interface for retrieving personnel information.
- Click **[Start]** to begin fetching personnel data from the device to the software.



Copyright © 2024 ARMATURA LLC. All rights reserved



View and Get Device Info: Get Transactions

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function pulls all transactions from the device.

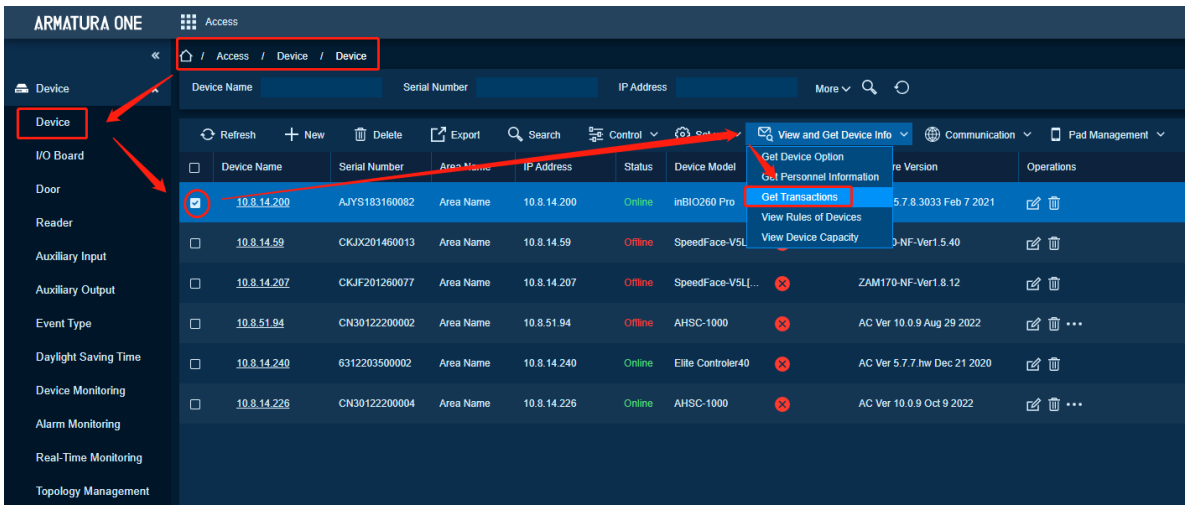
Trigger Results

All transactions stored in the device are retrieved and stored in the software report.

Steps:

- Go to **[Access] > [Device] > [Device] > [View and Get Device Info]** to access the device information page.
- Click **[Get Transactions]** to open the interface for event record retrieval.
- On the **Get Transactions** interface, choose one of the following options:

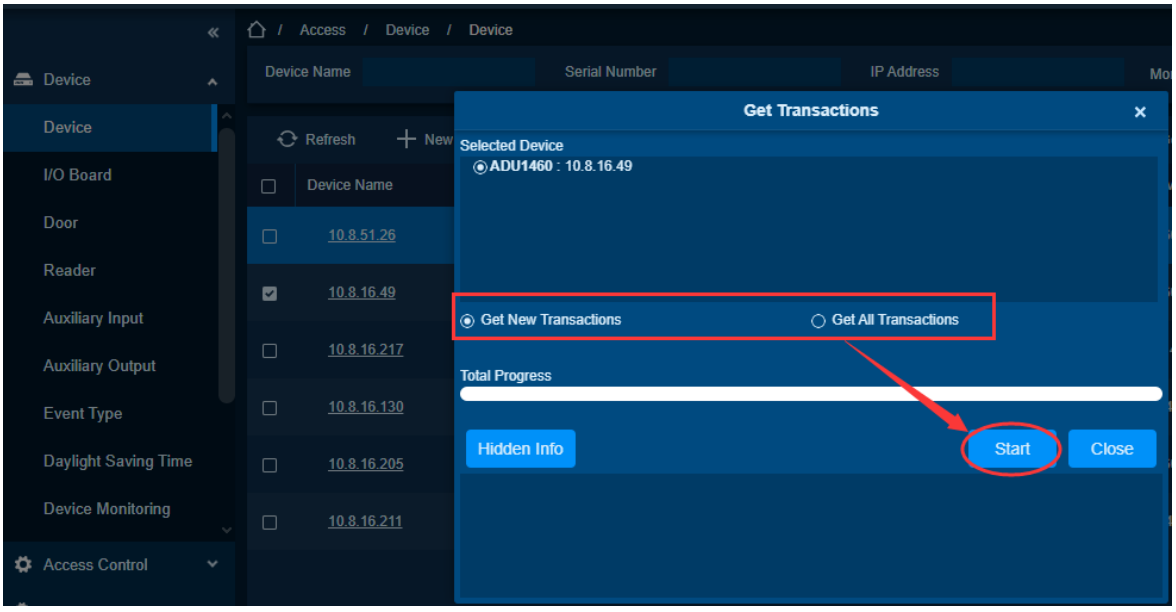
Copyright © 2024 ARMATURA LLC. All rights reserved



Get All Transactions: Retrieve all event records stored in the device.

Get New Transactions: Retrieve only new event records added since the last synchronization.

- Click **[Start]** to fetch the selected records into the software.



Note:

Real-time Communication: If the network and communication between the system and the device are functioning correctly, event records will be retrieved in real-time and saved in the database.

Manual Retrieval: In case of communication interruptions, use this function to manually retrieve event records from the device.

Automatic Synchronization: The system will automatically retrieve event records from the device daily at 00:00 unless configured otherwise.

Device Storage Limits: Access control devices can store up to **100,000 event records**. Once the record count exceeds **10,000**, the device will automatically delete the earliest records to free up space (default configuration). Ensure the device's event log settings align with system requirements to avoid losing critical event data.

Copyright © 2024 ARMATURA LLC. All rights reserved

View Rules of Devices

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device is online.

Usage Scenarios

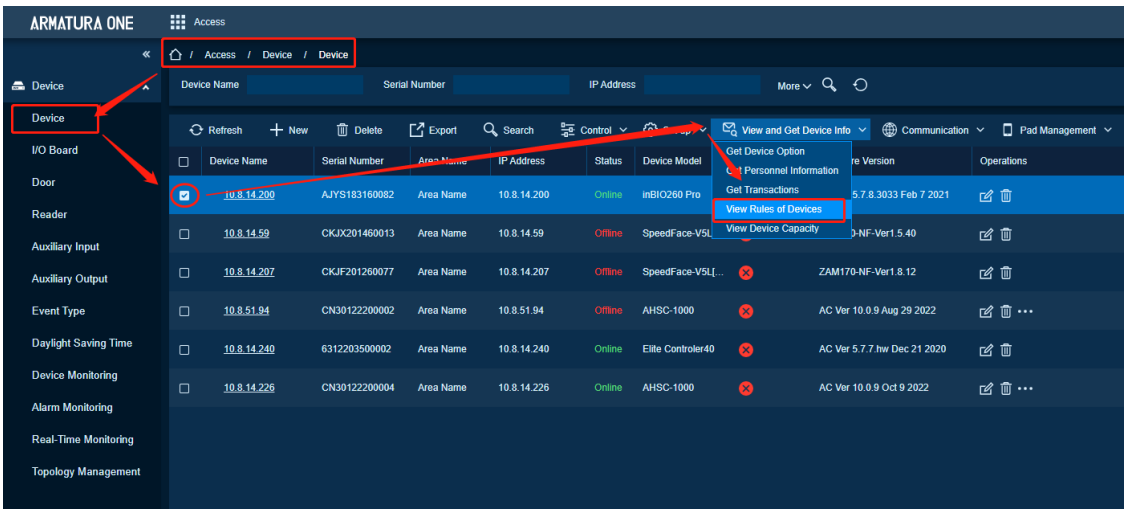
This function is used to review the access control rules configured on the connected device. It helps ensure that the access control rules are consistent with system policies and requirements.

Trigger Results

Displays the access control rules set on the device for review and verification.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [View and Get Device Info]**.
- On the device information page, click **[View Rules of Devices]**.
- The system will display the access control rules configured in the selected device.
- Exit the interface when finished reviewing by closing the Access Control Rules interface.



View Device Capacity

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device is online.

Usage Scenarios

This function is used to verify that the data on the device matches the data in the software. It also allows you to check the device's storage capacity for personnel records, fingerprints, and other data types.

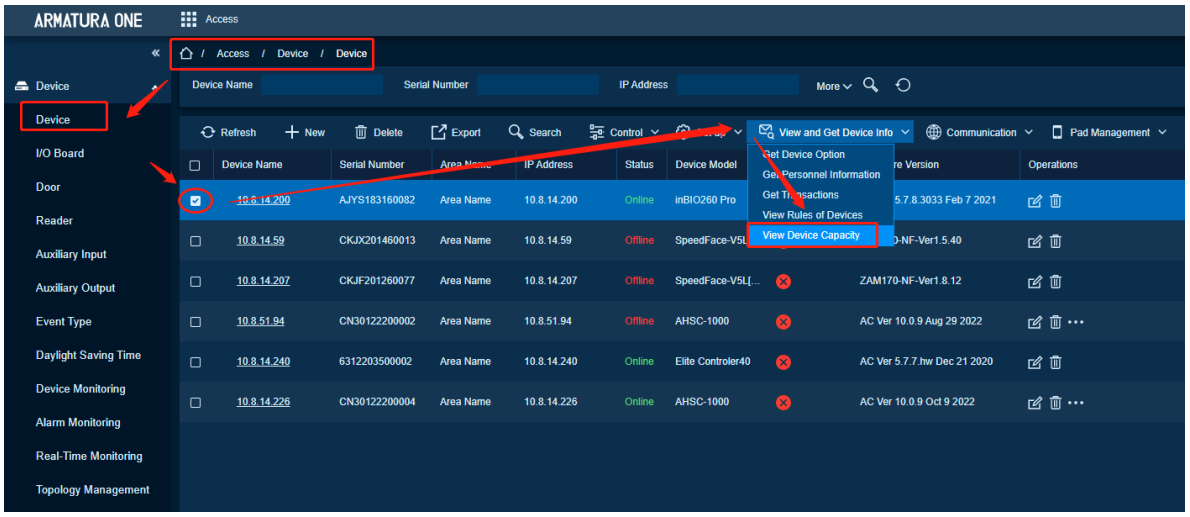
Copyright © 2024 ARMATURA LLC. All rights reserved

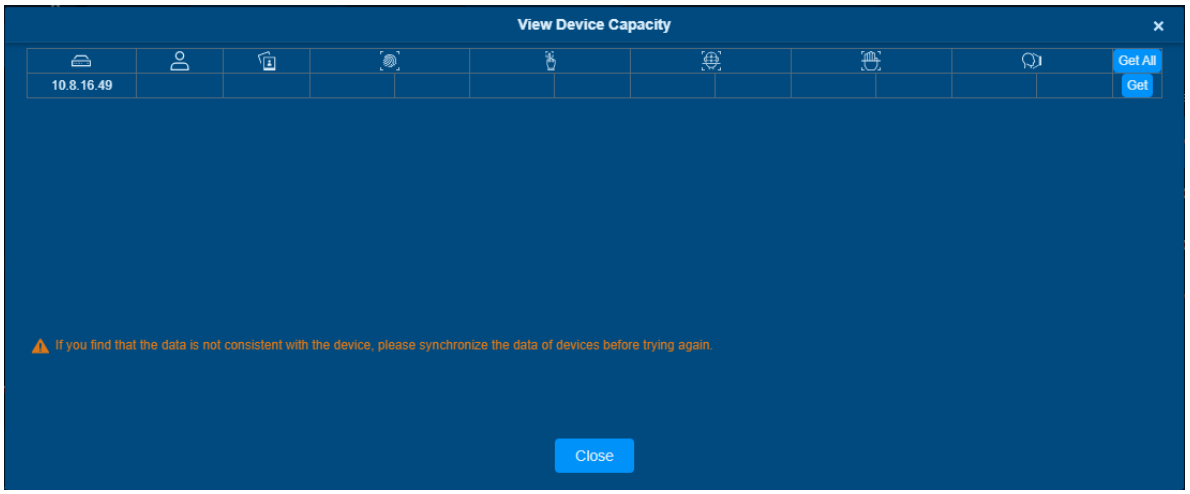
Trigger Result

Displays the capacity of each data type, such as personnel records, fingerprints, and other related information.

Steps:

- Navigate to **[Access] > [Device] > [Device] > [View and Get Device Info]**.
- On the information page, click **[View Device Capacity]**.
- A pop-up interface displaying device capacity details will appear.
- Click **[View]** to check specific data types individually.
- Click **[View All]** to retrieve and display all capacity data at once.
- Compare the retrieved data with the information stored in the software to ensure consistency.





Communication Settings: Modify IP Address

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device is online.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

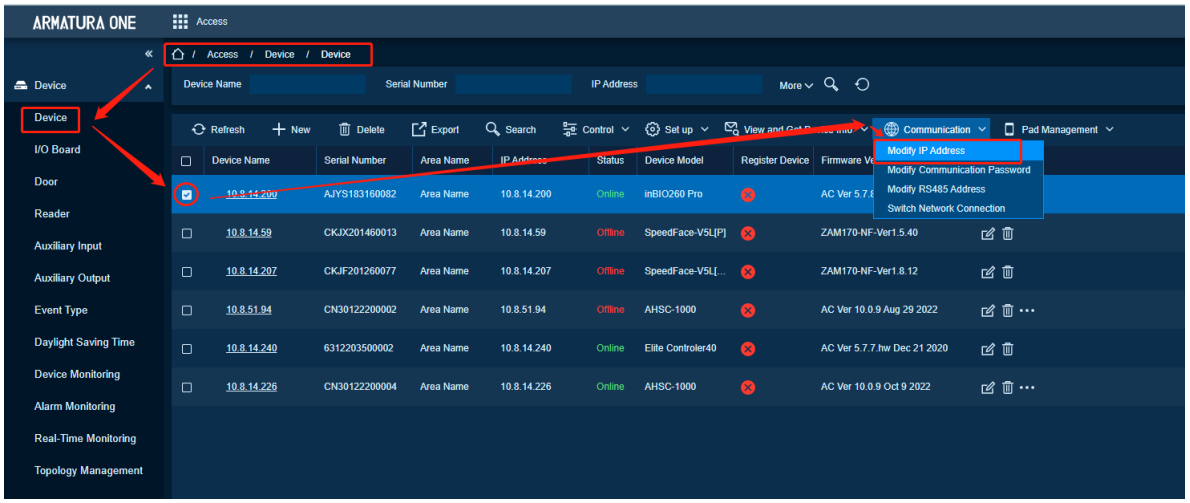
This function is used when the device requires an IP address change.

Trigger Result

The device's IP address is updated.

Steps:

- Click **[Access]** > **[Device]** > **[Device]** > **[Communication]** to open the view page.
- Select **[Modify IP Address]**.
- The system will redirect you to the IP address modification interface.
- Enter the new IP Address.
- Ensure the Gateway and IP Address are within the same network segment.
- Confirm the settings by clicking **[OK]** to apply and synchronize the updated IP address.



Note:

Misconfigured IP addresses can result in loss of communication with the device.

Modify Communication Password

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device is online.

Usage Scenarios

This function is used to change or update the device's communication password. If the communication password between the device and the software is inconsistent, the connection will fail.

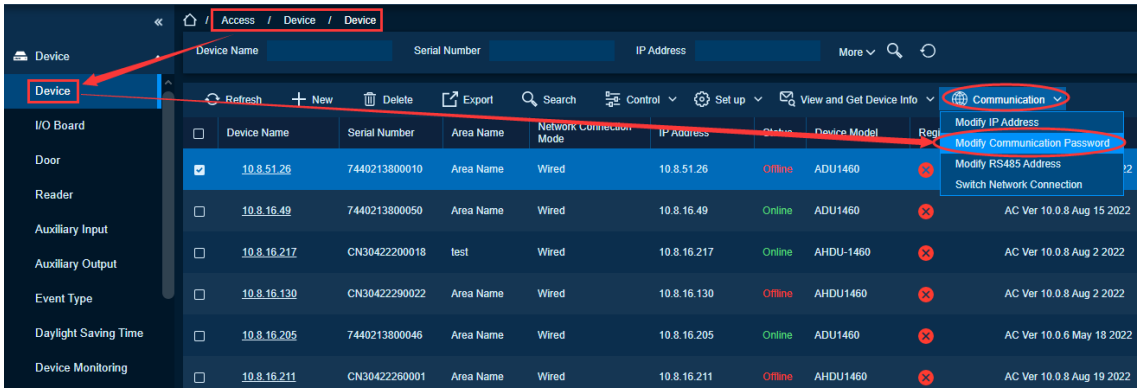
Trigger Result

The device’s communication password is updated in the system.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Click **[Access] > [Device] > [Device] > [Communication]** to open the view page.
- Select **[Modify Communication Password]** to proceed to the modification interface.
- Input the new communication password and confirm the changes.
- Click **[OK]** to apply the new password and synchronize it with the system.



Modify RS485 Address

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

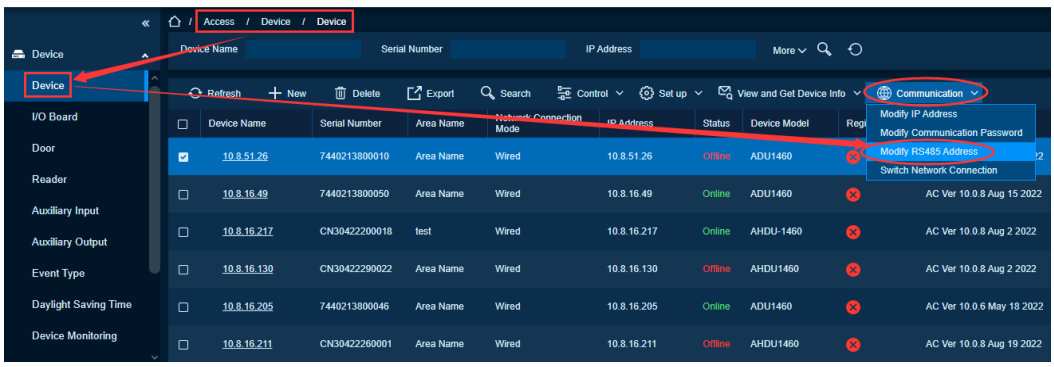
This function is used to modify the RS485 address of devices that communicate via RS485 and do not have an RS485 DIP switch.

Trigger Result

Updates the RS485 address of the device in the system.

Steps:

- Click **[Access] > [Device] > [Device] > [Communication]** to open the view page.
- Select **[Modify RS485 Address]** to proceed to the modification interface.
- Input the new RS485 address.
- Click **[OK]** to apply the changes and synchronize the RS485 address.



Copyright © 2024 ARMATURA LLC. All rights reserved

- Only devices without a DIP switch and using RS485 communication can have their addresses modified. Ensure the configuration aligns with the connected devices to avoid communication issues.

Switch Network Connection

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device is online.

Usage Scenarios

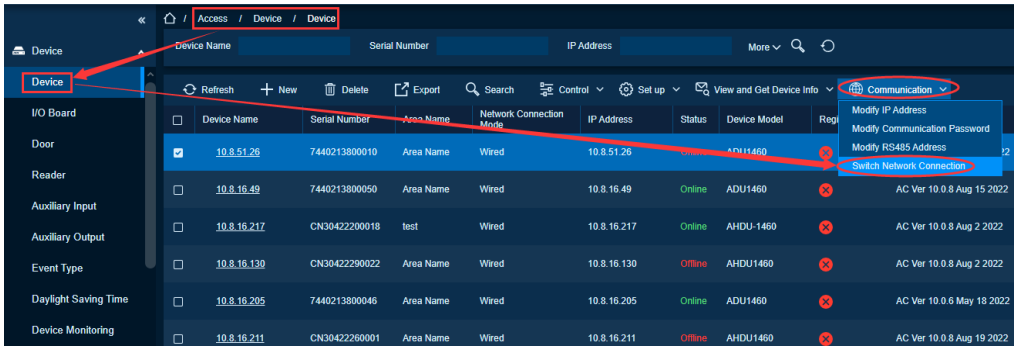
This function is used to switch between different network connection modes for the device to suit system requirements. It also allows for viewing and verifying the system parameters for network connections.

Trigger Result

The device's network connection mode is updated in the system.

Steps:

- Click **[Access] > [Device] > [Device] > [Communication]** to open the view page.
- Select **[Switch Network Connection]** to proceed to the configuration interface.
- Choose the appropriate mode for the device based on the system requirements.
- Confirm the settings by clicking **[OK]** to apply and synchronize the new connection mode.



Note:

If the **Control Panel Type** is not detected, delete the device manually and re-add it with the correct configuration.

If the device **[Control Panel Type]** is incorrect, manually delete the device and add it again.

* Ensure all mandatory fields (*) are correctly filled during configuration to prevent connection issues.

Copyright © 2024 ARMATURA LLC. All rights reserved

Add Sub-Device

Prerequisites for Use

Log into the system using an account with the required permissions. The **Primary Controller** must already be added successfully. This function is only supported for the AHSC-1000 device.

Usage Scenarios

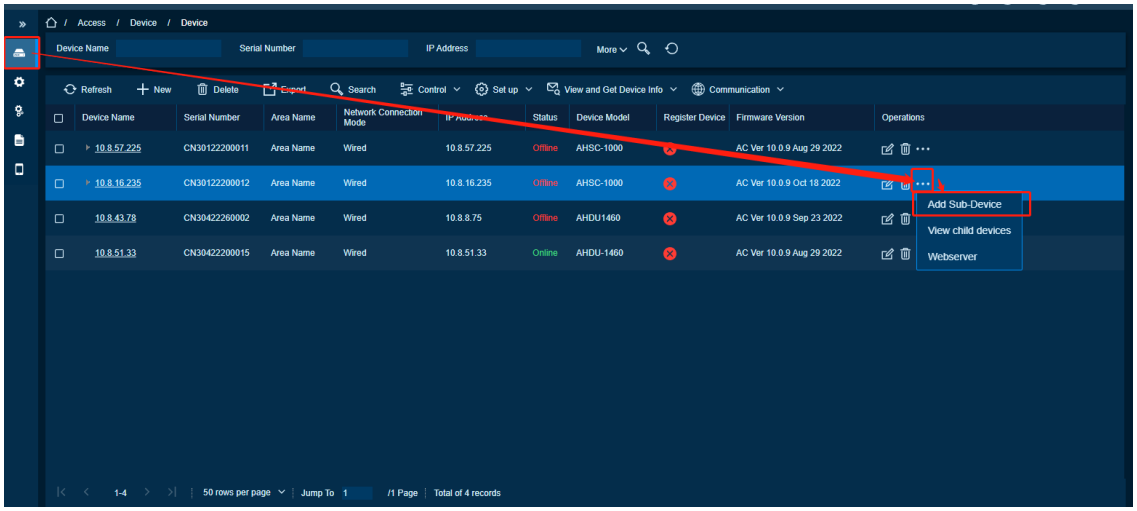
This function is used to add a **Secondary Controller** after the **Primary Controller** has been successfully set up.

Trigger Results

The primary-secondary relationship is established between controllers. Communication commands between the software and the panel will be sent only to the **Primary Controller**, which will then distribute the commands to the linked **Secondary Controller**s.

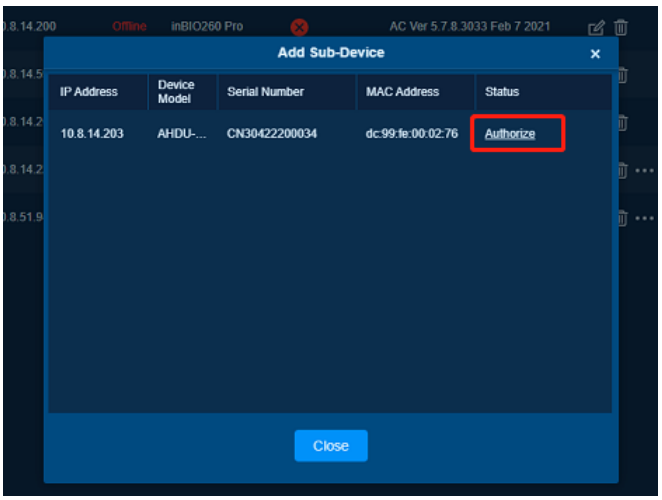
Steps:

- Navigate to **[Access]** > **[Device]** > **[Device]** to view the device list.
- Click the three dots menu **[…]** next to the **Primary Controller** and select **[Add Sub-Device]**.

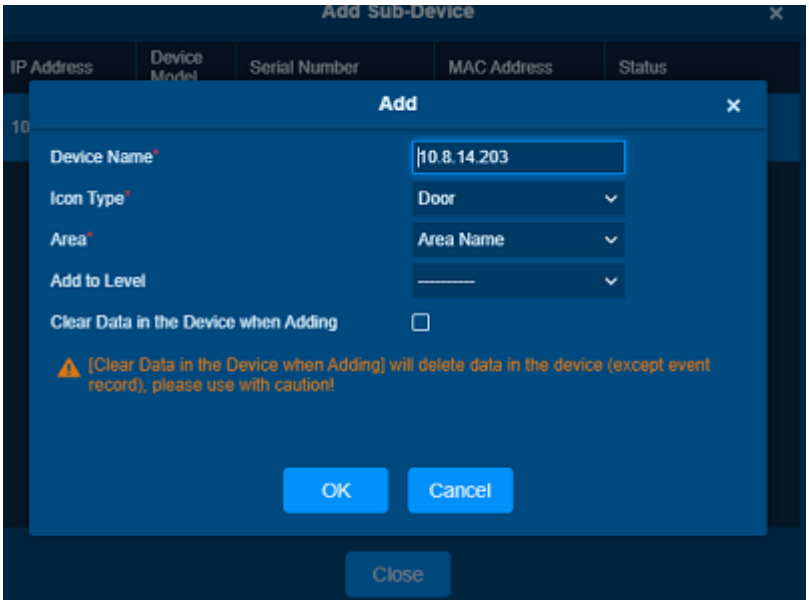


- In the Add Sub-Device page, click **[Authorize]** to connect the sub-device to the **Primary Controller**.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Click **[OK]** to save the configuration.



View Sub-Device [View Child Devices]

Prerequisites for Use

Log into the system using an account with the required permissions. The **Primary Controller** must already be added. This function is only supported for the AHSC-1000 device.

Usage Scenarios

This function is used to view the primary-secondary relationship between controllers.

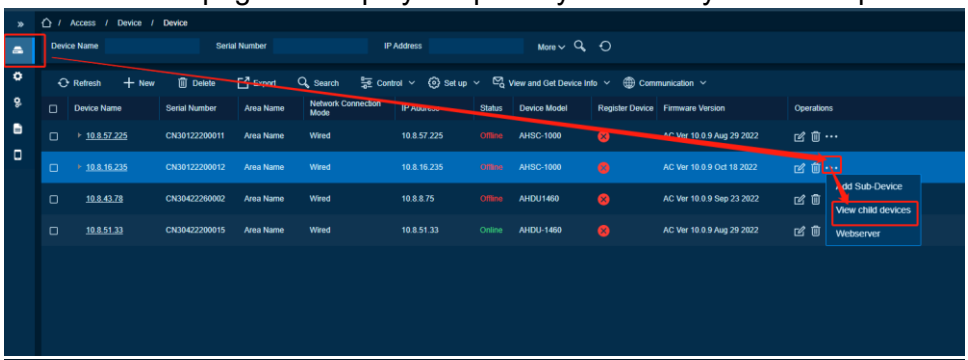
Trigger Result

Display details of the sub-device relationship.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access] > [Device] > [Device]** to view the device list.
- Click the three dots menu **[…]** next to the **Primary Controller** and select **[View Sub-Device/Child Devices]**.
- The **Add Sub-Device** page will display the primary-secondary relationship details.



Webserver

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function is used to access the webserver of the controller for configuration or monitoring.

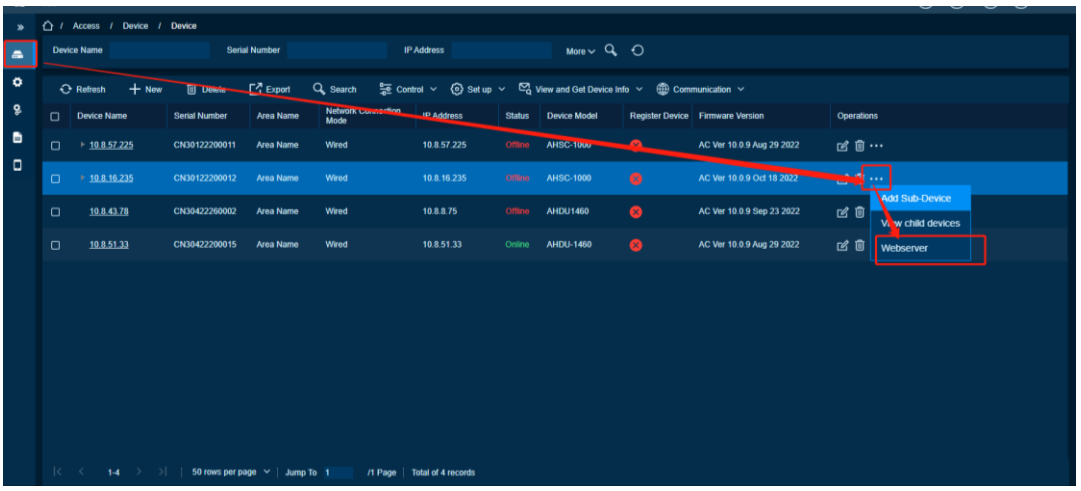
Trigger Results

The controller's webserver opens in a new browser tab or window.

Steps:

- Click **[Access] > [Device] > [Device]** to open the device list view.
- Click **[Webserver]** next to the desired device in the list.
- The controller's webserver interface will open in a new tab or window in your browser.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.1.2. I/O Board

Function Description

The I/O expansion board enables the expansion of the number of Auxiliary Inputs and Outputs that can be operated within the system.

New Device

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

When additional Inputs or Outputs need to be added to the current system.

Trigger Results

Adding additional Inputs and Outputs to the device.

Steps:

Parameter		Introduction
Name*		Editable field to set the name of the I/O Board .
Device Name*		Read-only field; select the target device.
Protocol Type*		Editable drop-down menu with options: OSDP/Aperio.
I/O Board Type*		Editable drop-down menu: If OSDP, options include AHEB0216, 1602, 0808. If Aperio, the option is AH30.
OS	RS-485 Port*	Editable; select the RS-485 Port based on the protocol.
	RS-485 Address*	Editable; range is 1–255.
Ap	Device Addressing Mode*	Select from Normal Address Offset or Legacy Address Offset.
	RS-485 Port*	Editable; select the RS-485 Port based on the protocol.
	RS-485 Address*	Editable; range is 1–15.

Copyright © 2024 ARMATURA LLC. All rights reserved

Aperio Devices

Prerequisites for Use

Log into the system with an account that has the required permissions and ensure the Aperio AH30 hub is connected via the AHSC-1000 using RS-485.

Usage Scenarios

This function allows you to connect Aperio devices for managing wireless locks.

Trigger Results

Virtual I/O boards are created in the **[I/O Board]** module.

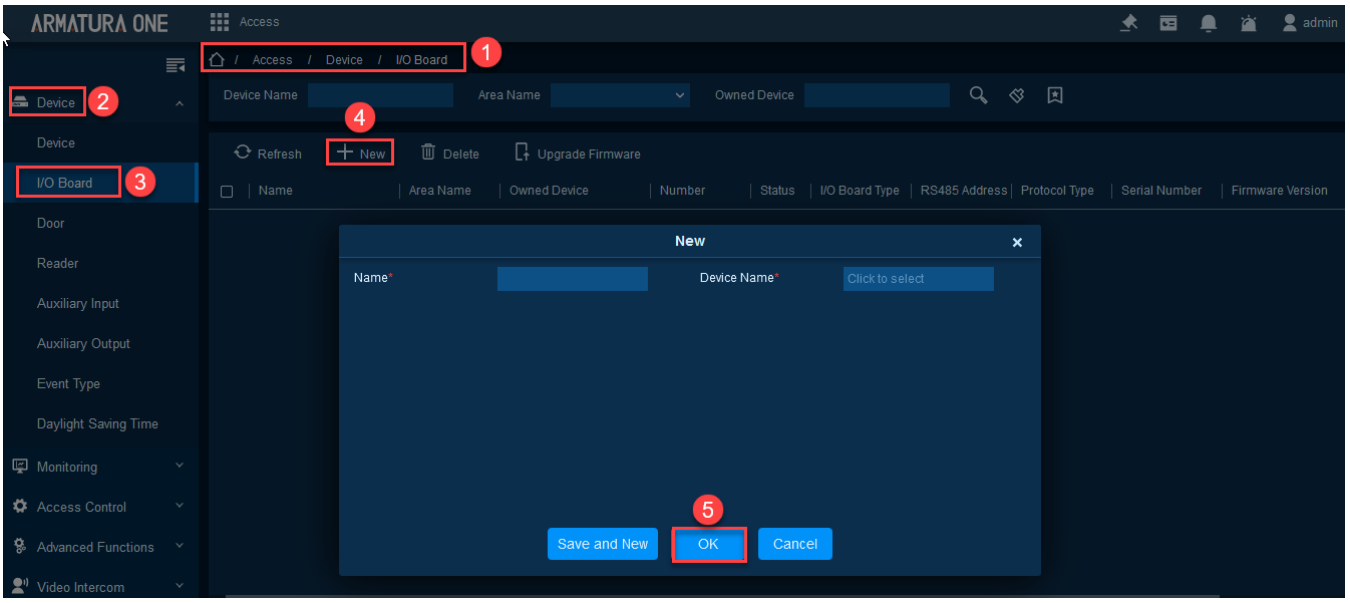
Corresponding virtual doors are added in the **[Door]** module.

Limitations

Only supported on AHSC-1000 modules.

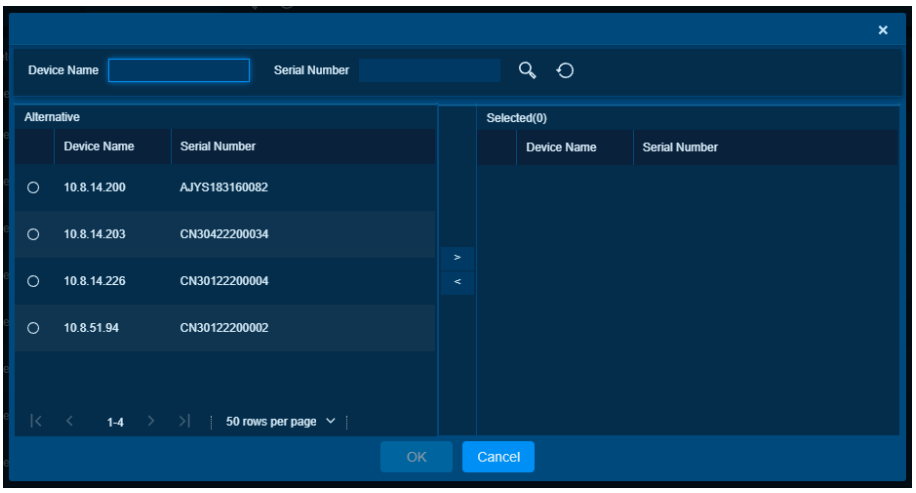
Steps:

- Navigate to **[Access]** > **[Device]** > **[I/O Board]** > **[New]** to open the new device interface.
- Fill in the name field.



- Click on Device Name to open the device selection window and select a target device.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Choose the Device Addressing Mode (Normal Address Offset or Legacy Address Offset).

Addressing table – normal address offset

An AH30 communication hub can pair with up to 8 locks. When pairing several locks to a communication hub, the following addresses are used for the address range 1-15. Above this range only one lock can be paired.

DIP 4 – DIP 1	AH30 Hub address	Lock addresses
0000		Reserved
0001	0x01	0x01, 0x11, 0x21, 0x31, 0x41, 0x51, 0x61, 0x71
0010	0x02	0x02, 0x12, 0x22, 0x32, 0x42, 0x52, 0x62, 0x72
0011	0x03	0x03, 0x13, 0x23, 0x33, 0x43, 0x53, 0x63, 0x73
0100	0x04	0x04, 0x14, 0x24, 0x34, 0x44, 0x54, 0x64, 0x74
0101	0x05	0x05, 0x15, 0x25, 0x35, 0x45, 0x55, 0x65, 0x75
0110	0x06	0x06, 0x16, 0x26, 0x36, 0x46, 0x56, 0x66, 0x76
0111	0x07	0x07, 0x17, 0x27, 0x37, 0x47, 0x57, 0x67, 0x77
1000	0x08	0x08, 0x18, 0x28, 0x38, 0x48, 0x58, 0x68, 0x78
1001	0x09	0x09, 0x19, 0x29, 0x39, 0x49, 0x59, 0x69, 0x79
1010	0x0A	0x0A, 0x1A, 0x2A, 0x3A, 0x4A, 0x5A, 0x6A, 0x7A
1011	0x0B	0x0B, 0x1B, 0x2B, 0x3B, 0x4B, 0x5B, 0x6B, 0x7B
1100	0x0C	0x0C, 0x1C, 0x2C, 0x3C, 0x4C, 0x5C, 0x6C, 0x7C
1101	0x0D	0x0D, 0x1D, 0x2D, 0x3D, 0x4D, 0x5D, 0x6D, 0x7D
1110	0x0E	0x0E, 0x1E, 0x2E, 0x3E, 0x4E, 0x5E, 0x6E, 0x7E
1111	0x0F	0x0F, 0x1F, 0x2F, 0x3F, 0x4F, 0x5F, 0x6F, 0x7F

When configuring installations that differ from the default configuration described in section DIP 1-5 – Selecting the EAC address/Automatic paring on page 38, use this table to keep track of what addresses are used by the locks/sensors in your installation in order to avoid addressing conflicts according to section "*Installation examples" on page 44* for mixed installations.

Aperio® Online Mechanical Installation Guide, Document No: ST-001323-E Date: 30 mars 2016

- Legacy Address Offset.

Addressing table – legacy address offset

Legacy addressing mode is an alternative addressing mode that can be set by the Programming Application in the configuration wizard. The lock addresses in this mode are set consecutively. For example, if communication hub has address 1, the locks will get address 1-8, 9-16, 17-24 etc.

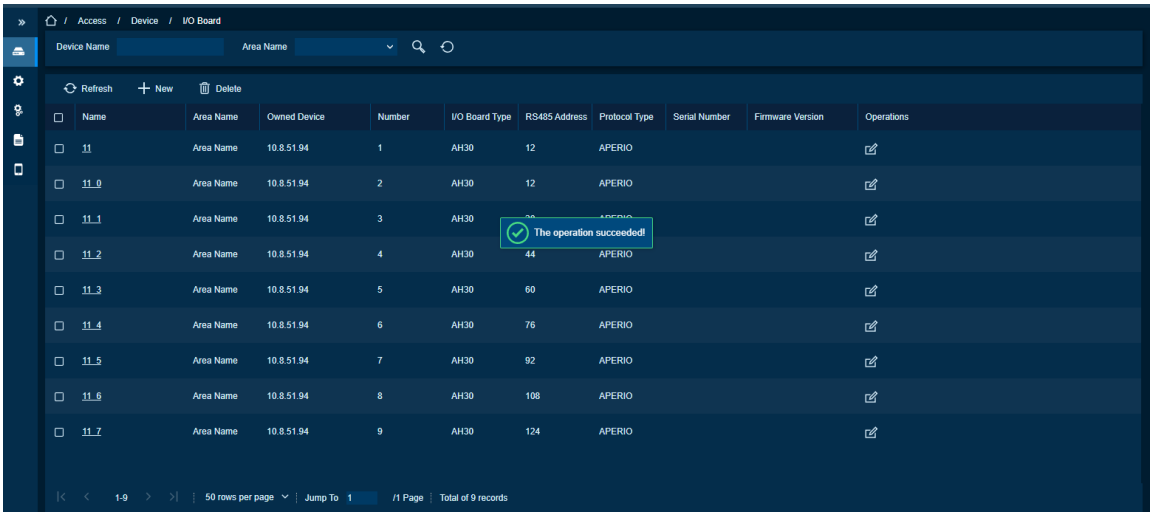
DIP 5 – DIP 1	AH30 Hub address	Lock addresses
0000		Reserved
0001	0x01	0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08
0010	0x02	0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x10
0011	0x03	0x11, 0x12, 0x13, 0x14, 0x14, 0x16, 0x17, 0x18
0100	0x04	0x19, 0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F, 0x20
...		

This mode is used for older EAC systems that cannot handle high EAC addresses where the limit for example is 32 or 64.

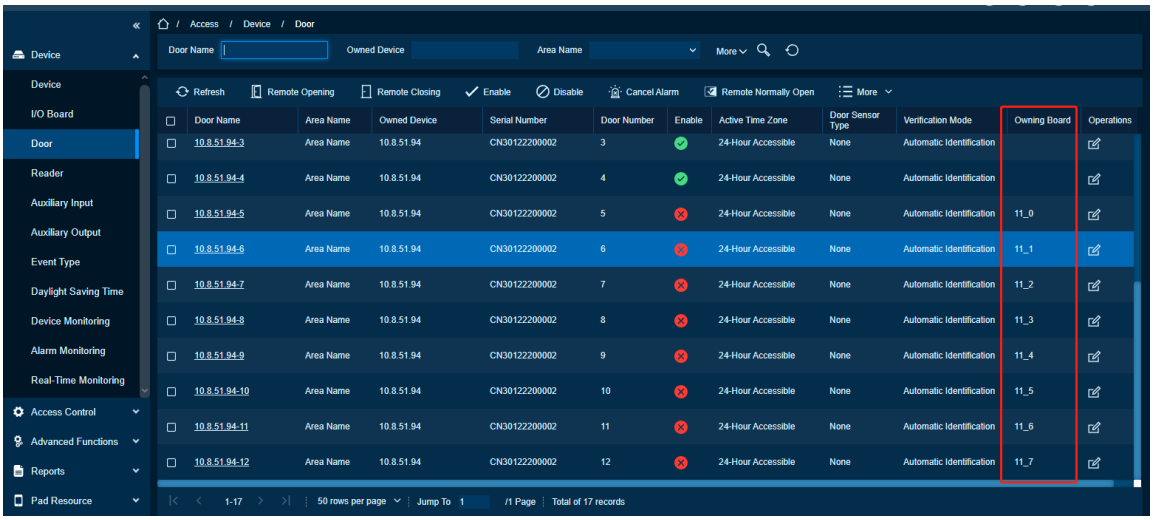
Copyright © 2024 ARMATURA LLC. All rights reserved

Picture regards from ST-001323-Aperio Online Mechanical Installation Manual-E-US.pdf

- Configure the RS-485 Port and verify that the protocol matches the port settings.
- Enter the RS-485 Address (range: 1–15).
- Click OK to save.
- The system will automatically generate virtual devices under the **[I/O Board]** module.



- Auto-generate doors linked to the virtual devices.



AHEB0216/0808/1602

Prerequisites for Use

Log into the system using an account with the required permissions. Connect the AHEB0216, 0808, or 1602 board via RS-485 to the AHSC-1000.

Usage Scenarios

Add auxiliary inputs and outputs to manage external devices.

Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Results

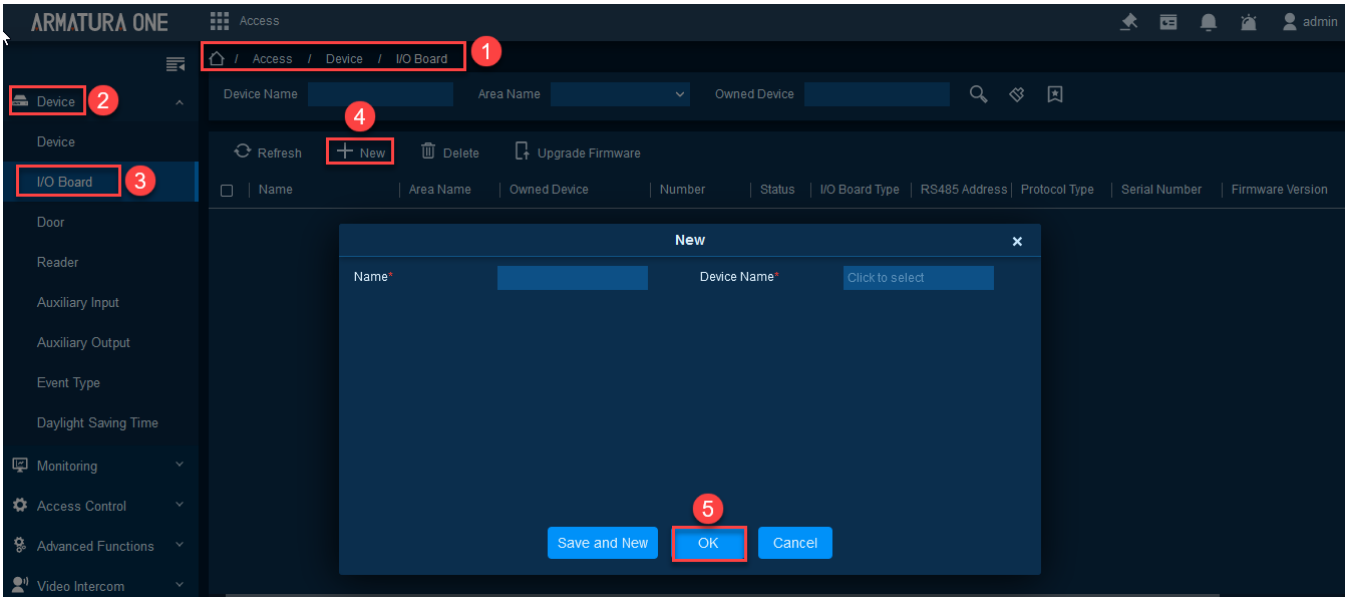
Auxiliary inputs and outputs are created under the **[Auxiliary Input]** and **[Auxiliary Output]** modules, respectively.

Limitations

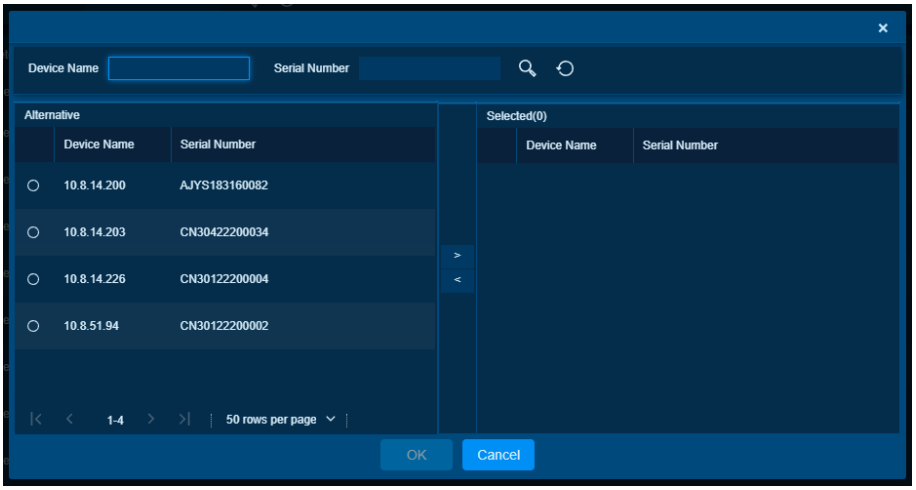
Supported only on AHSC-1000 and AHDU-1X60 controllers.

Steps:

- Navigate to **[Access]** > **[Device]** > **[I/O Board]** > **[New]** to access the setup page.
- Complete the necessary parameters and click OK.



- Select the Device Name and confirm the target device.



- Choose the appropriate RS-485 Port and verify it matches the protocol.
- Set the RS-485 Address (range: 1–255).
- Save the configuration by clicking OK.

Copyright © 2024 ARMATURA LLC. All rights reserved

Delete Device

Prerequisites for Use

Log into the system using an account with the required permissions. The I/O Board is already added to the expansion list.

Usage Scenarios

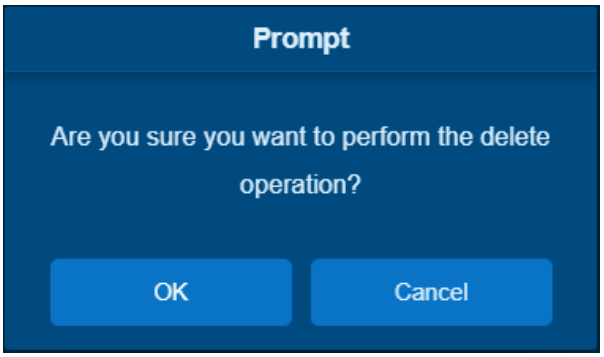
When the device is no longer needed in the current area.

Trigger Result

The selected I/O Board is deleted.

Steps:

- Navigate to **[Access Control Device]** > **[I/O Board]** > **[Delete]** to open the delete interface.
- Confirm the deletion by clicking OK.



Upgrade Firmware

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Upgrade the firmware of the selected I/O Board to enable new features or fixes.

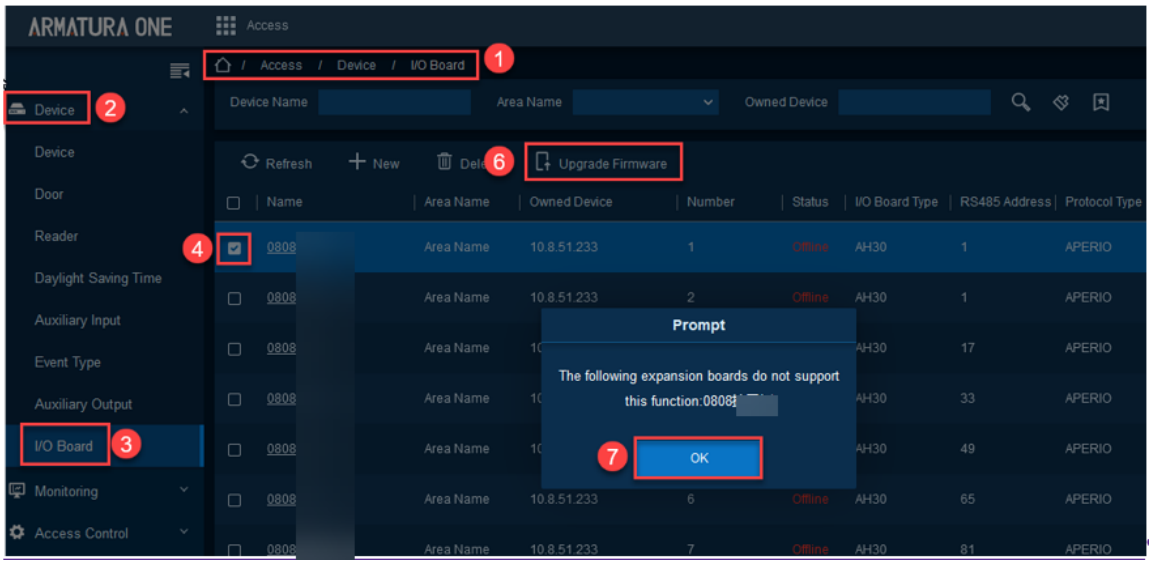
Trigger Results

The firmware is updated successfully.

Steps:

- Navigate to **[Access]** > **[Device]** > **[I/O Board]**.
- Select the I/O Board and click Upgrade Firmware.
- Follow the prompts and click OK to initiate the upgrade.

Copyright © 2024 ARMATURA LLC. All rights reserved



.

Edit

Prerequisites for Use

Log into the system using an account with the required permissions and the I/O Board is already added.

Usage Scenarios

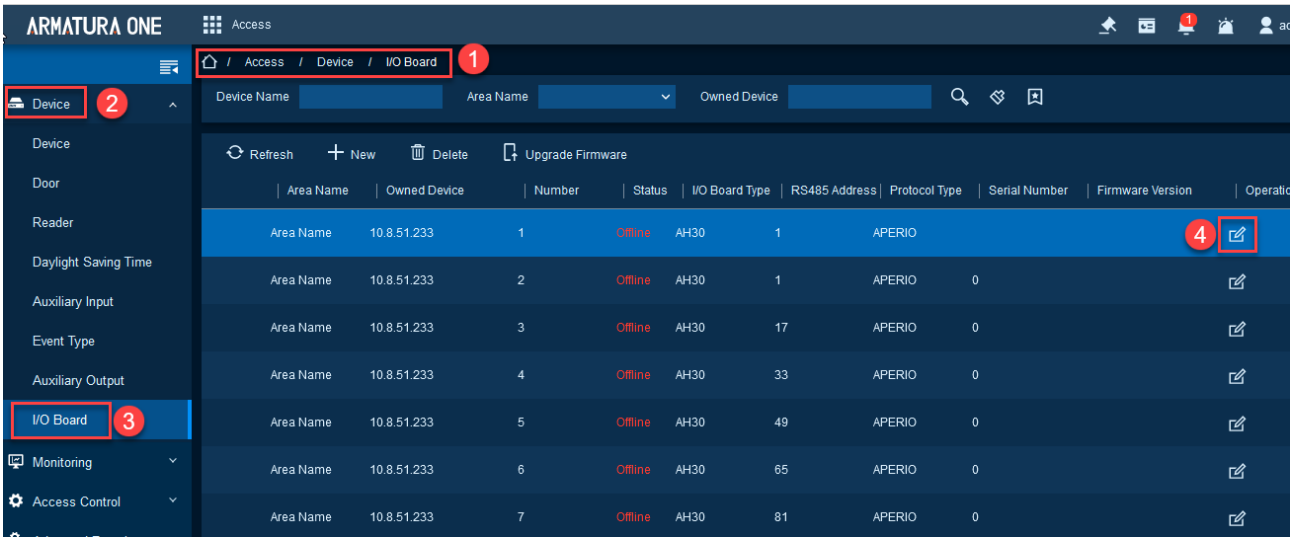
Update or modify parameters and configuration details for the selected I/O Board.

Trigger Result

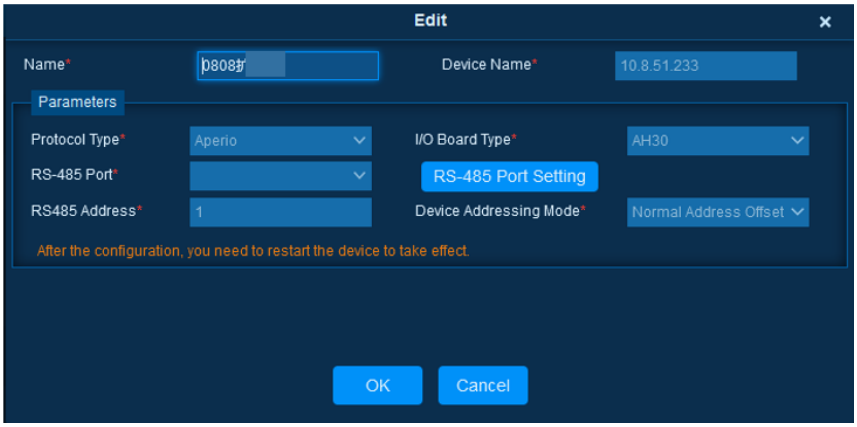
The new configuration is saved and applied.

Steps:

- Navigate to **[Access]** > **[Device]** > **[I/O Board]** to access the management interface.
- Select the desired I/O Board and edit the required parameters.
- Save the changes by clicking OK.



Copyright © 2024 ARMATURA LLC. All rights reserved



6.1.3. Door

Function Description

Operate and manage device doors, including remote operations, enabling/disabling doors, and configuring door parameters.

Edit Door

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device has been successfully added to the system.

Usage Scenarios

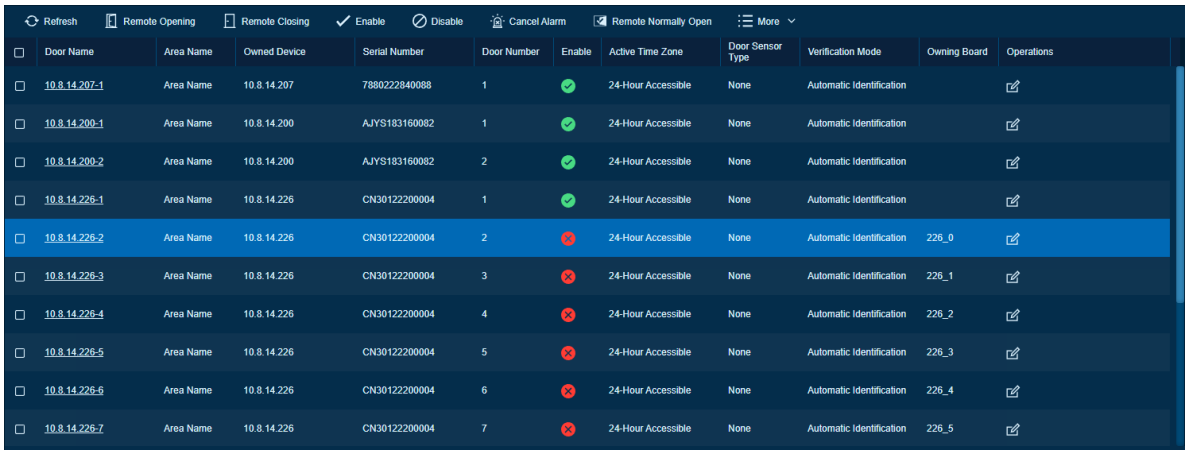
Modify parameters or update door configurations as needed.

Trigger Results

Changes to the door configuration are applied.

Steps:

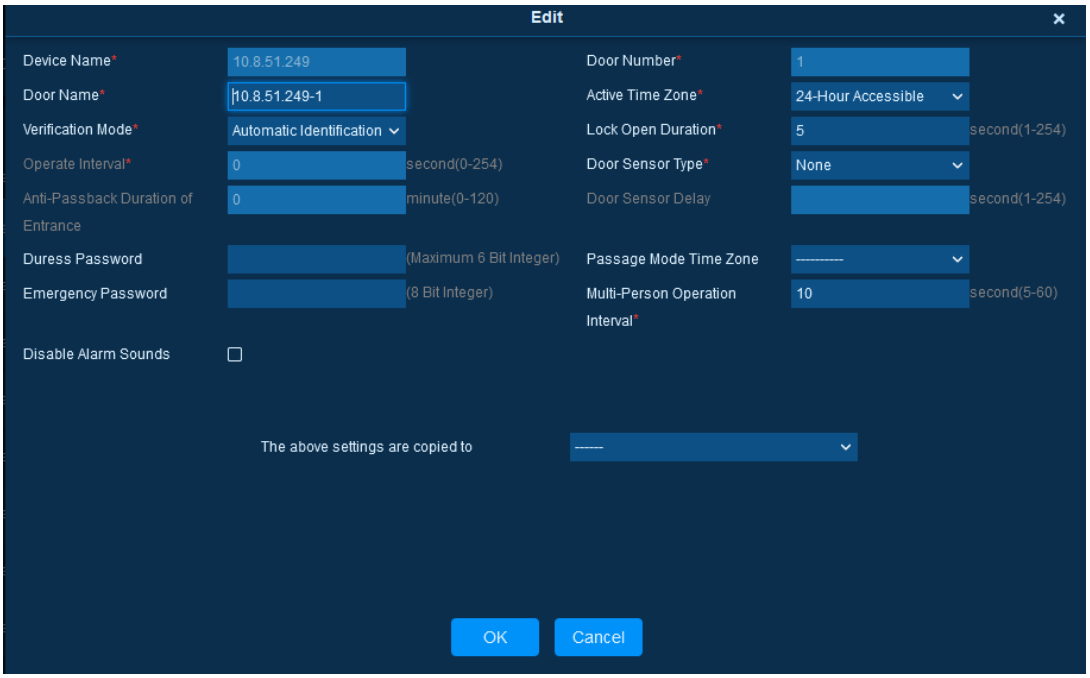
- Navigate to **[Access] > [Device] > [Door]** to enter the Door Management interface.
- The system filters and displays access devices within the selected area.



Copyright © 2024 ARMATURA LLC. All rights reserved

OmniAC Series

Select the desired door and click **[Door Name]** or the **[Edit]** button to open the editing interface.



Fields Overview:

Device Name: Displays the device name. This field is non-editable and can only be modified through the device settings.

Door Number: This field indicates the door number and is non-editable. The numbering starts from 1. For OmniAC readers, a single-door device has a default value of "1."

Door Name: This field is editable and initially defaults to "Device Name - Door Number." You can rename it, with a maximum character limit of 30.

Active Time Zone: Defines the operating schedule for the door. By default, it is set to **"24-Hour Accessible"**, meaning the reader is available for access at all times.

Passage Mode Time Zone: Passage Mode ensures that the door remains open during the selected time frame. This time zone range must be set within the Active Time Zone, and by default, it is set to "----," meaning there is no designated passage time. Additionally, if an admin user performs five consecutive verifications within five seconds, the door will exit Passage Mode and return to the closed state. If five more verifications are made during the passage time, the door will re-enter Passage Mode. This functionality is effective only during the Active Time Zone; outside of this period, other Passage Mode triggers, including the **First-Person Normally Open** feature, will not be activated.

Lock Open Duration: Specifies the time (in seconds) that the door remains unlocked after successful verification. By default, this duration is set to 5 seconds, and it can range from 0 to 254 seconds.

Door Sensor Type: This indicates the status of the door sensor. When set to **None**, it means no door sensor is installed, and detection will not occur. When set to **Normal Open (NO)**, the door sensor is disconnected when the door is closed and triggers when the sensor reconnects. Conversely, when set

Copyright © 2024 ARMATURA LLC. All rights reserved

to **Normal Close (NC)**, the door sensor is connected when the door is closed and triggers when the sensor disconnects. If **Normal Open** or **Normal Close** is selected, the **Door Sensor Delay** must be configured.

Door Sensor Delay: The delay time for the door sensor. Once the delay period has expired, an alarm event, **"Door Open Timeout"**, will be triggered. The default delay is set to 15 seconds, with a configurable range from 1 to 254 seconds.

Anti-Passback Duration: This feature restricts re-entry within a specified time frame. It is based on the lock opening duration, which includes the door sensor's exit delay, and extends the entry duration accordingly. To enable this feature, select the **[Delay Passage]** option when adding or editing staff information. For example, this can be used to allow additional time for individuals with disabilities to enter. The default value is 0 minutes, and the range can be set from 0 to 120 minutes.

Verification Mode: The available verification modes depend on the device type. For example, on the **OmniAC20/30**, the available modes include Only Pin, Only Password, Only Card, Only Palm Vein, Only Face, Card or Password, Card and Password, Face and Password, Face and Card, Palm Vein and Card, and Palm Vein and Face. The default mode is Automatic Identification.

Open Door Delay: This setting defines the duration (in seconds) that the door remains open after verification is completed. The default value is 0, and the range is from 0 to 60 seconds.

Duress Password: The Duress Password is a special password that allows access during asituation, while simultaneously triggering an alarm to indicate a duress event. This feature is designed to ensure that the user can open the door under duress without alerting the person forcing them to do so. When entered, the Duress Password opens the door and immediately activates an alarm, notifying security of the potential threat. The password is restricted to a maximum of 6 digits to ensure quick entry.

Emergency Password: The Emergency Password is a password that grants unrestricted access to the door during an emergency situation. It is typically used by administrators to bypass all access restrictions and allow immediate entry. The default length of the Emergency Password is 8 digits. The Emergency Password works in any verification mode, time zone, or verification method, making it effective for emergency situations where normal access controls may need to be overridden.

Multi-Person Operation Interval: The Multi-Person Operation Interval defines the time interval between two verification attempts using cards or fingerprints. This interval ensures that the system does not accept consecutive verifications too quickly, which can help prevent false access attempts. The range for this interval is from 5 to 60 seconds.

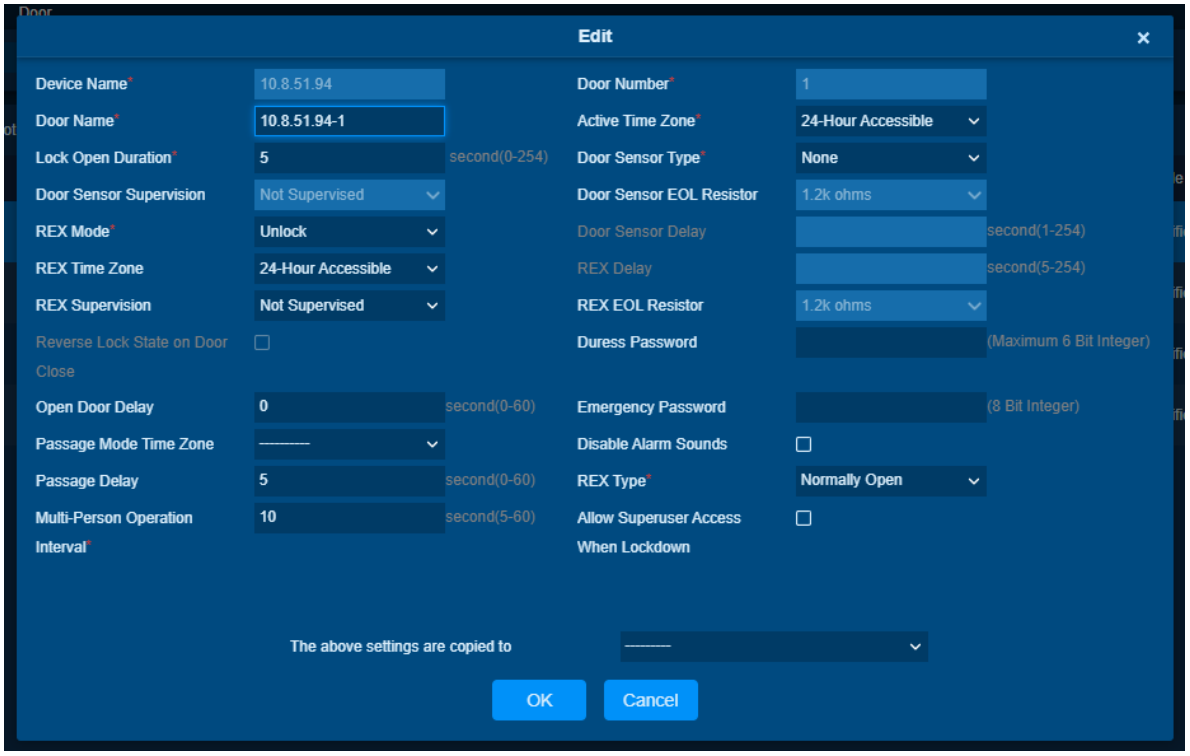
Disable Alarm Sound: Allows the user to mute alarm sounds on the real-time monitoring page, creating a quieter monitoring environment.

The above Settings are Copied to: This option allows you to replicate the current settings across multiple doors or devices for consistency. You can apply the settings to all doors of the current device, which will update all doors associated with the current access device, or to all doors of all devices, which will apply the settings across all doors within the current user’s level. After configuring the parameters, click **[OK]** to save the changes and exit.

Copyright © 2024 ARMATURA LLC. All rights reserved

Horizon Series Controllers

Select the door to be modified and click **[Door Name]** or **[Edit]** button below operations to open the Edit interface.



Field Descriptions:

Device Name: Displays the device name. This field is non-editable and can only be modified through the device settings.

Door Number: This field indicates the door number and is non-editable. The numbering starts from 1 and continues based on the number of doors available on the device, with a maximum of 4 doors.

Door Name: This field is editable and initially defaults to "Device Name - Door Number." You can rename it, with a maximum character limit of 30.

Active Time Zone: Defines the operating schedule for the door. By default, it is set to **"24-Hour Accessible"**, meaning the reader is available for access at all times.

Lock Open Duration: Specifies the time (in seconds) that the door remains unlocked after successful verification. By default, this duration is set to 5 seconds, and it can range from 0 to 254 seconds.

Door Sensor Type: This indicates the status of the door sensor. When set to **None**, it means no door sensor is installed, and detection will not occur. When set to **Normal Open (NO)**, the door sensor is disconnected when the door is closed and triggers when the sensor reconnects. Conversely, when set to **Normal Close (NC)**, the door sensor is connected when the door is closed and triggers when the sensor disconnects. If **Normal Open** or **Normal Close** is selected, the **Door Sensor Delay** must be configured.

Copyright © 2024 ARMATURA LLC. All rights reserved

REX Mode: REX (Request to Exit) Mode defines the alarm delay time for door detection after the exit button is pressed. When the door is forcibly unlocked, the system will check the door status after the specified delay. The default delay is set to 10 seconds, with a configurable range from 1 to 254 seconds. The exit button must be locked before this option can be set.

Door Sensor Delay: This setting defines the delay time for the door sensor after the door is opened. If the door is not within the Passage Open period, the device will begin counting as soon as the door is opened. Once the delay period expires, an alarm event, **"Door Open Timeout"**, will be triggered, and the alarm will stop when the door is closed. The default delay is set to 15 seconds, with a configurable range from 1 to 254 seconds. The **Door Sensor Delay** should always be set to a value greater than the **Lock Open Duration**.

Verification Mode: The available verification modes depend on the device type. The default mode is Automatic Identification.

Wiegand Format: This setting defines the Wiegand format for the door. By default, it is set to **Auto**. Additional Wiegand format settings can be configured under **[Personnel Management]** > **[Card Management]** > **[Wiegand Formats]**.

REX Time Zone: The **Request to Exit (REX) Time Zone** offers two options: **None** (which will not detect REX input) and **24-Hour Accessible**. By default, the value is set to **24-Hour Accessible**.

REX Delay: The **Request to Exit Delay** defines the alarm delay time for door detection after the exit button is locked. When the door is forcibly unlocked, the system will check the door status after the specified delay. The default delay is set to 10 seconds, with a configurable range from 1 to 254 seconds. The exit button must be locked before this option can be set.

Operate Interval: This defines the minimum time, in seconds, between consecutive verification attempts. If a user attempts a swap within this interval, an **"Operation Interval Too Short – Access Denied"** error will be triggered due to insufficient time between attempts. The default interval is set to 2 seconds, with a configurable range from 0 to 254 seconds.

Anti-Passback Duration: This feature restricts re-entry within a specified time frame. It is based on the lock opening duration, which includes the door sensor's exit delay, and extends the entry duration accordingly. To enable this feature, select the **[Delay Passage]** option when adding or editing staff information. For example, this can be used to allow additional time for individuals with disabilities to enter. The default value is 0 minutes, and the range can be set from 0 to 120 minutes.

Reverse Lock State on Door Close: Determines whether the door will lock automatically after closing. Enable this option to lock the door immediately after it closes. It will set to either lock or not lock the door after door closing. Check it for locking after door closing.

Duress Password: The Duress Password is a special password that allows access during a coercion situation, while simultaneously triggering an alarm to indicate a duress event. This feature is designed to ensure that the user can open the door under duress without alerting the person forcing them to do so. When entered, the Duress Password opens the door and immediately activates an alarm, notifying security of the potential threat. The password is restricted to a maximum of 6 digits to ensure quick entry.

Open Door Delay: The duration for which the door remains open after a successful verification (range: 1 to 60 seconds).

Copyright © 2024 ARMATURA LLC. All rights reserved

Emergency Password: The Emergency Password is a password that grants unrestricted access to the door during an emergency situation. It is typically used by administrators to bypass all access restrictions and allow immediate entry. The default length of the Emergency Password is 8 digits. The Emergency Password works in any verification mode, time zone, or verification method, making it effective for emergency situations where normal access controls may need to be overridden.

Passage Mode Time Zone: Passage Mode ensures that the door remains open during the selected time frame. This time zone range must be set within the Active Time Zone, and by default, it is set to "------," meaning there is no designated passage time. Additionally, if an admin user performs five consecutive verifications within five seconds, the door will exit Passage Mode and return to the closed state. If five more verifications are made during the passage time, the door will re-enter Passage Mode. This functionality is effective only during the Active Time Zone; outside of this period, other Passage Mode triggers, including the **First-Person Normally Open** feature, will not be activated.

Disable Alarm Sound: Allows the user to mute alarm sounds on the real-time monitoring page, creating a quieter monitoring environment.

Passage Delay: The **Passage Delay** feature allows specific personnel to be granted additional time to pass through the door upon access approval. This is particularly useful for individuals who may need more time to enter, such as those with disabilities. The **Delay Passage** setting can be configured in the **[Personnel]** > **[Edit Personnel]** page. By enabling this option for a person, their entry duration is extended, giving them more time to pass through the channel. This configuration ensures a more accessible and accommodating environment for individuals who require extra time.

Card Number Reversal: Enabling **Card Number Reversal** allows the reversal of card numbers. When disabled, card numbers cannot be reversed. The default setting is disabled.

Multi-Person Operation Interval: The Multi-Person Operation Interval defines the time interval between two verification attempts using cards or fingerprints. This interval ensures that the system does not accept consecutive verifications too quickly, which can help prevent false access attempts. The range for this interval is from 5 to 60 seconds.

Allow Superuser Access During Lockdown: The Allow Superuser Access When Lockdown setting enables superusers to access the door even when it is in lockdown mode. This option is useful in emergency situations where authorized personnel need to bypass lockdown restrictions. By default, this setting is disabled, ensuring that doors remain inaccessible during lockdowns unless explicitly overridden by superusers. You can toggle this setting based on your security policies to grant or restrict access for superusers during lockdown events.

The above Settings are Copied to: This option allows you to replicate the current settings across multiple doors or devices for consistency. You can apply the settings to all doors of the current device, which will update all doors associated with the current access device, or to all doors of all devices, which will apply the settings across all doors within the current user's level. After configuring the parameters, click **[OK]** to save the changes and exit.

Copyright © 2024 ARMATURA LLC. All rights reserved

Remote Opening

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device has been successfully added to the system.

Usage Scenarios

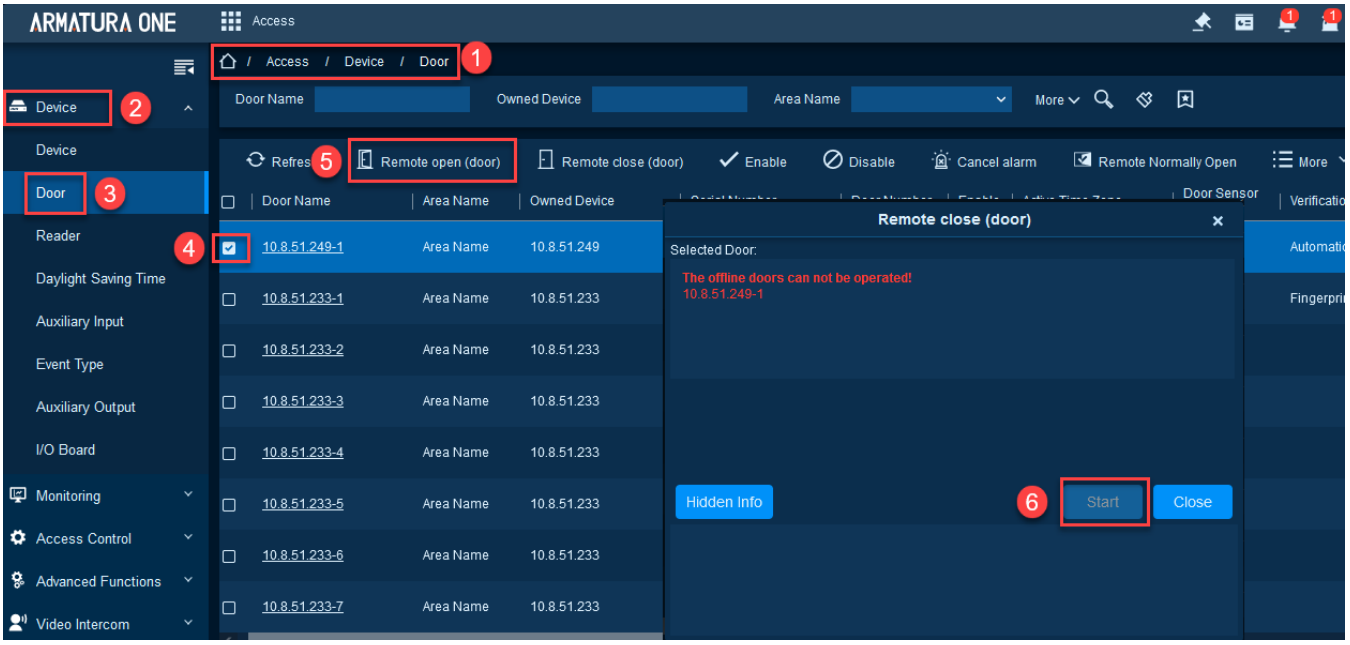
When the administrator needs to grant immediate access to a door.

Trigger Results

The designated door opens, allowing entry.

Steps:

- Navigate to **[Access] > [Device] > [Door]** to access the Door Management interface.
- Select the desired door and click **[Remote Opening]** to open the remote door interface.
- Set the desired **door opening interval** and click **[Start]** to remotely open the door.



Remote Closing

Prerequisites for Use

Log into the system using an account with the required permissions and ensure the device has been successfully added to the system.

Usage Scenarios

When the administrator needs to restrict access by closing a door remotely.

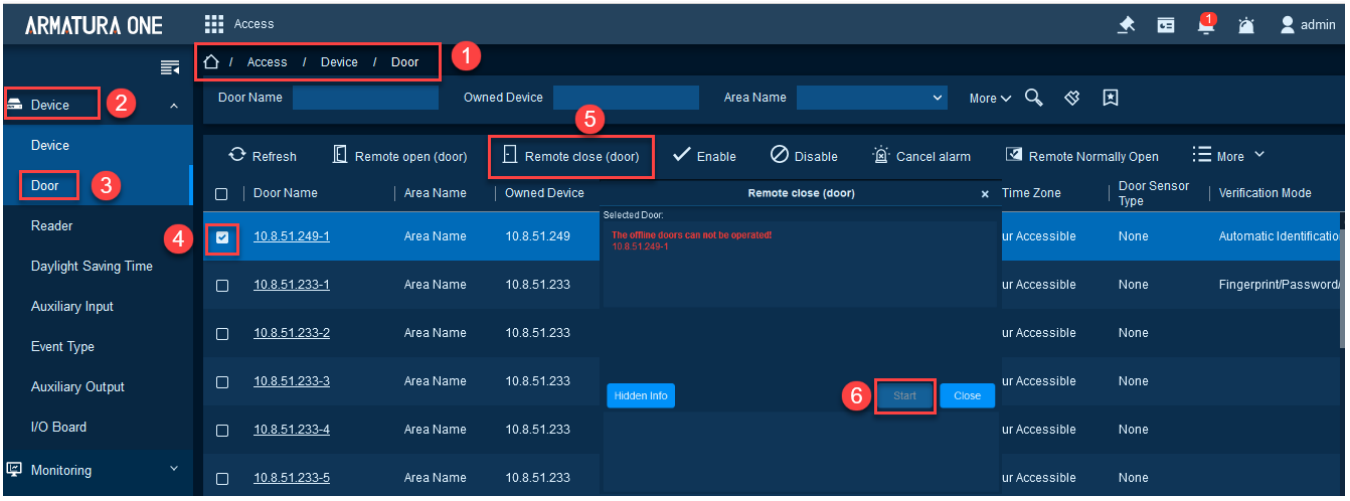
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

The specified door closes, preventing further entry.

Steps

- Navigate to **[Access]** > **[Device]** > **[Door]** to access the Door Management interface.
- Select the desired door and click **[Remote Closing]** to exit the remote closing interface.
- Enter the device connection password, if prompted, and click **[Start]** to remotely close the door.



Enable

Prerequisites for Use

Log into the system using an account with the required permissions, ensure the device has been successfully added, and verify that the door is currently in a disabled state.

Usage Scenarios

Activating the door to enable its functionality for access control.

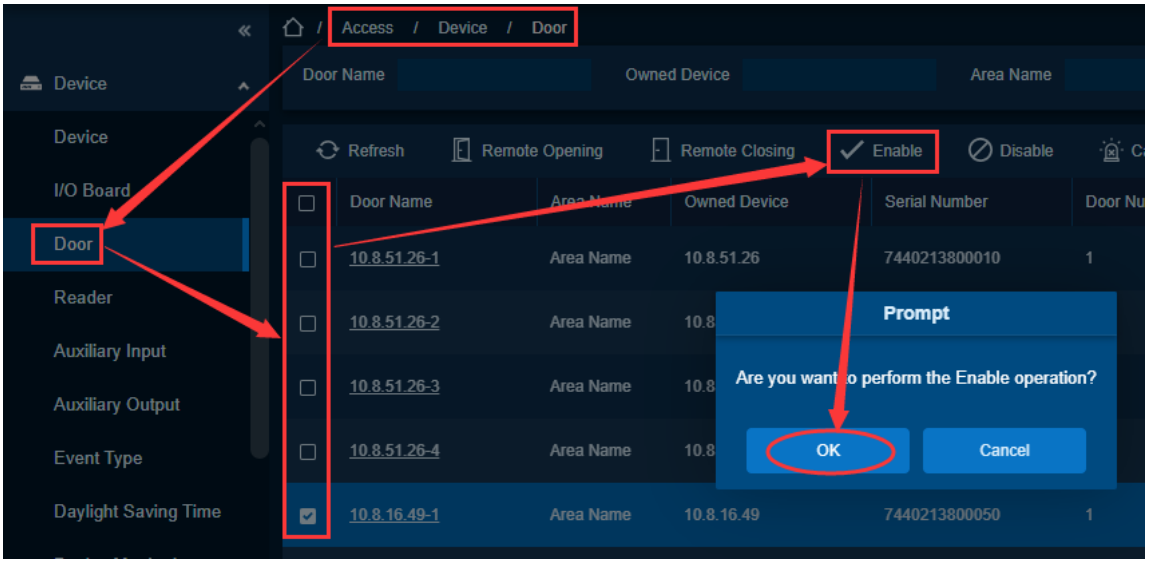
Trigger Results

Once enabled, the software can communicate with the door, uploading and managing data as required.

Steps:

- Navigate to **[Access] > [Device] > [Door]** to access the Door Management interface.
- Locate the desired door and click **[Enable]** to open the enable interface.
- Click **[OK]** to confirm and enable the door.

Copyright © 2024 ARMATURA LLC. All rights reserved



Disable

Prerequisites for Use

Log into the system using an account with the required permissions, ensure the device has been successfully added, and verify that the door is currently in an enabled state.

Usage Scenarios

Temporarily disabling a door due to malfunction or for maintenance.

Preparing to replace the door or configure another device.

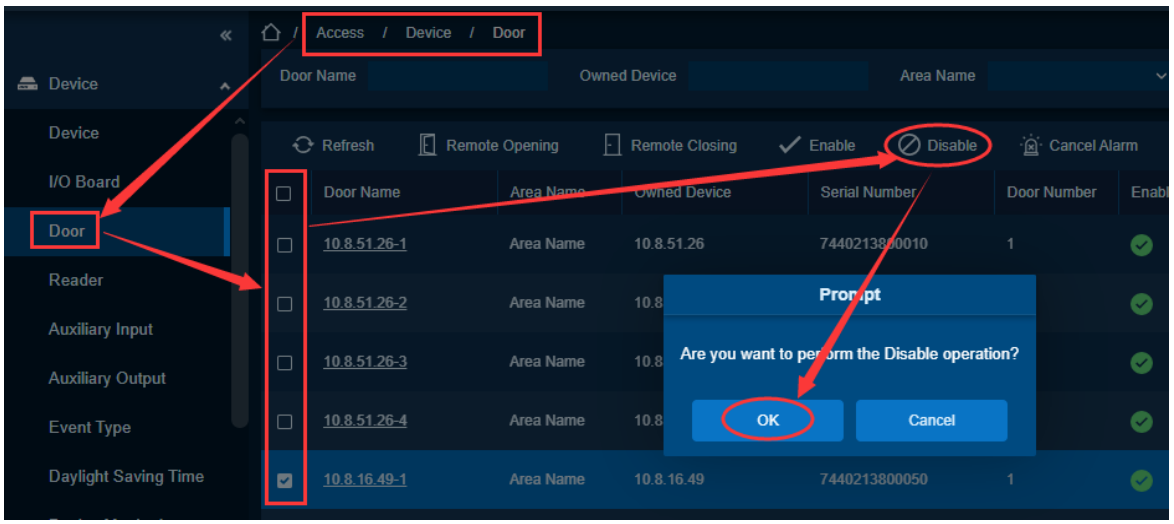
Trigger Results

The selected door is disabled, and it will no longer operate within the system.

Steps:

- Navigate to **[Access] > [Device] > [Door]** to access the Door Management interface.
- Locate the desired door and click **[Disable]** to open the disabled interface.
- Click **[OK]** to confirm and disable the door.

Copyright © 2024 ARMATURA LLC. All rights reserved



Cancel Alarm

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

The alarm event has been addressed and needs to be canceled to restore normal operation.

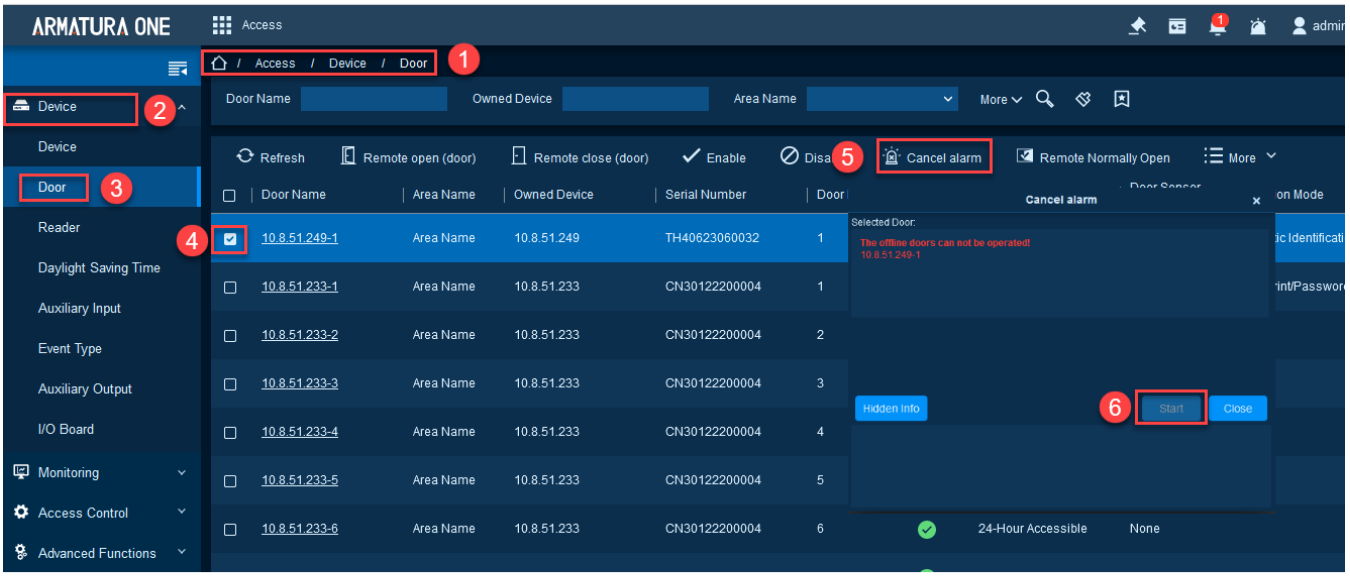
Trigger Results

The alarm is cancelled, and the alarm status is reset.

Steps:

- Navigate to **[Access] > [Device] > [Door]** to access the Door Management interface.
- Locate the specific door triggering the alarm and click **[Cancel Alarm]** to open the cancel alarm interface.
- Enter the device connection password in the provided field.
- Click **[Start]** to execute the operation and cancel the alarm.

Copyright © 2024 ARMATURA LLC. All rights reserved



Remote Normally Open

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

The door needs to be kept open for extended access, such as during events or maintenance activities.

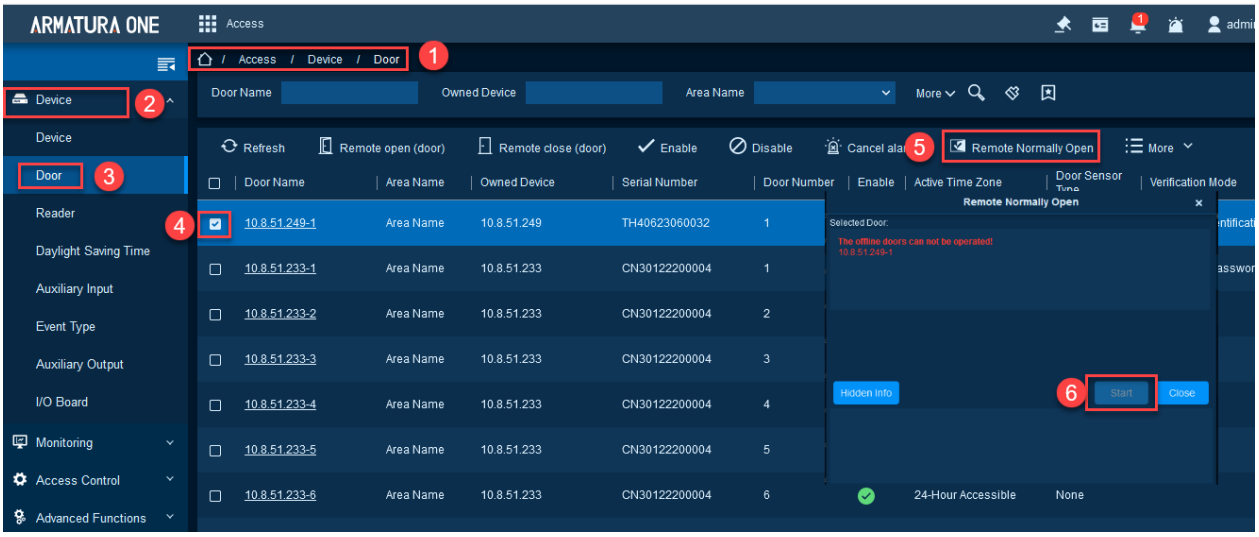
Trigger Results

Open the door and the door remains in an open state.

Steps:

- Navigate to **[Access] > [Device] > [Door]** to access the Door Management interface.
- Select the desired door and click **[Remote Normally Open]** to open the Remote Normally Open interface.
- Enter the **device connection password** in the designated field.
- Click **[Start]** to enable the Remote Normally Open state.

Copyright © 2024 ARMATURA LLC. All rights reserved



Initiate Lockdown

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

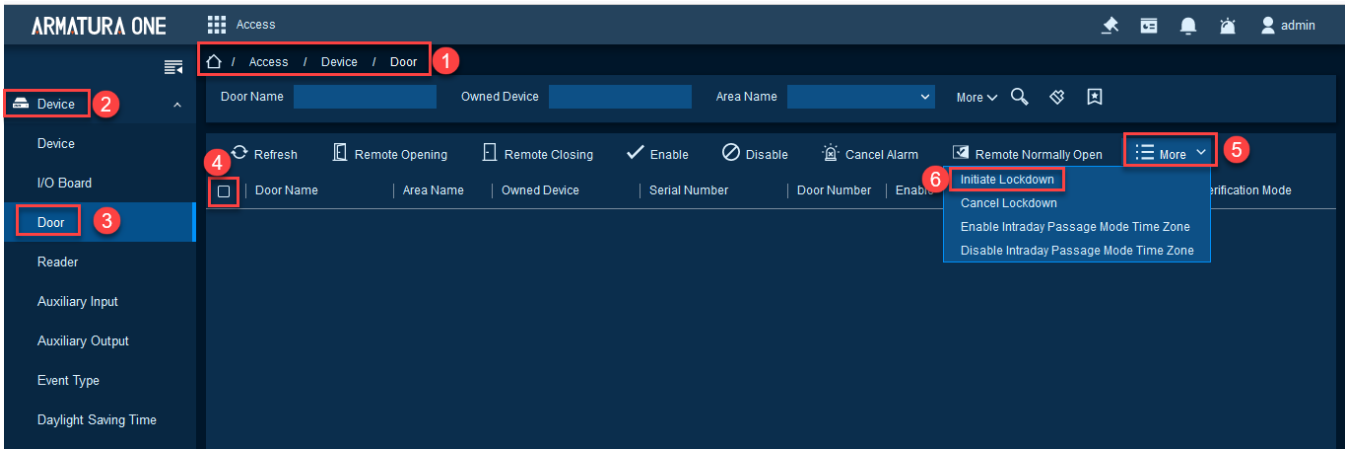
To restrict access and prevent door operation during emergencies or security-critical situations.

Trigger Result

The door is set to a locked state where it cannot respond to any operations, including card swiping, manual unlock attempts, or other commands.

Steps:

- Navigate to **[Access Control Device] > [Door]** to access the Door Management interface.
- Click **[More] > [Initiate Lockdown]** to open the lockdown interface.
- Enter the **device connection password** in the provided field.
- Click **[Start]** to activate the lockdown and lock the door.



Copyright © 2024 ARMATURA LLC. All rights reserved

Cancel Lockdown

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

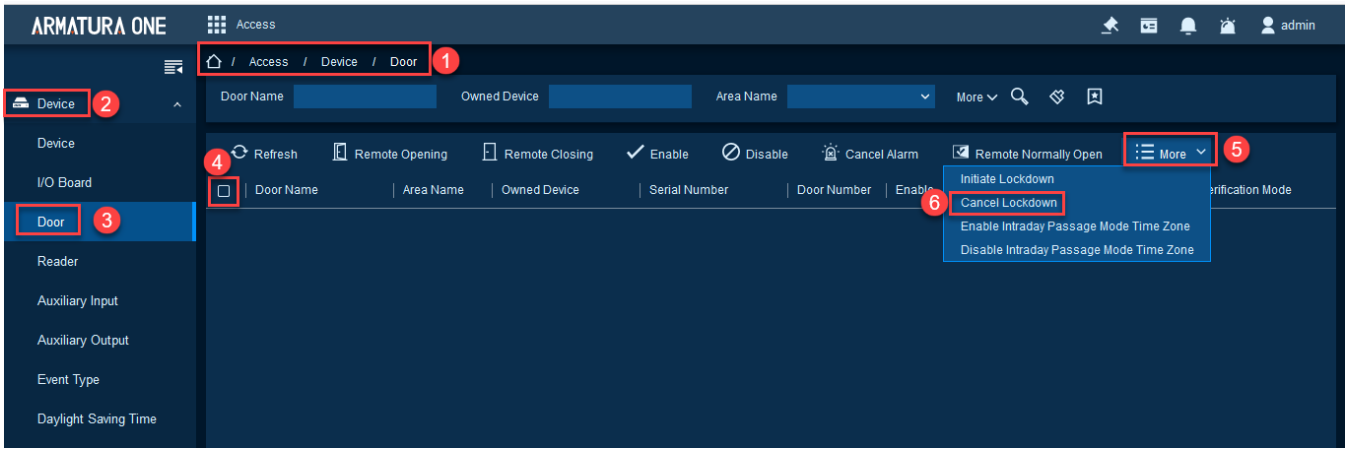
To cancel the lockdown mode, restoring its normal operations.

Trigger Results

The door is returned to its normal state, allowing it to respond to operations such as card swiping, manual commands, or other access requests.

Steps:

- Navigate to **[Access Control Device] > [Door]** to access the Door Management interface.
- Click **[More] > [Cancel Lockdown]** to open the cancel lockdown interface.
- Enter the **device connection password** in the provided field.
- Click **[Start]** to cancel the lockdown and restore normal door functionality.



Enable Intraday Passage Mode Time Zone

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

To set the door to remain open during a designated time.

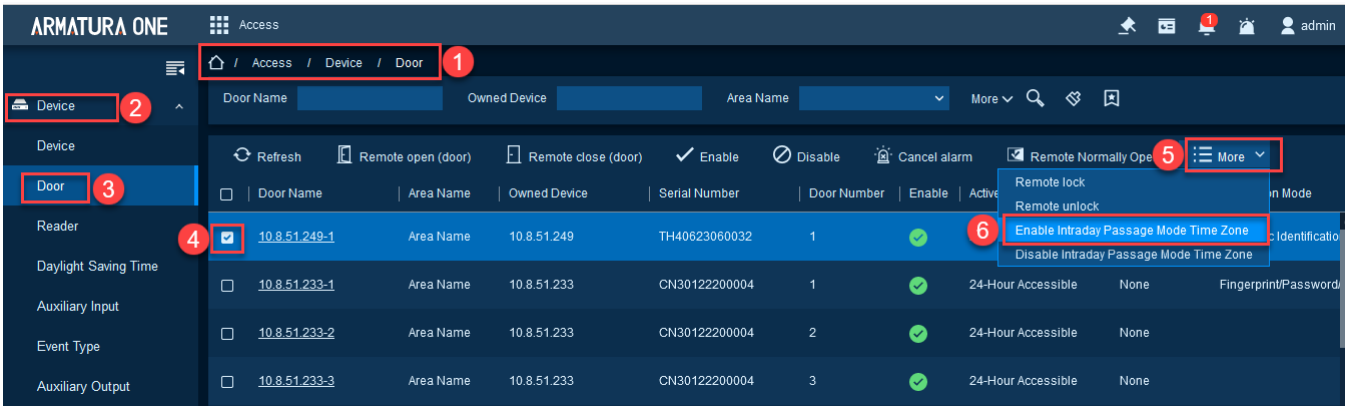
Trigger Results

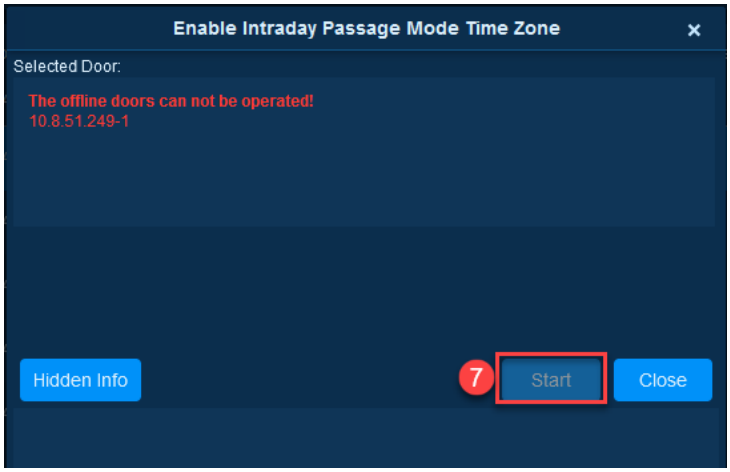
The door remains open during the specified time, allowing unrestricted entry and exit.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access] > [Device] > [Door]** to access the Door Management interface.
- Click **[More] > [Enable Intraday Passage Mode Time Zone]** to open the enable passage mode interface.
- Click **[Start]** to activate the passage mode for the specified time zone.





Disable Intraday Passage Mode Time Zone

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

To disable the **Normally Open Time Zone**.

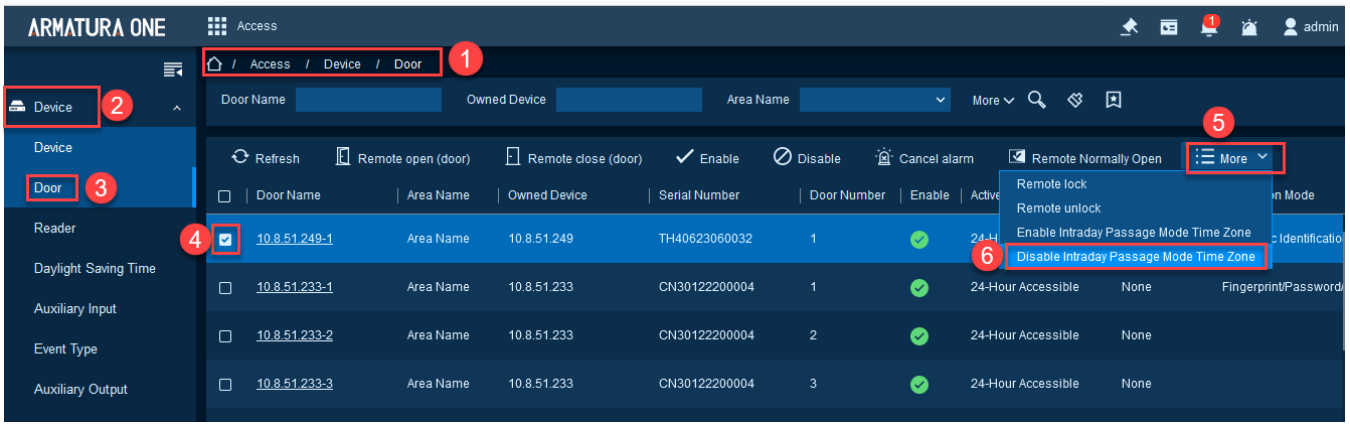
Trigger Results

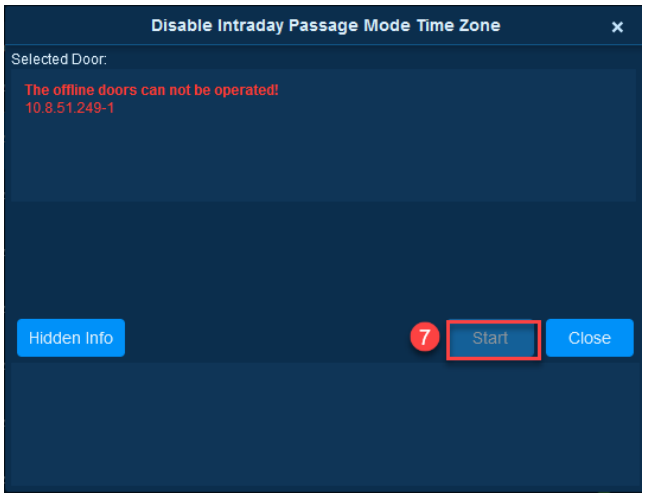
The **Normally Open Time Zone** is deactivated, preventing unrestricted entry and exit during the specified time.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access] > [Device] > [Door]** to access the Door Management interface.
- Click **[More] > [Disable Intraday Passage Mode Time Zone]** to open the disable passage mode interface.
- Enter the **device connection password** in the provided field.
- Click **[Start]** to disable the passage mode for the specified time zone.





6.1.4. Reader

Function Description

The Reader section displays the list of readers associated with the added device.

New Reader

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

To add a reader to the controller.

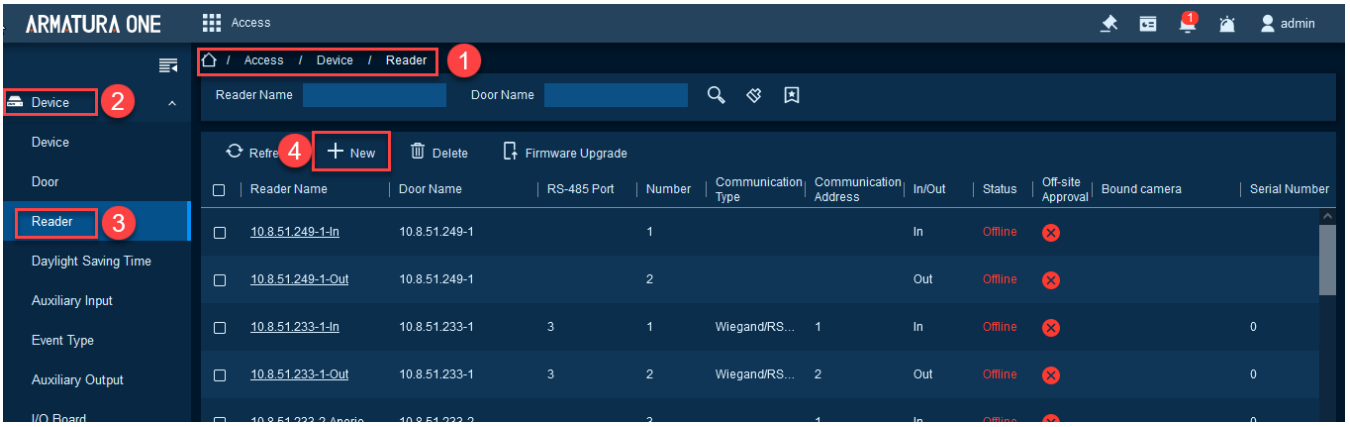
Copyright © 2024 ARMATURA LLC. All rights reserved

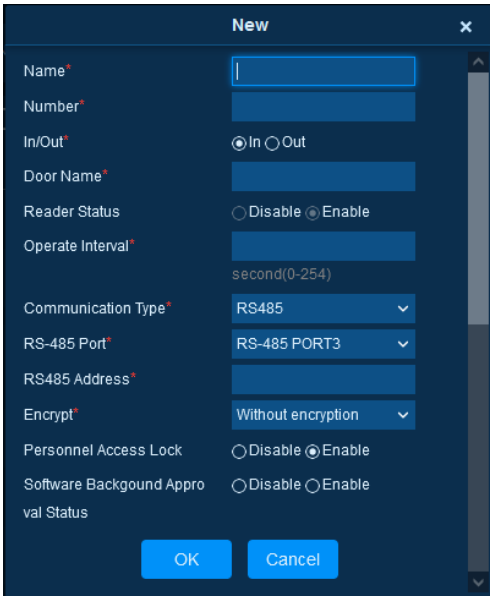
Trigger Results

The system modifies the configuration to include the newly added reader.

Steps:

- Navigate to **[Access] > [Device] > [Reader] > [New]** to open the interface for adding a new reader.
- Fill in the required parameters and click **[OK]** to add the reader to the list.





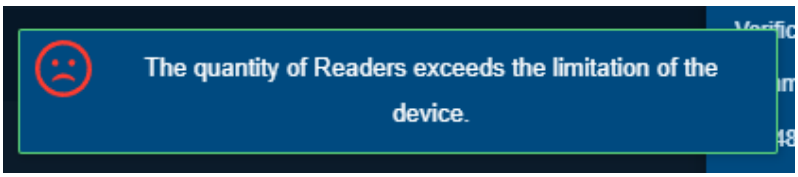
Note:

Reader-to-Door Ratio: The number of readers is determined by the number of doors on the controller. The default ratio is **1:2** (one door can support up to two readers).

Adding and Deleting: Readers can be deleted and re-added. However, the total number of readers cannot exceed the maximum allowed as per the **1:2 ratio**.

System Validation: The system will prompt an error if an attempt is made to exceed the allowable number of readers.

Copyright © 2024 ARMATURA LLC. All rights reserved



Edit Reader

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

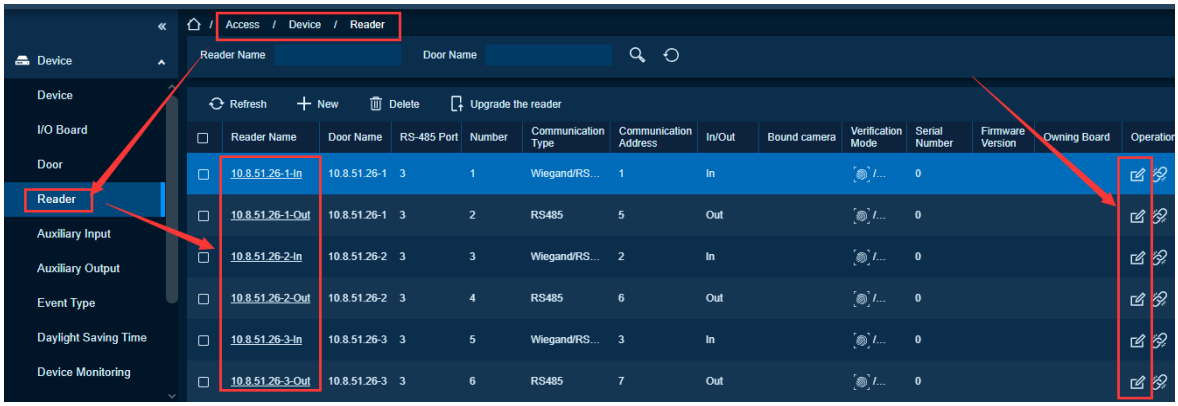
To modify the parameter configuration or update information for the corresponding reader.

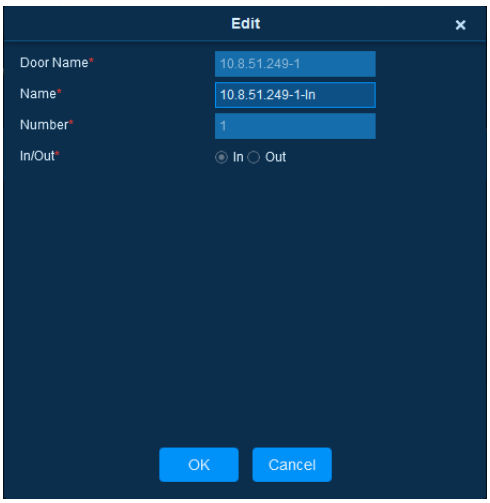
Trigger Results

The system updates the configuration for the selected reader based on the new parameters.

Steps:

- Navigate to **[Access] > [Device] > [Reader]**.
- In the **Action Menu**, locate the reader you wish to edit and click on the **Reader Name** or the **[Edit]** button to open the edit interface.





Copyright © 2024 ARMATURA LLC. All rights reserved

- Update the following fields as required:
  - **Door Name**: Select the door corresponding to the reader.
  - **Name**: Assign a name for the reader that will be displayed on the list page.
  - **Number**: Provide a unique number that serves as the reader's specific ID in the database.
  - **In/Out**: Indicate whether the reader is installed **Inside** or **Outside** the door.
- After completing the edits, click **[OK]** to save the changes.

Bind/Unbind Camera

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

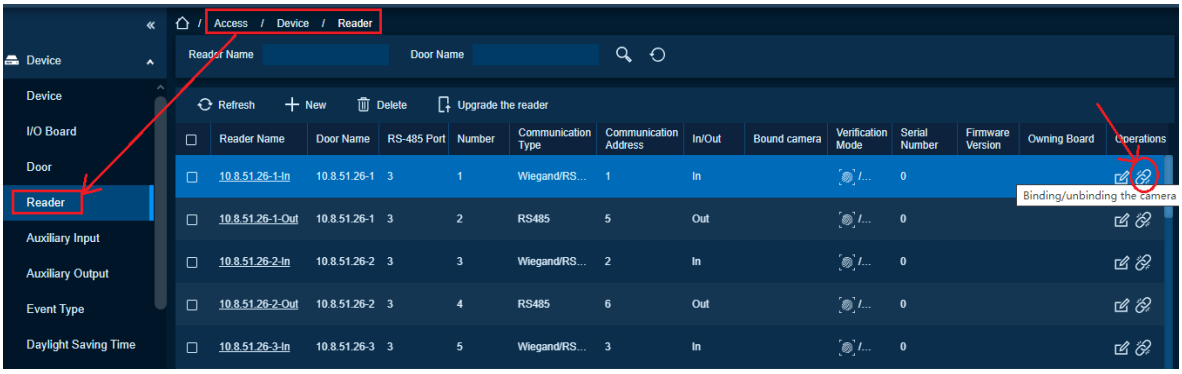
Establish a linkage to trigger video pop-ups, live streaming, or screenshots when specific events occur.

Trigger Result

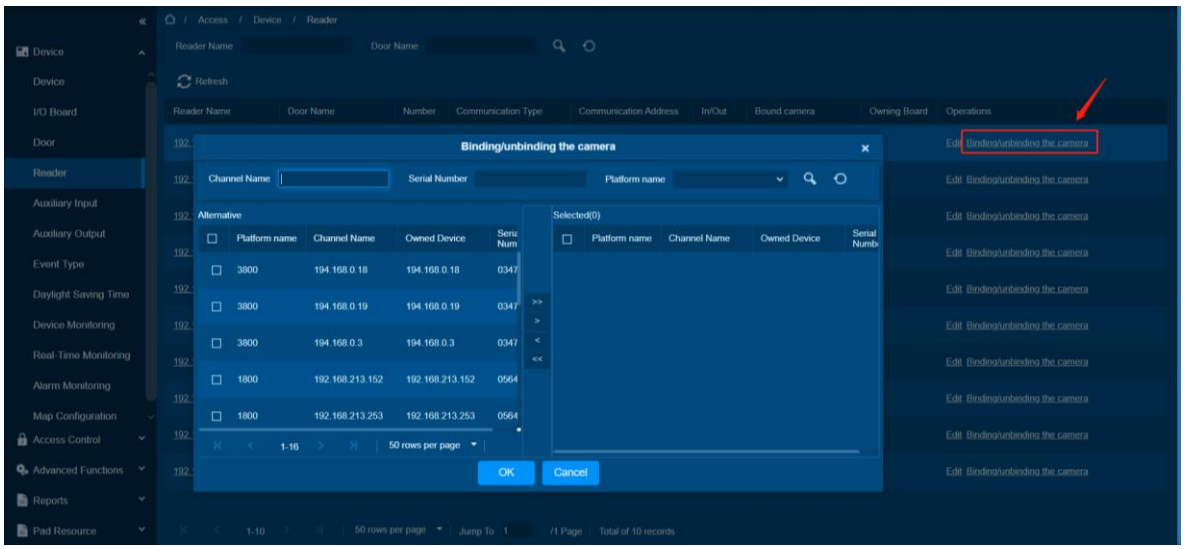
By binding a camera to a reader, the system can trigger video linkages (such as pop-up videos, live video streaming, or screenshots) in response to corresponding events.

Steps:

- Navigate to **[Access] > [Device] > [Reader]**.
- Click on **[Bind/Unbind Camera]** to open the selection interface.
- Select the appropriate camera from the list and move the required cameras to the **right list**.
- Click **[OK]** to finalize the camera binding.



Copyright © 2024 ARMATURA LLC. All rights reserved



Note:

A single reader can bind up to **5 cameras**.

Firmware Upgrade

Prerequisites for Use

Log into the system using an account with the required permissions, ensure the reader is connected to the controller via RS-485 or OSDP, and verify that the status is online.

Usage Scenarios

Perform a firmware upgrade to the reader via the controller.

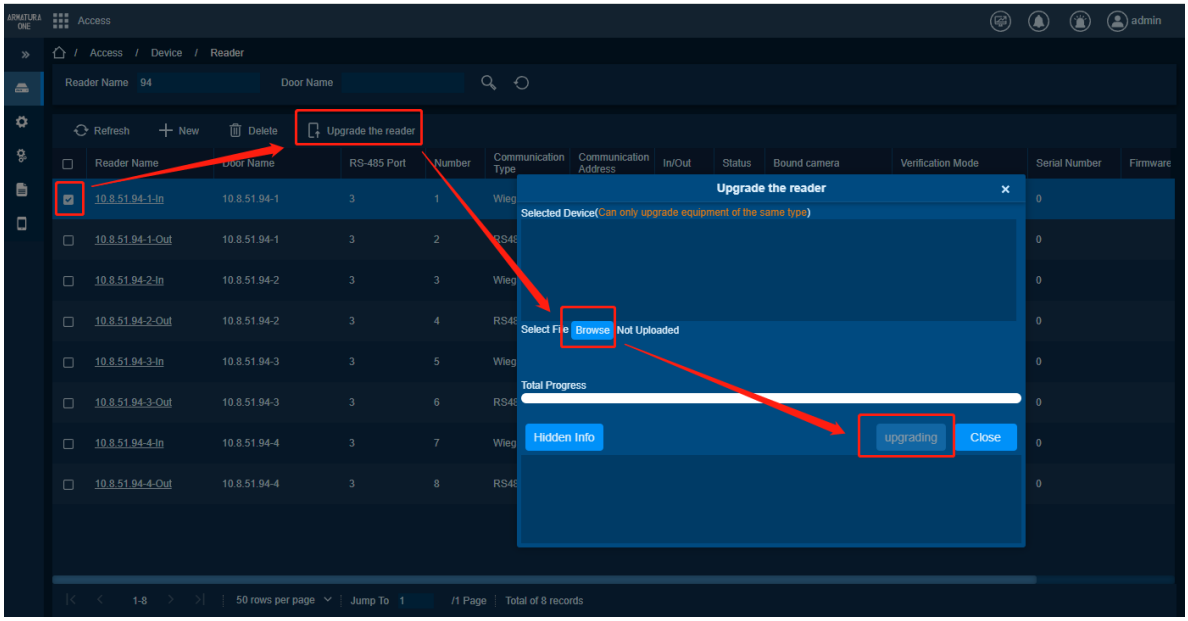
Trigger Result

The reader's firmware will be upgraded, and the reader will automatically reboot. The firmware version displayed in the system will be updated.

Steps:

- Navigate to **[Access] > [Device] > [Reader]**.
- Select the target reader from the list.
- Click on **[Firmware Upgrade]** to open the upgrade interface.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Click **[Browse]** and select the firmware file from your local computer. Ensure the firmware file is named rdfw.ar.
- Click **[Upgrade]** to start the process.
- Once the firmware upgrade is complete, the reader will reboot automatically.
- Verify that the **Firmware Version** column reflects the updated version.

Delete

Prerequisites for Use

Log into the system using an account with the required permissions and ensure that the reader is either no longer required or has been replaced.

Usage Scenarios

Remove a reader that is no longer in use or needs to be replaced.

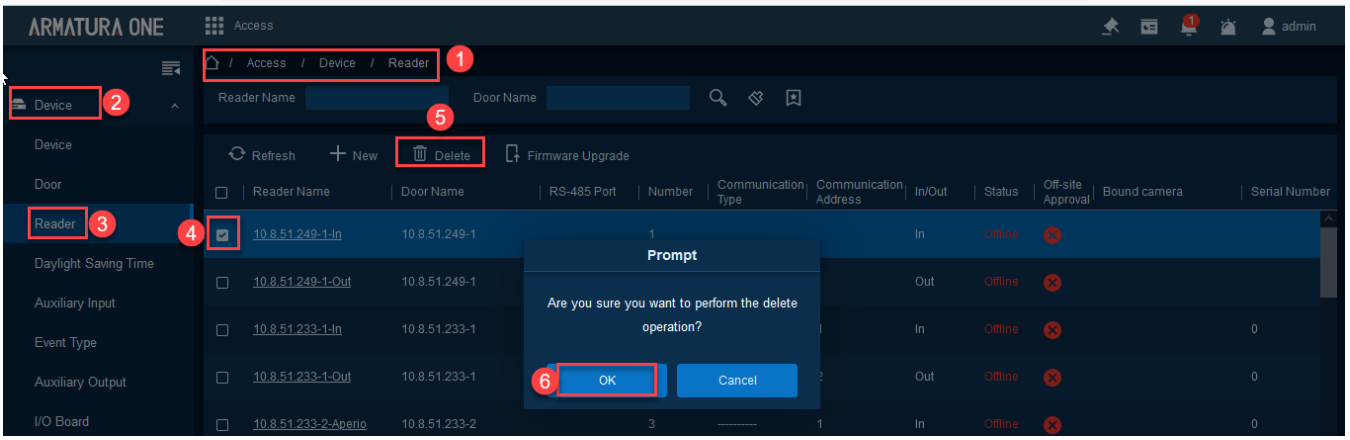
Trigger Result

The selected reader will be permanently deleted from the system.

Steps:

- Navigate to **[Access] > [Device] > [Reader]**.
- Click on **[Delete]** next to the reader you wish to remove.
- Follow any prompts to confirm the deletion.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.1.5. Auxiliary Input

Function Description

The **Auxiliary Input** section manages the auxiliary inputs list for the added device. Users can enable or disable auxiliary inputs, unbind them, or bind cameras for video integration.

Enable/Disable Auxiliary Input

Prerequisites for Use

Log into the system using an account with the required permissions. Ensure the target device is added and available for modification.

Usage Scenarios

Enable the auxiliary input to allow signal detection and trigger linked events.

Disable the auxiliary input to mask its signal and prevent any associated linkages.

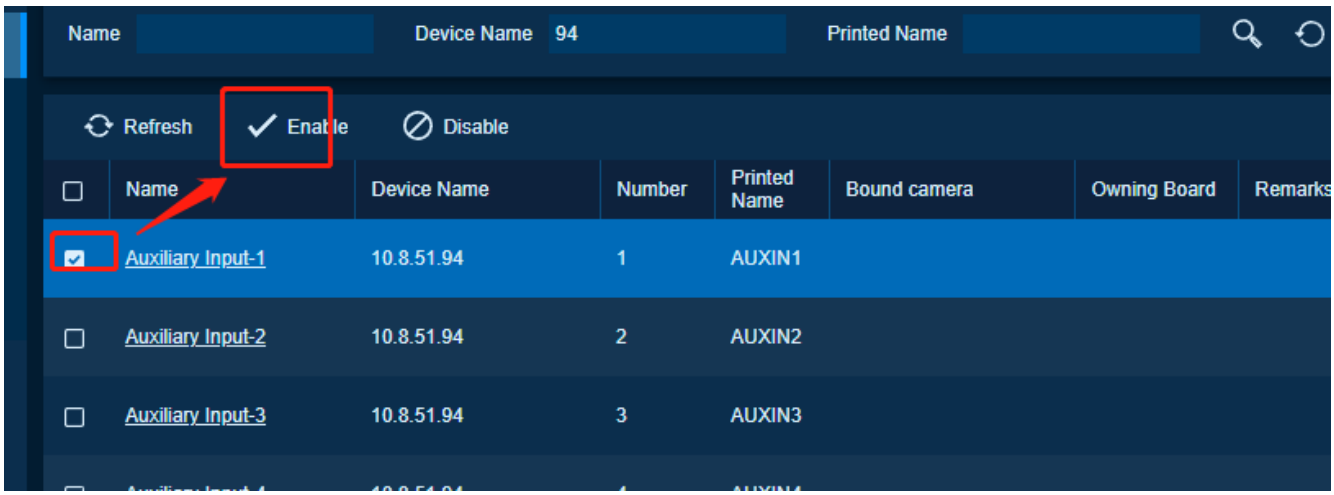
Trigger Result

- **Enabled**: The auxiliary input will be active and can trigger configured linkages.
- **Disabled**: The auxiliary input will be deactivated, and no linkages involving the input will be triggered.

Steps:

- Navigate to **[Access] > [Device] > [Auxiliary Input]**.
- Click **[Enable/Disable]** next to the desired auxiliary input.
- Follow any prompts to confirm the enabling or disabling of the input.

Copyright © 2024 ARMATURA LLC. All rights reserved



Edit Auxiliary Input

Prerequisites for Use

Log into the system using an account with the required permissions. Ensure the target device with auxiliary inputs is successfully added and online.

Usage Scenarios

Modify configurations or update details for auxiliary inputs.

Rename or adjust time zones for devices based on operational needs.

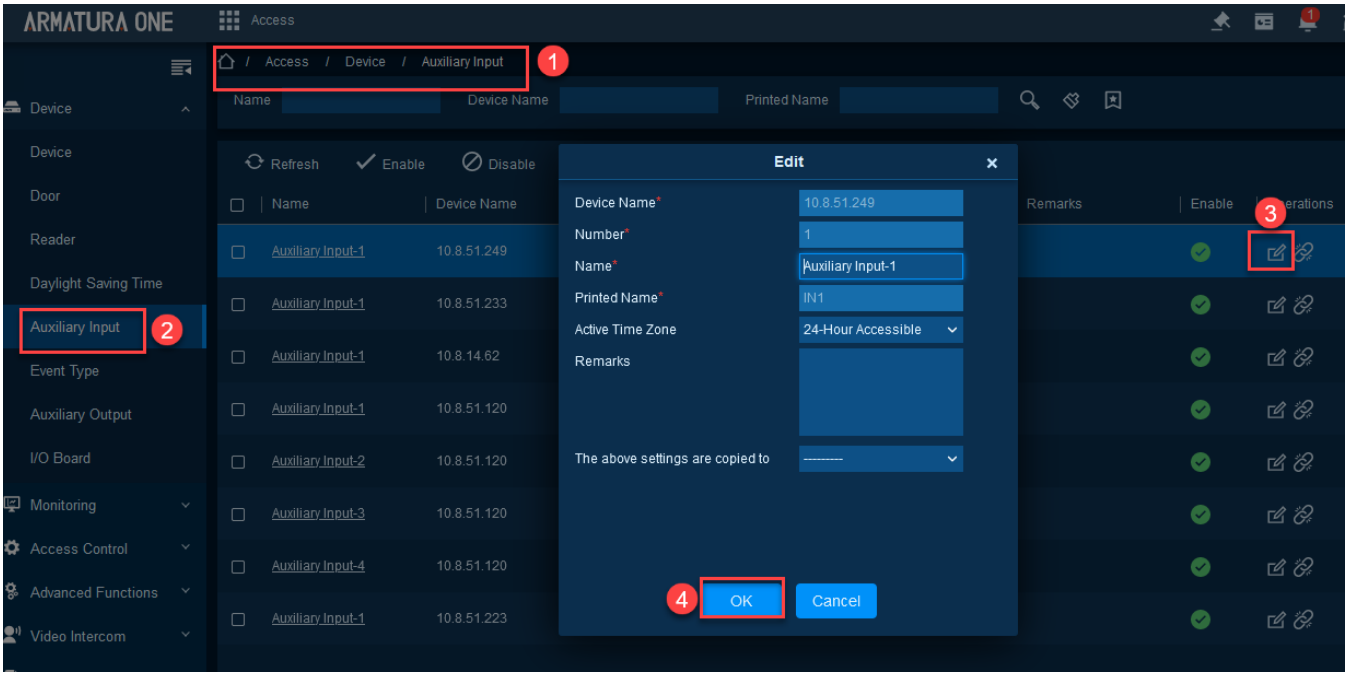
Trigger Result

Updates and changes to the auxiliary input's settings will take effect.

Steps:

- Go to **[Access] > [Device] > [Auxiliary Input]** via the Action Menu.
- Click on the **Name** or **[Edit]** button for the input you wish to modify.

Copyright © 2024 ARMATURA LLC. All rights reserved



Update the following parameters:

- **Device Name**: Displays the associated device (non-editable).
- **Number**: The unique identifier for the auxiliary input in the database (non-editable).
- **Name**: Enter a custom name for the input based on user preferences.
- **Printed Name**: Reflects the hardware's physical label, such as "IN5" (non-editable).
- **Active Time Zone**: Specify the time segment during which the auxiliary input is active.
- **Remarks**: Add any relevant comments or descriptions about the input.
- Click **[OK]** to save the updates and exit.

Note:

Only the following fields can be edited: **Name**, **Active Time Zone**, and **Remarks**.

Ensure the specified **Active Time Zone** aligns with the intended operational schedule.

Remarks should provide clear and descriptive information to assist other users.

Bind/Unbind Camera

Prerequisites for Use

Log into the system using an account with the required permissions. Ensure the auxiliary input and cameras are correctly added to the system. Configure the **Interaction Settings** under **Linkage** or **Global Linkage** to enable event-based video triggers.

Usage Scenarios

Bind cameras to an auxiliary input point to enable video linkage for events. Unbind cameras if the video linkages is no longer required.

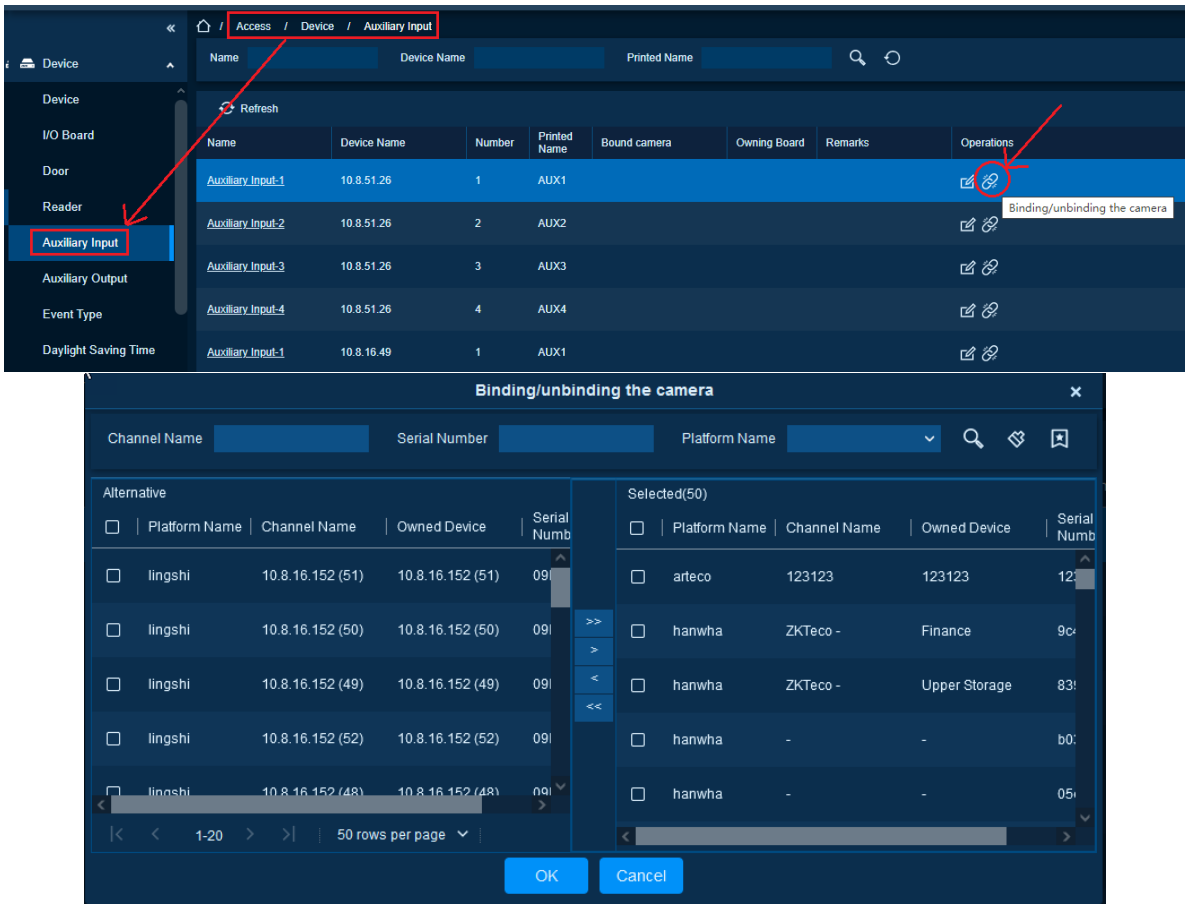
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Successfully bind one or more cameras to an auxiliary input point. When a corresponding events occurs, the system can trigger video feeds (pop-up videos, live streams, or screenshots).

Steps:

- Navigate to **[Access] > [Device] > [Auxiliary Input]** to display the auxiliary input list.
- Click on the name of the desired auxiliary input in the **Camera List** to access its camera binding interface.



- Transfer cameras from the **Available Devices** (left) to the **Selected Devices** (right):
- Use the transfer button **[3]** to move all devices to the right.
- Click **[OK]** to finalize the binding.
- The camera is successfully bound to the auxiliary input.

Note:

- Each auxiliary input point can bind more than one camera channel.
- Ensure that the cameras being bound are functional and correctly configured within the system.
- Video linkage settings must be pre-configured for seamless operation during events.

Copyright © 2024 ARMATURA LLC. All rights reserved

6.1.6. Auxiliary Output

Function Description

Displays the list of auxiliary outputs. These outputs can be edited and configured for various functionalities such as alarms and linkages. The auxiliary output relay can be operated remotely for actions like opening, closing, or maintaining a normally open state.

Edit Auxiliary Output

Prerequisites for Use

Log into the system using an account with the required permissions. Ensure the outputs are successfully added to the system.

Usage Scenarios

Modify parameter configurations and settings for an auxiliary output.

Connect auxiliary outputs to alarms or other devices for linkage purposes.

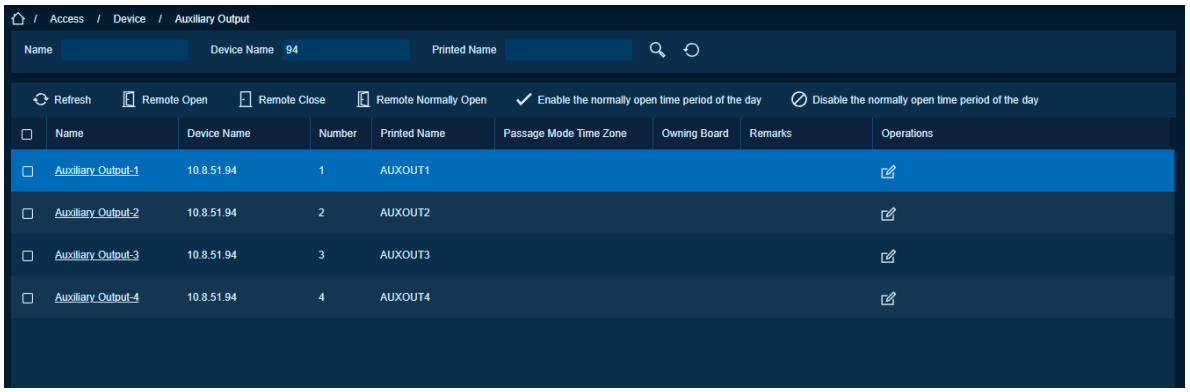
Trigger Results

Updates the configuration of the auxiliary output relay.

Enables remote operations such as opening, closing, or setting to normally open. The relay performs the specified actions based on these settings.

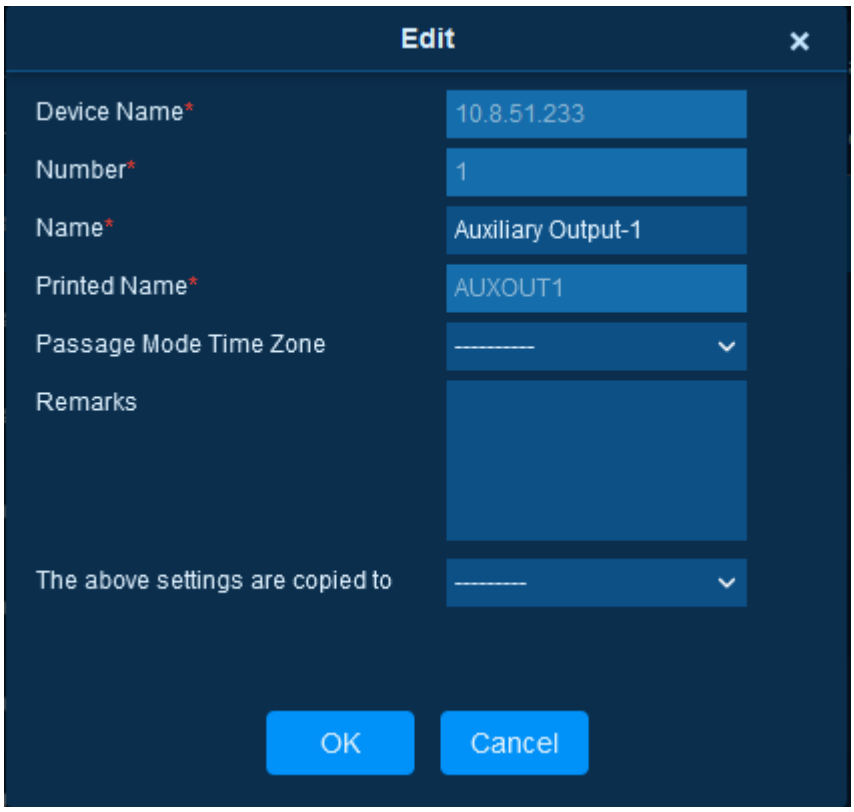
Steps:

- Navigate to **[Access] > [Device] > [Auxiliary Output]** from the Action Menu to display the auxiliary output interface.



- Select the desired auxiliary output and click **[Edit]** to modify its parameters.

Copyright © 2024 ARMATURA LLC. All rights reserved



Fields Description:

Name: Customize the auxiliary output name as per user preference.

Printed Name: Refers to the physical label on the hardware, such as **OUT2**.

Passage Mode Time Zone: Defines whether the auxiliary output will be in a normal open or normal closed state during the selected time zone.

After editing, click **[OK]** to save the changes and exit the interface.

Note:

Only the following fields can be modified: **Name, Passage Mode Time Zone, Remarks**

Ensure the auxiliary output configuration matches the system's intended linkage and alarm setups.

Remote Open

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Trigger an alarm sound or activate lighting remotely.

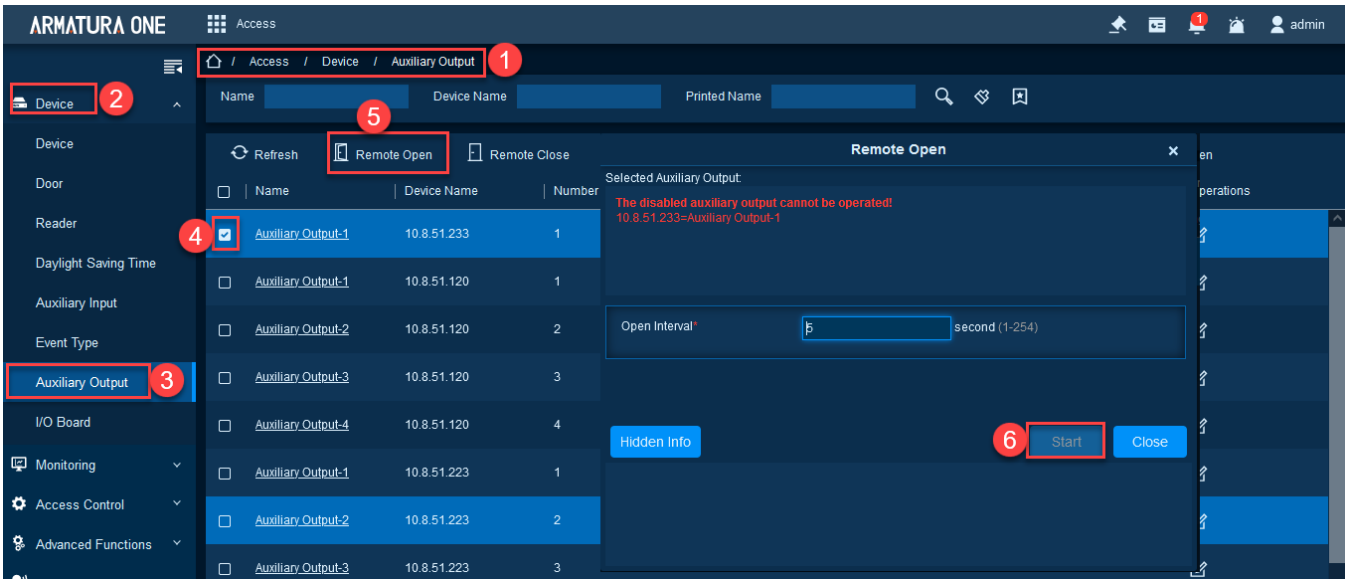
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Results

The auxiliary output is activated, initiating the connected device's operation.

Steps:

- Select the desired device.
- Click **[Remote Open]** to trigger the auxiliary output.



Remote Close

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Deactivate or close the auxiliary output.

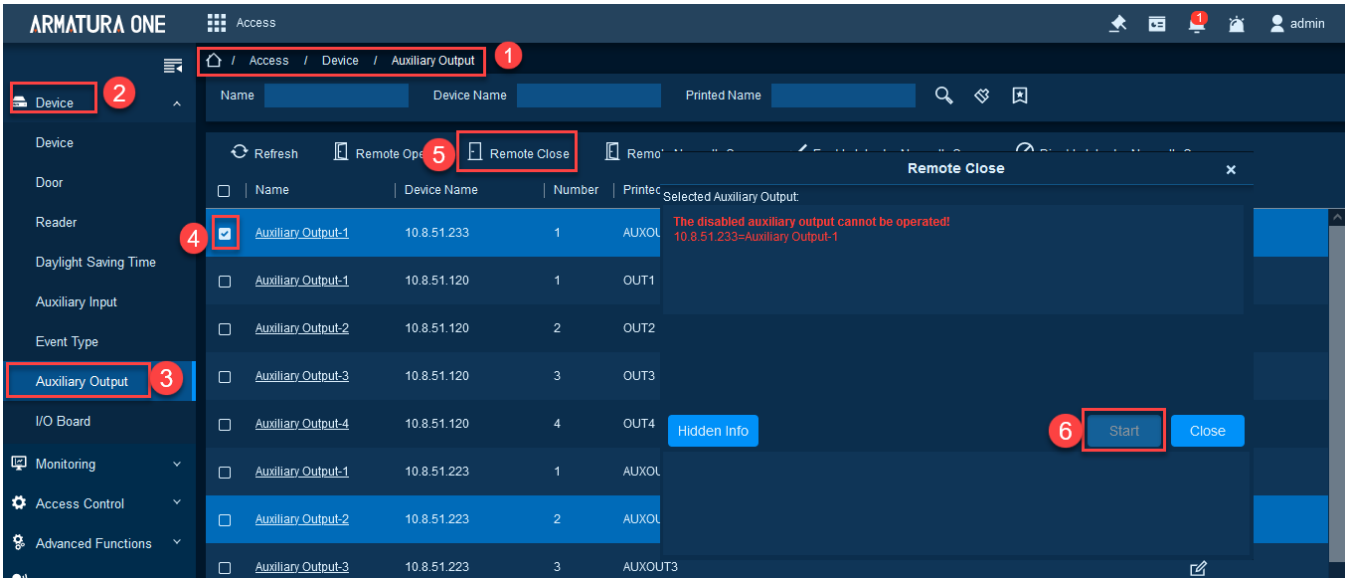
Trigger Results

The auxiliary output is deactivated to close the connection.

Steps:

- Select the desired device.
- Click **[Remote Close]** to deactivate the auxiliary output**.**

Copyright © 2024 ARMATURA LLC. All rights reserved



Remote Normally Open

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

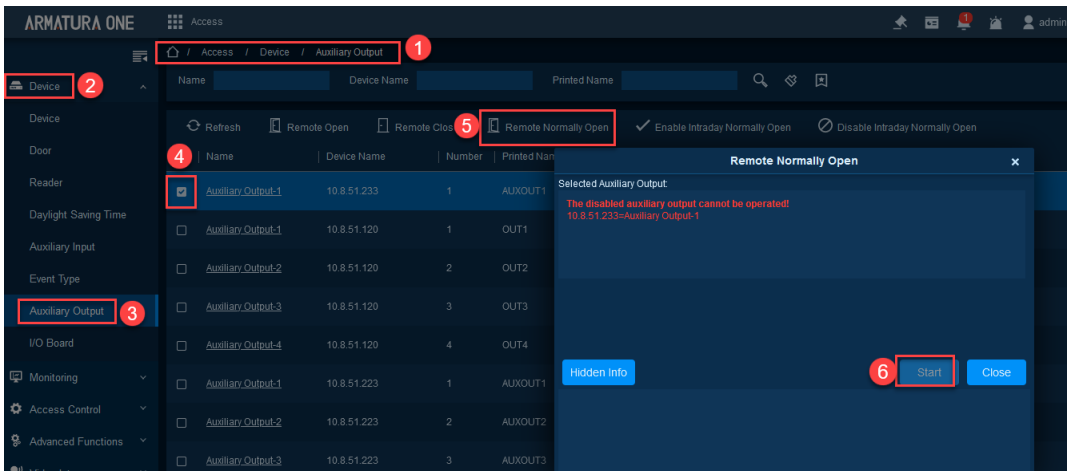
Keep the auxiliary output in a normally open state for a designated period.

Trigger Results

The auxiliary output remains open during the specified normal open time.

Steps:

- Select the desired device.
- Click **[Remote Normally Open]** to initiate the normally open state for the auxiliary output.



Copyright © 2024 ARMATURA LLC. All rights reserved

Enable Intraday Passage Mode Time Zone

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

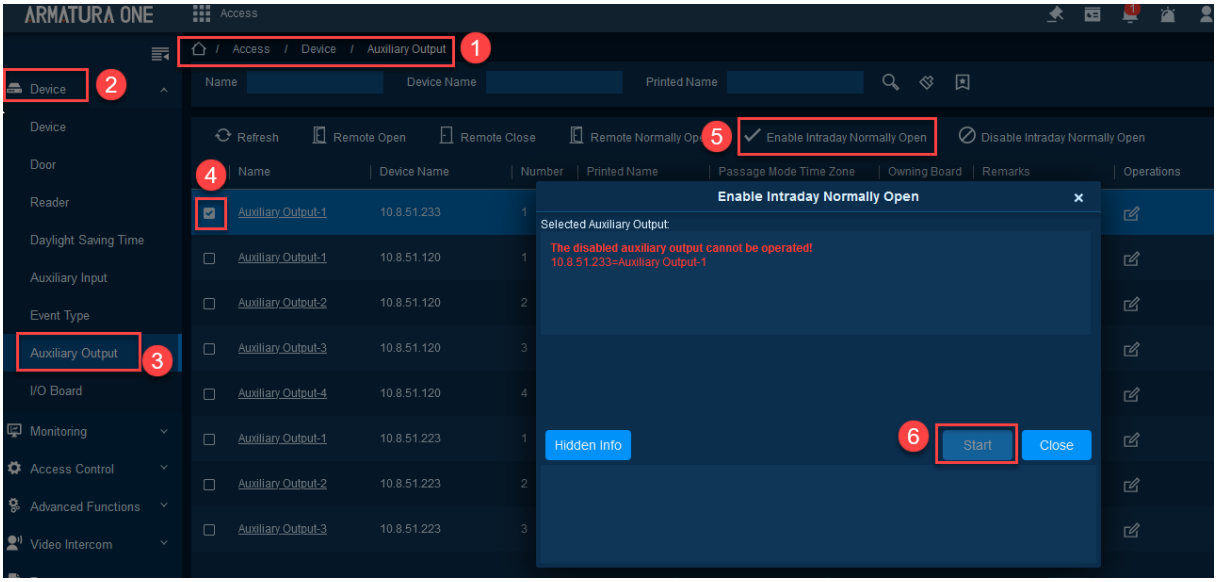
Open the auxiliary output during the designated normal open time.

Trigger Results

The auxiliary output is activated and remains open during the specified normally open time.

Steps:

- Navigate to **[Access] > [Device] > [Auxiliary Output]** to display the auxiliary output view page.
- Select the target device.
- Click **[Enable Intraday Passage Mode Time Zone]** to open the settings interface.
- Click **[Start]** to activate the normally open time zone for the day.



Disable Intraday Passage Mode Time Zone

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Prevents the use of the normally open time zone in special circumstances.

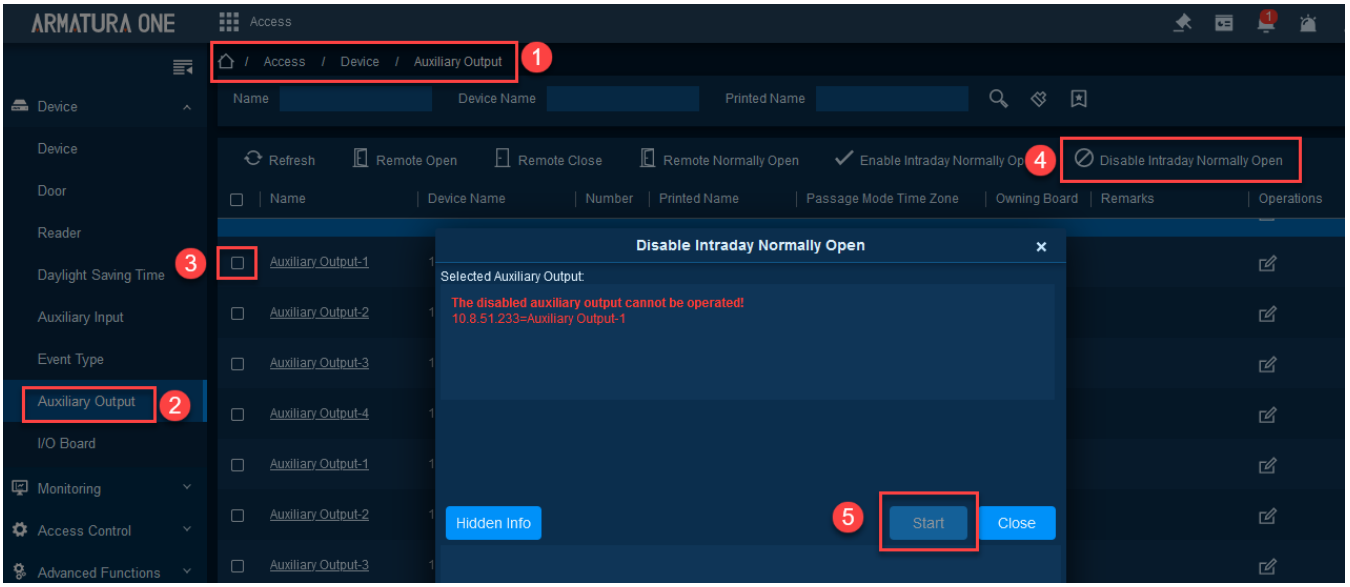
Trigger Results

The normal open time zone for the day is disabled, restricting free entry and exit during that time.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access] > [Device] > [Auxiliary Output]** to display the auxiliary output view page.
- Select the target device.
- Click **[Disable Intraday Normally Open]** to open the settings interface.
- Click **[Start]** to deactivate the normal open time zone for the day.



Note:

This feature is supported only by **AHSC-1000** and **AHDU-1X60** devices.

6.1.7. Event Type

Function Description

The **Event Type** section is used to display and manage various event types associated with the access control device. It provides detailed insights into event names, levels, serial numbers, and the ability to customize settings such as event sounds and standard operating procedures (SOPs).

Edit Event

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Required when the user needs to view or modify information related to a specific event type, including sound settings and standard procedures for handling events.

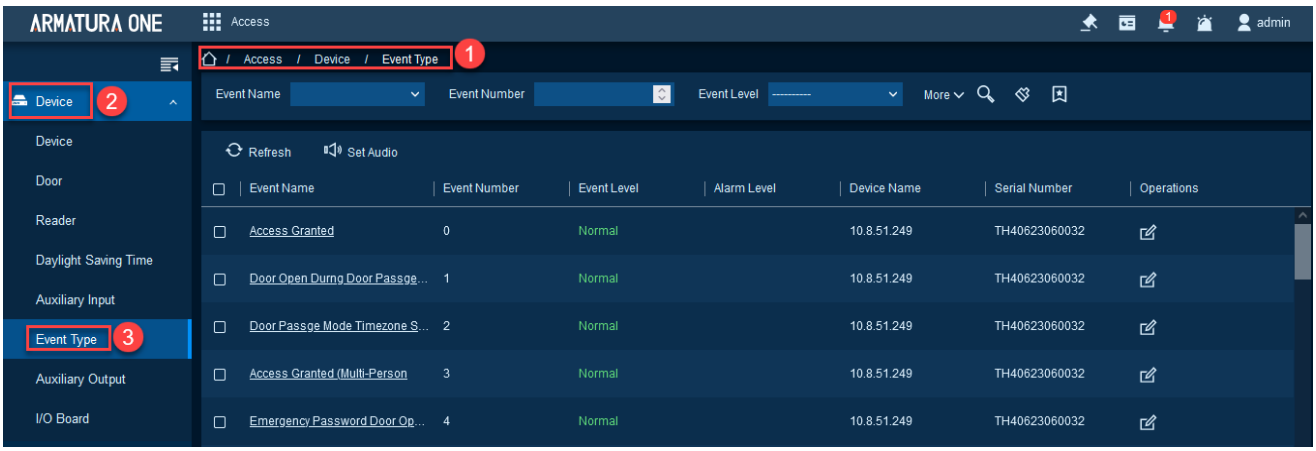
Trigger Result

Allows the user to view or edit details such as the event name, level, serial number, and sound settings, as well as upload related standard operating procedures.

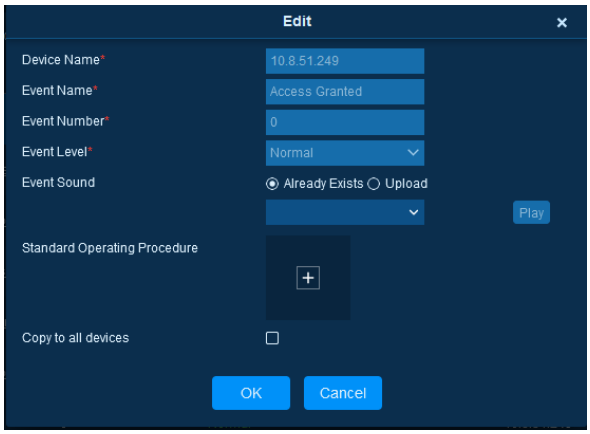
Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access] > [Device] > [Event Type]** to access the event type page.



- Locate the desired event and click **[Edit]** or the event name to modify the settings.



Modify the following fields as needed:

Device Name: Displays the corresponding device for the event type (non-editable).

Event Name: Displays the name of the event (non-editable).

Event Number: Displays the unique event number provided by the controller (non-editable).

Event Level: Choose from the following options: **Normal, Exception, Alarm**

Event Sound: Customize the sound to be played when the event occurs during real-time monitoring.

Standard Operating Procedures: Upload the standard operating procedure (SOP) file from your local computer. This document can include the specific steps for handling the event.
Copy the Above Settings to All Devices: Enable this option to apply the current event's configuration to all devices within the same user level that share the same event number.

Copyright © 2024 ARMATURA LLC. All rights reserved

- Click **[OK]** to save the changes and exit the edit interface.

Set Audio

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

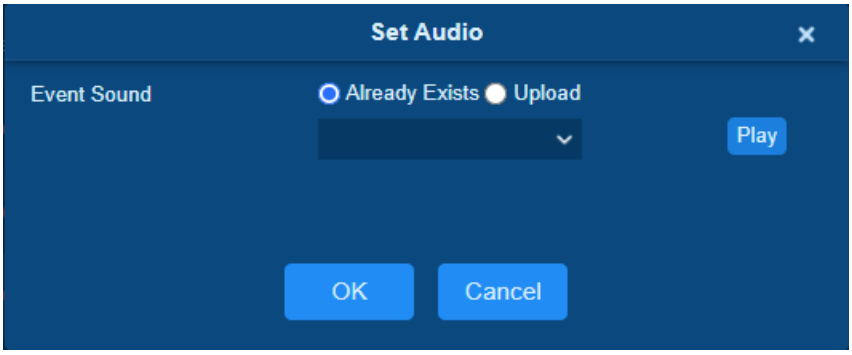
When specific events require a custom sound notification to alert users during real-time monitoring.

Trigger Result

Enables the user to assign or upload custom audio files for events.

Steps:

- Navigate to **[Access] > [Device] > [Event Type]** to view the list of events.
- Select the desired event from the list.
- Click **[Set Audio]** to open the audio configuration interface.
- Upload the desired audio file from your local PC:
  - The file must be in **.wav** or **.mp3** format.
  - The file size must not exceed **10MB**.
- After selecting the file, click **[OK]** to save the configuration.



Note:

Ensure the uploaded audio file is clear and appropriately descriptive for the event.

This feature is particularly useful for differentiating between events with similar triggers or levels.

Custom audio files should comply with organizational guidelines to maintain professionalism and avoid distractions.

6.1.8. Daylight Saving Time (DST)

Function Description

Daylight Saving Time (DST) is a system for adjusting local time to save energy by making better use of daylight. Clocks are moved forward by one hour during summer (DST start) and moved back by one hour in autumn (DST end).

For instance, during DST, clocks might be adjusted as follows:

- Start Time: "Second Monday in March, 02:00" (Clocks move forward by 1 hour).

Copyright © 2024 ARMATURA LLC. All rights reserved

- End Time: "First Sunday in November, 02:00" (Clocks move back by 1 hour).

The DST feature in the system allows for automated adjustments based on local requirements.

Add Daylight Saving Time

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

When local regulations or organizational needs require implementing Daylight Saving Time.

Trigger Results

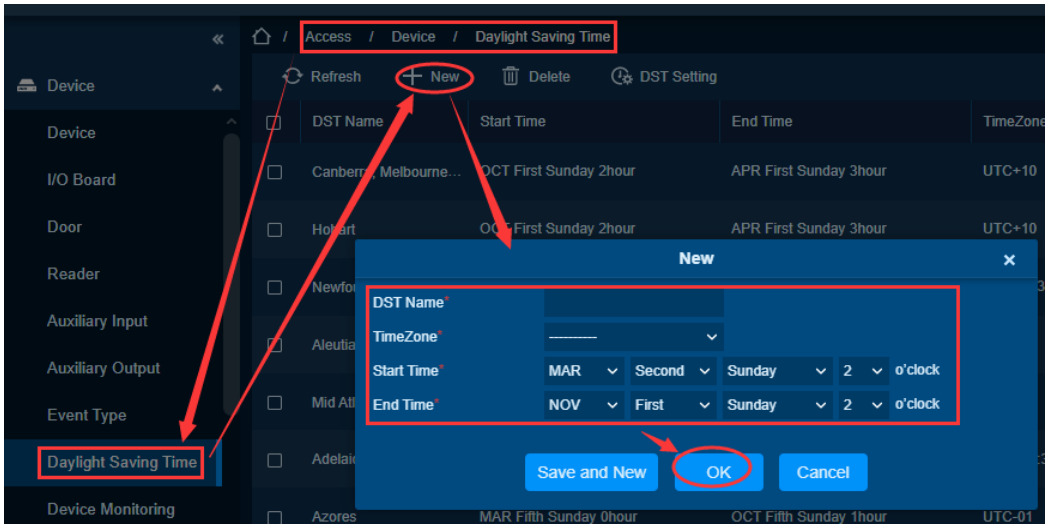
The system will automatically adjust the clock:

Move forward by one hour at the specified start time.

Move backward by one hour at the specified end time.

Steps:

- Go to **[Access]** > **[Device]** > **[Daylight Saving Time]** > **[New]** to create a new DST entry.
- Configure the following fields:
    - Start Time: Specify the start time in the format Month-Weeks-Week-Hour: Minute. For example: Second Monday in March, 02:00.
    - End Time: Specify the end time in the same format as above. For example: First Sunday in November, 02:00.
- Save the changes by clicking **[OK]**.



Edit Daylight Saving Time

Copyright © 2024 ARMATURA LLC. All rights reserved

Prerequisites for Use

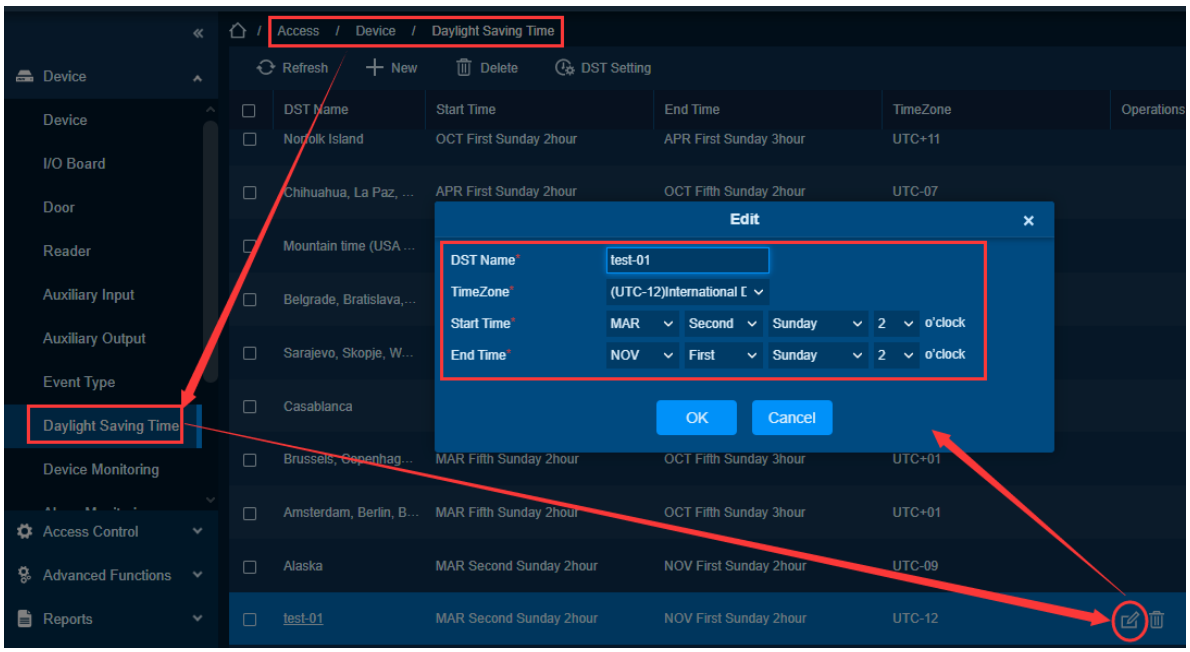
Log into the system using an account with the required permissions.

Usage Scenarios

When an existing DST entry needs to be updated due to changes in local regulations or correction of configuration errors.

Steps:

- Navigate to **[Access]** > **[Device]** > **[Daylight Saving Time]**.
- Select the desired entry and click **[Edit]**.
- Modify the required fields (e.g., start time, end time).
- Save the changes by clicking **[OK]**.



Delete Daylight Saving Time

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

When the DST feature is no longer required, or the existing configuration is incorrect and needs to be removed.

Trigger Results

The specified DST configuration will be deleted.

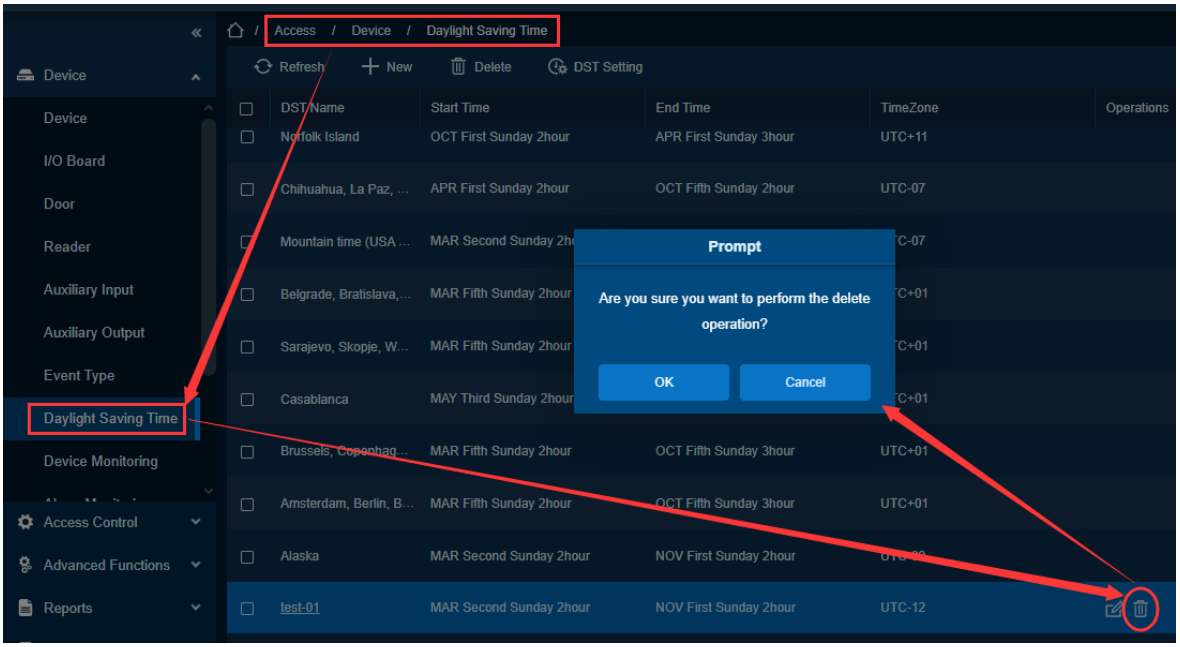
Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access] > [Device] > [Daylight Saving Time]** to display the list of configured entries.
- Select the DST entry to be deleted.
- Click **[Delete]** to open the confirmation dialog.
- Confirm the deletion by clicking **[OK]**.

Note:

- The system uses the "Month-Weeks-Week-Hour: Minute" format for DST configuration.
- Ensure the DST settings comply with local regulations or organizational requirements.
- Verify that devices connected to the system support DST adjustments.



Copyright © 2024 ARMATURA LLC. All rights reserved

6.2. Monitoring

Functions	Operation Instructions
Device Monitoring	Clear commands, view commands, clear all commands.
Real-Time Monitori	Perform actions such as remotely opening/closing doors auxiliary input/output controls, cancelling alarms, remote lock/unlock, remote normally open, and enabling/disablir the day's normally open time zone.
Topology Managem	Quickly check if any device, reader, or I/O expansion bo is offline from the Status Monitoring admin view.

6.2.1. Device Monitoring

Function Description

Device Monitoring allows users to view and manage all devices within their authorized access level. The system displays device operation information, including:

- Device Name
- Serial Number
- Area
- Operation Status
- Current Status
- Command List
- Related Operations

To access Device Monitoring, click **[Access] > [Device Monitoring]**.

Export Device Monitoring Data

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

When event data needs to be exported for analysis or record-keeping.

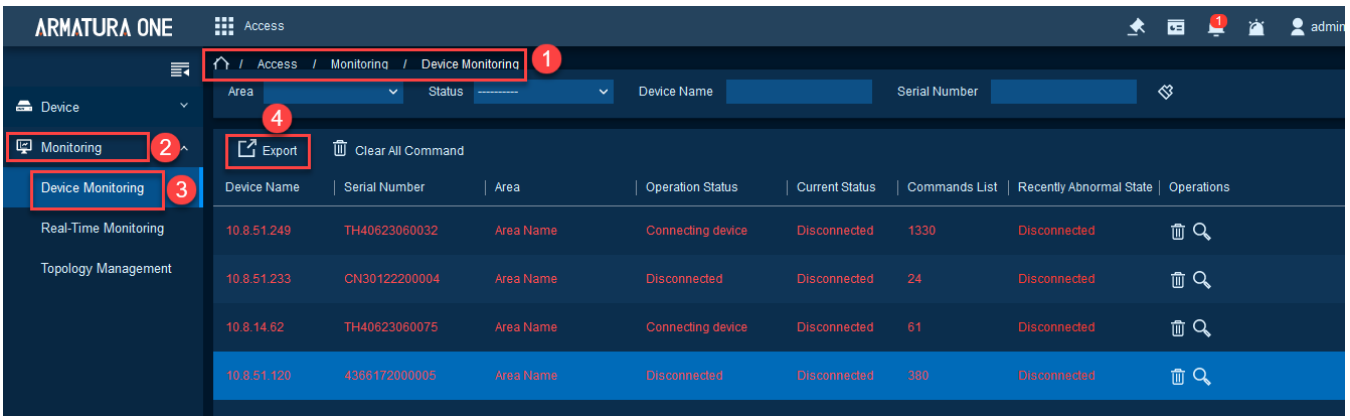
Trigger Result

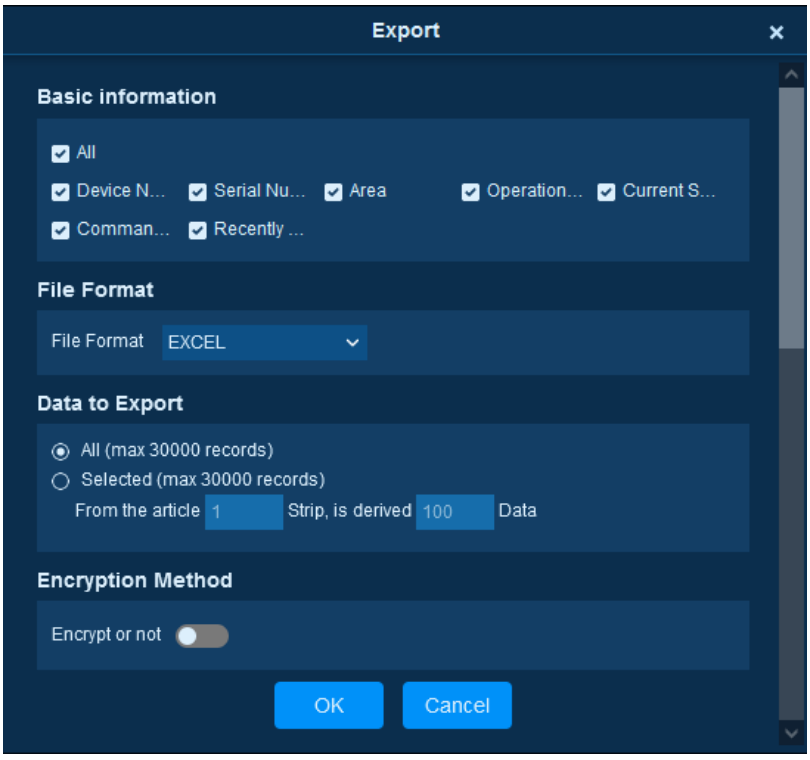
Exports data for all devices or a selected subset.

Steps:

- Navigate to **[Access]** > **[Device Monitoring]** to access the interface.

Copyright © 2024 ARMATURA LLC. All rights reserved





- Select the desired device(s) and data to export.
- Choose the file format: EXCEL, PDF, or CSV.
- Save the exported file to your local machine.

Device Monitoring

Device Name	Serial Number	Area	Operation Status	Current Status	Commands List	Recently The Abnormal State
192.168.218.60	20100501999	Area Name	Get real-time event	Normal	0	None

Delete

Prerequisites for Use

Log into the system using an account with the required permissions.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

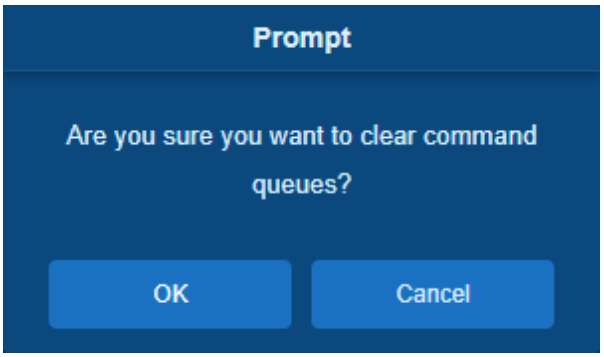
Clear unnecessary commands from the list.

Trigger Result

Deletes specific or all pending commands for a device.

Steps:

- Go to **[Access]** > **[Device Monitoring]**.
- Select the desired device and click **[Clear Command]** in the operations column.
- Confirm the action by clicking **[OK]**.



Note:

- After clearing commands:
- Perform the **Synchronize All Data to Devices** operation to re-synchronize data between the software and the device.
- Synchronization cannot occur if the device's user or fingerprint capacity is fully utilized. In this case:
    - Replace the device with one that has a higher capacity, or
    - Reduce the number of authorized users for the device.
- The "Operate State" indicates the current communication content of the device and is primarily used for debugging.
- A **command queue** with more than 0 commands means data synchronization is incomplete. Wait for synchronization to finish before performing further operations.

Clear Command

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

When commands are frozen or backed up.

Trigger Results

Deletes all commands in the queue for a selected device.

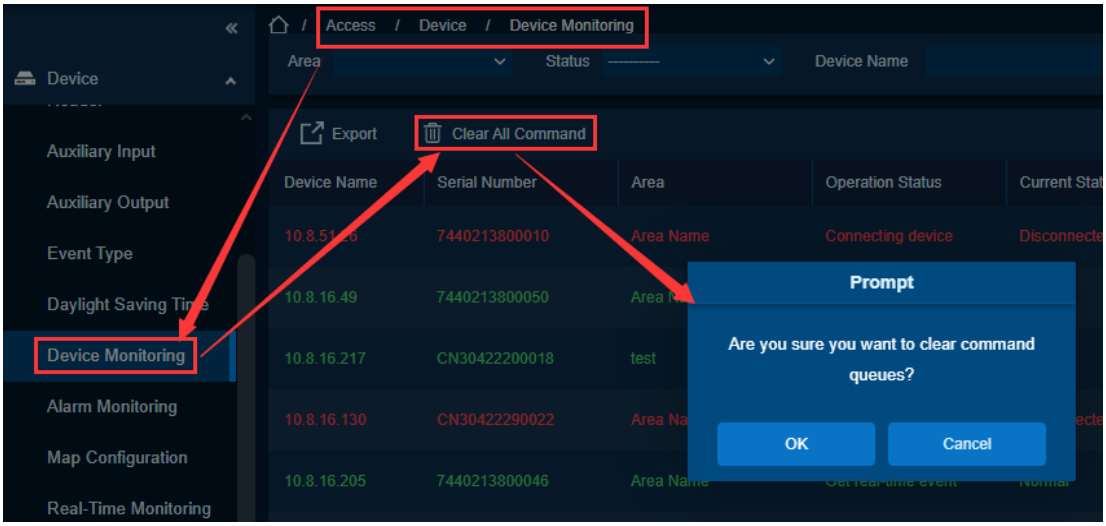
Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Go to **[Access] > [Device Monitoring]**.
- Click **[Clear All Command]** from the Action Menu.
- Confirm the action by clicking **[OK]**.

Note:

Clearing commands may require re-synchronization if data is not fully uploaded to the device.



6.2.2. Real-Time Monitoring

Function Description

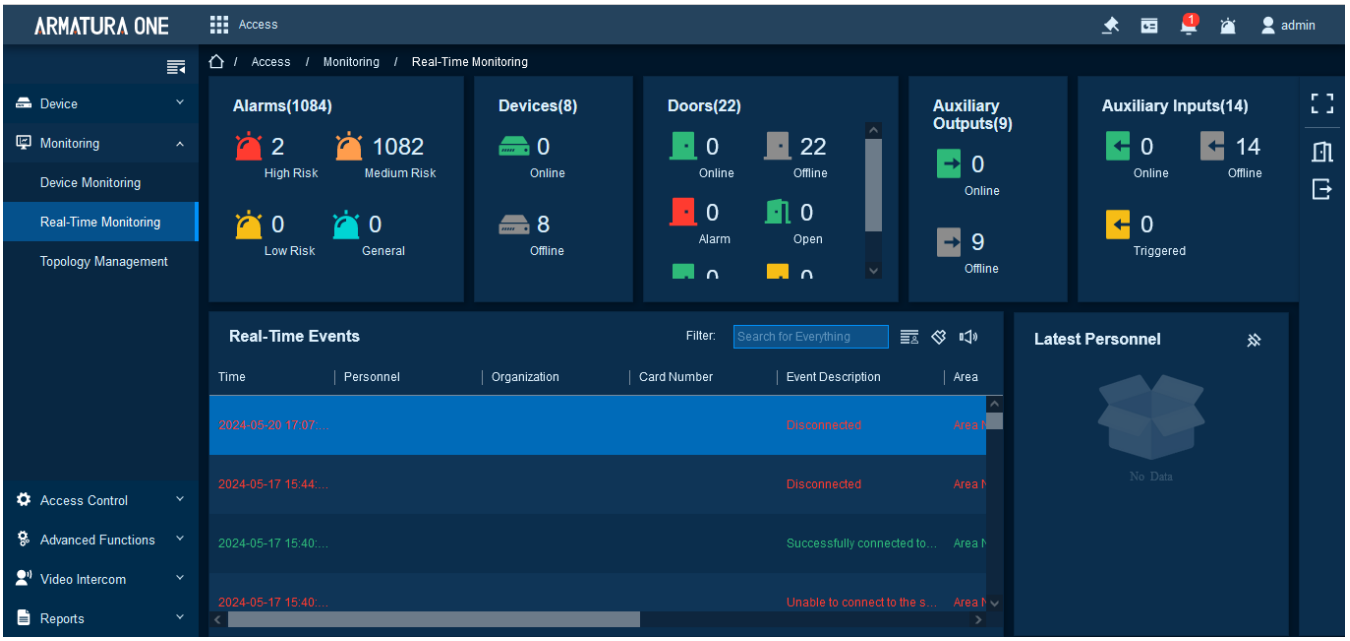
The **Real-Time Monitoring** feature allows users to monitor the status and events of doors under the access control panels in real-time. This includes:

- Device status
- Event status
- Door status
- Real-Time Alarms
- Real-Time Events

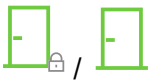
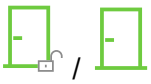
The Real-Time Monitoring interface provides visual indicators for each status, represented by different icons.

Real-Time Monitoring Interface

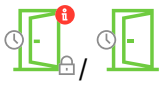
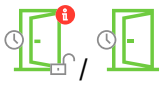
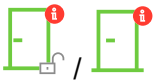
Copyright © 2024 ARMATURA LLC. All rights reserved



The interface displays real-time status updates with icons representing various device and door conditions. The table below explains the meaning of each icon and its corresponding status:

Icons	Status	Icons	Status
	Device Disabled		Door Offline
	Door Sensor Not Set, Relay Closed /Without Relay Status		Door Sensor Not Set, Relay Opened/Without Relay Status
	Online Door Status Closed, Relay Closed/Without Relay Status		Online Door Status Closed, Relay Opened/Without Relay Status
	Online Door Status Opened, Relay Closed/Without Relay Status		Online Door Status Opened, RELAY Opened/Without Relay Status
	Door Opened Alarm; Relay Closed		Door Opened Alarm; Relay Opened

Copyright © 2024 ARMATURA LLC. All rights reserved

	Door Opening Timeout, Relay Closed /Without Relay Status, Door Sensor Opened		Door Opening Timeout, Relay Opened/Without Relay Status
	Door Opening Timeout, Relay Closed/ Door Sensor Closed		Door Opening Timeout, Relay Opened/ Door Sensor Closed
	Door Closed Alarm, Relay Closed/Without Relay Status		Door Closed Alarm, Relay Opened/Without Relay Status
	Door Sensor Not Set, Door Alarm, Relay Closed		Door Sensor Not Set, Door Alarm, Relay Opened
	Door Opening Timeout, Without Relay Status/Door Sensor Closed		Door Locking
	Door Always Locked		Door Closed
	Door Closed Unlocked		Door Disabled
	Door No Sensor		Door No Sensor Old
	Door No Sensor Unlocked		Door Offline
	Door Offline to Device		Door Open Timeout Old

Copyright © 2024 ARMATURA LLC. All rights reserved

	Door Opened		Door Opened
	Door Opened Unlocked		
Note: If there is no relay status displayed, it means the current firmware does not support the "detect relay status" function.			

Event Monitoring

Prerequisites for Use

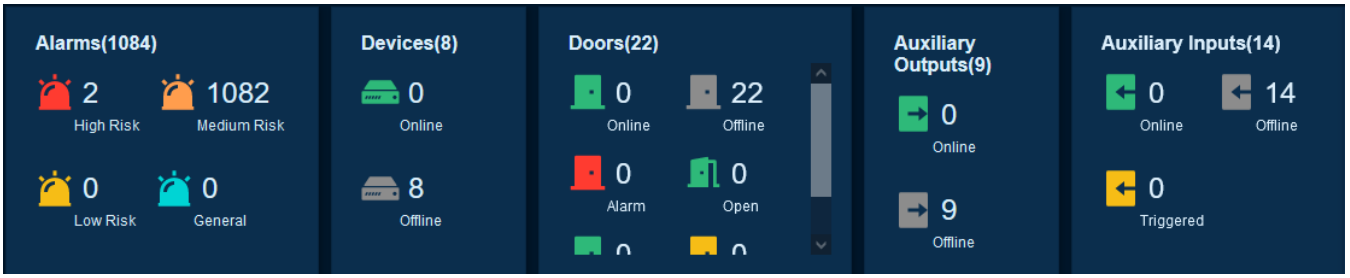
Log into the system using an account with the required permissions.

Usage Scenarios

The Event Monitoring feature allows users to view the real-time status of devices directly from the software and monitor and respond to alarms and events as they occur. This functionality ensures that administrators can actively manage and maintain device operations while addressing issues promptly.

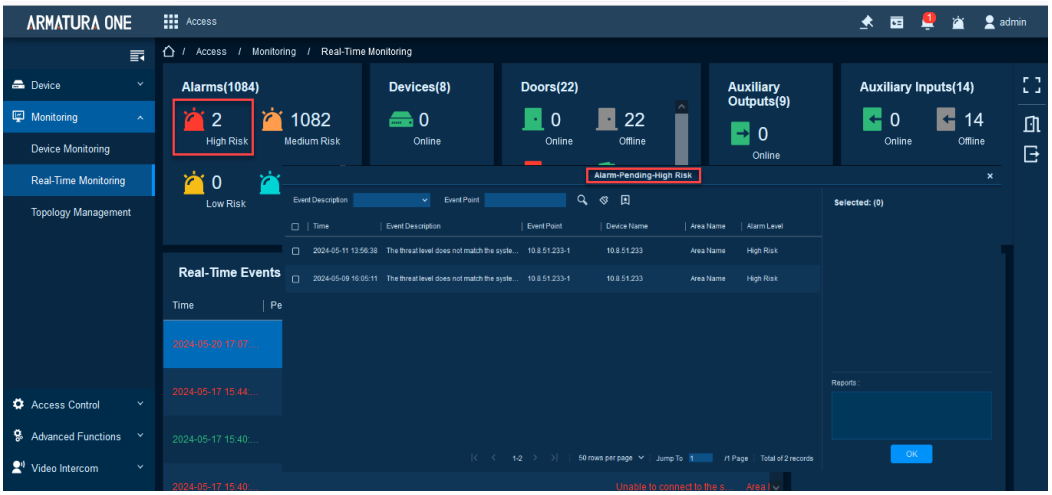
Illustration

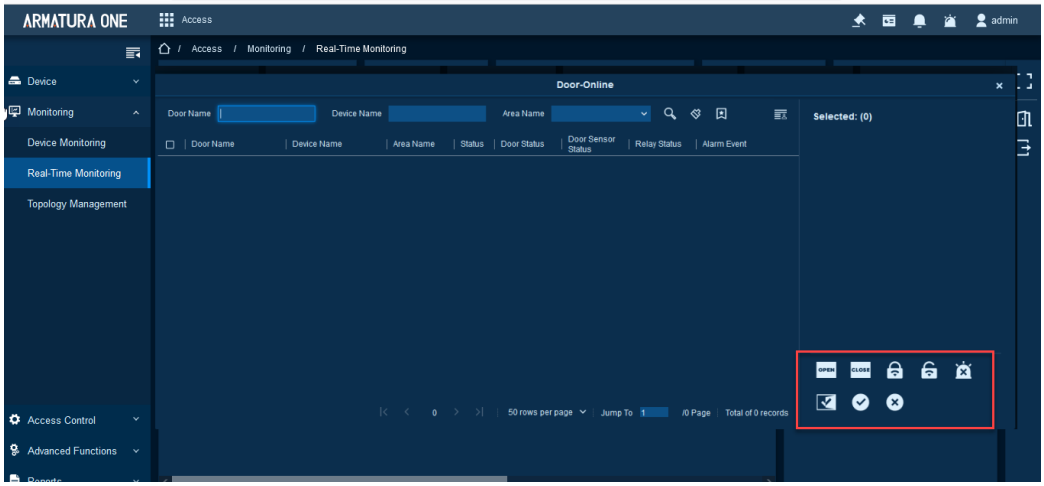
The Event Monitoring interface provides a device status preview to view the current status of devices in real-time. It also includes alarm details, such as the number of alarms per device, the overall status of events, and the number of alarm events.



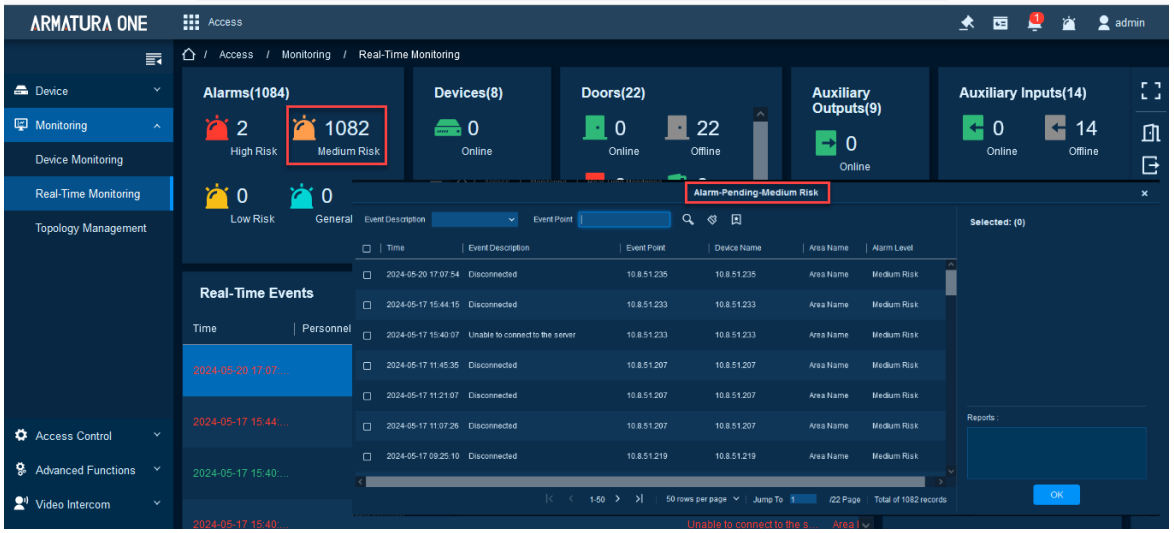
Alarm-Pending-High Risk

Copyright © 2024 ARMATURA LLC. All rights reserved





Alarm-Pending-Medium Risk



Door Monitoring

Copyright © 2024 ARMATURA LLC. All rights reserved

Prerequisites for Use

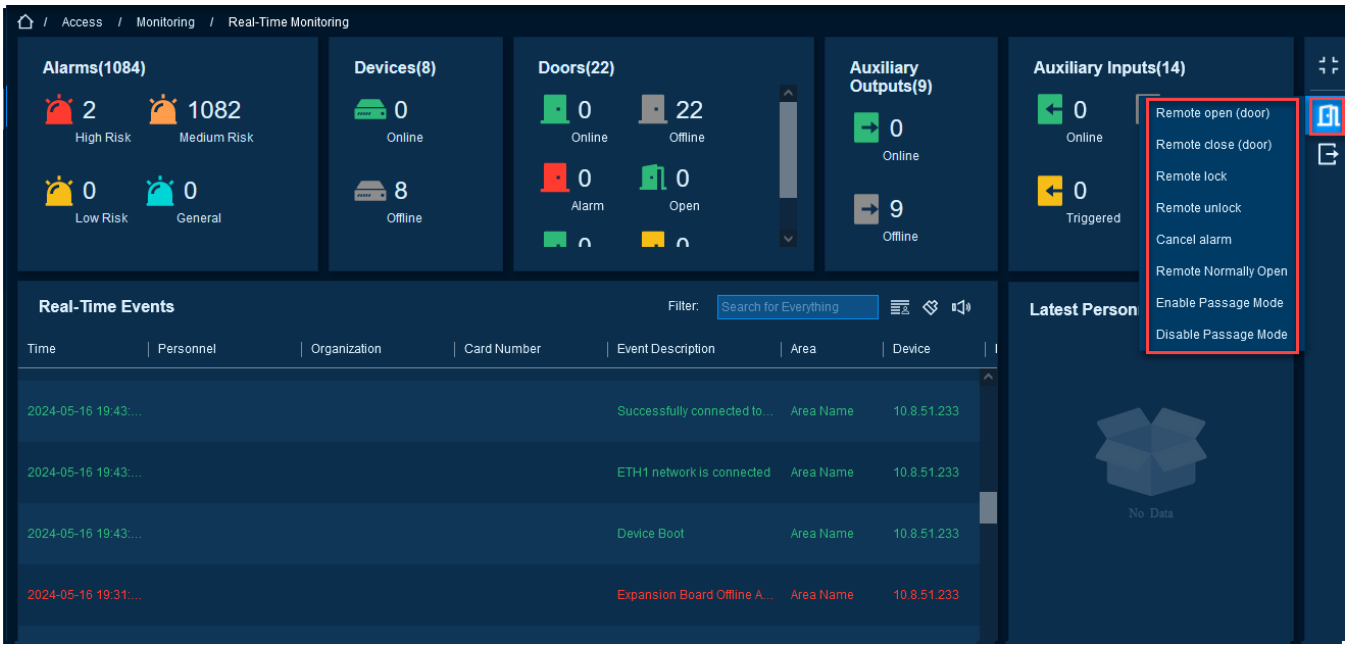
Log into the system using an account with the required permissions.

Usage Scenarios

Monitor the **real-time status** of doors in the system. Perform remote operations such as opening, unlocking, and cancelling alarms.

Trigger Results

View the **real-time status** of devices and doors, and provide a visual representation of door statuses, enabling quick and effective control.



Key Operations

Remote Opening/Closing

Control one or multiple doors remotely.

Steps:

- Select the desired door(s).
- Click **Batch Operation** and choose **[Remote Opening/Closing (Door)]**.
- Confirm the action by clicking **[OK]**.

Note:

The user can define the door opening duration (default is 15 seconds). For continuous access, enable **Passage Mode** or set the door to **Normal Open**.

Remote Lock

Lock the door remotely to prevent any operations, including card reading or remote access.

Copyright © 2024 ARMATURA LLC. All rights reserved

Only supported by specific devices.

Remote Unlock

Unlock a locked door remotely.

Only supported by specific devices.

Cancel Alarms

Cancel the alarm sound for a single door or all doors.

Steps:

- Hover over the door icon displaying the alarm.
- Select **[Cancel Alarm]** from the menu.

Note:

If the alarm cancellation fails, verify that all devices are connected and check the network status.

Remote Normally Open

- **Set the door to Normal Open.**

Enable Passage Mode

- **Enable the door's normally open mode during a specified time quantum.**

Disable Passage Mode

- **Disable the door's normally open mode during a specified time quantum, reverting it to normal operations.**

Note:

- During **remote opening**, users can define the opening duration. Select **[Enable Passage Mode]** to activate continuous access or **Normal Open** to keep the door open for 24 hours.
- Before closing a door, ensure **[Disable Passage Mode]** is selected to avoid enabling other open time zones. Follow this by selecting **Remote Closing** for proper closure.

Auxiliary Input Monitoring

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Monitor the **real-time events** of auxiliary inputs via the software for event tracking and system operation.

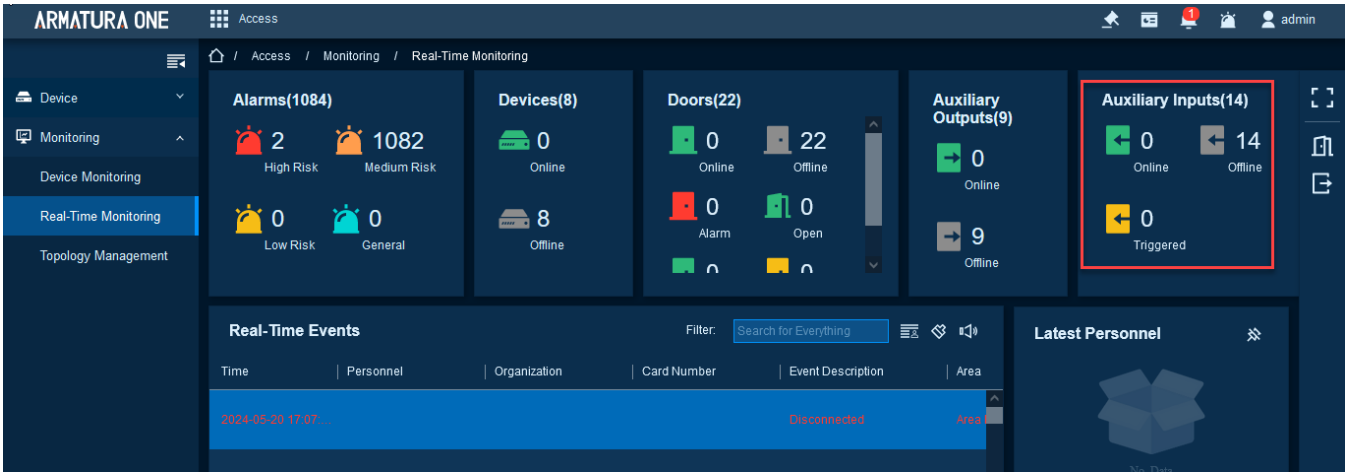
Trigger Result

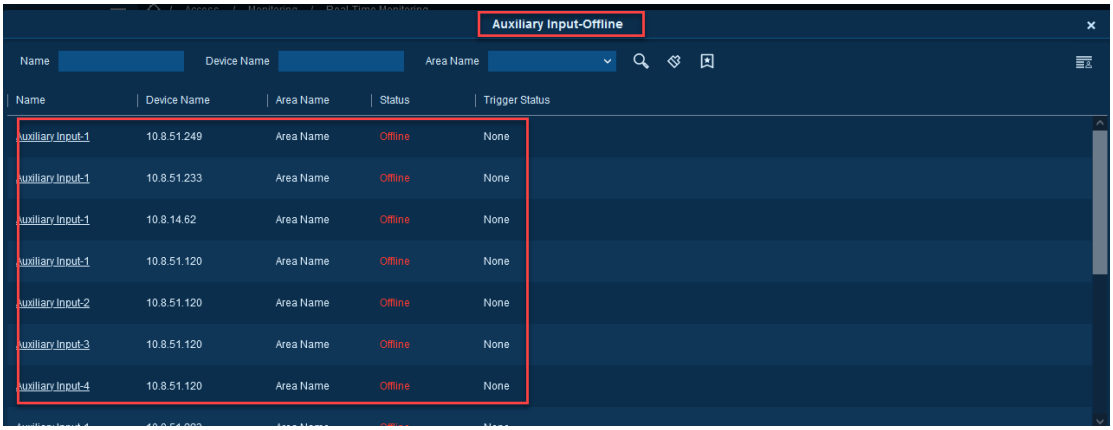
Displays real-time auxiliary input events in the monitoring interface.

Copyright © 2024 ARMATURA LLC. All rights reserved

Interface Overview

The **Auxiliary Input Monitoring** interface shows the status of auxiliary inputs, enabling quick identification of events and statuses.





Auxiliary Output Monitoring

Prerequisites for Use

Log into the system using an account with the required permissions.

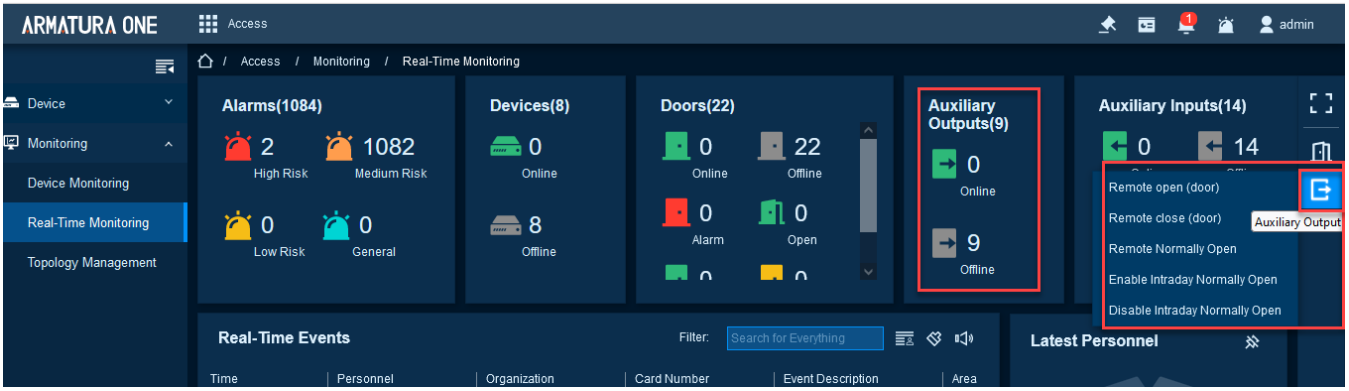
Usage Scenarios

Control devices remotely through three main operations: Remote Open to temporarily activate the output, Remote Close to deactivate the output, and Remote Normally Open to maintain the output in an active state. These controls are essential for managing connected peripheral devices such as alarms, lighting systems, and other equipment.

Trigger Result

Enables remote operation of auxiliary output devices through the centralized monitoring interface.

Copyright © 2024 ARMATURA LLC. All rights reserved



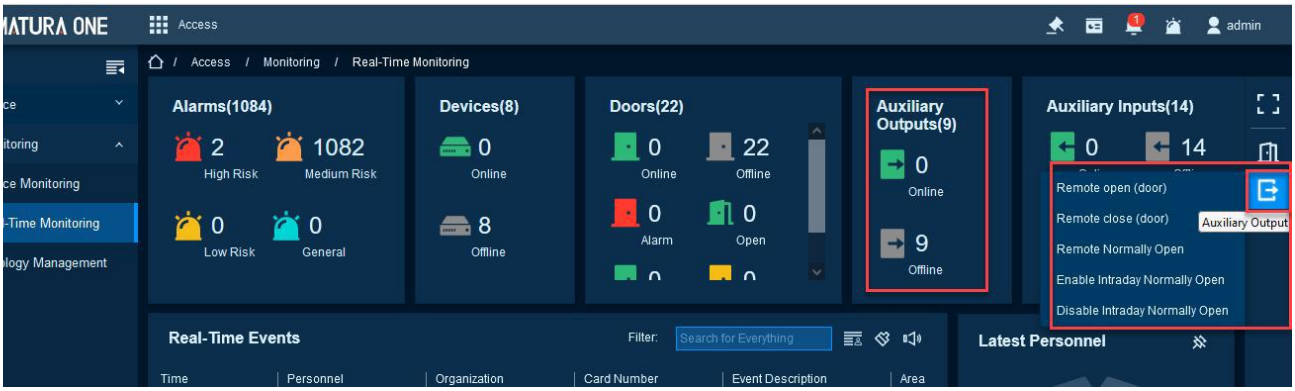
Auxiliary Output Operations

Remote Opening/Closing

Control one or multiple auxiliary output devices remotely.

Steps:

- Select the desired auxiliary device(s).
- Choose the operation:
    - Remote Open
    - Remote Close
    - Remote Normally Open
- For batch operations:
    - Select Batch Operation.
    - Click **[Remote Opening/Closing]**

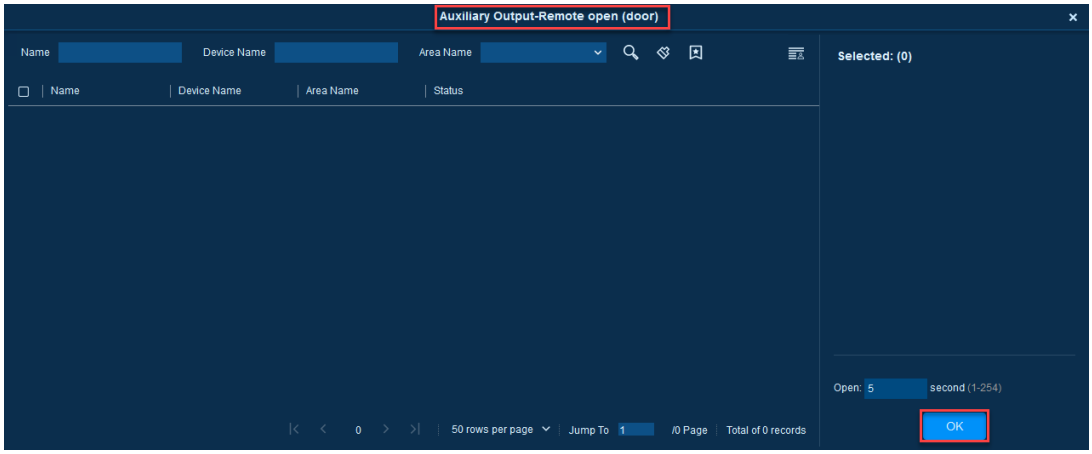


Remote Opening/Closing (Doors):

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

1. Select Device(s):
    - To control a single auxiliary device or all auxiliary devices, select the desired option from the interface.
2. Perform Batch Operation:
    - Click **[Batch Operation]** and choose **[Remote Opening/Closing (Doors)]**.
3. Confirm Action:
    - Click **[OK]** to execute **[Remote Opening/Closing (Doors)]**.



Remote Normally Open: Sets the auxiliary device to a Normal Open state.

Enable Intraday Normally Open: During the specified normally open time, the auxiliary output remains open. The auxiliary output operates in a **Normal Open** state during the designated time period.

Disable Intraday Normally Open: Disables the **Normal Open** time zone for the day. Prevents entry and exit during the normally open time zone by disabling the auxiliary output's **Normal Open** state.

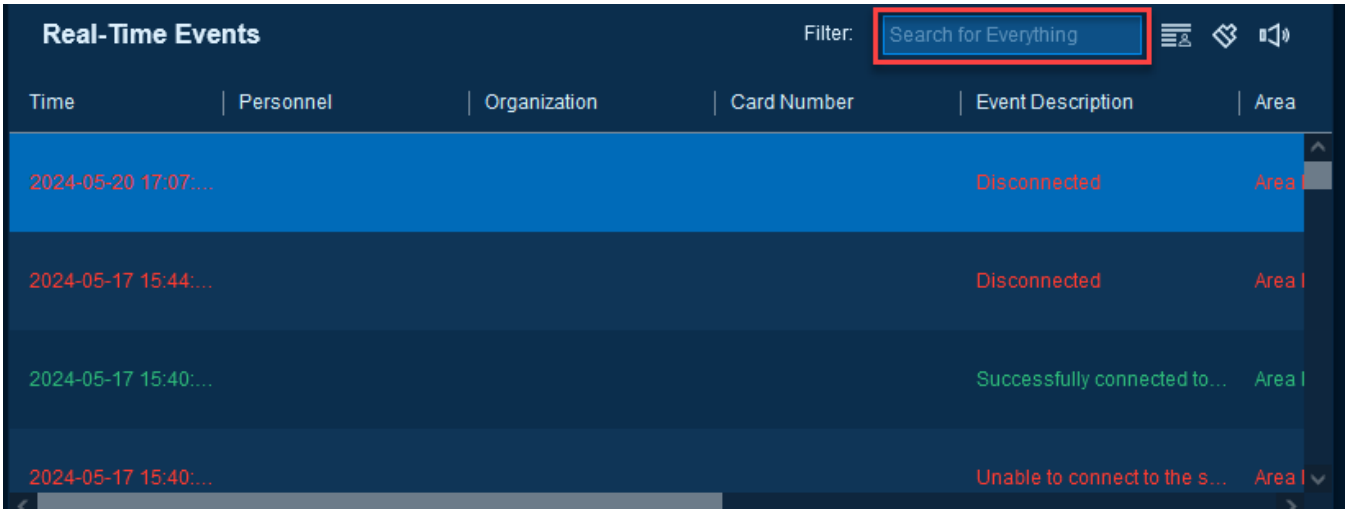
Search device And Filter: System supports **searching** for devices by partial or complete identifiers.

Filtering Options:

- Filter devices by:
    - **Door Status**
    - **Relay Status**
    - **Auxiliary Input Status**
    - **Auxiliary Output Status**

This feature allows efficient device management and status monitoring.

Copyright © 2024 ARMATURA LLC. All rights reserved



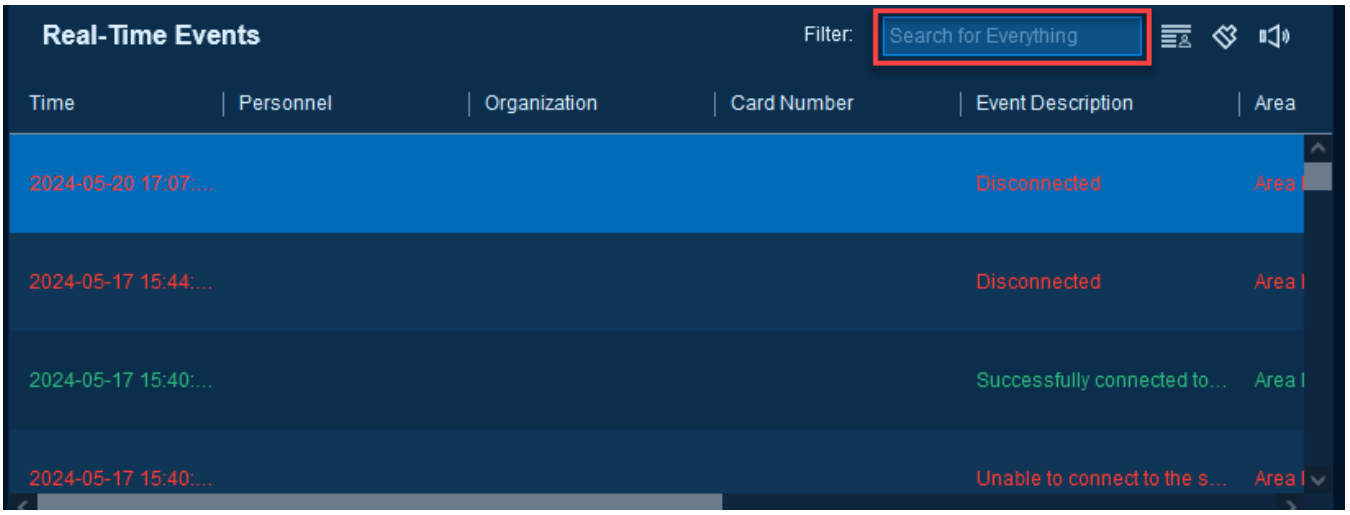
Real Time Alarm

The **Real-Time Alarm** interface provides a clear overview of all alarm events. Users can access detailed information for each alarm, including:

- **Event Description**
- **Event Time**
- **Event Point**
- **Alarm Level**
- **Personnel Information**

The interface displays alarms in real time, categorized by event type, time, and associated personnel or devices.

Enables users to quickly pinpoint the source and status of alarms for prompt resolution.



Copyright © 2024 ARMATURA LLC. All rights reserved

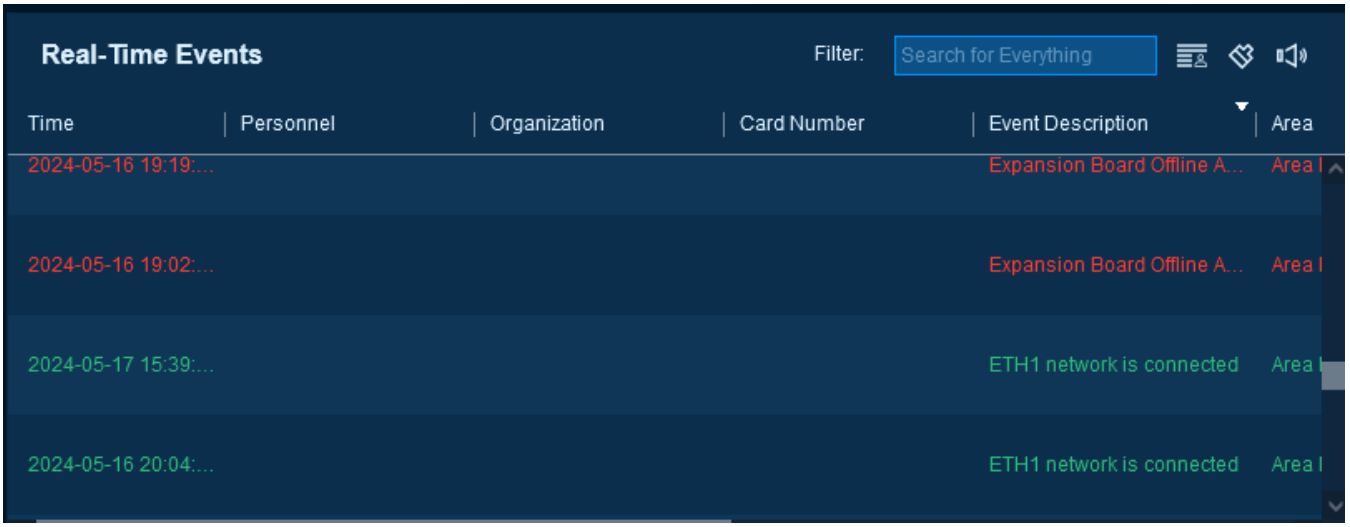
Real-Time Events

The **Real-Time Events** section records all events from connected devices. It categorizes events into:

- **Emergency Events**
- **Important Events**
- **General Events**
- **Prompt Events**

The interface provides a consolidated list of events with details such as Event Type, Timestamp, Related Device or Personnel, and Event Status.

It monitors ongoing activities and events across devices, and track critical system alerts and operational statuses.

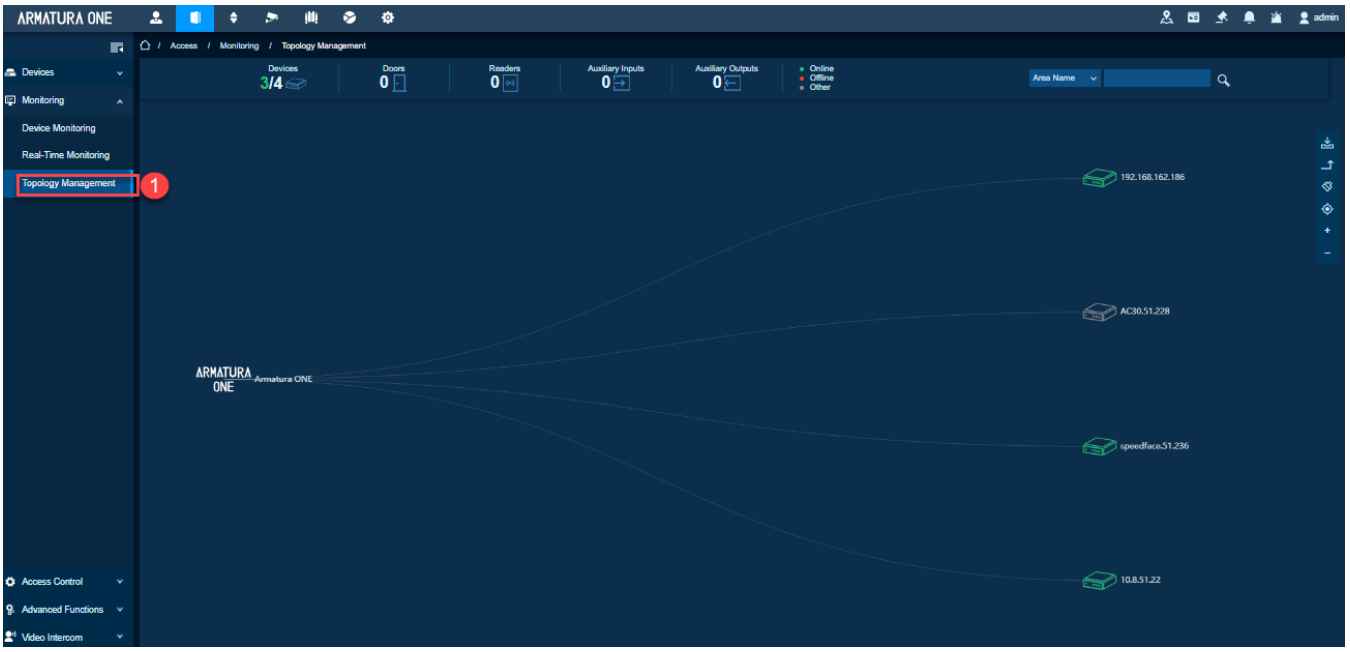


Copyright © 2024 ARMATURA LLC. All rights reserved

6.2.3. Topology Management

Function Description

Topology Management provides a detailed and interactive map to visualize the relationships between controllers, doors, readers, and I/O expansion boards. It serves as a central interface to monitor the system's hierarchical structure and operational status.



Status Monitoring

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Quickly identify if a device, reader, or I/O expansion board is offline.

Capabilities

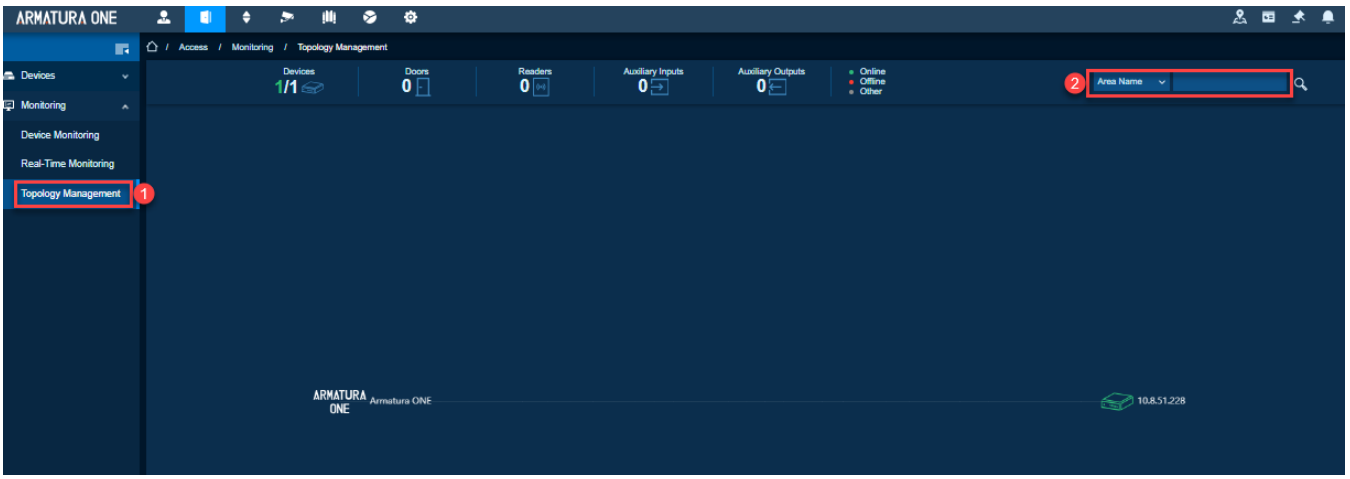
Provides real-time status of connected components for quick diagnostics.

Topology Map

The topology map enables users to:

- Visualize the system's architecture, including controllers, doors, readers, and I/O relationships.
- Navigate through the hierarchical structure using intuitive controls.

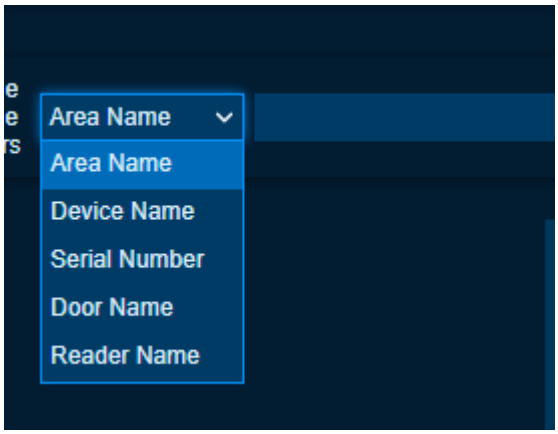
Copyright © 2024 ARMATURA LLC. All rights reserved



Supported Functions

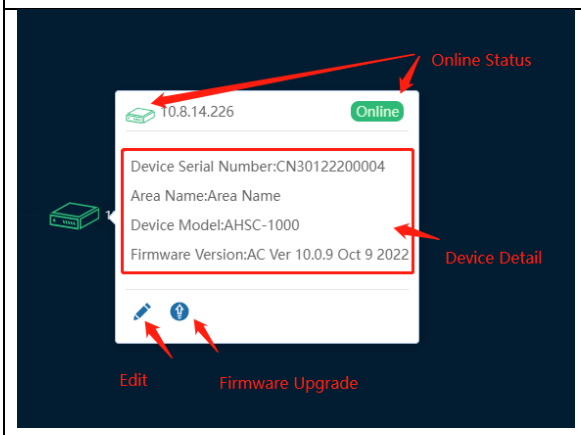
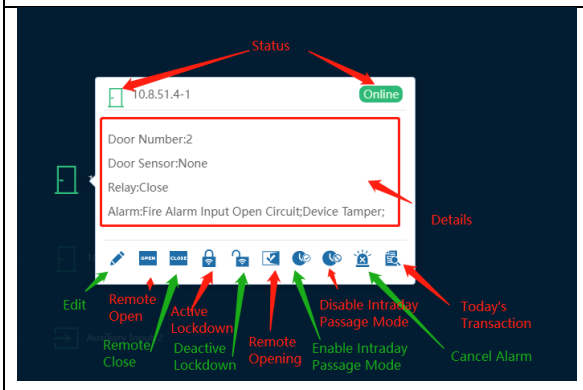
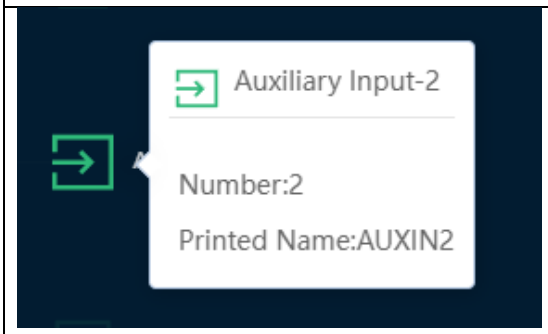
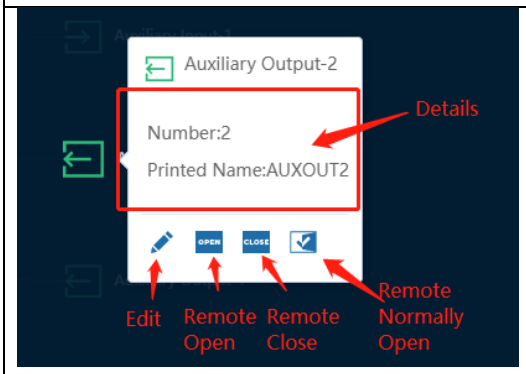
Search and Filter:

- Search by **Area Name**, **Device Name**, **Serial Number**, **Door Name**, or **Reader Name** to quickly locate components.



Icon	Introduction
Download	Save the topology map as a .png file
Back to previous level	Navigate backwards in the hierarchy
Refresh	Update the map to display the latest status
Location	Center the map on a specific component
Zoom IN	Adjust the map view with zoom buttons or the mouse scroll wheel
Zoom Out	Adjust the map view with zoom buttons or the mouse scroll wheel

Copyright © 2024 ARMATURA LLC. All rights reserved

View	Introduction
	**Device Monitoring** Device Status Green: Online Red: Offline Grey: Unknown
	**Door Monitoring** Door Status Green: Online Red: Offline Grey: Unknown
	**Aux IN Monitoring** • Monitors the operational state of auxiliary inputs.
	**Aux Out Monitoring** • Monitors the operational state of auxiliary outputs.

Copyright © 2024 ARMATURA LLC. All rights reserved

6.3. Access Control

Functions description:

The **Access Control** module enables the configuration and management of access control devices. It supports advanced features such as time settings, access level assignments by personnel and departments, interlocking, linkage, anti-passback, and more.

Function List:

Function	Description
Time Zones	Manage time zones for access control operations. Add, edit, delete time zones.
Holidays	Configure holiday settings for access control devices. Add, edit, delete holidays
Access Levels	Manage access levels and their associated doors. Add, edit, add doors, door control-remote door open, door control-remote door close, door control-cancel alarm, door control-remote normally open, door control-enable, door control-disable, door control-remote lock, door control-remote unlock, door control-enable the day's normally open time zone, door control-disable the day's normally open time zone, delete the door, export.
Set Access by Levels	Configure access for personnel based on access levels. Add, delete, export personnel.
Set Access by Person	Assign access control settings to individual personnel. Access control settings, add belonged access levels, delete belonged access levels, export.
Set Access by Department	Assign default access levels to departments. Add default access levels, delete default access levels.
Interlock	Manage interlocking functionality between multiple doors. Add, edit, delete
Linkage	Configure actions triggered by specific events. Add, edit, delete
Anti-passback	Prevent unauthorized re-entry without first exiting. Add, edit, delete
First Person Normally Open	Configure doors to remain open once a designated person accesses them. Add, edit, delete personnel.
Multi-person Group	Manage groups requiring multiple individuals for access. Add, edit, delete personnel.
Multi People Opening Door	Require multiple people to verify for door access. Add, edit, delete.
Verification Mode	Configure door verification methods (e.g., card, PIN, biometrics). Add, edit, delete door.
Verification Mode Group	Manage personnel assigned to specific verification mode groups. Add, delete personnel.
Parameter Settings	Configure system-wide parameters for access control. Type of Getting Transactions setting, Transactions Auto-Export setting, Real Time Monitoring setting, Compare photo delivery settings.

Copyright © 2024 ARMATURA LLC. All rights reserved

6.3.1. Time Zones

Function Description

The **Time Zones** feature allows users to configure specific time intervals during which doors can be opened or closed, as well as define access periods for various device functions. Time Zones ensure precise control over door operations and device access.

Add Time Zone

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

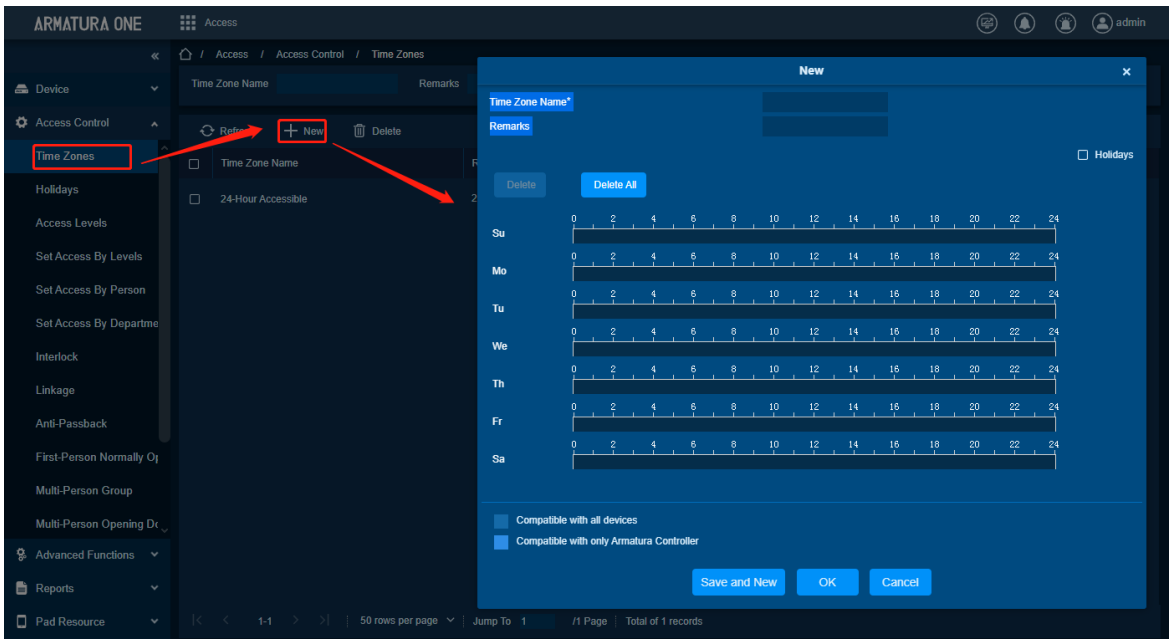
Doors need to be accessible only during specific time intervals, and users or readers may require restricted access to specified doors based on time. Time Zones are utilized for features such as defining normal open periods, setting access levels to restrict door access to specific users during defined periods, and configuring first-person normally open settings.

Trigger Results

Time Zones determine the usability of doors and readers during valid time periods, and outside the defined intervals, access is restricted. The system supports up to 255 Time Zones, each with configurable time intervals.

Steps:

- Go to **[Access Control] > [Time Zones] > [New]** to open the time zone configuration interface.



Configure the Time Zone Parameters:

- **Time Zone Name**: Enter a unique name for the Time Zone (up to 30 characters).
- **Remarks**: Provide a detailed description of the Time Zone, including its purpose and primary applications (up to 50 characters).

Copyright © 2024 ARMATURA LLC. All rights reserved

- Each Time Zone includes **three intervals** for each day of the week and for **three holiday types**.
- Define the Start and End Times for each interval in the format **HH:MM-HH:MM**.
- Example configurations:
    - **Normal Open**: Set **00:00-23:59** for Interval 1 and **00:00-00:00** for Intervals 2 and
    - **Normal Close**: Set **00:00-00:00** for all intervals.
- If only one interval is required, configure Interval 1; Intervals 2 and 3 will default to **00:00-00:00**.
- For two intervals, configure Interval 1 and 2; Interval 3 will default to **00:00-00:00**.
- Ensure intervals do not overlap or cross days; otherwise, the system will prompt an error.

Holiday Type:

- Specify up to three Holiday Types. These intervals are used for access on designated holidays.
- If no Holiday Type is entered, the system defaults to regular intervals.

Optional Configuration:

- Use the **Copy on Monday** option to replicate Monday's settings across other weekdays for quicker setup.

Save the Time Zone:

- After completing the configuration, click **[OK]** to save the Time Zone.
- The new Time Zone will appear in the list of configured Time Zones.

Note:

The system includes a default Time Zone named **[24 hours Accessible]**, which cannot be modified or deleted.

Time Zones can only be used if correctly configured without overlapping intervals.

Time Zones can be applied to various features, such as access levels, reader usability, and Normal Open/Close periods.

Edit Time Zone

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

The door opening time for a device needs to be updated or corrected.

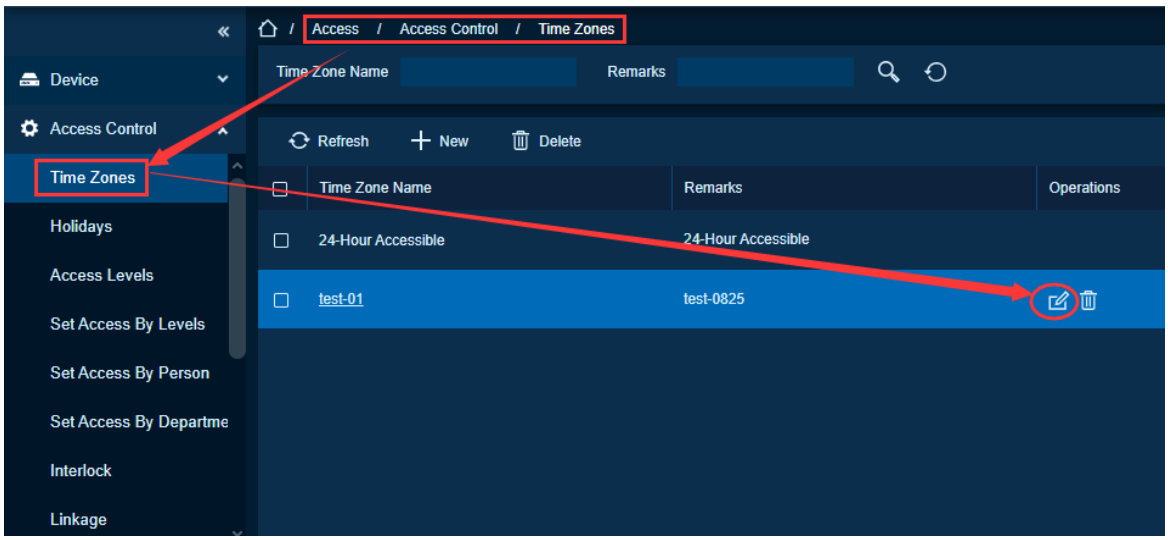
Trigger Result

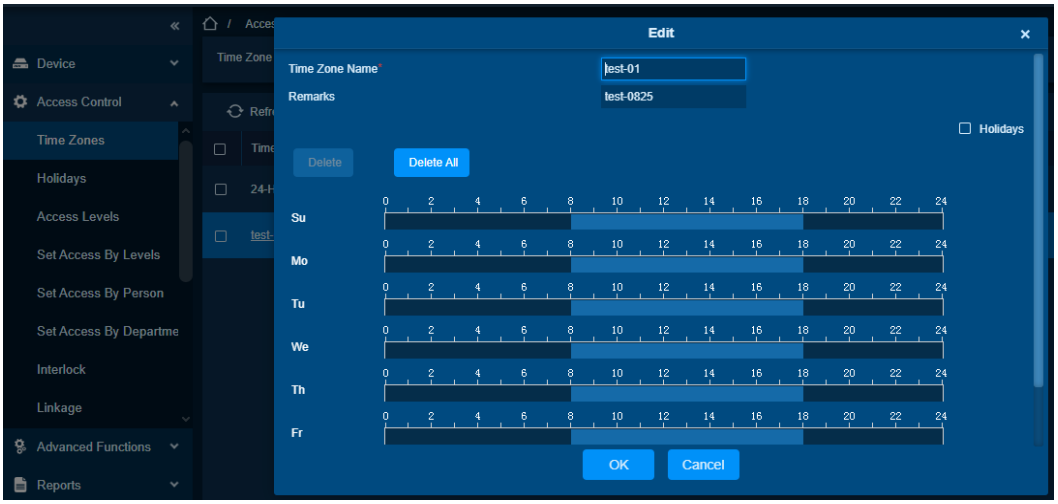
The configured time intervals for the device are updated according to the new requirements.

Steps:

- Navigate to **[Access Control] > [Time Zones]** to view the list of configured Time Zones.
- Click the **[Edit]** button.
- After making the necessary updates, click **[OK]** to save the changes.

Copyright © 2024 ARMATURA LLC. All rights reserved





Delete Time Zone

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

The door access time is no longer required for access control, or an incorrect time configuration needs to be removed.

Trigger Result

The specified Time Zone is permanently removed from the system and can no longer be applied to any doors or access control features.

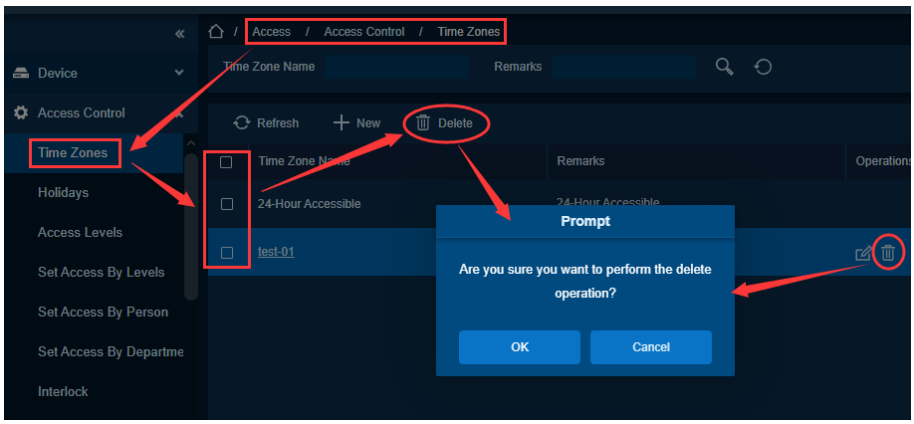
Steps:

- Click the **[Delete]** button under the **Related Operation** column.
- Click **[OK]** to confirm and delete the Time Zone.
- Click **[Cancel]** to abort the operation.

Copyright © 2024 ARMATURA LLC. All rights reserved

Delete Multiple Time Zones:

- Select the checkboxes next to the Time Zones you wish to delete.
- Click the **[Delete]** button above the list of Time Zones.
- Click **[OK]** to confirm deletion, or **[Cancel]** to cancel the operation.



6.3.2. Holiday Management

Function Description

Holidays may require different access control times compared to regular weekdays. The system enables users to manage access control settings for holidays, including **adding**, **modifying**, and **deleting** holiday configurations.

Add Holiday

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Holidays require specific access control times different from normal weekdays.

Trigger Result

Doors and other access control features will operate based on the specified holiday settings.

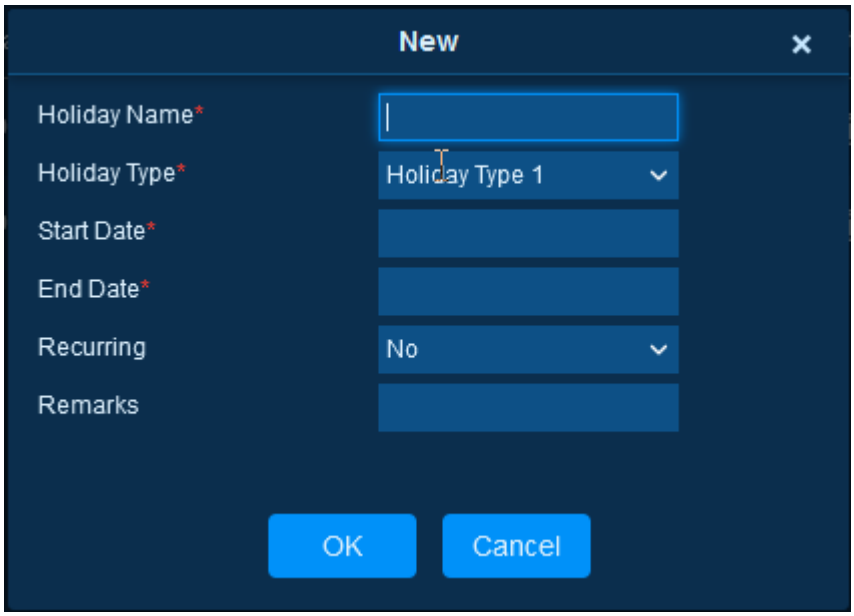
Steps:

- Navigate to **[Access Control] > [Holidays] > [New]** to open the holiday configuration interface.
- Fill in Holiday Details**:**
  Holiday Name: Enter a descriptive name for the holiday (up to 30 characters).
  Holiday Type: Select one of the three holiday types (Holiday Type 1/2/3). Each type can include up to 32 holidays.
  Start/End Date:
  - Specify the holiday duration using the date format **YYYY-MM-DD**.
  - The **Start Date** must not be later than the **End Date**; otherwise, an error will be displayed.
  - The year of the **Start Date** cannot be earlier than the current year.

Copyright © 2024 ARMATURA LLC. All rights reserved

- Holidays cannot span across different years.

- Specify whether the holiday recurs annually.
  Yes: Use this setting for holidays with fixed dates, such as **New Year's Day (January 1)**.
  No: Use this setting for holidays with varying dates, such as **Mother's Day (second Sunday of May)**.
- Save the Holiday Configuration:
  After entering all the details, click **[OK]** to save.
  The new holiday will now appear on the holiday list.



Fields Overview

Field	Description
Holiday Name	Custom name for the holiday, up to 30 characters.
Holiday Type	Select from Holiday Type 1, 2, or 3. Each type can have up to 32 holidays.
Start/End Date	Specify the holiday duration. Ensure the Start Date is earlier than or equal to the End Date.
Recurring	Choose **Yes** for fixed-date holidays (e.g., New Year's Day) and **No** for variable-date holidays (e.g., Mother's Day).

Fields are as follows:

Holiday Name: Any character, up to a combination of 30 characters.

Holiday Type: Holiday Type 1/2/3, namely, a current holiday record belongs to the three holiday types and each holiday type includes up to 32 holidays.

Start/End Date: The date format: 2010-1-1. Start Date cannot be later than End Date, otherwise the system will prompt an error message. The year of Start Date cannot be earlier than the current year, and the holiday cannot be set across two different years.

Copyright © 2024 ARMATURA LLC. All rights reserved

Recurring: It refers a holiday whether to require modification in different years. The default is No. For example, the Near Year's Day is on January 1 each year and can be set as Yes. The Mother's Day is on the second Sunday of each May; this date is not fixed and should be set as No.

For example, the date of Near Year's Day is set as January 1, 2010, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of Friday, but the Access Control Time of Holiday Type 1.

After editing, click **[OK]** button to save, and it will display in the holiday list.

Edit Holiday

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

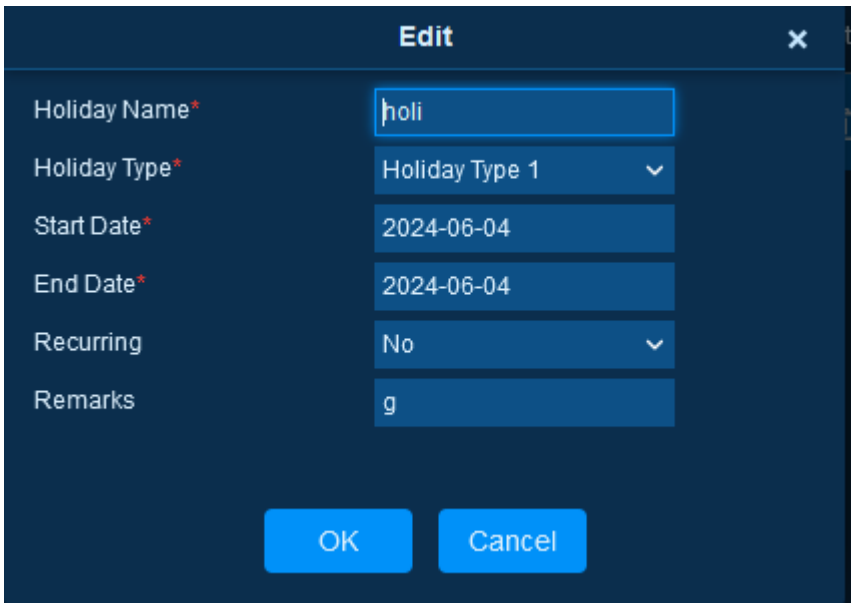
Special holiday time settings may require modification, or current holiday configurations may be incorrect and need adjustments.

Trigger Result

The holiday time will be updated with the new settings.

Steps:

- Navigate to the holiday list.
- Click on the **[Holiday Name]** or the **[Edit]** button under the Operations column to open the edit interface.
- Adjust the holiday name, type, date range, or recurring status as needed.
- After making the modifications, click **[OK]** to save and exit the edit interface.



Copyright © 2024 ARMATURA LLC. All rights reserved

Delete Holidays

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

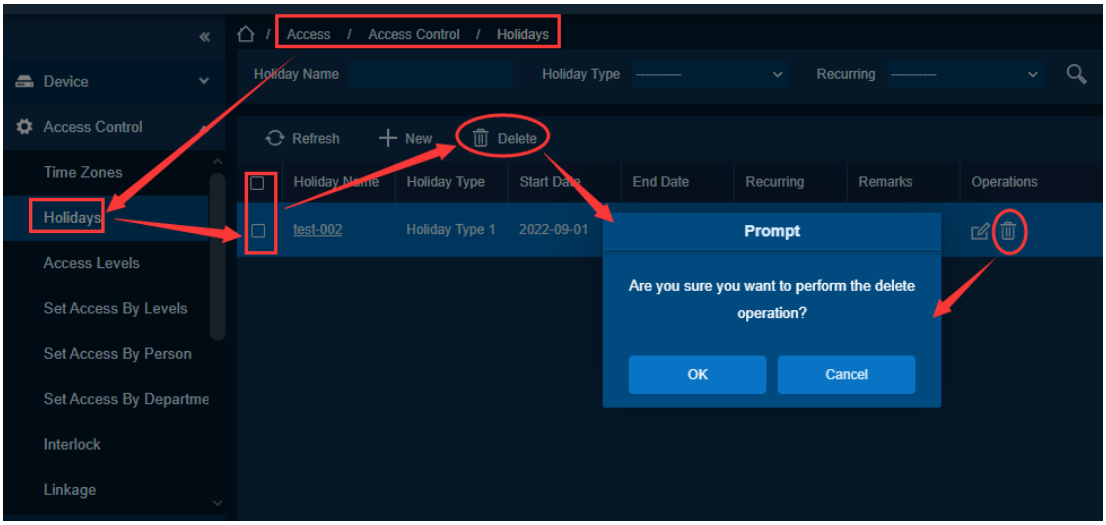
This function is used when the holiday time is no longer needed, or when the holiday configuration requires reconfiguration.

Trigger Results

Deletes the selected holiday configuration from the list.

Steps:

- Navigate to the **Access Control** holiday list.
- Click the **[Delete]** button under the **Operations** column for the desired holiday.
- Click **[OK]** to confirm the deletion.
- Click **[Cancel]** to abort the operation.



- Click **[OK]** to delete, click **[Cancel]** to cancel the operation.

Note:

Holidays currently in use for access control or linked to other configurations cannot be deleted. If a holiday is in use, it is recommended to modify its settings instead of deleting it.

6.3.3. Access Levels

Function Description

Access levels define which doors can be opened by individuals or groups of individuals during specific time zones.

Copyright © 2024 ARMATURA LLC. All rights reserved

Add Access Level

Prerequisites for Use

Log into the system using an account with the required permissions.

Ensure that access control time zones and areas have already been configured within the access control module.

Usage Scenarios

To apply unified access permissions for specific doors, incorporating time and area restrictions.

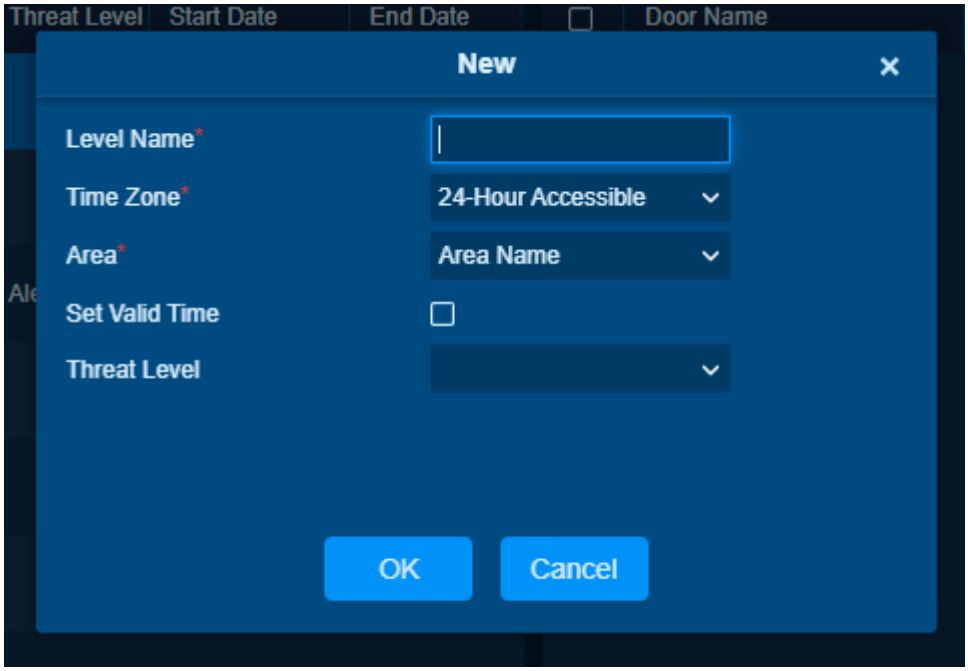
Trigger Result

Creates a new access level, specifying the associated area and time restrictions.

Steps:

Navigate to the Add Levels Interface:

- Go to **[Access Control] > [Access Levels] > [New]** to open the Add Levels editing interface.



Input Level Details:

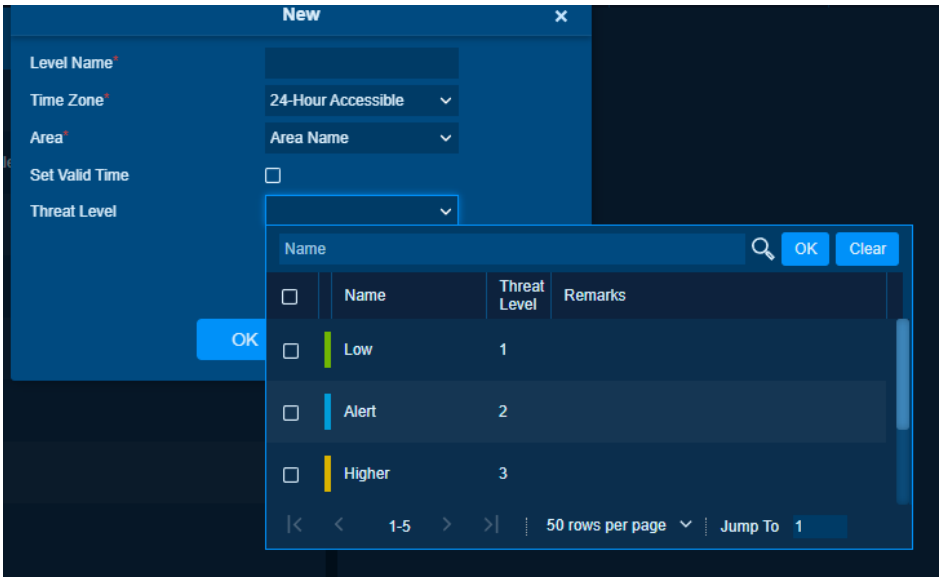
- **Level Name:** Enter a unique name for the level.
- **Time Zone:** Select the appropriate time zones for access.
- **Area:** Assign specific areas to define access privileges for users.
- **Valid Time:** Specify a validity period for this access level, during which it remains active.

Copyright © 2024 ARMATURA LLC. All rights reserved

- **Access Level Threat Level:** Assign a threat level for the access level. If the system's threat level changes, access will be evaluated based on whether the access level's threat level matches the current system threat level.

Configure Threat Level:

- If the current threat level of the access level does not match the system's threat level, access through this level will be restricted. Refer to the **Threat Level** documentation for more details.

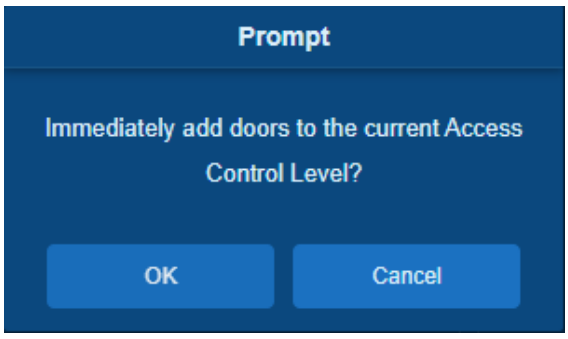


Save Access Level:

- Click **[OK]** to save the new access level.
- A system prompt will appear: **"Immediately add doors to the current Access Control Level"**
    - Click **[OK]** to proceed with adding doors.
    - Click **[Cancel]** to return to the access levels list without assigning doors.

Assign Doors to Access Level:

Select and add doors from various panels to the access level as required. This step is optional and can be completed immediately or later.



Note:

Each access level must have a unique name.

Copyright © 2024 ARMATURA LLC. All rights reserved

Doors from multiple access control panels can be added to a single access level.

The validity period defines the operational timeframe for the access level. Ensure the time period is accurately configured to meet requirements.

Edit Access Level

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

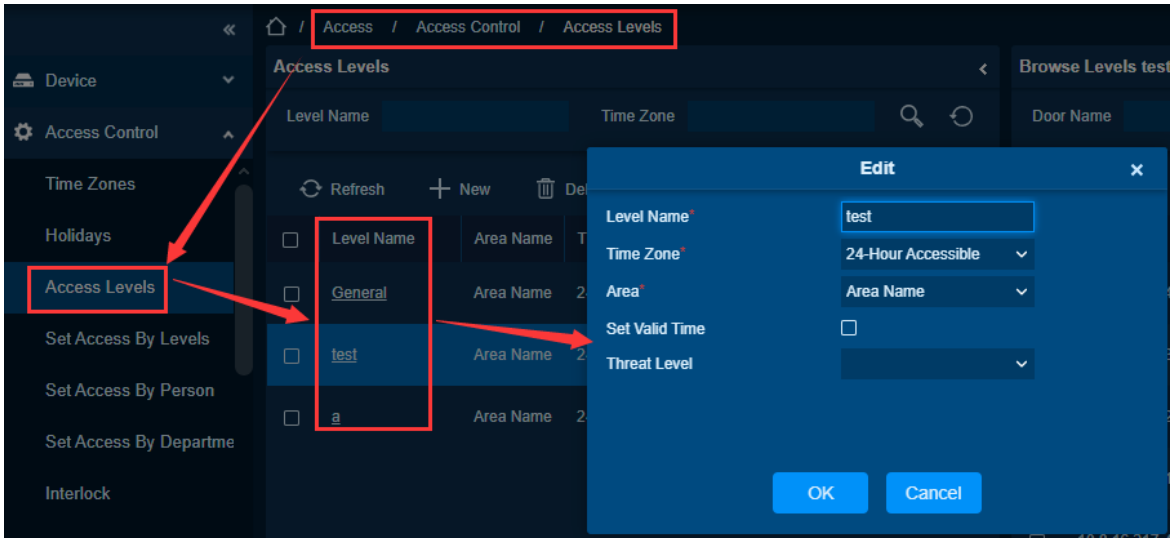
This function is used to adjust access permissions for specific doors, including modifying the access group name, time zones, or assigned areas.

Trigger Result

Updates the access levels associated with the specified area and time zones.

Steps:

- Go to **[Access] > [Access Control] > [Access Levels]** to open the access authority group interface.
- Locate the desired access level from the list.
- Click **[Edit]** next to the selected access level to open the editing interface.
- Adjust the access group name, access control time zones, or area settings as required.
- Click **[OK]** to save the modifications.



Delete Access Level

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

When an access level is no longer needed for managing door permissions.

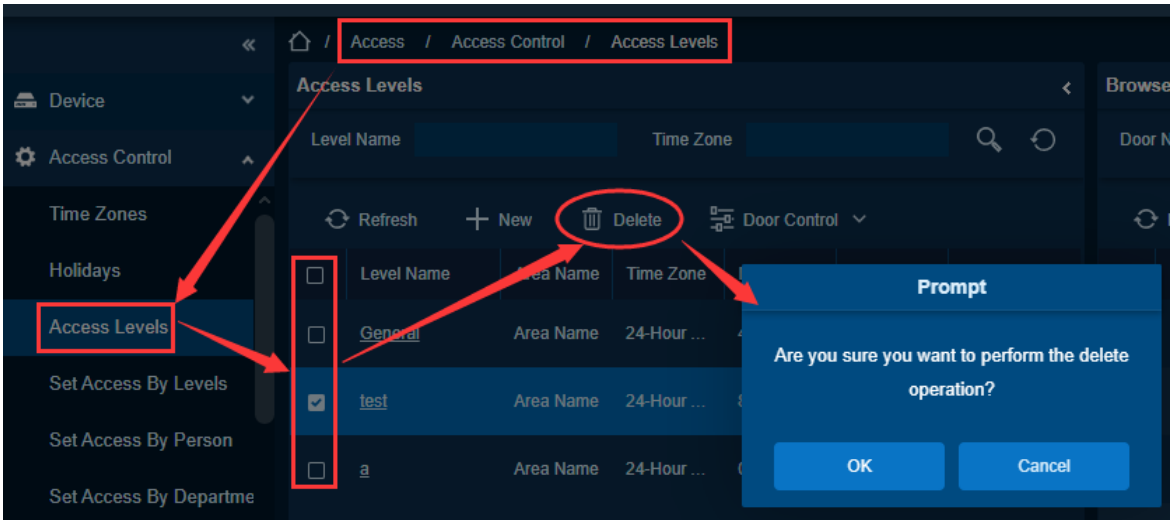
Trigger Result

Copyright © 2024 ARMATURA LLC. All rights reserved

Removes the selected access level from the system.

Steps:

- Go to **[Access]** > **[Access Control]** > **[Access Levels]** to open the access levels interface.
- Locate the access level to be deleted.
- Click **[Delete]** next to the corresponding access level.
- A confirmation prompt will appear. Click **[OK]** to delete the access level or **[Cancel]** to abort the action.



Add Door to Access Level

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

To assign access levels to specific doors for controlled access.

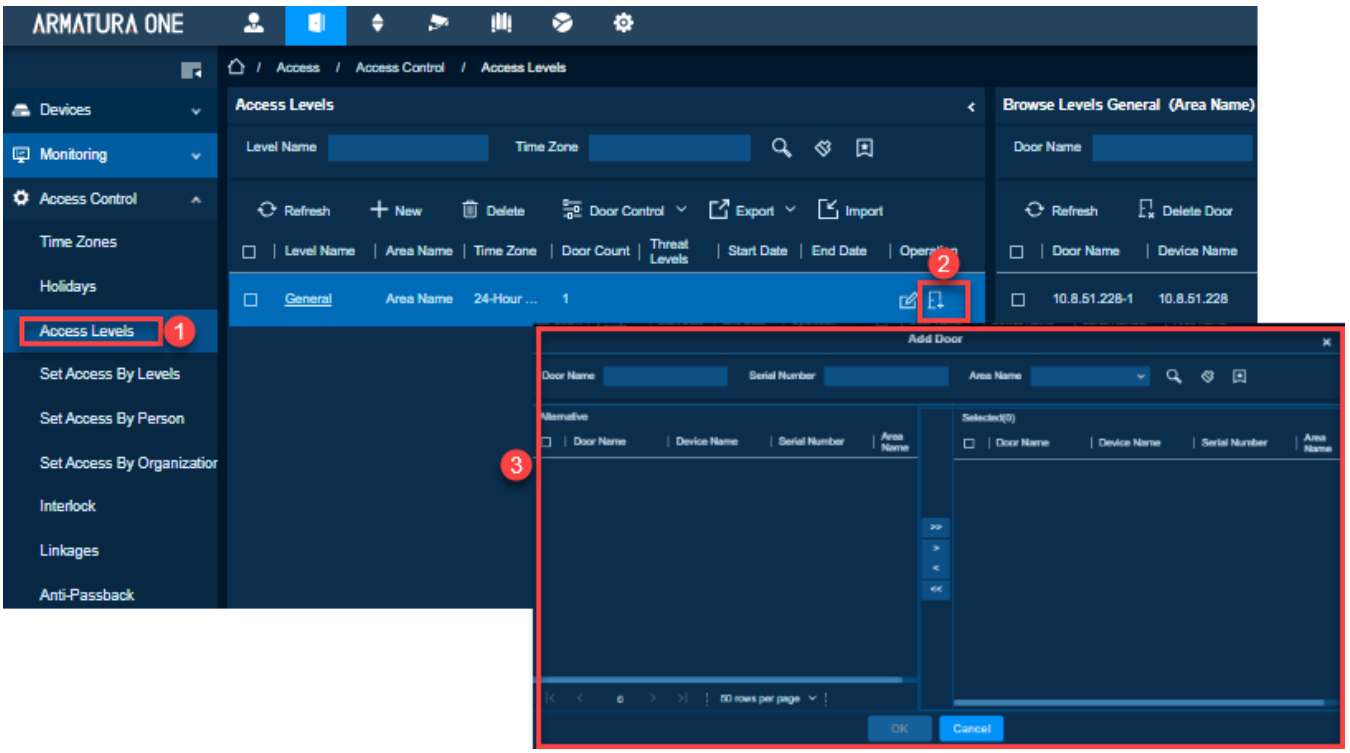
Trigger Results

The access level settings are applied to the selected door, enabling access according to the defined permissions.

Steps:

- Go to **[Access] > [Access Control] > [Access Levels]** to display the access levels interface.
- Identify and select the desired access level from the list.
- Click **[Add Door]** to open the interface for adding doors.
- Choose the doors to be included in the access level and confirm the selection.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Door from Access Level

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

To remove access levels for certain doors when they no longer require controlled access.

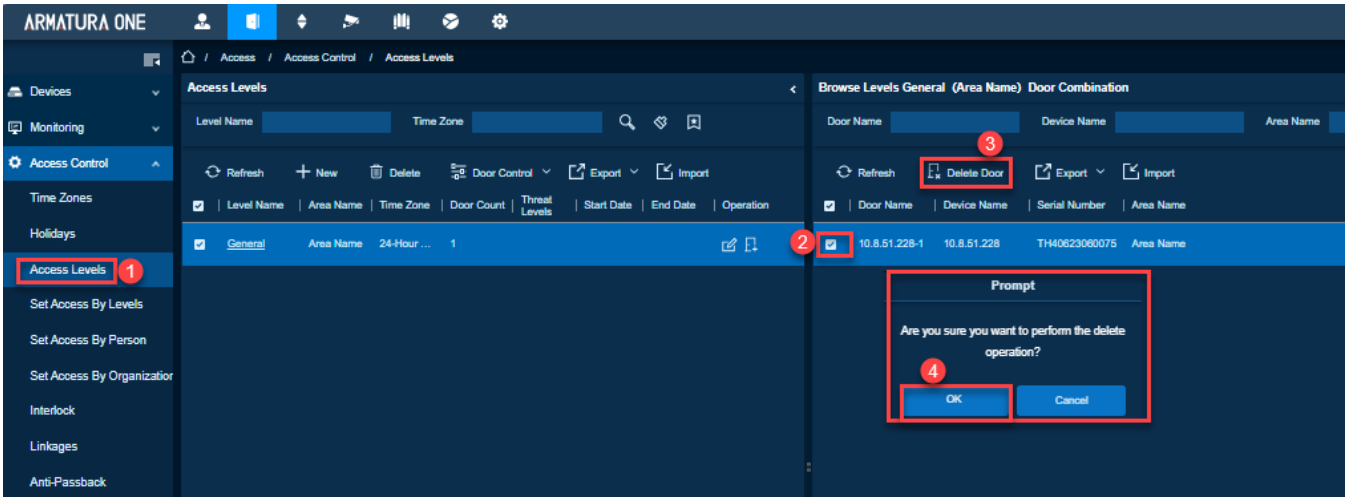
Trigger Result

The selected door is removed from the specified access level, and the associated permissions are revoked.

Steps:

- Go to **[Access]** > **[Access Control]** > **[Access Levels]** to display the access levels interface.
- Identify and select the desired access level from the list.
- Click **[Delete Door]** and select the door to be removed.
- Confirm the operation to remove the door from the access level.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export Access Level's Door List

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

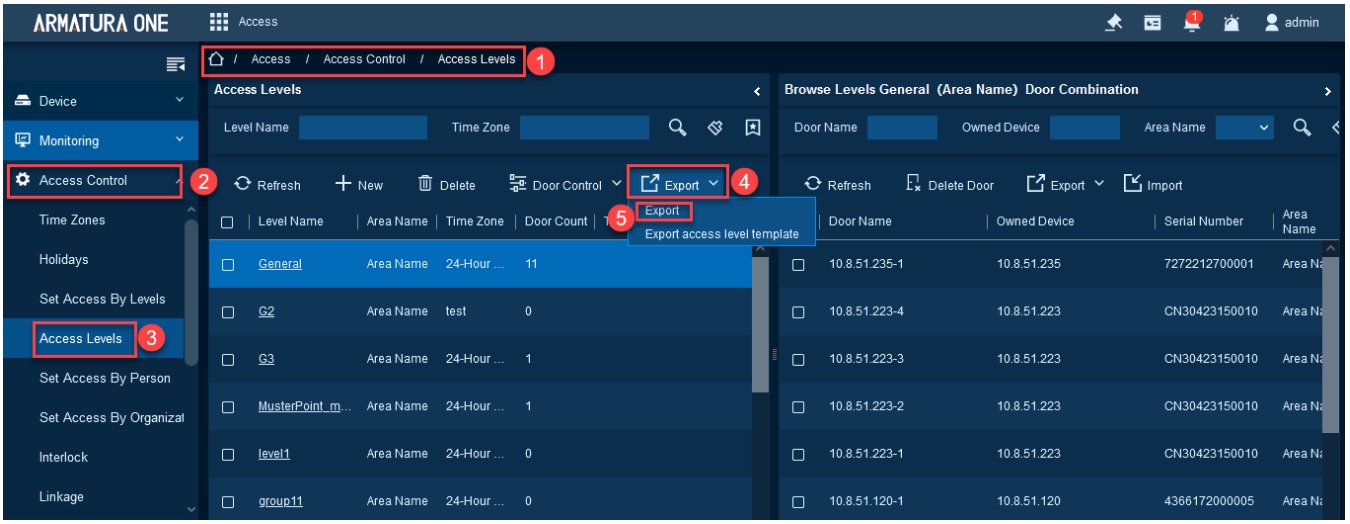
To export a list of doors included in an access level for reference or analysis.

Trigger Result

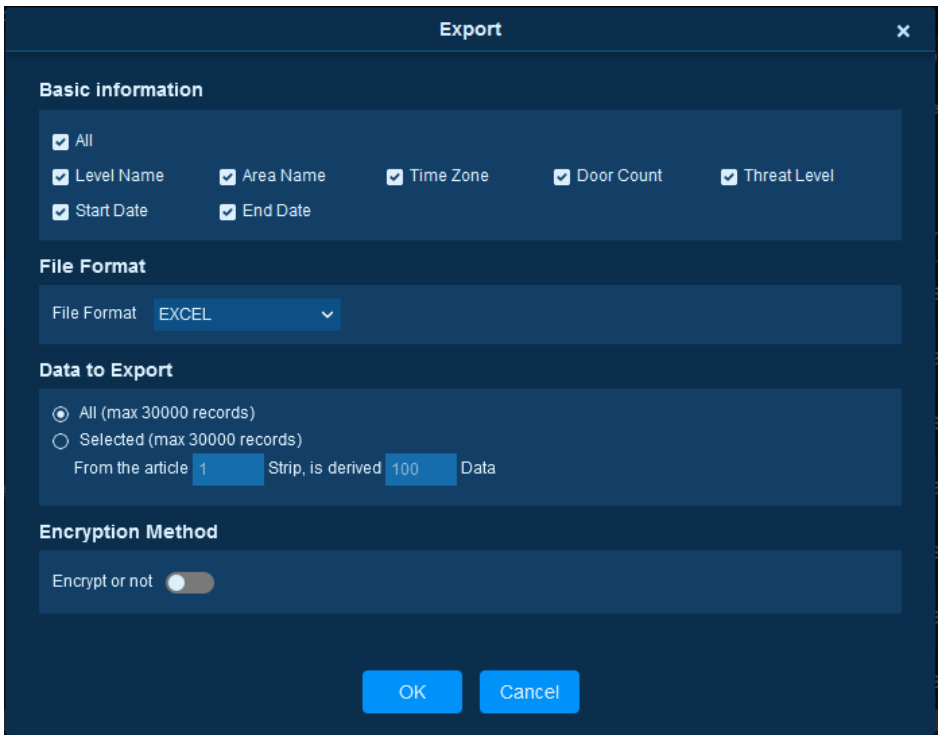
The list of doors and their devices is exported in the chosen format.

Steps:

- Go to **[Access] > [Access Control] > [Access Levels]** to display the access levels interface.
- Identify and select the desired access level from the list.
- In the right-hand column, click **[Export]** and select the desired file format (e.g., Excel, PDF, or CSV).
- Confirm the export method and click **[OK]** to download the file.



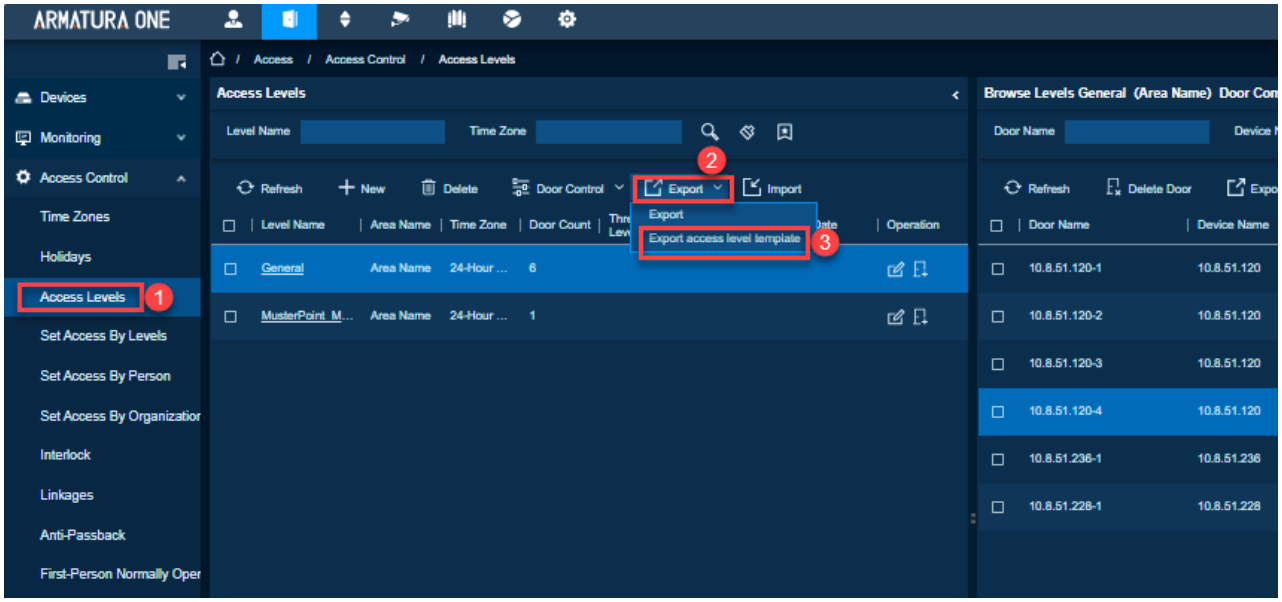
Copyright © 2024 ARMATURA LLC. All rights reserved



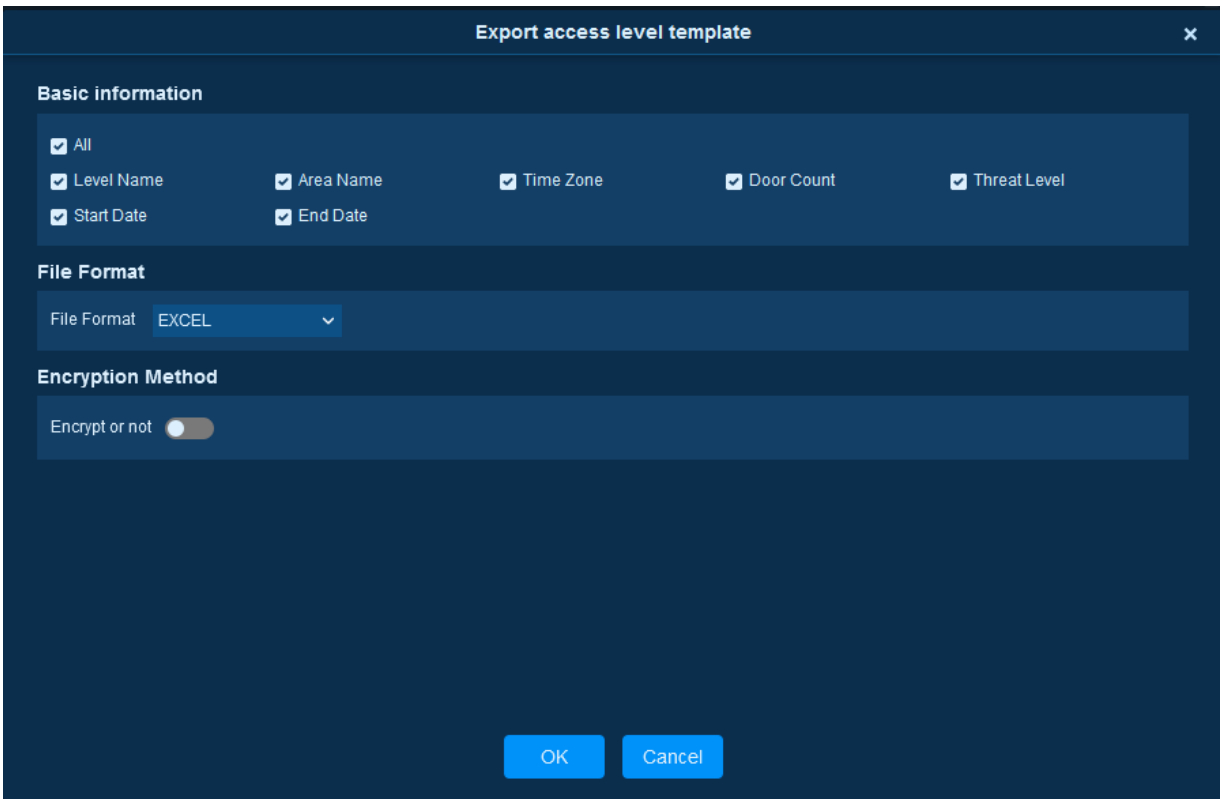
Export An Access Level Template

Steps:

- Go to **[Access]** > **[Access Control]** > **[Access Levels]** to display the access levels interface.
- Identify and select the desired access level from the list.
- In the right-hand column, click **[Export]**, then select **[Export Access Level Template]** as the file format.
- Choose the export method and click **[OK]** to download the template.



Copyright © 2024 ARMATURA LLC. All rights reserved



Door Control - Remote Open Door

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Perform a batch remote opening of doors under a specified access level.

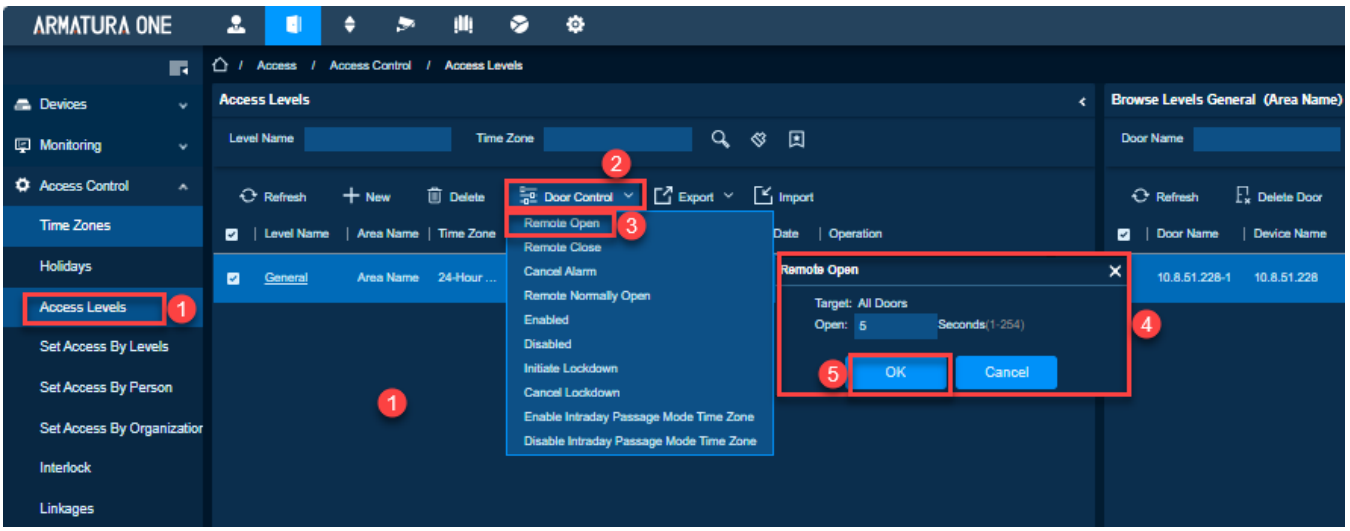
Trigger Result

All doors associated with the selected access level are opened remotely.

Steps:

- Go to **[Access]** > **[Access Control]** > **[Access Levels]** to display the access levels interface.
- Identify and select the desired access level from the list.
- Click **[Door Control]** > **[Remote Opening]**.
- Click **[OK]** to trigger remote door opening.

Copyright © 2024 ARMATURA LLC. All rights reserved



Door Control - Remote Door Closing

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Perform a batch remote closing of doors under a specified access level.

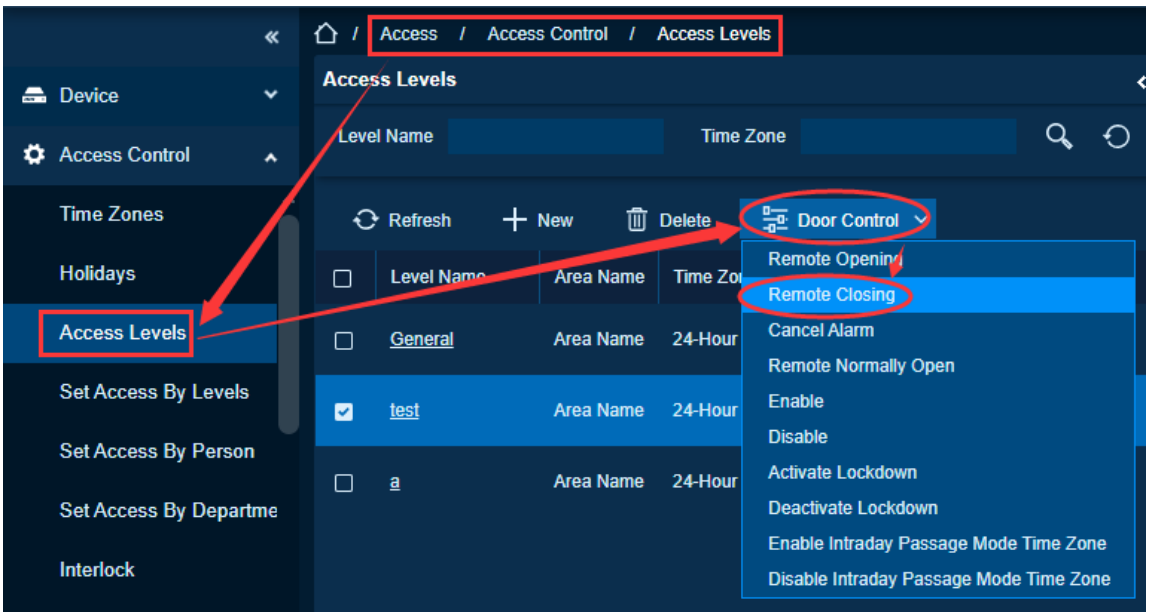
Trigger Result

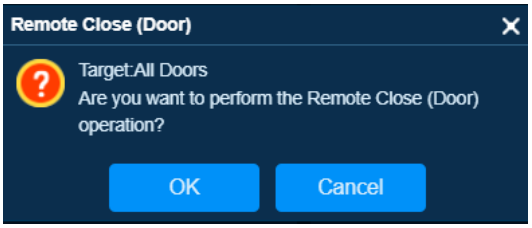
All doors associated with the selected access level are closed remotely.

Steps:

- Go to **[Access] > [Access Control] > [Access Levels]** to display the access levels interface.
- Identify and select the desired access level from the list.
- Click **[Door Control] > [Remote Closing]**.
- Enter the user login password to confirm the operation.
- The doors will close remotely once the command is triggered.

Copyright © 2024 ARMATURA LLC. All rights reserved





Door Control - Cancel Alarm

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Perform a batch cancellation of alarms for all doors under the specified access levels.

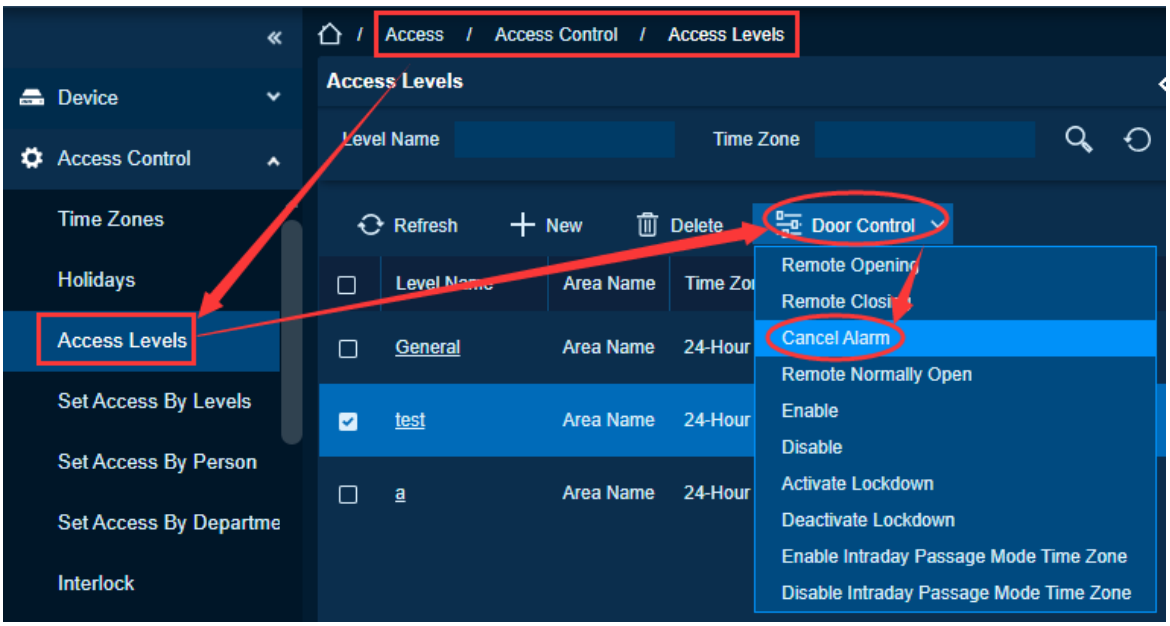
Trigger Result

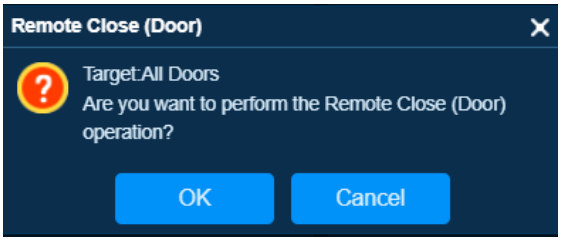
Alarms for all doors in the selected access levels are canceled.

Steps:

- Navigate to **[Access Control]** > **[Access Levels]** > **[Door Control]** > **[Cancel Alarm]**.
- Select the corresponding access levels.
- Enter the user login password to confirm.
- The alarms for all associated doors will be canceled.

Copyright © 2024 ARMATURA LLC. All rights reserved





Door Control - Remote Normally Open

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Batch set doors to a normally open state remotely.

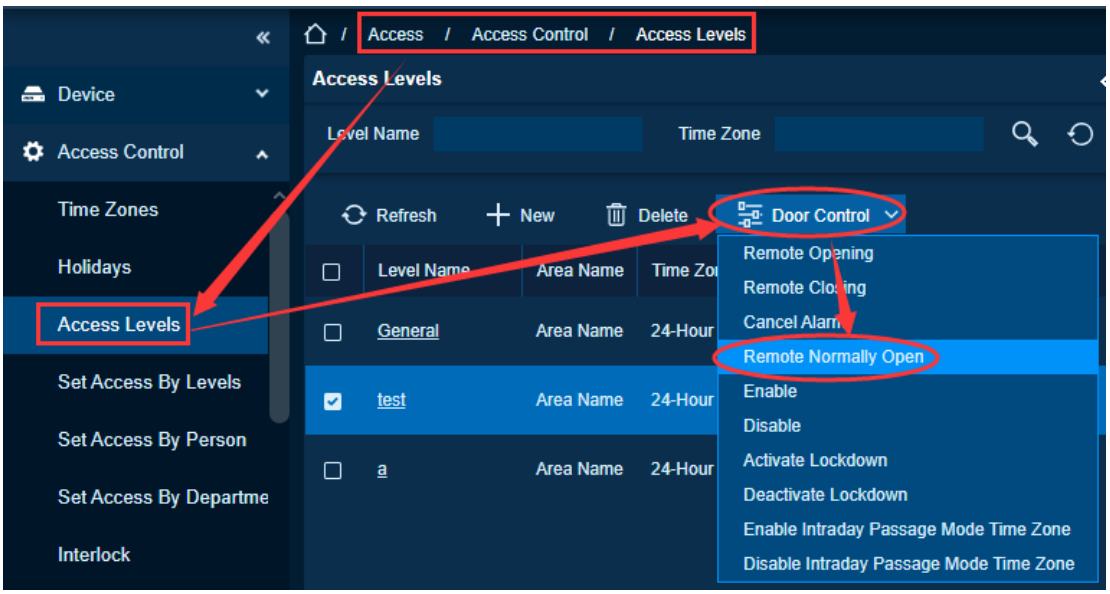
Trigger Result

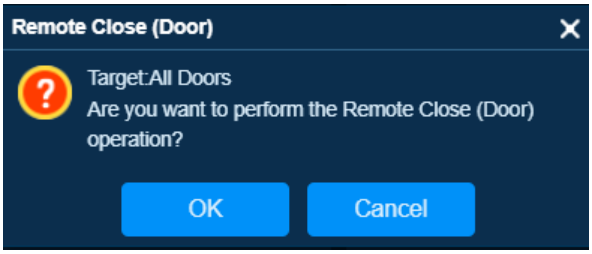
All doors in the selected access levels are set to a normally open state.

Steps:

- Navigate to **[Access Control]** > **[Access Levels]** > **[Door Control]** > **[Remote Normally Open]**.
- Select the desired access levels.
- Enter the user login password to confirm the operation.
- The doors will be set to a normally open state.

Copyright © 2024 ARMATURA LLC. All rights reserved





Door Control - Enable

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Batch enable all doors under the specified access levels.

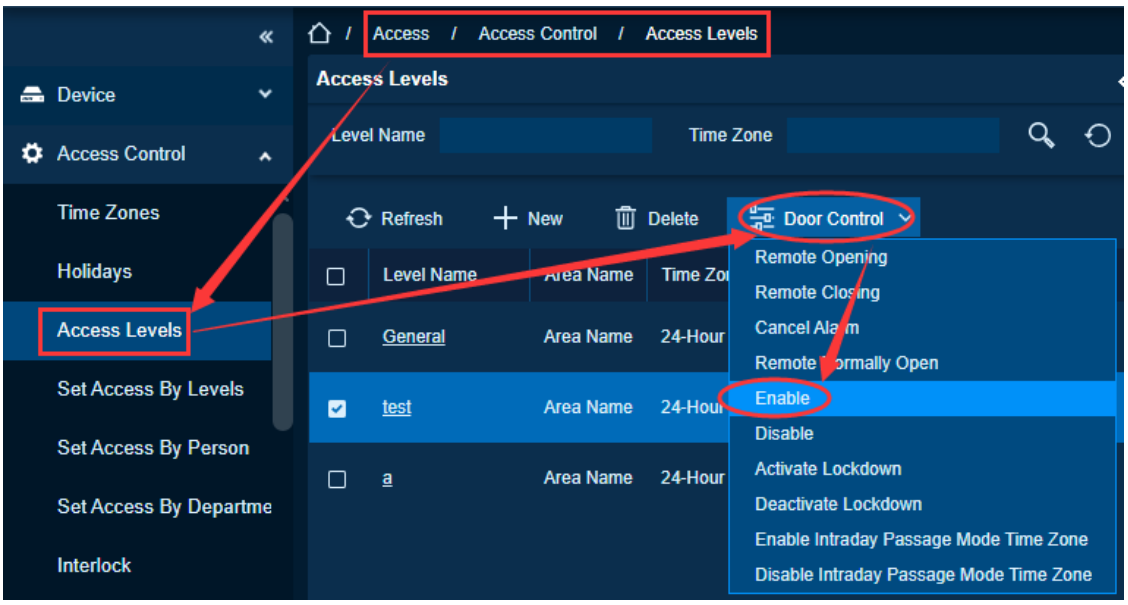
Trigger Result

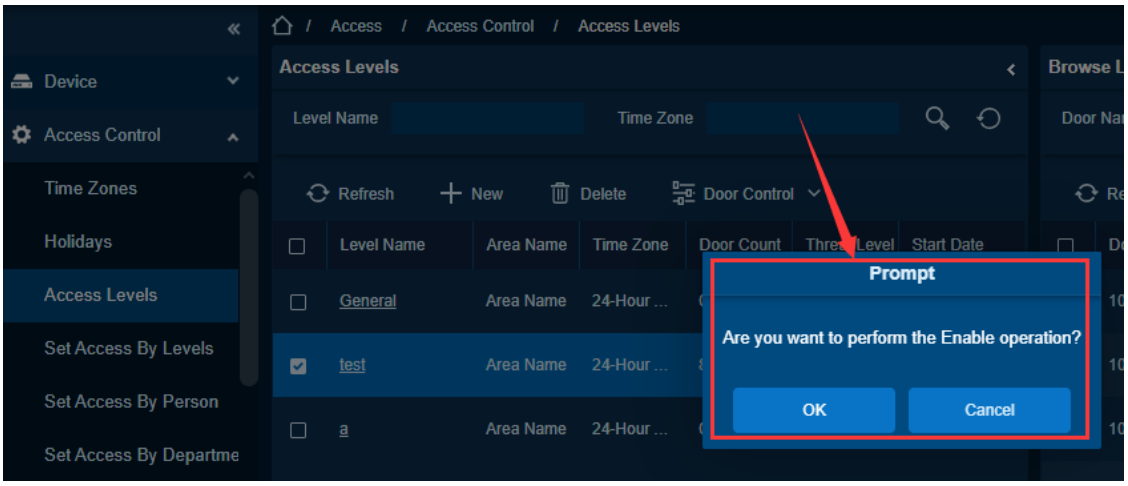
All doors in the selected access levels are enabled.

Steps:

- Navigate to **[Access Control]** > **[Access Levels]** > **[Door Control]** > **[Enable]**.
- Select the access levels to enable.
- Enter the user login password.
- The doors are enabled.

Copyright © 2024 ARMATURA LLC. All rights reserved





Door Control - Disable

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Batch disable all doors in the selected access levels.

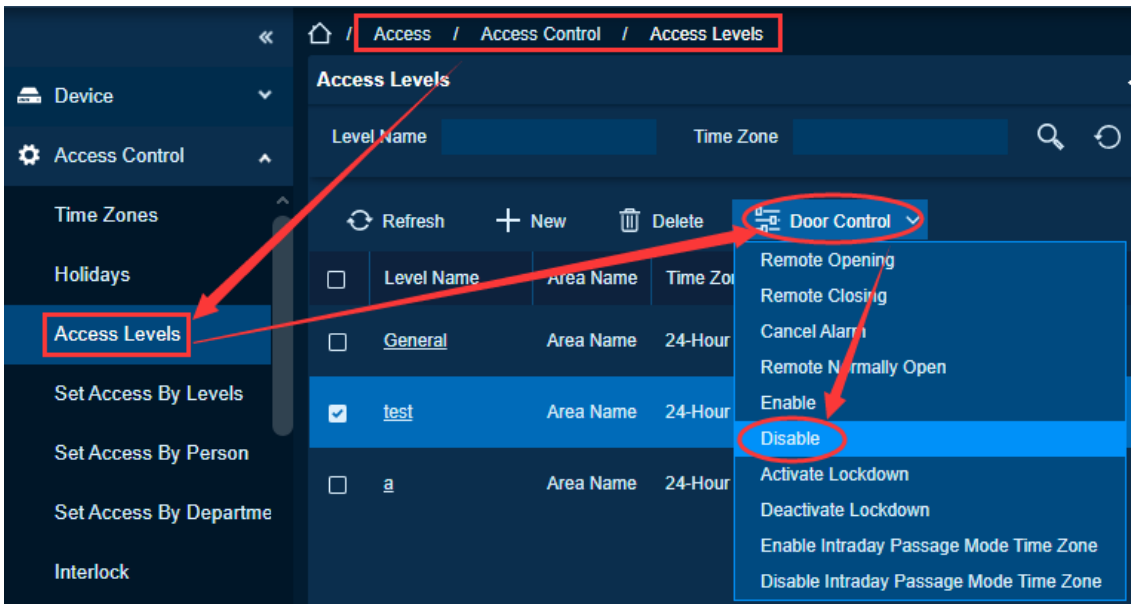
Trigger Result

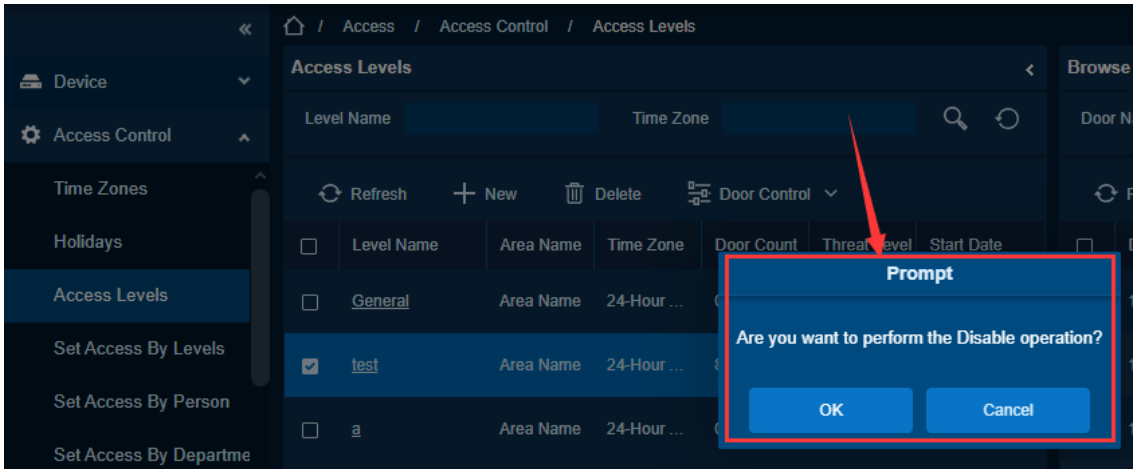
All doors in the selected access levels are disabled.

Steps:

- Navigate to **[Access Control]** > **[Access Levels]** > **[Door Control]** > **[Disable]**.
- Select the desired access levels.
- Enter the user login password.
- The doors are disabled.

Copyright © 2024 ARMATURA LLC. All rights reserved





Door Control – Initiate Lockdown

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Batch lock down all doors in the specified access levels.

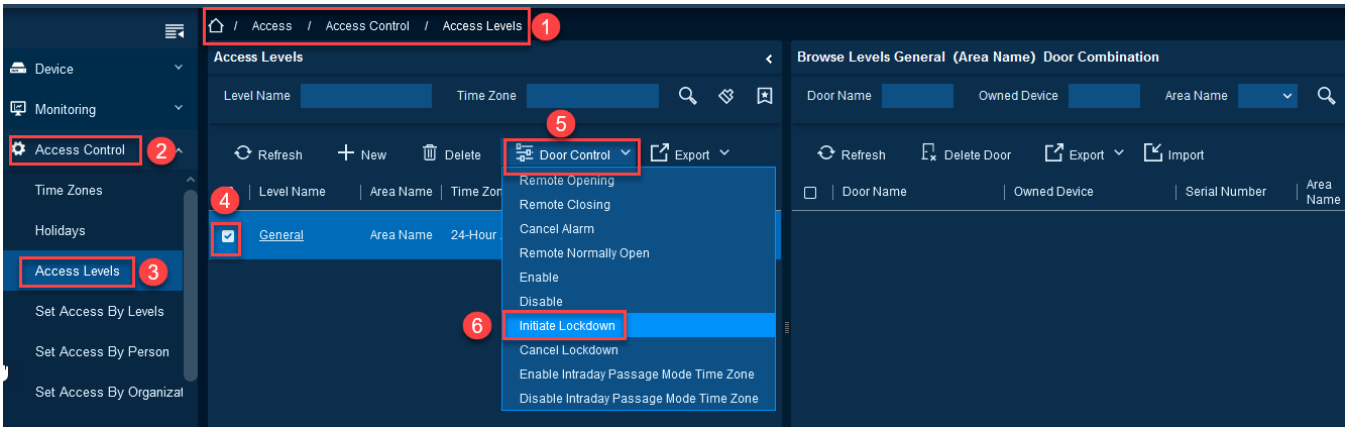
Trigger Result

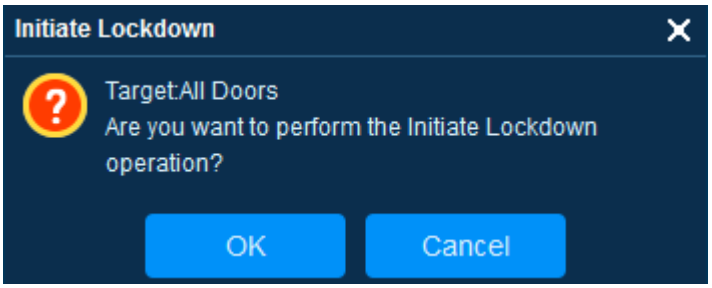
All doors in the selected access levels are set to a locked state where no operations can be performed.

Steps:

- Navigate to **[Access Control]** > **[Access Levels]** > **[Door Control]** > **[Initiate Lockdown]**.
- Select the access levels.
- Enter the user login password to confirm.
- The doors are locked down.

Copyright © 2024 ARMATURA LLC. All rights reserved





Door Control – Cancel Lockdown

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Cancel lockdown for all doors in the selected access levels.

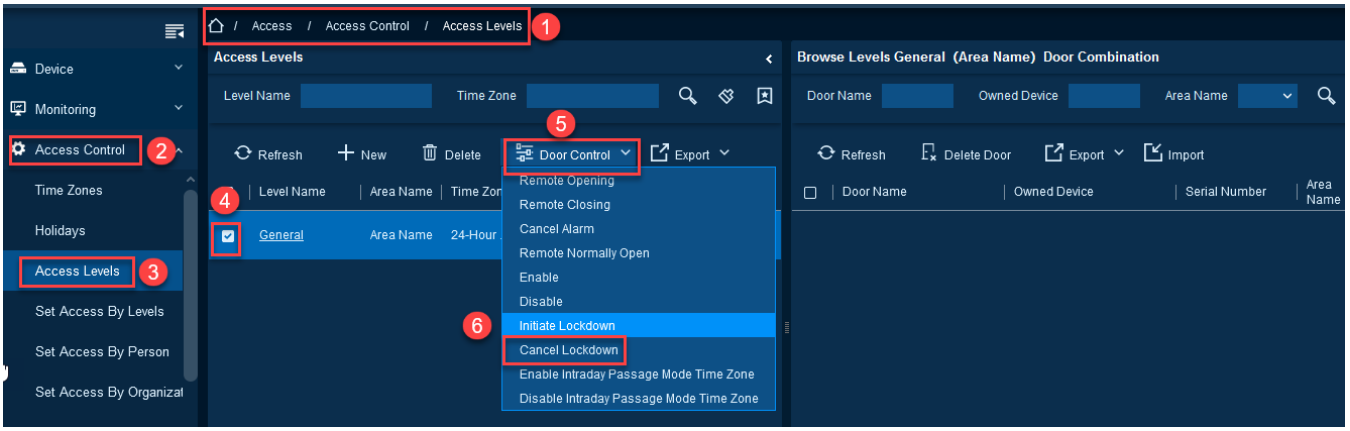
Trigger Result

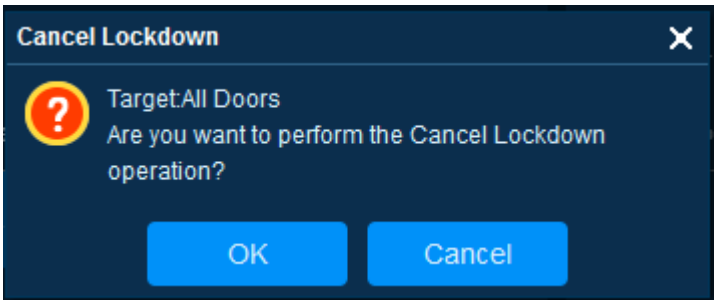
Lockdown is canceled, and doors are returned to a normal state.

Steps:

- Navigate to **[Access Control]** > **[Access Levels]** > **[Door Control]** > **[Cancel Lockdown]**.
- Select the desired access levels.
- Enter the user login password.
- Lockdown is canceled for the doors.

Copyright © 2024 ARMATURA LLC. All rights reserved





Door Control - Enable Intraday Passage Mode Time Zone

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Batch enable the normally open time zone for all doors in the specified access levels.

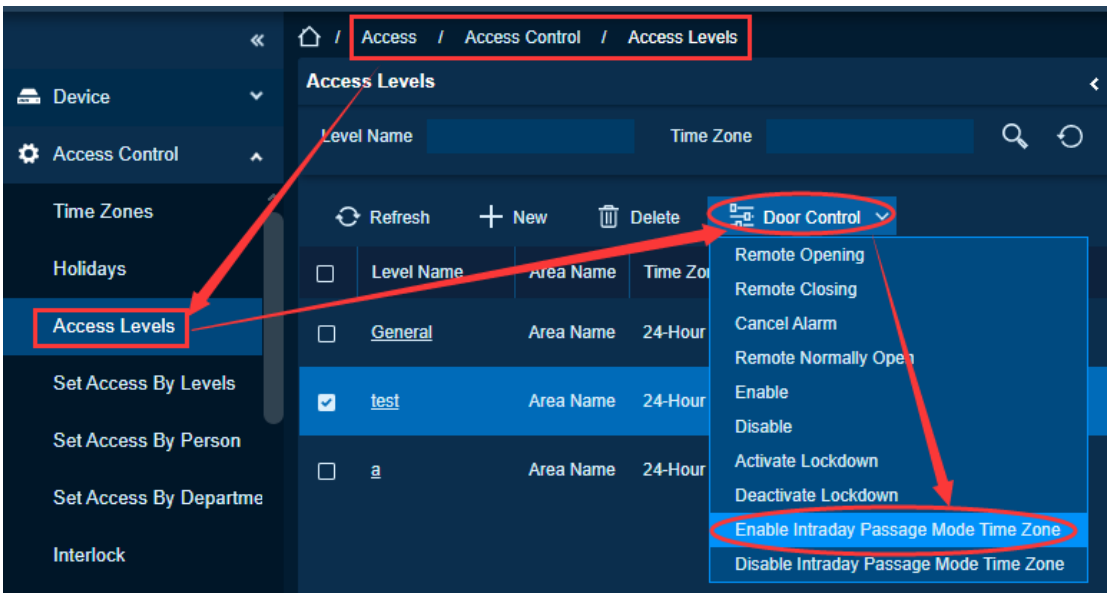
Trigger Result

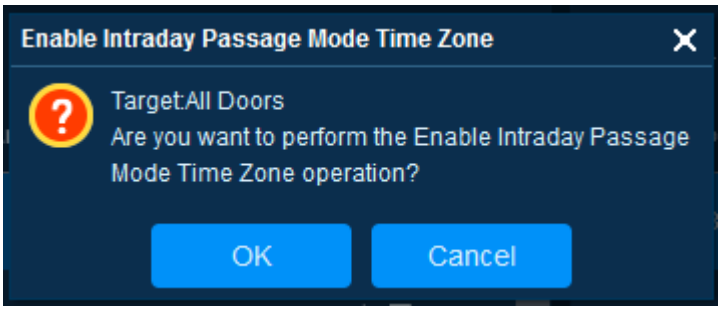
The Normally Open Time Zone is enabled for all doors in the selected access levels.

Steps:

- Navigate to **[Access Control]** > **[Access Levels]** > **[Door Control]** > **[Enable Intraday Passage Mode Time Zone]**.
- Select the access levels.
- Click **[OK]** to confirm the operation.
- The Normally Open Time Zone is enabled.

Copyright © 2024 ARMATURA LLC. All rights reserved





Door Control - Disable Intraday Passage Mode Time Zone

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Disable the normally open time zone for all doors in the specified access levels.

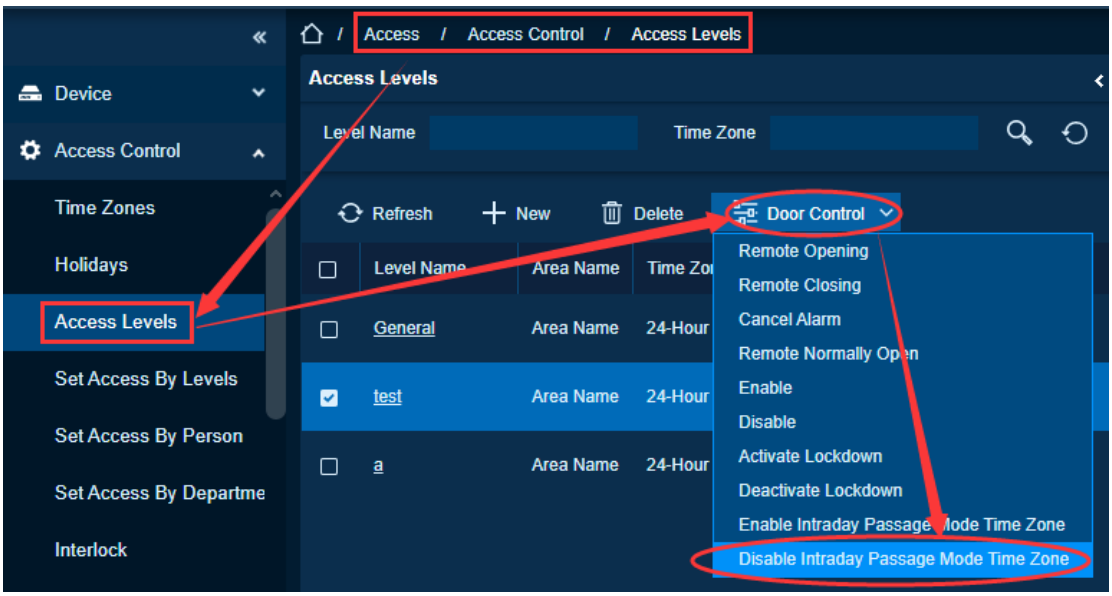
Trigger Result

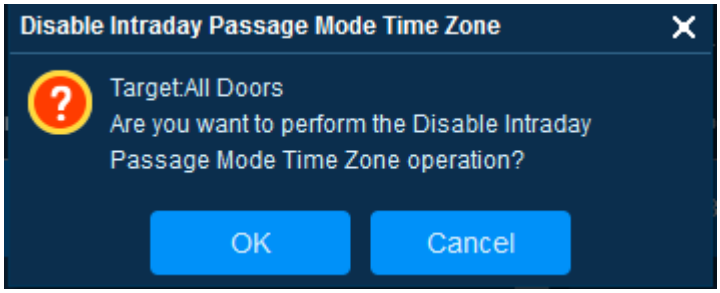
The Normally Open Time Zone is disabled for all doors in the selected access levels.

Steps:

- Navigate to **[Access Control] > [Access Levels] > [Door Control] > [Disable Intraday Passage Mode Time Zone]**.
- Select the desired access levels.
- Click **[OK]** to confirm the operation.
- The Normally Open Time Zone is disabled.

Copyright © 2024 ARMATURA LLC. All rights reserved





Door Export

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Export a list of doors for easier viewing.

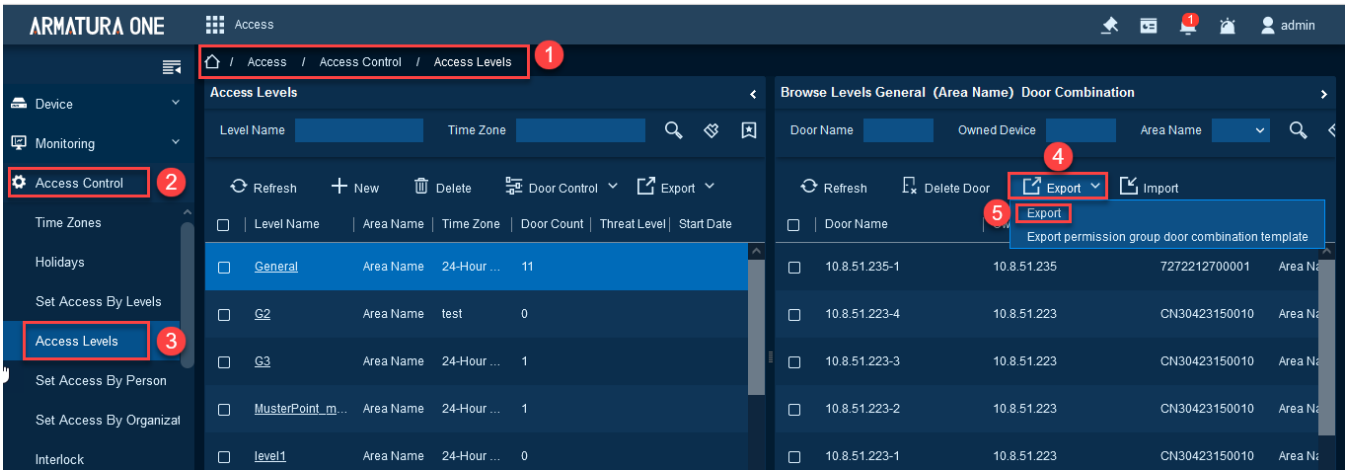
Trigger Result

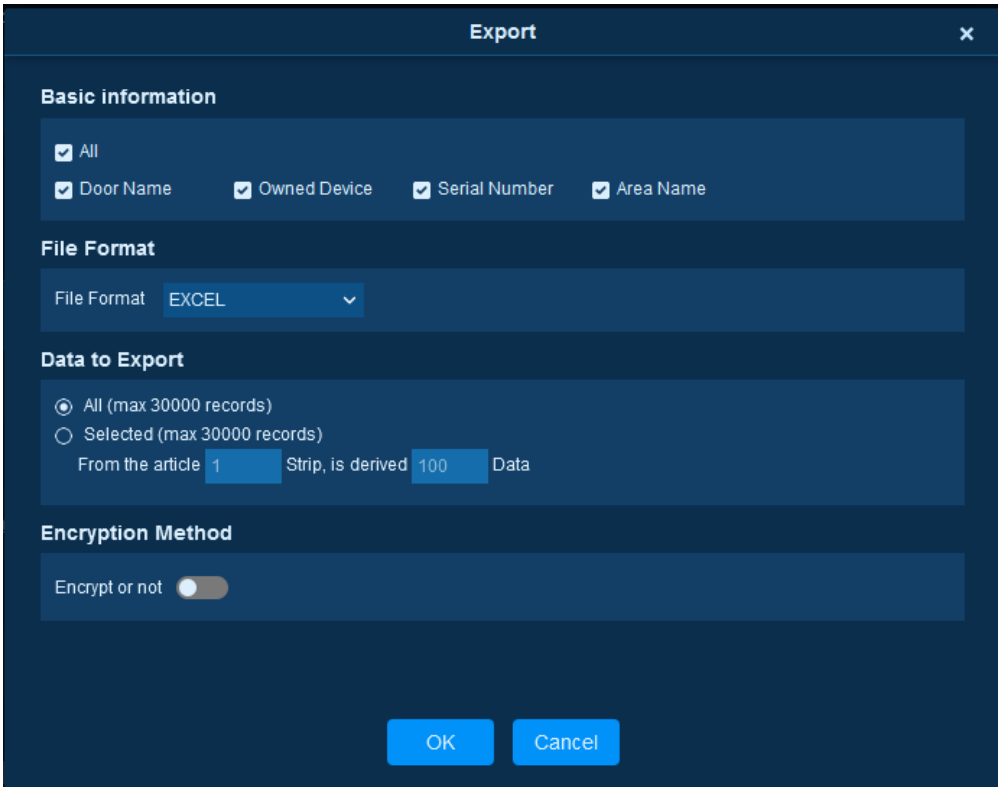
Export a file containing door names and associated devices in multiple formats.

Steps:

- Navigate to **[Access Control] > [Access Levels] > [Door Control] > [Export]**.
- Select the desired access levels.
- Choose the file format and export method.
- Click **[OK]** to export.

Copyright © 2024 ARMATURA LLC. All rights reserved





Export Permission group Door combination Template

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Export door permission combinations for a specific group.

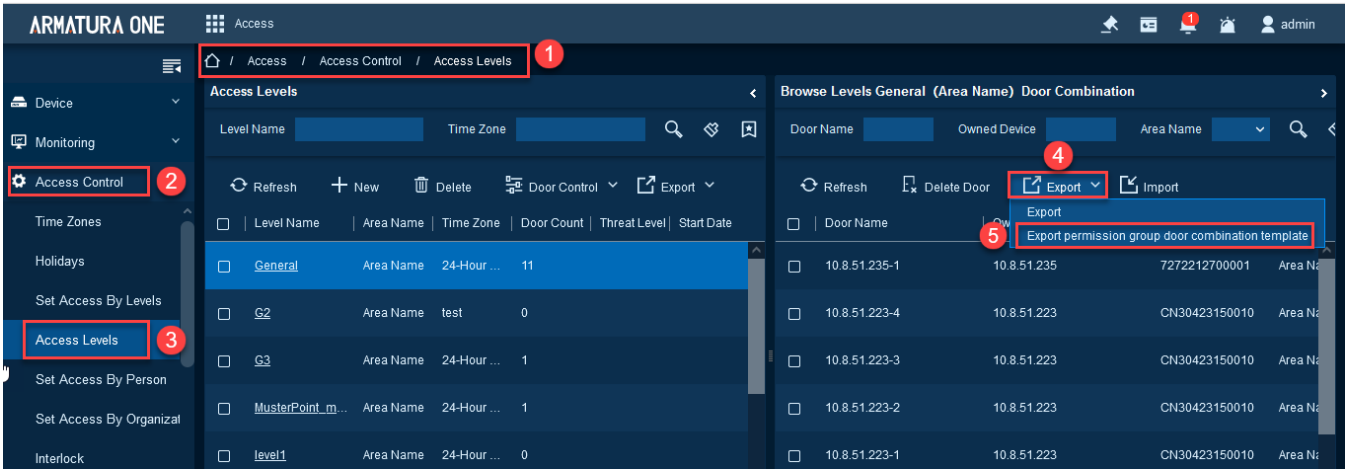
Trigger Result

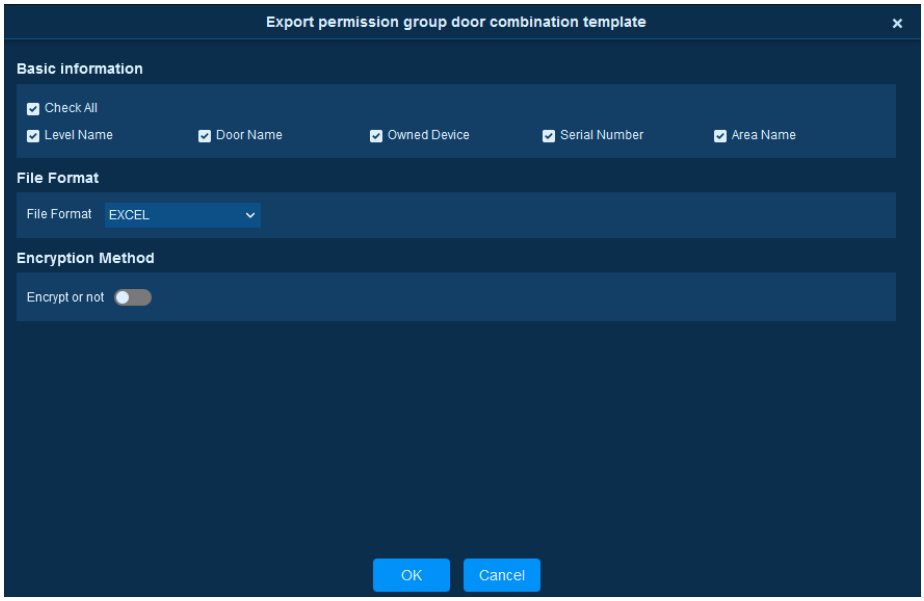
Permission group door combinations are exported in the selected file format.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access Control]** > **[Access Levels]** > **[Door Control]** > **[Export Permission Group Door Combination Template]**.
- Select the desired access levels.
- Choose the file format and export method.
- Click **[OK]** to export.





Import

Prerequisites for Use

Log in to the system with the current account and have the necessary menu authority.

Usage Scenarios

Import door-related data for a specific access level.

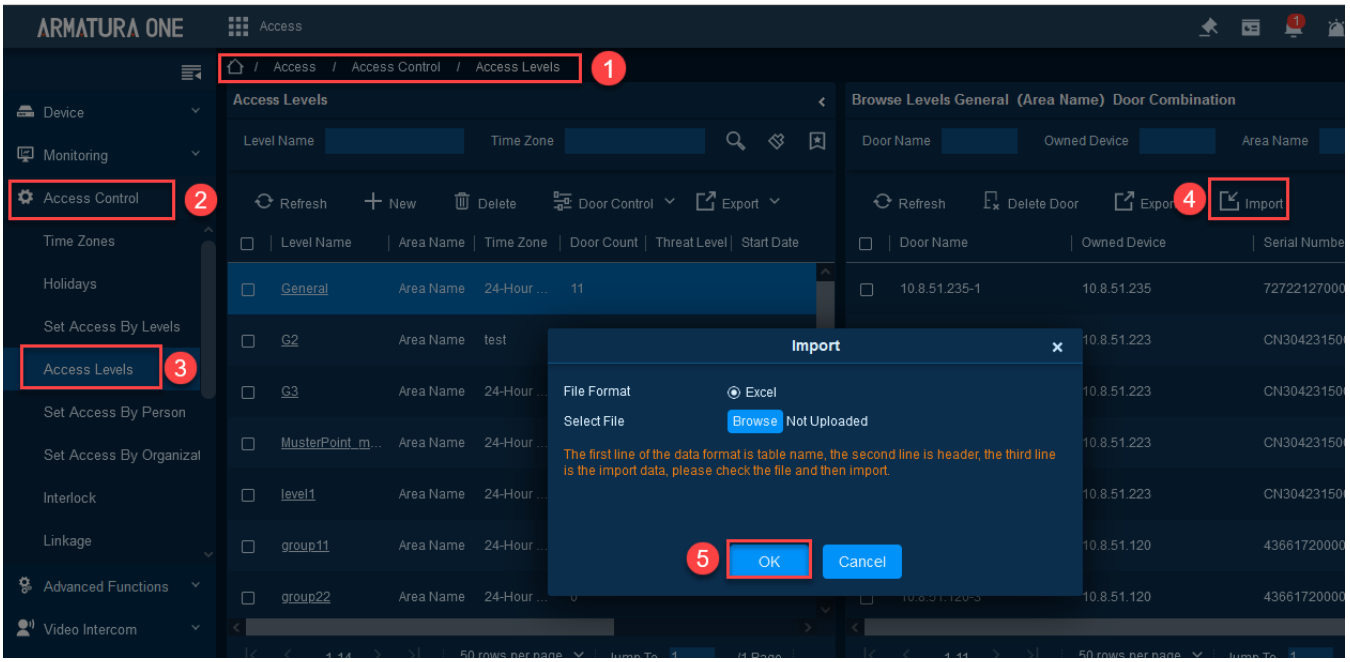
Trigger Result

Data, including door names and devices, is imported into the system.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access Control]** > **[Access Levels]** > **[Door Control]** > **[Import]**.
- Select the desired access levels.
- Choose the file format and import method.
- Click **[OK]** to import.



6.3.4. Set Access by Levels

Function Description

This feature allows users to manage personnel access permissions by adding or removing individuals within specific access levels.

Add Personnel

Prerequisites for Use

Log into the system using an account with the required permissions. Access levels must already be configured.

Usage Scenarios

Assign personnel access to specific doors within the corresponding access levels for management purposes.

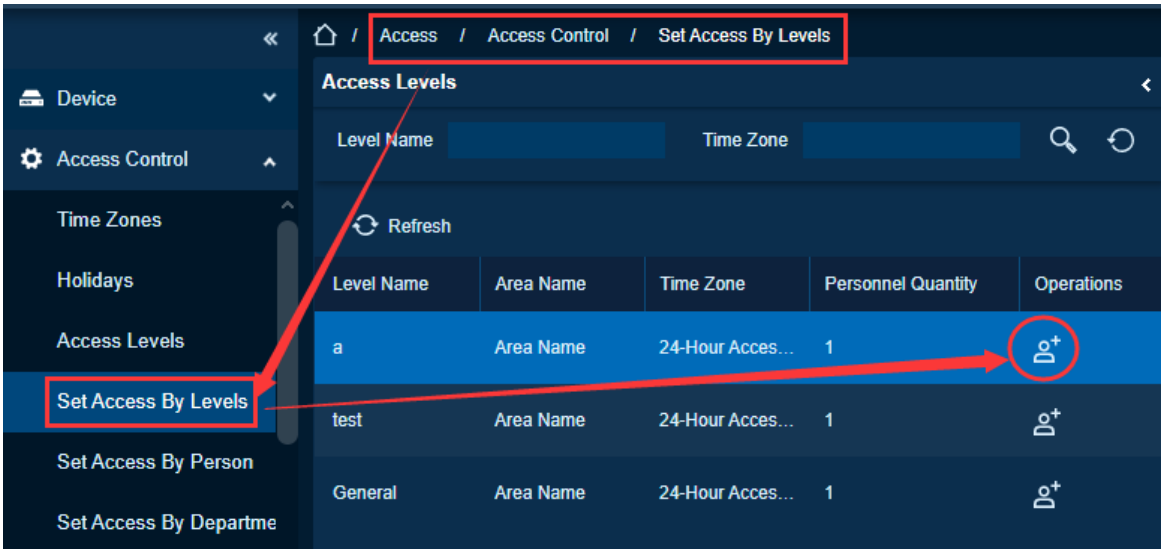
Trigger Result

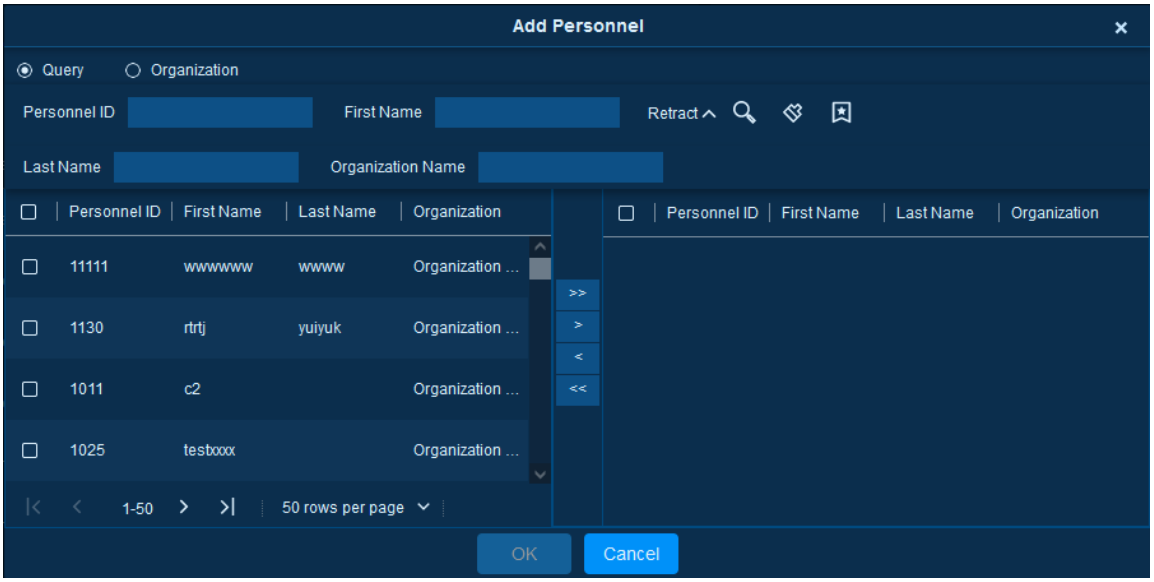
Personnel are added to the specified access levels, granting them door access based on the configured permissions.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access Control] > [Access Levels] > [Set Access by Levels]**.
- In the list on the left, select an access level. Personnel who currently have access rights within this level will be displayed in the list on the right.
- Click **[Add Personnel]** under Operations in the left panel. The **Add Personnel** dialog box will appear.
- Select the desired personnel (multiple selections allowed).
- Use the arrow button > to move the selected personnel to the list on the right.
- Click **[OK]** to save the changes and exit the interface.





Delete Personnel

Prerequisites for Use

Log in to the system with the current account and have the required menu authority.

Access levels must already be configured and contain at least one personnel entry.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

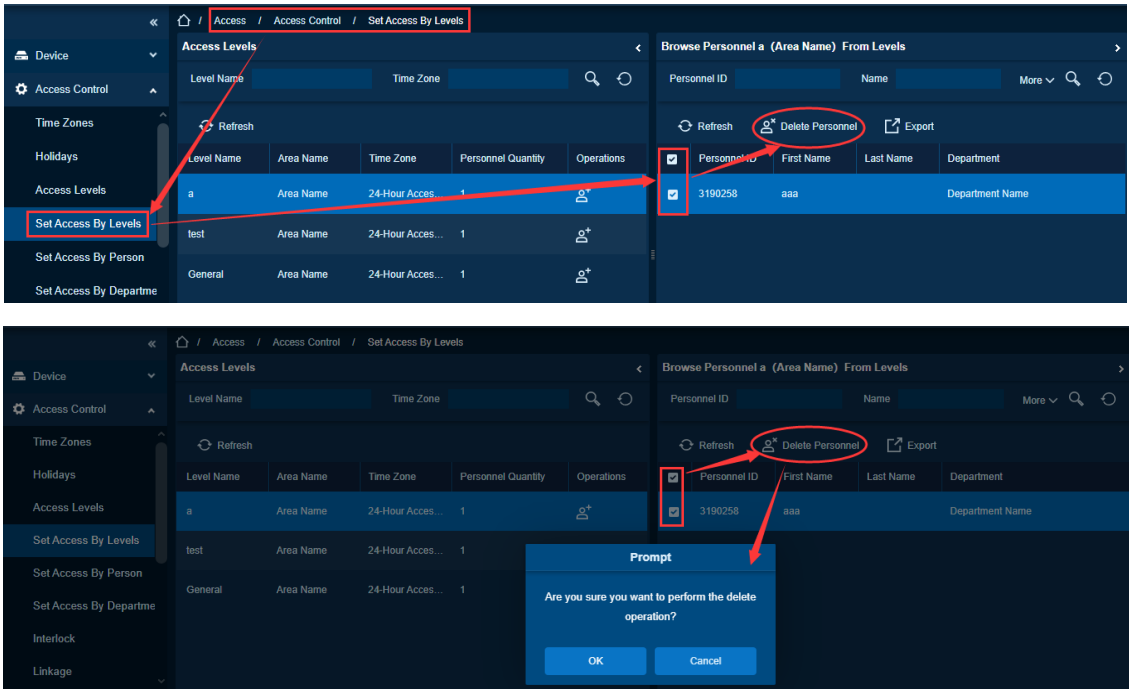
Personnel need to be removed from an access level due to changes in group assignments or because access is no longer required.

Trigger Result

Personnel are removed from the selected access levels.

Steps:

- Navigate to **[Access Control] > [Access Levels] > [Set Access by Levels]**.
- Select the access level from the list on the left. Personnel associated with the level will appear in the list on the right.
- Select the personnel to be removed from the list on the right.
- Click **[Delete Personnel]** above the list.
- Confirm the action by clicking **[OK]** to delete.



Export Set Access by Level's

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Export access level details for multiple users to facilitate external review or record-keeping.

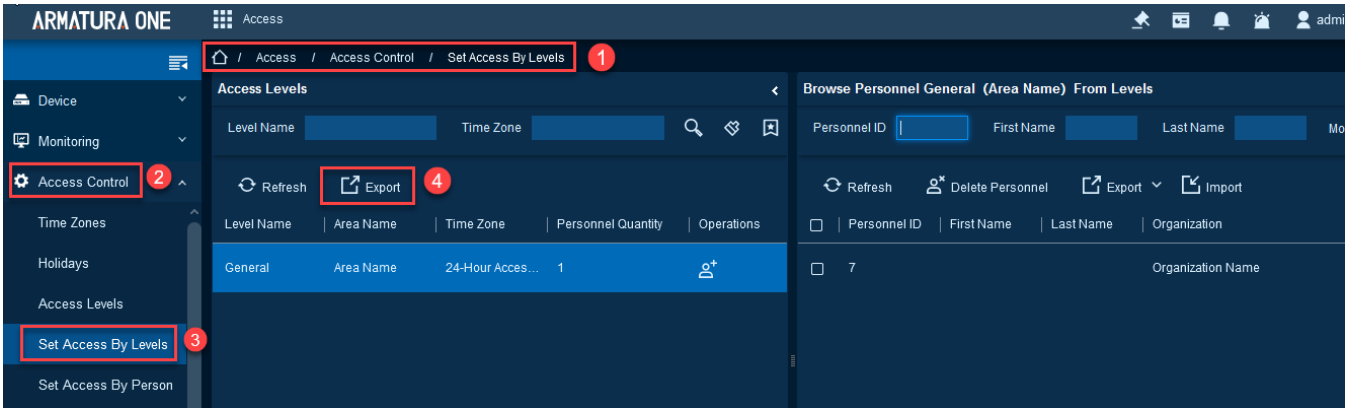
Trigger Result

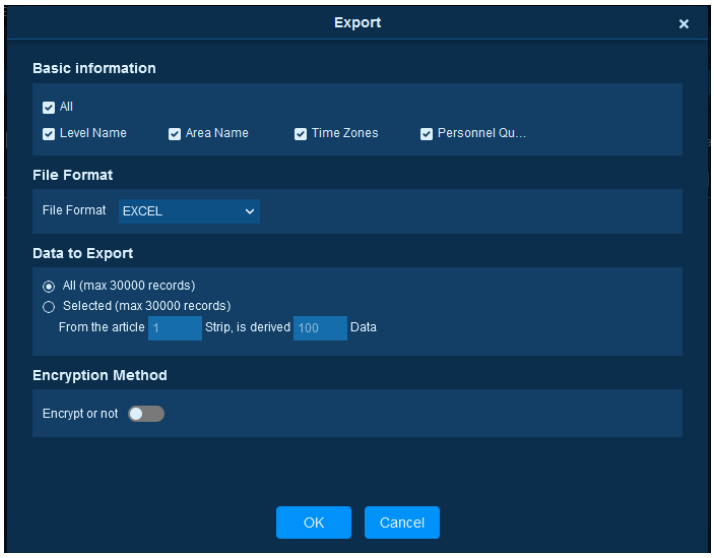
Access level data, including personnel names and associated devices, is exported in the selected file format.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access Control] > [Access Levels] > [Set Access by Levels]**.
- Select the desired access levels.
- Click **[Export]** in the corresponding column on the right.
- Choose the desired file format (e.g., Excel, PDF) and export method.
- Click **[OK]** to export.



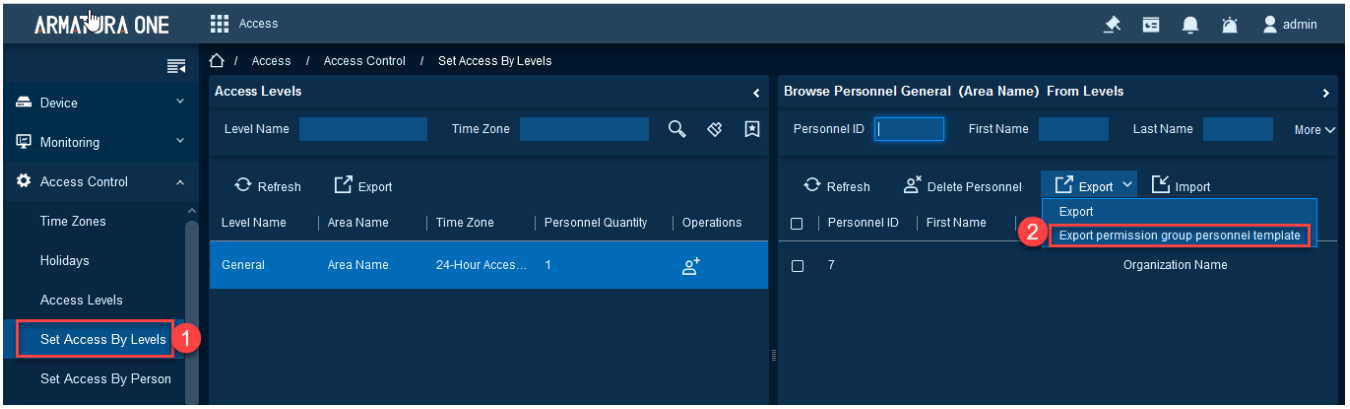


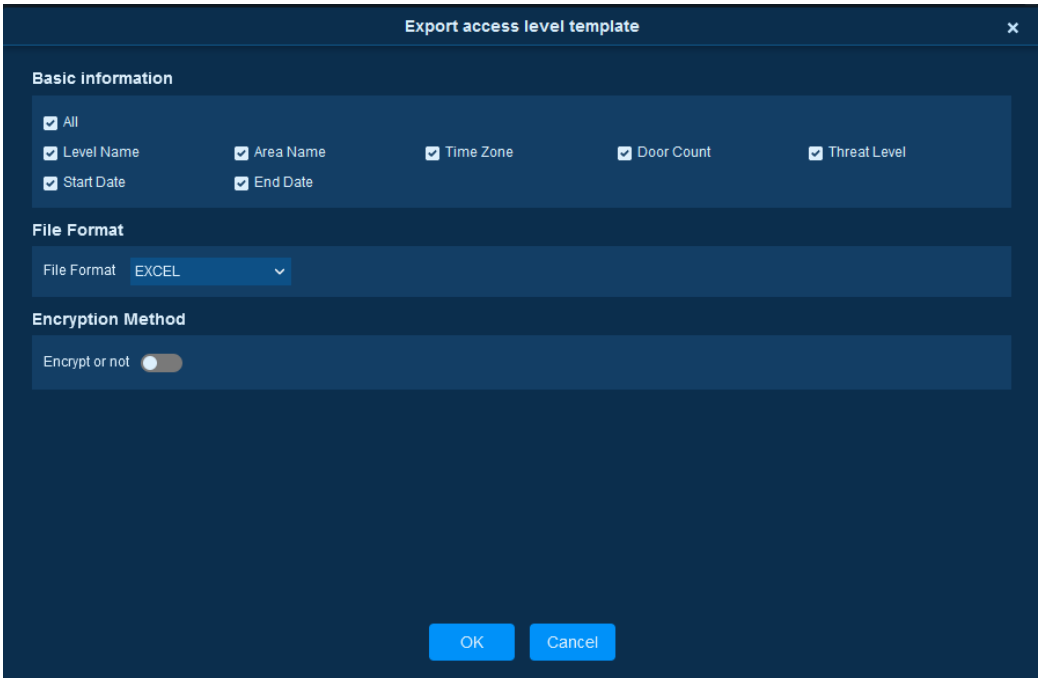
Export Access Level Template

Steps:

- Navigate to **[Access Control] > [Access Levels] > [Set Access by Levels]**.
- Select the relevant access levels.
- Click **[Export]**, then select **[Export Access Level Template]**.
- Choose the desired file format and export method.
- Click **[OK]** to export.

Copyright © 2024 ARMATURA LLC. All rights reserved





Import

Prerequisites for Use

Log into the system using an account with the required permissions. Existing access level records must be available for import.

Usage Scenarios

Import access level data to generate attendance records.

Trigger Result

Attendance records are created using the imported access level data.

Steps:

- Navigate to **[Access Control] > [Access Levels] > [Set Access by Levels]**.
- Click **[Import]**.
- Follow the on-screen prompts to upload and confirm the import process.

Copyright © 2024 ARMATURA LLC. All rights reserved

6.3.5. Set Access by Person

Function Description

This function allows administrators to manage access control permissions for individuals by assigning or removing access levels and configuring specific settings, such as superuser status and operational permissions.

Add Access Level to Person's Access Levels

Prerequisites for Use

Log into the system using an account with the required permissions. Access levels must already be configured.

Usage Scenarios

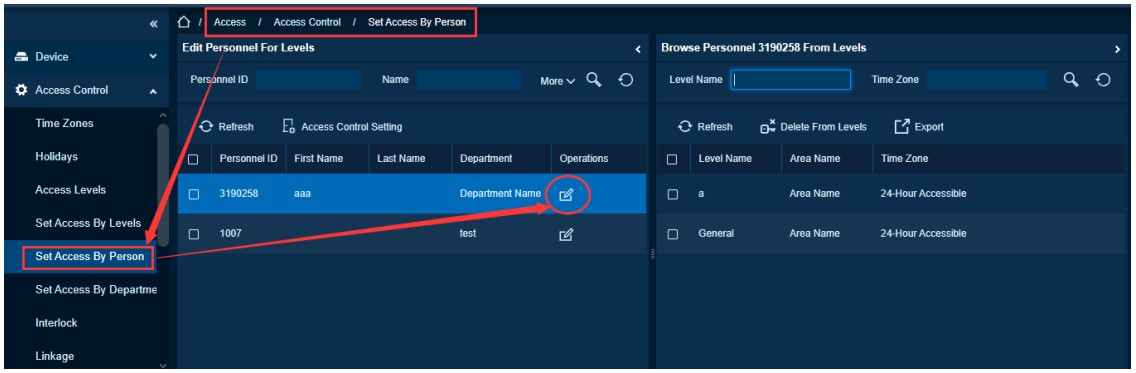
A person needs to be granted access control permissions for multiple access levels.

Trigger Result

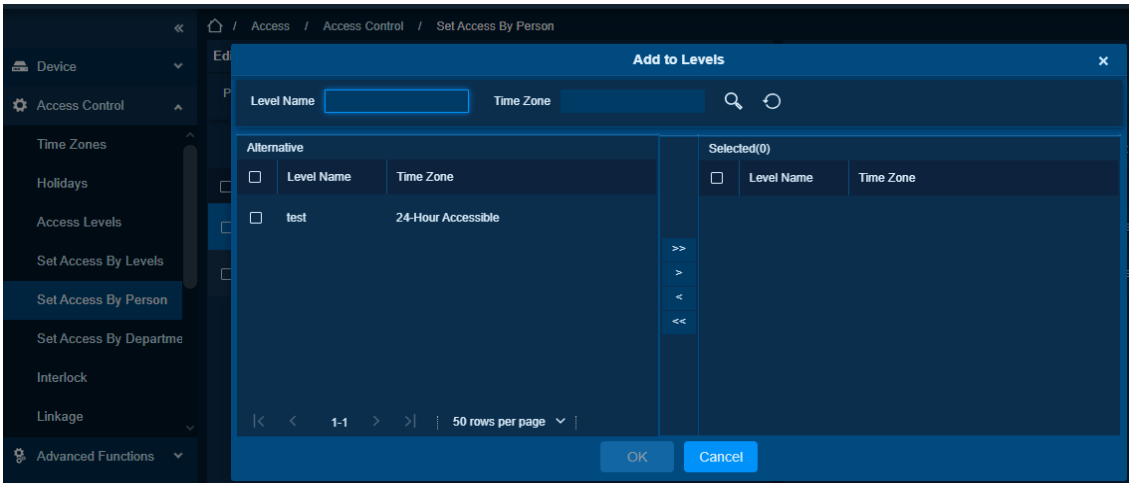
The individual is assigned multiple access control permissions.

Steps:

- Navigate to **[Access Control] > [Access Control] > [Set Access by Person]**.
- Select the **Employee** whose access levels you want to manage.
  The assigned access levels will be displayed in the list on the right.
- Click **[Add to Levels]** under Related Operations.
- In the **Add to Levels** dialog box:
  Select one or more access levels from the list.
  Use the arrow button > to move them to the selected list on the right.
- Click **[OK]** to save and assign the selected levels (multiple), and click to move it to the selected list on the right; then click **[OK]** to save.



Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Access Level from Person's Access Levels

Prerequisites for Use

Log into the system using an account with the required permissions. Access levels must already be configured.

Usage Scenarios

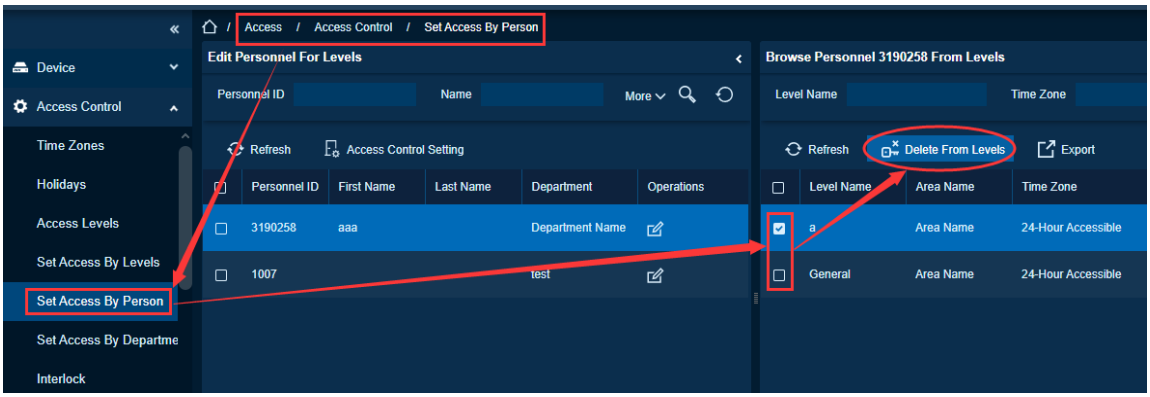
A person needs to have their access control permission removed for one or more access levels.

Trigger Result

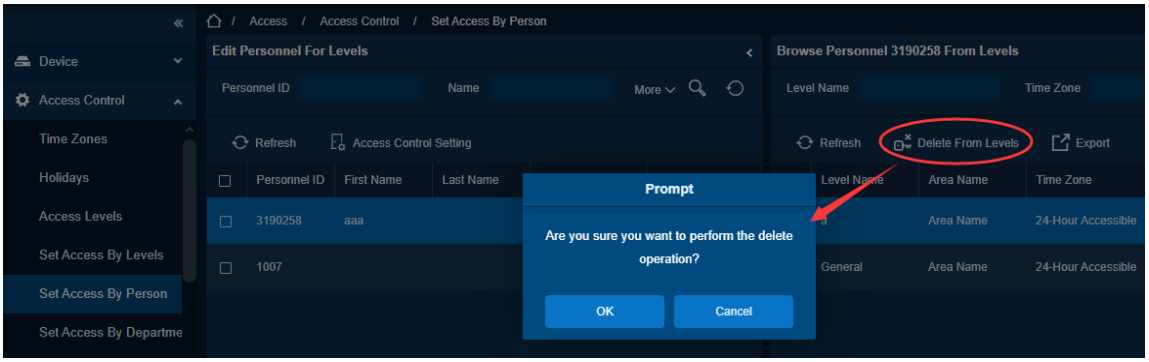
The individual's access control permissions for the selected levels are removed.

Steps:

- Select the **Employee** from the list to view their assigned access levels on the right.
- Choose one or more levels to remove.
- Click **[Delete from Levels]** above the list.
- Confirm the action by clicking **[OK]** to delete the selected levels.



Copyright © 2024 ARMATURA LLC. All rights reserved



Configure Access by Person

Prerequisites for Use

Log into the system using an account with the required permissions. Access levels must already be configured.

Usage Scenarios

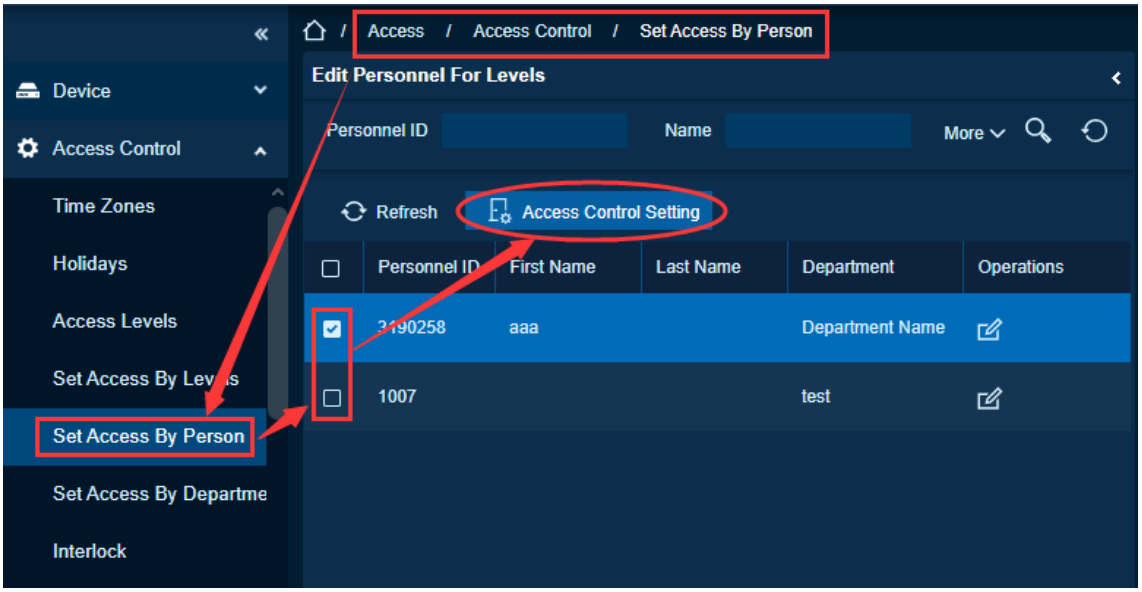
It is necessary to configure specific access control options for an individual, such as: Superuser status, Operational permissions, Extended passage time, Banned list inclusion, Validity period of permissions

Trigger Result

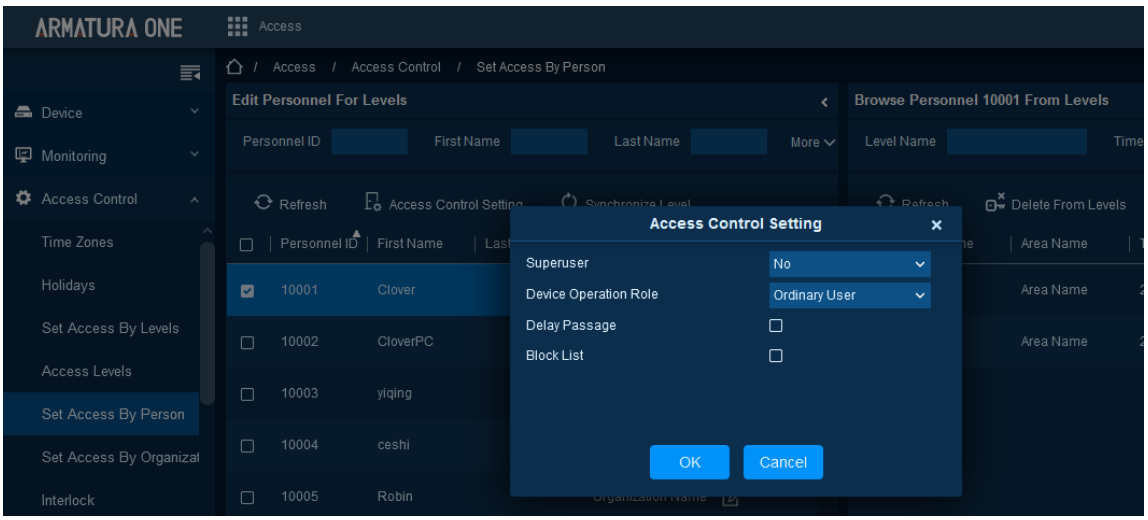
The person's access control configuration is updated based on the selected options.

Steps:

- Navigate to **[Access Control]** > **[Access Control]** > **[Set Access by Person]**.
- Select the individual to configure their access settings.



Copyright © 2024 ARMATURA LLC. All rights reserved



- In the configuration interface, set the following as needed:

Superuser Status: Enable or disable superuser privileges.

Operation Authority: Grant or restrict operational permissions.

Extended Passage Time: Specify additional time for passage.

Banned List: Add or remove the individual from the banned list.

Validity Period: Set the start and end date for the permissions.

- Click **[OK]** to save the configuration.

Synchronize Level

Prerequisites for Use

Log into the system using an account with the required permissions. Access levels must already be configured and assigned to the individual.

Usage Scenarios

A superuser needs to update and synchronize multiple access levels to ensure consistency across the system.

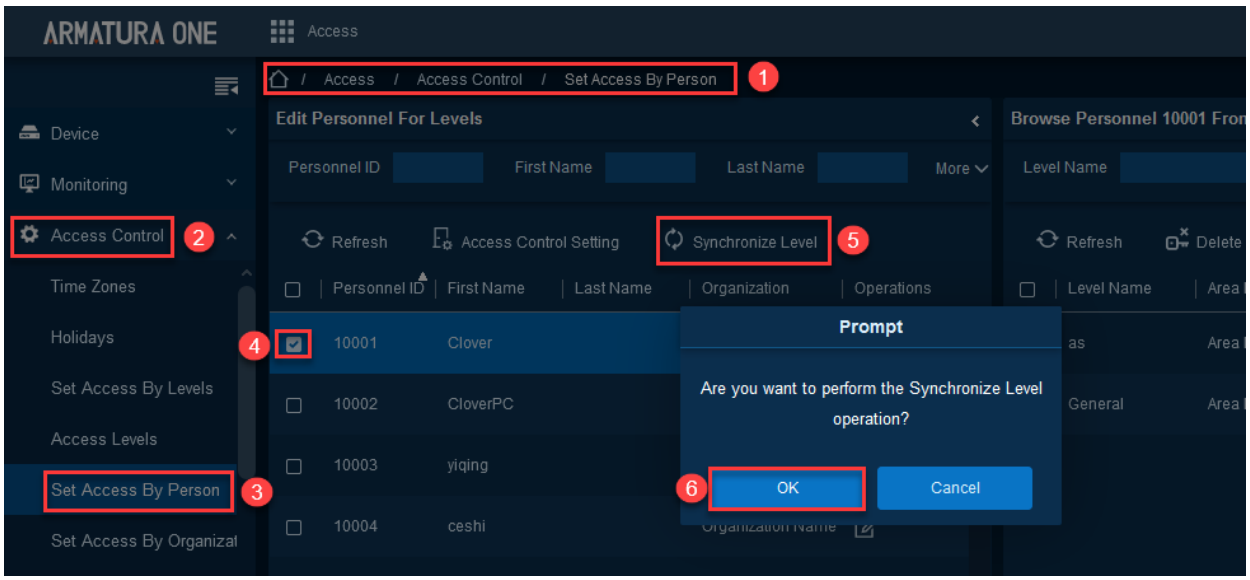
Trigger Result

The system synchronizes the assigned access levels for the selected person.

Steps:

- Navigate to **[Access Control]** > **[Set Access by Person]**.
- Select a person from the list on the left.
- Click **[Synchronize Level]** in the menu.
- Confirm the action by clicking **[OK]** to initiate the synchronization process.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.3.6. Set Access by Organization

Function Description

This feature allows users to manage access control settings for organizations by editing or deleting their access levels. Changes to organizational access settings will automatically update the access permissions for all personnel in the organization.

Edit to Default Levels

Prerequisites for Use

Log into the system using an account with the required permissions. Access levels must already be configured.

Usage Scenarios

When an organization requires access control permissions across multiple access levels.

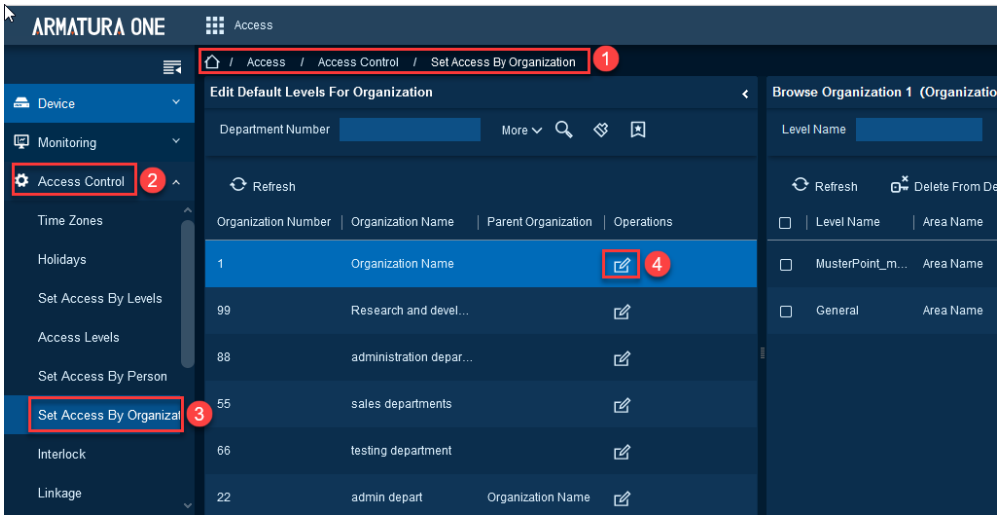
Trigger Result

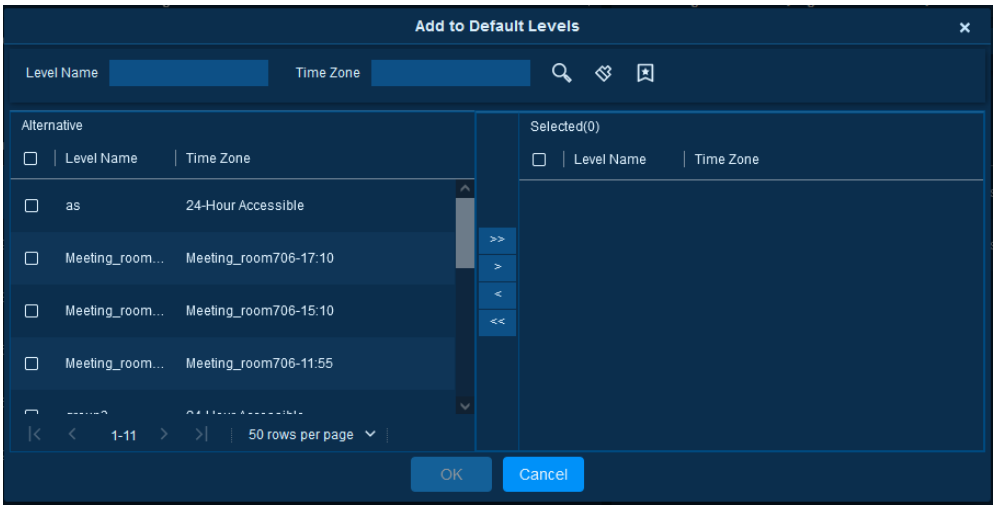
The organization gains access control permissions for the specified access levels.

Steps:

- Navigate to **[Access] > [Access Control] > [Set Access by Organization]** to access the organization-level access settings interface.
- Select the relevant organization from the list.
- Click **[Edit Add Default Levels]** to open the access level selection window.
- Choose the desired access levels from the available options.
- Use the arrow button > to move the selected access levels to the "Selected Levels" column on the right.
- Click **[OK]** to confirm and save the changes.

Copyright © 2024 ARMATURA LLC. All rights reserved





Delete the Default Levels

Prerequisites for Use

Log into the system using an account with the required permissions. The organization must already have access levels assigned.

Usage Scenarios

When the organization no longer requires access control permissions for specific access levels.

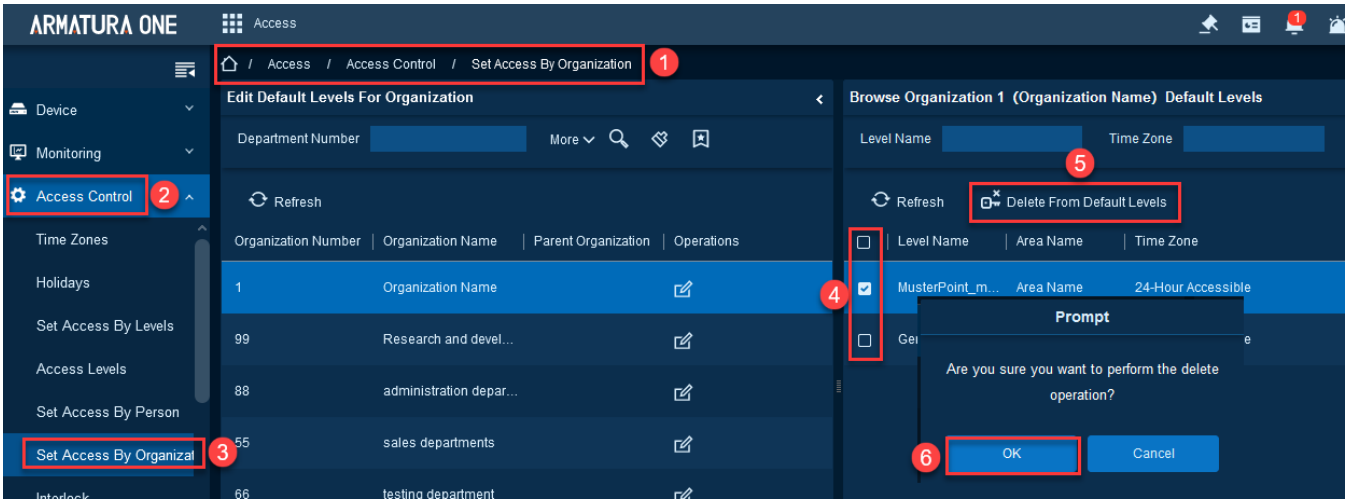
Trigger Result

The selected default access levels are removed from the target department or organization.

Steps:

- Navigate to **[Access] > [Access Control] > [Set Access by Organization]** to display the organization's access level settings.
- Select the relevant access levels from the "Assigned Levels" list on the right.
- Click **[Delete from Default Levels]** to remove the selected access levels.
- Confirm the action by clicking **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.3.7. Interlock

Function Description

The interlock function allows users to configure locking rules for two or more doors belonging to the same access controller. When one door is opened, the others remain closed, or their opening is restricted based on predefined rules. This feature is commonly used in high-security areas.

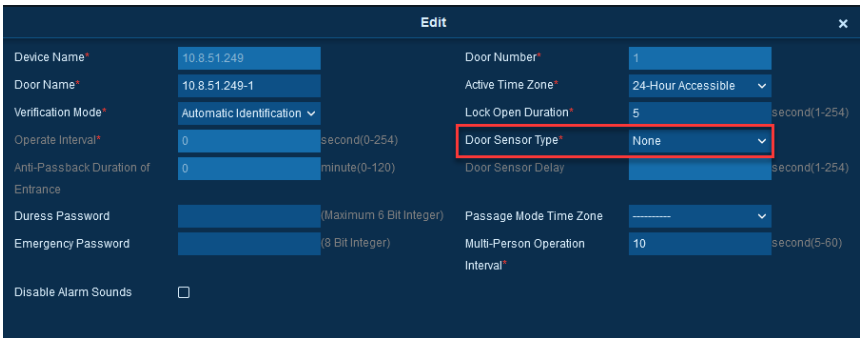
Add Interlock

Prerequisites for Use

Log into the system with an account that has the required authority.

Device Configuration:

- Navigate to **[Access] > [Device] > [Door]** and:
  - Edit the target doors.
  - Set the **Door Sensor Type** to **Normally Open** or **Normally Closed**.



Usage Scenarios

Required in areas with high-security demands, such as data centers, laboratories, or vaults, to ensure that only one door can be open at a time.

Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

The interlock is successfully implemented, controlling door operations based on the defined interlock rules.

Steps:

- Navigate to **[Access Control] > [Interlock] > [New]** to open the interlock setup interface.

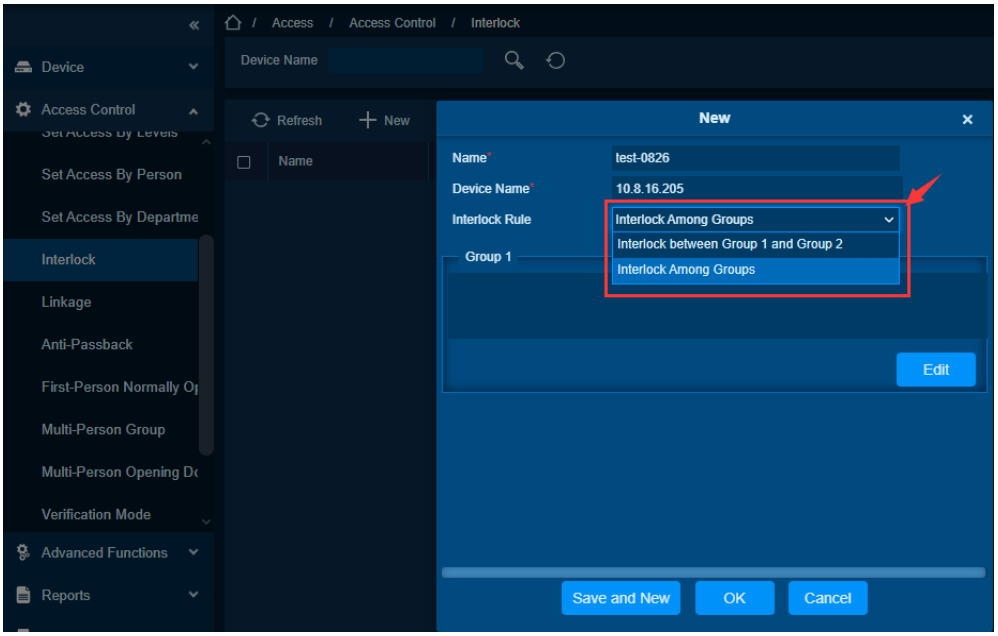
Select Target Device:

- Click **Device Name** and choose the device where the interlock rules will be applied.

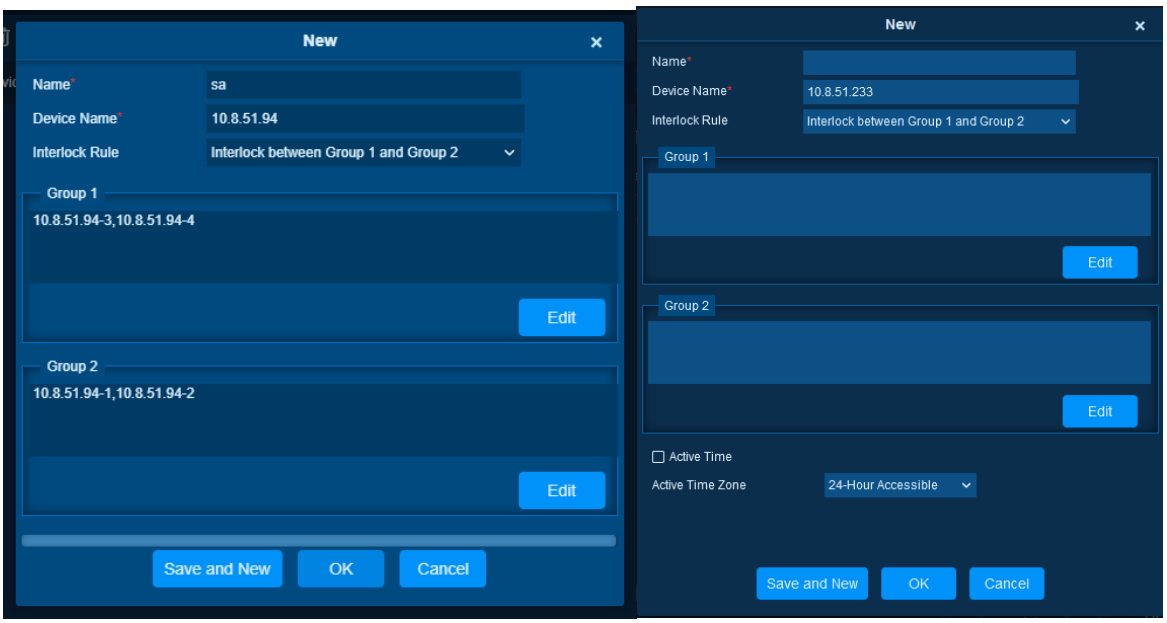
Configure Interlock Rules:

- Tick the desired interlock rule:
    - **Interlock between Group 1 and Group 2:** Defines interlock rules between two groups of doors.
    - **Interlock Among Groups:** Establishes interlock rules across multiple doors in the same group.

Armatura Controller



Copyright © 2024 ARMATURA LLC. All rights reserved



Active Time Configuration for Interlock Rules

Active Time refers to the specific periods during which a device's interlock rule is functional. This includes any time spent interacting with or operating the device, ensuring that access control is dynamically applied based on specified time intervals.

Active Time

Unchecked:

The interlock rule remains active without any time restrictions, functioning continuously.

Checked:

Additional fields appear, allowing users to define specific active times for the interlock rule.

This enables time-based interlock control, ensuring the rule is only active during the specified periods.

Active Time Zone

Purpose:

- Specifies the time zone settings for the active time of the interlock rule.

Options:

- **24-Hour Accessible:**
  - The interlock rule applies without time restrictions, active throughout the day (24 hours).
  - Suitable for environments requiring constant security enforcement.

Copyright © 2024 ARMATURA LLC. All rights reserved

Interlock Rules:

Interlock Between Group 1 and Group 2:

- Configures interlock functionality between two distinct groups of doors.

Interlock Among Groups:

- Applies interlock functionality across multiple doors within the same group.

Example:

Rule	Interlock between Group 1 and Group 2	Interlock Among Group
Group	Group 1: Door 1, Door 2 Group 2: Door 3, Door 4	Group: Door 1, Door 2, Door 3, Door 4
Door 1 Verify	Check Door 3 and Door 4 door sensor status	Check Door 2, Door 3, and Door 4 door sensor status
Door 2 Verify	Check Door 3 and Door 4 door sensor status	Check Door 1, Door 3, and Door 4 door sensor status
Door 3 Verify	Check Door 1 and Door 2 door sensor status	Check Door 1, Door 2, and Door 4 door sensor status
Door 4 Verify	Check Door 1 and Door 2 door sensor status	Check Door 1, Door 2, and Door 3 door sensor status

Edit Interlock

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

Modification is required for previously set interlock configurations to meet heightened security requirements.

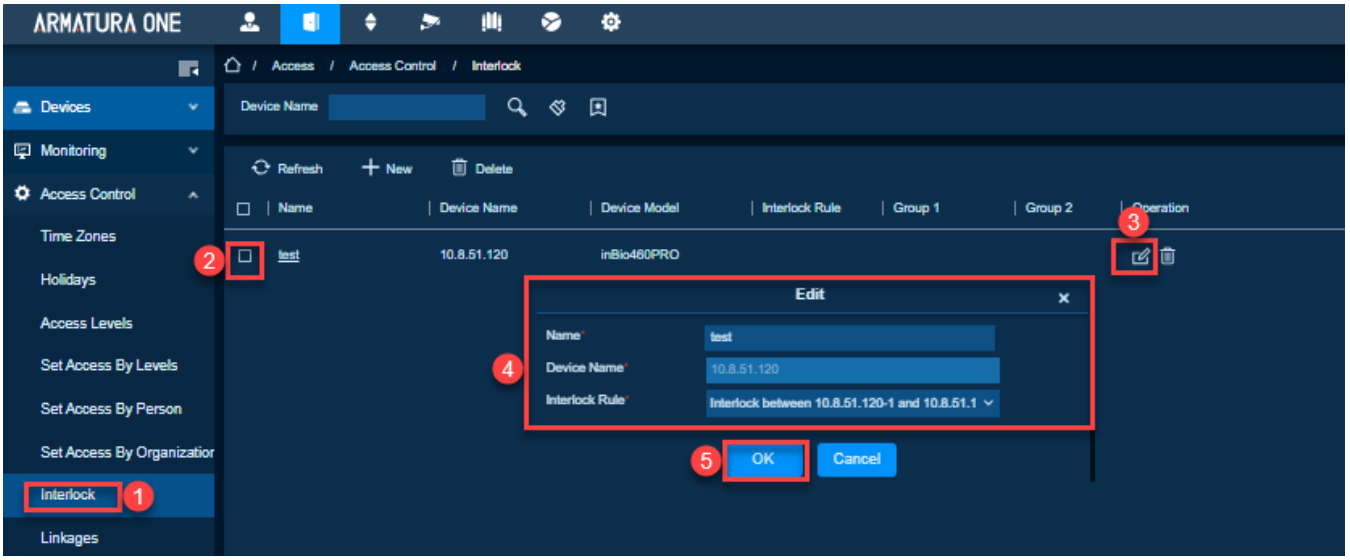
Trigger Result

The interlock rules are successfully modified, and the doors operate based on the updated interlock configuration.

Steps:

- Navigate to **[Access] > [Access Control] > [Interlock]** to access the interlock management interface.
- Locate the target device name.
- Click **[Edit]** to modify the interlocking rules as needed.
- Save changes to apply the updated interlock settings.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Interlock

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

Interlock is no longer required for a specific area, or the doors do not need interlock control.

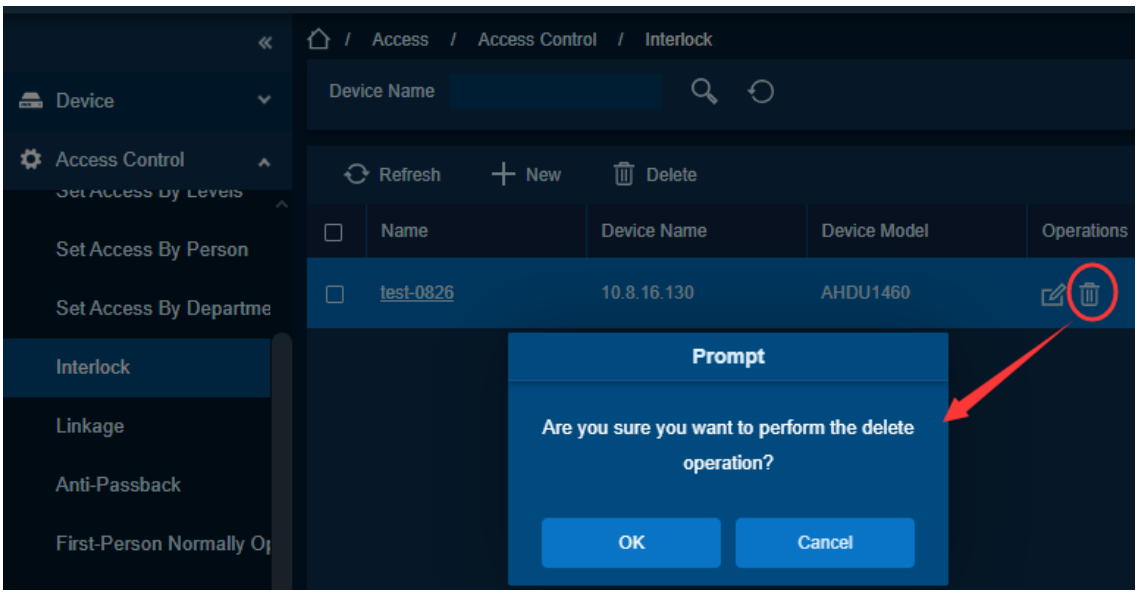
Trigger Result

The interlock configuration is successfully deleted, and the doors are no longer controlled by interlock rules.

Steps:

- Navigate to **[Access] > [Access Control] > [Interlock]** to access the interlock management interface.
- Locate the target device name.
- Click **[Delete]** to remove the interlock rule.
- Confirm the deletion to finalize the process.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.3.8Linkage

Function Description

Linkage settings enable the configuration of automated actions triggered by events at input points of the access control system. These actions can include opening doors, sending SMS or email alerts, activating alarms, or handling system abnormalities, which are displayed in the monitoring interface in real-time.

Add Linkage

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

When an event is triggered by a device, door, reader, or auxiliary input, the system performs a defined action such as opening a door, sending SMS, or sending an email notification.

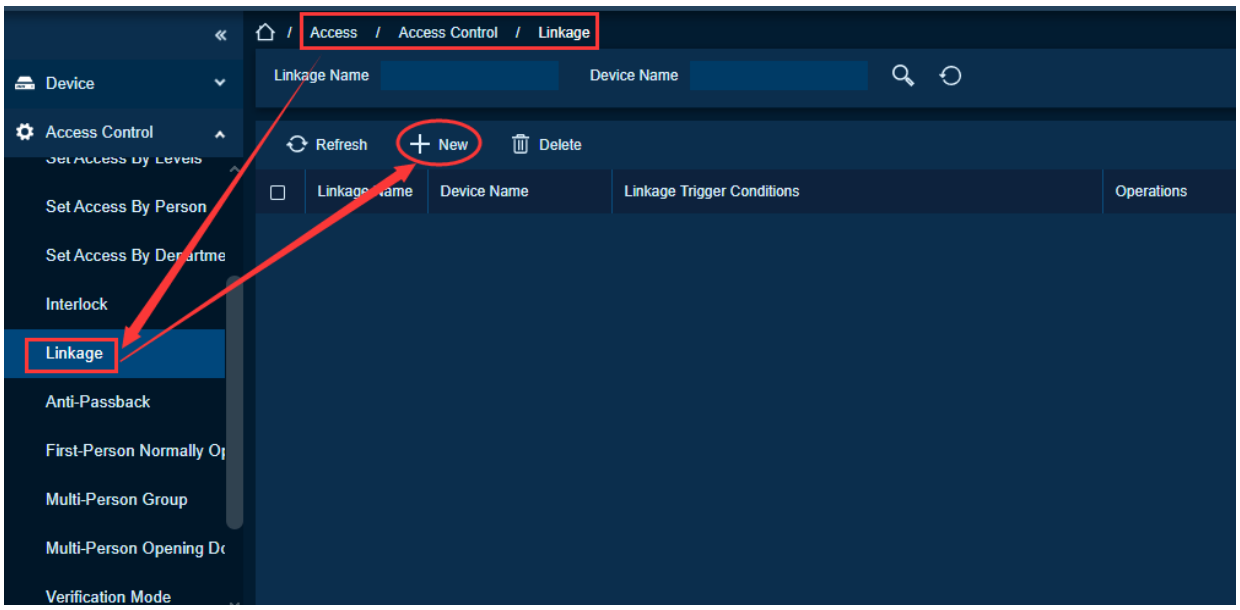
Trigger Result

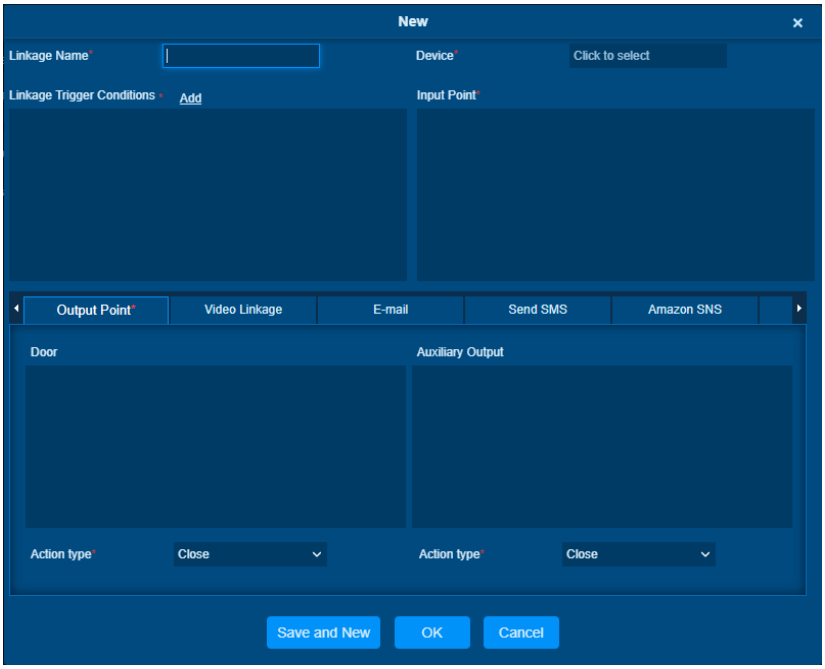
When an input point triggers the specified event, a predefined action (e.g., unlocking a door, sending an alert) is executed at the designated output point. The event and corresponding action are logged and displayed in the event list for monitoring.

Steps:

- Navigate to **[Access Control] > [Linkage] > [New]** to create a new linkage.
- Enter a **Linkage Name** to identify the linkage event.
- Select the target **Device** and click **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved





Note:

Upon selecting a device, the system displays the available linkage settings.

The system verifies the device's connectivity and extended parameter availability:

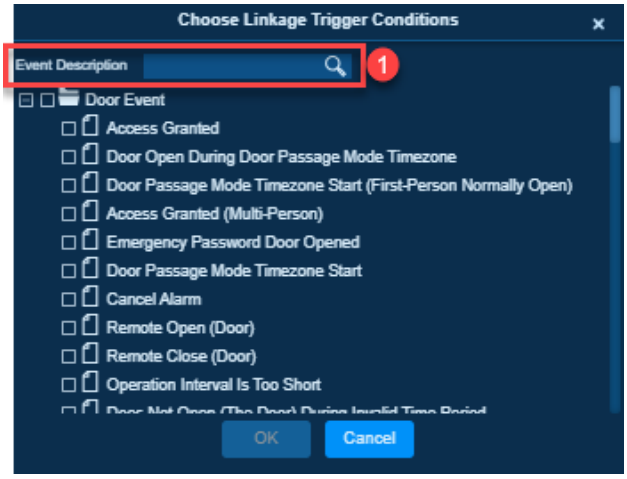
- **Unavailable Parameters**: If the device lacks extended parameters, no linkage can be set.
- **Available Parameters**: The system displays linkage options based on the **Door Quantity**, **Auxiliary Input**, and **Auxiliary Output** of the selected device.

Configure **Linkage Trigger Conditions**:

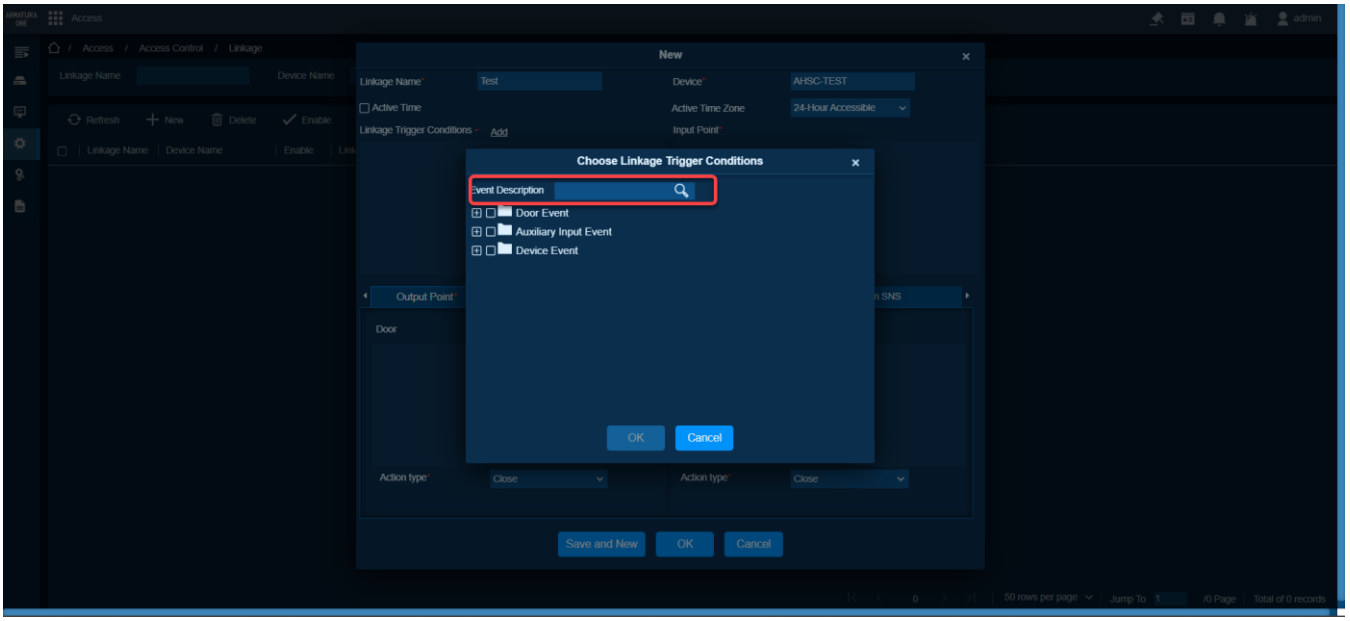
- Define the events or input signals (e.g., door open, card swipe) that will activate the linkage.
- Specify the desired actions or outputs (e.g., door unlock, alarm activation, notification dispatch).

Copyright © 2024 ARMATURA LLC. All rights reserved

OmniAC Series



Horizon Series

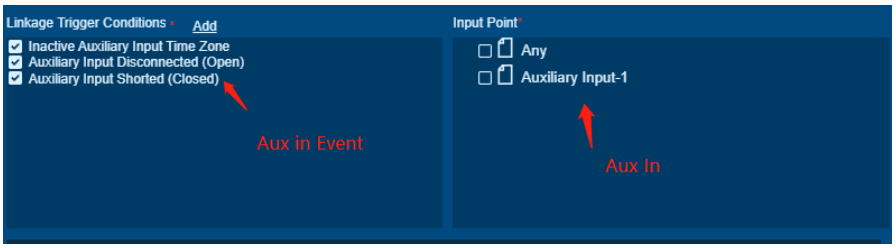


Select Input Point:

Choose the Input Point based on the condition to trigger the linkage:

- Device: Select the device's input point.
- Door: Choose input points such as door sensors or reader verification points.
- Auxiliary Input: Filter and select relevant auxiliary input points.

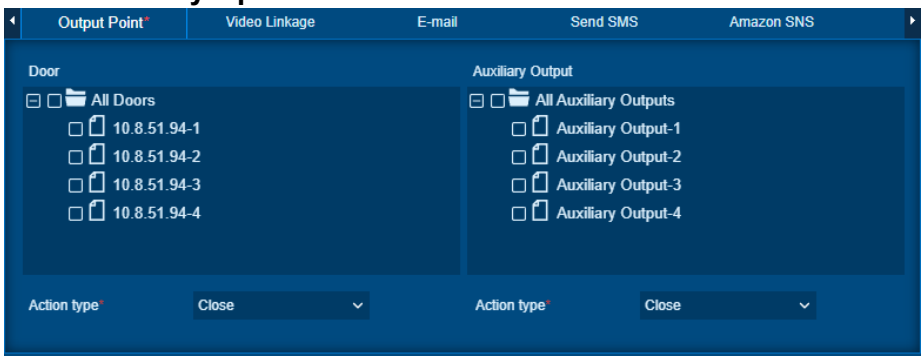
Copyright © 2024 ARMATURA LLC. All rights reserved



Specify the **Output Point** for the action to be performed:

Target Door or Auxiliary Output:

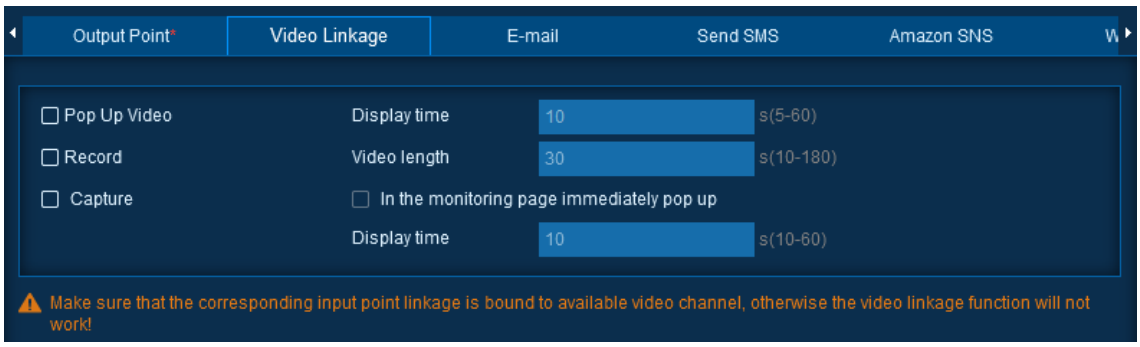
- For **Door Actions**, select one of the following:
  - **Close**
  - **Open**
  - **Normally Open**
  - **Lock**
  - **Unlock**
- For **Auxiliary Output Actions**, select one of the following:
  - **Close**
  - **Open**
  - **Normally Open**



Set Video Linkage:

Configure below actions related to video linkage.

Copyright © 2024 ARMATURA LLC. All rights reserved

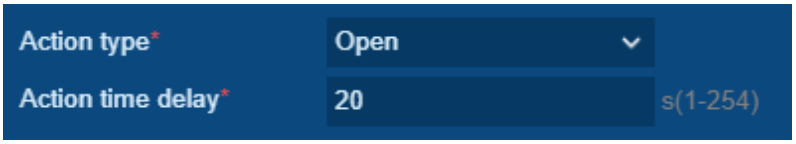


- **Pop-Up Video**: Enable or disable a real-time preview page in monitoring. Set the pop-up duration.
- **Record**: Enable or disable background video recording and configure the recording duration.
- **Capture**: Enable or disable background snapshots.

Delay:

Set the delay duration for the action. Valid range: **1 to 254 seconds**.

This setting is only applicable when the **Action Type** is "Open."



After completing the linkage configuration, click **[OK]** to save and exit.

The newly created linkage setting will appear in the linkage list for reference.

Example Use Case

- **Trigger Condition**: Normal Punching Open Door.
- **Input Point**: Door 1.
- **Output Point**: Lock 1.
- **Action Type**: Open.
- **Delay**: 60 seconds.

Result: When "Normal Punching Open Door" is triggered at **Door 1**, the system executes the action **Open** at **Lock 1**, keeping the door open for **60 seconds**.

Note:

Device Modifications: During editing, users cannot modify the device associated with the linkage setting, but can update the Linkage Setting Name and Configuration. When a device is deleted, all associated linkage settings are automatically removed from the system.

Restrictions on Adding or Editing Linkage Settings

Specific Input Point vs. 'Any' Input Point: When a linkage setting exists with a specific input point (such as a door or auxiliary input), new or edited linkage settings for the same device and trigger

Copyright © 2024 ARMATURA LLC. All rights reserved

conditions cannot use 'Any' as the input point. Conversely, if a linkage setting exists with the input point 'Any', new or edited linkage settings for the same device and trigger conditions cannot specify a particular input point.

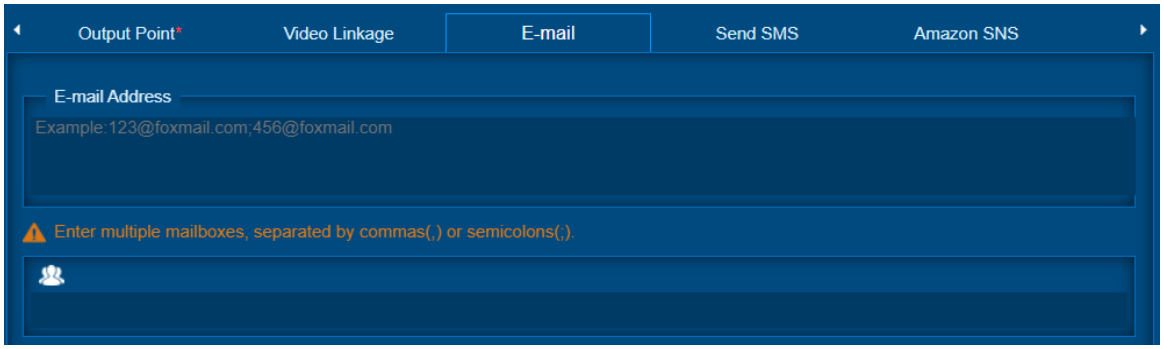
Identical Input and Output Points: The system prevents configuration of linkage settings with matching input and output points. For instance, a setting where both input and output points are assigned to Door 1 is not permitted.

Consecutive Logical Linkages: The same device supports consecutive logical linkage settings, allowing sequential actions such as Trigger Condition A leading to Output Action X, followed by Trigger Condition B leading to Output Action Y.

Multiple Trigger Conditions: Each linkage setting can incorporate multiple trigger conditions, enabling sophisticated event-based responses and actions within the system.

Set Email Notification

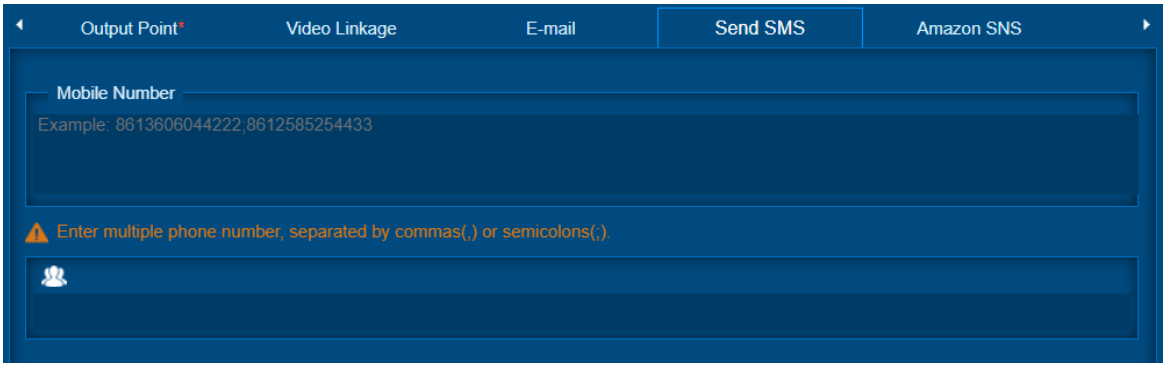
Ensure that the **Email service** is configured in the system module.



Email Address: Specify the email address to receive notification messages when the linkage is triggered.
Select Personnel: Choose personnel from the system to be notified via email.
Note: The selected personnel must have their email information configured in the Personnel Module.

Set SMS Notification.

- Ensure that the **SMS service** is configured in the system module.



Mobile Phone Number:

- Specify the mobile phone number to receive SMS notifications when the linkage is triggered.

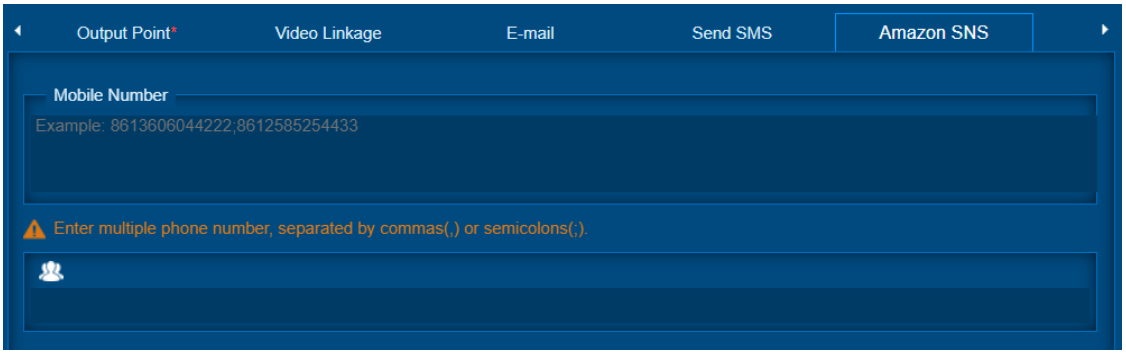
Copyright © 2024 ARMATURA LLC. All rights reserved

Select Personnel:

- Choose personnel from the system to be notified via SMS.
- **Note**: The selected personnel must have their **phone number information** configured in the **Personnel Module**.

Set Amazon SNS Notification.

- Ensure that the **Amazon SNS service** is configured in the system module.



Mobile Phone Number:

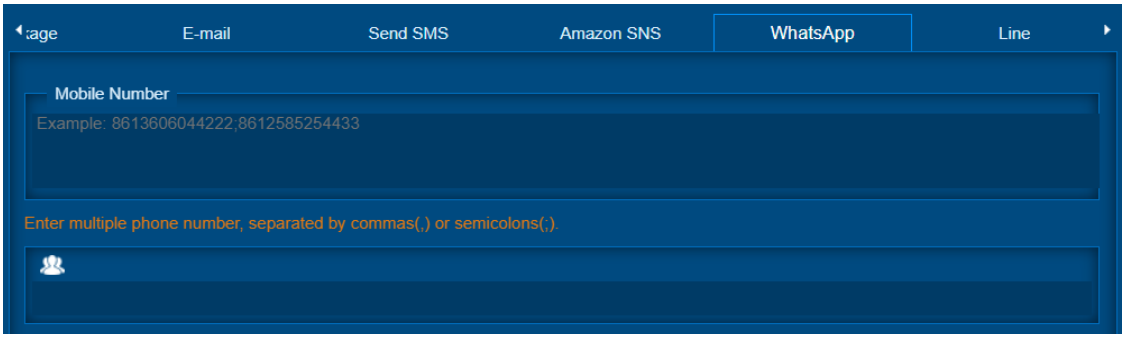
- Specify the mobile phone number to receive notifications via Amazon SNS when the linkage is triggered.

Select Personnel:

- Choose personnel from the system to receive notifications via Amazon SNS.
- **Note**: The selected personnel must have their **phone number information** configured in the **Personnel Module**.

Set WhatsApp Notification

- Ensure that the **WhatsApp service** is configured in the system module.



Mobile Phone Number:

- Specify the mobile phone number linked to the WhatsApp account to receive notifications when the linkage is triggered.

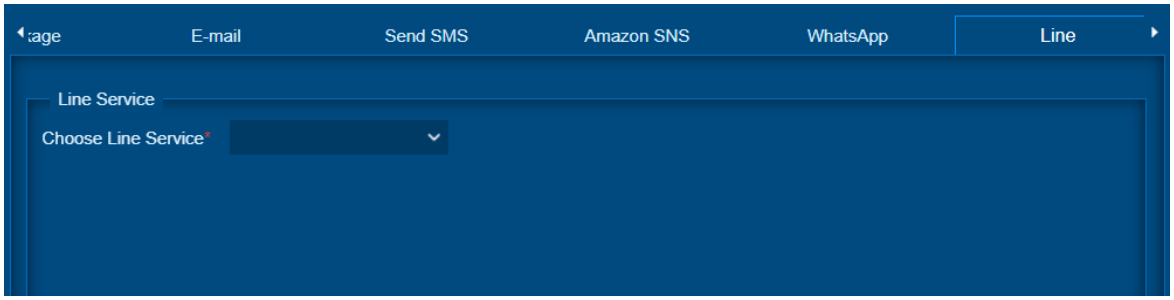
Copyright © 2024 ARMATURA LLC. All rights reserved

Select Personnel:

- Choose personnel from the system to receive WhatsApp notifications.
- **Note**: The selected personnel must have their **phone number information** configured in the **Personnel Module**.

Set Line Notification

- Ensure that the **Line service** is configured in the system module.



Choose Line Service:

Select the Line service or group to receive notifications when the linkage is triggered.

Edit Linkage

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

When it is necessary to modify the linkage action of the output port triggered by a specific input port, such as changing the behavior of doors or auxiliary outputs based on a specific event.

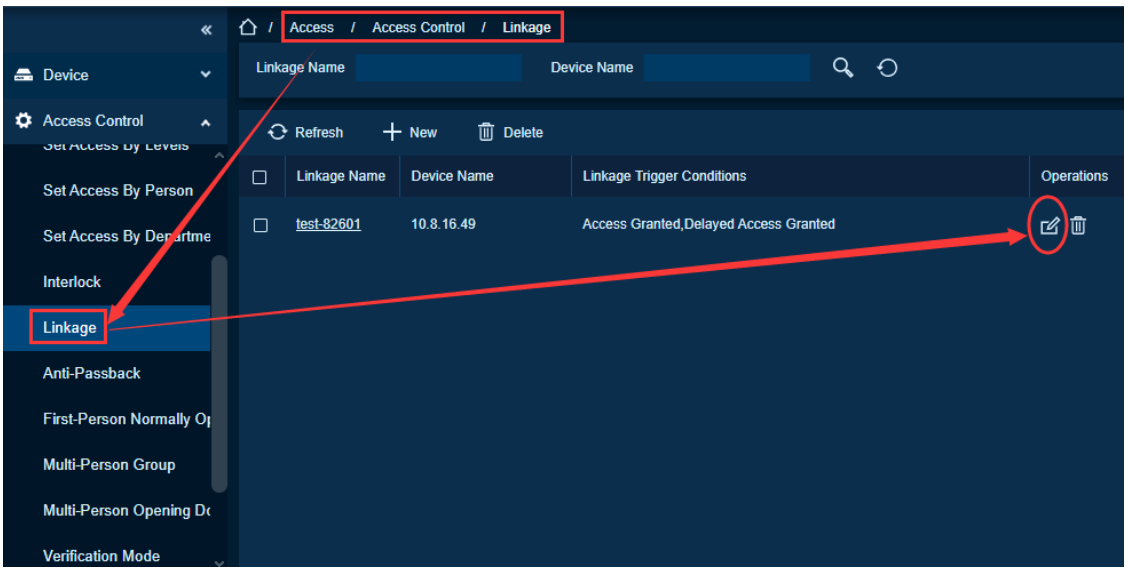
Trigger Result

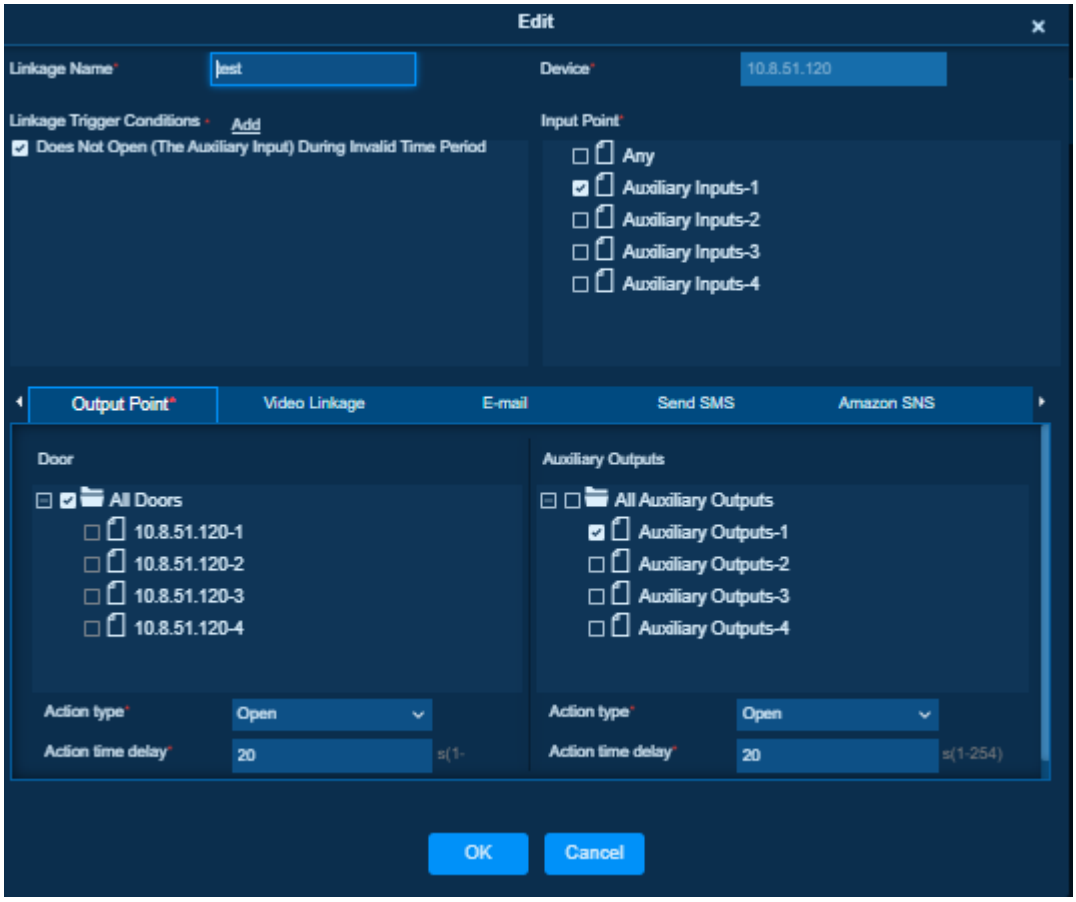
When the modified linkage event is triggered at the specified **Input Point**, the corresponding **Output Point** will perform the updated action. The event and actions will be displayed in the **Event Monitoring List** for tracking and monitoring.

Steps:

- Navigate to **[Access] > [Access Control] > [Linkage]** to display the list of current linkage settings.
- Locate the desired linkage rule in the list and click **[Edit]** to modify its settings.

Copyright © 2024 ARMATURA LLC. All rights reserved





Active Time Configuration

Active Time:

- **Checkbox (Active Time)**:
  - **Unchecked**: The linkage rule will be active at all times without time restrictions.
  - **Checked**: Enables time-specific configuration for when the linkage rule will be active.

Copyright © 2024 ARMATURA LLC. All rights reserved

- **Additional Settings**:
    - When the checkbox is selected, additional fields for setting active time become available.

Active Time Zone:

- **Dropdown Menu**:
    - Specify the time zone applicable to the active time settings.
- **24-Hour Accessible**:
    - The linkage rule is active throughout the day, with no time-based restrictions.

Delete Linkage

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

When it is necessary to remove a previously configured linkage action between an **Input Point** and an **Output Point**. For example, if a linkage event is no longer required for a door or auxiliary output.

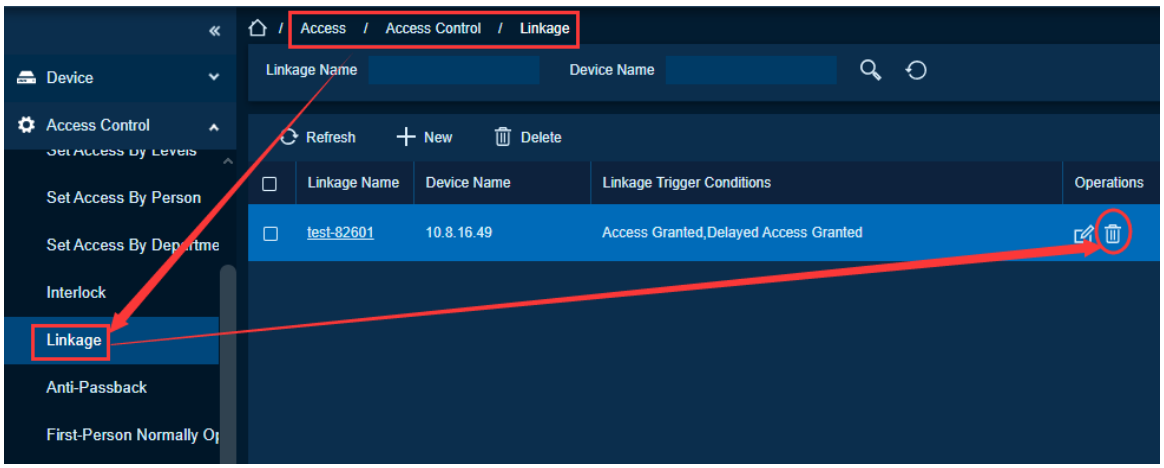
Trigger Result

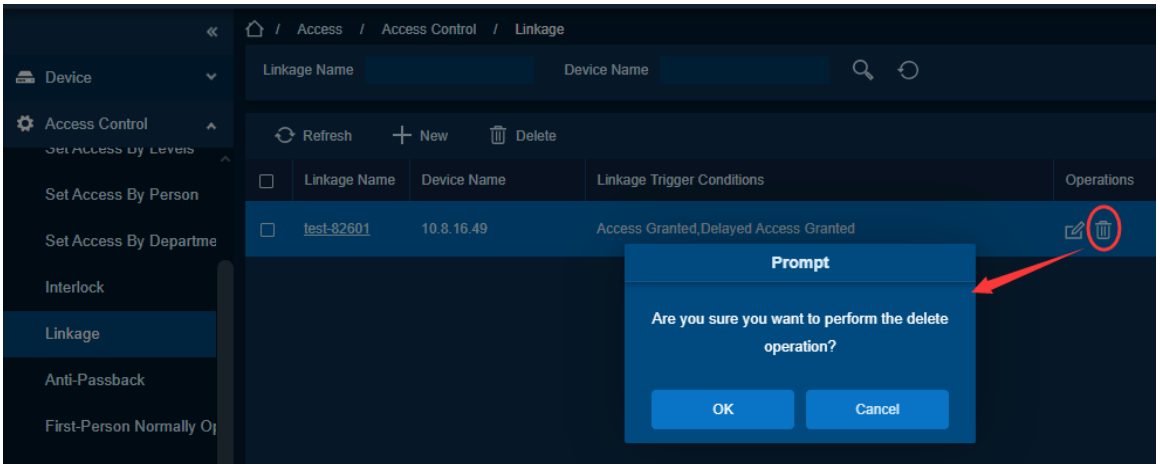
The specified linkage event is deleted. Once removed, events triggered by the **Input Point** will no longer generate actions at the **Output Point**.

Steps:

- Navigate to **[Access]** > **[Access Control]** > **[Linkage]** to display the list of current linkage settings.
- Identify the linkage you wish to remove from the list.
- Click **[Delete]** next to the selected linkage.
- Confirm the deletion in the prompt that appears.

Copyright © 2024 ARMATURA LLC. All rights reserved





Copyright © 2024 ARMATURA LLC. All rights reserved

6.3.9Anti-Passback

Function Description

The **Anti-Passback** feature ensures that cardholders adhere to strict entry and exit protocols. It requires personnel to swipe their card when entering and exiting specific areas, maintaining consistency in entry and exit records. The system supports **In**, **Out**, and **In/Out** anti-passback rules.

Add Anti-Passback Rule

Prerequisites for Use

Log into the system using an account with the required permissions. Devices that support anti-passback should be correctly configured and operational.

Usage Scenarios

Ideal for high-security areas requiring controlled personnel entry and exit.

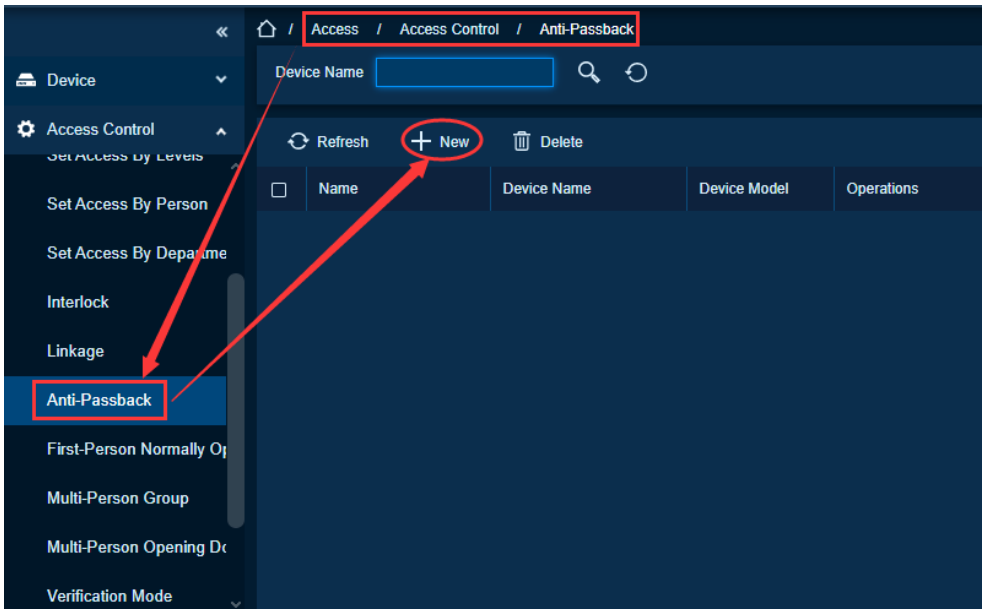
Enforces strict compliance with access protocols to maintain safety and accountability.

Trigger Result

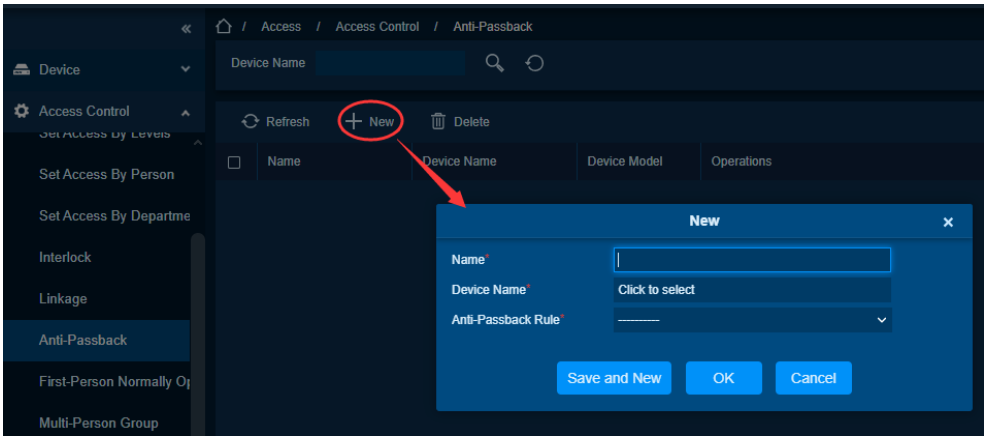
Once anti-passback rule is added entry and exit rule will be enabled. Unauthorized entry or exit attempts will be denied, and an **Anti-Passback** event will be generated.

Steps:

- Go to **[Access Control] > [Anti-Passback] > [New]** to open the edit interface.



Copyright © 2024 ARMATURA LLC. All rights reserved



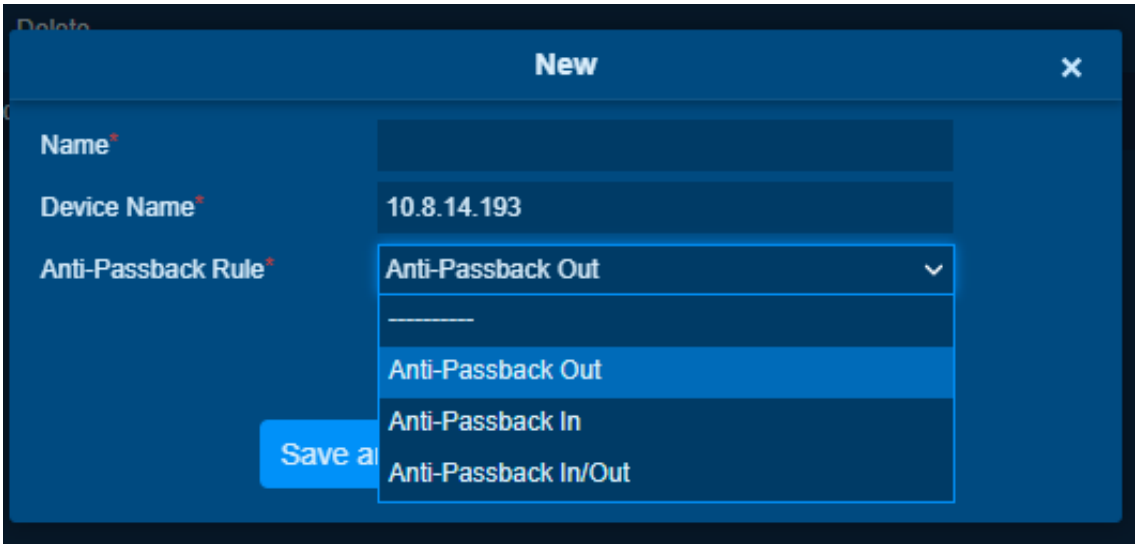
Select devices:

Devices already configured with anti-passback settings will not appear in the dropdown list.

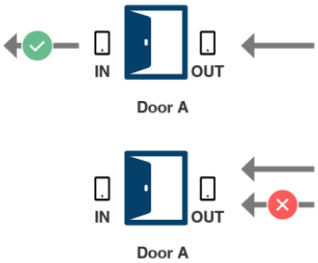
Once existing anti-passback rules are deleted, the devices will reappear in the dropdown for selection.

The device options vary based on the number of doors it controls.

- **OmniAC Series**

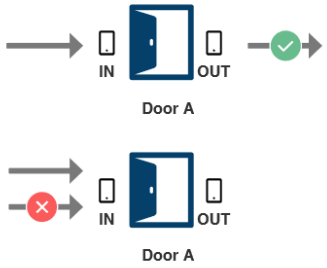


IN Reader (e.g., OmniAC 20) and **OUT Reader (slave device)** configuration:
Anti-Passback Out: When exiting via the OUT Reader, the system verifies if the cardholder has a transaction from the IN Reader. If not, access is denied, and an Anti-Passback event is generated.

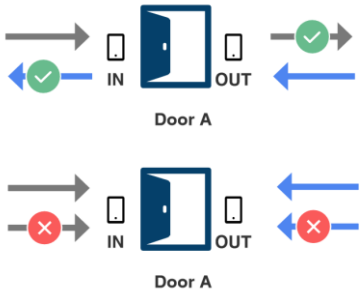


Copyright © 2024 ARMATURA LLC. All rights reserved

Anti-Passback In: When entering via the IN Reader, the system checks for a transaction from the OUT Reader. If not found, access is denied, and an Anti-Passback event is logged.

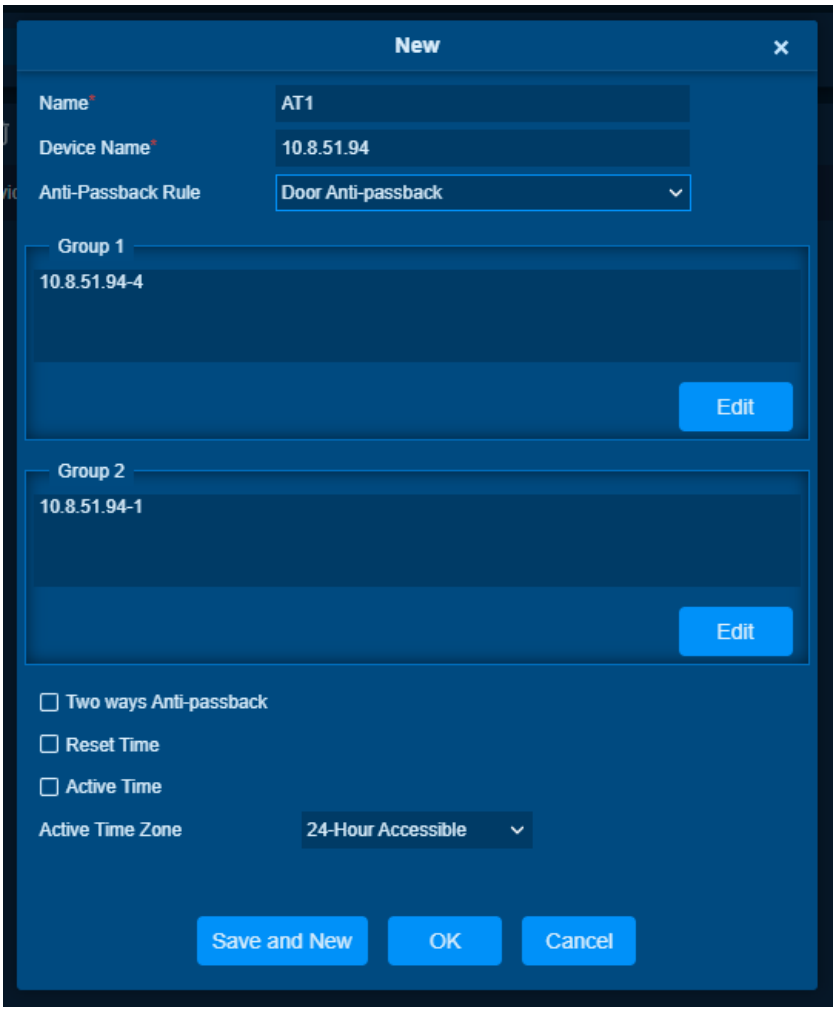


Anti-Passback In/Out: The system ensures the cardholder has corresponding transactions for both entry and exit between the IN Reader and OUT Reader. Missing transactions trigger access denial and an Anti-Passback event.



Copyright © 2024 ARMATURA LLC. All rights reserved

- **Horizon Series Controllers**



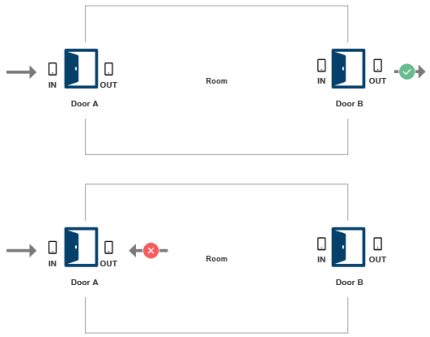
Set Anti-Passback Rules:
One-Way Anti-Passback:

- Personnel can only enter through a designated **IN Door** and exit through a designated **OUT Door**.
- Example:
  - Group 1: Door A (IN).
  - Group 2: Door B (OUT).
  - If a cardholder enters Door A (IN) and exits via Door A (OUT) instead of Door B, access is denied, and an **Anti-Passback** event is logged.

Copyright © 2024 ARMATURA LLC. All rights reserved

Two-Way Anti-Passback:

- Personnel can alternate between multiple doors, but each transition requires a valid transaction.



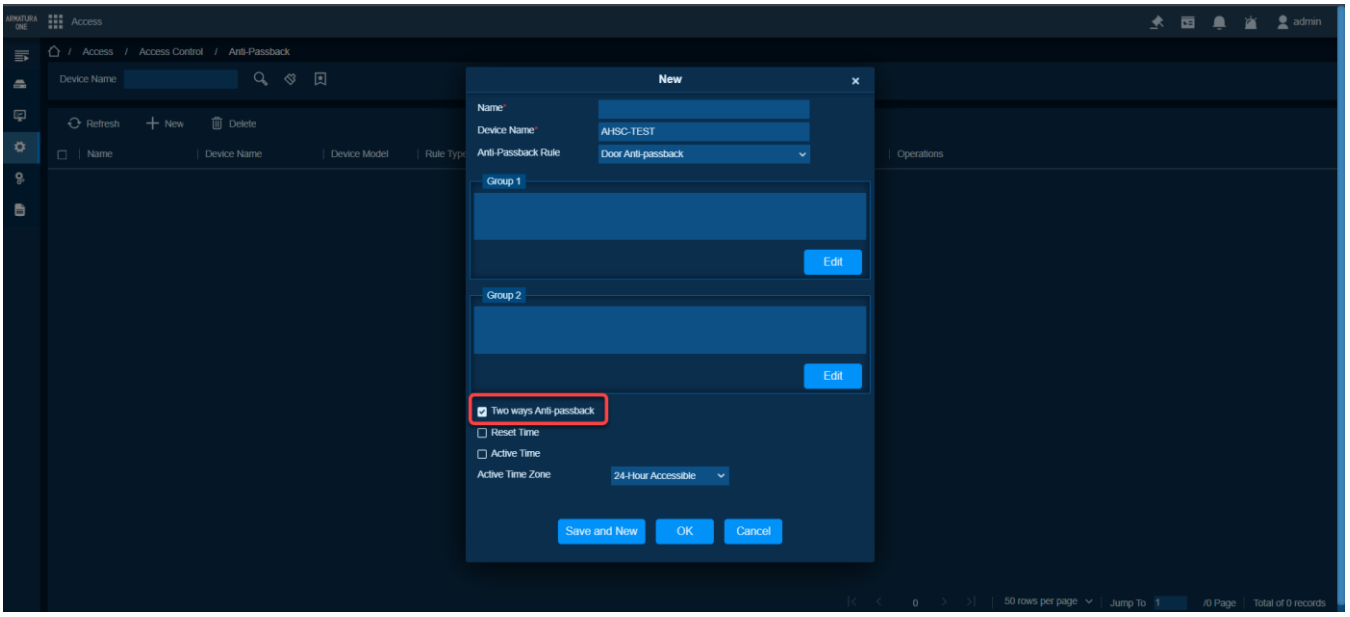
Note:

Deleting an anti-passback rule will make the corresponding device reappear in the dropdown for new configurations.

The feature is flexible, supporting various levels of enforcement:

- **Door-specific** configurations.
- Comprehensive rules across multiple devices.

Copyright © 2024 ARMATURA LLC. All rights reserved

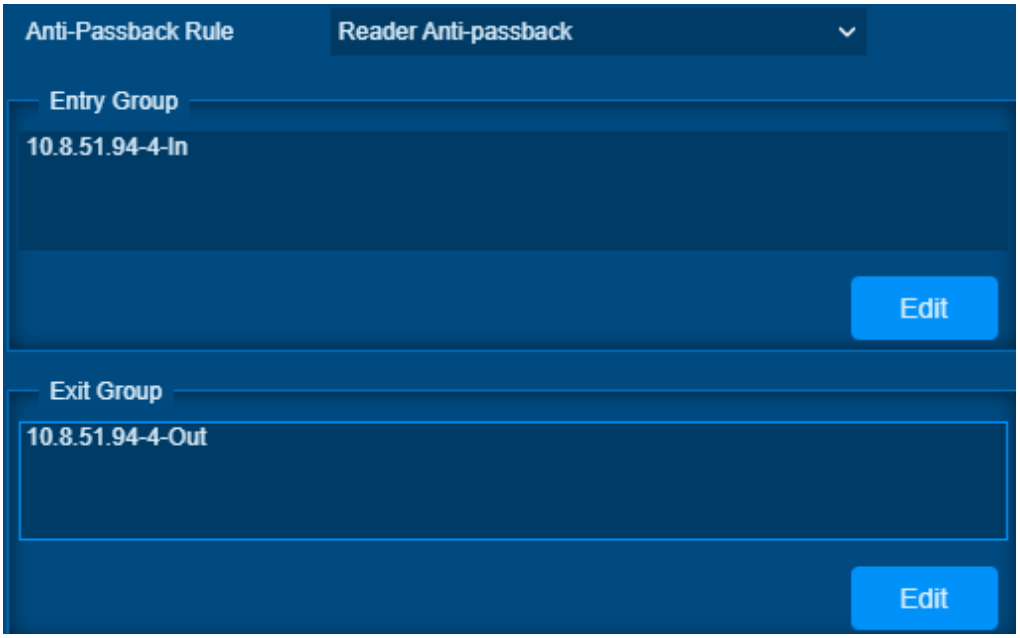


- **Reader Anti-Passback**

Rule 2: Reader Anti-Passback

Reader Anti-Passback ensures that personnel can only follow designated entry and exit routes for a specific reader associated with a door.

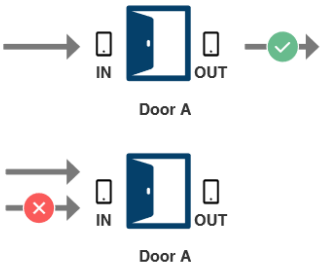
- **Group 1**: Reader IN (Door A).
- **Group 2**: Reader OUT (Door A).



Example:

Personnel can only enter via **Reader IN (Door A)** and exit via **Reader OUT (Door A)**. If personnel attempt to enter and exit from the same reader (e.g., **Reader IN (Door A)**), the system will deny access and log an **Anti-Passback** event.

Copyright © 2024 ARMATURA LLC. All rights reserved



Note:

One-Way Anti-Passback Design:

The system does not restrict personnel from entering via **Reader OUT (Door A)** and exiting via **Reader IN (Door A)** unless configured otherwise.

To enforce **Two-Way Anti-Passback**, you need to:

- Set a new rule with **Group 1: Reader OUT (Door A)** and **Group 2: Reader IN (Door A)**.
- Alternatively, select the checkbox for **Two-Way Anti-Passback**.

Two-Way Anti-Passback:

- When personnel punch at a reader, the system checks whether a corresponding transaction exists for the opposite direction on another reader.

Additional Configurations

1. **Reset Time**:
    - Define a specific period for checking Anti-Passback rules when personnel punch at a reader.
2. **Active Time**:
    - Specify the validity period for the rule.
3. **Active Time Zone**:
    - Set the valid time zone for the rule, ensuring the Anti-Passback feature applies only within specified hours.

Special Notes on Reader and Controller Types

- **Reader Types**:
    - The door readers include:
        - **Wiegand readers** connected to access controllers.
        - **InBio readers**.
    - For single and two-door controllers with Wiegand readers, both "In" and "Out" readers are supported.
    - For four-door controllers, only **In Readers** are available.

Copyright © 2024 ARMATURA LLC. All rights reserved

- **Reader Numbers**:
  - Odd numbers (e.g., 1, 3) are for **In Readers**.
  - Even numbers (e.g., 2, 4) are for **Out Readers**.
  - Reader numbering corresponds to the RS485 address or device number.
- When configuring Anti-Passback between doors or readers, ensure that **In** and **Out Readers** align with your requirements. The configuration applies regardless of whether the reader is a **Wiegand reader** or **InBio reader**.

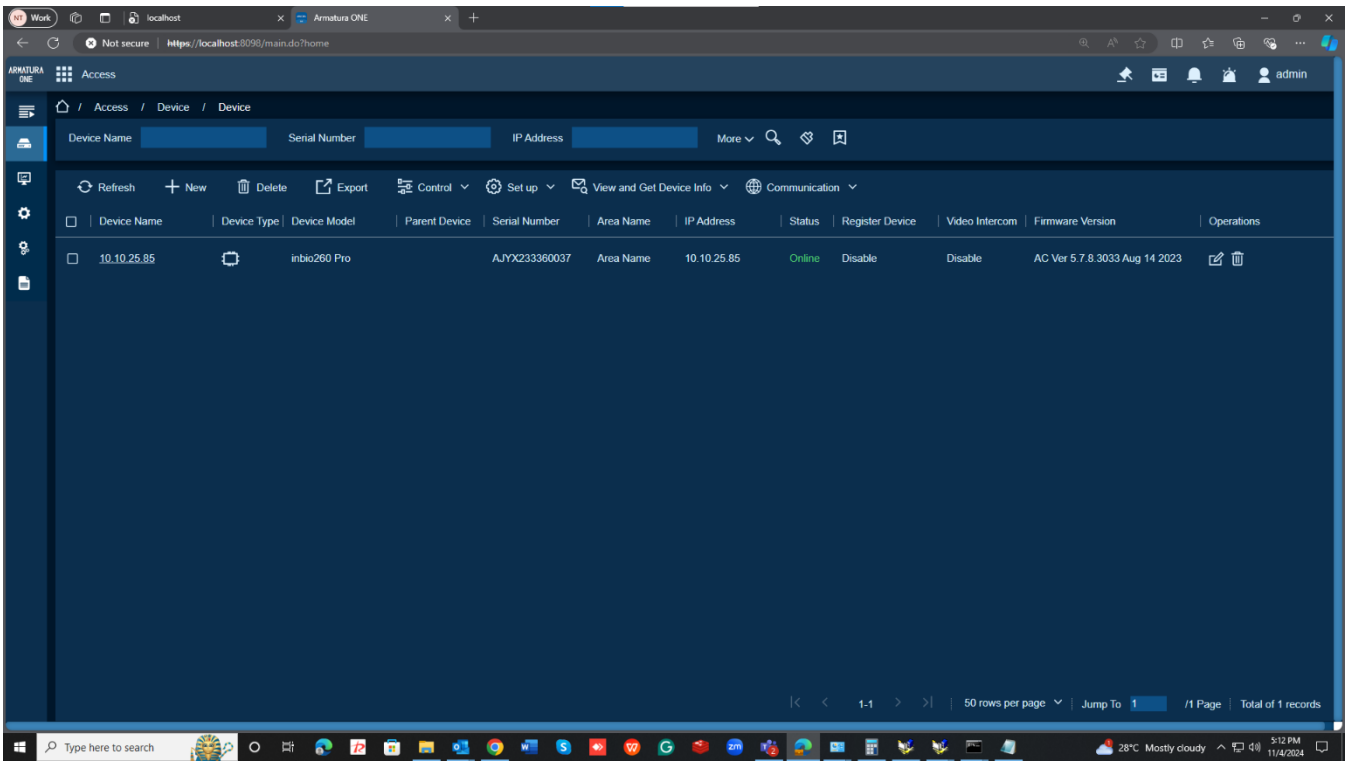
Steps

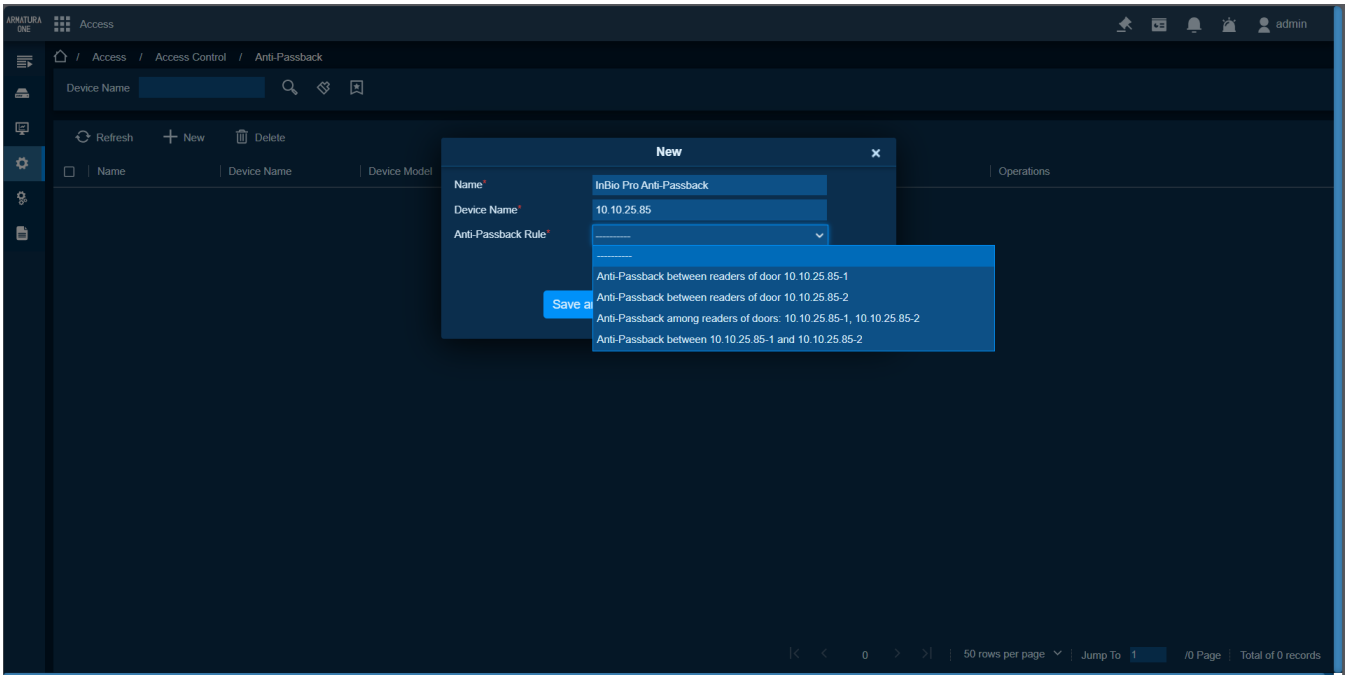
1. **Select Anti-Passback Rule**:
   - Navigate to **[Access Control] > [Anti-Passback]**.
   - Choose the desired rule (e.g., **Reader Anti-Passback**) and tick the checkbox.
2. **Complete Configuration**:
   - Click **[OK]** to finalize the setup.
   - The added Anti-Passback settings will appear in the configuration page.

Controller Compatibility

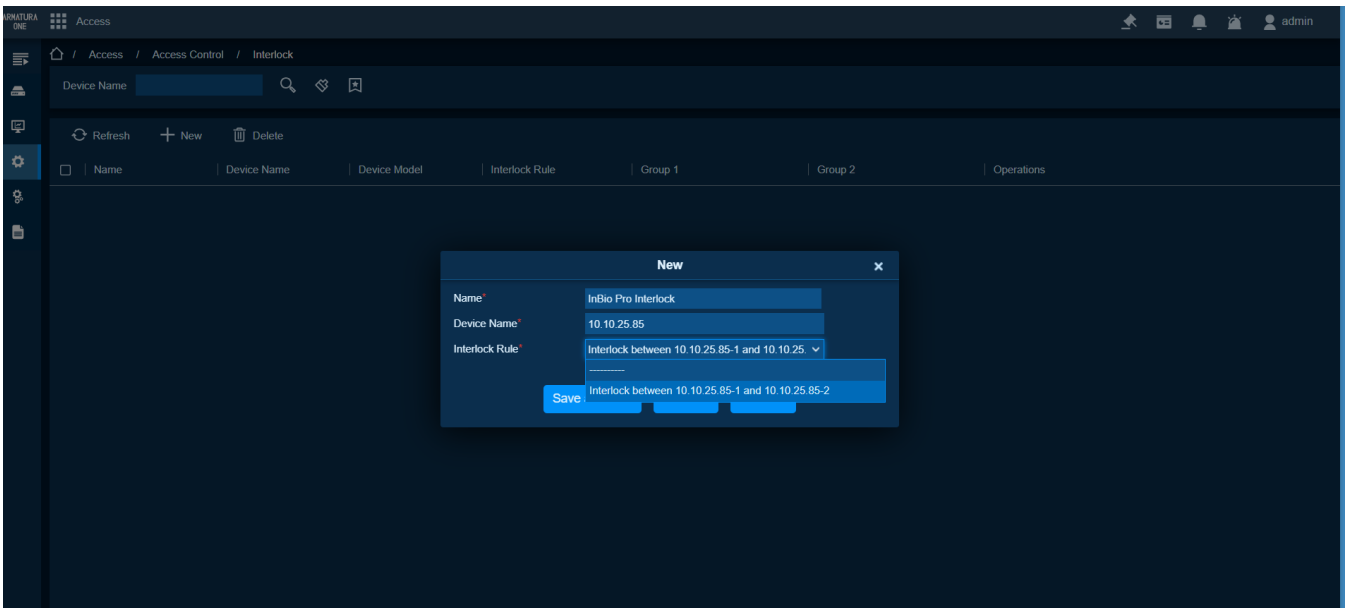
- The configuration page differs between:
  - **InBio Pro Controllers**.
  - **C3 Pro Controllers**.
  - **AHDU Controllers**.

Copyright © 2024 ARMATURA LLC. All rights reserved





Copyright © 2024 ARMATURA LLC. All rights reserved



Edit Anti-Passback

Prerequisites for Use

Log in to the system using a user account with the required menu authority.

Usage Scenarios

Anti-Passback settings may need adjustments in high-security environments to enhance entry and exit management of personnel.

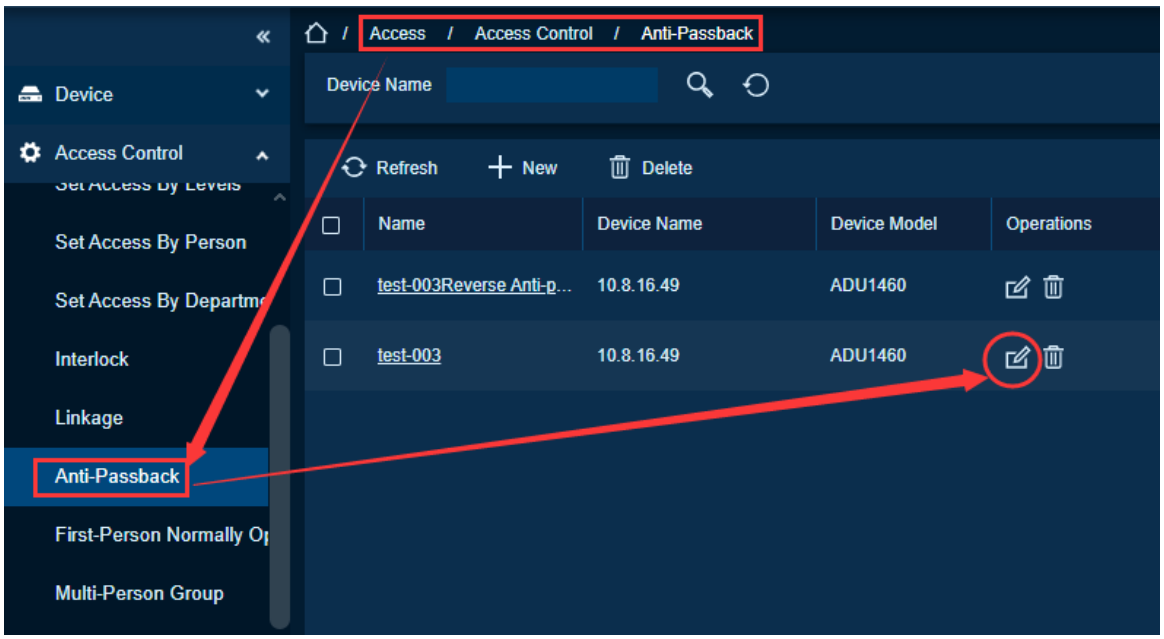
Trigger Result

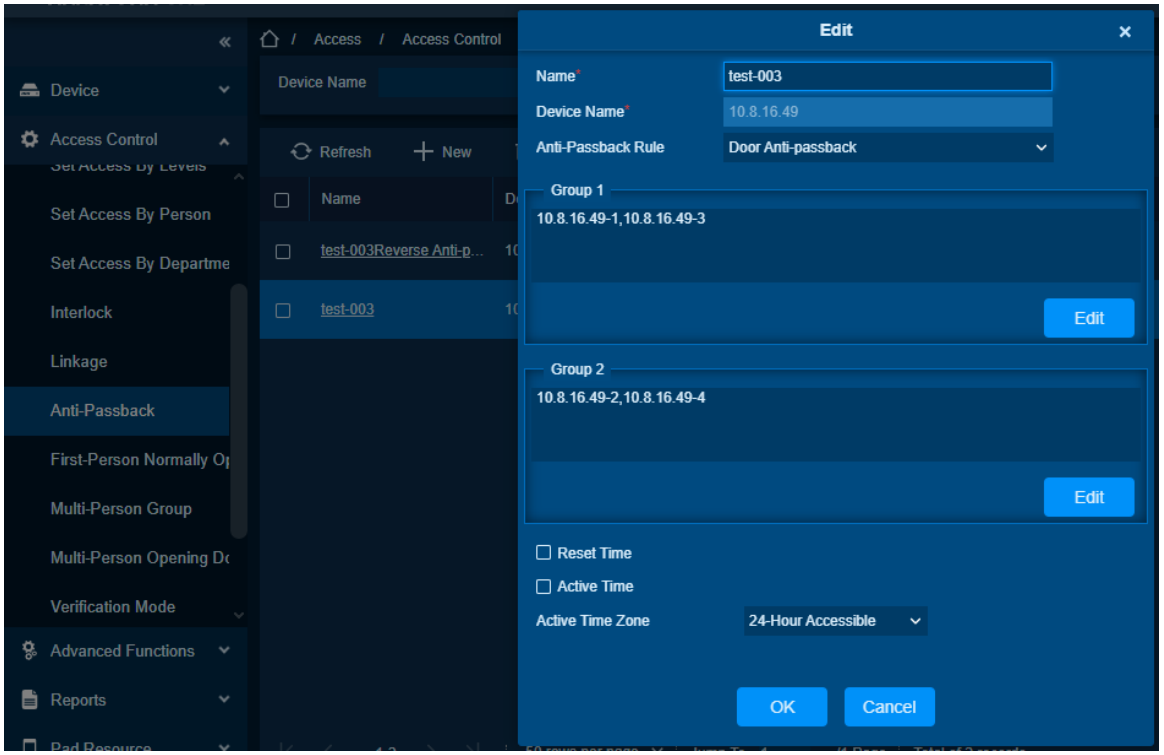
Modifies Anti-Passback rules to enforce updated entry and exit policies strictly.

Steps:

- Navigate to **[Access]** > **[Access Control]** > **[Anti-Passback]**.
- Identify the target device for which you wish to modify the Anti-Passback rules.
- Click the **[Edit]** button corresponding to the device.
- Make the necessary changes to the Anti-Passback settings, such as:
    - Modifying the group configurations.
    - Adjusting the reset time, active time, or active time zones.
    - Changing from One-Way to Two-Way Anti-Passback or vice versa.
- After editing, click **[OK]** to save the modifications.

Copyright © 2024 ARMATURA LLC. All rights reserved





Delete Anti-Passback

Prerequisites for Use

Log in to the system using a user account with the necessary menu authority.

Usage Scenarios

When the requirement for strict entry and exit control in a particular area is no longer necessary.

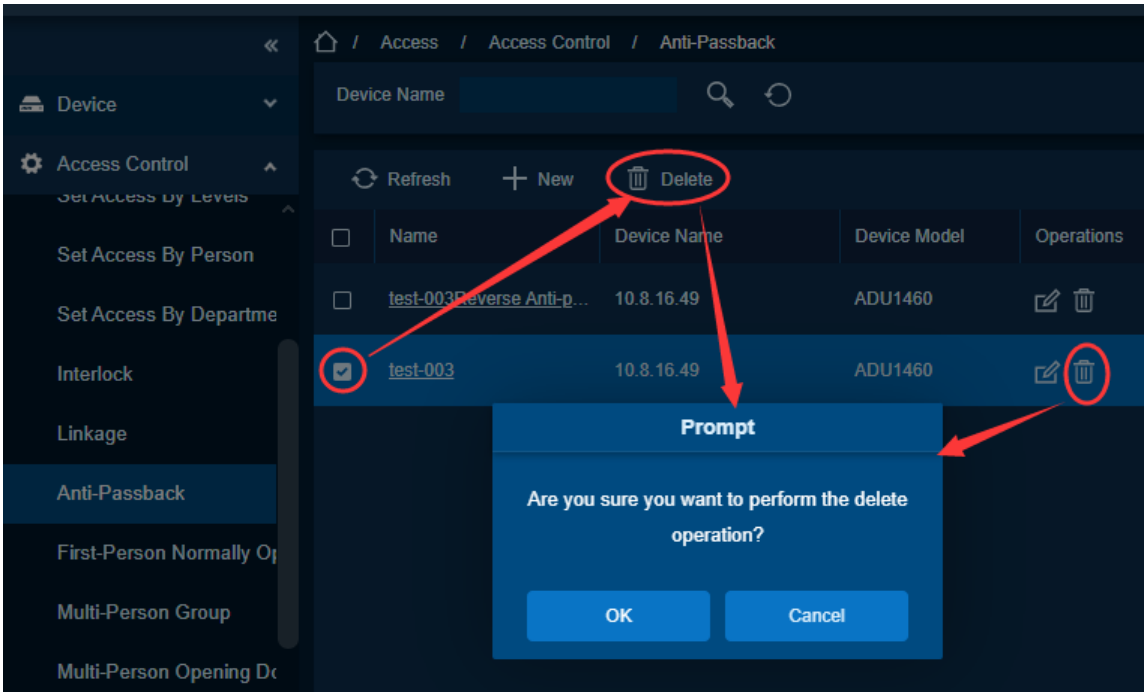
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Once the Anti-Passback rule has been removed, the system stops the rules for the selected device immediately.

Steps:

- Navigate to **[Access] > [Access Control] > [Anti-Passback]**.
- Identify the device for which the Anti-Passback rule needs to be deleted.
- Click the **[Delete]** button corresponding to the selected device's Anti-Passback rule.
- Confirm the action by clicking **[OK]** if prompted or cancelling if no longer required.



Result

The Anti-Passback rule is successfully deleted. The system no longer applies the Anti-Passback policy to the specified device.

6.3.10 First-Person Normally Open

Function Description

The **First-Person Normally Open** feature allows a door to remain in a normally open state during a specified interval after the first verification by a user with the First-Person Normally Open privilege. Once the interval expires, the door automatically returns to its closed state.

- **Configuration** **Options**:
  Users can configure First-Person Normally Open for specific doors, specifying the applicable doors, time zones, and users with this privilege. Multiple time zones can be set for a single door.

Copyright © 2024 ARMATURA LLC. All rights reserved

- **Display**:
  The interface for each door will display the count of existing First-Person Normally Open configurations.
- **Management**:
  Users can add or edit First-Person Normally Open settings by selecting doors and time zones. After adding, authorized personnel can also be assigned. Personnel management (browsing or deleting) is available within the interface.

Add First-Person Normally Open

Prerequisites for Use

Log in to the system with a valid account that has the required menu authority.

Usage Scenarios

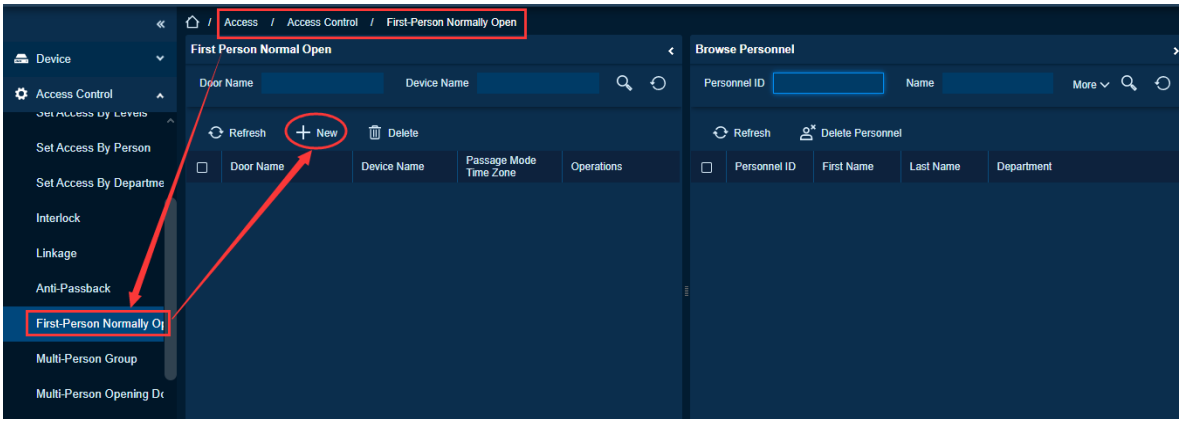
Doors need to remain open for a specific period in scenarios such as main entrance or public meeting rooms.

Trigger Result

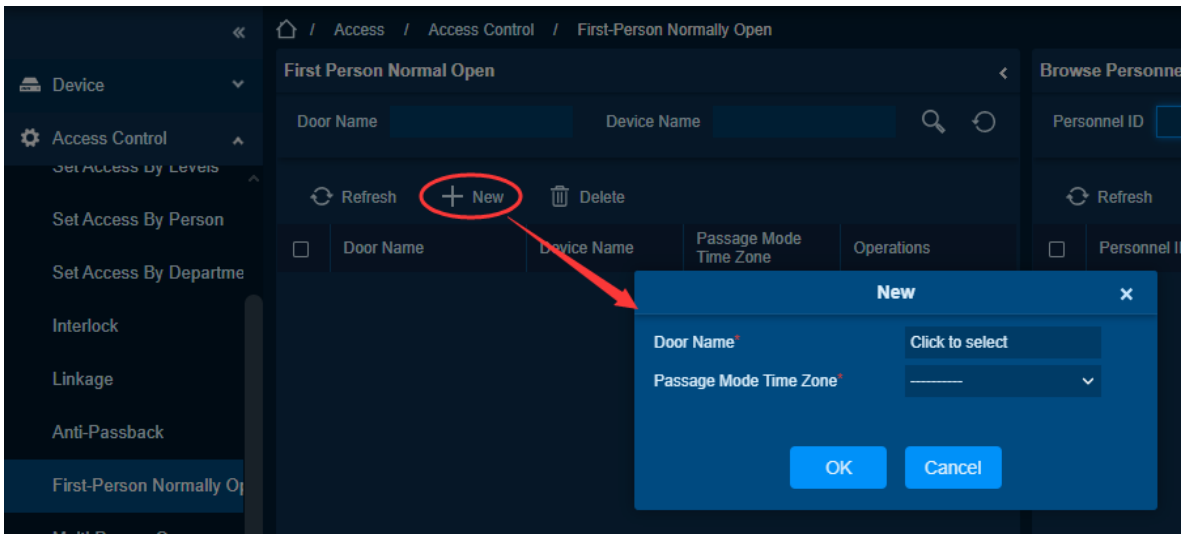
When a person with First-Person Normally Open privileges verifies their credentials, the door transitions to the **normally open** state for the defined duration.

Steps:

- Navigate to **[Access Control]** > **[First-Person Normally Open]** > **[New]**.
- Select the Door Name from the dropdown list.
- Specify the Passage Mode Time (the interval during which the door remains open).
- Click **[OK]** to save the settings.

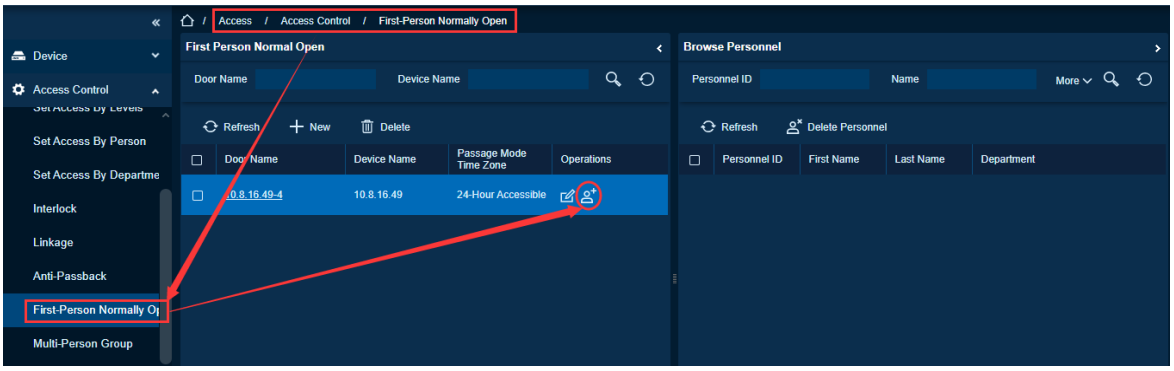


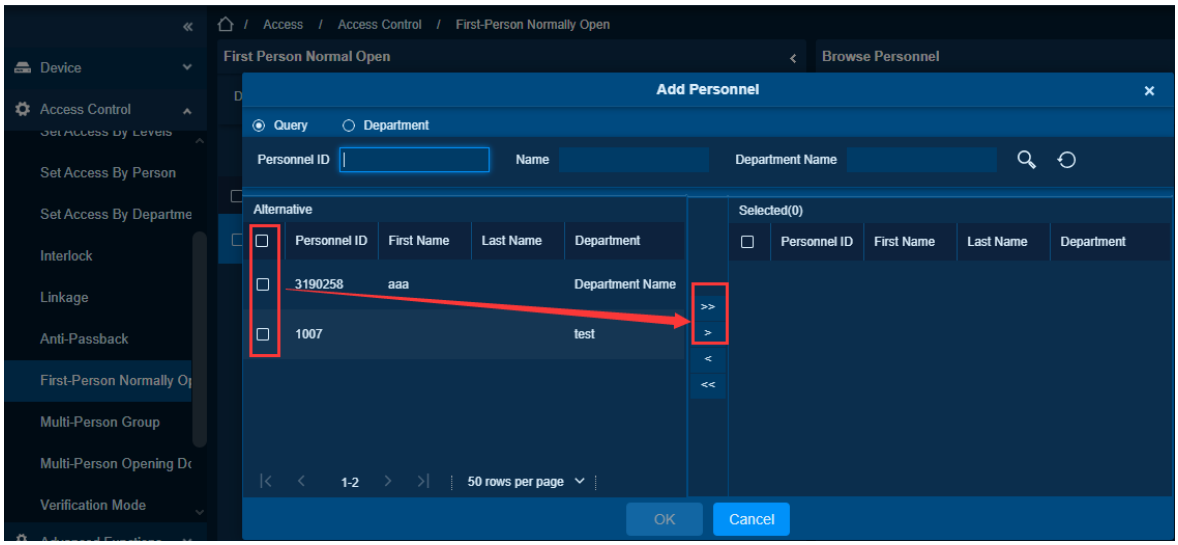
Copyright © 2024 ARMATURA LLC. All rights reserved



Add Authorized Personnel:

- Click **[Add Personnel]** under **Related Operation**.
- Choose the personnel who should have the **First-Person Normally Open** privilege (these personnel must already have an associated access control level).
- Click **[OK]** to save the selection.

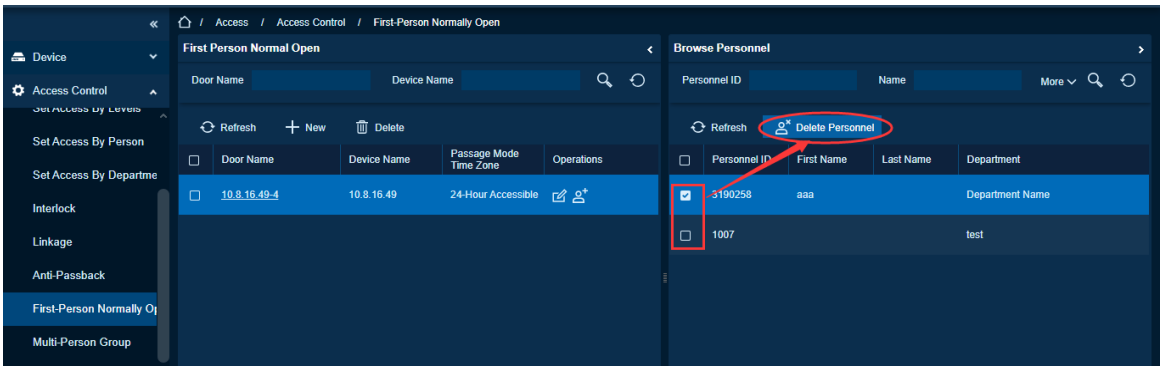


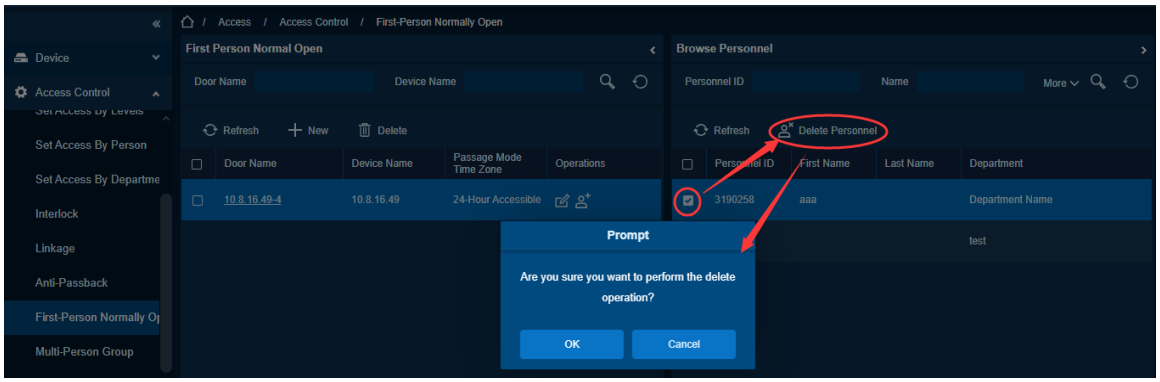


Copyright © 2024 ARMATURA LLC. All rights reserved

Manage Personnel:

- To remove personnel from the **First-Person Normally Open** privilege:
  - Select the door associated with the setting.
  - Choose the person to be removed from the list on the right.
  - Click **[Delete Person]** to delete the selected individual.





Edit First-Person Normally Open

Prerequisites for Use

Log in with a valid account that has the required menu authority.

Usage Scenarios

Modify the time during which the door remains open under the First-Person Normally Open settings.

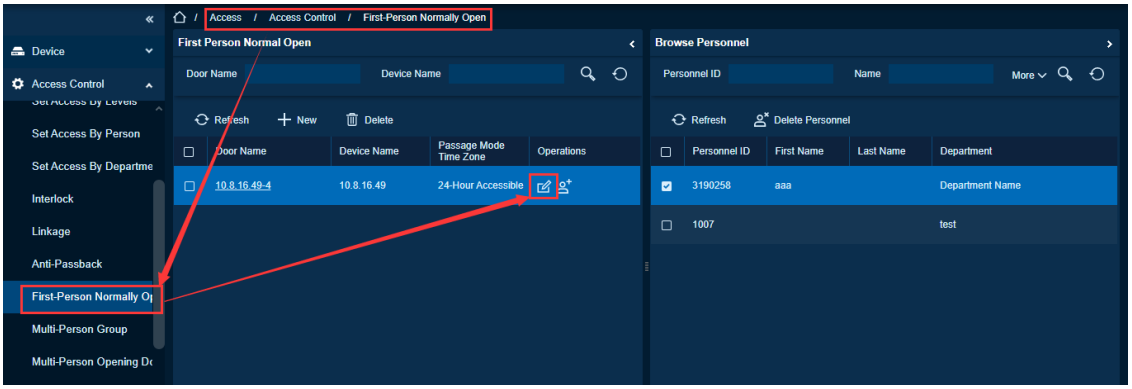
Trigger Result

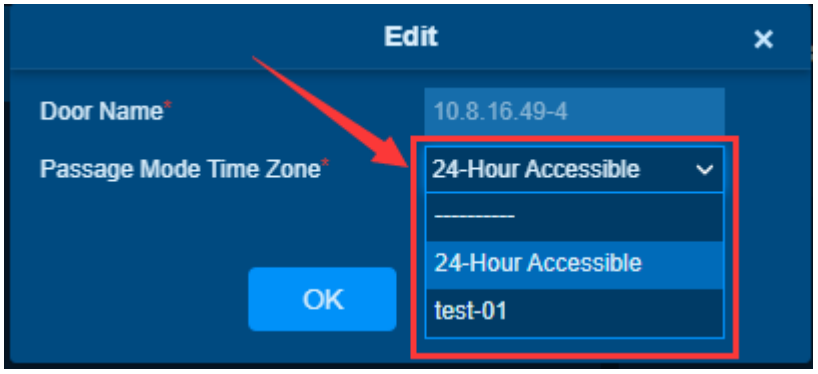
After a person with First-Person Normally Open authority opens the door, the updated time settings will dictate how long the door remains normally open.

Steps:

- Navigate to **[Access] > [Access Control] > [First-Person Normally Open]**.
- In the interface, select the door for which the First-Person Normally Open is configured.
- Click **[Edit]** to adjust the time settings for the Passage Mode.
- **Save Changes**: Make the necessary modifications and click **[OK]** to save.

Copyright © 2024 ARMATURA LLC. All rights reserved





Delete First-Person Normally Open

Prerequisites for Use

Log in with a valid account that has the required menu authority.

Usage Scenarios

The First-Person Normally Open setting is no longer needed for the door.

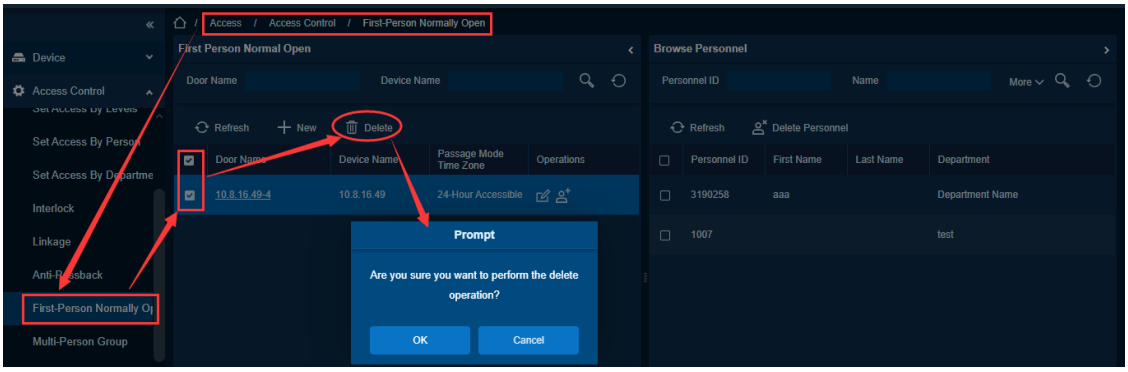
Trigger Result

The function to keep the door open after the first person's access is removed.

Steps:

- Navigate to **[Access]** > **[Access Control]** > **[First-Person Normally Open]**.
- Select the door for which the First-Person Normally Open setting should be removed.
- Click **[Delete]** to delete the configuration.
- Confirm the action in the prompt to finalize the removal of the settings.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.3.11 Multi-Person Group

Function Description

The door opens only after successful consecutive verifications by multiple persons belonging to a specific Multi-Person Group. If a non-member of the group attempts verification, the process is interrupted.

Add Multi-Person Group

Prerequisites for Use

Log in with the current account and ensure the appropriate menu authority.

Usage Scenarios

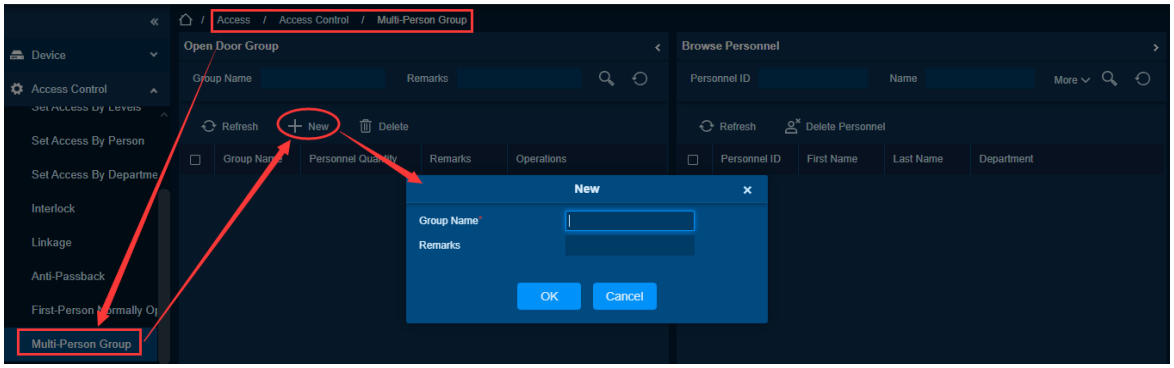
Required in situations where a door can only be accessed when multiple authorized personnel are present and verified consecutively.

Trigger Result

The door will open after successful verification by all members of the Multi-Person Group.

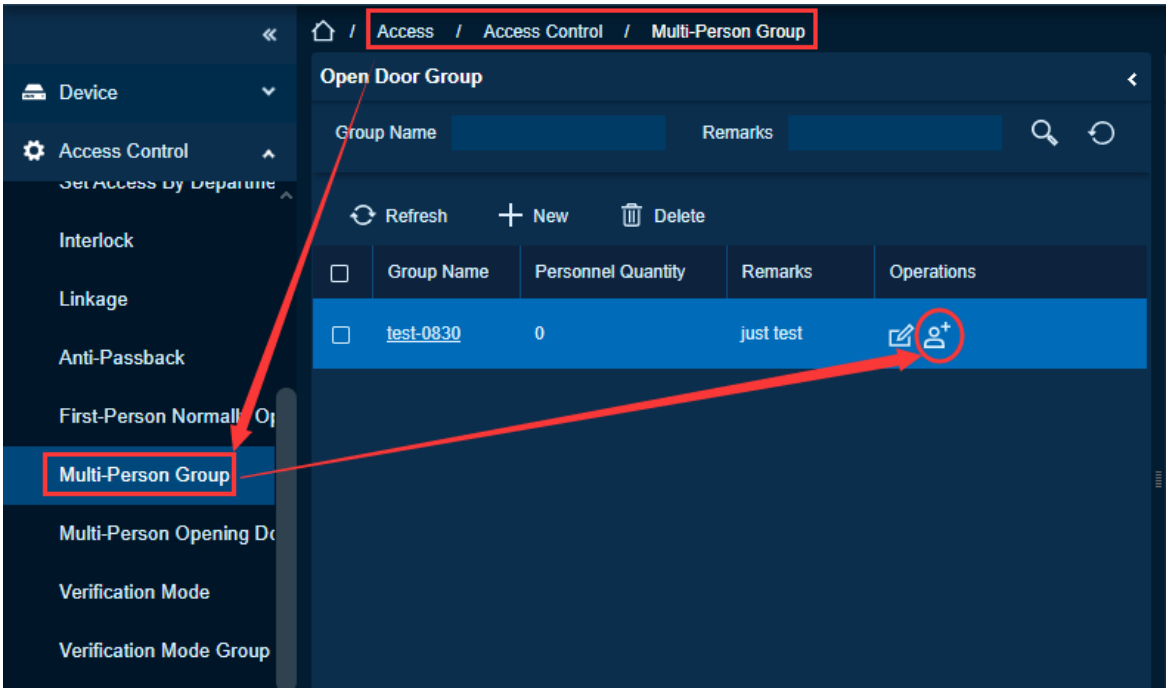
Steps:

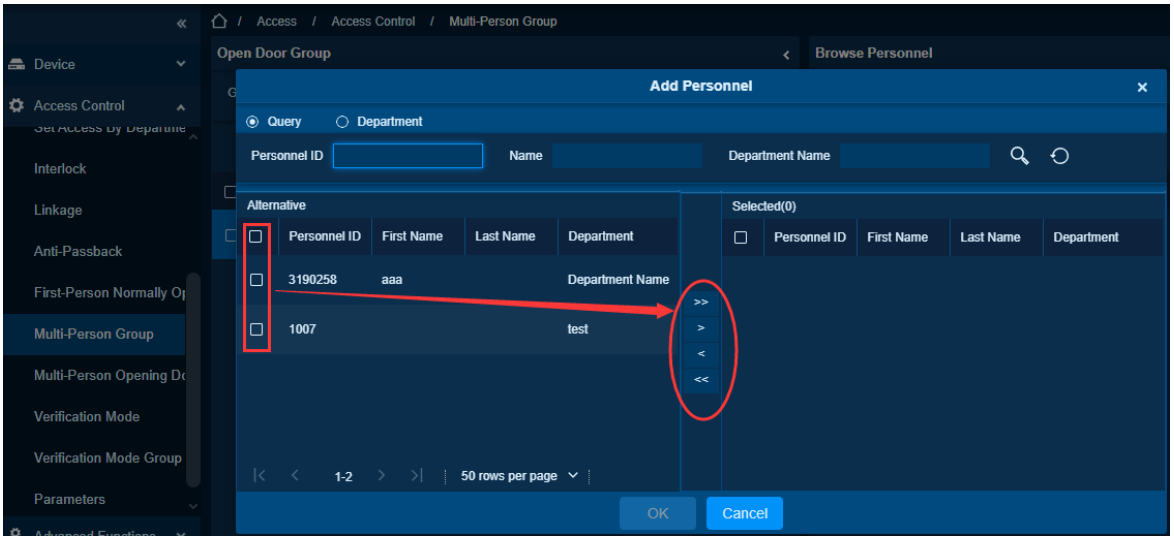
- Go to **[Access Control]** > **[Multi-Person Group]** > **[New]** to open the edit interface.



Copyright © 2024 ARMATURA LLC. All rights reserved

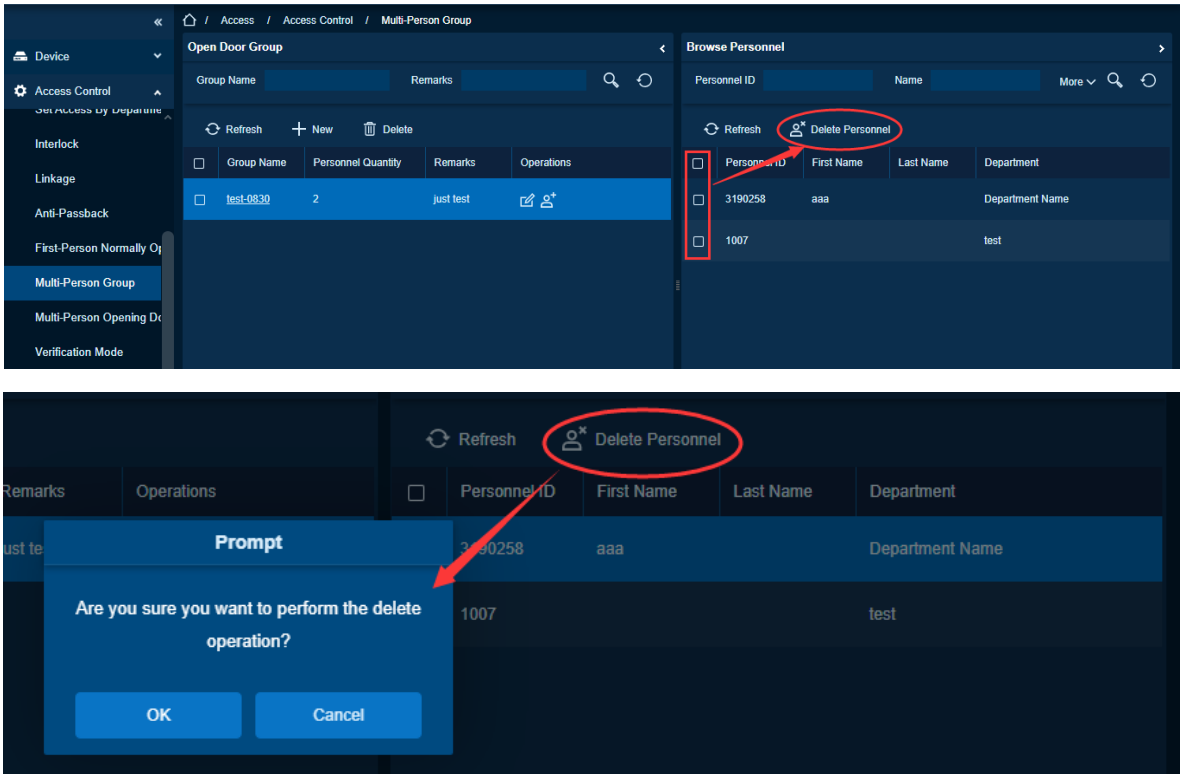
- Group Name: Enter a unique name for the group, up to 30 characters.
- Click **[OK]** to save. The newly created Multi-Person Group will be displayed in the list.
- Click **[Add Personnel]** under Related Operations.
- Select personnel from the available list and add them to the group.
- Click **[OK]** to save and return.





- To remove a member, select the personnel from the group list and click **[Delete Personnel]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Note:

Each person can belong to only one **Multi-Person Group**.

Ensure that personnel added to the group already have access levels configured.

Edit Multi-Person Group

Prerequisites for Use

Log in with the current account and ensure menu authority is enabled.

Usage Scenarios

Modify the name or remarks for an existing multi-person group.

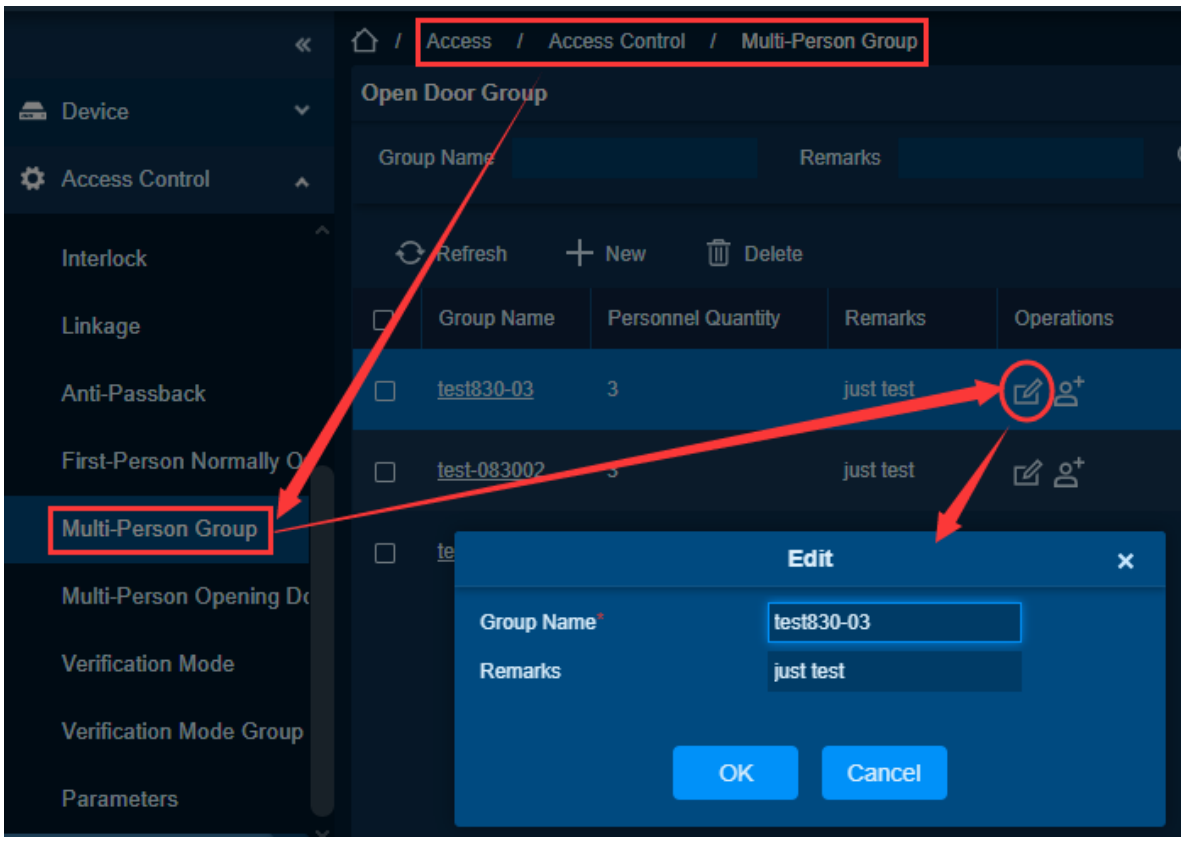
Trigger Result

Updates the multi-person group with the new group name and/or remarks.

Steps:

- Go to **[Access] > [Access Control] > [Multi-Person Group]** to access the list of groups.
- Select the desired group and click **[Edit]**.
- Update the group name or remarks as required.
- After editing, click **[OK]** to save the modifications.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Multi-Person Group

Prerequisites for Use

Log in with the current account and ensure menu authority is enabled.

Usage Scenarios

The requirement for multi-person verification to open a door is no longer needed.

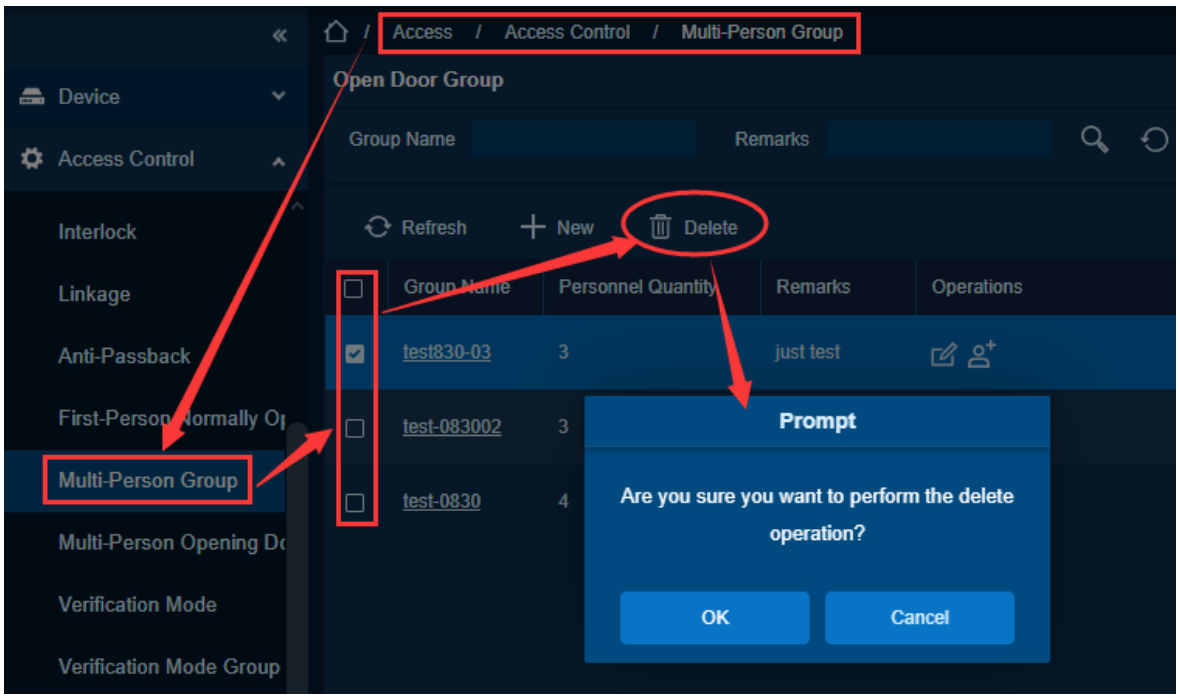
Trigger Result

Deletes the specified multi-person group.

Steps:

- Go to **[Access] > [Access Control] > [Multi-Person Group]** to access the list of groups.
- Select the group to be removed and click **[Delete]**.
- Click **[OK]** to confirm and permanently delete the group.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.3.12 Multi-Person Opening Door

Function Description

The **Multi-Person Opening Door** feature allows setting permissions for personnel within one or more **Multi-Person Groups** to collectively open a door. This can involve single or multiple groups, and the configuration ensures that a defined number of people from the group(s) must verify within a specific time interval to successfully open the door.

Add Multiple People Opening Door Rule

Prerequisites for Use

Log in with the current account and ensure menu authority is enabled.

At least one **Multi-Person Group** must already be configured.

Usage Scenarios

Situations requiring doors to be opened only when a specific number of authorized individuals verify their credentials simultaneously.

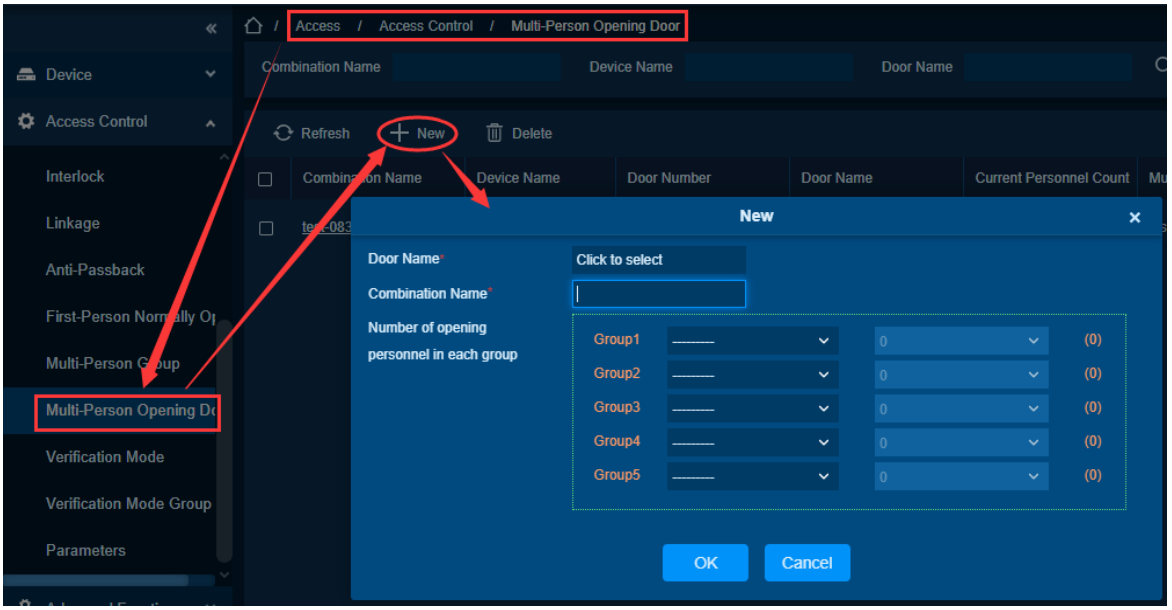
Trigger Result

Assigns permissions for personnel within **Multi-Person Groups**, enabling them to collectively open doors.

Steps:

- Go to **[Access]** > **[Access Control]** > **[Multi-Person Opening Door]** > **[New]**.
- Configure the number of people required for door opening from each group.

Copyright © 2024 ARMATURA LLC. All rights reserved



- The maximum total across all groups cannot exceed 5 people.
- Numbers in brackets next to each group indicate the actual number of members currently in that group.
- By default, the Credit Card Interval is set to 10 seconds. This means that the verification interval between personnel must not exceed 10 seconds.
- Modify the interval if supported by the device.
- Click **[OK]** to finalize and save the Multi-Person Opening Door rule.

Note:

At least one group must have a non-zero number of door-opening personnel configured.

If the total number of people set for door opening exceeds the current actual members of the group, the **Multi-Person Opening Door** function will be disabled.

Ensure that the device supports modification of the **Credit Card Interval** if changes are required.

Edit Multi-Person Opening Door Rule

Prerequisites for Use

Log into the system with an account that has the required authority and ensure at least one Multi-Person Group exists in the system.

Usage Scenarios

Configure existing Multi-Person Opening Door rules to modify rule names or adjust door assignments within the rule.

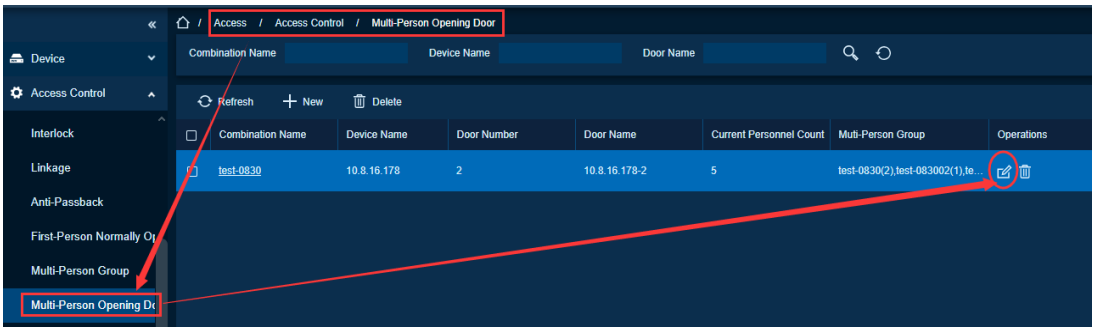
Copyright © 2024 ARMATURA LLC. All rights reserved

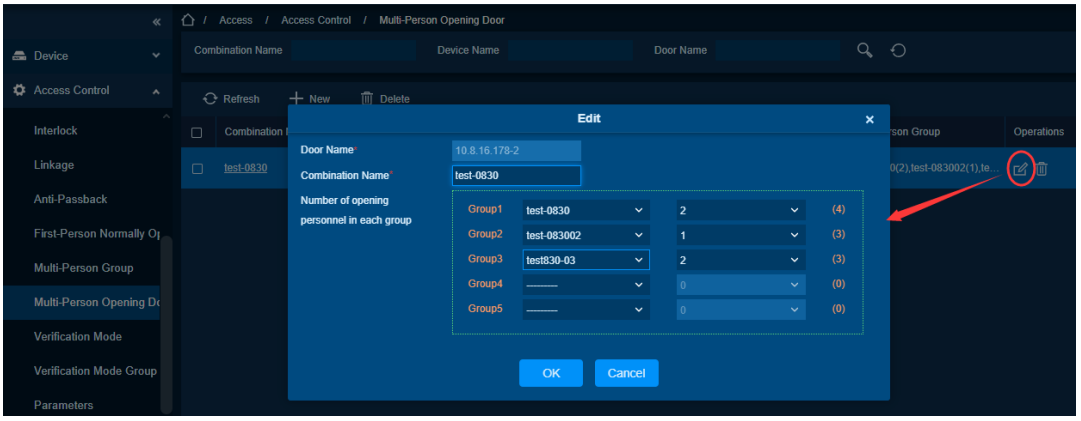
Trigger Result

Personnel within the Multi-Person Group must collectively authenticate at newly assigned doors according to the updated configuration.

Steps:

- Go to **[Access] > [Access Control] > [Multi-Person Opening Door]** to display the current rules.
- Choose the desired door associated with the rule.
- click **[Edit]** to modify the Multi-Person Opening Door rule。
- After completing the modifications, click **[OK]** to save the updated configuration.





Delete Multi-Person Opening Door Rule

Prerequisites for Use

The system requires both a valid login with menu authority and at least one existing Multi-Person Group.

Usage Scenarios

This function is used when the Multi-Person Opening Door rules are no longer needed for specific devices or personnel groups.

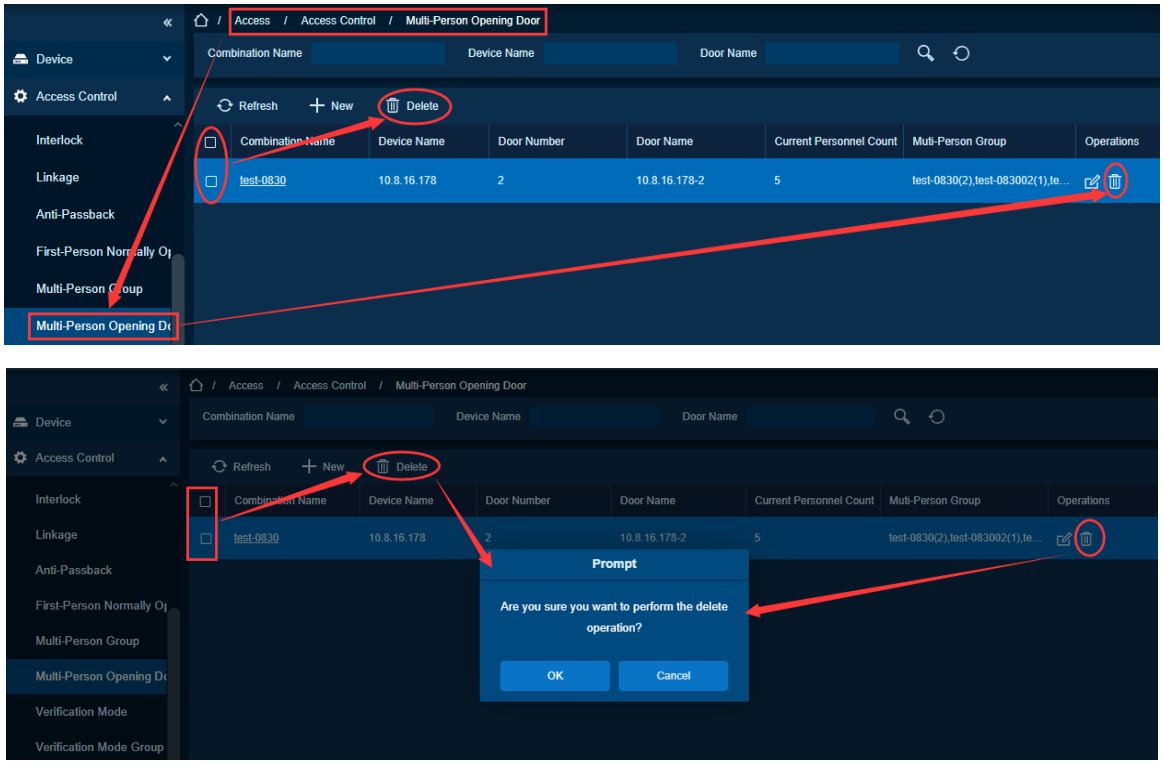
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Upon completion, the multi-person verification requirement is removed from designated doors, allowing standard single-person authentication.

Steps:

- Go to **[Access]** > **[Access Control]** > **[Multi-Person Opening Door]** to view the existing rules.
- Choose the rule associated with the specific door.
- Click **[Delete]** to remove the Multi-Person Opening Door rule.
- Confirm the deletion by clicking **[OK]**. The rule will be permanently removed.



6.3.13 Verification Mode

Function Description

The **Verification Mode** allows configuration of specific verification methods for doors or individuals during specified time periods. This is useful for scenarios requiring varying security levels depending on time or personnel.

New Verification Mode

Prerequisites for Use

The system requires a valid login with menu authority.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

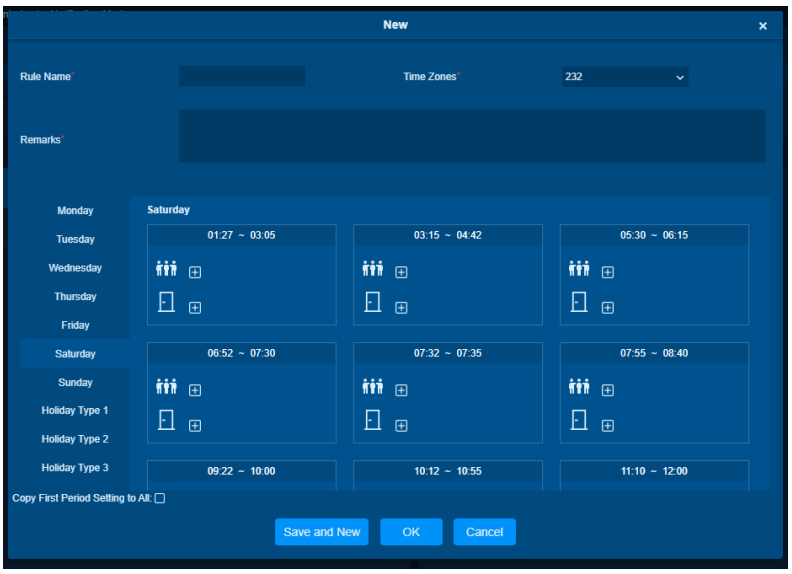
At the lobby entrance barrier, employees use card verification during business hours (08:00-18:00) and enhanced card plus fingerprint verification during off-hours (00:00-07:59, 18:01-23:59). For specific roles like security guards, face verification may be required continuously throughout the day.

Trigger Results

The system enforces configured verification methods for designated personnel and access points according to defined time schedules.

Steps:

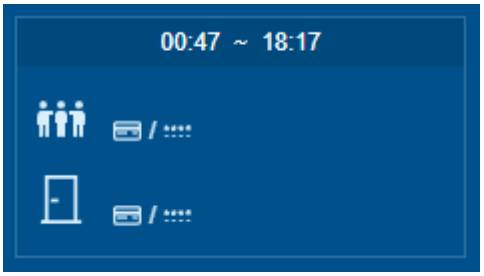
- Go to **[Access Control] > [Verification Mode] > [New]** to open the page for creating a verification mode rule.



Rule Name: Enter a name that clearly identifies the rule (e.g., "Lobby Entrance Verification").

Time Zones: Select time zones from **[Access] > [Access Control] > [Time Zones]**.

Verification Mode Settings: Define the verification method for each day of the week (Monday to Sunday).



Personnel Verification: Assign specific verification methods for individual personnel.

Door Verification: Assign verification methods for specific doors.

Copyright © 2024 ARMATURA LLC. All rights reserved

If a person is assigned to **Personnel Verification**, they will follow this setting first—even if it differs from **Door Verification** or **Reader Parameter** settings.

If a person is not assigned to **Personnel Verification**, they will follow the **Reader Verification** rules.

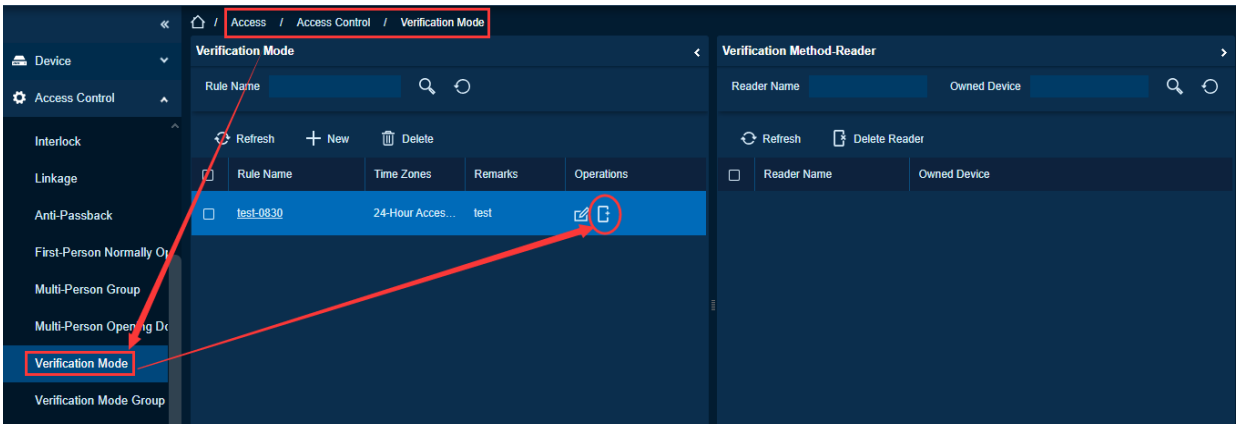
Click **[OK]** to save the verification mode.

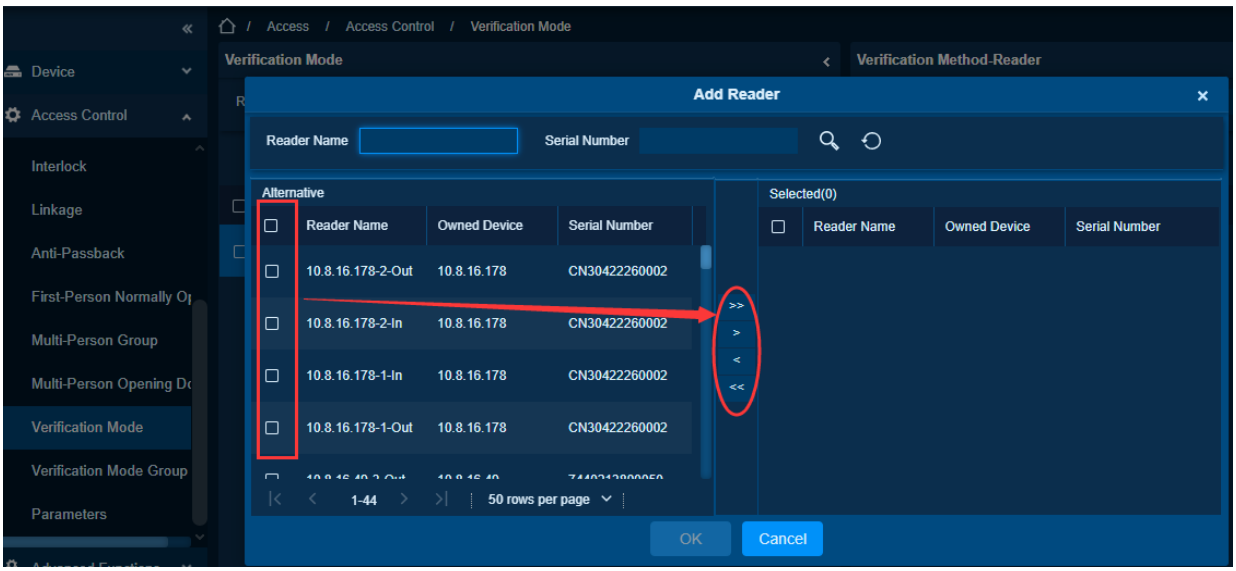
On the list page, you can **add or delete doors** to include them in the verification mode rule.

Add Reader

Steps to Add a Reader:

- Navigate to **[Access Control] > [Verification Mode]** to access the verification mode interface.
- Click **[Add Reader]** under the operations column.
- On the left side, select the reader's name and click the arrow >> to move it to the right side.
- Click **[OK]** to save the configuration.





Delete Reader

Copyright © 2024 ARMATURA LLC. All rights reserved

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

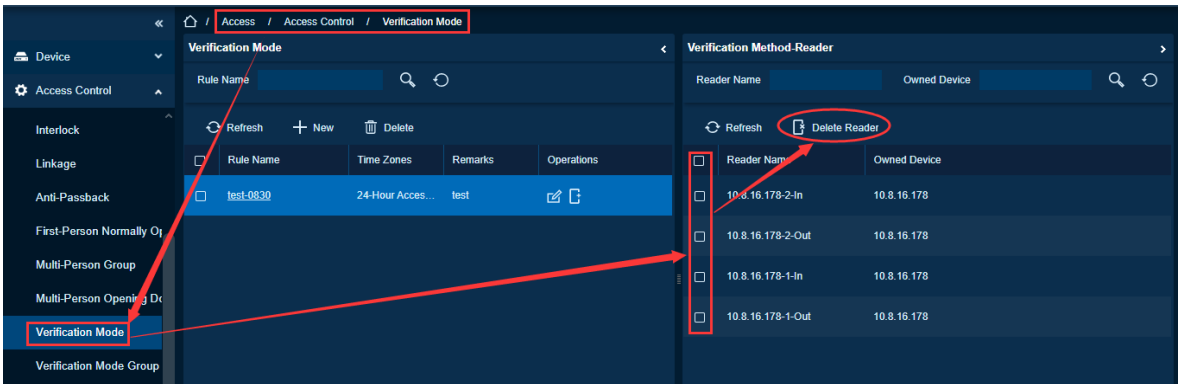
The system no longer requires verification through multiple readers for door access.

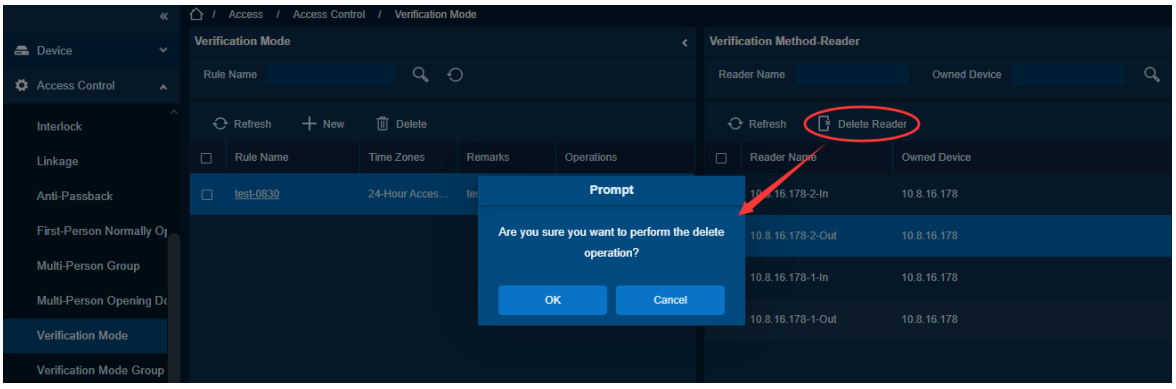
Trigger Result

Removes the selected reader from the list, disabling it from participating in the verification process.

Steps:

- Navigate to **[Access Control] > [Verification Mode]** to access the verification mode interface.
- Select the reader you wish to remove and click **[Delete]**.
- Confirm the deletion.





Note:

If a rule includes a verification mode for personnel, **RS485 readers** cannot be selected when adding doors.

Changes to the reader configuration must be made on the reader settings page **before** adding doors.

Edit Verification Mode

Prerequisites for Use

Log into the system with an account that has the required authority.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

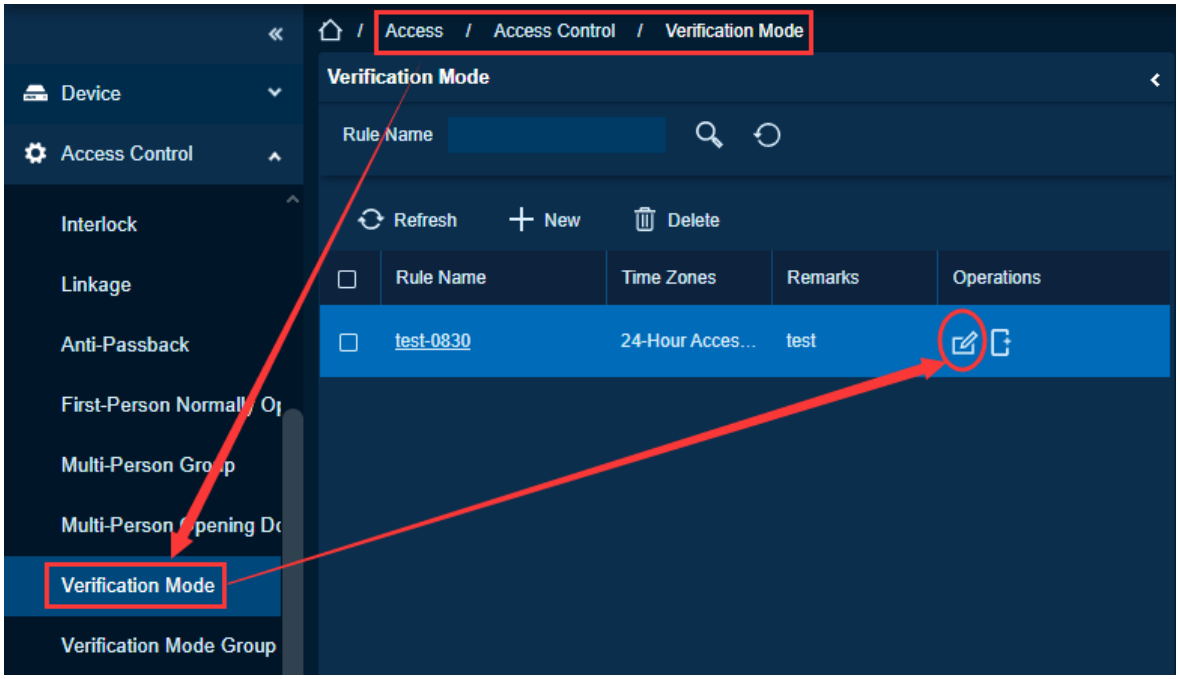
To modify the verification method or the time for verification on doors in batches.

Trigger Result

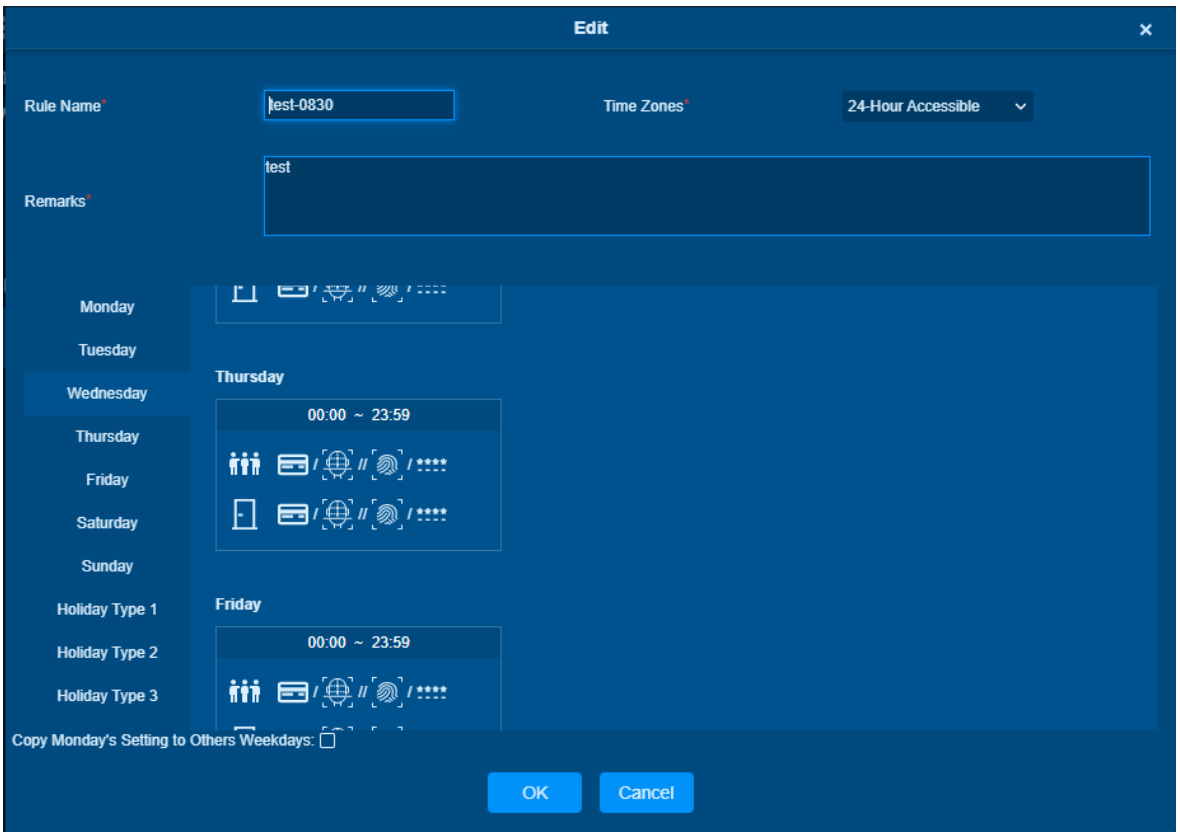
Allows verification using the updated verification methods and time settings.

Steps:

- Navigate to **[Access]** > **[Access Control]** > **[Verification Mode]** to access the interface.
- Select the rule name you wish to edit.
- Click **[Edit]** and modify the verification mode settings.
- Save the updated configuration.



Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Verification Mode

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

When a specific verification mode is no longer required.

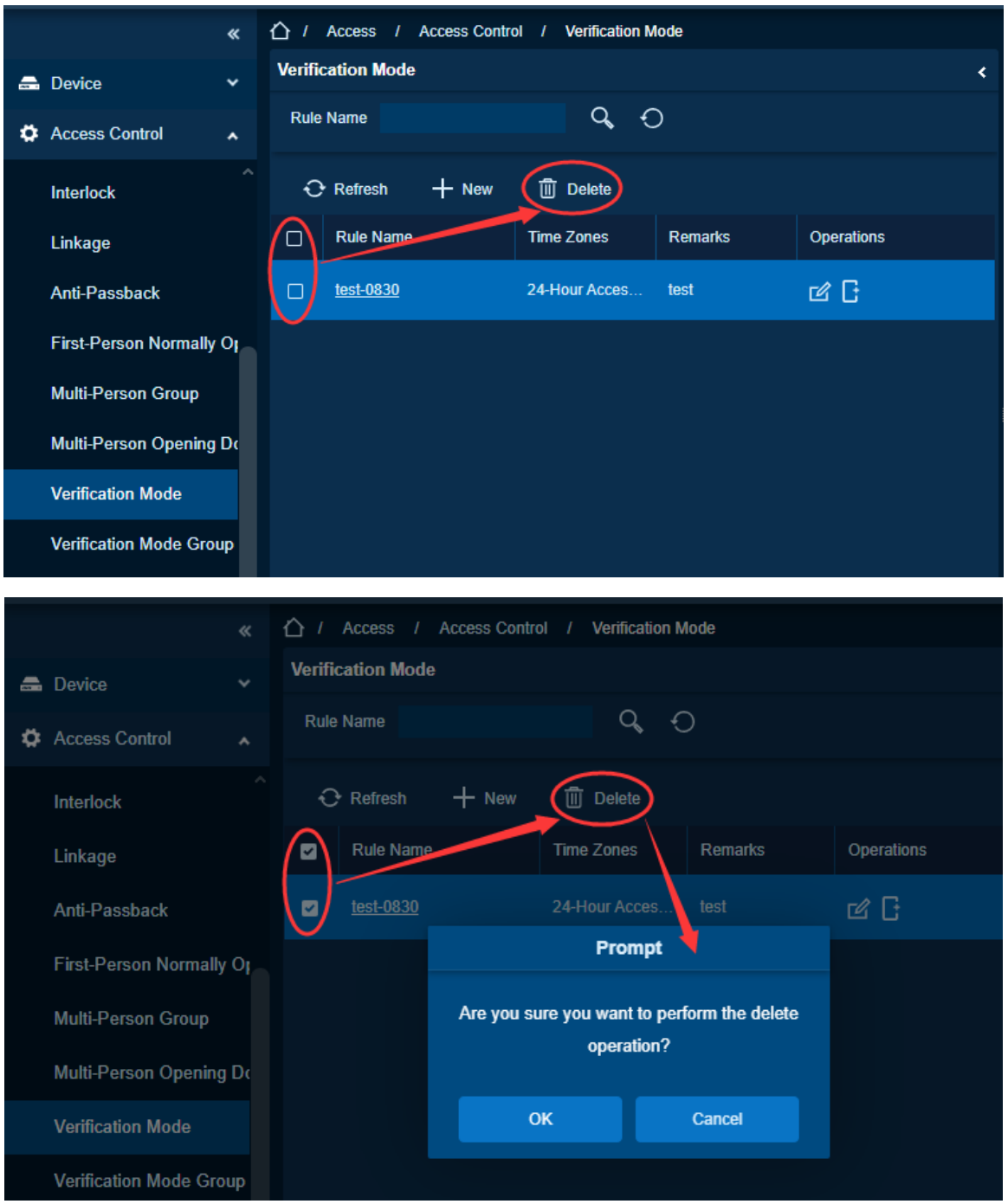
Trigger Result

Disables verification via the deleted verification method and time.

Steps:

- Navigate to **[Access]** > **[Access Control]** > **[Verification Mode]** to access the interface.
- Select the rule name for the verification mode you wish to delete.
- Click **[Delete]** and confirm to remove the rule.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.3.14 Verification Mode Group

Function Description

The Verification Mode Group allows assigning personnel to predefined verification mode rules. This ensures that individuals can verify access at specific doors according to the assigned verification methods and schedules.

Add Personnel

Prerequisites for Use

Copyright © 2024 ARMATURA LLC. All rights reserved

Log into the system with an account that has the required authority.

Usage Scenarios

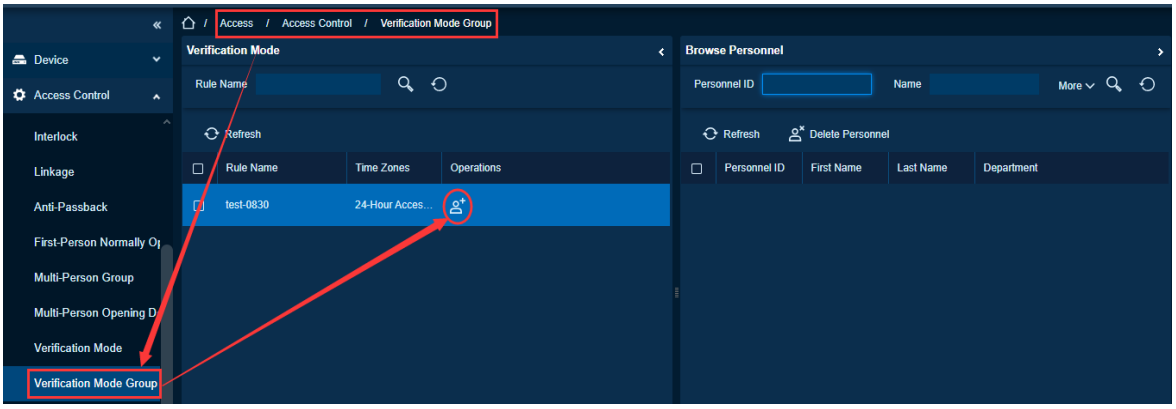
Adding personnel in batches to enable verification using specific methods and times for designated doors.

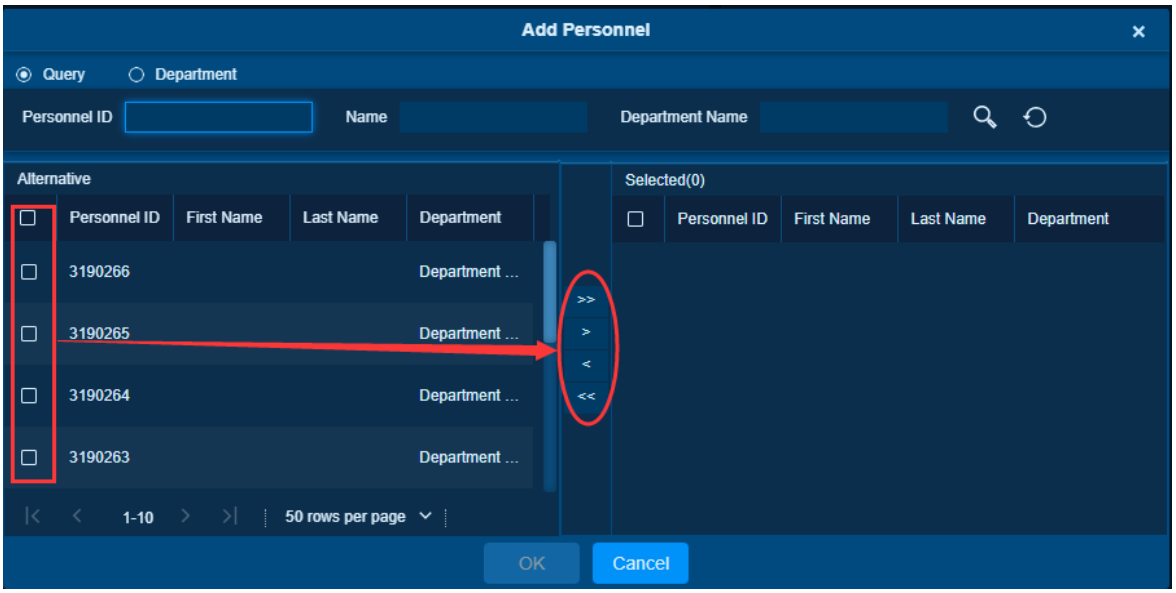
Trigger Result

Personnel added to the Verification Mode Group can use the defined verification method during the assigned time.

Steps:

- Navigate to **[Access] > [Access Control] > [Verification Mode Group]**.
- Select the rule name from the list.
- Click **[Add Person]** to open the personnel selection interface.
- Choose personnel to add to the group and click **[OK]** to save.





Delete Personnel

Copyright © 2024 ARMATURA LLC. All rights reserved

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

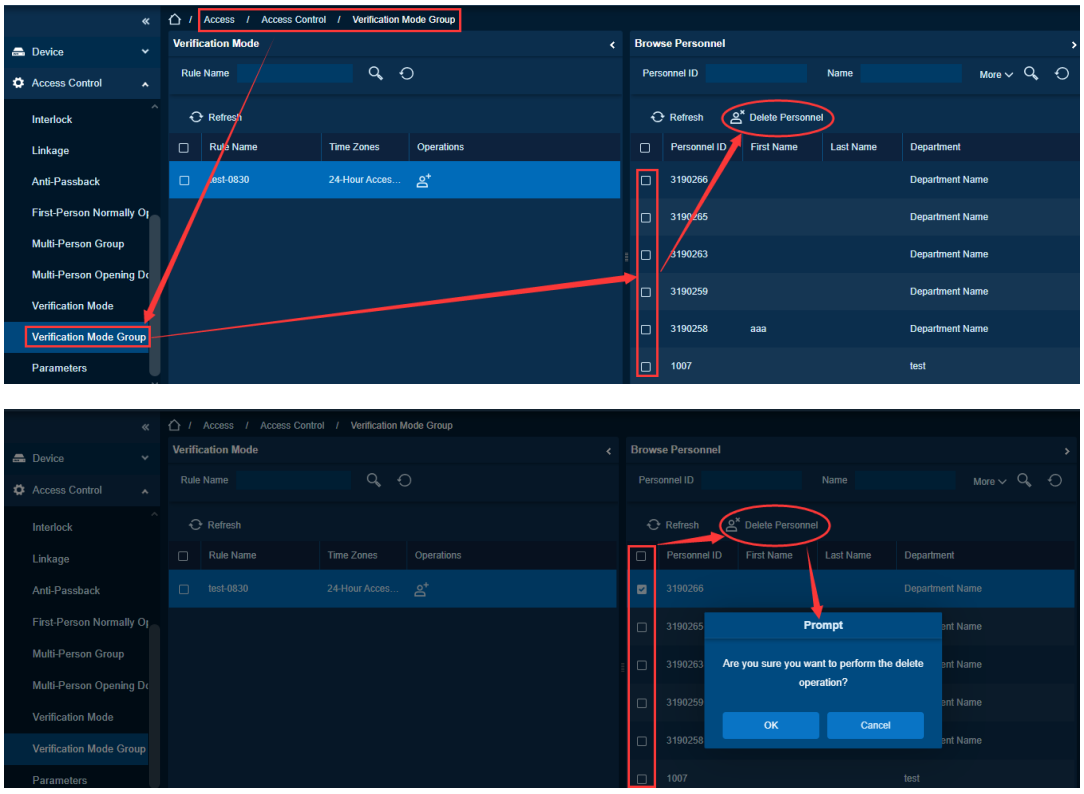
Removing personnel who no longer need to verify access based on the corresponding verification mode rules.

Trigger Result

Personnel removed from the group will no longer be able to verify using the specific verification method or schedule.

Steps:

- Navigate to **[Access] > [Access Control] > [Verification Mode Group]**.
- Select the rule name from the list.
- Click **[Delete Personnel]** to open the personnel management interface.
- Select the personnel to remove and click **[OK]** to confirm the deletion.



6.3.15 Parameters

Function Description

The **Parameters** section allows users to configure key access control settings, including event record management, real-time monitoring preferences, and automated data export rules. These settings ensure that access control operations are tailored to the system's requirements and enhance usability.

Copyright © 2024 ARMATURA LLC. All rights reserved

Parameter Settings

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

Adjusting the method for obtaining event records.

Configuring automatic export of transaction records.

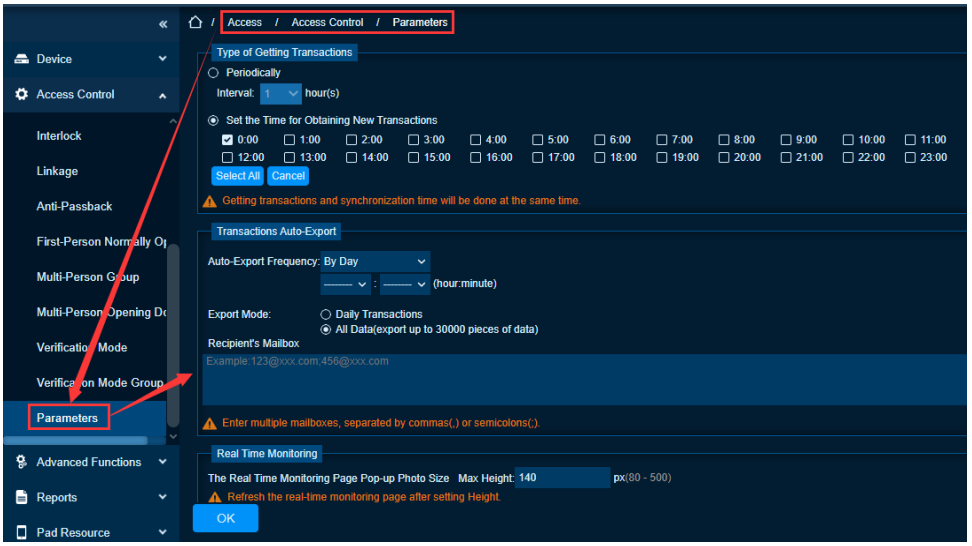
Setting real-time monitoring features, including photo pop-ups and email notifications.

Trigger Results

Access control operates based on the configured rules, allowing flexibility in data handling, monitoring, and system interactions.

Steps:

- Navigate to **[Access Control]** > **[Parameters]** to access the parameter settings interface.



Type of Getting Transactions

Periodically: The system downloads new transaction records at user-defined intervals, which can be configured through the Set Interval option.

By Time: The system downloads new transaction records at a specified time each day, configurable through the Set Time option.

Copyright © 2024 ARMATURA LLC. All rights reserved

Transaction Auto-Export: Export settings can be configured for daily or monthly schedules. Daily exports occur at a specified time and can include either daily transactions or complete system data up to 30,000 records. Monthly exports occur on a designated day and can include monthly transactions or complete system data. Recipients receive exports via their configured email addresses.

The Real Time Monitoring Page Pop-up Staff Photo Size: When access events occur, the system displays personnel photos in pop-up windows. Photo dimensions can be adjusted between 80 and 500 pixels for optimal visibility.

Alarm Monitoring Recipient Mailbox: Configure an email address to receive alerts from the system in case of an alarm or event.

Compare Photo Delivery Settings: Enable the system to send comparison photos to the device for local storage.

Deliver Permission Thread Pool Settings: Configure background processing parameters for multi-threaded access permission verification.

Transactions Auto-Export

Function Description

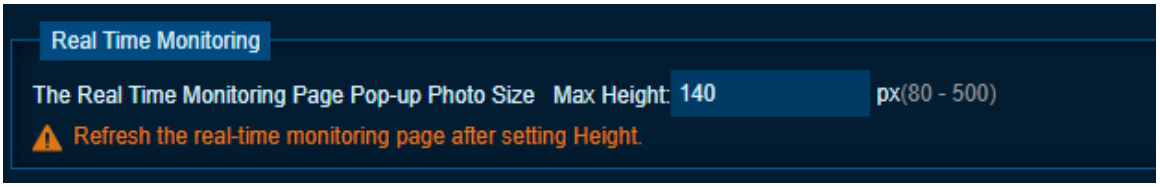
This feature automates the export of transaction data based on predefined schedules and data types. It supports both daily and monthly export options, allowing users to streamline reporting and data analysis.

Configuration:

Export Frequency: The daily option allows specification of export times for either daily transactions or complete system data, with system data exports limited to 30,000 records per batch. The Monthly option enables exports on a specified day each month, offering either monthly transaction data or comprehensive system records.

Recipient Email Configuration: Configure recipient email addresses for automated delivery of exported data files.

Real Time Monitoring



Copyright © 2024 ARMATURA LLC. All rights reserved

During access control events, the system displays a personnel photo pop-up window. Users can optimize the visibility of these photos by setting their display size between 80 and 500 pixels.

Alarm Monitoring Recipient Mailbox

Configure email addresses within the system to receive automatic notifications when alarms or critical events occur, ensuring timely awareness of security incidents.

Compare Photo Delivery Settings

This feature allows the system to send a comparison photo to the device for local storage during access control operations.

Cloud Building Setting

This setting ensures that all device and system data is stored securely in a cloud-based building infrastructure.

Copyright © 2024 ARMATURA LLC. All rights reserved

6.4 Advanced Functions

Function Description

Advanced access control functions provide enhanced capabilities for managing complex access control scenarios. These features are optional and require a license for activation. Contact a business representative or pre-sales engineer to obtain and enable these features.

Function List

Functions	Description
Zone	Add, edit, delete, and view the access control rules for a specific area.
Reader Definition	Perform batch operations such as adding, editing, and deleting readers.
View People in the Area	Delete or export personnel records associated with a specific area.
Global Anti-passback	Configure, edit, or delete anti-passback rules for personnel across multiple areas.
Global Linkage	Add, edit, delete, enable, or disable linkage actions for personnel.
Global Interlock Group	Manage global interlock groups, including adding, editing, or deleting them.
Global Interlock	Define and manage interlock settings for doors on a global scale.
Person Availability	Manage access control area attributes for personnel by adding, editing, deleting, and setting them.
Number Control	Define and manage maximum or minimum occupancy for specific areas.

Note:

Except for **Global Linkage**, using other advanced functions requires enabling **Background Verification**. Ensure this feature is activated before configuring advanced access control functions.

6.4.1Zone

Function Description

The Zone feature partitions physical areas for enhanced access control functionality. This foundational component enables advanced features such as Global Zone Anti-Passback (APB), allowing sophisticated rules and restrictions within defined spaces.

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Zone configuration is essential for implementing advanced access control operations and creating structured area partitions for improved security management and monitoring.

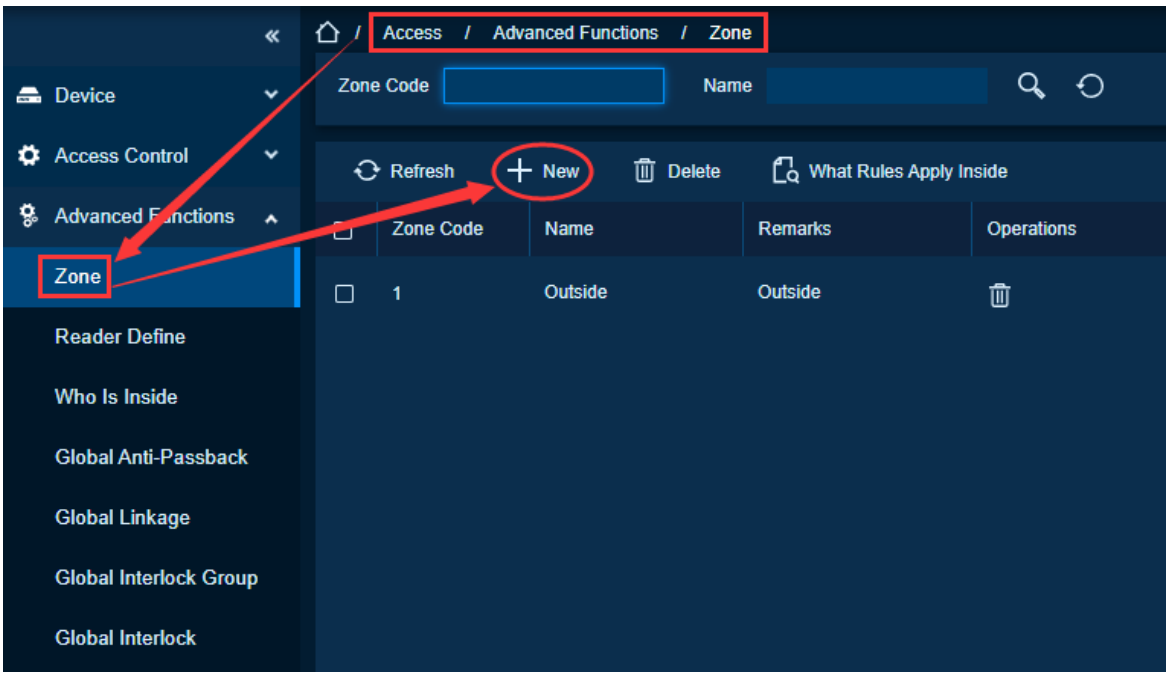
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

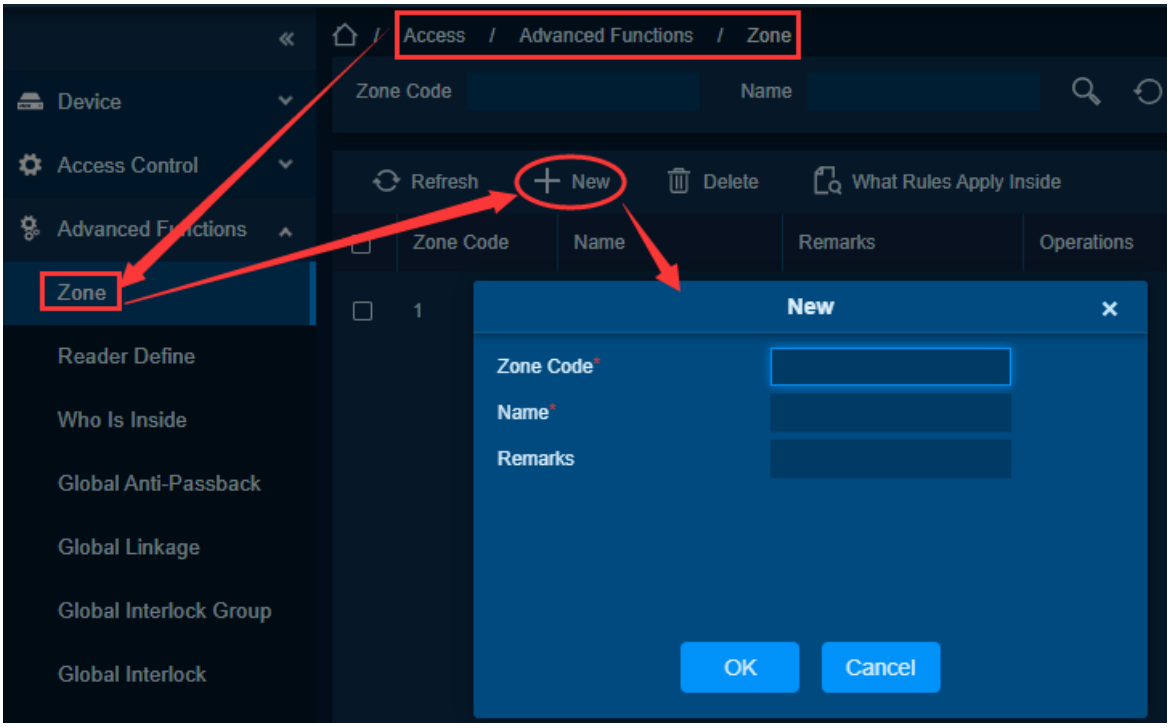
Zone creation enables the configuration and activation of advanced access control features within the defined areas.

Steps:

- Navigate to **[Advanced Functions] > [Zone] > [New]** to access the Add Zone interface.



- Set **Zone Code**, **Zone Name**, **Parent Zone**, and **Remark**. Click **[OK]** to save the configuration and exit the interface.



Copyright © 2024 ARMATURA LLC. All rights reserved

Edit Access Control Area

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

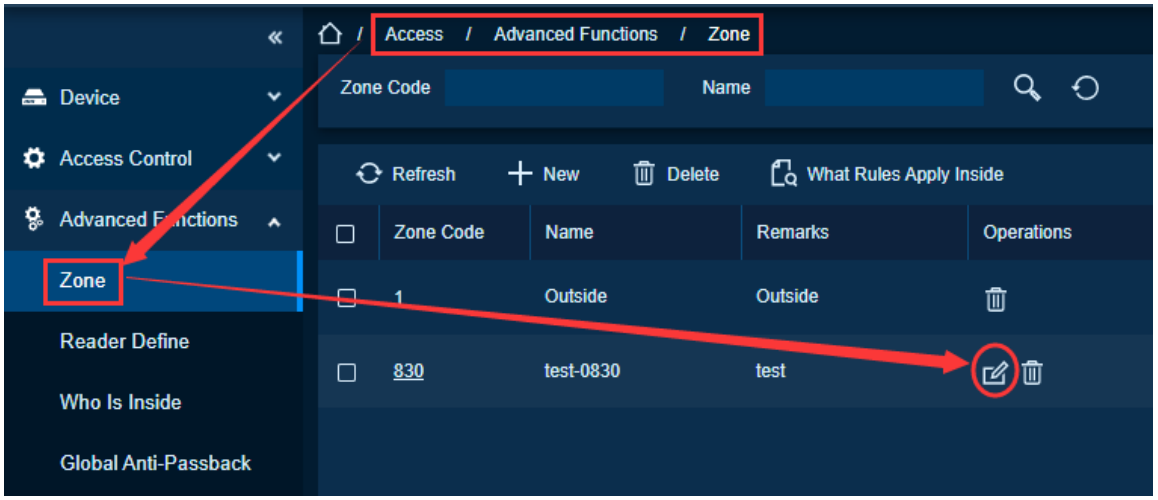
This function allows updates when access control area configurations require modification due to changes or corrections in area settings.

Trigger Result

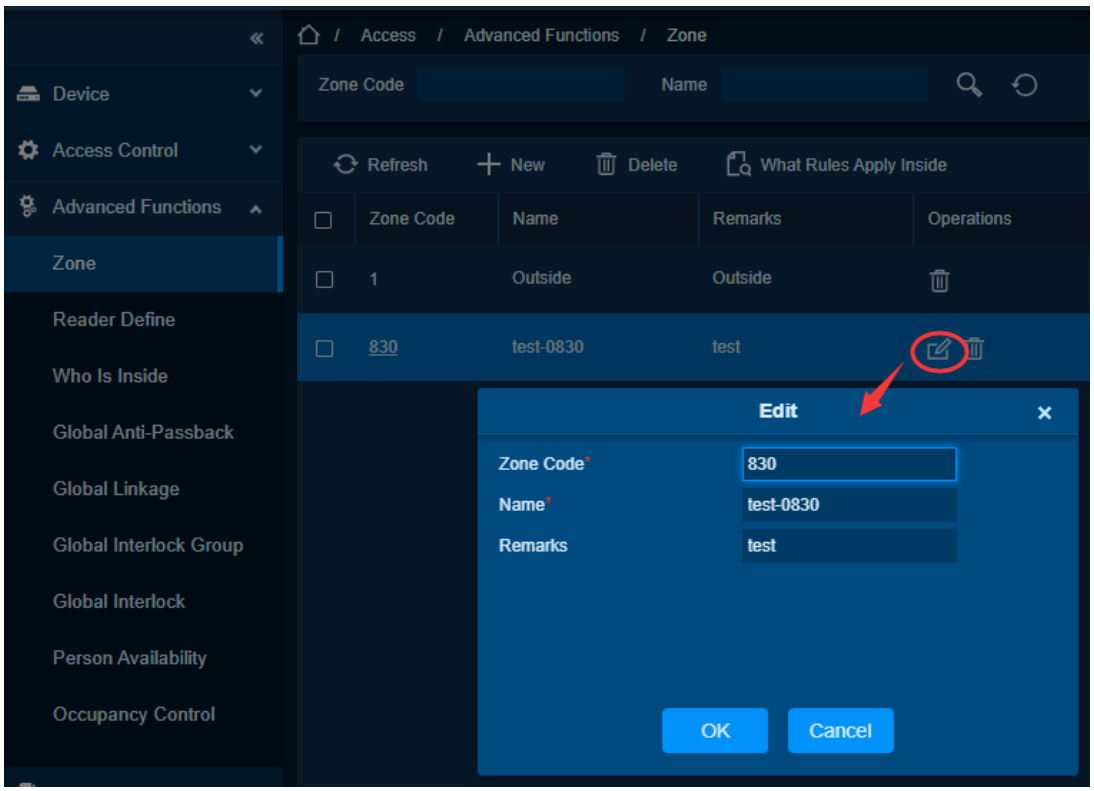
Successfully modifying the area ensures the continued functionality of advanced access control features.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Zone]** to display the access control area interface.
- Locate and select the access control area to be modified.
- Click **[Edit]** to make changes to the selected area.
- Apply the modifications and click **[OK]** to save and update the area settings.



Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Access Control Area

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function is utilized when an access control area becomes obsolete and requires removal from the system.

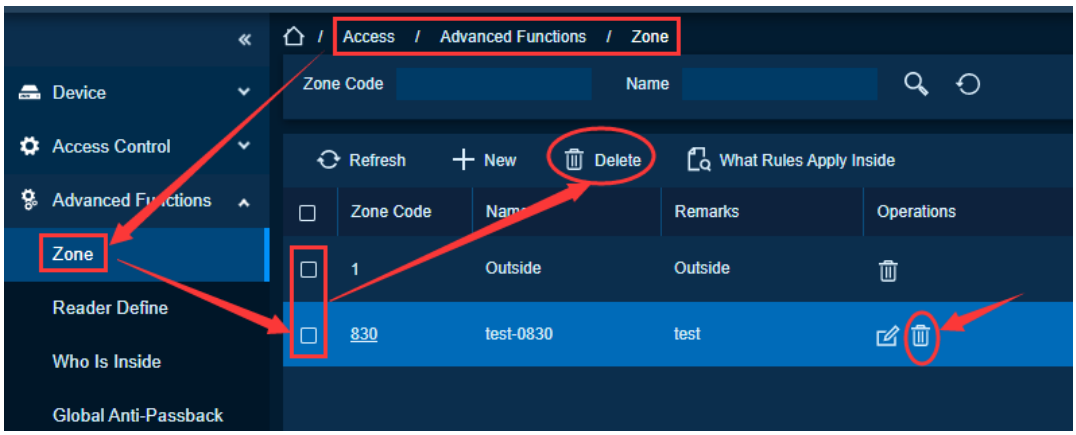
Trigger Result

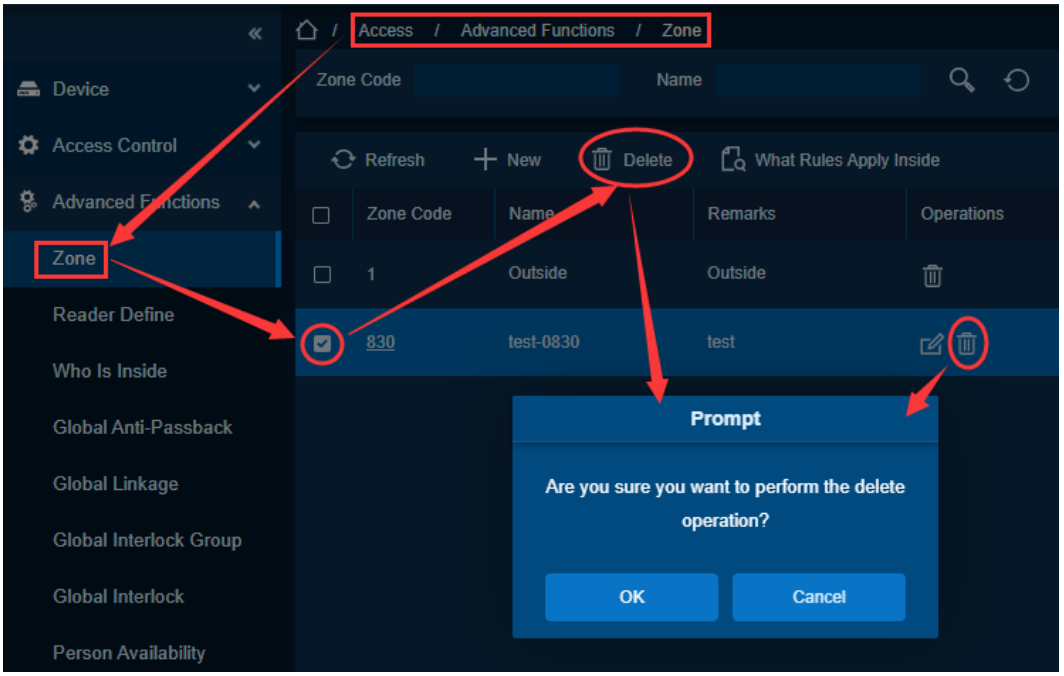
Upon deletion, all advanced access control functions associated with the removed area become inactive.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Zone]** to display the access control area interface.
- Locate and select the access control area to be removed.
- Click **[Delete]** to remove the area from the system.
- Confirm the deletion action by clicking **[OK]** to finalize the process.

Copyright © 2024 ARMATURA LLC. All rights reserved





What Rules Apply Inside

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function enables users to review active access control rules within specific areas, including global linkage settings and personnel permissions.

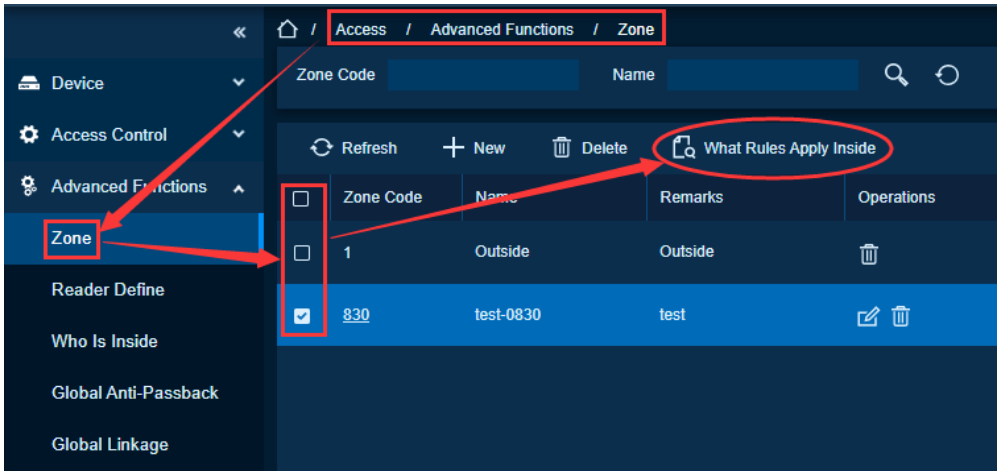
Trigger Result

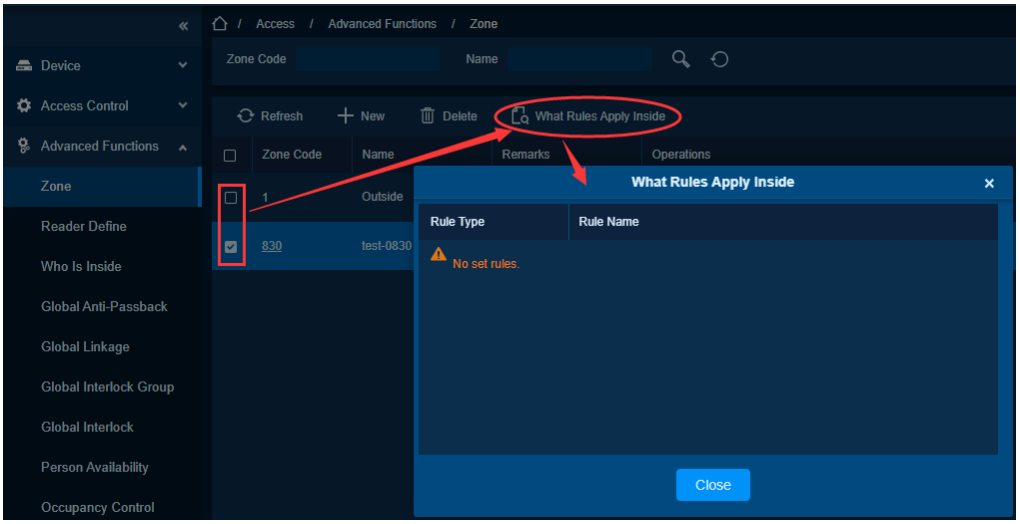
The system provides a comprehensive view of all rules and configurations currently active within the selected access control area.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Zone]** to open the access control area interface.
- Locate and select the specific access control area.
- Click **[What Rules Apply Inside]** to display a list of access control rules applied to the selected area.





6.4.2Reader Define

Function Description

Reader Define establishes control parameters for readers across multiple access zones, enabling advanced features like global anti-passback. Proper configuration of Reader Definitions is essential for implementing these security functions.

New Reader Definition

Prerequisites for Use

Log into the system using an account with the required permissions.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

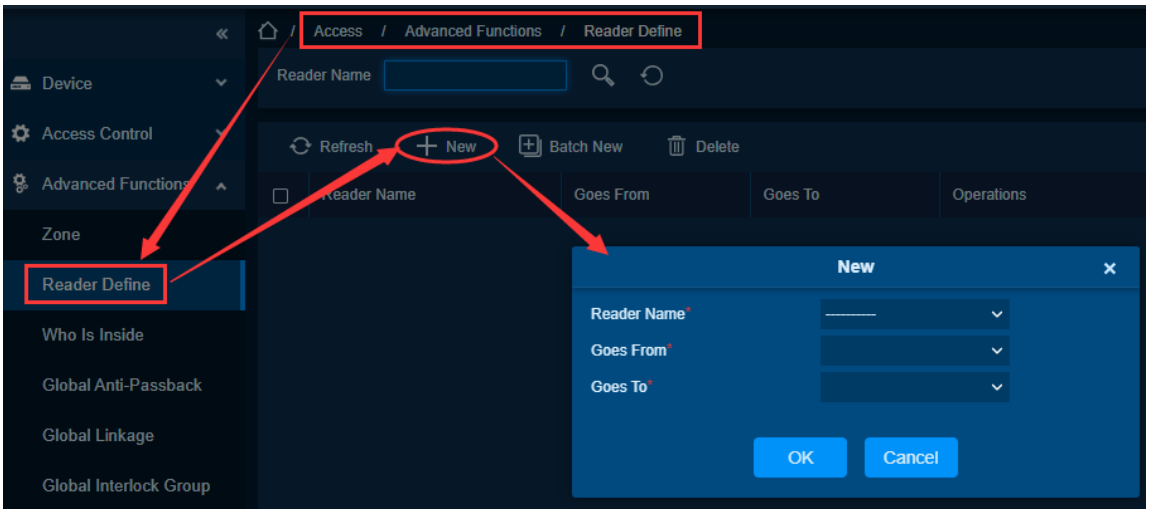
This configuration is essential when implementing global anti-passback functionality across the access control system.

Trigger Result

Upon completion, the system establishes entry and exit zone parameters for readers, enabling global anti-passback implementation.

Steps:

- Navigate to **[Access]** > **[Advanced Functions]** > **[Reader Define]** > **[New]** to open the add interface.



- Configure the following parameters, Reader Name, Goes From, and Goes To: Define the destination access zone.
- Click **[OK]** to save and exit.
- The added Reader Definition will appear in the list.

Add Reader Definitions in Batches

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function enables simultaneous configuration of multiple readers with identical access control zone settings.

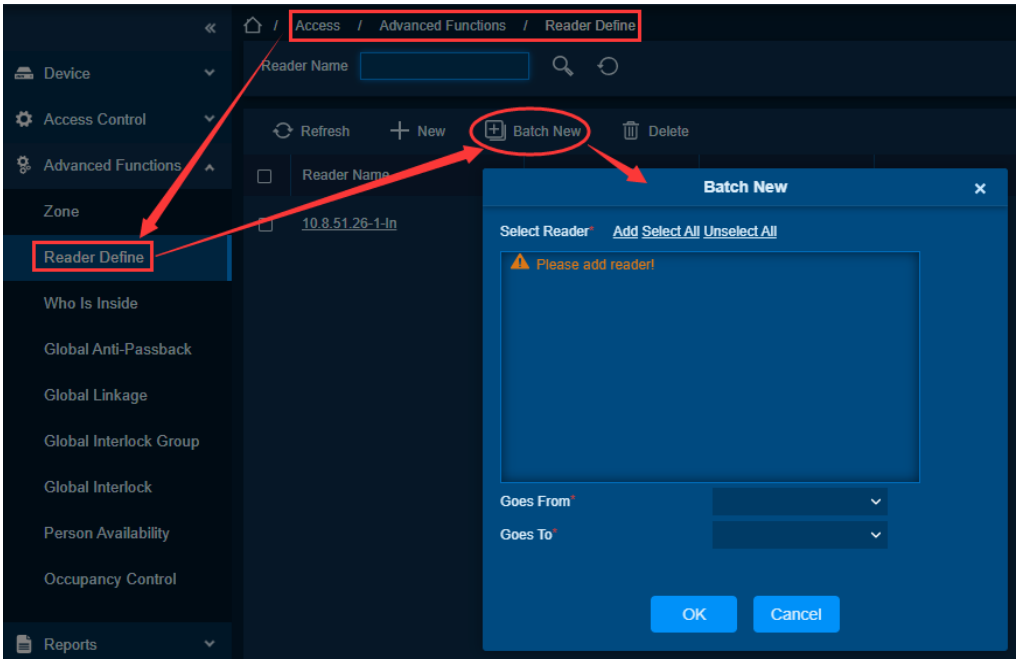
Trigger Result

Upon completion, the system establishes zone parameters for multiple readers simultaneously, enabling global anti-passback implementation across the defined set.

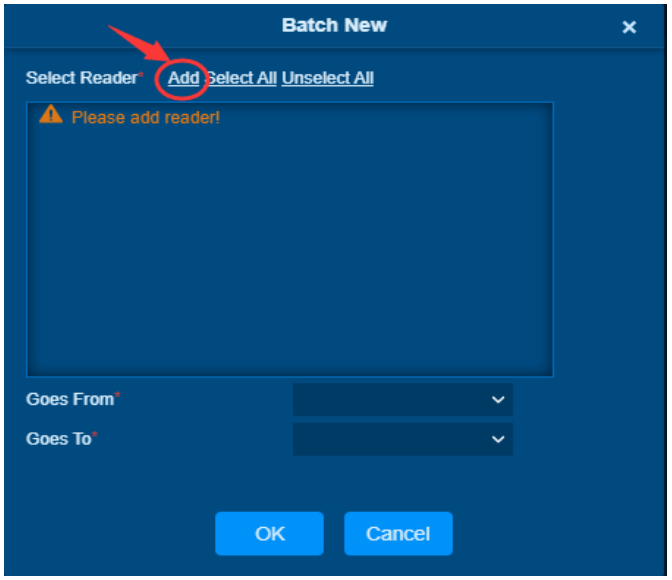
Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

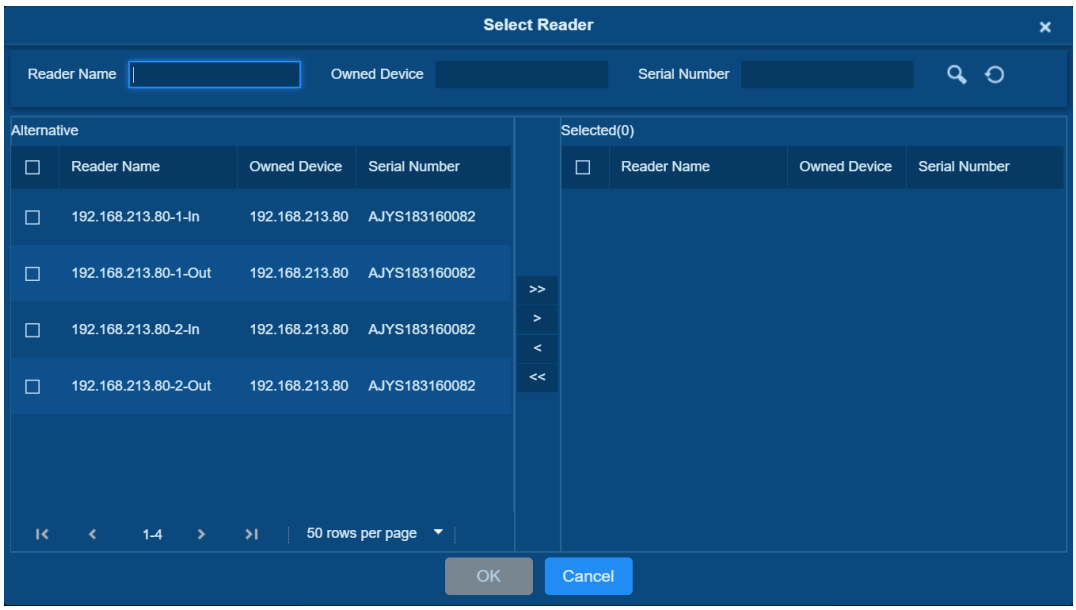
- Navigate to **[Access] > [Advanced Functions] > [Reader Define] > [Batch New]**.
- Click **[OK]** to save the batch definitions.



- Click **[Add]**, select multiple readers from the left list, move them to the right, and click **[OK]**.



Copyright © 2024 ARMATURA LLC. All rights reserved



- Configure the **Goes From** and **Goes To** fields for the selected readers.

Edit Reader Definition

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function allows the modification of existing reader definitions when zone assignments need to be updated.

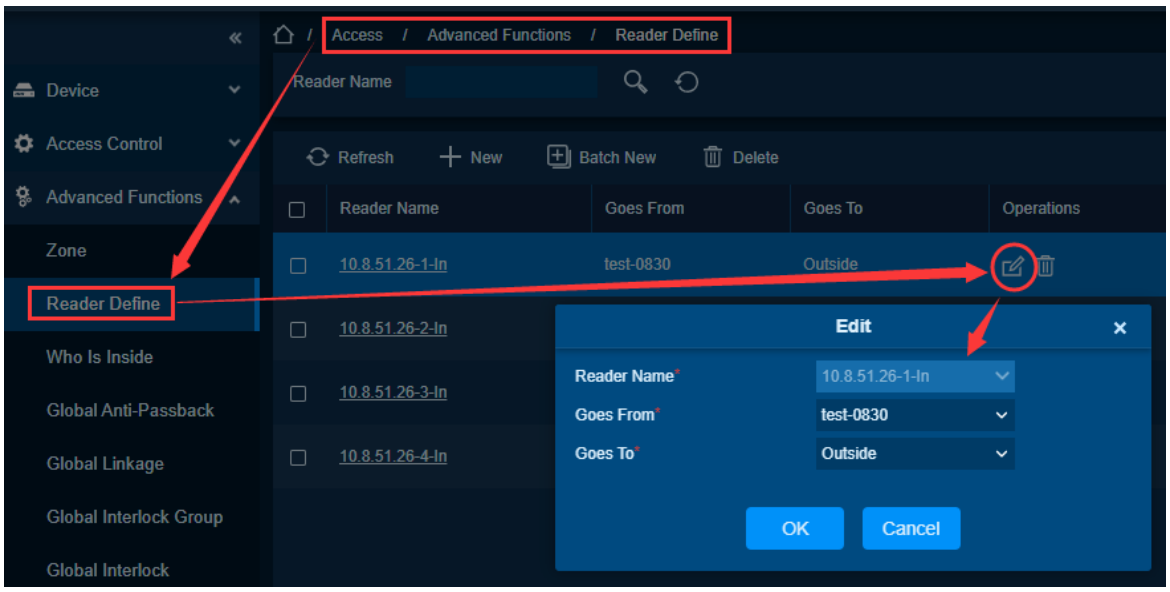
Trigger Result

The system updates global anti-passback settings according to the modified reader definition parameters.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Reader Define]** to access the reader definition interface.
- Select the target reader definition and click **[Edit]** to modify the necessary configuration fields.
- Click **[OK]** to save changes.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Reader Definition

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function is used when a reader definition becomes obsolete or global anti-passback functionality is no longer required.

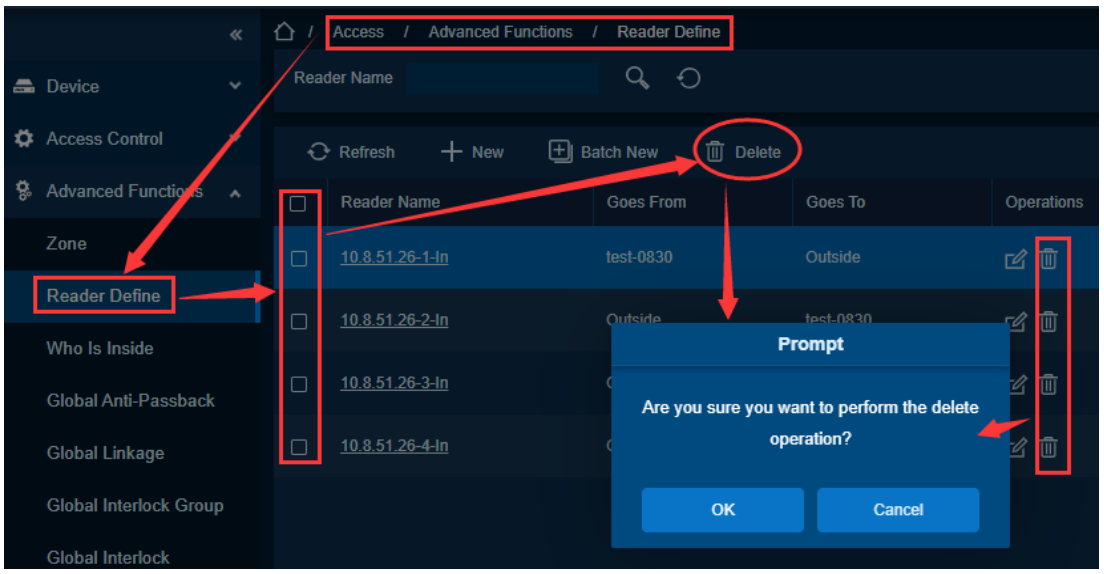
Trigger Result

Upon completion, the system removes the reader definition and disables its associated global anti-passback functionality.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Reader Define]** to access the reader definition interface.
- Select the target reader definition, click **[Delete]**
- Confirm the removal by clicking **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.4.3Who Is Inside

Function Description

The "Who Is Inside" feature allows users to view personnel status in a zone-by-zone tree structure after entering the zone. This function helps monitor personnel in each access control area and provides options for deleting or exporting personnel information.

Delete Personnel

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function removes individual access privileges from specific areas and clears associated anti-passback status settings.

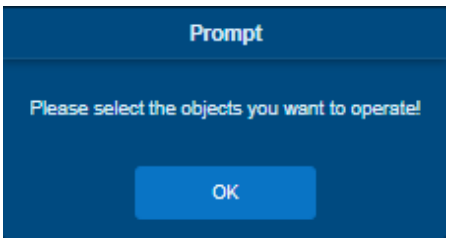
Trigger Result

Upon completion, the system revokes the selected individual's access permissions for the specified area.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Who is inside] > [View Personnel in the Area]** to display the personnel interface.
- Select the person to be deleted.
- Click **[Delete Personnel]** to remove the person from the area.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export Personnel Information

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

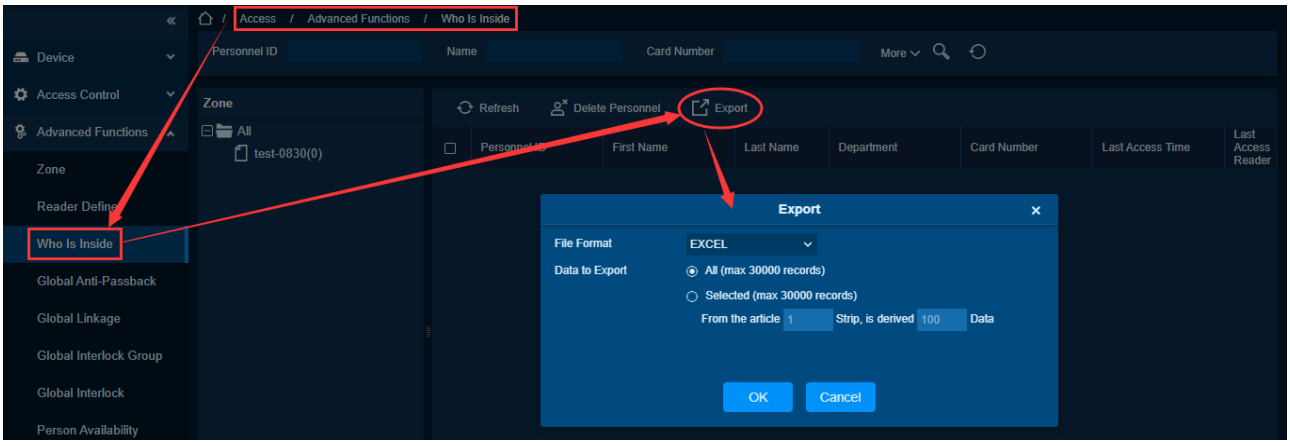
This function enables generation of personnel reports in various formats including Excel, PDF, and CSV for documentation and analysis purposes.

Trigger Result

The system generates and saves personnel data files in the selected format for the specified area.

Steps:

- Navigate to **[Access]** > **[Advanced Functions]** > **[Who is inside]** to display the area personnel interface.
- Click **[Export]**.
- Select the desired file format (Excel, PDF, or CSV) and save the exported personnel information.



6.4.4Global Linkage

Function Description

Global Linkage enables configuration of coordinated actions across multiple devices, encompassing door control, auxiliary outputs, video integration, schedule management, and event notifications.

Copyright © 2024 ARMATURA LLC. All rights reserved

New Global Linkage

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

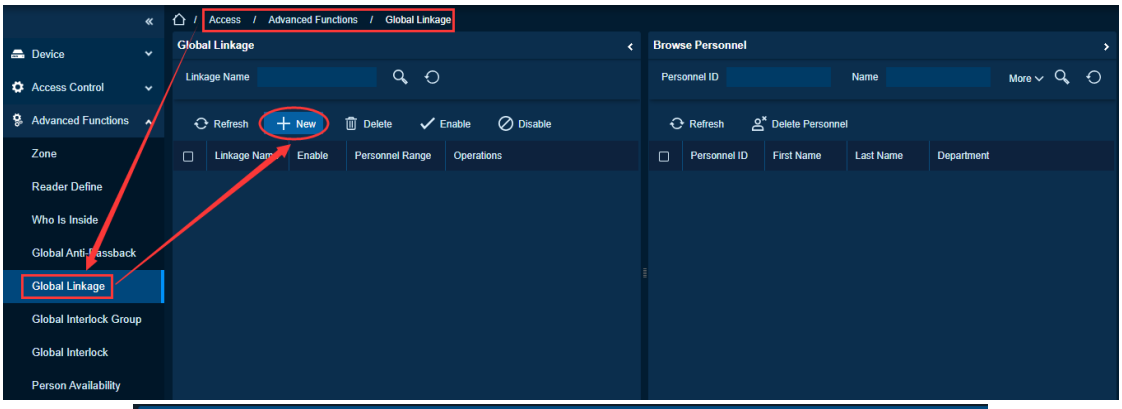
This function establishes automated cross-device responses and actions throughout the access control system.

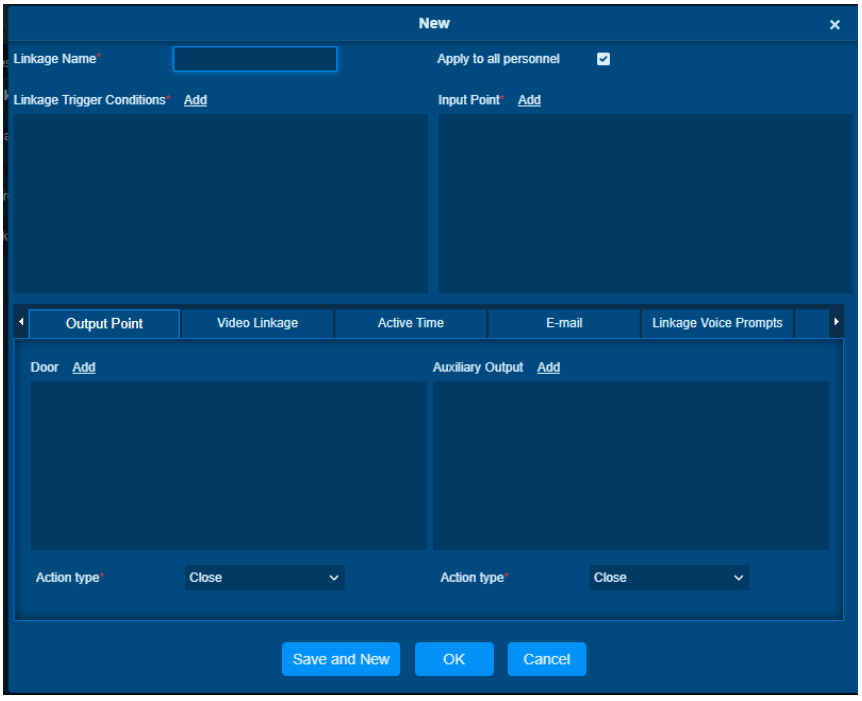
Trigger Result

Upon configuration, the system enables coordinated control and automation across multiple connected devices.

Steps:

- Navigate to **[Advanced Functions] > [Global Linkage] > [New]**.





Copyright © 2024 ARMATURA LLC. All rights reserved

- Configure settings by specifying personnel coverage through Apply to All Personnel, defining Active Time periods for linkage enforcement, and establishing Trigger Conditions by selecting input points and their corresponding output actions.
- Complete the setup by clicking **[OK]** to save and add the new Global Linkage to the system.

Edit Global Linkage

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

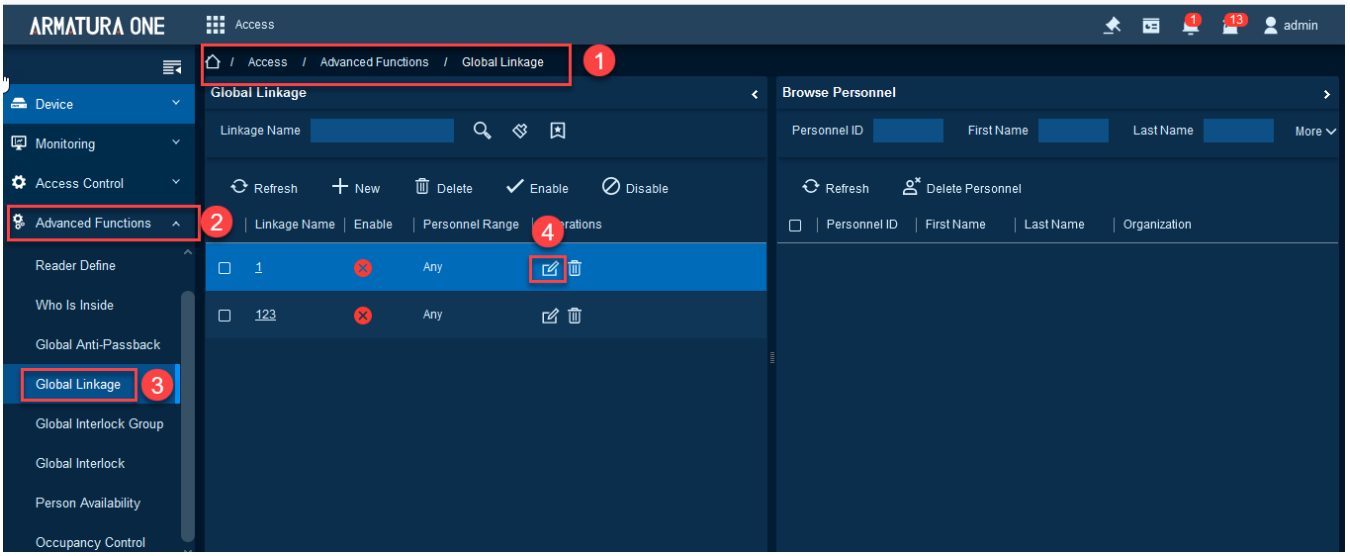
Modify the settings of a previously configured linkage.

Trigger Result

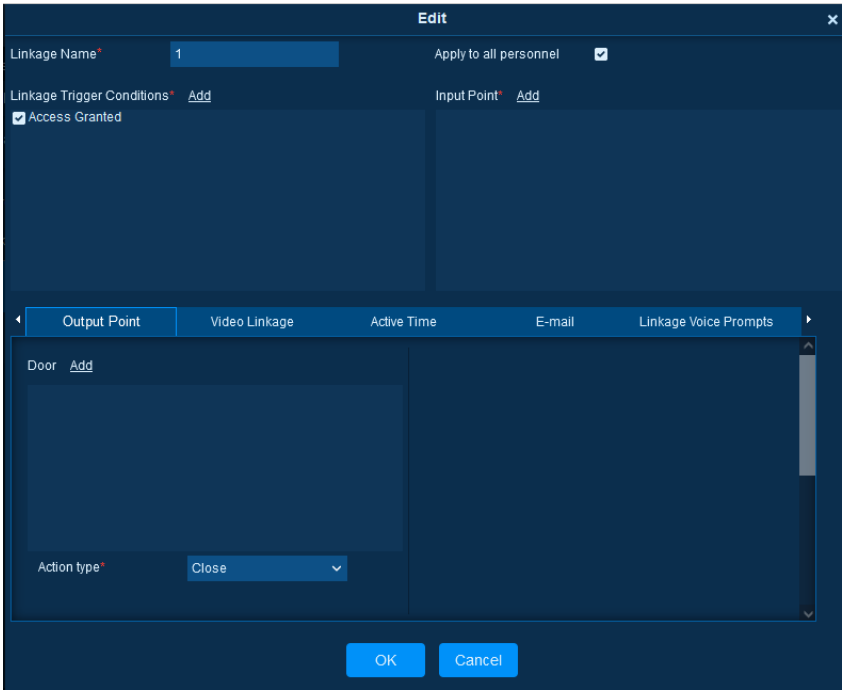
The modified settings will take effect across devices.

Steps:

- Navigate to **[Access]** > **[Advanced Functions]** > **[Global Linkage]**.
- Select the desired linkage and click **[Edit]**.
- Modify the settings as required, then save the changes.



Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Personnel

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

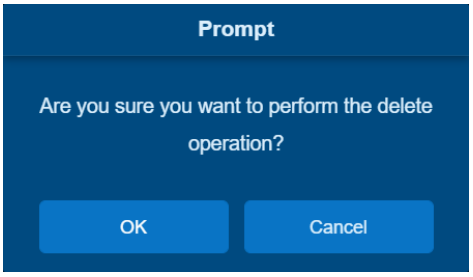
This function removes individual access to global linkage operations.

Trigger Result

Upon completion, the selected individual loses authorization to perform associated linkage operations.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Global Linkage]**.
- Select the linkage event involving the person and click **[Delete Person]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

Delete Global Linkage

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

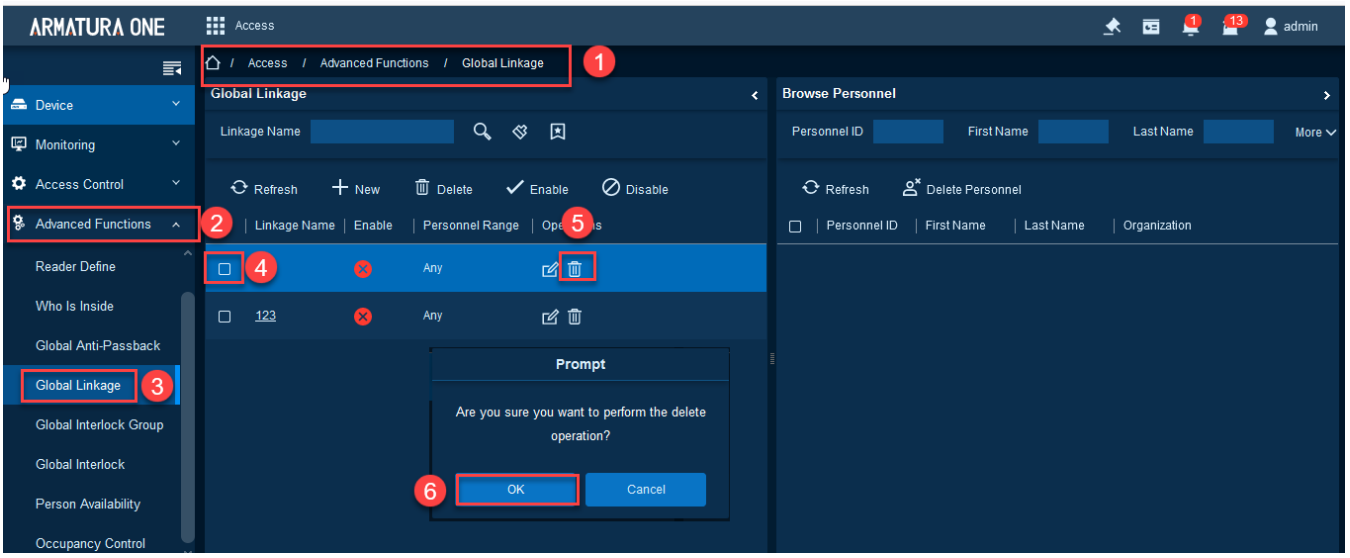
This function removes obsolete or unnecessary global linkage configurations from the system.

Trigger Result

Upon deletion, the specified linkage operations become inactive and can no longer be executed.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Global Linkage]**.
- Select the linkage event and click **[Delete]**.



Enable Global Linkage

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function activates previously configured global linkage settings.

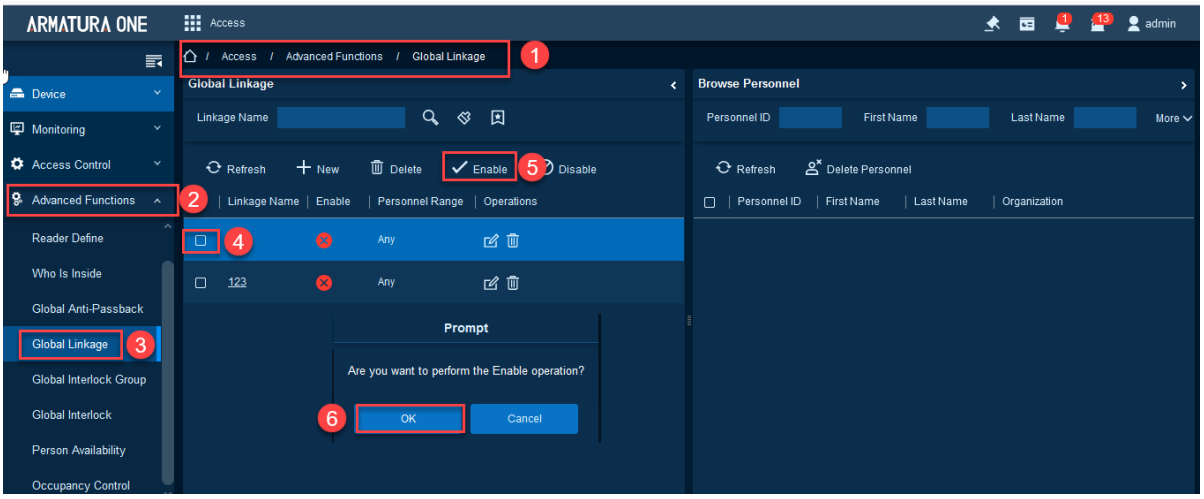
Trigger Result

Upon activation, the system enables the linkage operations and displays a green status indicator.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Global Linkage]**.
- Select the desired linkage event and click **[Enable]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Disable Global Linkage

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

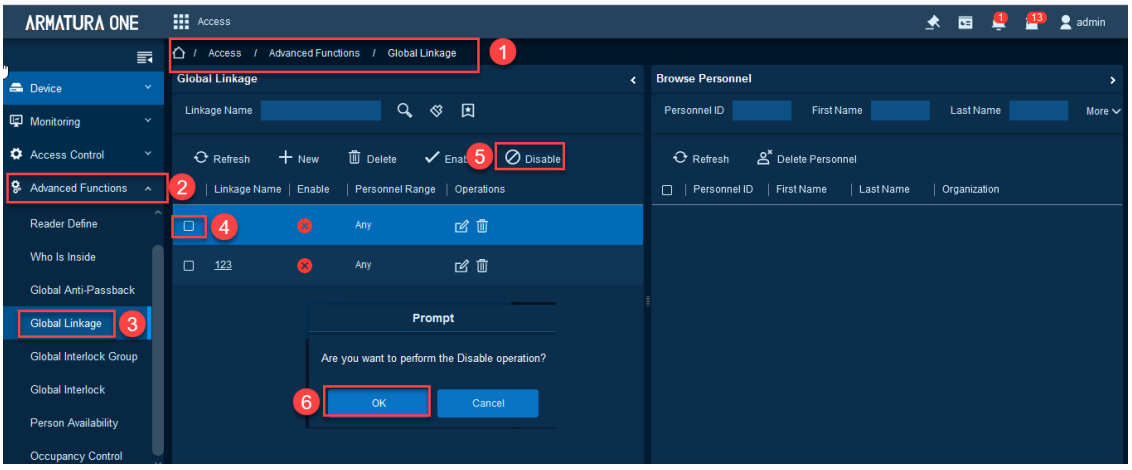
This function temporarily suspends active global linkage configurations.

Trigger Result

Upon deactivation, the system disables the linkage operations and displays a red status indicator.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Global Linkage]**.
- Select the desired linkage event and click **[Disable]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

6.4.5Global Interlock Group

Function Description

Global Interlock Group manages door organization for implementing Global Interlock functionality. This feature requires enabled background authentication on participating devices.

New Global Interlock Group

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

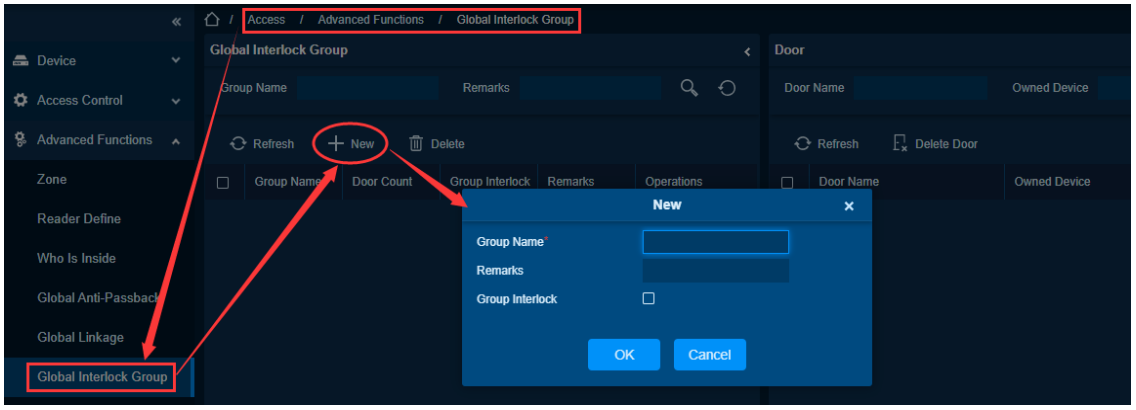
This function enables door grouping for implementing coordinated global interlock rules.

Trigger Result

Upon completion, the system enables configuration of global interlock operations for the grouped doors.

Steps:

- Navigate to **[Access]** > **[Advanced Functions]** > **[Global Interlock Group]** > **[New]**.

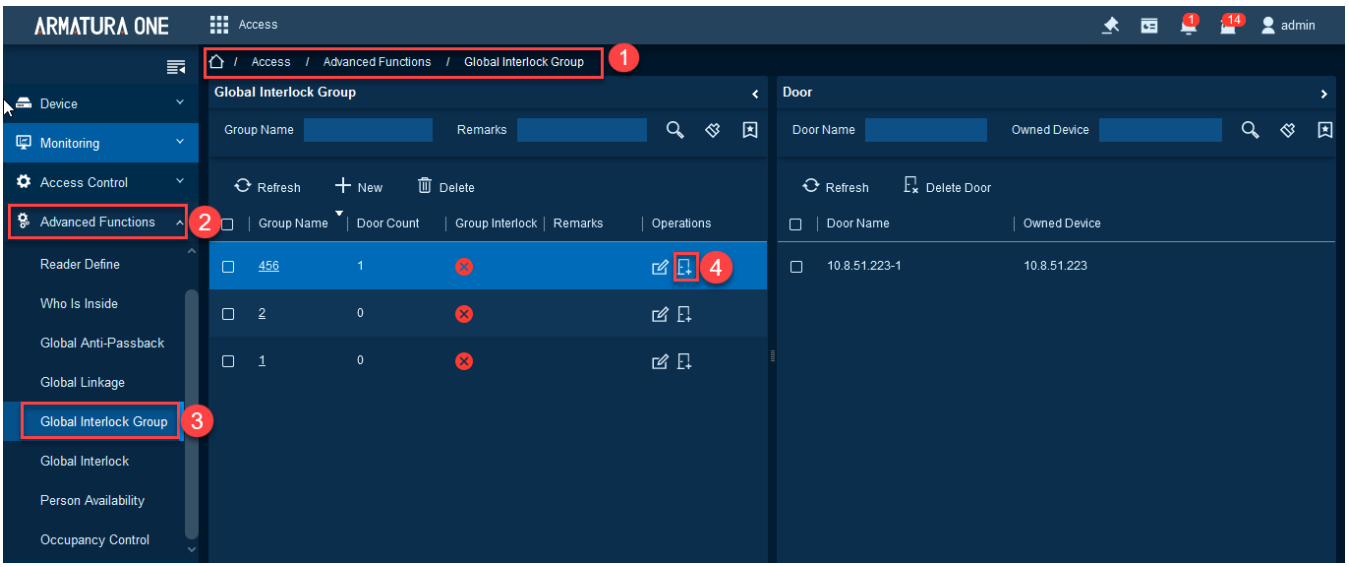


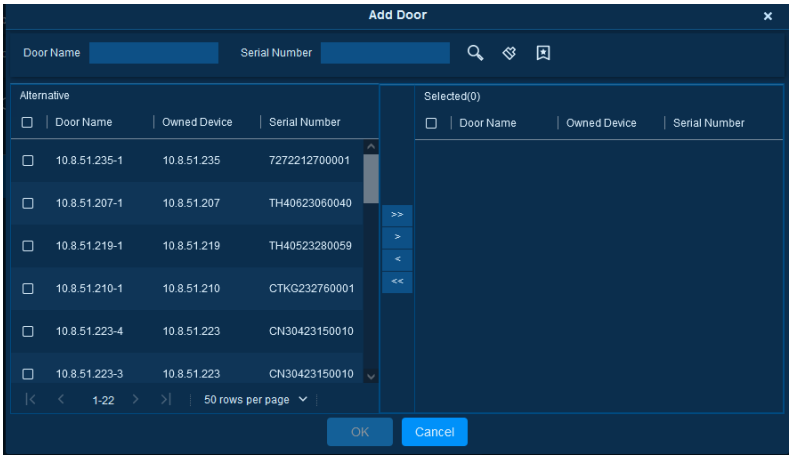
- Enter a unique Group Name using up to 30 characters and enable Group Interlock to configure global rules.
- Complete the setup by clicking **[OK]**, then decide whether to add doors immediately.
- The system will display all added doors in the list.

Add Door

- Navigate to **[Access] > [Advanced Functions] > [Global Interlock Group]** to display the Global Interlock Group interface.
- Select the desired interlock group and click **[Add Door]**.
- Choose the doors to add and save.

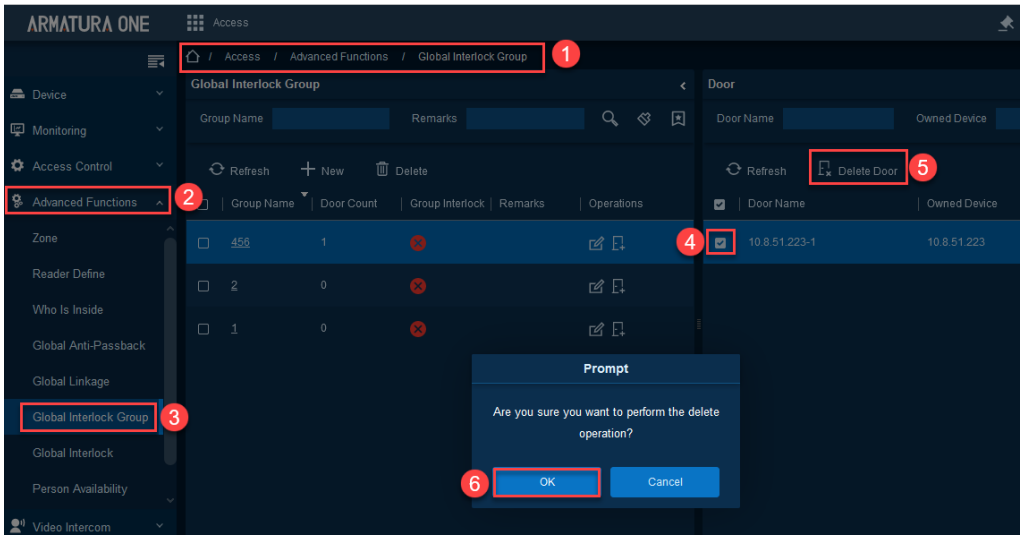
Copyright © 2024 ARMATURA LLC. All rights reserved





Delete the door

- Navigate to **[Access] > [Advanced Functions] > [Global Interlock Group]** to display the Global Interlock Group interface.
- Select the interlock group of the door to be removed and click **[Delete Door]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

Edit Global Interlock Group

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

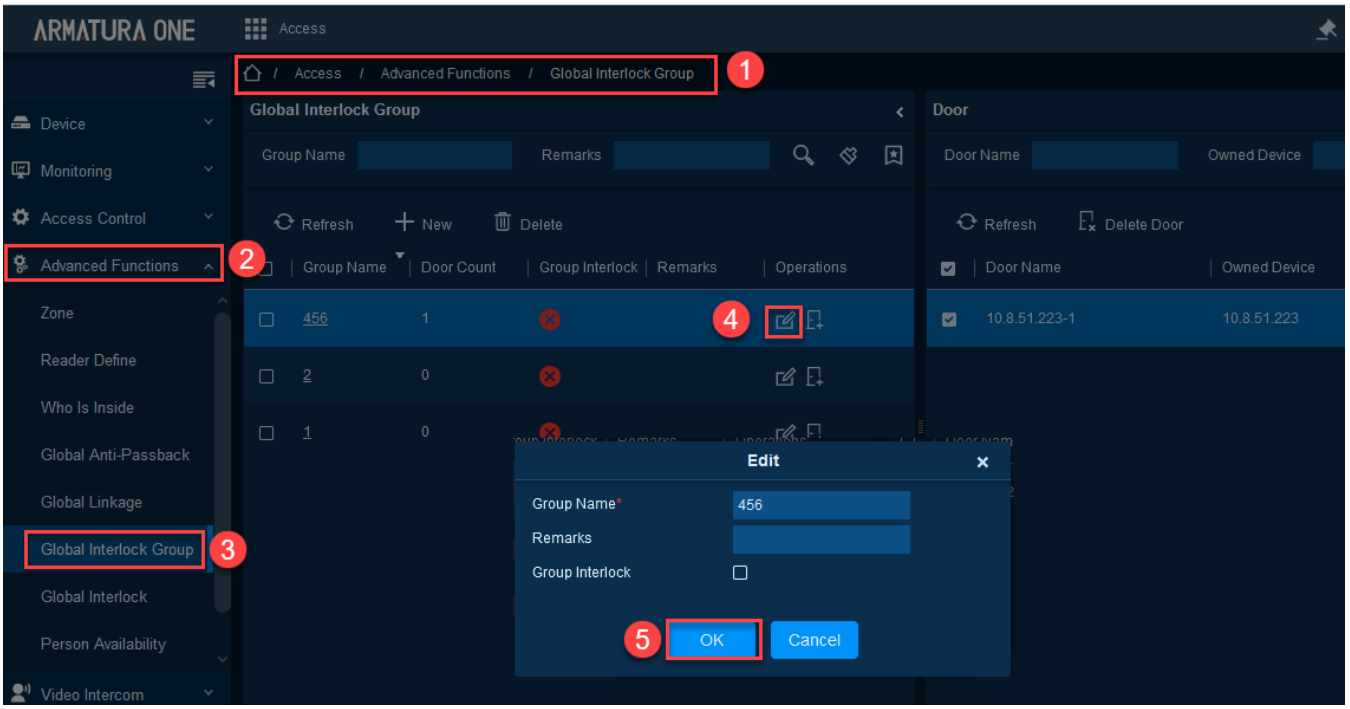
This function allows modification of existing door groupings within Global Interlock configurations.

Trigger Result

The system updates Global Interlock settings according to the modified door group configurations.

Steps:

- Navigate to **[Access]** > **[Advanced Functions]** > **[Global Interlock Group]** to display the Global Interlock Group interface.
- Select the group to be modified and click **[Edit]**.



Delete Global Interlock Group

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function removes specified door groups from Global Interlock functionality.

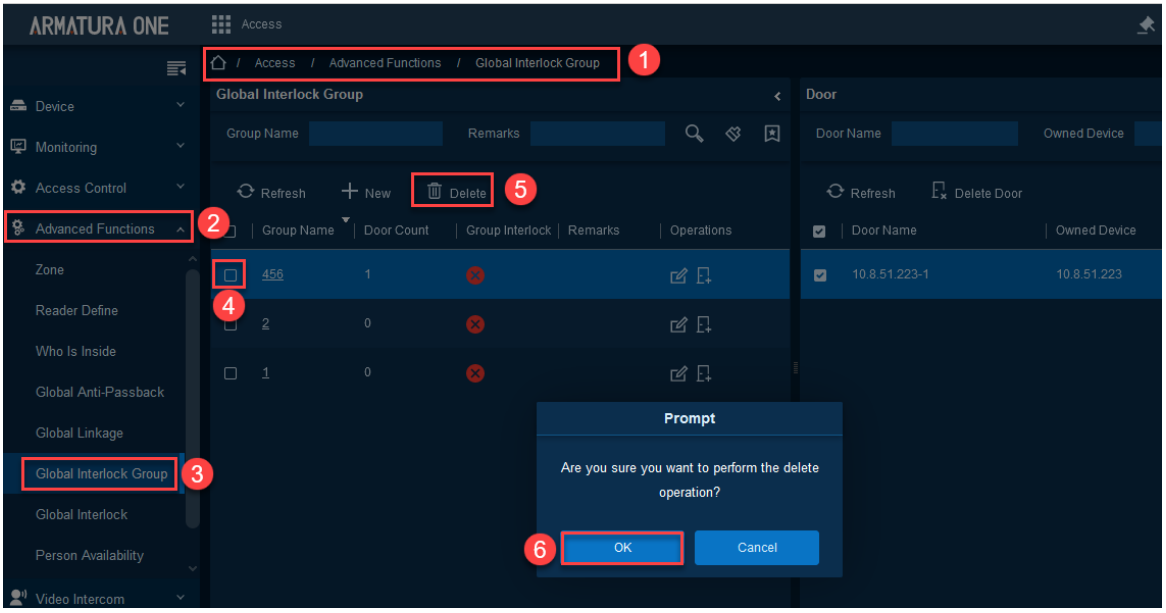
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Upon completion, the system disables Global Interlock operations for the deleted door group.

Steps:

- Navigate to **[Access]** > **[Advanced Functions]** > **[Global Interlock Group]** to display the Global Interlock Group interface.
- Select the group to be removed and click **[Delete]**.



6.4.6Global Interlock

Function Description

Global Interlock enables configuration of coordinated interlock settings across multiple devices to enhance access control security.

Add Global Interlock

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

This function establishes cross-device interlock configurations for enhanced access control management.

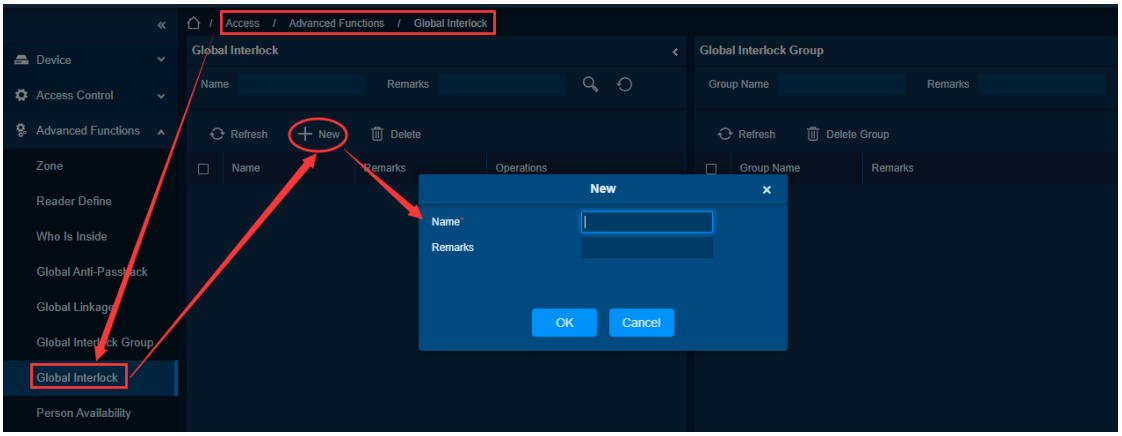
Trigger Result

Upon completion, the system activates coordinated interlock functionality across the configured devices.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access]** > **[Advanced Functions]** > **[Global Interlock]** > **[New]**.



- Create a unique configuration name using up to 30 characters and ensure no doors are duplicated within the same interlock group.
- Click **[OK]** to save and activate the configuration.

Edit Global Interlock

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

This function enables modification of existing interlock settings to update cross-device configurations.

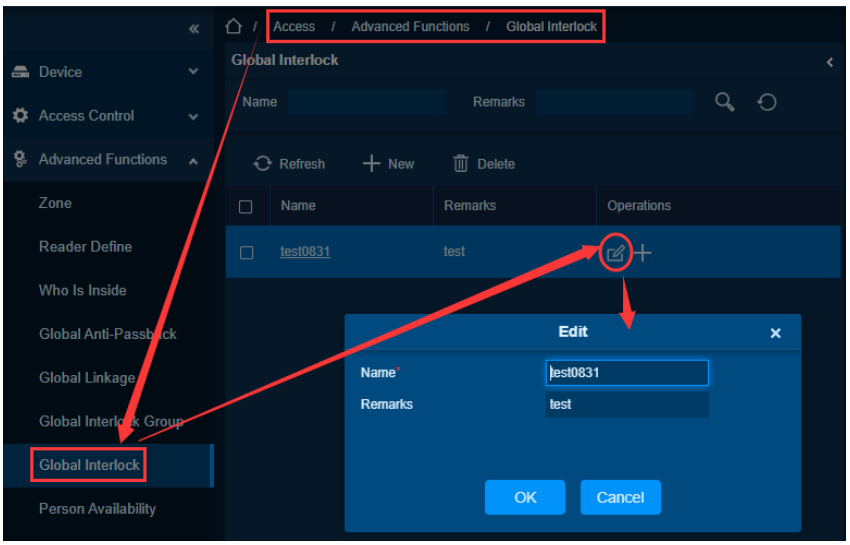
Trigger Result

Upon completion, the system implements updated interlock settings across configured devices.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Global Interlock]** to display the interface.
- Select the interlock configuration to be edited and click **[Edit]**.
- Modify the desired settings and click **[OK]** to save changes.

Copyright © 2024 ARMATURA LLC. All rights reserved



Add Group

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

This function establishes interlock security measures across multiple connected devices in the system.

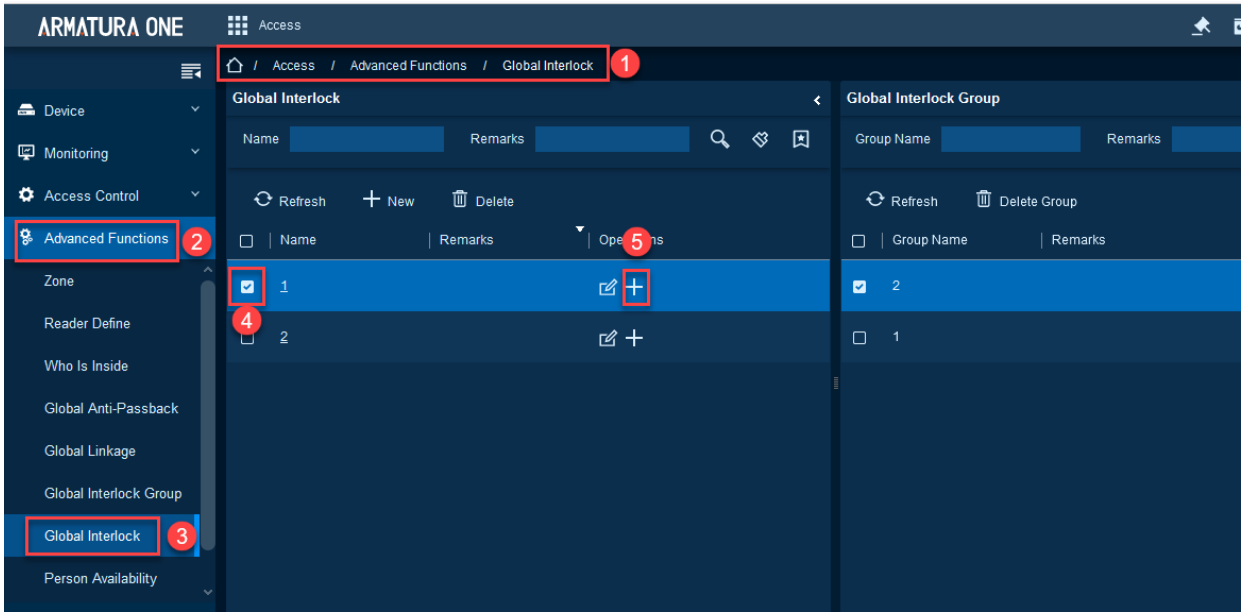
Trigger Result

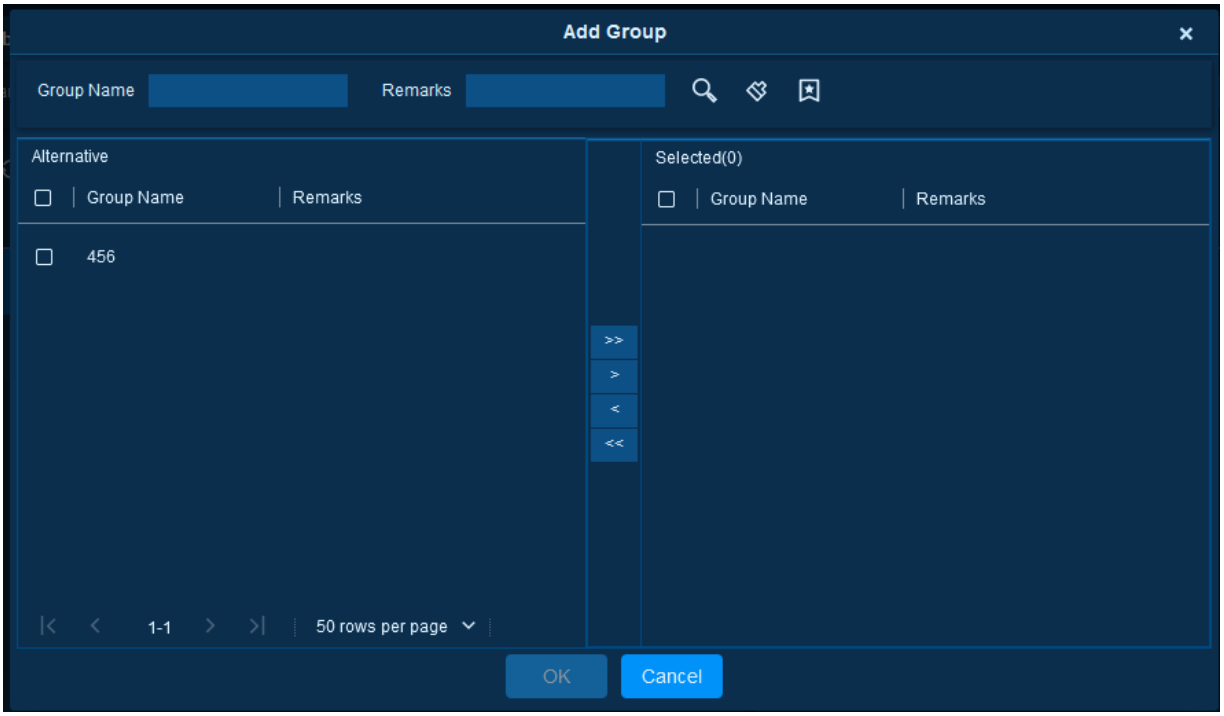
The system enables coordinated interlock functionality across multiple connected devices.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Global Interlock]** to display the interface.
- Select the interlock configuration to be deleted and click **[Delete]**.
- Confirm the deletion in the prompted interface.

Copyright © 2024 ARMATURA LLC. All rights reserved





Delete Global Interlock

Prerequisites for Use

Log into the system with an account that has the required authority.

Usage Scenarios

This function removes obsolete or unnecessary interlock configurations from the system.

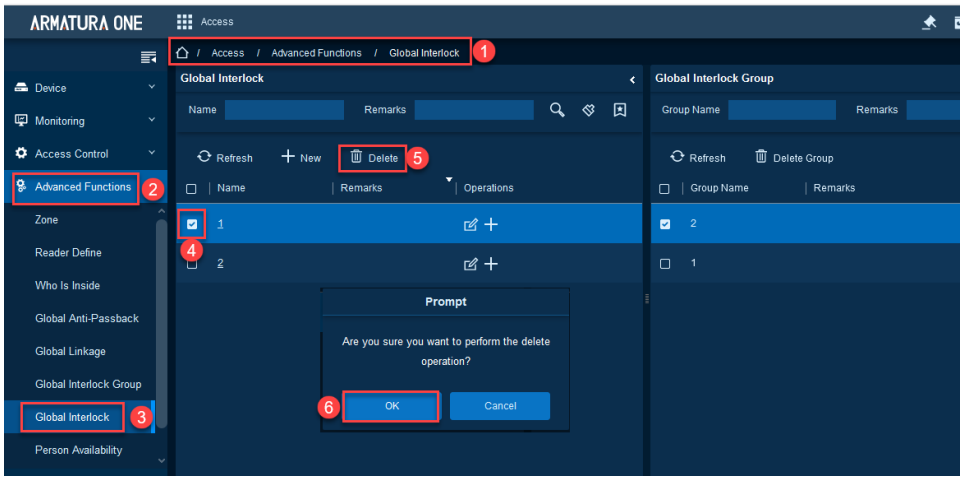
Trigger Result

Upon deletion, the system deactivates interlock operations for the selected configuration.

Copyright © 2024 ARMATURA LLC. All rights reserved

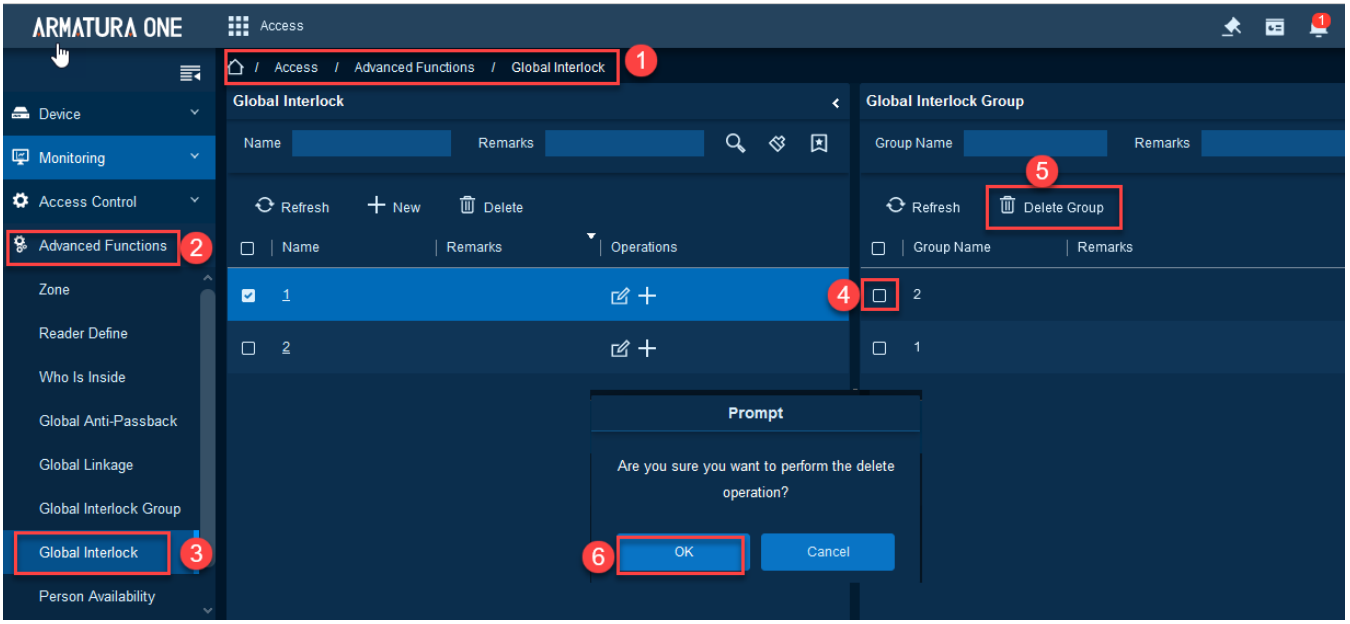
Steps:

- Navigate to **[Access] > [Advanced Functions] > [Global Interlock]** to display the interface.
- Select the interlock configuration to be deleted and click **[Delete]**.
- Confirm the deletion in the prompted interface.



Delete the Group

- Navigate to **[Access]** > **[Advanced Functions]** > **[Global Interlock Group]** to display the interface.
- Select the interlock group containing the door to be removed and click **[Delete the Group]**.
- Confirm the deletion to finalize the process.



6.4.7Person Availability

Copyright © 2024 ARMATURA LLC. All rights reserved

Function Description

Person Availability enables administrators to manage personnel access by setting validity periods, usage limits after first entry, and maximum usage counts within advanced access control areas.

Add Person

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

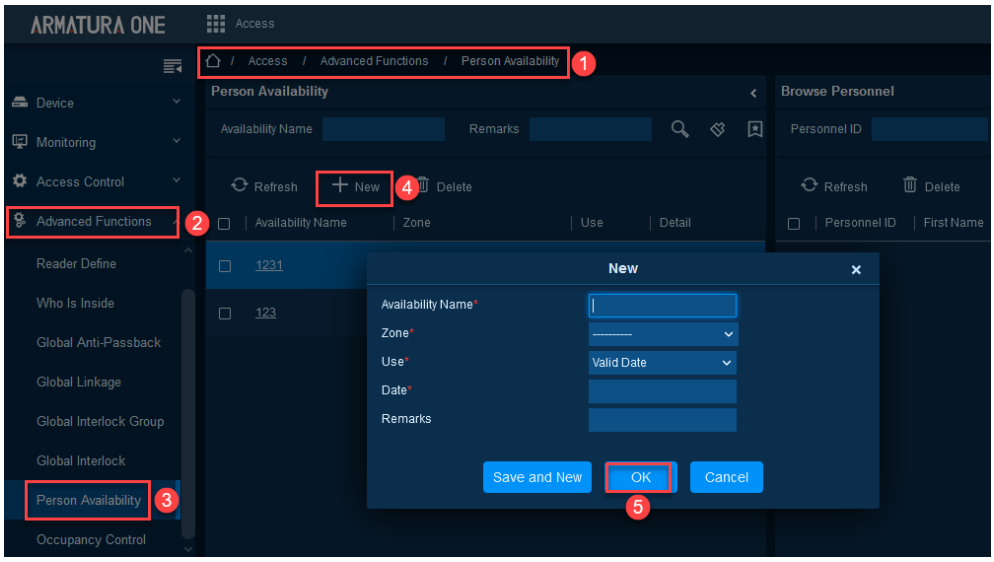
This function enables customized access control attributes for individual personnel based on specific area requirements.

Trigger Result

Upon completion, the system implements personalized access control parameters for designated individuals within specified areas.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Personnel Validity]**.
- Click **[New]** to access the setup interface.
- Enter details to add the person and their associated attributes.
- Click **[OK]** to save.



Add Personnel

Prerequisites for Use

Log into the system using an account with the required permissions.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

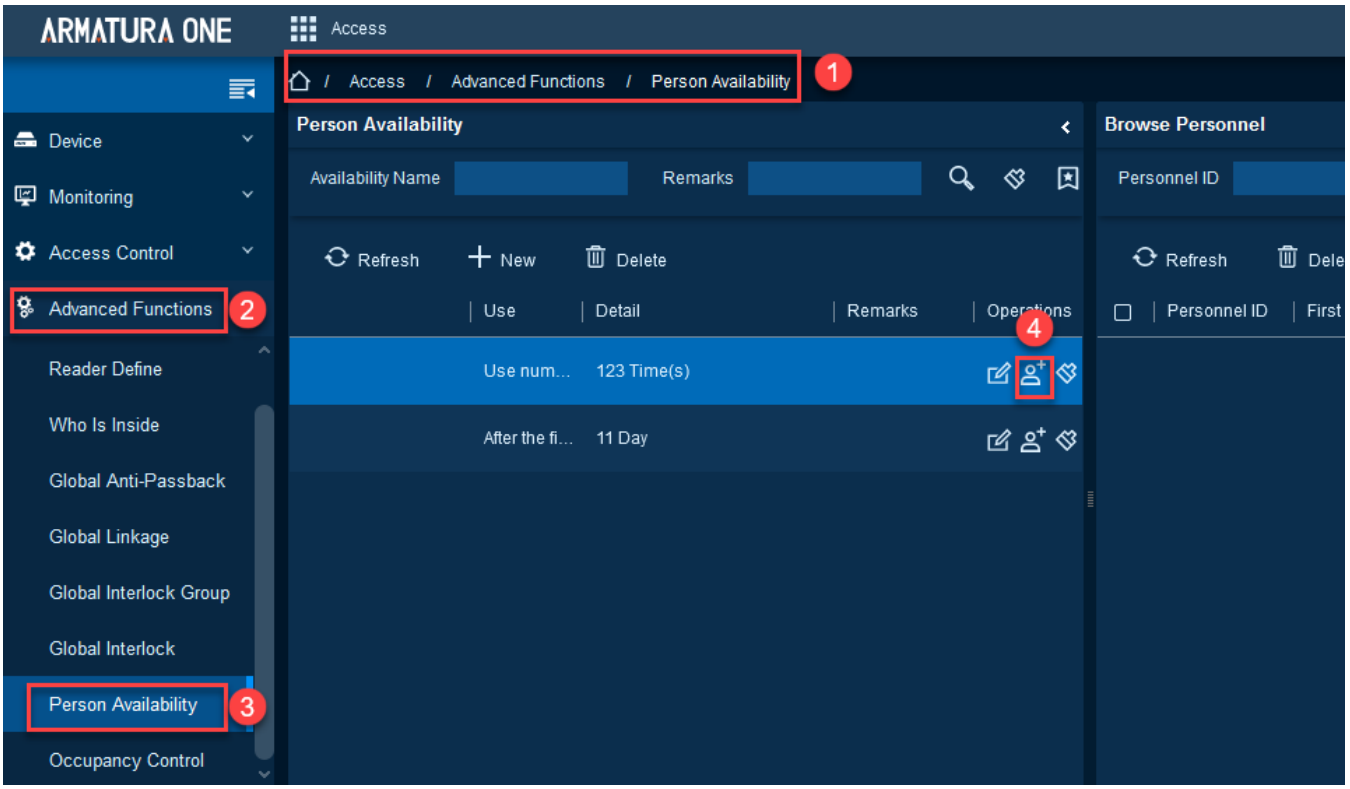
This function establishes specific access restrictions based on time periods or usage frequency for designated personnel.

Trigger Result

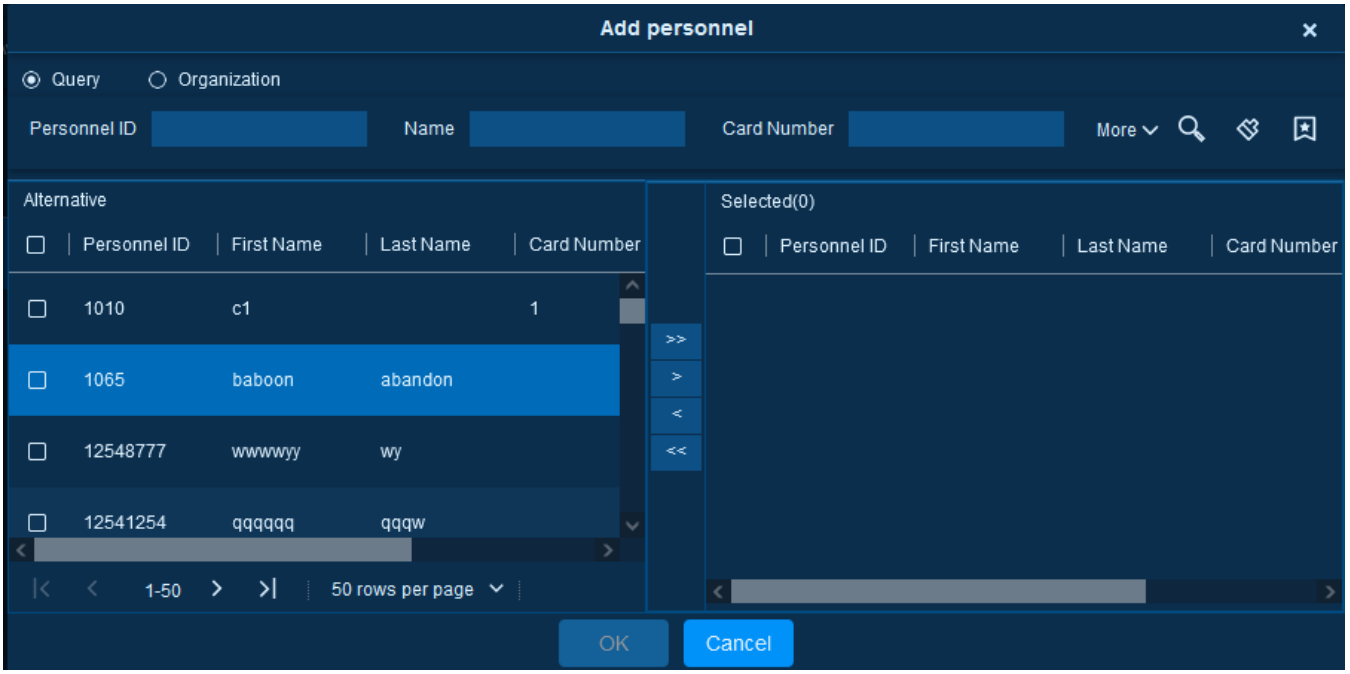
Upon completion, the system implements customized access limitations for individuals within specified control areas.

Steps:

- Navigate to **[Access]** > **[Advanced Functions]** > **[Personnel Availability]**.
- Select the personnel validity record and click **[Add Personnel]**.
- Enter details for the new personnel.
- Click **[OK]** to save.



Copyright © 2024 ARMATURA LLC. All rights reserved



Edit Personnel

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function updates existing personnel access restrictions including effective periods and usage limitations.

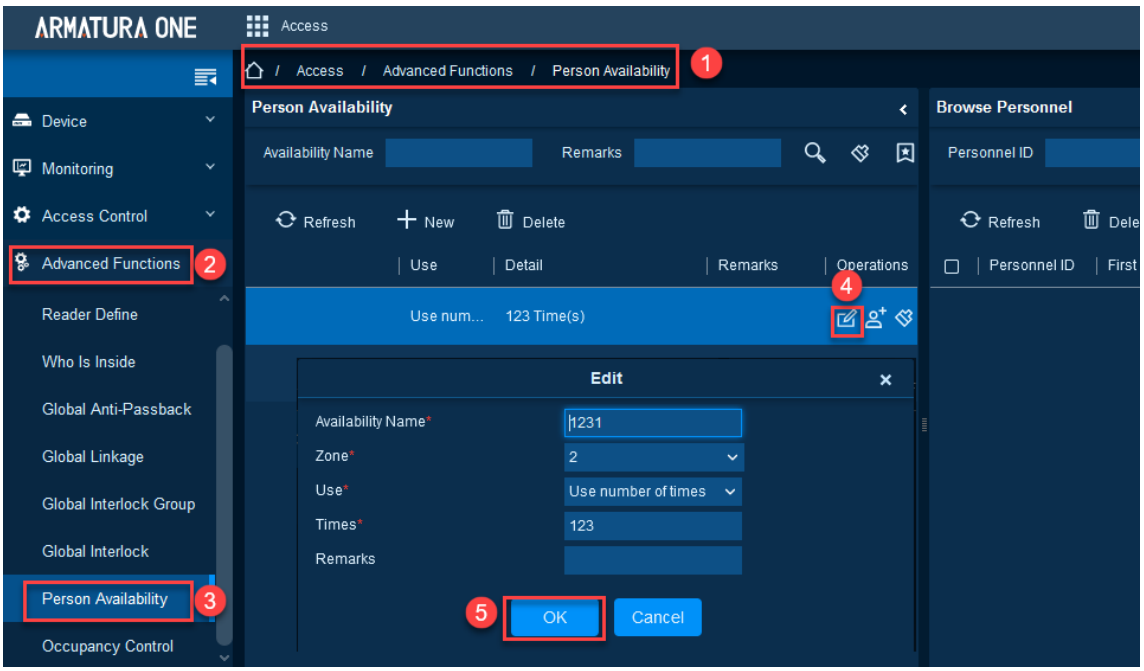
Trigger Result

Upon completion, the system implements modified access parameters for the selected personnel within control areas.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Personnel Availability]**.
- Select the personnel record to edit and click **[Edit]**.
- Update the required details and click **[OK]** to save changes.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Personnel

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function removes existing access control limitations for specified personnel.

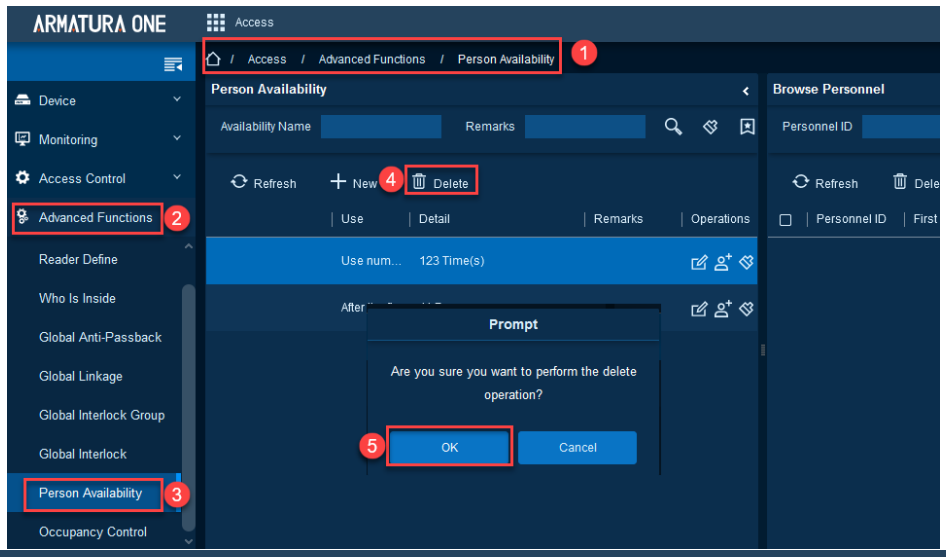
Trigger Result

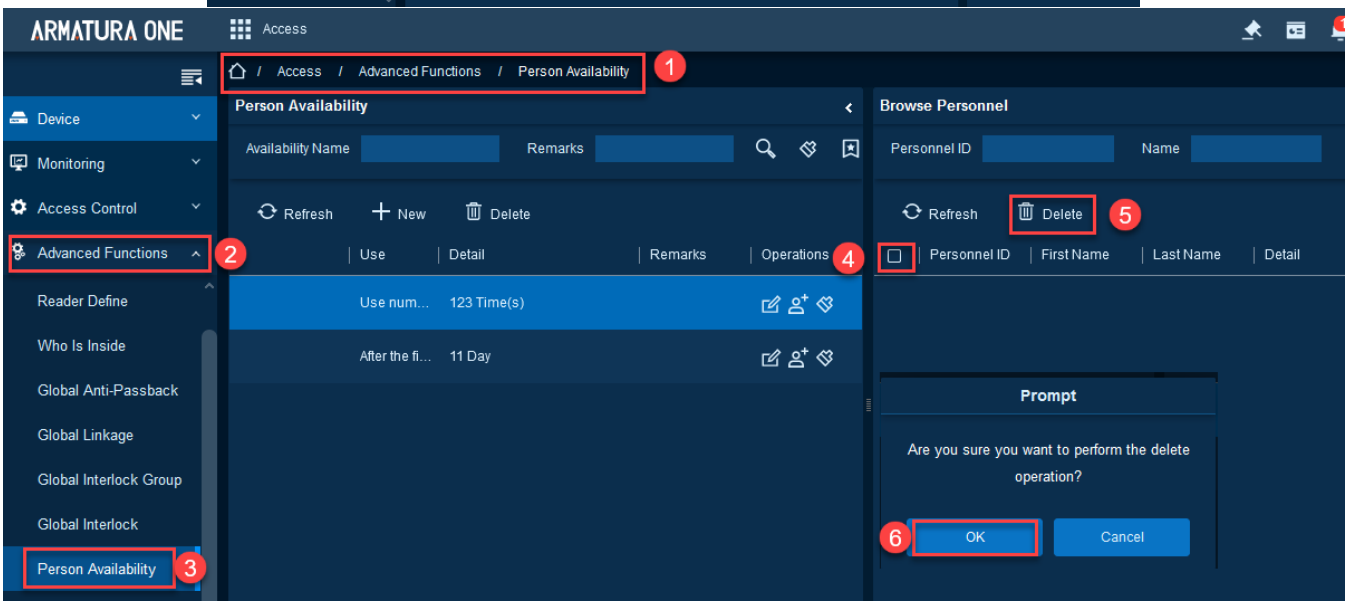
Upon completion, the system removes all access restrictions for the selected personnel within control areas.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Person Availability]**.
- Select the personnel to delete and click **[Delete]**.
- Confirm the deletion to remove the personnel's availability.

Copyright © 2024 ARMATURA LLC. All rights reserved





Reset Operation

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function clears and resets personnel availability settings when reconfiguration is needed.

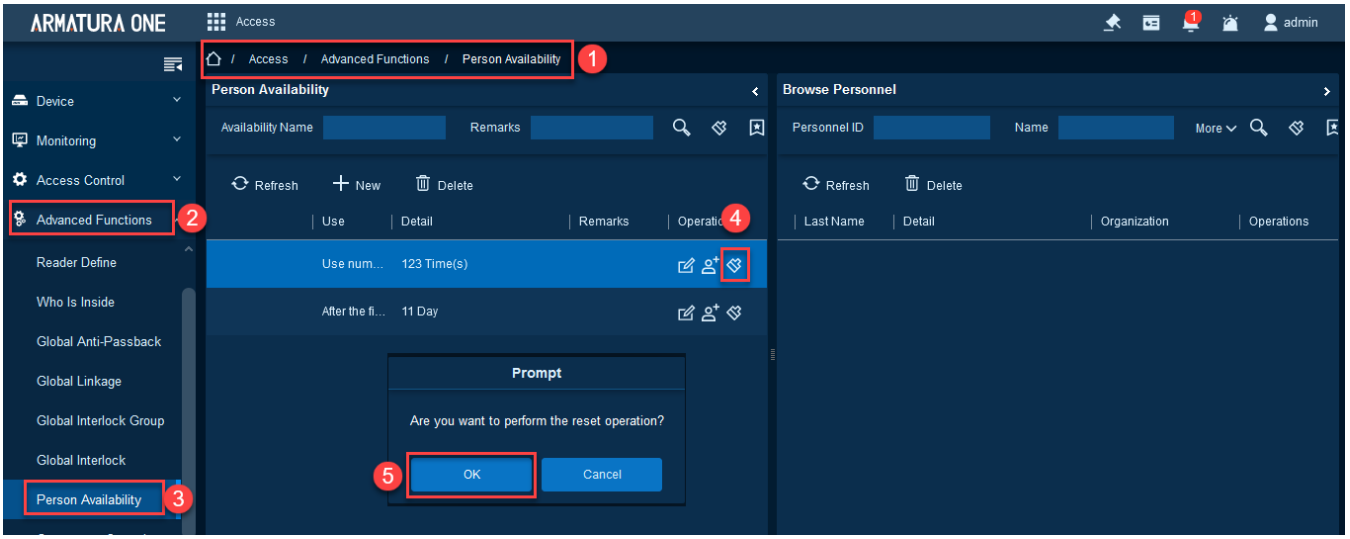
Trigger Result

Upon completion, the system restores default availability settings for the selected personnel.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Person Availability]**.
- Select the personnel availability to reset and click **[Reset]**.
- Confirm the reset operation to finalize changes.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.4.8Occupancy Control

Function Description

Occupancy Control enables management of area capacity by establishing maximum and minimum occupancy thresholds within designated spaces.

Add Number of Personnel

Prerequisites for Use

Log into the system using an account with the required permissions, ensuring that devices are properly integrated devices in the access control module, and a defined access control area.

Usage Scenarios

This function implements capacity management by setting occupancy limits for specific areas.

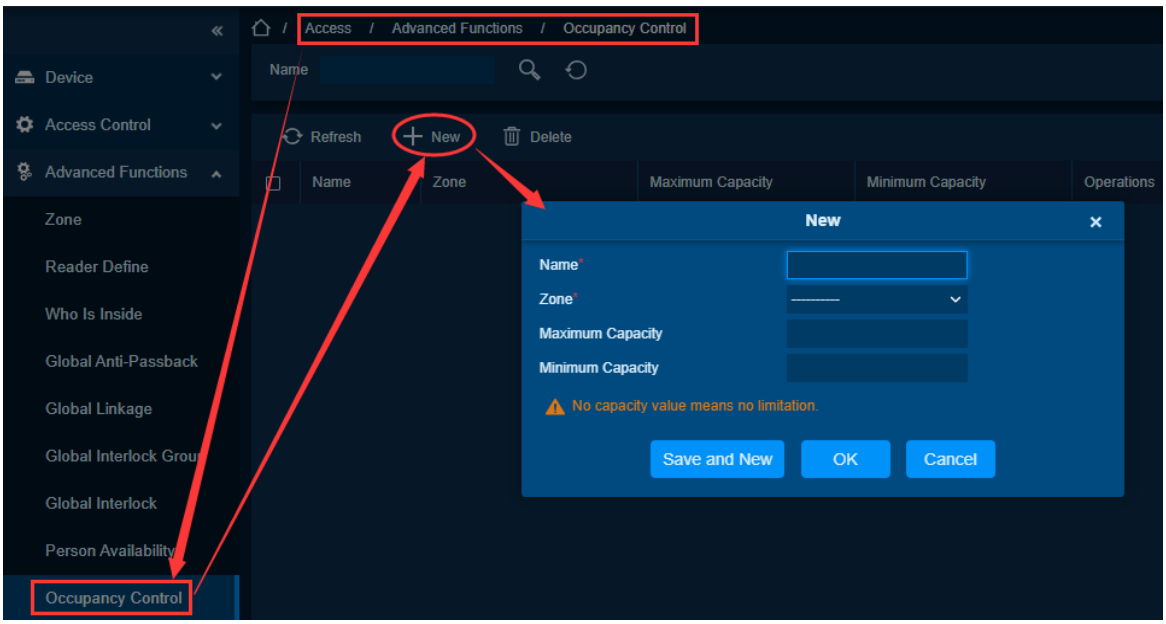
Trigger Result

Upon completion, the system enforces defined maximum and minimum occupancy parameters for the specified control area.

Steps:

- Navigate to **[Access]** > **[Advanced Functions]** > **[Occupancy Control]** > **[New]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Configure the following:

Maximum Occupancy: The upper limit of people allowed in the area.

Minimum Occupancy: The lower limit of people allowed in the area.

- Click **[OK]** to save. Personnel access will be restricted based on the defined occupancy limits.

Edit Number of Personnel

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function modifies existing occupancy thresholds for specific areas.

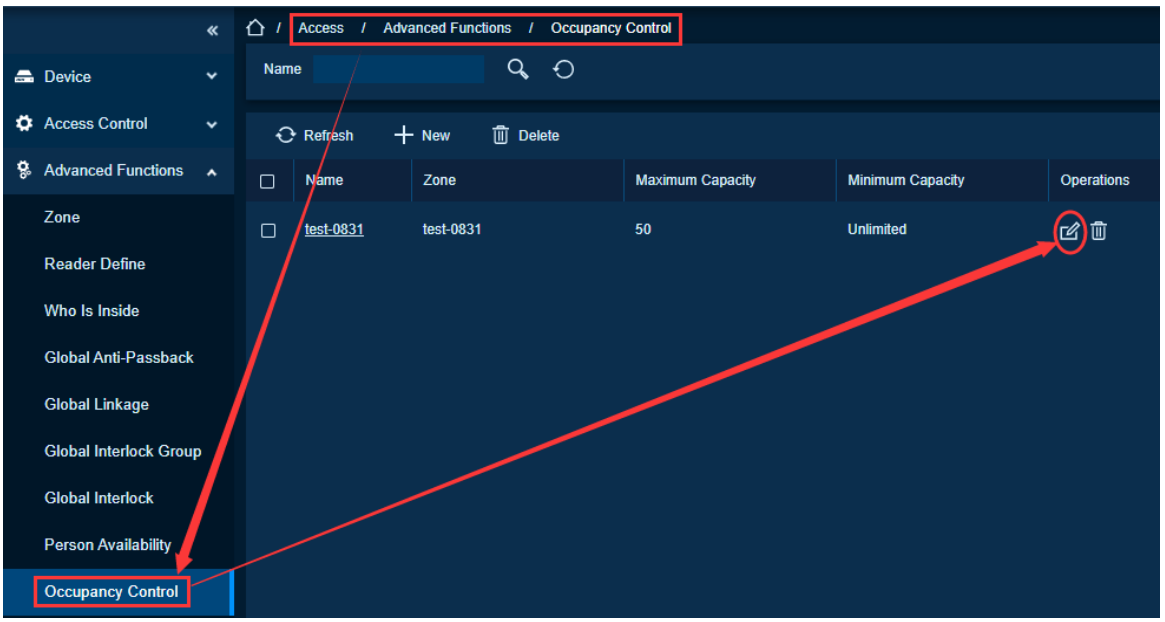
Trigger Result

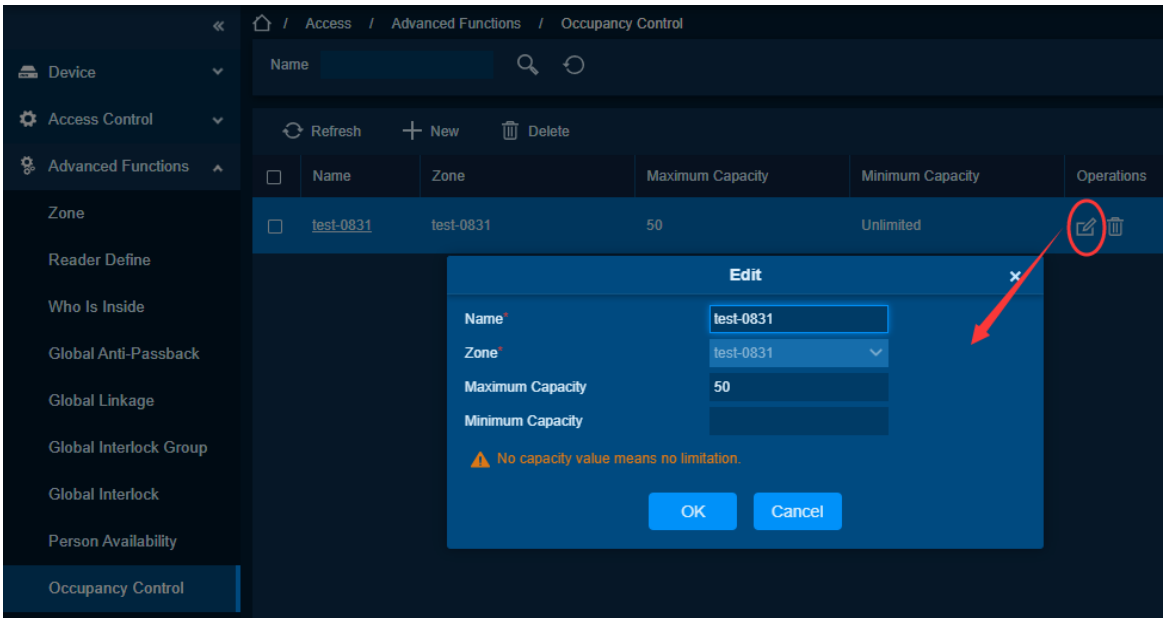
Upon completion, the system implements updated capacity limits for the designated control area.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Occupancy Control]**.
- Select the occupancy control rule to edit.
- Click **[Edit]** to open the editing interface.
- Adjust the maximum and minimum values as needed.
- Click **[OK]** to save the changes.

Copyright © 2024 ARMATURA LLC. All rights reserved





Delete Number of Personnel

Prerequisites for Use

Log into the system using an account with the required permissions, ensuring that devices are properly integrated into the access control module.

Usage Scenarios

This function removes occupancy restrictions from areas no longer requiring capacity management.

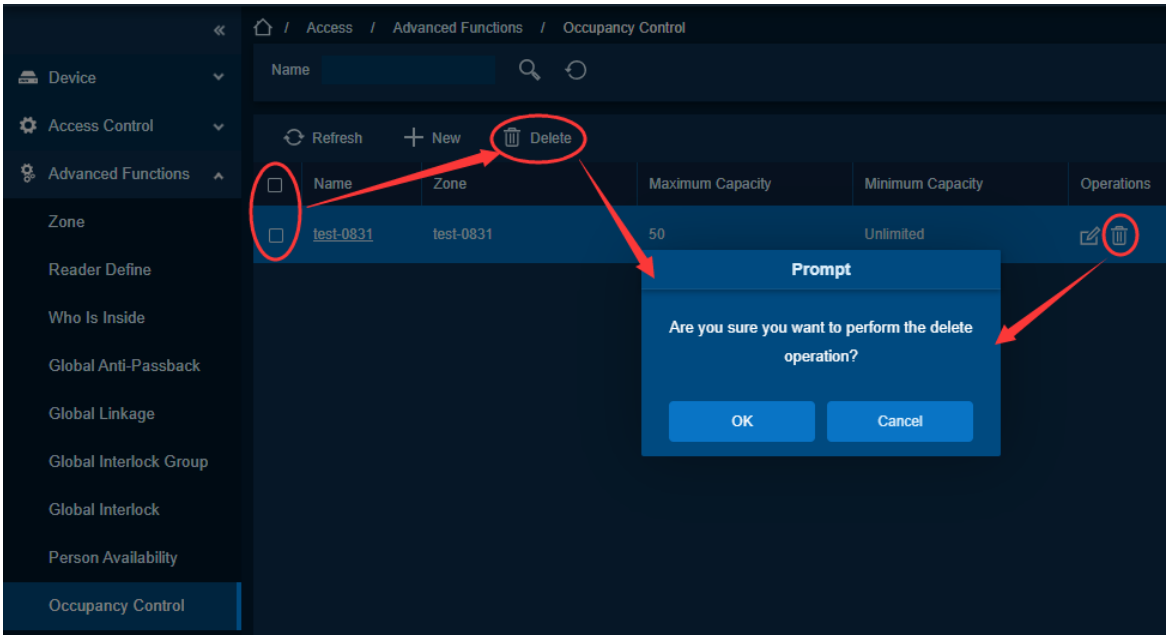
Trigger Result

Upon completion, the system disables occupancy limit controls for the specified area.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Occupancy Control]**.
- Select the occupancy control rule to delete.
- Click **[Delete]** to remove the rule.
- Confirm the deletion to finalize.



6.4.9Muster Point

Function Description

Muster Point establishes designated safe assembly locations for emergency evacuations and personnel accountability.

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function creates designated emergency assembly points for safe personnel gathering during evacuations.

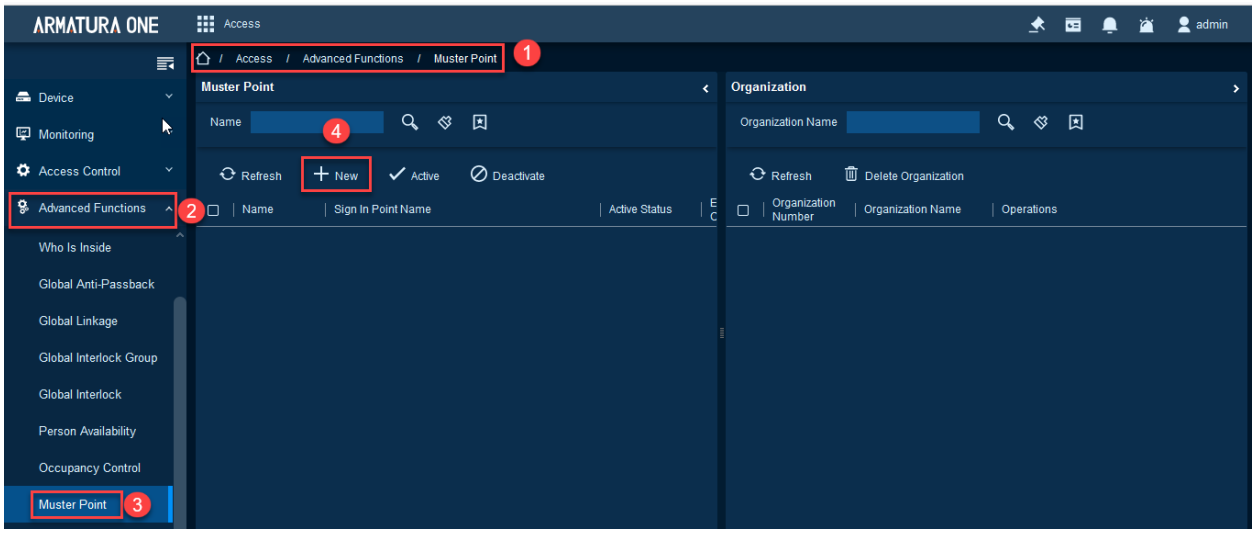
Trigger Result

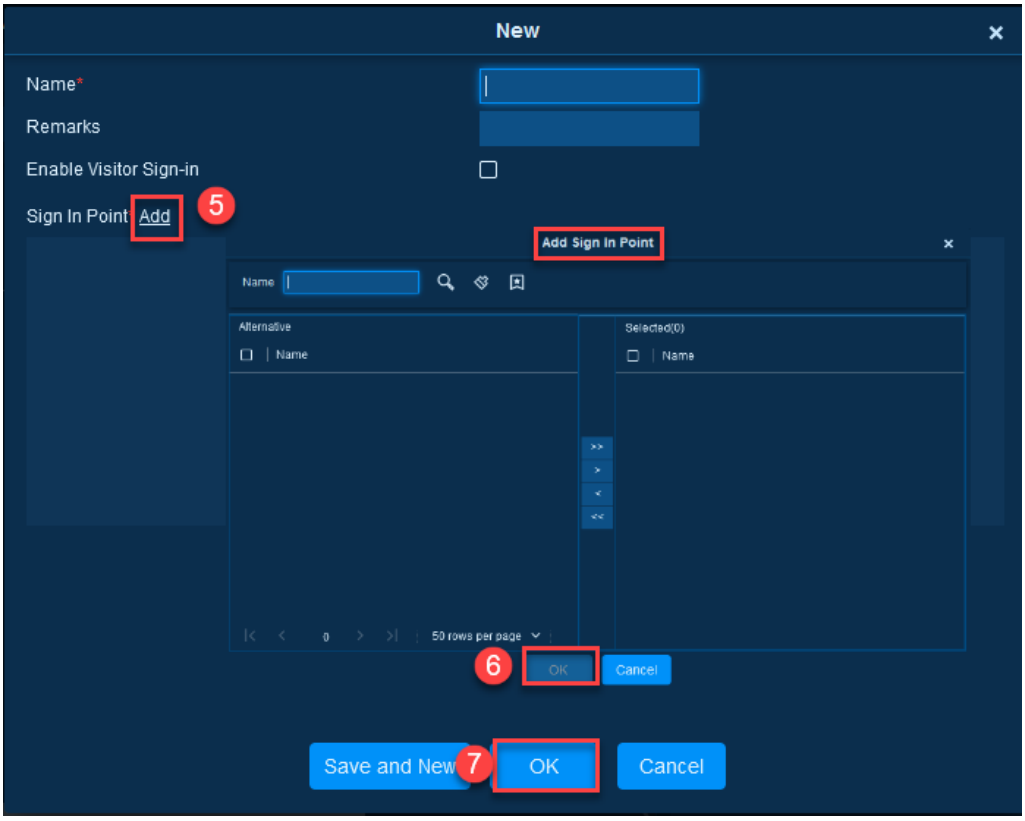
Upon completion, the system establishes a secure muster point at a safe distance from potential emergency zones.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Muster Point]**.
- Click **[New]** to open the add muster point interface.
- Enter the details of the **Sign-In Point** (e.g., location, name).
- Click **[OK]** to save the muster point.

Copyright © 2024 ARMATURA LLC. All rights reserved



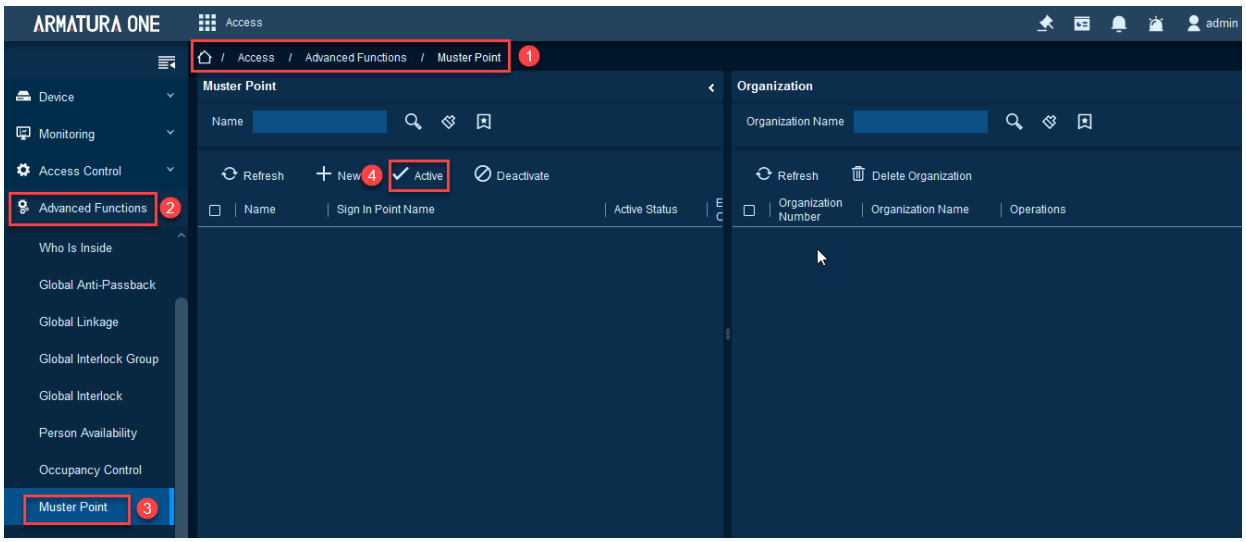


Activate Muster Point

Steps

- Navigate to **[Access] > [Advanced Functions] > [Muster Point]**.
- Select the muster point to activate.
- Click **[Activate]**, and a pop-up window will appear.
- Click **[OK]** to confirm activation.

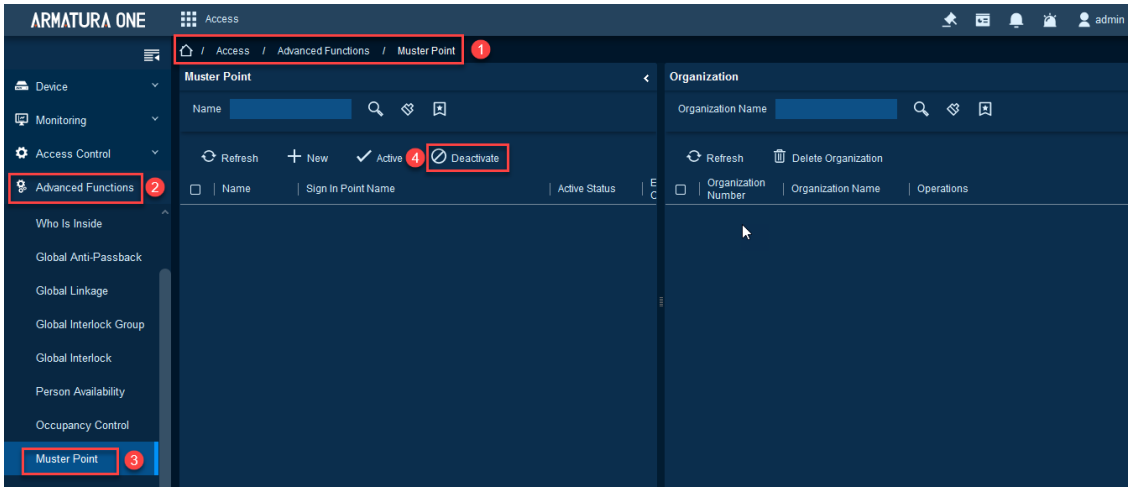
Copyright © 2024 ARMATURA LLC. All rights reserved



Deactivate Muster Point

Steps

- Navigate to **[Access]** > **[Advanced Functions]** > **[Muster Point]**.
- Select the muster point to deactivate.
- Click **[Deactivate]**, and a pop-up window will appear.
- Click **[OK]** to confirm deactivation.

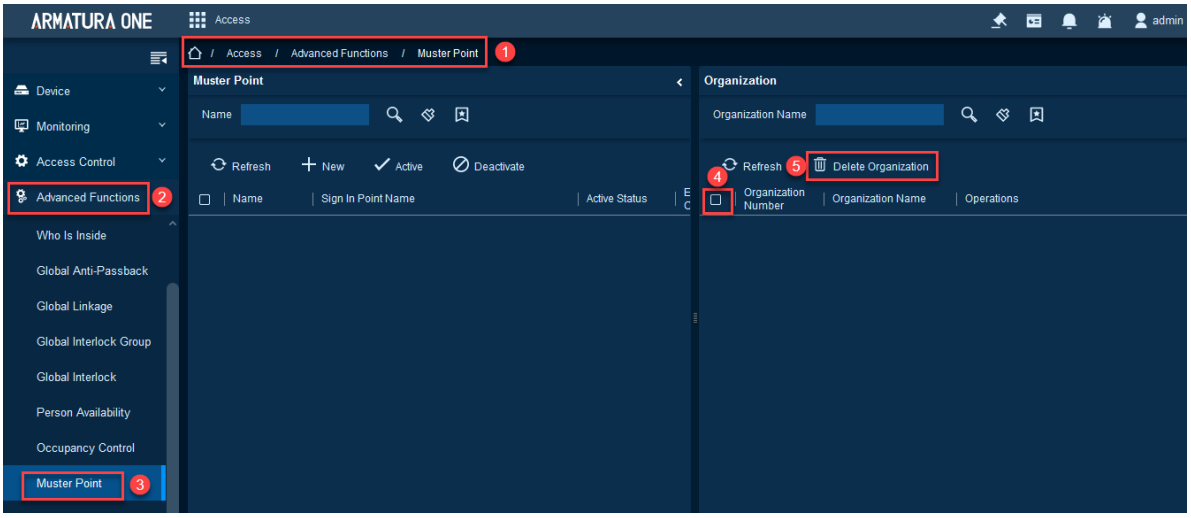


Delete Muster Point

Steps

- Navigate to **[Access] > [Advanced Functions] > [Muster Point]**.
- Select the muster point or the person associated with the muster point to delete.
- Click **[Delete]** to enter the delete interface.
- Confirm the deletion to remove the muster point.

Copyright © 2024 ARMATURA LLC. All rights reserved



6.4.10 Muster Point Report

Function Description

Muster Point Report generates comprehensive records of muster point activities, including manual sign-in tracking and data export capabilities for emergency response analysis.

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function enables manual recording of personnel check-ins at designated muster points during emergency situations.

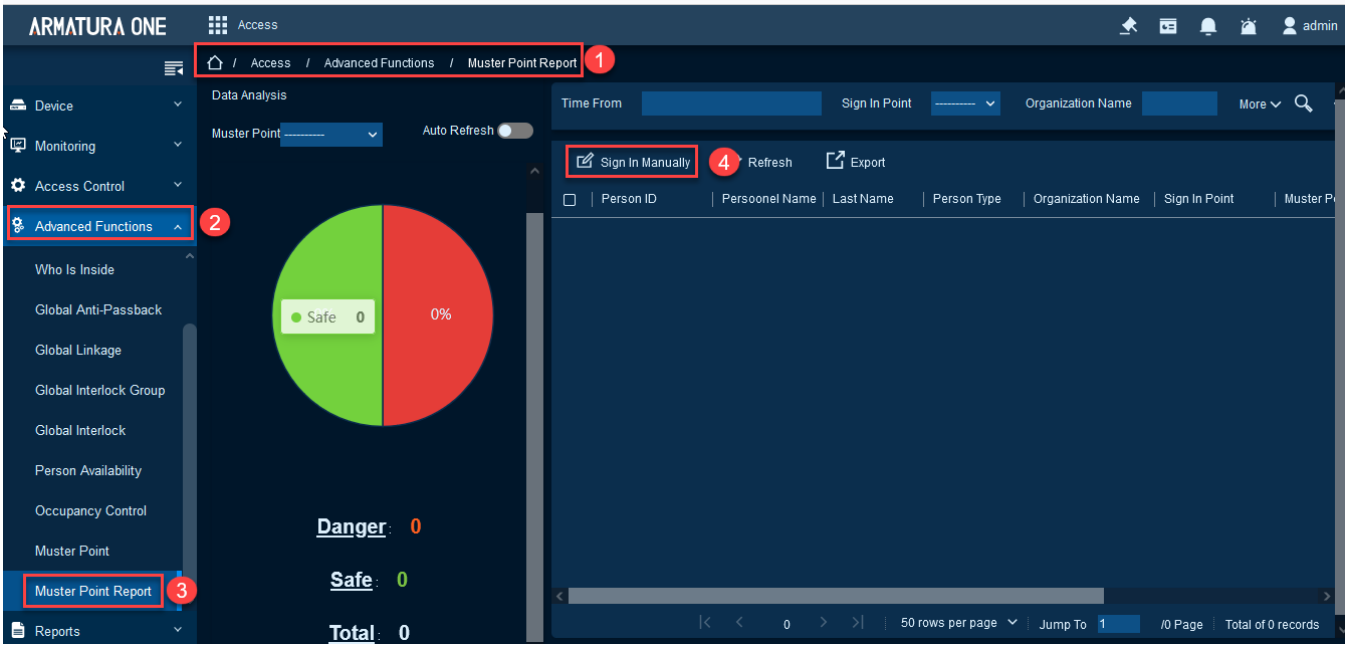
Trigger Result

Upon completion, the system documents individual sign-in events at specified muster points.

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Muster Point Report]**.
- Access the **Muster Point Report** interface.
- Use the available functionality to record manual sign-ins.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

This function enables export of access control and muster point activity records for analysis and documentation.

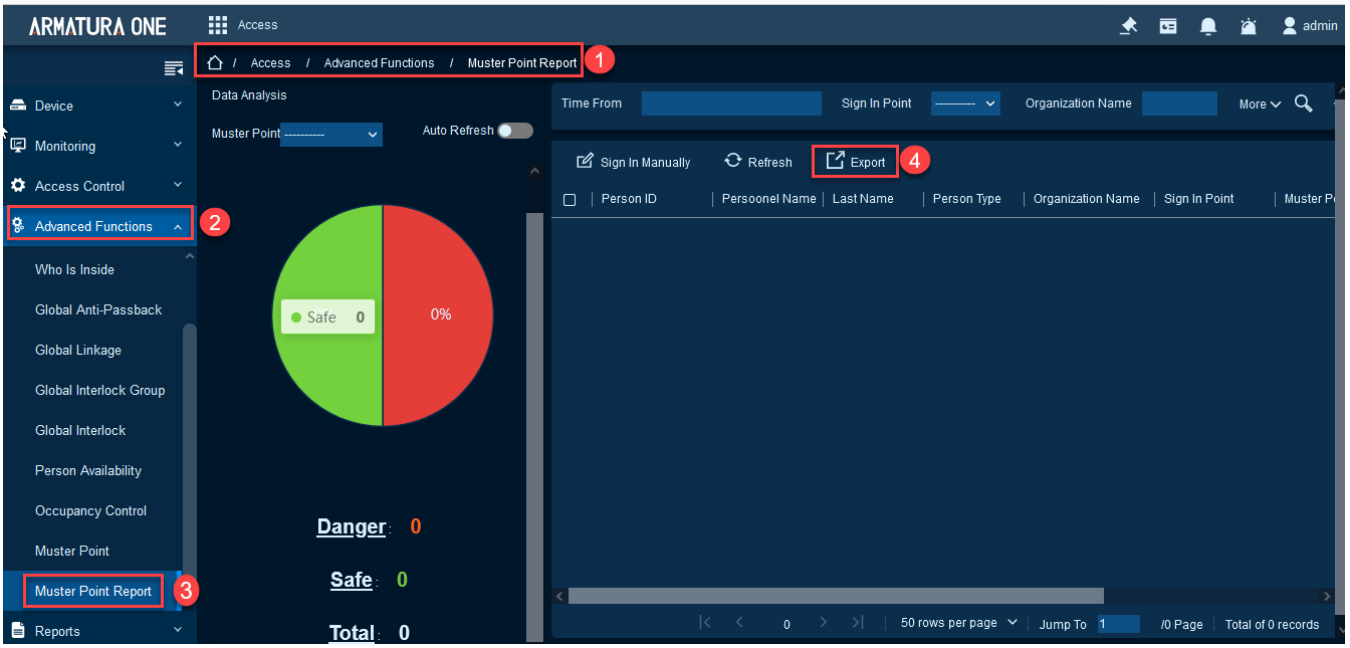
Trigger Result

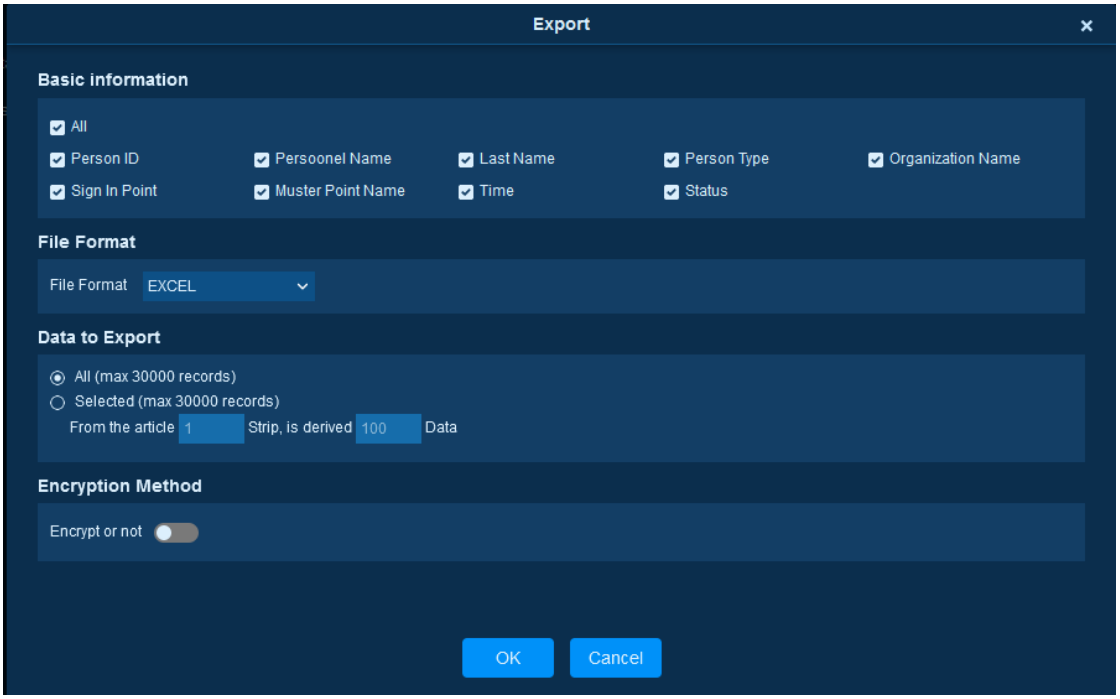
Upon completion, the system generates a comprehensive data file in the selected format (Excel, PDF, or CSV).

Steps:

- Navigate to **[Access] > [Advanced Functions] > [Muster Point Report]** to open the report interface.
- Click **[Export]** to open the export options.
- Select the desired file format (Excel, PDF, CSV) and confirm to export the data.

Copyright © 2024 ARMATURA LLC. All rights reserved





Copyright © 2024 ARMATURA LLC. All rights reserved

6.5 Reports

Function List

Functions	Description
All Records	Includes all records.
Today's Visit Record	Contains all visit records for the current day.
All Exception Records	Displays all exception records.
Query by Door	Provides the basic information of all personnel associated with specific doors.
Query by Personnel	Displays detailed query information for specific personnel.
Personnel Entry and Exit Records	Tracks and lists personnel entry and exit records.
Device Log	Displays detailed logs of device operations.
Device Face Extraction Failure Log	Contains details about failed face extraction attempts by devices.
Access Control Alarm Record	Contains detailed records of access control alarms.

Export

Function Description

The Export function enables report generation and download based on specific query criteria. Reports can include comprehensive transaction data, current day events, or exception events.

Use Cases

The function supports statistical analysis of device data including card verifications, door operations, and standard access records. Users can filter data by various verification modes: Only Card, Only Fingerprint, Only Password, Card plus Password, Card plus Fingerprint, and Card or Fingerprint.

Note:

Event records generated using an **emergency password** to open doors will only include the **password verification mode**.

Copyright © 2024 ARMATURA LLC. All rights reserved

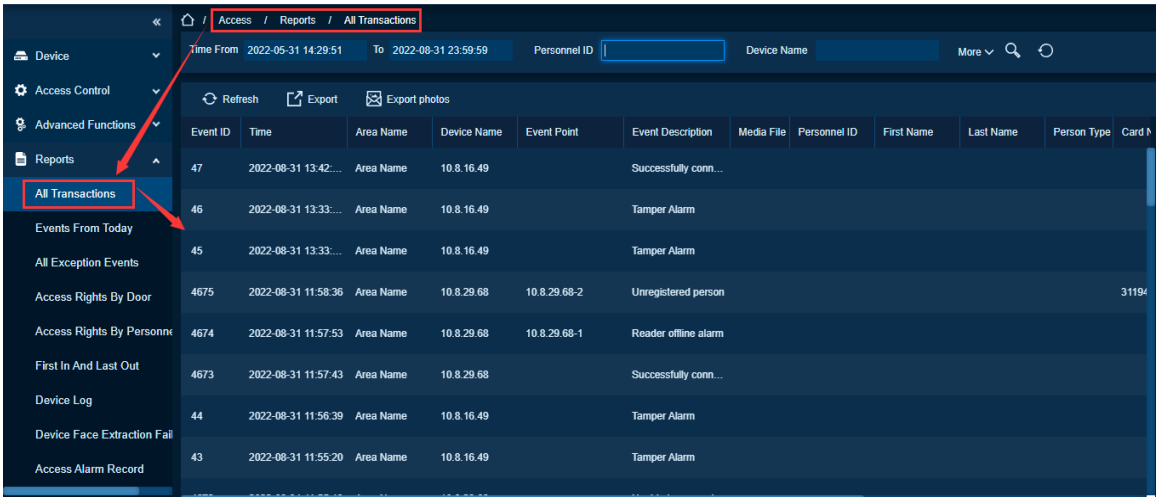
6.5.1All Transactions

Function Description

The All Transactions report enables users to view and filter access control event records based on specified conditions. Due to the large volume of event records, the system defaults to displaying data from the latest three months when querying.

View All Transactions

- Navigate to **[Access] > [Reports] > [All Transactions]**.
- Use filters to refine the displayed records based on: Date Range, Device, Personnel, and Event Types.



Export

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

When users need access to all event records in a downloadable file format for analysis or storage.

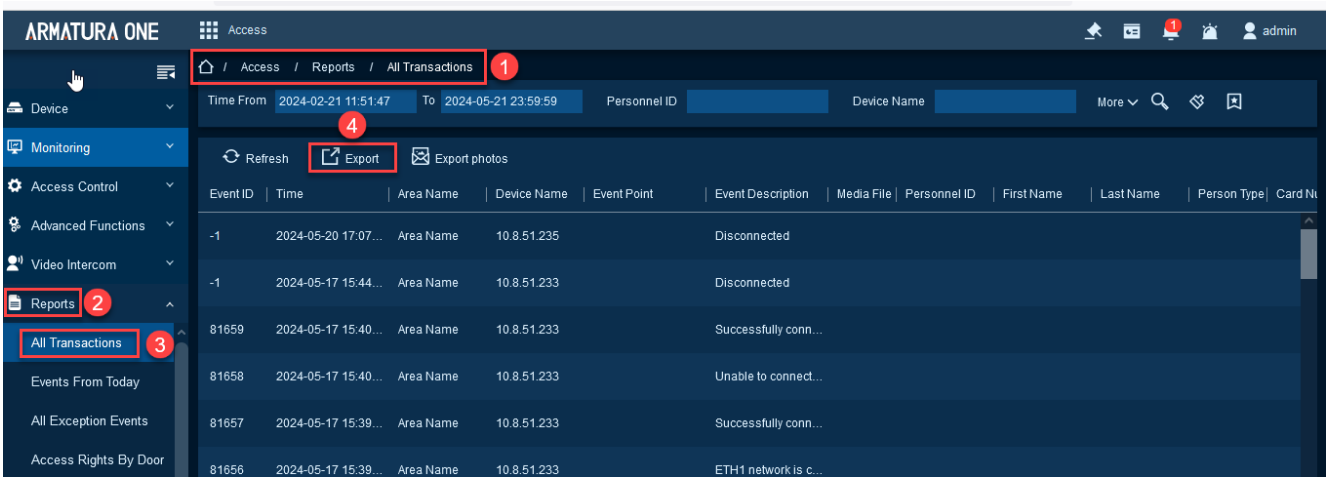
Trigger Result

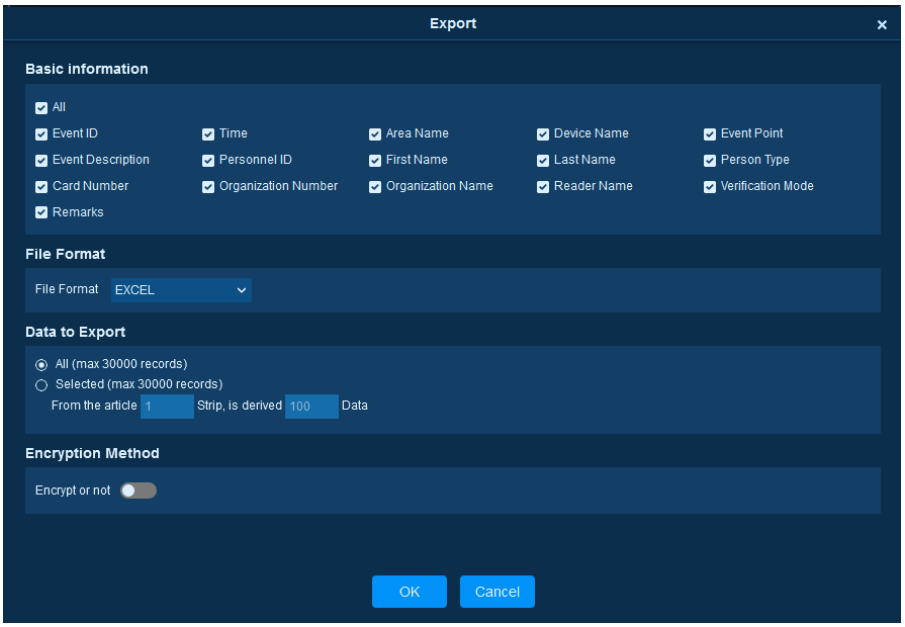
Export all transaction records in Excel, PDF, or CSV format.

Steps:

- Navigate to **[Access] > [Reports] > [All Transactions]** to display the list of access control records.
- Click **[Export]**.
- Select the desired file format (**Excel/PDF/CSV**) and download the report.

Copyright © 2024 ARMATURA LLC. All rights reserved





Export Photos

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Users need a consolidated view of all photos related to access control events within a specific timeframe or device.

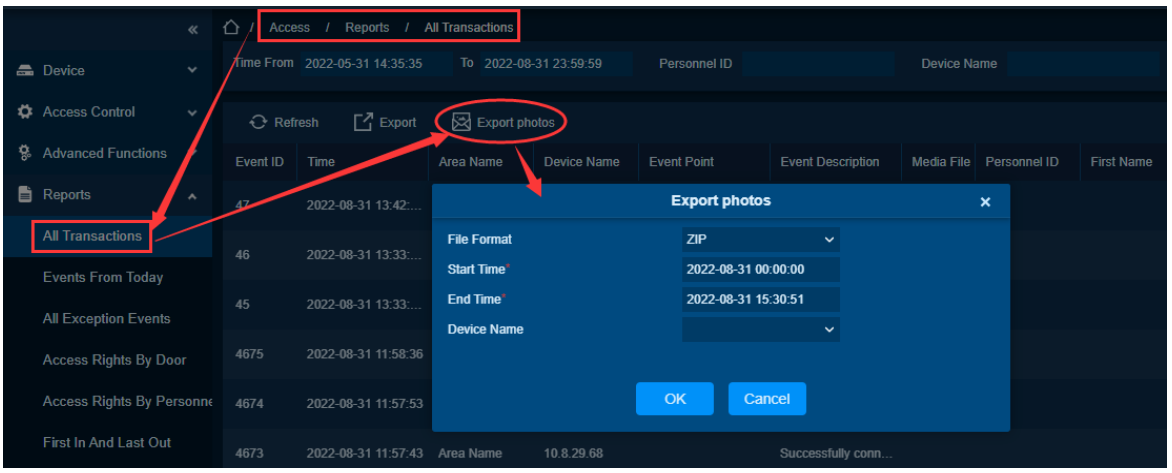
Trigger Result

Export all photos associated with access control event records.

Steps:

- Navigate to **[Access] > [Reports] > [All Transactions]**.
- Click **[Export Photos]** to initiate the export process.
- Save the photos for further review or analysis.

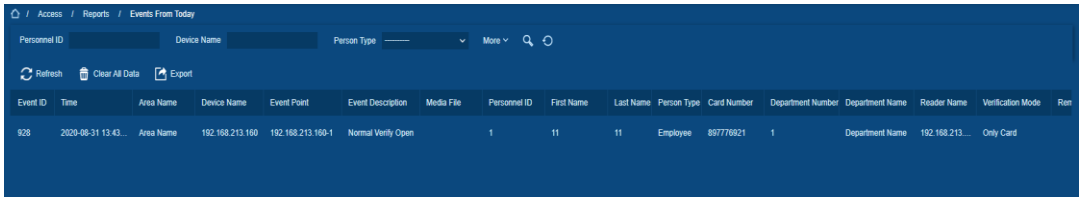
Copyright © 2024 ARMATURA LLC. All rights reserved



6.5.2Events From Today

Function Description

The Events From Today report allows users to view and manage system event records generated on the current day. It provides an overview of all access control activities that occurred today. Navigate to **[Access] > [Reports] > [Events From Today]**. The system will display a list of all access control records for the current day.



Export Today's Records

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Quickly access and export records of today's activities for audit, review, or reporting purposes.

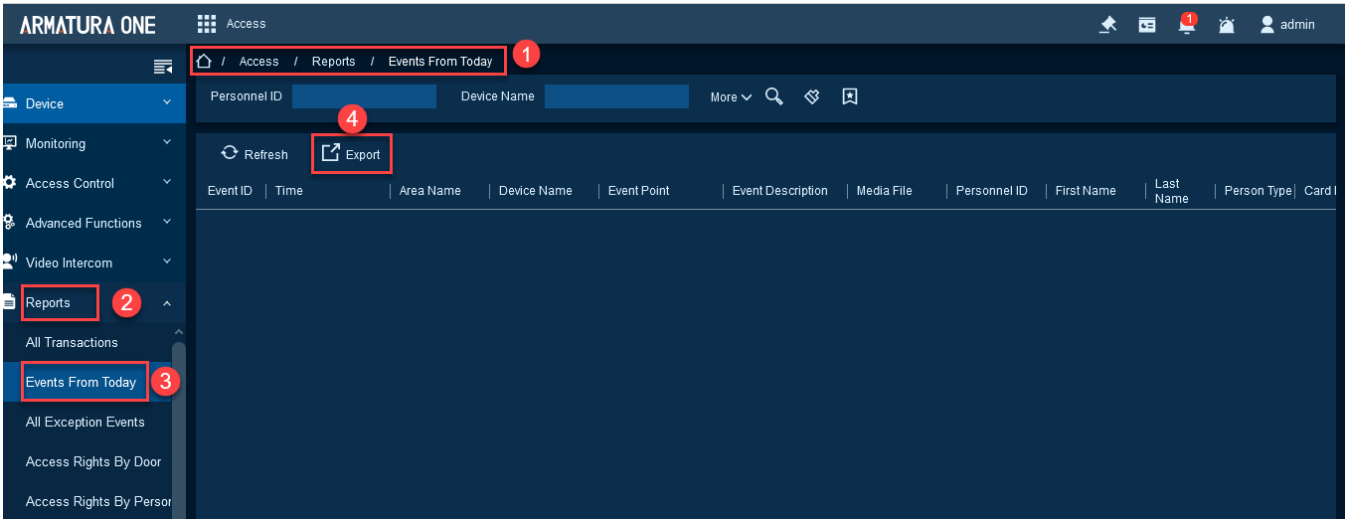
Trigger Results

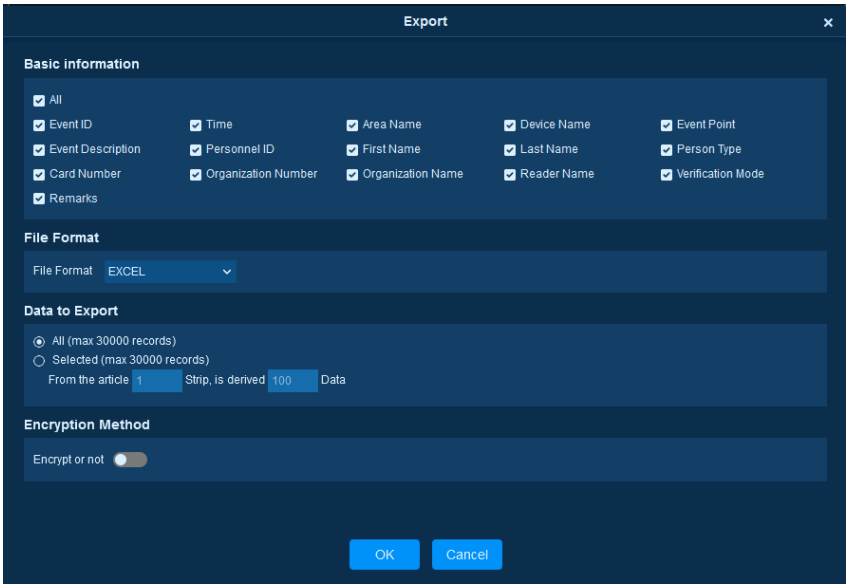
Export all records from today into Excel, PDF, or CSV file formats.

Steps:

- Navigate to **[Access]** > **[Reports]** > **[Events From Today]**.
- Click **[Export]**.
- Select the desired export format (Excel/PDF/CSV).
- Download the exported file for review or storage.

Copyright © 2024 ARMATURA LLC. All rights reserved



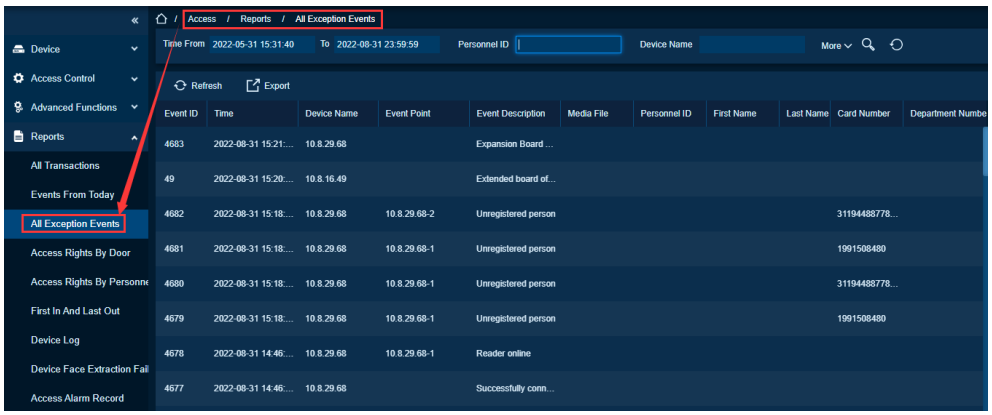


6.5.3All Exception Events

Function Description

The **All Exception Events** report allows users to review records of all abnormal or exceptional events. These records include detailed information such as the time of the event, a description of the event, and information about the personnel involved. Navigate to **[Access] > [Reports] > [All Exception Events]**. Specify conditions to filter the exception events, similar to the options in **[All Transactions]**. View the resulting list of all abnormal event records, which includes: **Event Generation Time, Event Description, Personnel Information**

Copyright © 2024 ARMATURA LLC. All rights reserved



Export Exception Records

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

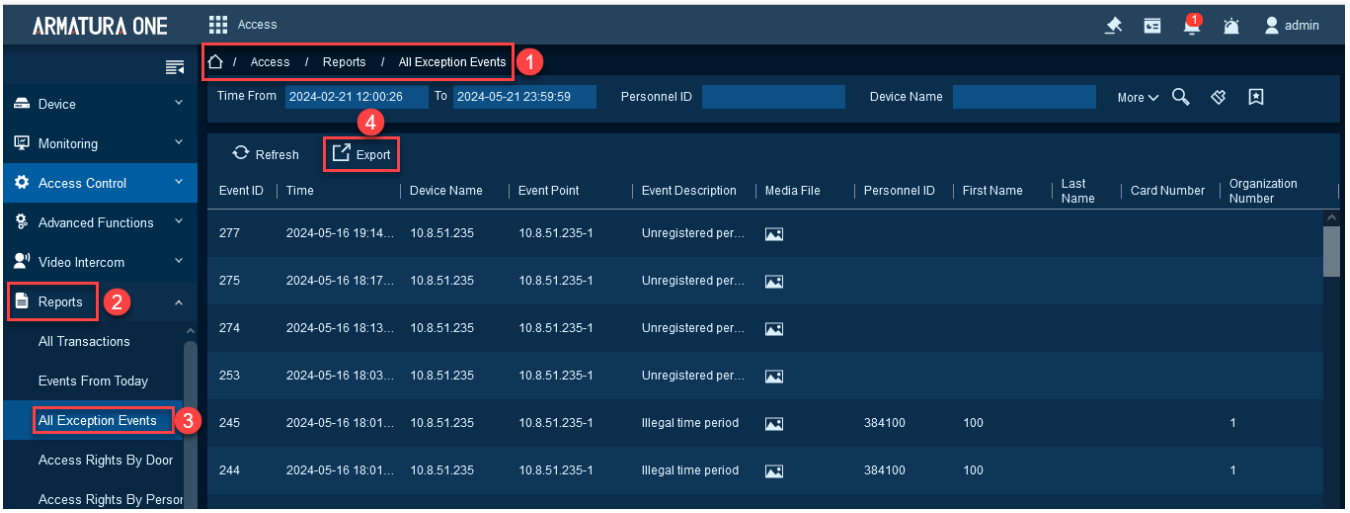
Export and store exception records for audits, analysis, or compliance reporting.

Trigger Results

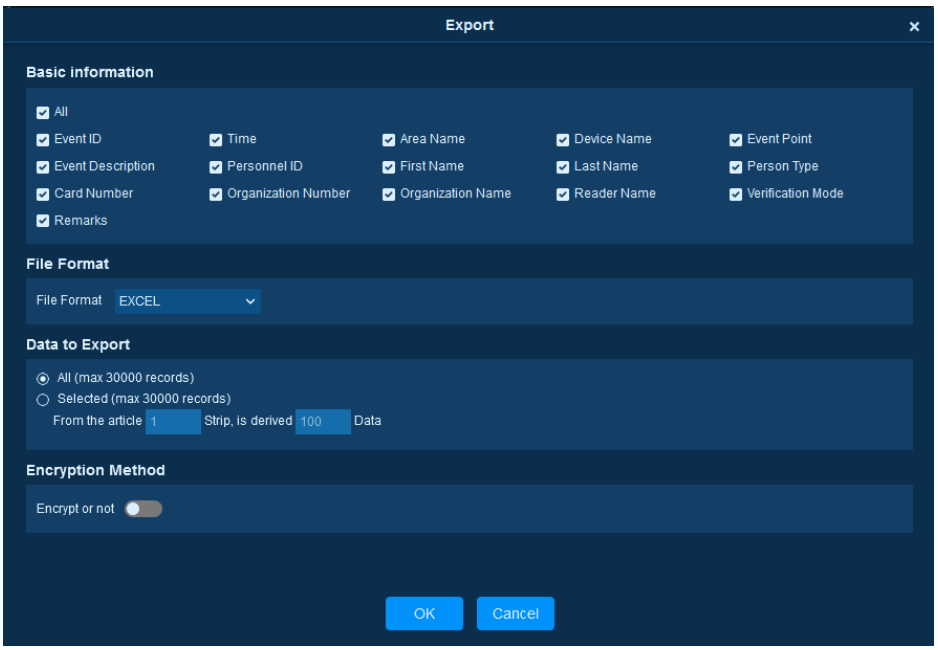
Export all abnormal records into file formats such as **Excel**, **PDF**, or **CSV**.

Steps:

- Navigate to **[Access]** > **[Reports]** > **[All Exception Events]**.
- Click **[Export]**.
- Choose the desired file format (Excel, PDF, CSV).
- Download and save the exported file for further use.



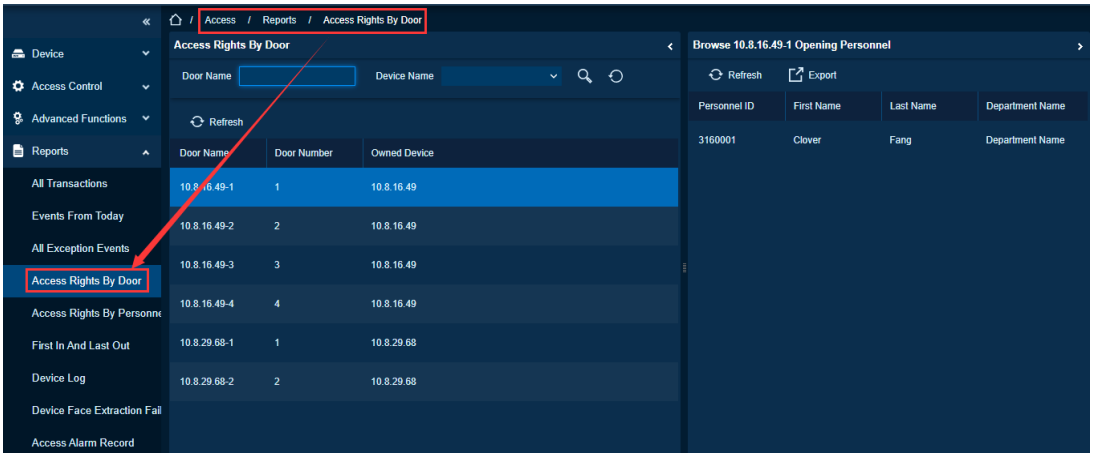
Copyright © 2024 ARMATURA LLC. All rights reserved



6.5.4Access Rights by Door

Function Description

View access levels associated with a specific door. On selecting a door, the personnel with access levels to that door will be displayed. Navigate to **[Access] > [Reports] > [Access Rights by Door]**. On the left, select a door from the list of all doors in the system. On the right, view personnel having access to the selected door.



Export

Prerequisites for Use

Log into the system using an account with the required permissions.

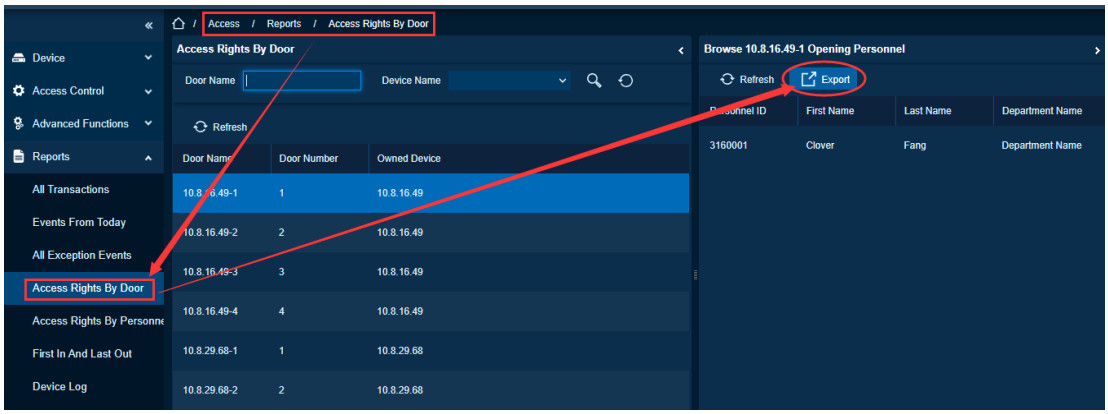
Trigger Result

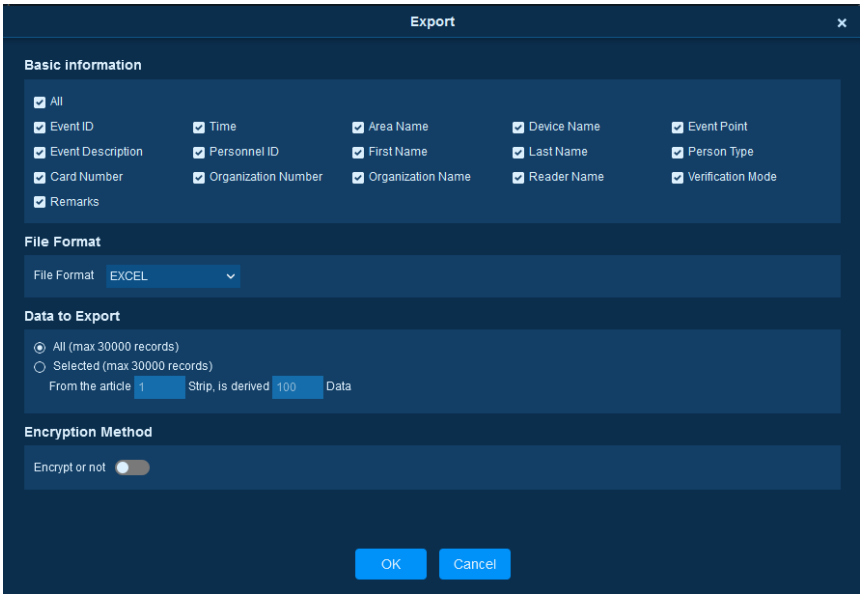
Export personnel information (names, departments, contact details) associated with the selected door to an **Excel/PDF/CSV** file.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Access]** > **[Reports]** > **[Access Rights by Door]**.
- Click **[Export]** in the operation bar to export personnel data.



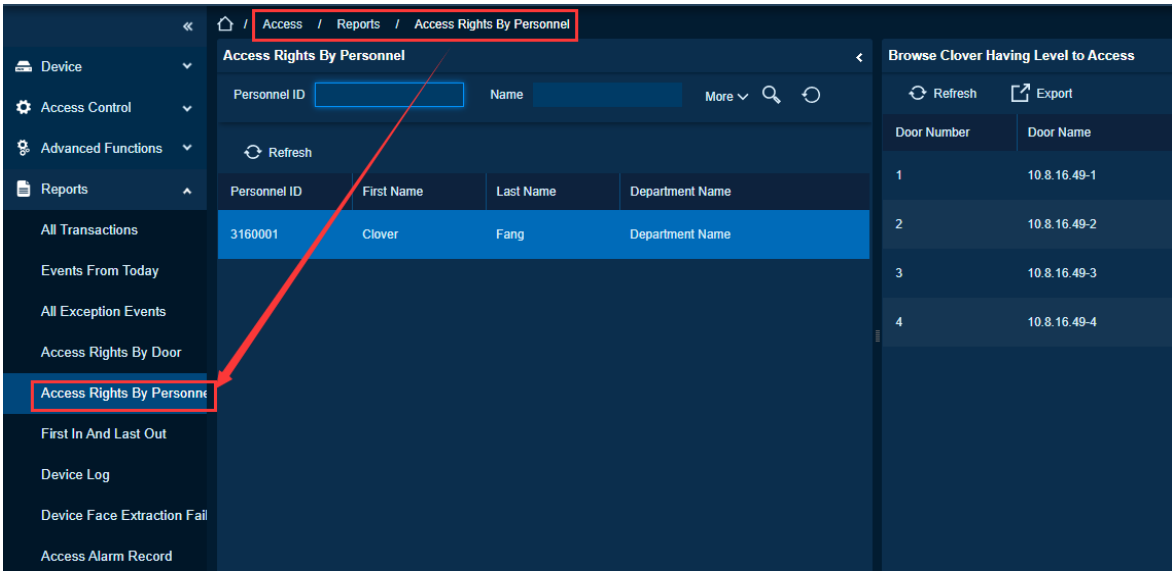


6.5.5Access Rights by Personnel

Function Description

View access levels associated with each personnel and their permitted doors. Navigate to **[Access] > [Reports] > [Access Rights by Personnel]**. Select a personnel record on the left. On the right, view the doors they can access.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export

Prerequisites for Use

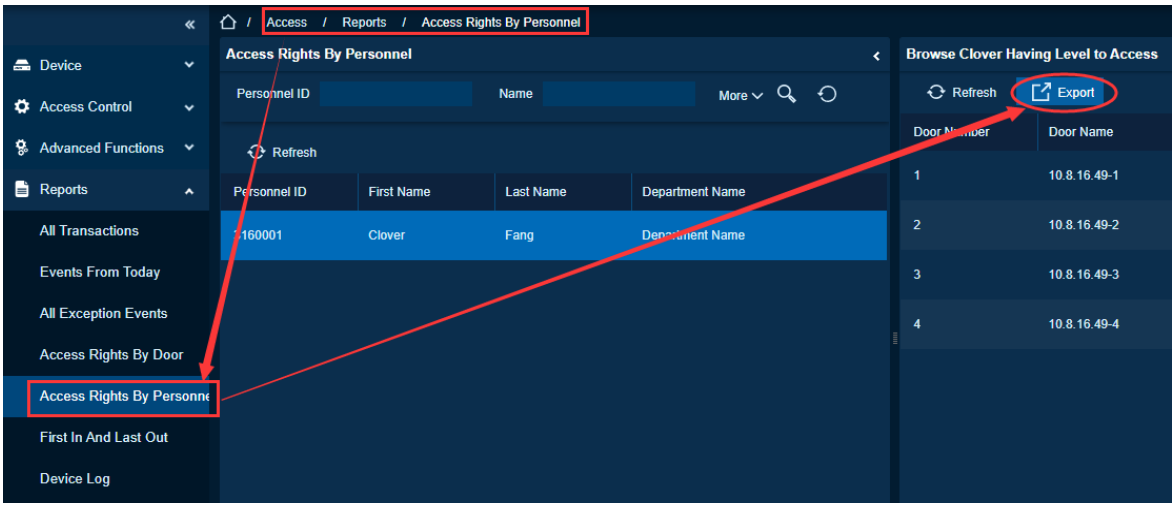
Log into the system using an account with the required permissions.

Usage Scenarios

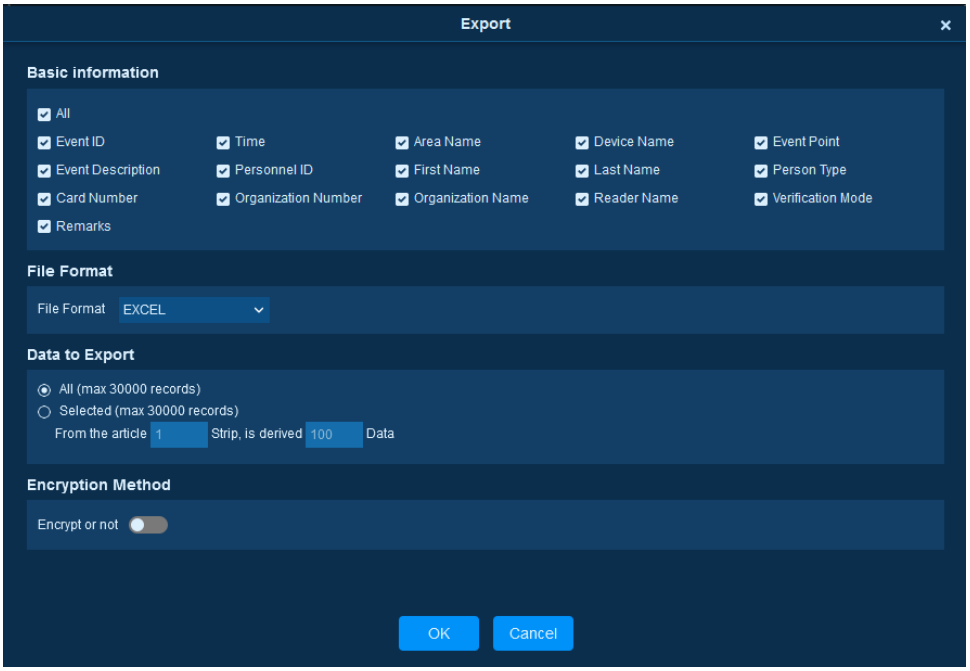
Export the list of doors that the personnel can access to an **Excel/PDF/CSV** file.

Steps:

- Navigate to **[Access] > [Reports] > [Access Rights by Personnel]**.
- Click **[Export]** in the operation bar.



Copyright © 2024 ARMATURA LLC. All rights reserved



6.5.6First In and Last Out

Export

Prerequisites for Use

Log into the system using an account with the required permissions.

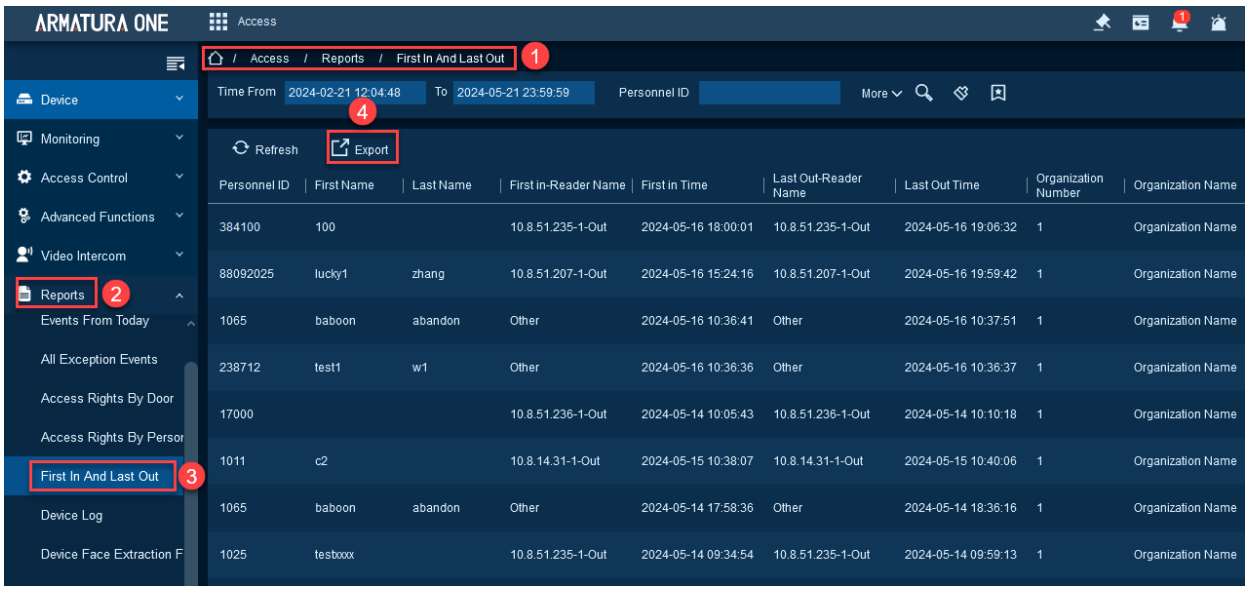
Usage Scenarios

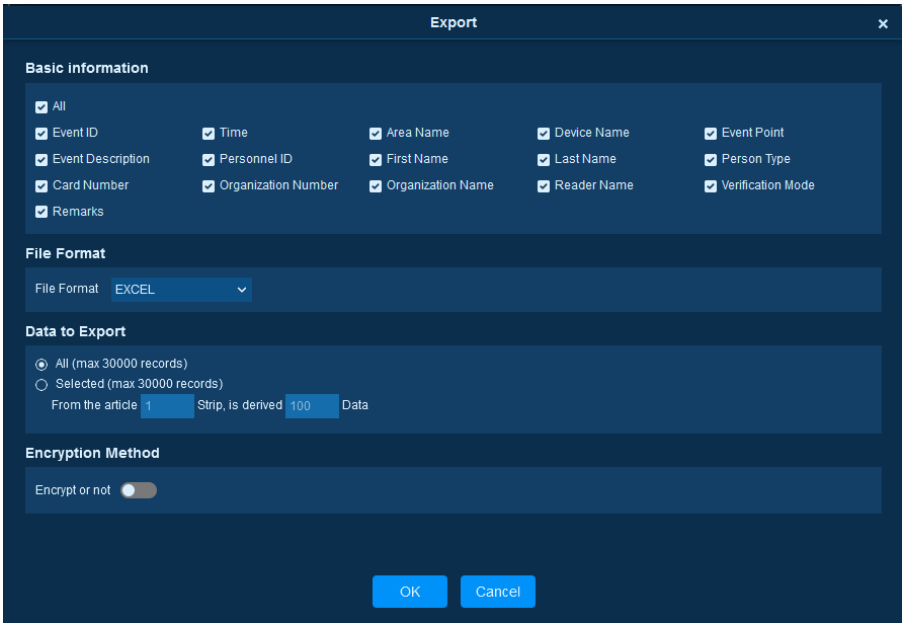
Export personnel entry and exit records, including their first entry and last exit times, into **Excel/PDF/CSV** format.

Steps:

- Navigate to **[Access] > [Reports] > [First In And Last Out]**.
- View the status table of personnel access.
- Click **[Export]**.

Copyright © 2024 ARMATURA LLC. All rights reserved





Copyright © 2024 ARMATURA LLC. All rights reserved

6.5.7 Device Log

Function Description

Displays all operation logs for devices, including details about operating users, events, and associated devices.

Export

Prerequisites for Use

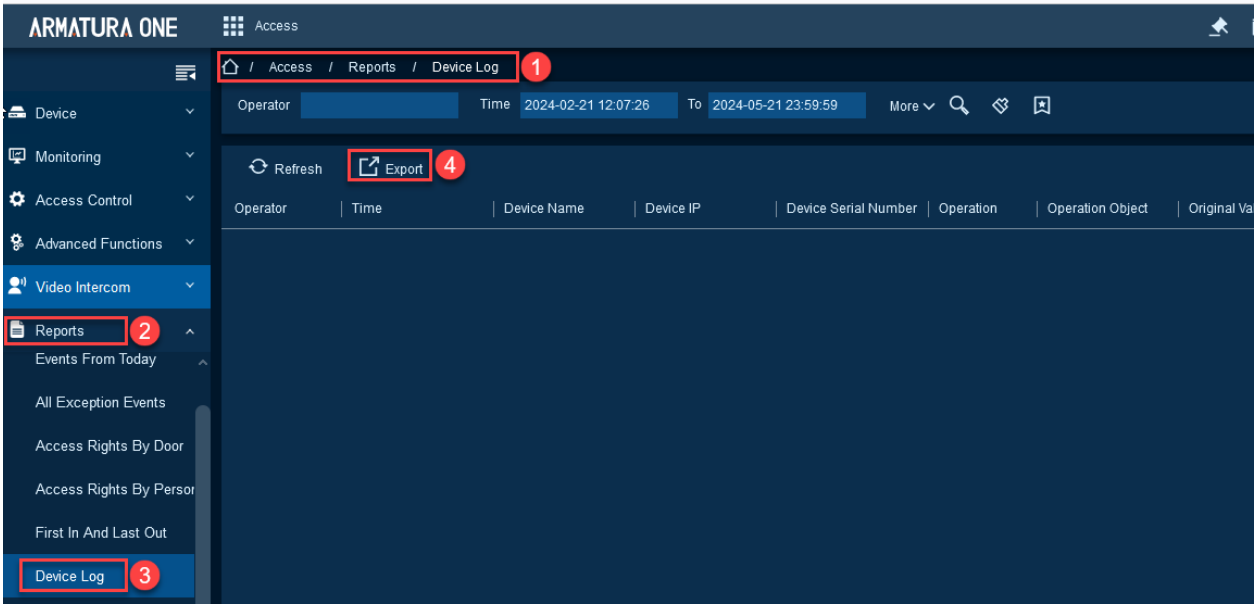
Log into the system using an account with the required permissions.

Trigger Result

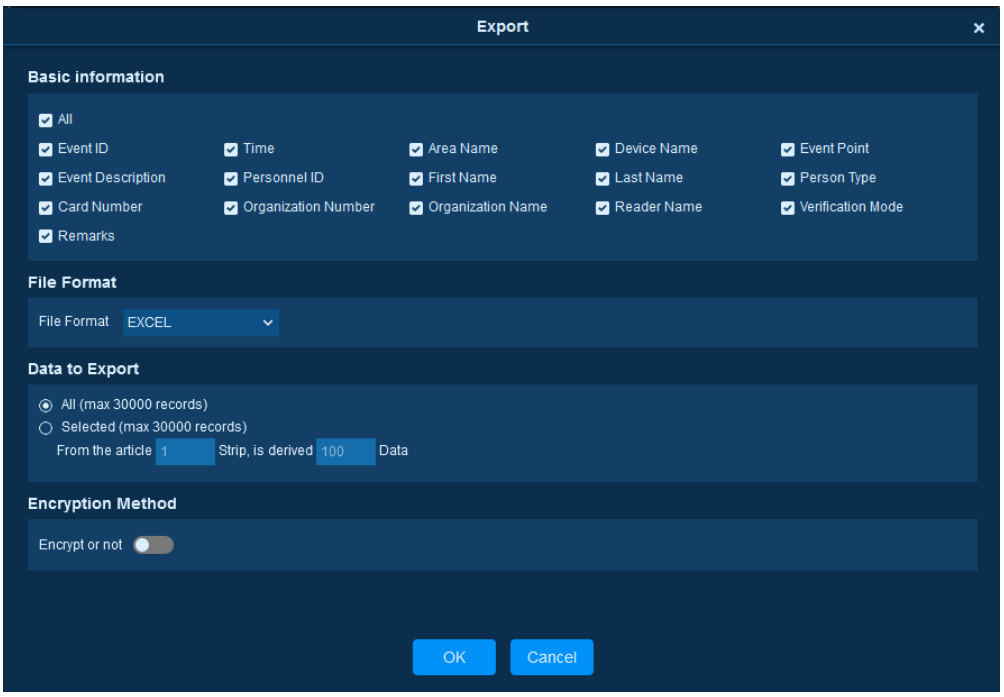
Export device log records to an **Excel/PDF/CSV** file.

Steps:

- Navigate to **[Access] > [Reports] > [Device Log]**.
- View all device operation logs.
- Click **[Export]**.



Copyright © 2024 ARMATURA LLC. All rights reserved



6.5.8Device Face Extraction Failure Log

Function Description

Provides details of device face extraction failures, including error types, descriptions, and associated media files.

Export

Prerequisites for Use

Log into the system using an account with the required permissions.

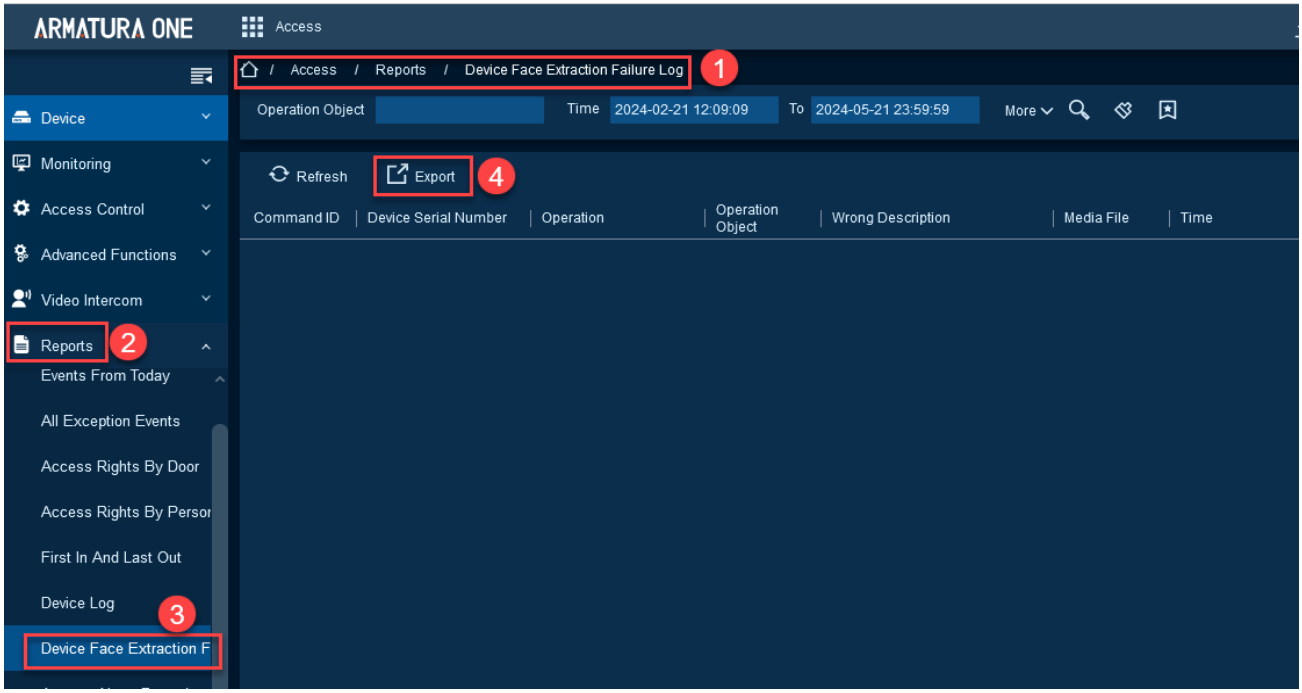
Trigger Result

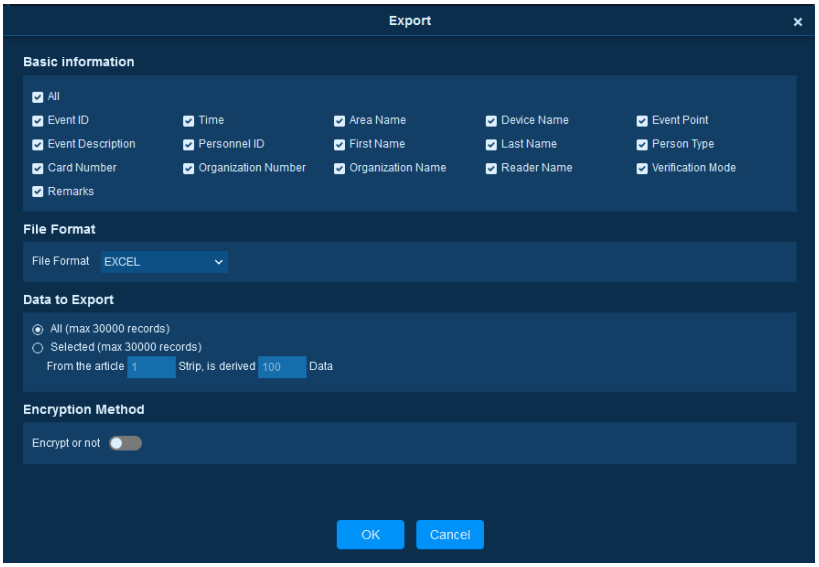
Export face extraction failure records to an **Excel/PDF/CSV** file.

Steps:

- Navigate to **[Access]** > **[Reports]** > **[Device Face Extraction Failure Log]**.
- View all face extraction failure records.
- Click **[Export]**.

Copyright © 2024 ARMATURA LLC. All rights reserved





6.5.9Access Alarm Records

Function Description

Displays details of access control alarm events, including the event description, time of occurrence, and the device that triggered the alarm.

Export

Prerequisites for Use

Log into the system using an account with the required permissions.

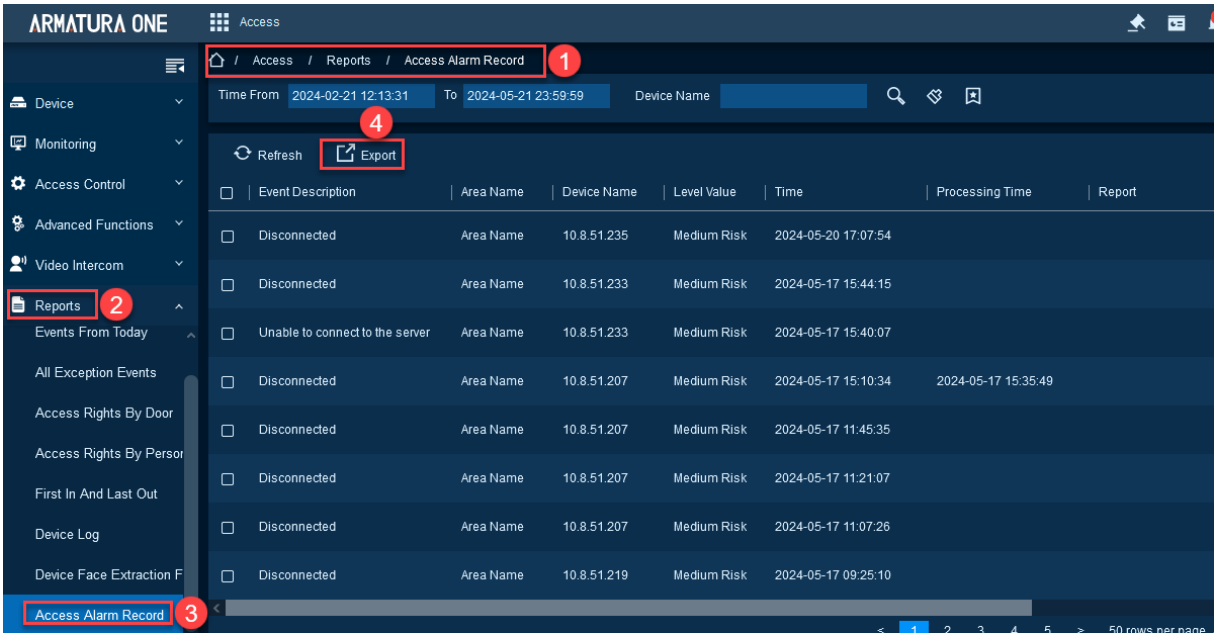
Copyright © 2024 ARMATURA LLC. All rights reserved

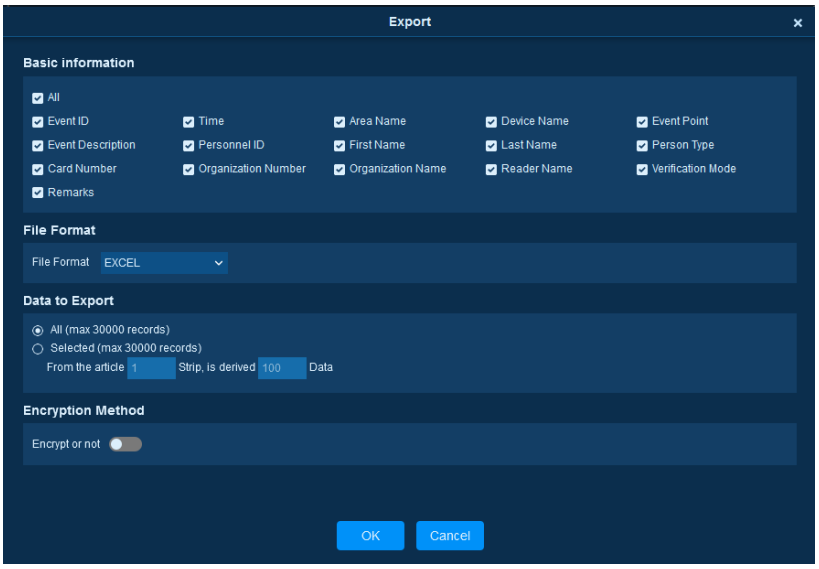
Trigger Result

View and optionally export alarm records for further analysis.

Steps:

- Navigate to **[Access]** > **[Reports]** > **[Access Alarm Record]**.
- Select a record and click **[Details]** to view specific event details.
- Click **[Export]** to export the records into an **Excel/PDF/CSV** file.





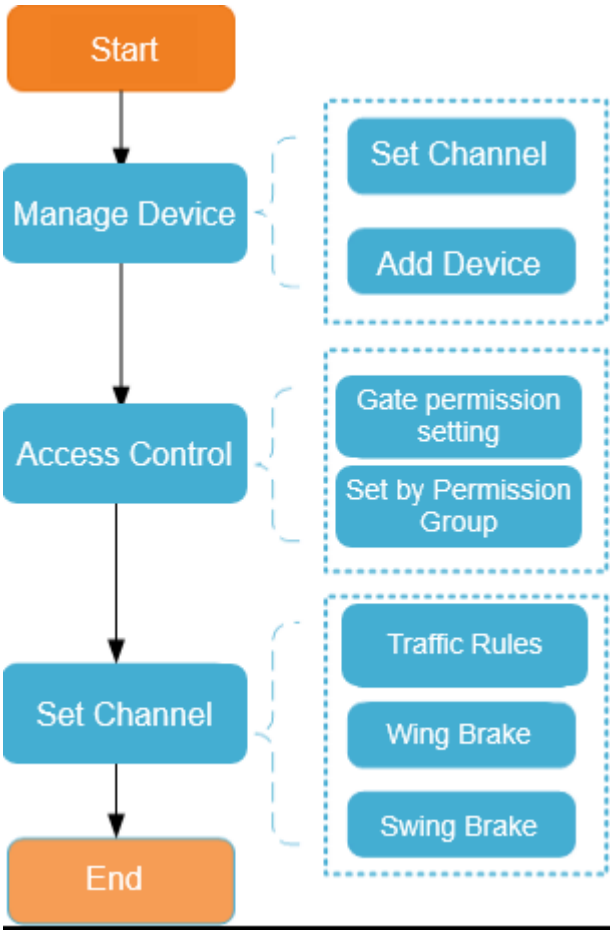
Copyright © 2024 ARMATURA LLC. All rights reserved

7 Entrance Control

The entrance control system connects to gate control boards via devices such as TDA integrated machines. It manages gates' entry and exit parameters, allowing for automated and efficient gate management.

Workflow

The channel service configuration process is outlined below, detailing how to create and manage channel devices.



7.1 Channel Device

The system integrates the channel control board and communicates via RS485 to manage gate access.

7.1.1 Passage

Setting up a passage (channel) within a specific area allows users to organize and manage devices under that passage effectively. Passages can also filter devices by region during real-time monitoring.

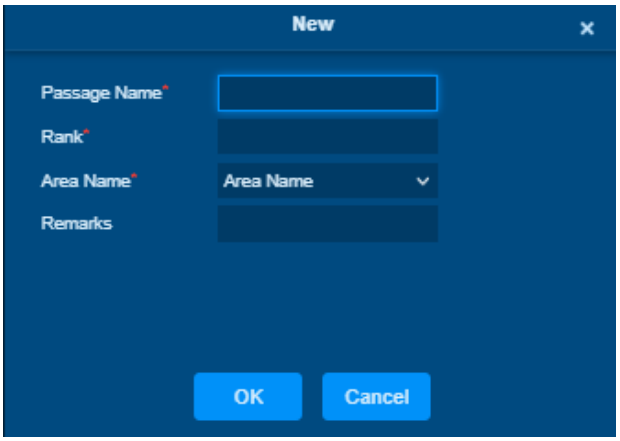
Add a Passage

Steps:

- Navigate to **[Entrance Control]** > **[Channel Device]** > **[Passage]**.

Copyright © 2024 ARMATURA LLC. All rights reserved

- In the channel interface, click **[New]**.



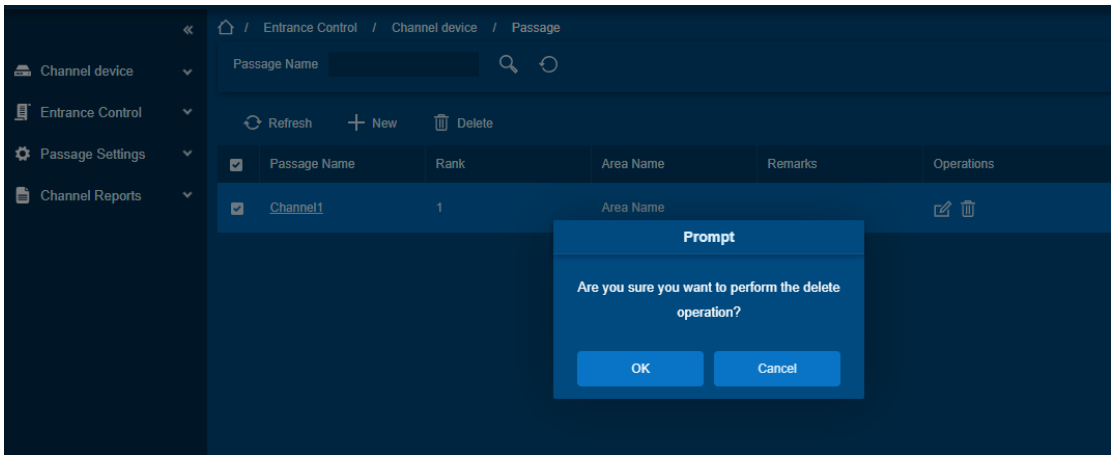
- Fill in the required parameters:

Parameter	How to set
Passage name	Any character, a combination of up to 20 characters, cannot be repeated.
Rank	Only numbers are supported, up to six digits, repeatable. The smaller the ranking, in real-time monitoring, the display will move forward.
Area Name	Select the region to which the channel belongs.
Remarks	Any character with a maximum character length of 100.

- Click **[OK]** to save the new passage configuration.

Delete Passage

- Navigate to **[Entrance Control] > [Channel Device] > [Passage]**.
- Select the passage to be deleted.
- Click **[Delete]**, and confirm by clicking **[OK]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

Note:

A passage cannot be deleted if devices are assigned to it. Remove devices from the passage first.

Edit

Prerequisites for Use

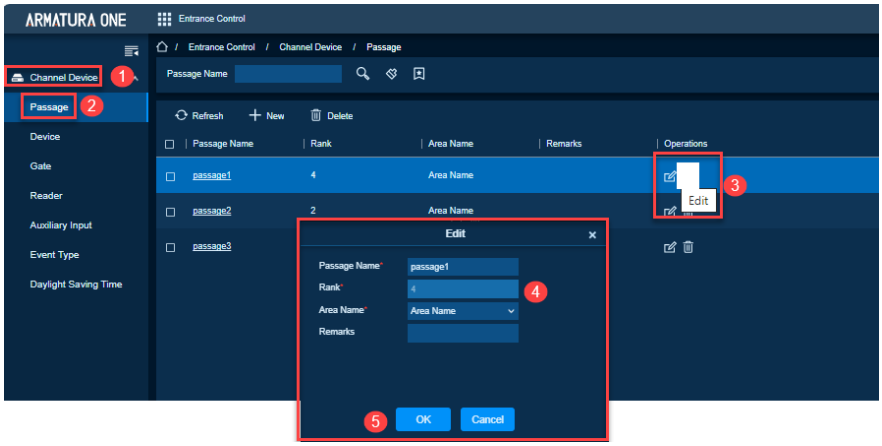
The system requires an existing passage.

Usage Scenarios

This function enables modification of existing passage configuration settings.

Trigger Result

Upon completion, the system implements and saves the updated passage parameters.



Steps:

- Navigate to **[Entrance Control] > [Channel Device] > [Passage]**.
- Locate the passage to edit.
- Click the **Edit (** **)** icon under Operations.
- Make the necessary changes and save.

Copyright © 2024 ARMATURA LLC. All rights reserved

7.1.2 Device

The Device module in the Entrance Control system provides comprehensive features for managing and configuring channel devices connected to the gate control board.

Search for Channel Devices

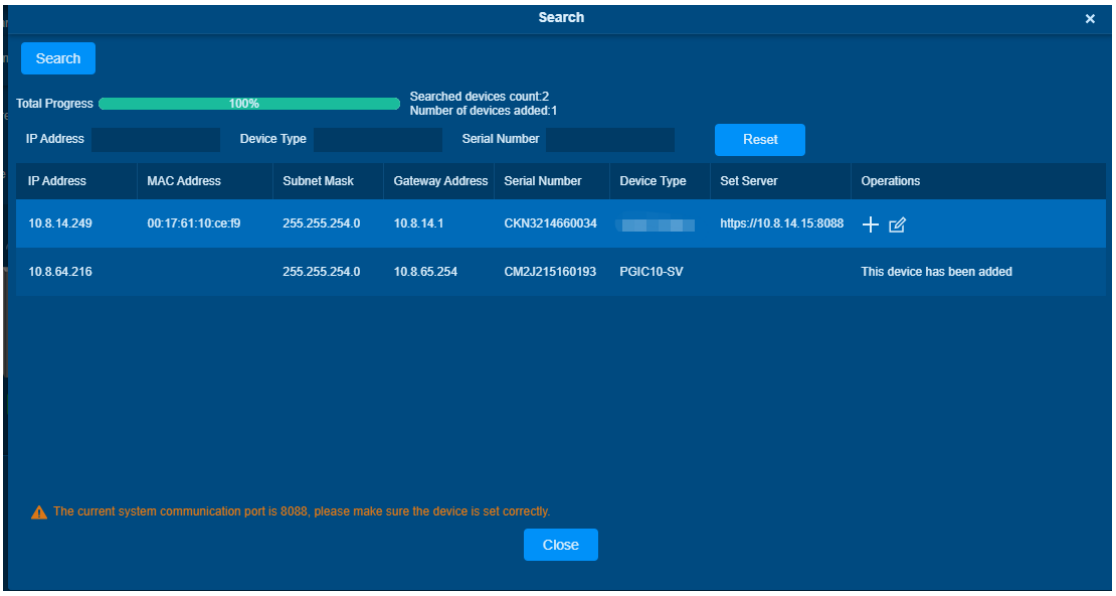
Prerequisites for Use

Ensure that the **IP allocation** is configured before adding channel devices.

Set the **server address**, including the IP and port of the current server.

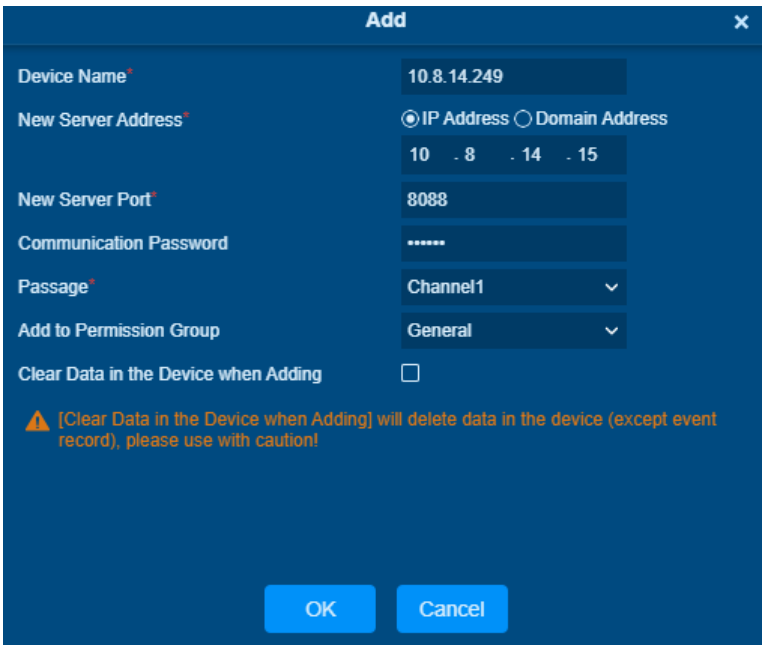
Steps:

- Navigate to **[Entrance Control] > [Channel Device] > [Device]**.
- Click **[Search]** to open the search box.
- Click **[Search]** again to display a list of available devices.



- Select a device from the list and click **[Add]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Enter the device details as follows:

Parameter	How to set
Device name	Any unique name (up to 20 characters).
New Server Address	Select IP Address or Domain Address based on the device configuration. IP Address: It displays the device Ip Domain Address: the network address or identifier of the device user are configuring.
New Server Port	Enter the ADMS port (default: 8088).
Communication Password	Set the password for backend software integration.
Passage	Assign the device to a channel.
Add to Permission Group	Automatically adds the device to a permission group.
Clear data in device when adding	Deletes all device data except event records when added.

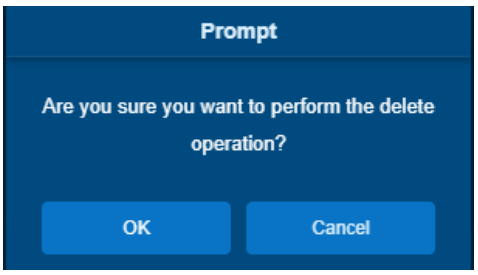
- Click **[OK]** to complete the addition of channel device.

Delete a Device

Steps:

- In the **[Entrance]**, click **[Channel Device]** > **[Device]** and select device to be deleted.
- Click **[Delete]** to delete the device.

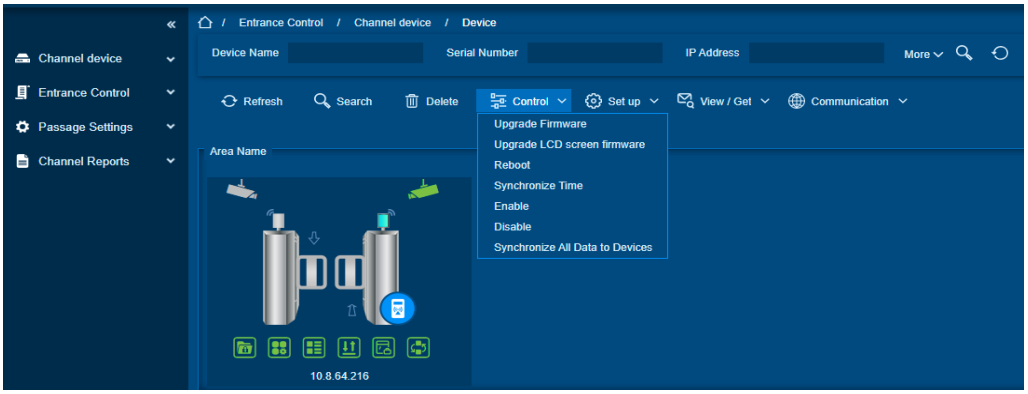
Copyright © 2024 ARMATURA LLC. All rights reserved



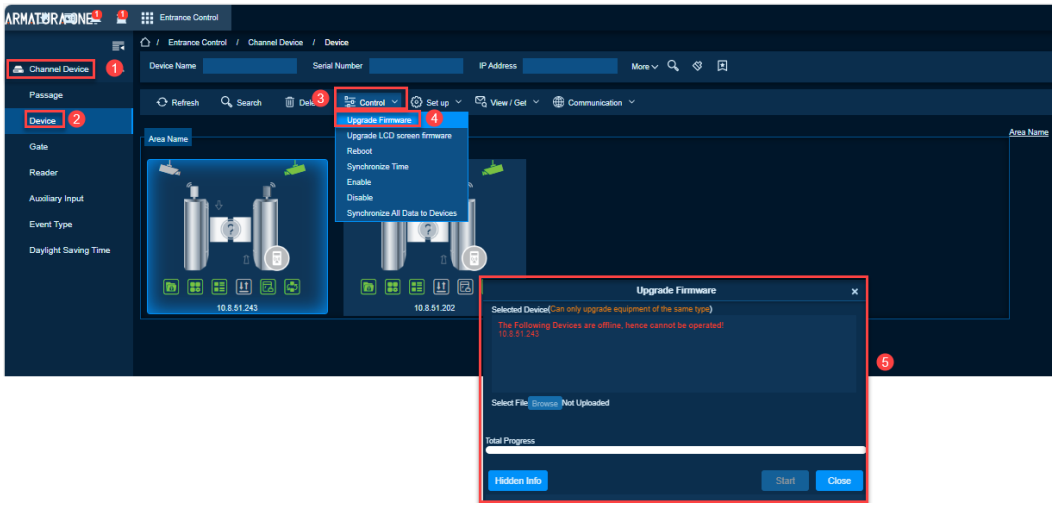
- Click **[OK]** to perform the delete operation**.**

Control Options

- **Upgrade Firmware**
  - Select a device, click **[Upgrade Firmware]**, and browse for the firmware file (emfw.cfg).
  - Click **[Start]** to begin the upgrade.



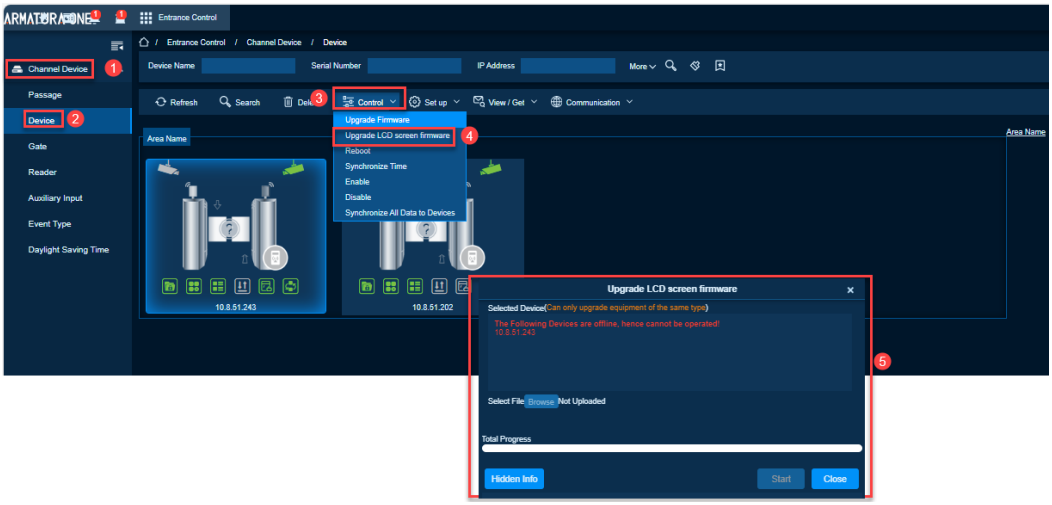
- **Upgrade LCD Screen Firmware**
  - Similar to firmware upgrades, select the LCD firmware file and click **[Start]**.



Reboot

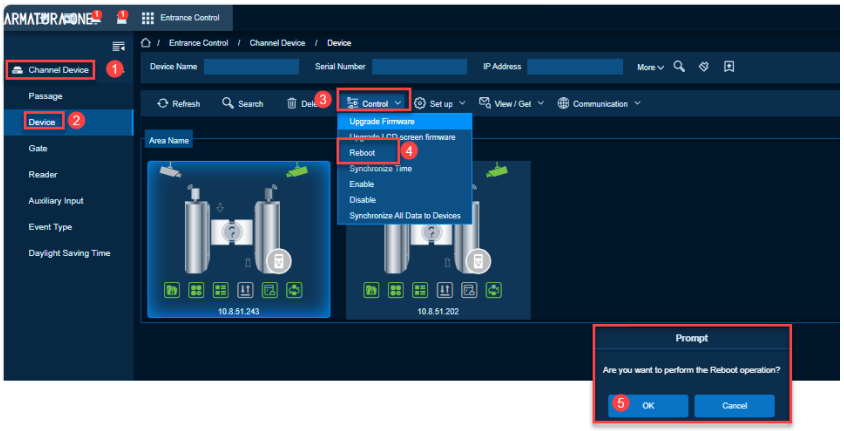
Select a device and click **[Reboot]** to restart.

Copyright © 2024 ARMATURA LLC. All rights reserved



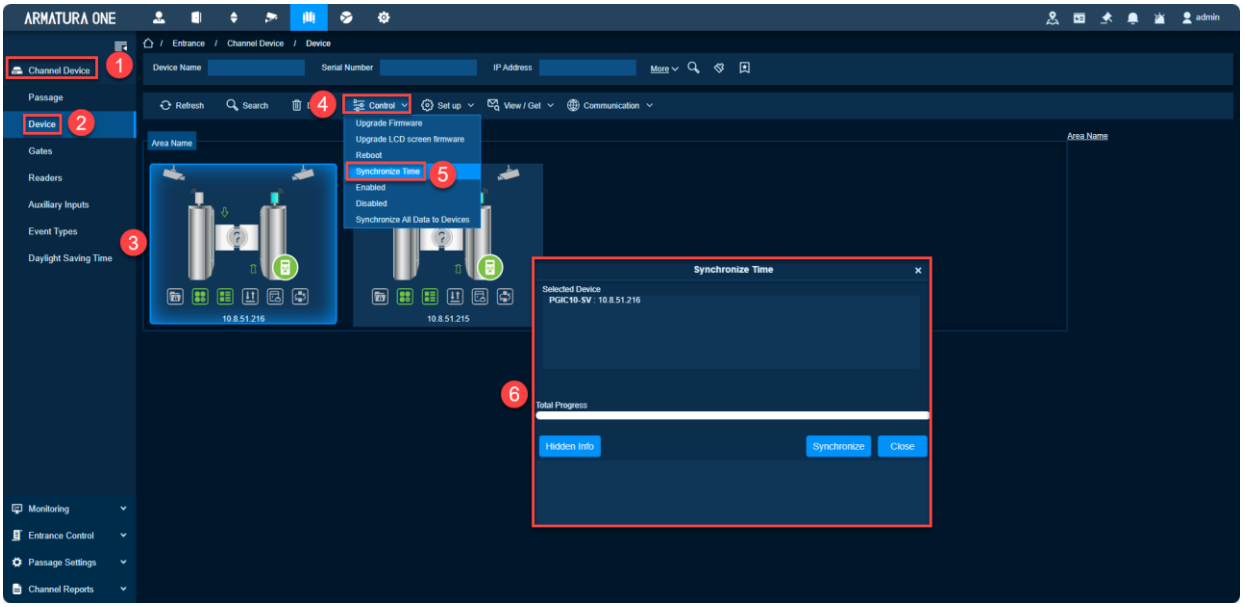
Synchronize Time

Select a device and click **[Synchronize Time]** to align with the server.



Enable/Disable Device

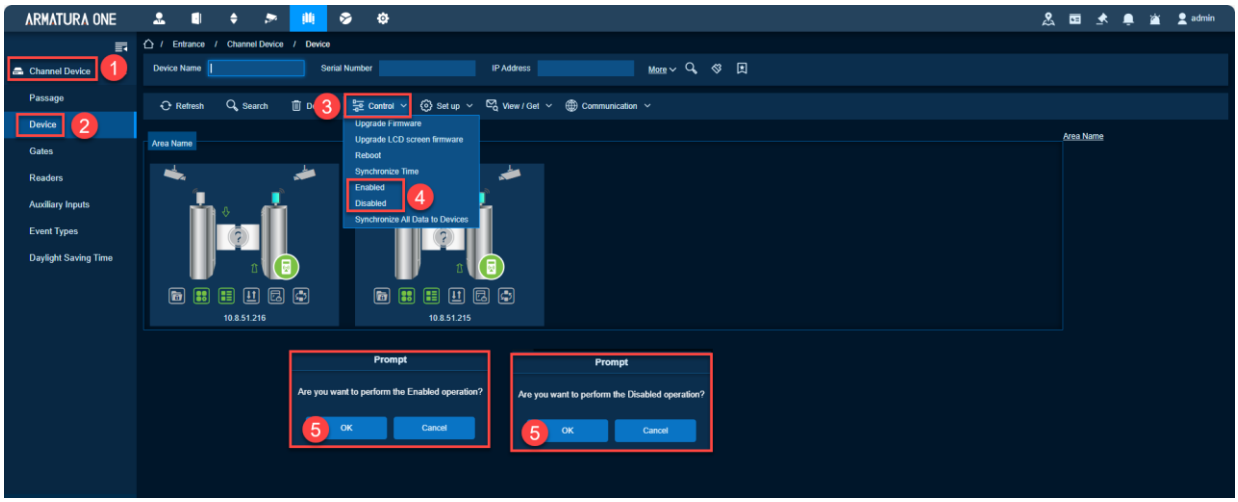
Use **[Disable/Enable]** to change the operational status of the device.

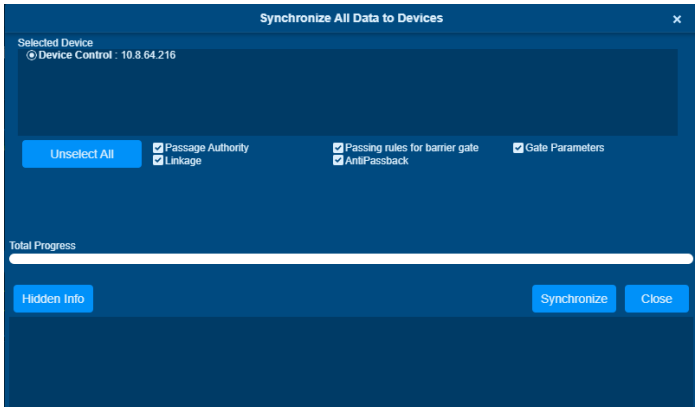


Copyright © 2024 ARMATURA LLC. All rights reserved

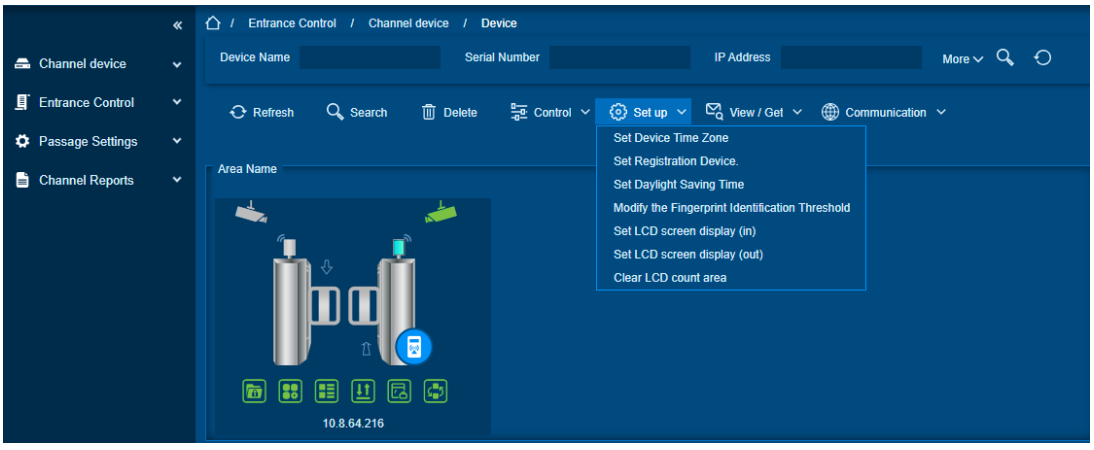
Synchronize All Data to Devices

Select **[Synchronize All Data to Devices]** to reinitialize device settings.





Setup Options



Purpose:

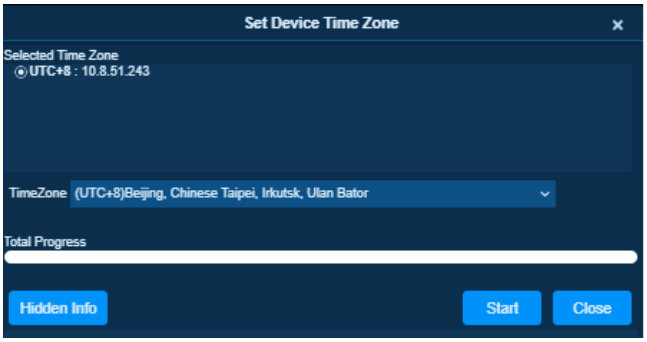
Adjust the time zone for devices displaying incorrect time.

Steps:

- Navigate to **[Channel Device] > [Device] > [Set-up]** in the **Entrance Control** interface.
- Select the device to be configured.

Copyright © 2024 ARMATURA LLC. All rights reserved

- Click **[Set Device Time Zone]**.
- Choose the appropriate time zone for the selected device.



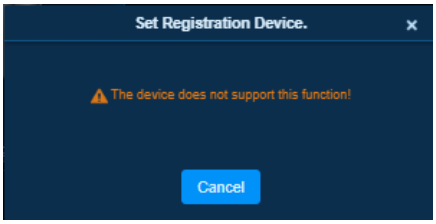
Set Registration Device

Purpose:

Enable standalone passage devices to automatically upload personnel and data.

Steps:

- Go to **[Channel Device] > [Device] > [Set-up]**.
- Select the device to configure.
- Click **[Set Registration Device]** to finalize the setup.



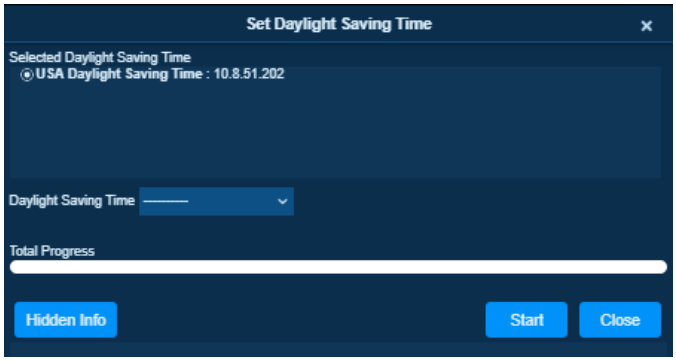
Set Daylight Saving Time (DST)

Purpose:

Accommodate daylight saving time by adjusting the clock forward or backward as needed.

Steps:

- Navigate to **[Channel Device] > [Device] > [Set-up]**.
- Select the device for DST configuration.
- Click **[Set Daylight Saving Time]**.
- Set the DST schedule, specifying the forward and backward time adjustments.



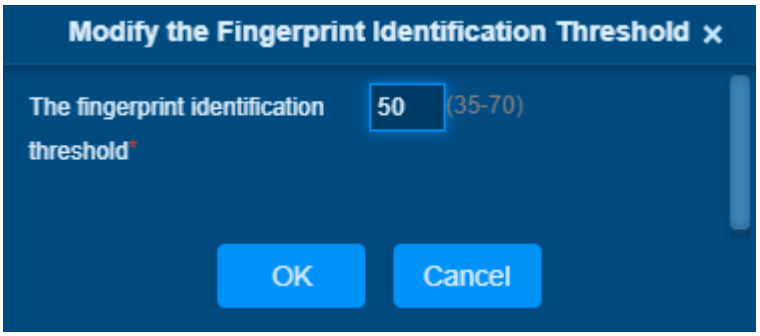
Copyright © 2024 ARMATURA LLC. All rights reserved

Modify the Fingerprint Identification Threshold

Purpose:
Adjust the sensitivity of fingerprint recognition (range: **35–70**, default: **55**).

Steps:

- In the **Entrance Control** interface, go to **[Channel Device] > [Device] > [Set-up]**.
- Select the target device.
- Click **[Modify the Fingerprint Identification Threshold]**.
- Set the desired threshold value and save the changes.



Set LCD Screen Display (In)/(Out)

Purpose:
Configure the LCD screen to display specific content in three sections:

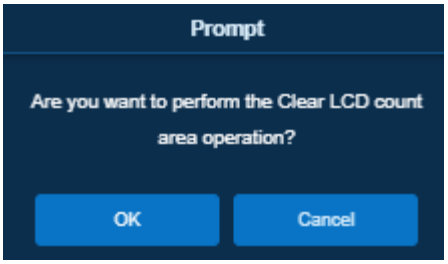
- **Upper Section (30%)**: Video area.
- **Middle Section (30%)**: Gate channel information.
- **Lower Section (40%)**: Picture cycling.

Steps:

- Navigate to **[Channel Device] > [Device] > [Set-up]**.
- Select the device for configuration.
- Click **[Set LCD Screen Display (In)/(Out)]**.
- Customize the content for each section and confirm the settings.

Clear LCD Count Area

Purpose:
Reset the counting area of the LCD screen.



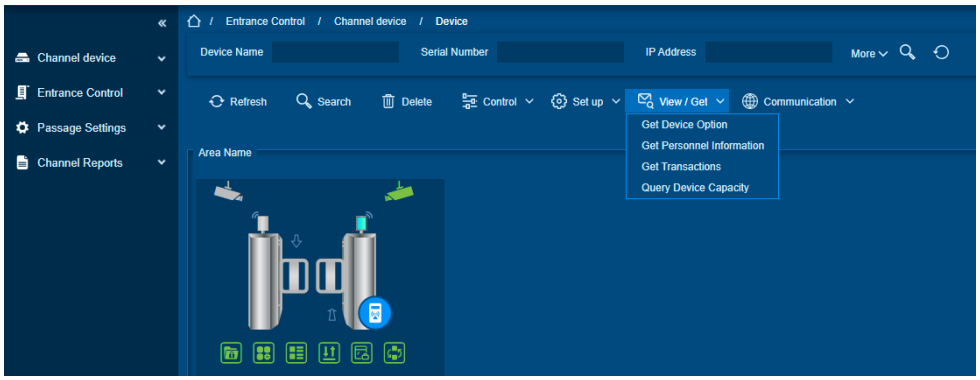
Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Channel Device] > [Device] > [Set-up]**.
- Select the device requiring a reset.
- Click **[Clear the LCD Counting Area]** to clear and restart the counting area.

View/Get

The **View/Get** section allows administrators to view device details, retrieve personnel information, and access transaction logs. It also enables checking the device's capacity and synchronizing data.

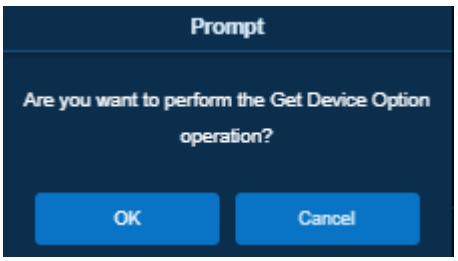


Get Device Option

Purpose:
View the common parameters of a device, such as firmware version and configuration details.

Steps:

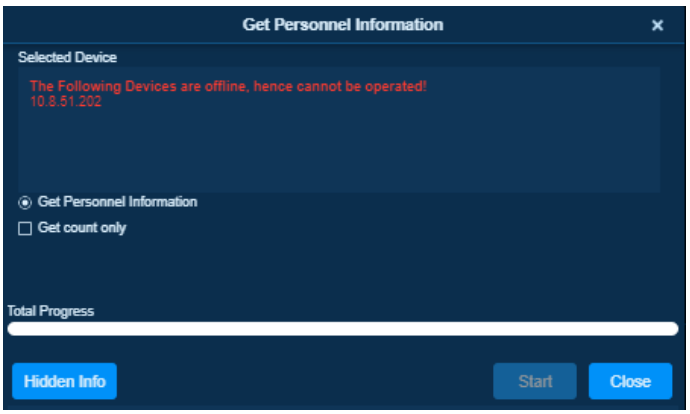
- Navigate to **[Channel Device] > [Device] > [View/Get]** in the **Entrance Control** interface.
- Select the device for which you want to retrieve options.
- Click **[Get Device Option]** to view the device's parameters.



Get Personnel Information

Purpose:
Retrieve data about individuals stored on the device, including fingerprints, palm prints, and identification numbers.

Copyright © 2024 ARMATURA LLC. All rights reserved



Steps:

- Navigate to **[Channel Device] > [Device] > [View/Get]** in the **Entrance Control** interface.
- Select the device from which you want to retrieve personnel data.
- Click **[Get Personnel Information]** to display personnel information stored on the device.

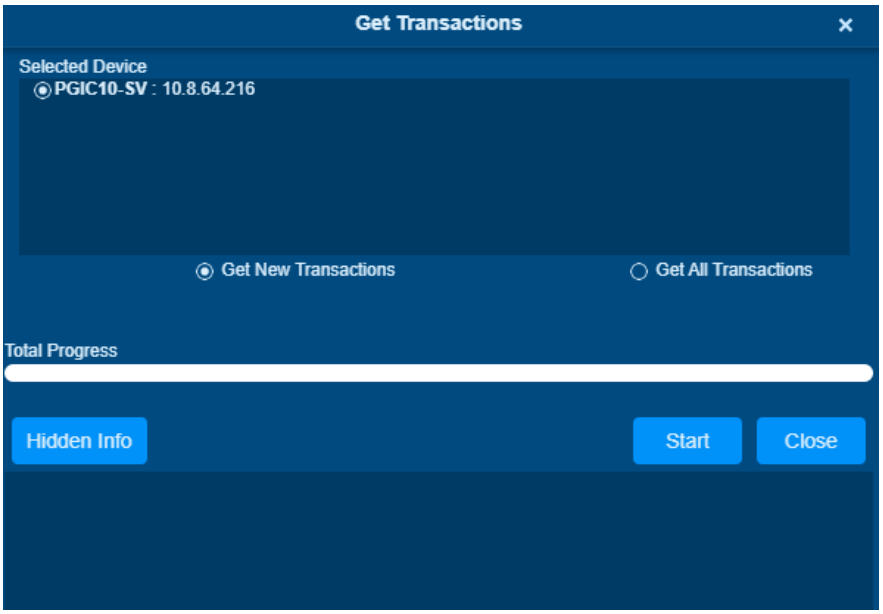
Get Transactions

Purpose:

Retrieve event records from the device, such as new records or all available records.

Steps:

- Go to **[Channel Device] > [Device] > [View/Get]** in the **Entrance Control** interface.
- Select the device for which you want to retrieve transactions.
- Click **[Get Transactions]** to view transaction data.



Copyright © 2024 ARMATURA LLC. All rights reserved

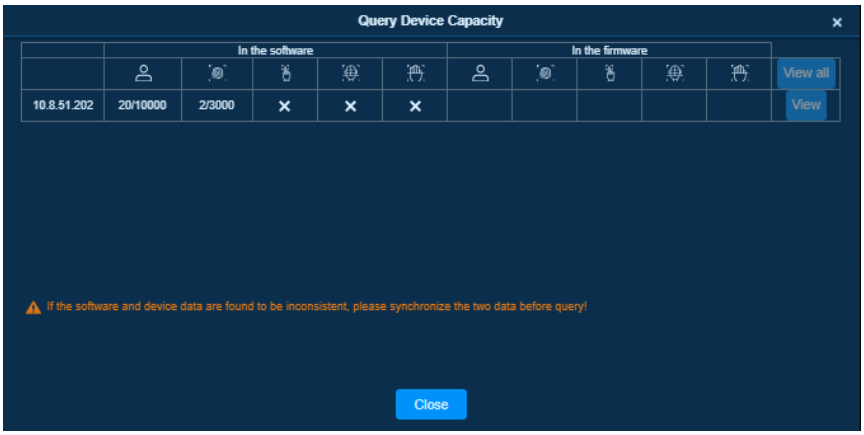
Additional Notes:

- When the network is stable, the system retrieves event records in real time.
- If communication is interrupted, real-time updates will stop. In such cases, you can manually retrieve records from the device.

Query Device Capacity

Purpose:

View the device's storage capacity and usage information, including Number of persons, Fingerprints, Finger veins, Faces, Palm prints



Steps:

- Navigate to **[Channel Device] > [Device] > [View/Get]** in the **Entrance Control** interface.
- Select the target device.
- Click **[Query Device Capacity]** to view capacity details and manually obtain updated usage data.

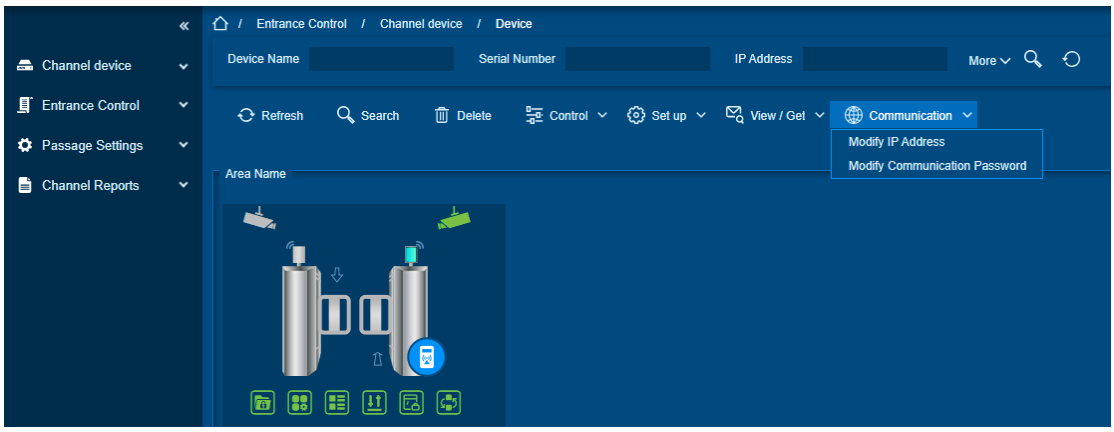
Additional Notes:

- If there is a mismatch between the software data and the device data, manually synchronize the information.
- Ensure stable network communication for accurate data synchronization.

Communication

The **Communication** section within the **Entrance Control** interface enables administrators to manage device network settings, including IP address modifications and communication password updates. These configurations ensure secure and stable device connectivity.

Copyright © 2024 ARMATURA LLC. All rights reserved



Communication Option

Modify IP Address

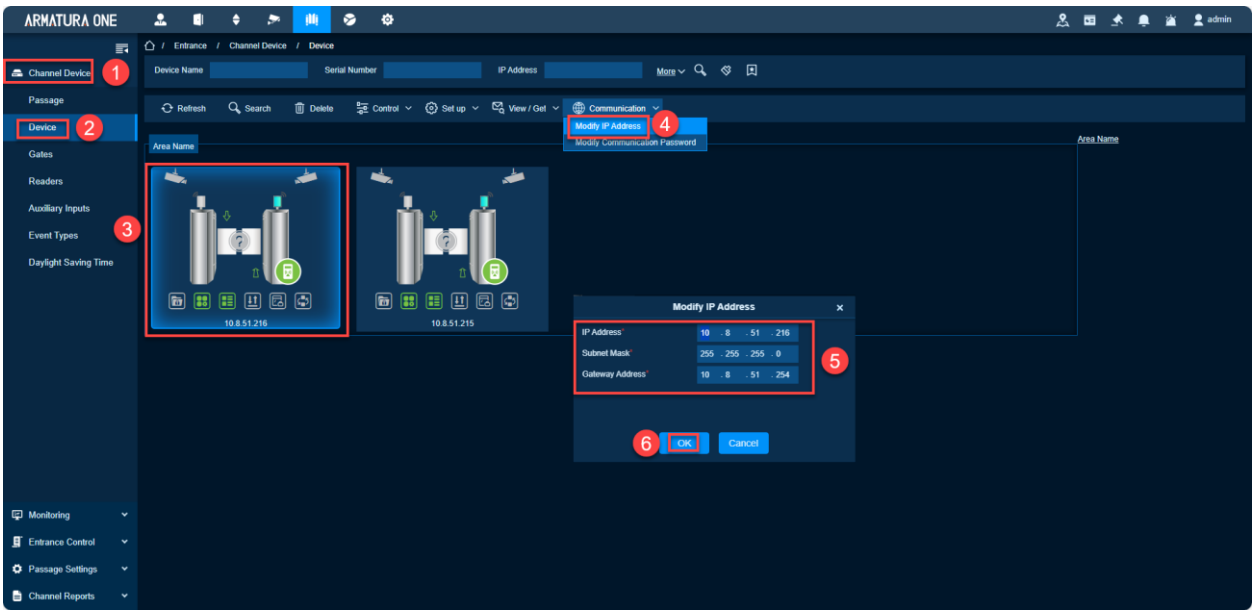
Purpose:

Update the device's IP address, gateway, and subnet mask to ensure it communicates correctly with the network.

Steps:

- Navigate to **[Channel Device] > [Device] > [Communication]** in the **Entrance Control** interface.
- Select the target device.
- Click **[Modify IP Address]** to open the modification interface.
- The system will attempt to retrieve the real-time network gateway and subnet mask from the device.
    1. If this retrieval fails, you cannot proceed with the IP address modification.
- Enter the following details:
    1. **New IP Address**
    2. **Gateway**
    3. **Subnet Mask**
- Click **[OK]** to save the changes and exit.

Copyright © 2024 ARMATURA LLC. All rights reserved



Copyright © 2024 ARMATURA LLC. All rights reserved

Modify Communication Password

Purpose:

Enhance security by updating the device's communication password.

Steps:

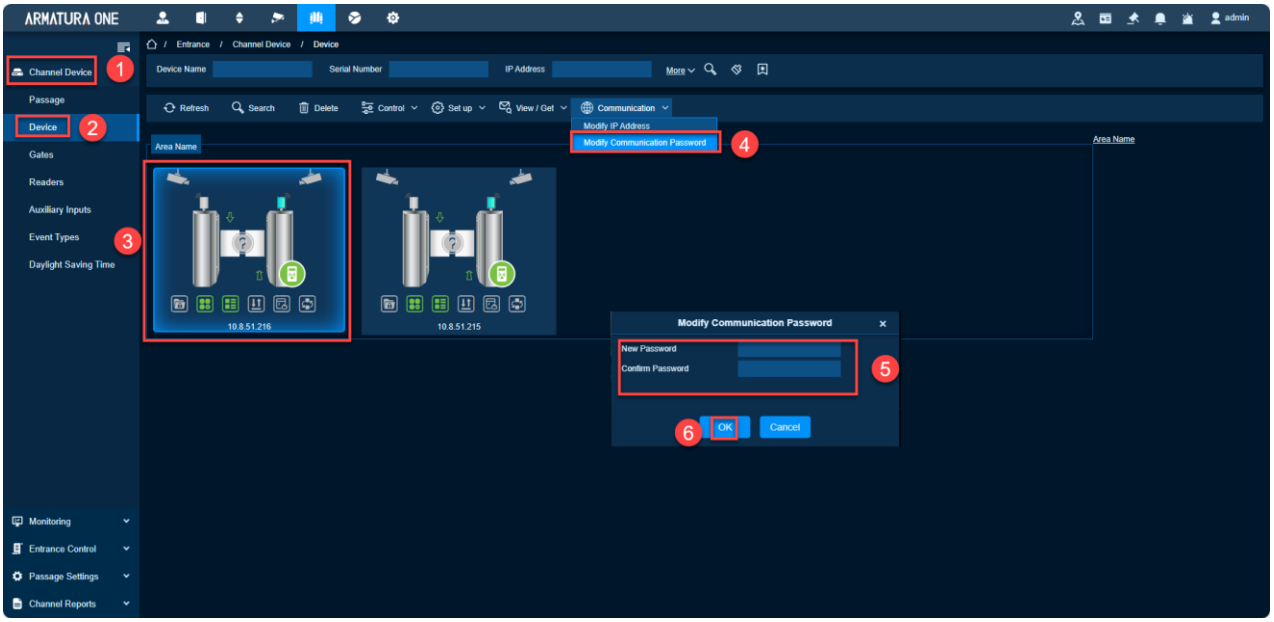
- Navigate to **[Channel Device] > [Device] > [Communication]** in the **Entrance Control** interface.
- Select the target device.
- Click **[Modify Communication Password]** to open the password modification interface.
- The system will prompt you to:
  - Enter the **old communication password** for verification.
  - Input the **new password** twice for confirmation.
- Click **[OK]** to save the new password.

Password Guidelines:

Avoid using spaces in the password.

Use a combination of letters and numbers to create a strong password.

Assign unique passwords for each device to enhance security.



Note:

Network Stability: Ensure that the network is stable during the modification process to avoid communication errors.

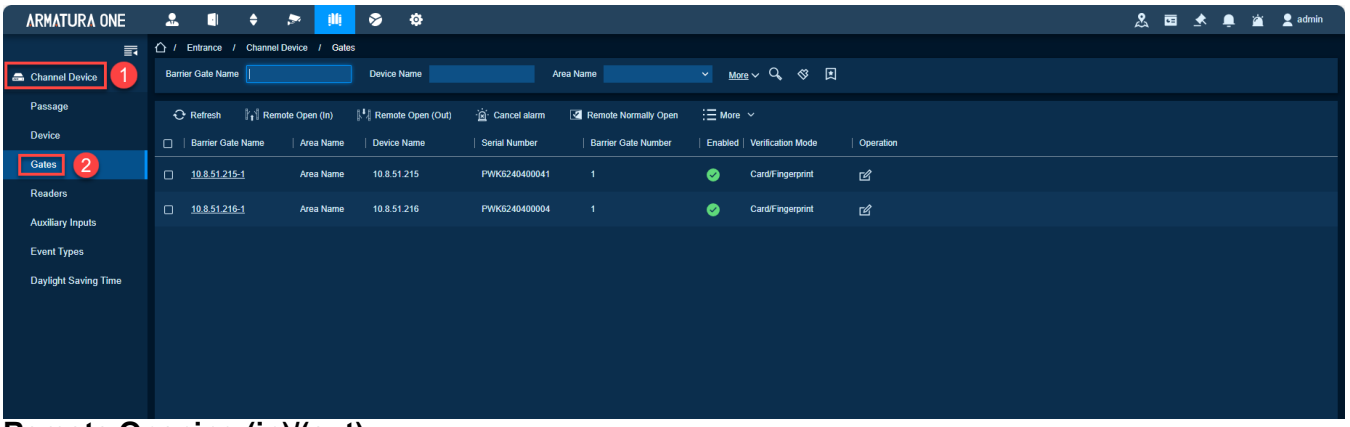
Password Management: Maintain a secure record of communication passwords for future reference. Misplacing passwords can lead to administrative access issues.

Security Tip: Regularly update communication passwords to safeguard against unauthorized access.

Copyright © 2024 ARMATURA LLC. All rights reserved

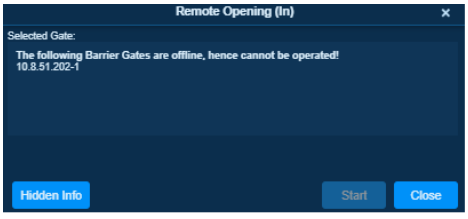
7.1.3 Gates

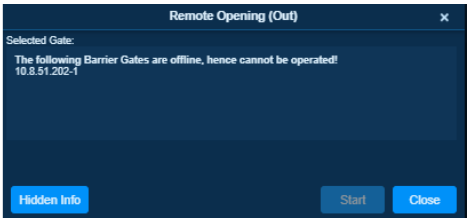
In the **Entrance** module, select **[Channel Device]** > **[Gate]**.



Remote Opening (in)/(out)

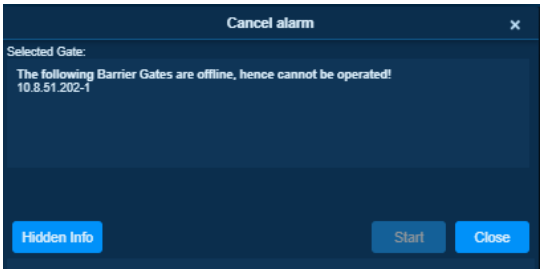
In the **Entrance** interface, click on **[Channel Device]** > **[Gate]**. This interface allows users to control either a single gate or all gates. To control a specific gate, right-click on it and select **[Remote Opening (In/Out)]** from the pop-up dialog box. To control all gates, simply click **[Remote Opening (In/Out)]** behind Current All.





Cancel the Alarm

Once an alarm door is displayed on the interface, an alarm sound will be played. Users can cancel the alarm for either a single gate or all gates



In the **Entrance** interface, click **[Channel Device]** > **[Gate]** and select the alarm gate to be modified. Then click **[Cancel the Alarm]** to cancel the alarm.

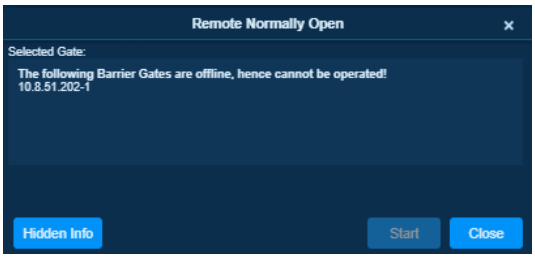
Note:

If alarm cancel the alarm fails, check for any disconnected devices. If any are found, verify the network connection

Copyright © 2024 ARMATURA LLC. All rights reserved

Remote Normally Open

Remote normally open will set the gate as normal open by remote.



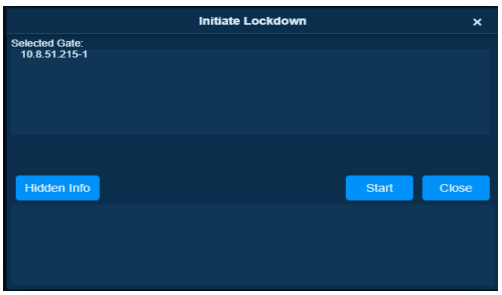
In the **Entrance** interface, click on **[Channel Device]** > **[Gate]**, and select the gate user wish to set to normal open. Then click **[Remote Normal Open]** to remotely configure the gate as normal open

More Options

In the **Entrance** interface, click **[Channel Device]** > **[Gate]** >**[More]** to activate the door lockdown status.

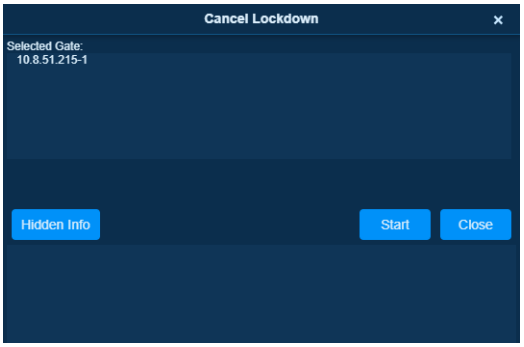
1. **Initiate Lockdown**

   Initiate Lockdown will remotely set the gate status to lockdown mode. After this, the door will not receive any operations, such as card readings or remote commands. This function is supported only by certain devices



2. **Cancel Lockdown**

   Cancel Lockdown cancels the lockdown of the gate. This function is supported only by certain devices.

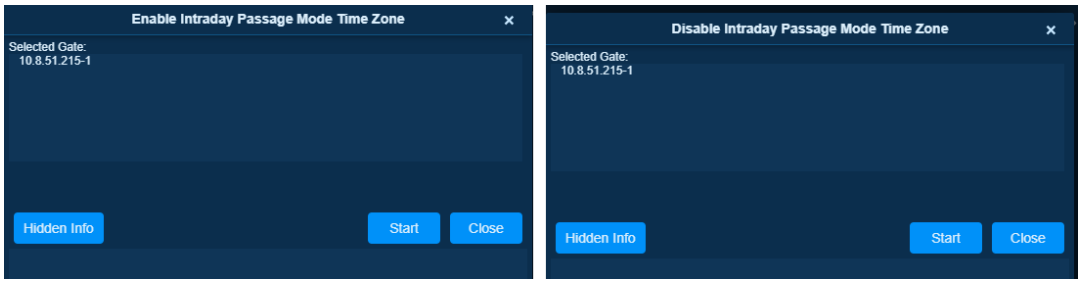


3. **Enable / Disable Intraday Passage Mode Time Zone**

   In remote opening, users can define the door opening duration (the default is 15 seconds). User can select **[Enable Intraday Passage Mode Time Zone]** to activate the intraday door passage

Copyright © 2024 ARMATURA LLC. All rights reserved

mode time zones, or set the door to Normal Open, which will allow it to remain open 24 hours without any time zones limitation.



To close a door, first select **[Disable Intraday Passage Mode Time Zone]** to prevent other normal open time zones from opening the door. Then, select **[Remote Closing]** to close the door

Edit

Prerequisites for Use

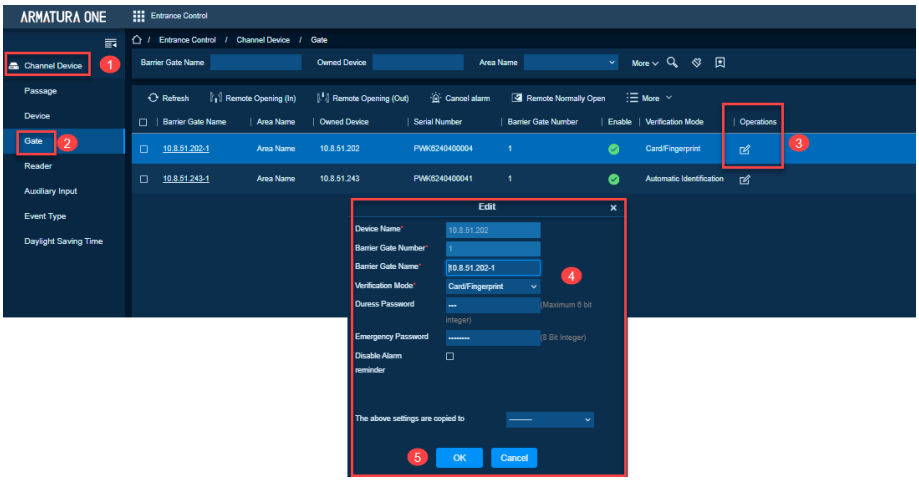
The system requires an existing gate configuration in the database.

Usage Scenarios

This function enables modification of existing gate configuration settings.

Trigger Results

The system implements and saves the updated gate parameters.



Steps:

- Navigate to **[Channel Device] > [Gate]** in the **Entrance Control** interface.
- Locate the gate you wish to edit.
- Click the **edit icon (** **)** under the **Operations** column to open the gate modification interface.
- Make the necessary changes to the gate details.
- Click **[OK]** to save the modifications.

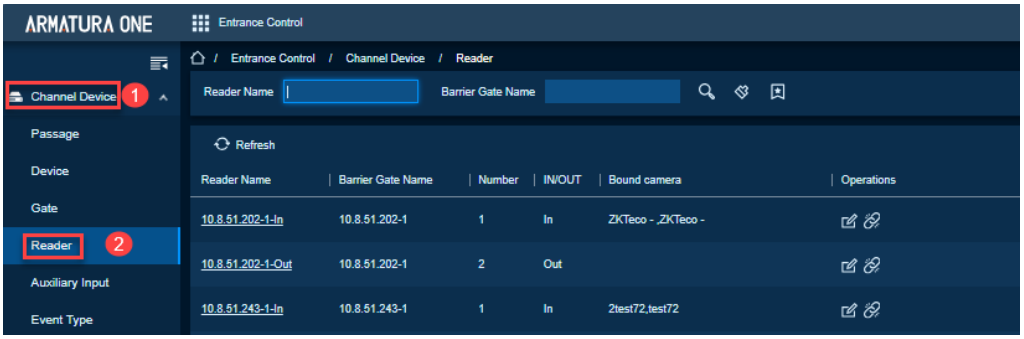
Copyright © 2024 ARMATURA LLC. All rights reserved

7.1.4 Reader

Each Entry device has a reader, and the user can view the reader information in this interface.

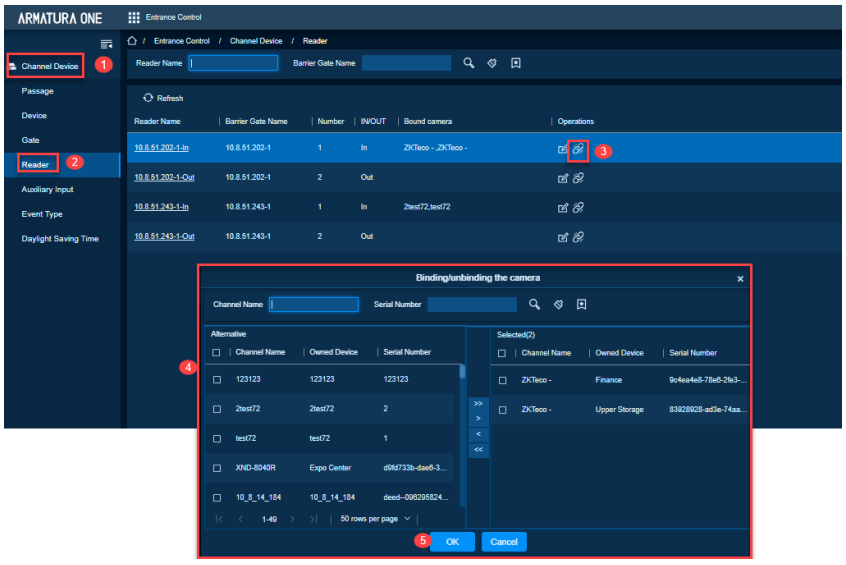
Steps:

Click **[Entrance Control]** > **[Channel Device]** > **[Reader]** to view the reader information such as reader name, barrier gate name, bound camera, and in/out details.



Binding/Unbinding the camera

Binding and Unbinding camera option allows the reader to be connected to the cameras, enabling the system to create a video linkage (including pop-up videos, recordings, or screenshots) whenever a corresponding event occurs. Prior to this, the interaction settings must be configured in either Linkage or Global Linkage.



Note:

An auxiliary input point can bind more than one channel.

Copyright © 2024 ARMATURA LLC. All rights reserved

Edit

Prerequisites for Use

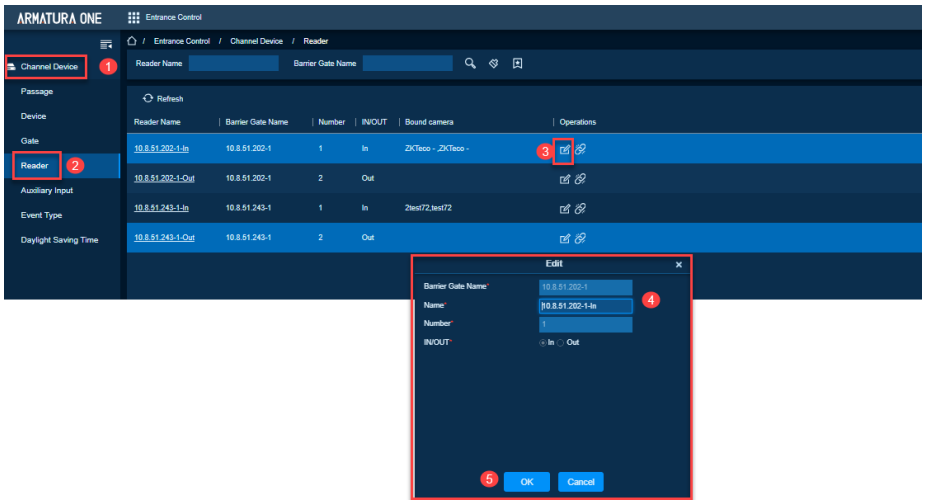
The system requires an existing reader configuration in the system.

Usage Scenarios

This function enables modification of existing reader settings to maintain accurate system configurations.

Trigger Result

The system implements and saves the updated reader parameters.



Steps:

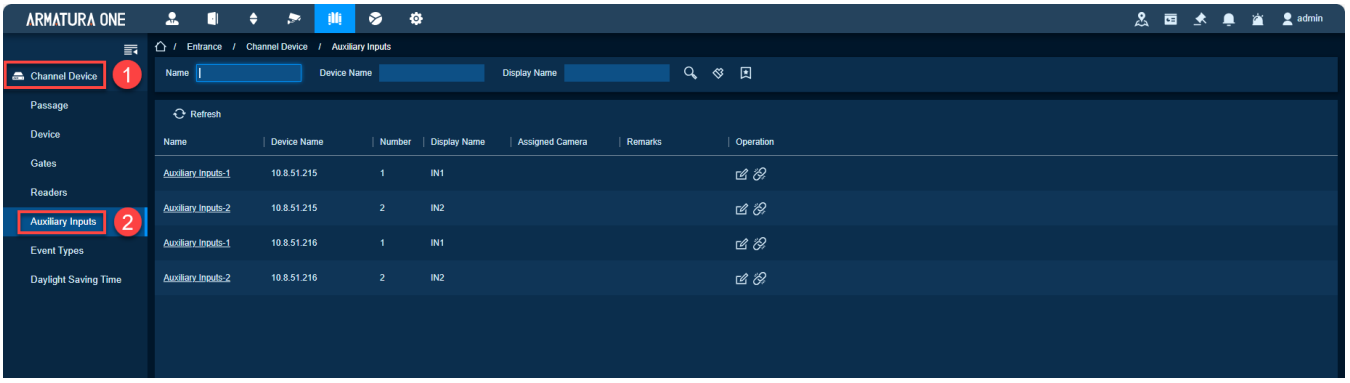
- Navigate to **[Channel Device] > [Reader]**.
- Locate the desired reader in the list.
- Click the **edit icon (** **)** under the **Operations** column.
- Modify the reader's details as needed.
- Click **[OK]** to save changes.

Copyright © 2024 ARMATURA LLC. All rights reserved

7.1.5 Auxiliary Input Management

Function Description

Auxiliary inputs connect to devices such as infrared sensors or smoke sensors. This interface allows users to manage and configure these inputs, including binding them to cameras for event-triggered video linkage. To access the Auxiliary Input interface, navigate to **[Entrance Control]** > **[Channel Device]** > **[Auxiliary Input]**. Once there, you can view and manage the auxiliary input settings from the displayed interface.



Bind/Unbind Camera

Function Description

The system enables camera and auxiliary input integration, providing enhanced monitoring through video pop-ups, event-triggered recordings, and automated screenshots when sensors detect activity.

Prerequisite

The system requires pre-configured settings in the Linkage or Global Linkage modules before camera binding can be established.

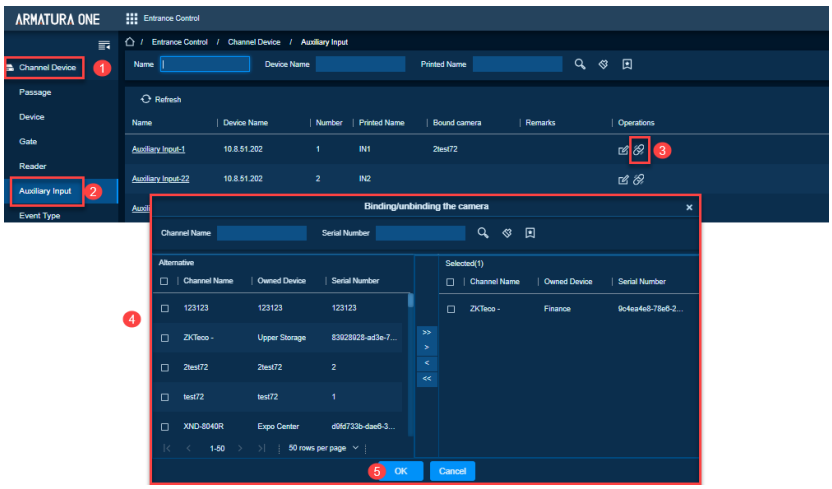
Note

Multiple camera channels can be associated with a single auxiliary input point for comprehensive monitoring coverage.

Steps

- Select the auxiliary input in the interface.
- Use the **Bind/Unbind Camera** option to connect or disconnect a camera from the auxiliary input.

Copyright © 2024 ARMATURA LLC. All rights reserved



Edit Auxiliary Input

Prerequisites for Use

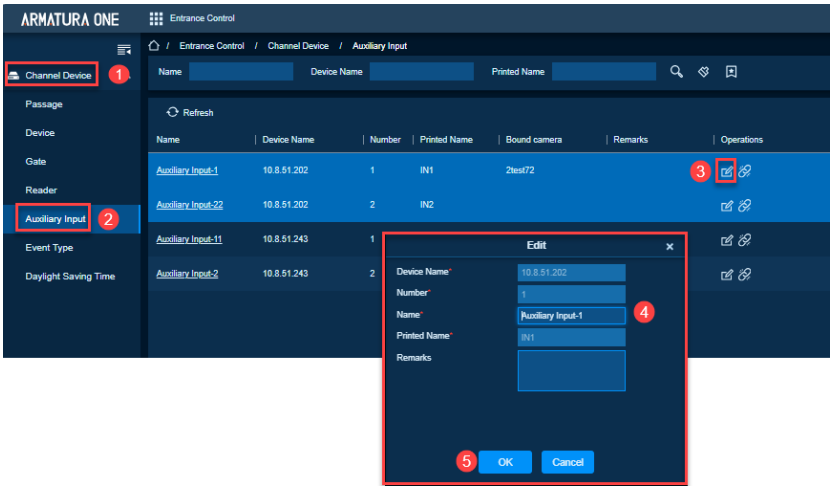
The system requires an existing auxiliary input configuration.

Usage Scenarios

This function enables modification of existing auxiliary input settings to maintain accurate system configurations.

Trigger Result

The system implements and saves the updated auxiliary input parameters.



Steps:

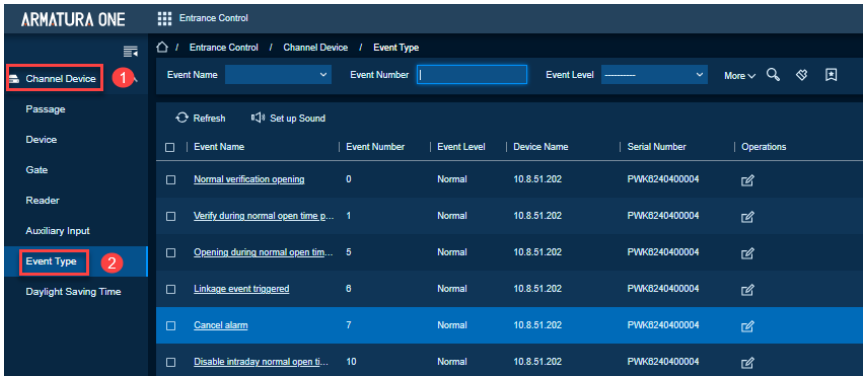
- Navigate to **[Channel Device] > [Auxiliary Input]**.
- Locate the desired auxiliary input in the list.
- Click the **edit icon (** **)** under the **Operations** column.
- Modify the auxiliary input details as needed.
- Click **[OK]** to save the changes.

Copyright © 2024 ARMATURA LLC. All rights reserved

7.1.6 Event Type Management

Function Description

The **Event Type** section displays all event types associated with channel devices and provides options to set sound alerts for events and edit event type details. To access the Event Type interface, navigate to **[Entrance Control]** > **[Channel Device]** > **[Event Type]**. The interface will then display a list of event types associated with the channel devices, allowing you to manage and configure them as needed.



Set up sound

Prerequisites for Use

The system requires an existing event type configuration.

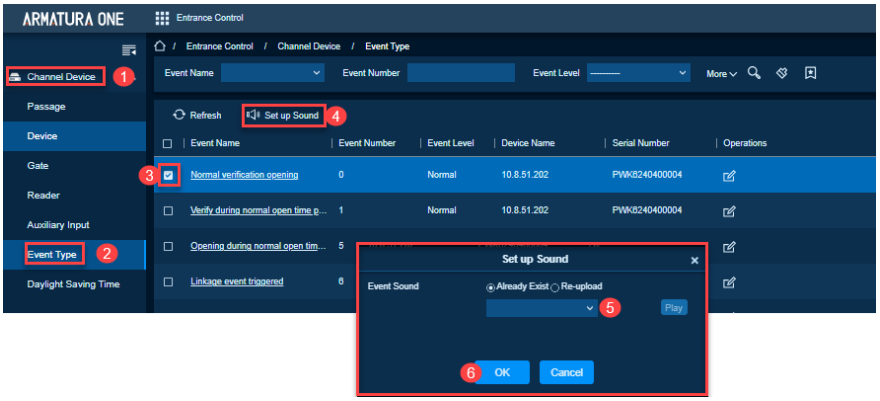
Usage Scenarios

Enables setting customized audio alerts for specific events.

Users can upload local audio files for event notifications.

Trigger Result

Once configured, the sound will be applied as a trigger result for the specified events.



Format: .wav or .mp3

Size: Must not exceed **10MB**

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Entrance Control] > [Channel Device] > [Event Type]**.
- The interface will display a list of event types associated with the channel devices.

Edit Event Type

Prerequisites for Use

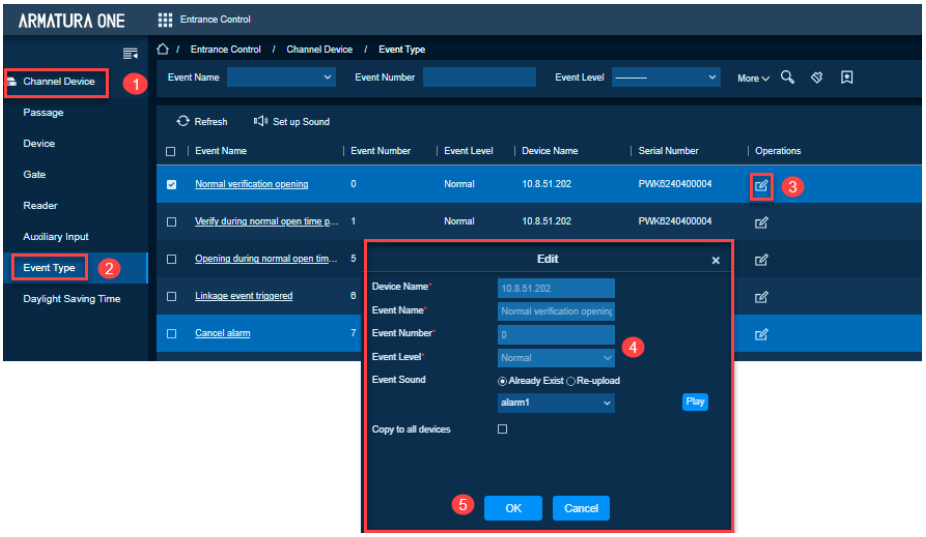
The system requires an existing event type configuration.

Usage Scenarios

This function enables modification of existing event type settings to align with updated management requirements.

Trigger Result

The system implements and saves the updated event type parameters.



Steps:

- Navigate to **[Channel Device] > [Event Type]**.
- Locate the desired event type in the list.
- Click the **edit icon (** **)** under the **Operations** column.
- Modify the event type details as required.
- Click **[OK]** to save the changes.

Copyright © 2024 ARMATURA LLC. All rights reserved

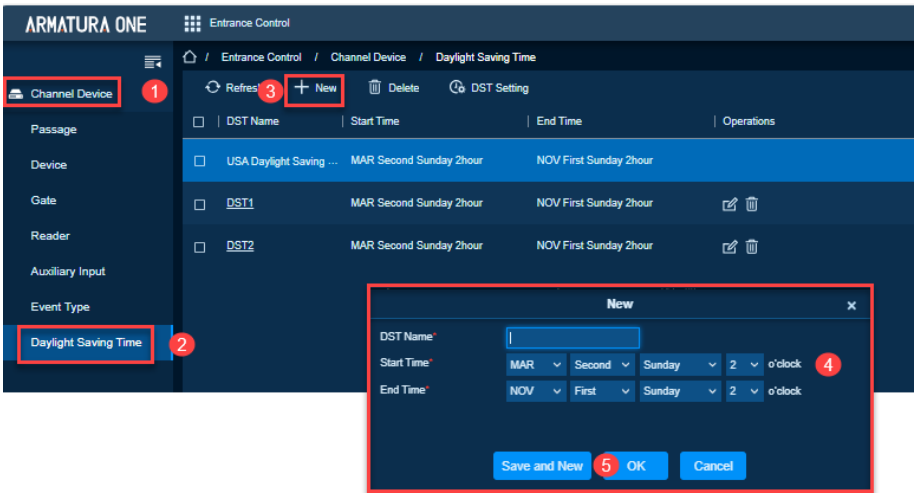
7.1.7 Daylight Saving Time

Daylight Saving Time (DST) adjusts the system's clock forward or backward by one hour during specified periods to save energy. This feature allows users to configure DST start and end times based on regional requirements.

Add New DST Configuration

Navigate to **[Entrance Control] > [Channel Device] > [Daylight Saving Time]**.

Click **[New]** to open the DST configuration page.



Example Start Time: "Second Monday in March, 02:00" – The system will advance by one hour at this time.

Example End Time: "First Sunday in November, 02:00" – The system will revert by one hour at this time.

Parameter	How to set
DST Name	Enter any character combination of up to 20 characters (must be unique).
Start and End Time	Set as "Month-Weeks-Week Day: Hour: Minute". Both start and end times are required.

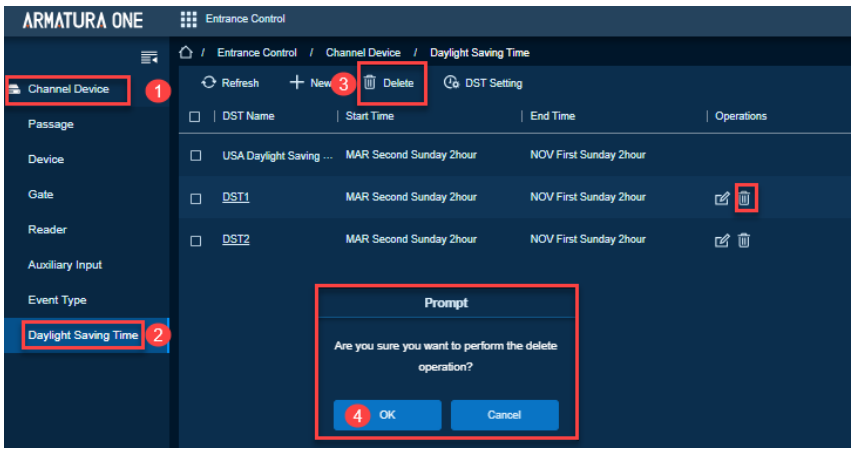
- **After entering the required parameters, click [OK] to save the DST configuration.**

Delete DST Configuration

Steps:

- Navigate to **[Entrance Control] > [Channel Device] > [Daylight Saving Time]**.
- Select the DST configuration to be deleted.
- Click **[Delete]** and confirm by clicking **[OK]** to remove the DST configuration.

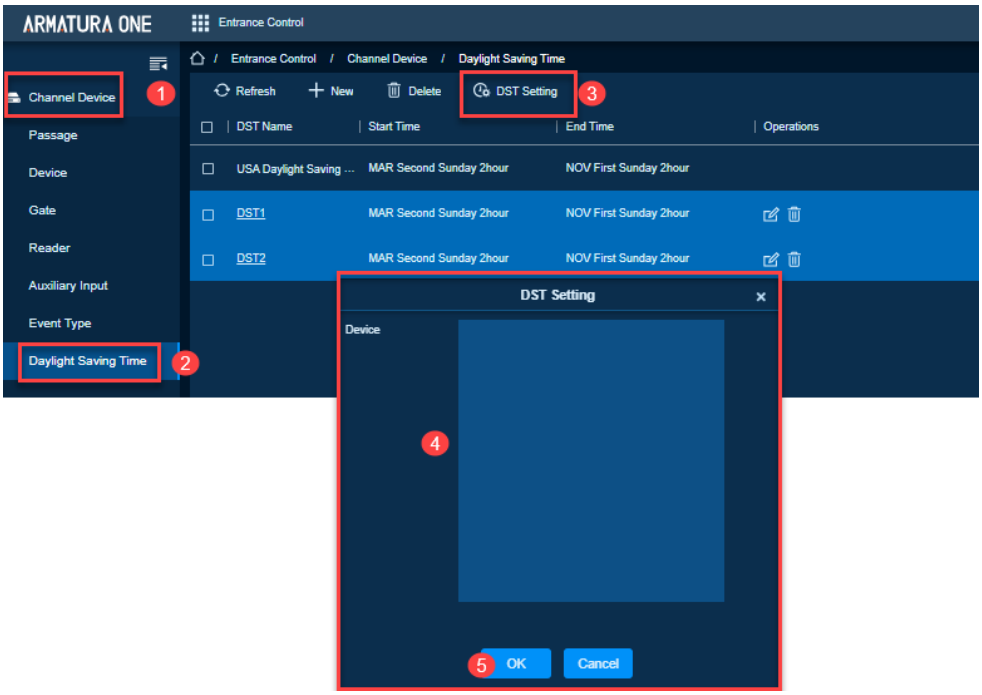
Copyright © 2024 ARMATURA LLC. All rights reserved



Set DST for a Device

Steps:

- Navigate to **[Entrance Control] > [Channel Device] > [Daylight Saving Time]**.
- Select the DST configuration that needs to be applied.
- Click **[DST Setting]** to open the device selection window.
- Choose the device(s) from the list.



- Click **[OK]** to save and apply the settings.

Edit DST Configuration

Prerequisites for Use

The system requires an existing DST configuration.

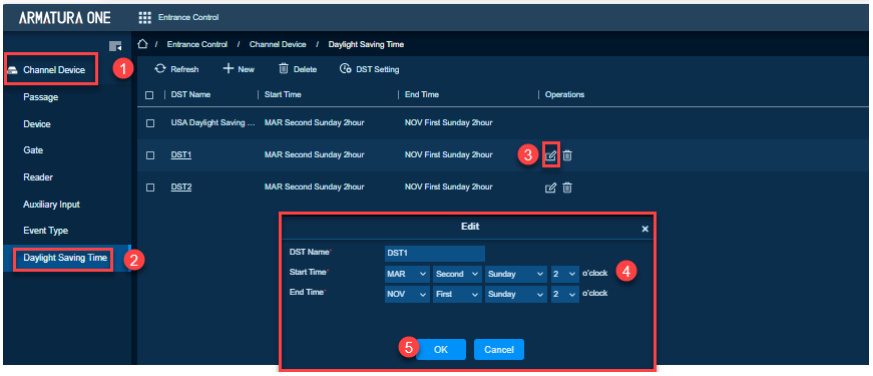
Usage Scenarios

Copyright © 2024 ARMATURA LLC. All rights reserved

This function enables modification of existing DST settings to align with updated time parameters.

Trigger Result

The system implements and saves the updated DST parameters.



Steps:

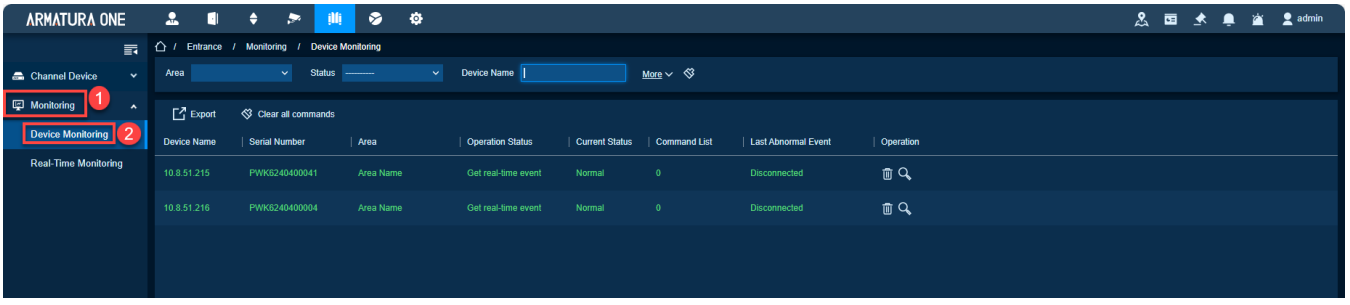
- Navigate to **[Channel Device] > [Daylight Saving Time]**.
- Click the **Edit** icon under **Operations** next to the DST configuration.
- Modify the desired details of the DST.
- Save the changes by clicking **[OK]**.

7.2 Monitoring

7.2.1 Device Monitoring

The **Device Monitoring** feature provides an overview of all devices under the current user's access level. It includes operational details like device name, serial number, area, operational status, commands list, and related operations.

Accessing Device Monitoring: Navigate to **[Entrance Control] > [Channel Device] > [Device Monitoring]** to view a list of device details.



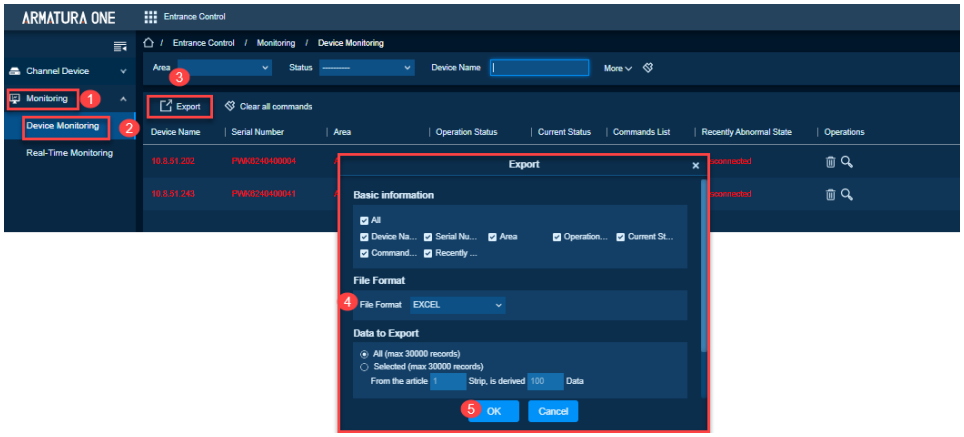
Export Device Commands:

Export a list of device commands for reporting or auditing purposes.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

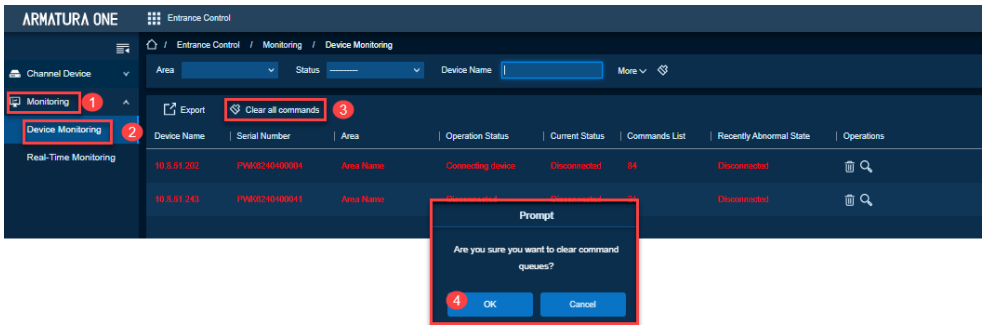
- Click **[Entrance Control] > [Channel Device] > [Device Monitoring]**.
- Click **[Export]**.
- Choose a file format: Excel, PDF, or CSV, and download the exported file.



Clear All Commands: Remove unnecessary or outdated commands from the command queue.

Steps:

- Navigate to **[Entrance Control] > [Monitoring] > [Device Monitoring]**.
- Select the commands you wish to delete.
- Click **[Clear All Commands]** in the operations column to remove them.

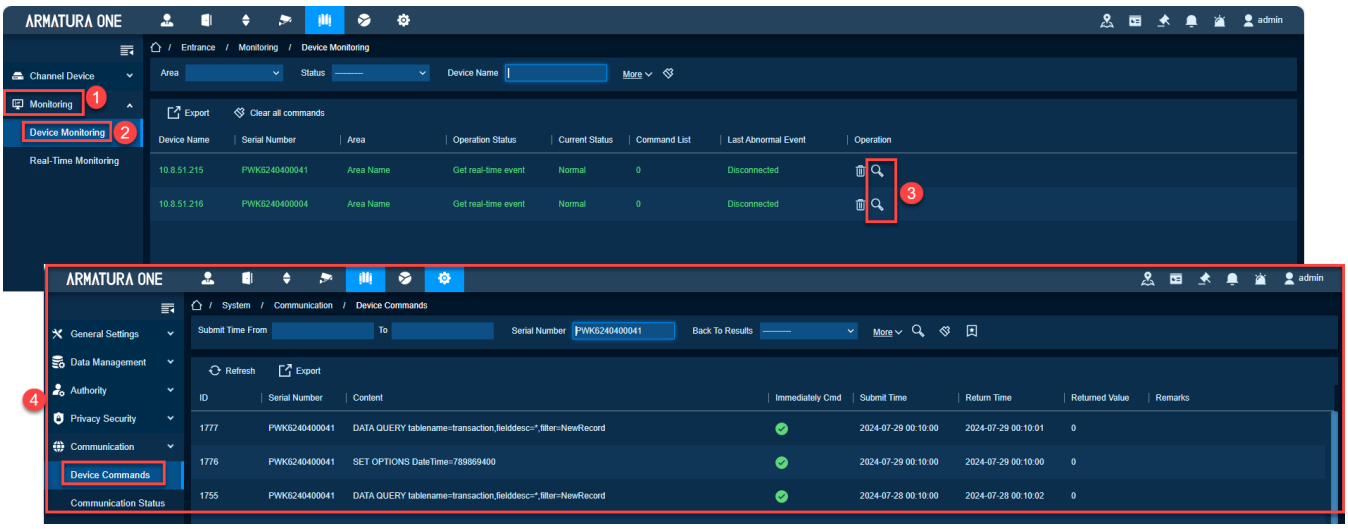


View Commands: Review the list of commands sent to a specific device.

Steps:

- In the **Device Monitoring** interface, locate the desired device.
- Click the **[View Command]** icon to open a detailed list of commands, including their status and execution details.

Copyright © 2024 ARMATURA LLC. All rights reserved



7.2.2 Real-Time Monitoring

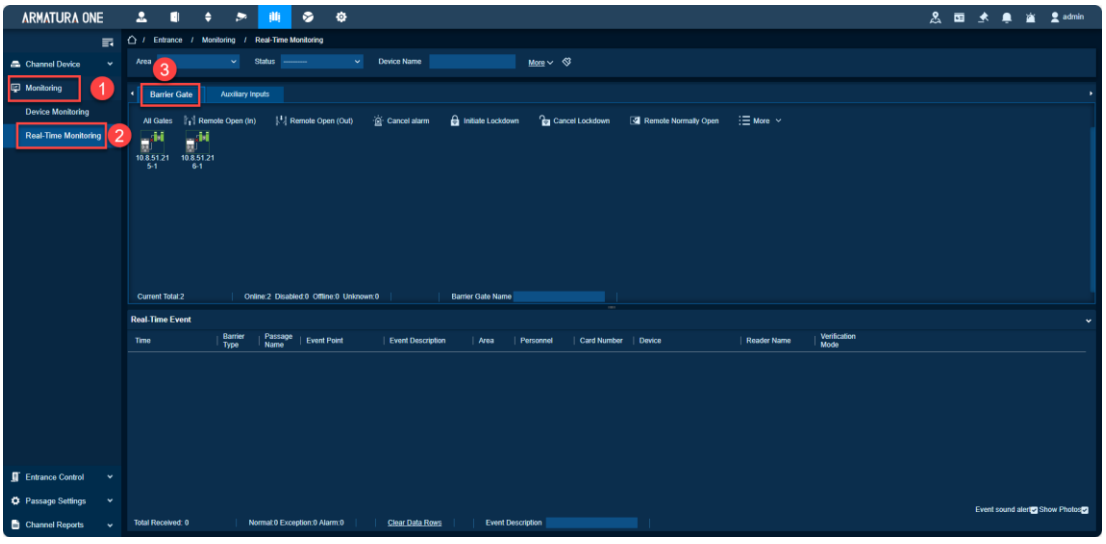
The Real-Time Monitoring feature provides an intuitive interface for overseeing the operational status of connected devices, including gates, sensors, and auxiliary inputs. Users can execute remote operations such as opening and closing gates, canceling alarms, initiating or canceling lockdowns, and configuring operational modes. This functionality enables comprehensive real-time management of the access control system.

Remote Gate Opening (in)/(out)

The system allows for remote opening of gates either **In** or **Out**.

Steps:

- Navigate to **[Entrance Control] > [Monitoring] > [Real-Time Monitoring]**.
- Check the icon status of the connected devices to confirm they are online.
- Locate the desired gate under **[Barrier Gate]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

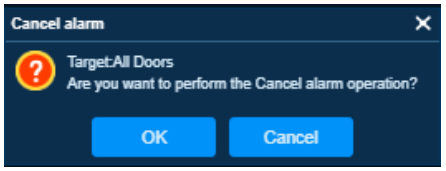
- Select an online gate device and click **[Remote Opening In]** (similar steps apply for **Out**).
- A security prompt will request the user's password. Enter the password and click **[OK]**.
- On the remote door-opening screen, specify the desired opening time and click **[OK]**.
- If successful, the system will display "Operation succeeded," completing the process.

Cancel the alarm

This feature allows users to stop active alarm notifications for a specific gate or all gates.

Steps:

- Navigate to **[Channel Device] > [Real-Time Monitoring]**.
- Identify and select the alarmed gate.
- Click **[Cancel the Alarm]** to deactivate the alarm.



Note:

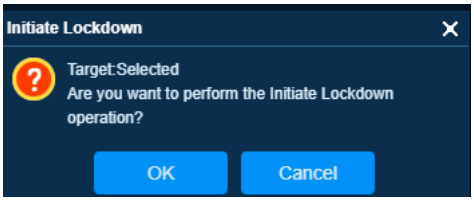
If alarm cancellation fails, verify the device's network connection and ensure it is not disconnected.

Initiate Lockdown

Use this option to remotely set a gate to lockdown mode. In this mode, the door will not respond to card readings or remote operations.

Steps:

- Navigate to **[Channel Device] > [Real-Time Monitoring]**.
- Select the desired gate and click **[Initiate Lockdown]**.
- Confirm the status change, indicating the gate is now locked.



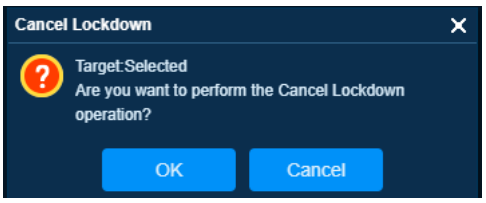
Note:

This feature is supported only on specific devices.

Cancel Lockdown

This feature cancels an active lockdown, restoring normal operations.

Copyright © 2024 ARMATURA LLC. All rights reserved

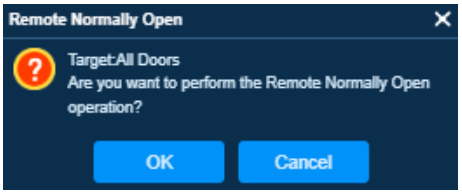


Steps:

- Navigate to **[Channel Device] > [Real-Time Monitoring]**.
- Select the locked gate and click **[Cancel Lockdown]**.
- Confirm the action to unlock the gate.

Remote Normally Open

Configure a gate to remain in a permanently open state using this feature.



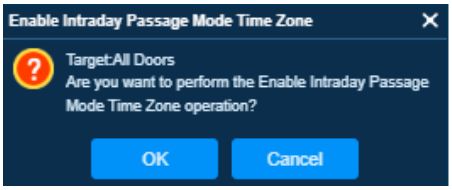
Steps:

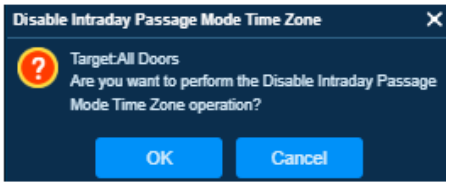
- Navigate to **[Channel Device] > [Real-Time Monitoring]**.
- Select the target gate and click **[Remote Normal Open]**.
- Confirm the configuration to enable the "Normally Open" status remotely.

More Options

Enable/Disable Intraday Passage Mode Time Zone:

1. **Enable:**
    - Allows defining door opening durations. By default, this is set to 15 seconds.
    - Enable the **Intraday Passage Mode Time Zone** to configure specific time zones or set the door to remain open 24/7.





1. **Disable:**
    - Prevent time zones from keeping the door open by disabling **Intraday Passage Mode Time Zone**.
    - Follow up with **Remote Closing** to ensure the door is closed.

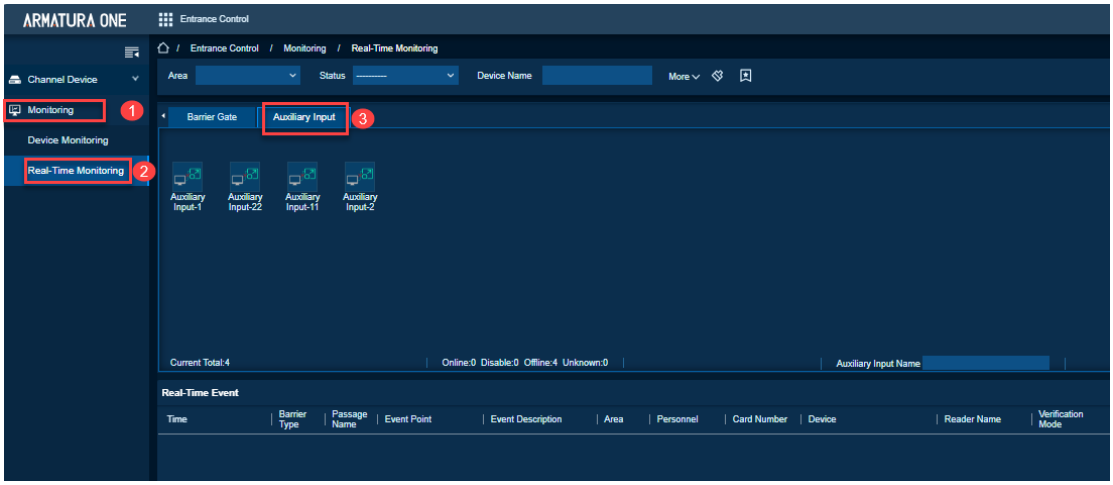
Copyright © 2024 ARMATURA LLC. All rights reserved

Auxiliary Input Monitoring

Monitor real-time statuses of connected auxiliary devices, such as infrared sensors or smog detectors.

Steps:

- Navigate to **[Entrance Control] > [Channel Device] > [Real-Time Monitoring]**.
- Select **[Auxiliary Input]** to view the list of connected auxiliary devices and their real-time statuses.



7.3 Entrance Control

By configuring gate authority groups and assigning them to personnel, users can effectively control access to gates. This section also supports advanced configurations, such as Anti-Passback and linkage settings, to meet complex entry and exit requirements.

7.3.1 Barrier Gate Permission Group

Function Description

Organizing gates into permission groups is essential for access control. This process involves creating permission groups, assigning gates to the groups, and defining the associated zones.

Creating a New Gate Permission Group

Steps:

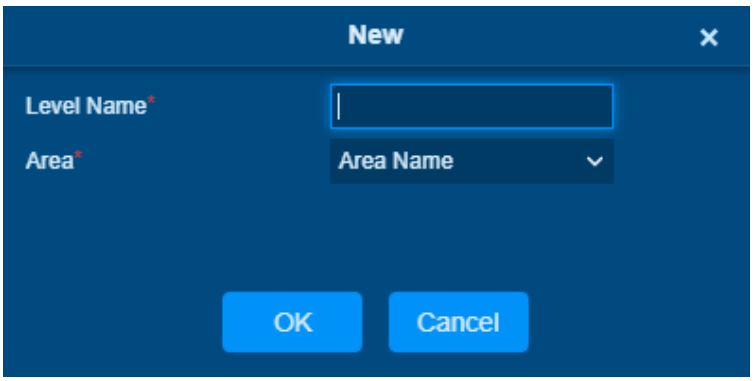
Navigate to the Barrier Gate Permission Group Interface:

- Go to **[Entrance Control] > [Barrier Gate Permission Group].**
- Click **[New]** in the left column to open the gate permission group creation interface.

Fill in Group Details:

- Provide the required parameters as outlined below.

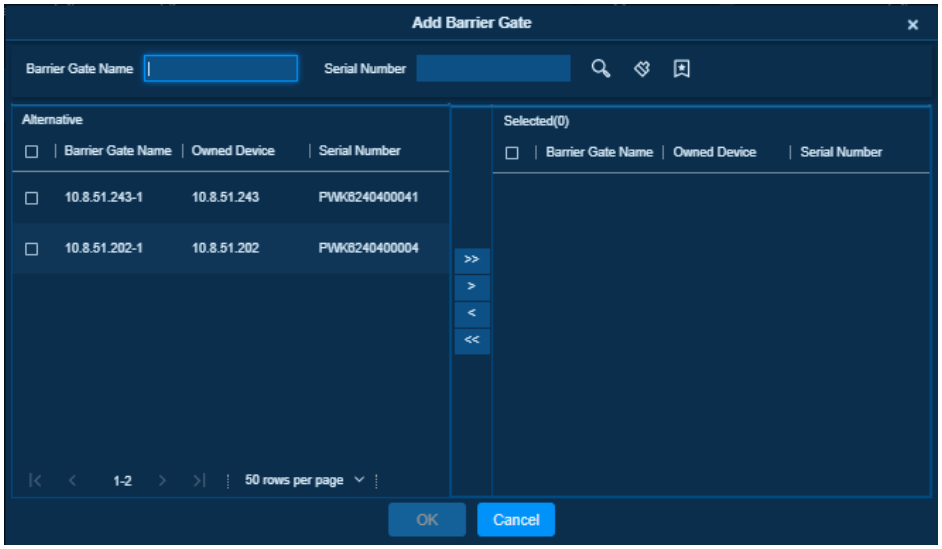
Copyright © 2024 ARMATURA LLC. All rights reserved



Parameter	How to set
Level Name	Enter a unique name with a combination of up to 20 characters. It must not be repeated.
Area	Assign the group to a specific zone. Users with permissions in this zone can manage the group.

Description of Added Gate Permission Parameters

- Click **[OK]** to save the new permission group.
- In the permission group interface, click the **[Add Barrier Gate]** icon next to the group.
- A selection interface will appear. Choose the gates to include in the group.



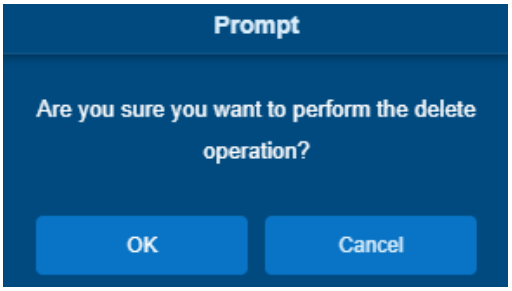
- Click **[OK]** to complete the gate permissions setup.

Copyright © 2024 ARMATURA LLC. All rights reserved

Delete a Gate Permission Group

Steps:

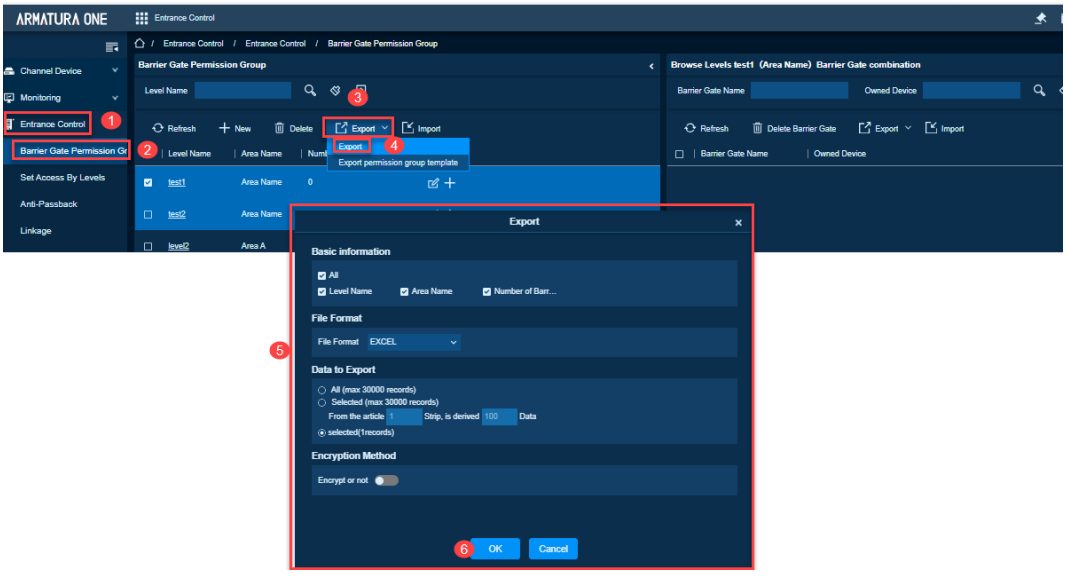
- Go to **[Entrance Control] > [Barrier Gate Permission Group]** and select the group to delete.
- Click **[Delete]** and confirm by clicking **[OK].**



Exporting Gate Permission Details

Steps:

- Go to **[Entrance Control] > [Barrier Gate Permission Group].**
- Click **[Export]** to export records in **Excel, PDF, or CSV** formats.



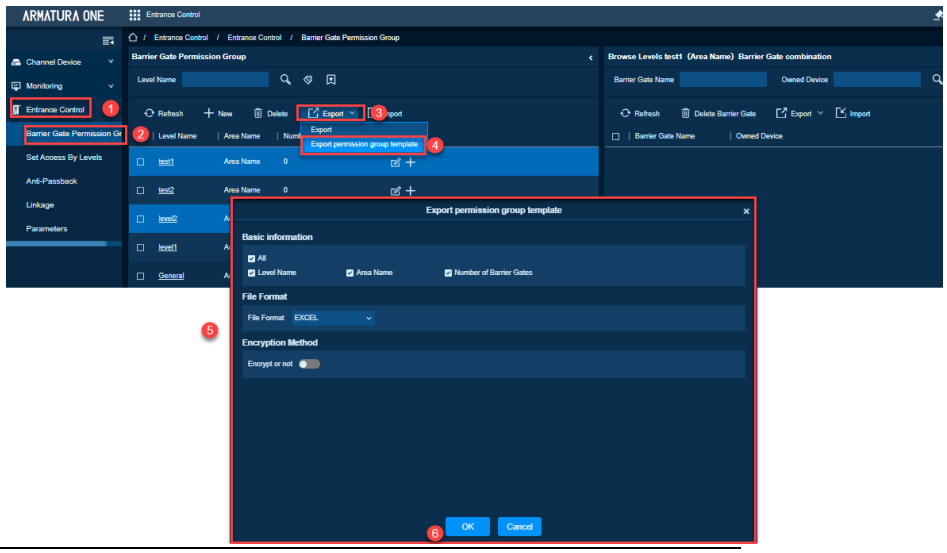
Enter your password when prompted, select the file format, and click **[OK].**

Exporting Permission Group Template

Steps:

- Navigate to **[Entrance Control] > [Barrier Gate Permission Group].**
- Click **[Export Permission Group Template].**

Copyright © 2024 ARMATURA LLC. All rights reserved



- Enter your password, choose the file format (Excel, PDF, or CSV), and click **[OK].**

Importing Permission Group Details

Prerequisites for Use

Administrative privileges for the import function. A template matching the software language must be prepared with valid personnel IDs. Correctly formatted certificate types, certificate numbers, mobile numbers, and email addresses. Start dates that are not earlier than the current date.

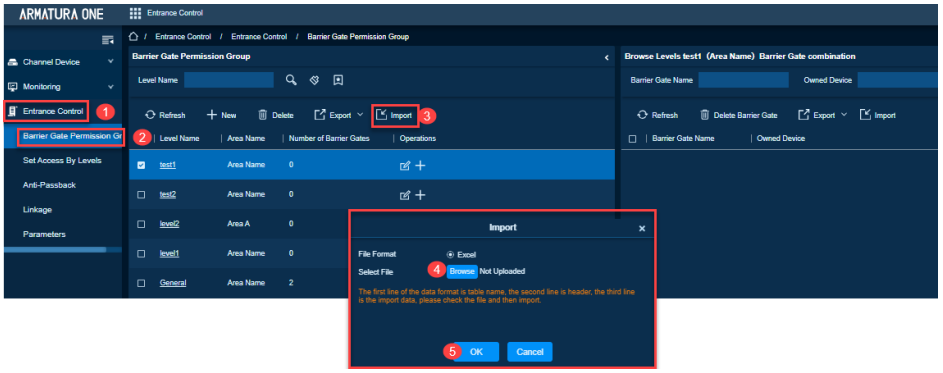
Usage Scenarios

For teams with two or more members, export the appointment template, fill in the required details, and use the import function to complete the permission group setup.

Trigger Result

Operations	Description
Import Template	Add all personnel in the imported form to the appointment list.

Steps:



Copyright © 2024 ARMATURA LLC. All rights reserved

- Click **[Import].**
- In the pop-up, click **[Browse]** to select the template.
- Click **[OK]** to import and complete the setup.

Editing a Barrier Gate Permission Group

Prerequisites for Use

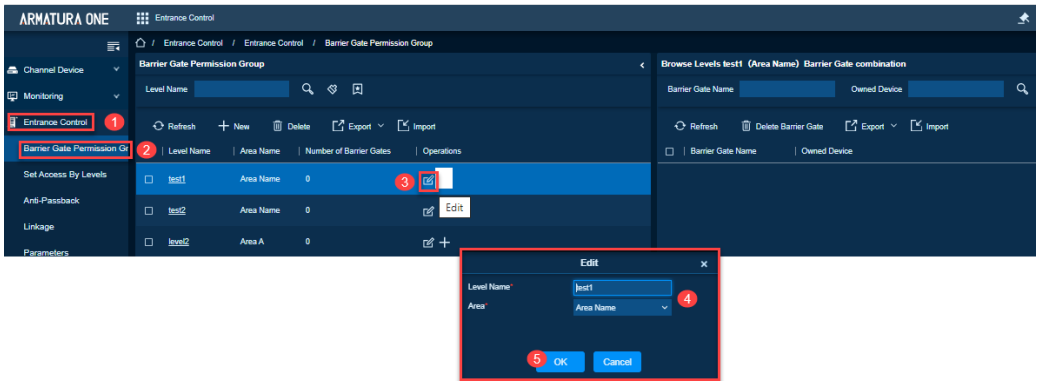
The permission group must already exist in the system.

Usage Scenarios

When details of an existing permission group need to be updated.

Trigger Result

Updated information will be reflected in the permission group configuration.



Steps:

- Navigate to **[Entrance Control]** > **[Barrier Gate Permission Group]**.
- Click the **[Edit]** icon next to the group to be modified.
- Make the necessary changes and click **[OK]** to save.

7.3.2 Set Access By Levels

This function enables the assignment of gate permission groups to designate personnel. By associating personnel with specific permission groups, you can effectively manage access control to barriers.

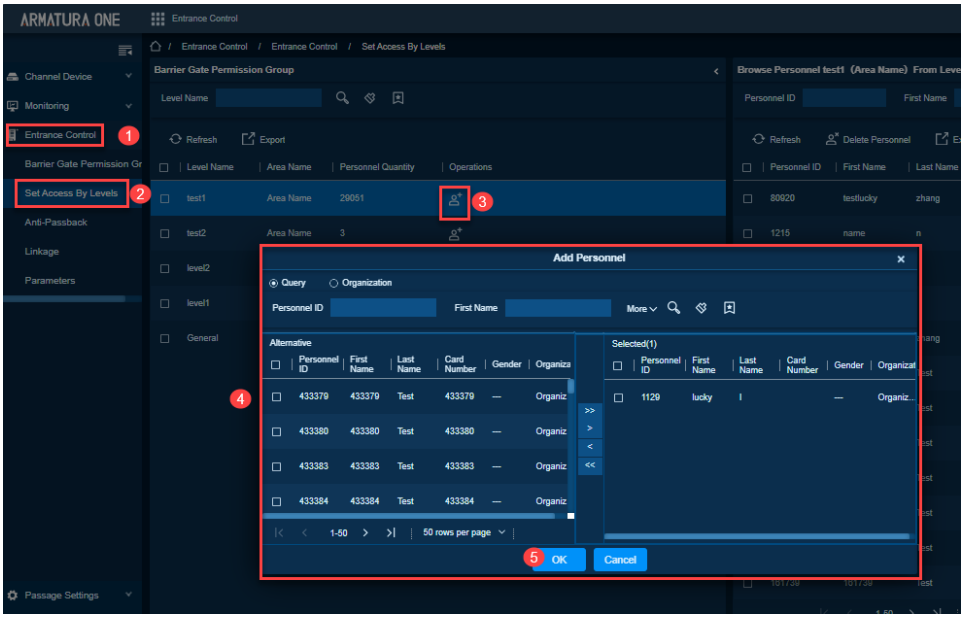
Add Person to Permission Group

Steps:

- In the **Entrance Control** module, go to **[Entrance Control] > [Set Access By Levels].**
- Click the **[Add Person]** icon in the operation bar of the corresponding permission group. This will open the **Add Person** interface.

Copyright © 2024 ARMATURA LLC. All rights reserved

- In the pop-up interface, select the relevant personnel for the permission group. Ensure that the individuals meet the requirements for access control.

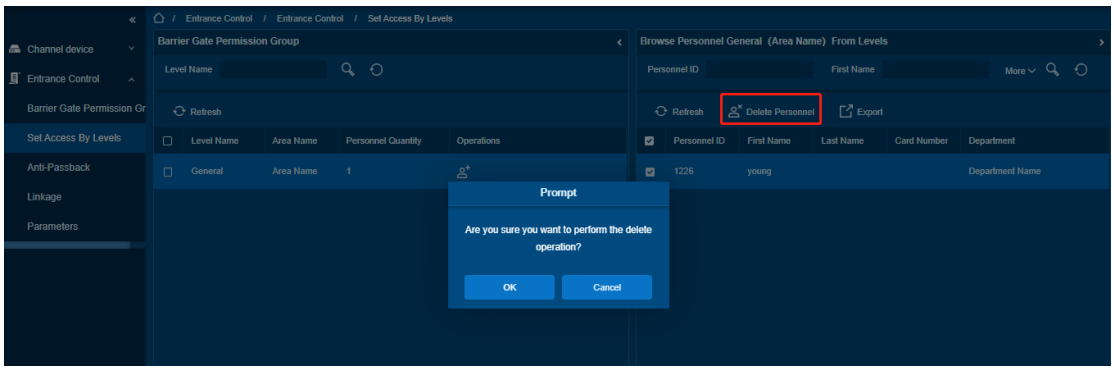


- Click **[OK]** to finalize the assignment of personnel permissions to the group.

Delete Personnel from Permission Group

Steps:

- Go to **[Entrance Control] > [Set Access By Levels].**
- Identify the individual to be removed from the permission group.
- Click **[Delete Personnel]** and confirm the action by clicking **[OK].** The individual will no longer have access permissions associated with this group.



Export Barrier Gate Permission Details

User can export barrier gate details into an Excel, PDF, or CSV file. See figure below.

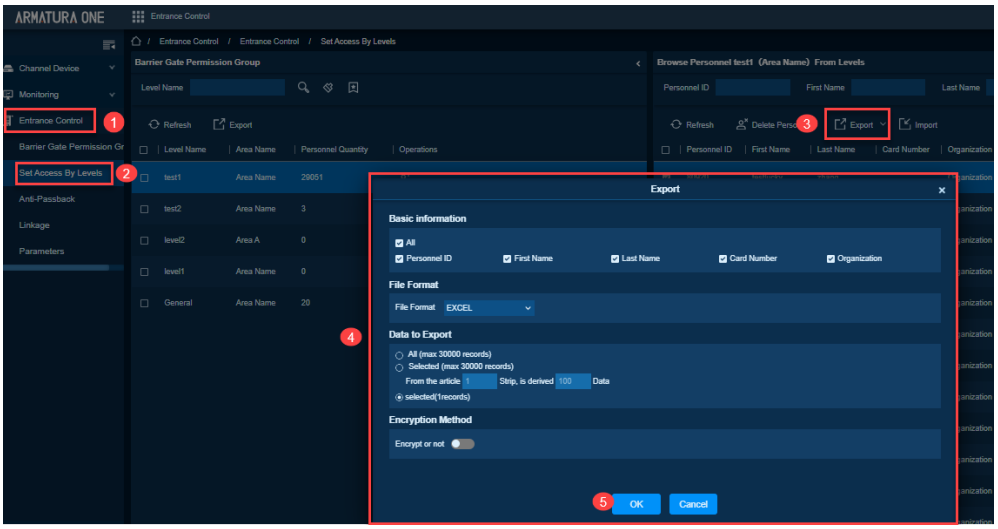
Usage Scenarios

Generate detailed records of personnel assigned to gate permission groups for auditing or documentation.

Steps:

Copyright © 2024 ARMATURA LLC. All rights reserved

- In **[Entrance Control] > [Set Access By Levels],** click **[Export].**
- Enter the user password when prompted, and select the desired export format (Excel, PDF, or CSV).



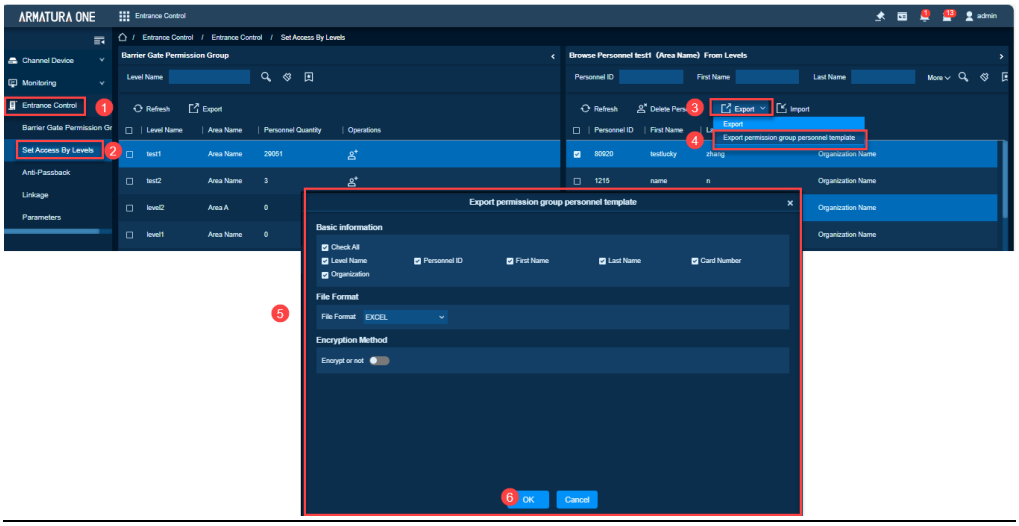
- Click **[OK]** to save the file locally.

Export Permission Group Personnel Template

Prepare a template for batch operations, including adding new personnel to permission groups.

Steps:

- Navigate to **[Entrance Control] > [Set Access By Levels]** and click **[Export Permission Group Template].**
- Enter the user password when prompted and select the desired export format (Excel, PDF, or CSV).



- Click **[OK]** to download the template.

Copyright © 2024 ARMATURA LLC. All rights reserved

Import Personnel Data into Permission Group

Prerequisites for Use

The system requires administrator privileges, language-matched import templates, and accurate personnel records with valid IDs, certificate information, contact details, and start dates.

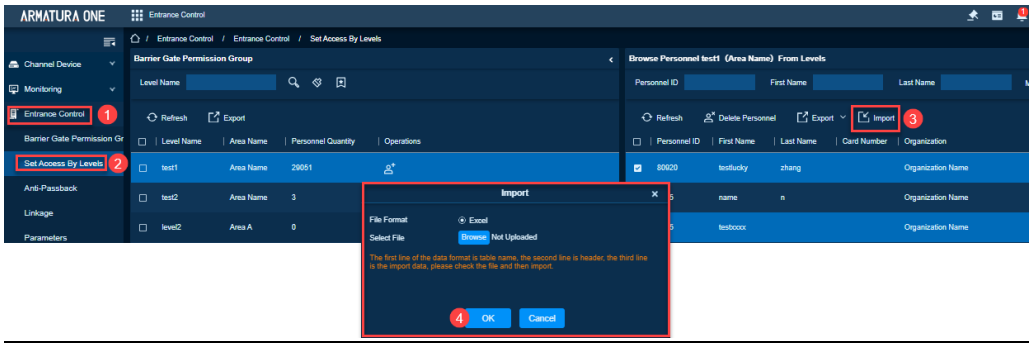
Usage Scenarios

This function enables bulk personnel additions and permission assignments for efficient team management.

Trigger Results

Operations	Description
Import Template	Updates permission group memberships based on the imported personnel data.

Steps:



- In the permission group interface, click **[Import].**
- Click **[Browse]** in the pop-up window and choose the completed import template file.
- Click **[OK]** to process the file and assign personnel to the permission group.

7.3.3 Anti-Passback

Anti-Passback is a security feature requiring cardholders to swipe their cards for both entry and exit through specified channels. It ensures strict adherence to one entry and one exit sequence, enhancing security in sensitive environments like special units, research facilities, and bank vaults.

Add New Anti-Passback

Steps:

- In the **Entrance Control** module, go to **[Entrance Control] > [Anti-Passback].**
- Click **[New]** to open the configuration interface.
- Choose the specific devices to be included in the Anti-Passback configuration.

Copyright © 2024 ARMATURA LLC. All rights reserved

Note:

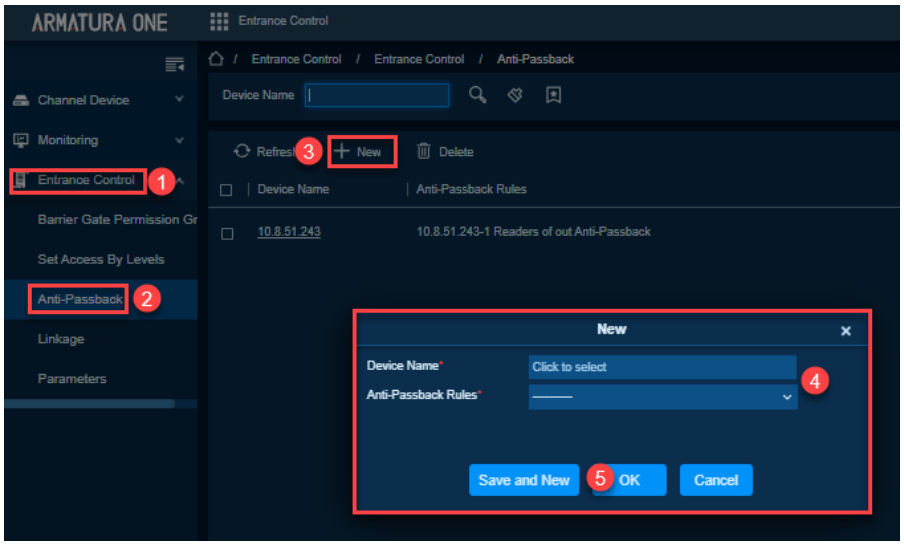
Devices already configured for Anti-Passback will not appear in the device list.

Deleted Anti-Passback information will make the devices reappear in the list for future configurations.

Select the desired **Anti-Passback Rule** from the options provided.

Examples include ensuring cardholders swipe cards at entry and exit points through different channels.

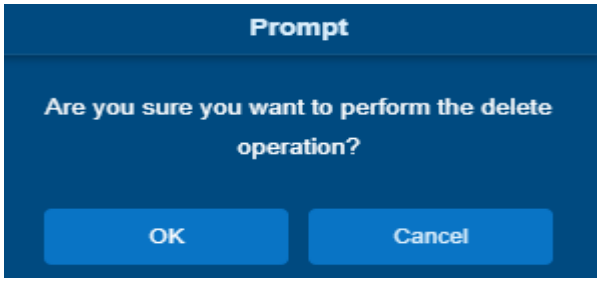
Click **[OK]** to save the settings. The newly configured Anti-Passback settings will now appear in the Anti-Passback rule list.



Delete Anti-Passback

Steps:

- Go to **[Entrance Control] > [Anti-Passback].**
- Identify the device or Anti-Passback rule to remove from the list.
- Click **[Delete]** and then **[OK]** to confirm and remove the Anti-Passback settings.



Edit Anti-Passback

Prerequisites for Use

The device name must already exist in the Anti-Passback configuration.

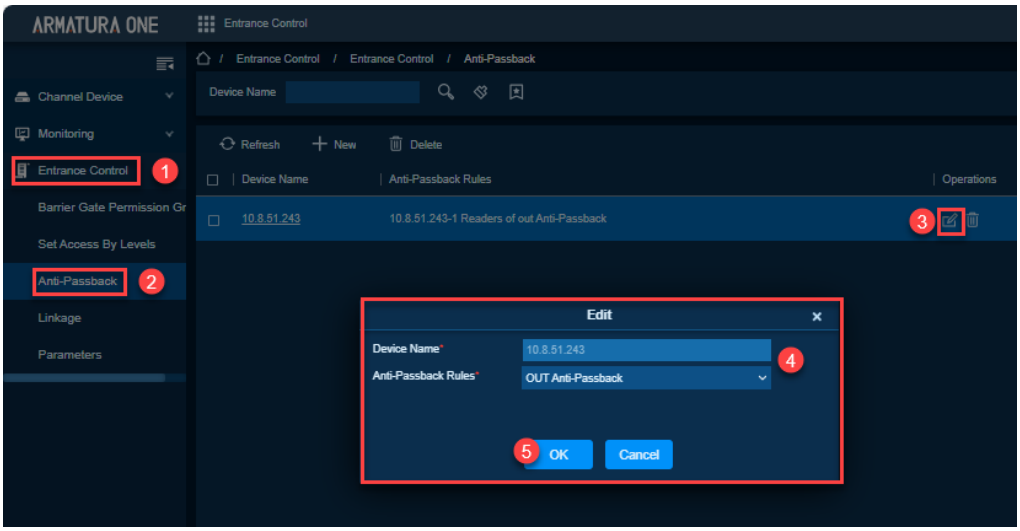
Usage Scenarios

Modify existing Anti-Passback settings to accommodate updated requirements or rectify errors.

Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Ensures updated and accurate Anti-Passback configuration.



Steps:

- Open **[Entrance Control] > [Anti-Passback].**
- Click the **[Edit]** icon under the operations column corresponding to the Anti-Passback rule.
- Modify the device name or other Anti-Passback settings as needed.
- Confirm updates by clicking **[OK].**

7.3.4 Linkage

Function Description

The Linkage function triggers specific actions (e.g., gate operations, alarms, or system notifications) when an event occurs at a designated input point. These actions are executed at a corresponding output point and displayed in real-time monitoring.

Prerequisites for Use

Before configuring a new linkage, ensure the following:

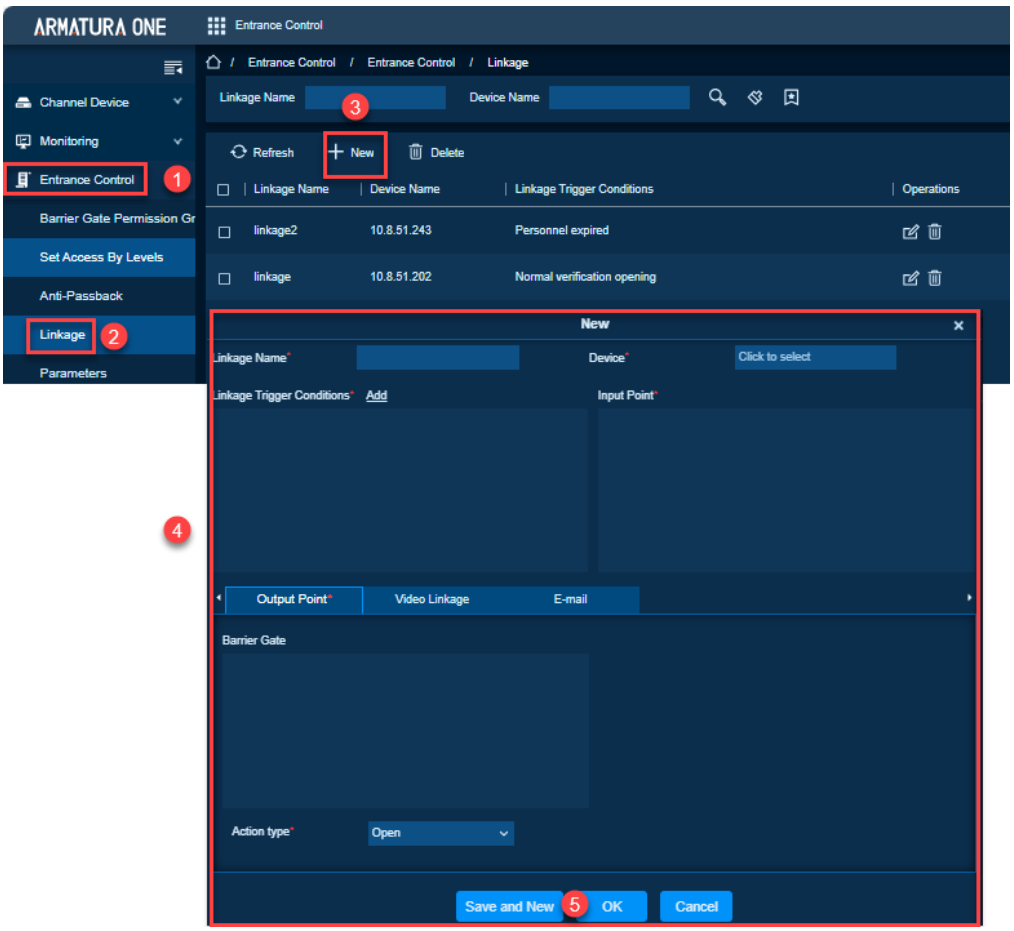
1. **Gate Device Setup:** Input and output points, as well as cameras, must be added and configured.
2. **Mailbox Configuration:** Ensure email parameters are set up to send notifications.

Add New Linkage

Steps:

- In the **Entrance Control** module, select **[Entrance Control] > [Linkage]**.
- In the Linkage Settings interface, click **[New]** to open the configuration form.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Fill in the required parameters as described below:

Parameter	Description
Linkage name	Custom name for the linkage, making it easy to reference later.
Device	Select the access control device to be linked.
Linkage trigger Conditions	Specify the condition (event type) that will trigger the linkage operation.
Input point	Choose the device's input point for triggering the action.
Output point	Select the output point where the linkage action will occur.
Action Type	Define the linkage action type, including device operations, video linkage, and email notifications.

- Configure the linkage actions based on the requirements:

Parameter	How to set
Output point operation	Choose between **Closed**, **Open**, and **Normally Open**. Set the delay time for the output point action if required.

Copyright © 2024 ARMATURA LLC. All rights reserved

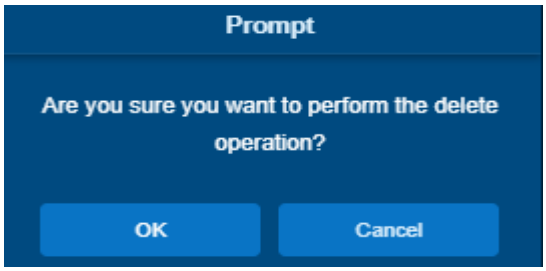
Parameter	How to set
Video linkage	Enable **Pop-Up Video** with a set display duration, or enable **Recording** and specify the duration. Optionally configure **Capture** to take photos and set their display settings in real-time monitoring.
E-Mail	Enter the recipient's email address to receive notifications for triggered events.

- Click **[OK]** to save and finalize the linkage settings. The newly added linkage will now appear in the linkage list.

Delete Linkage

Steps:

- Go to **[Entrance Control] > [Linkage].**
- Identify the linkage to remove from the list.
- Click **[Delete]** and confirm by selecting **[OK]** to finalize the removal.



Edit Linkage

Prerequisites for Use

A Linkage Name must already exist in the system.

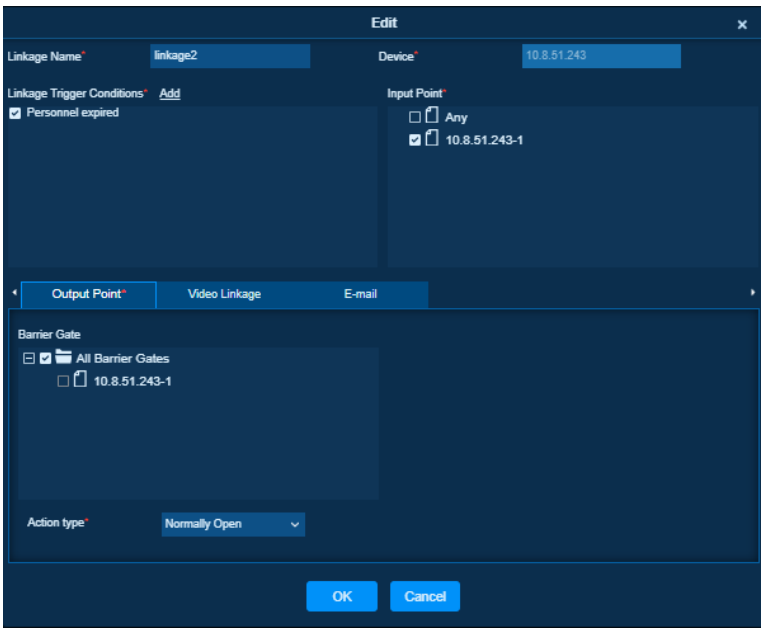
Usage Scenarios

Modify existing linkage configurations to accommodate updated requirements or rectify errors.

Trigger Result

The updated linkage settings will be applied to the system.

Copyright © 2024 ARMATURA LLC. All rights reserved



Steps:

- Go to **[Entrance Control] > [Linkage].**
- Click the **[Edit]** icon under the operations column corresponding to the Linkage Name.
- Modify the desired parameters as needed.
- Click **[OK]** to apply the modifications.

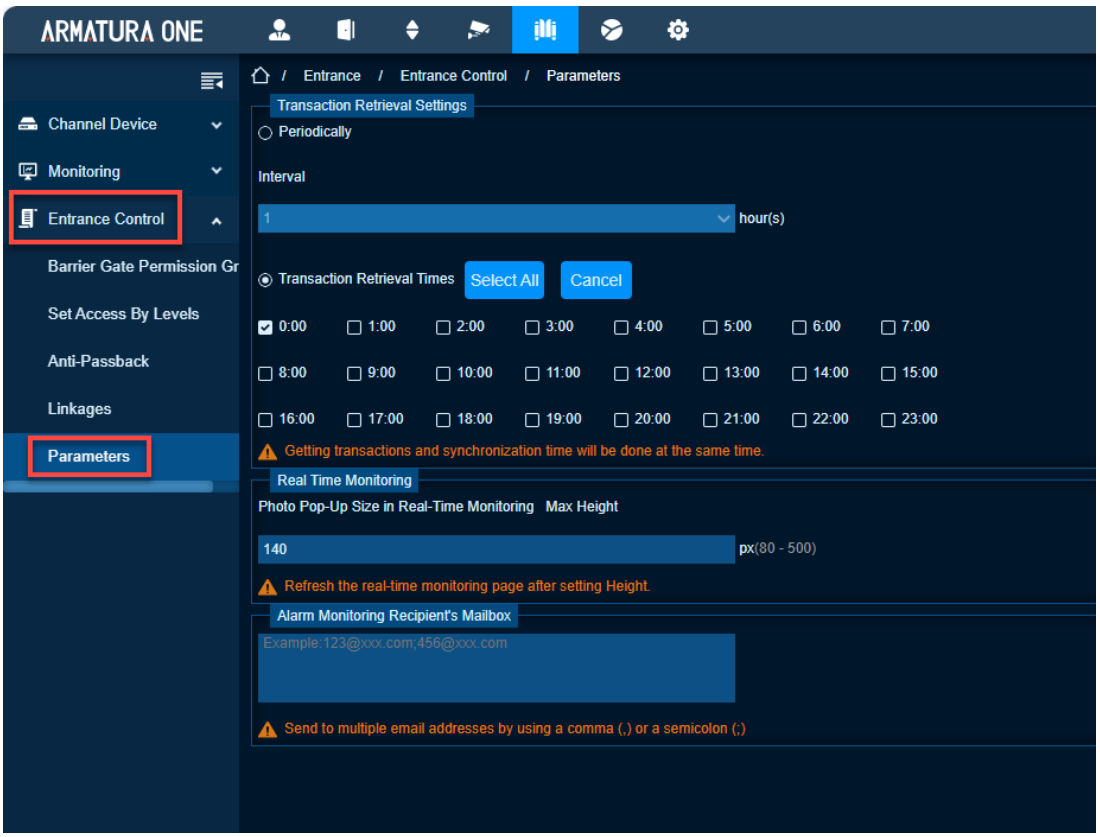
7.3.5 Parameters

The Parameters section allows users to customize transaction retrieval, real-time monitoring configurations, and email alert settings for efficient gate and system management.

Accessing the Parameter Settings

Navigate to **[Entrance Control]** > **[Entrance Control]** > **[Parameter]** to open the parameter setting interface.

Copyright © 2024 ARMATURA LLC. All rights reserved



Feature	Description
Type of Getting Transactions	Configure how the system retrieves transactions from devices.
Periodically	The system retrieves new transactions at set intervals, starting from the specified activation time.
Transaction Retrieval Times	Automatically downloads new transactions when the specified time is reached.
Real-Time Monitoring Page Pop-Up Staff Photo Size	Configures the size of personnel photos that appear when an access control event is triggered. Photo size ranges from 80 to 500 pixels.
Alarm Monitoring Recipient's Mailbox	Enter the recipient's email address to receive notifications for triggered events.

Copyright © 2024 ARMATURA LLC. All rights reserved

7.4 Passage Settings

The Passage Settings module enables administrators to define gate traffic rules for managing access, controlling time periods, and configuring operational modes for gates such as flap barriers and swing barriers.

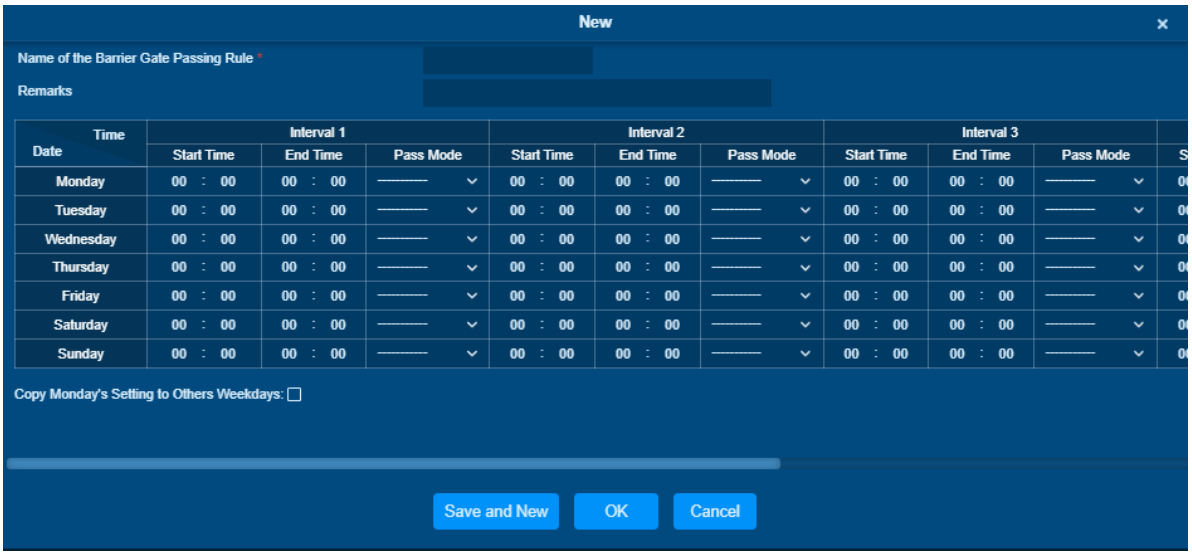
7.4.1 Barrier gate passing Rules

The Barrier Gate Passing Rules allow the configuration of passage modes and time intervals for gates, enabling different entry and exit functionalities during specified periods.

Add New Barrier Gate Passing Rules

Steps:

- Navigate to **[Entrance Control] > [Passage Settings] > [Barrier Gate Passing Rules].**
- Click **[New]** to open the interface for adding gate traffic rules.



Refer to the following table for parameter descriptions and configuration instructions:

Parameter	How to set
Name of the Barrier Gate Passing Rules	Enter a unique name for the rule, up to 30 characters.
Remarks	Provide an explanation of the rule, including its purpose and application. Maximum of 50 characters.
Time interval	Define up to 5 time intervals within a week.
Time Interval-Start/End time	Set the start and end time for each interval.
Pass Mode	Select a passage mode from the drop-down list. Default options include: *Two-way controlled*

Copyright © 2024 ARMATURA LLC. All rights reserved

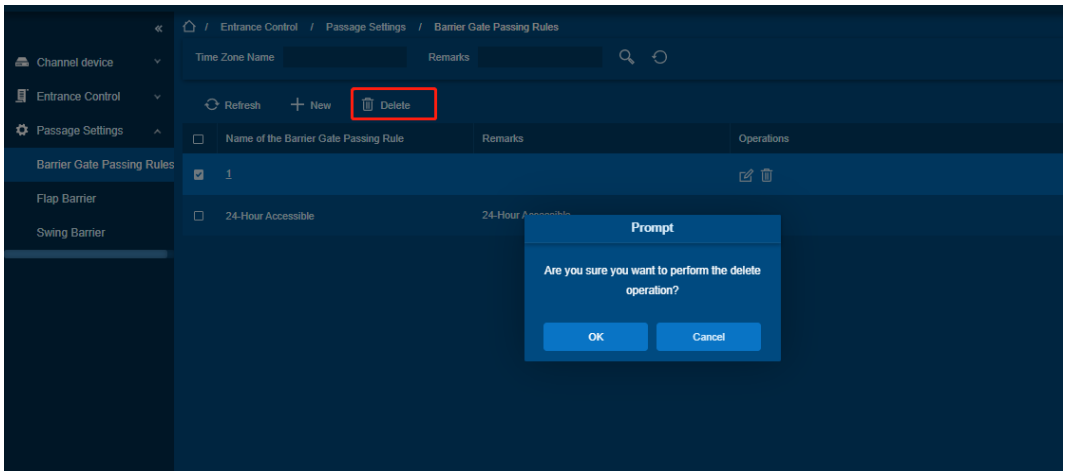
	Free entry and exit controlled *Controlled entry and exit free* *Two-way freedom* *Forbidden entry and exit controlled* *Forbidden entry and exit free entry* *Free entry and exit forbidden entry* *Two-way prohibition* *Remote normal opening* |
Copy Monday time to other working days	Quickly replicate Monday's settings to other workdays.

- After configuring the parameters, click **[OK]** to save and apply the new gate traffic rule.

Delete Barrier Gate Passing Rules

Steps:

- Navigate to **[Passage Settings] > [Barrier Gate Passing Rules].**
- Choose the rule to be deleted.



- Click **[Delete]** and confirm by clicking **[OK].**

Edit Barrier Gate Passing Rules

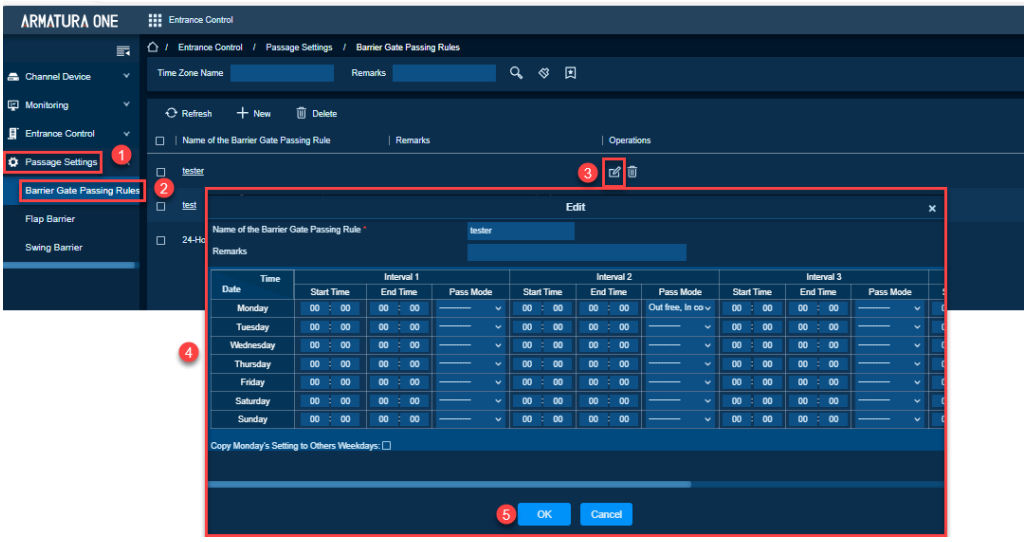
Prerequisites for Use

The **Barrier Gate Passing Rules** must be added before editing.

Usage Scenarios

Modify details such as time intervals, passage modes, or remarks.

Copyright © 2024 ARMATURA LLC. All rights reserved



Steps:

- Navigate to **[Passage Settings] > [Barrier Gate Passing Rules].**
- Click the **edit icon** under the operations column for the desired rule.
- Make the necessary adjustments to the rule.
- Click **[OK]** to save and apply the modifications.

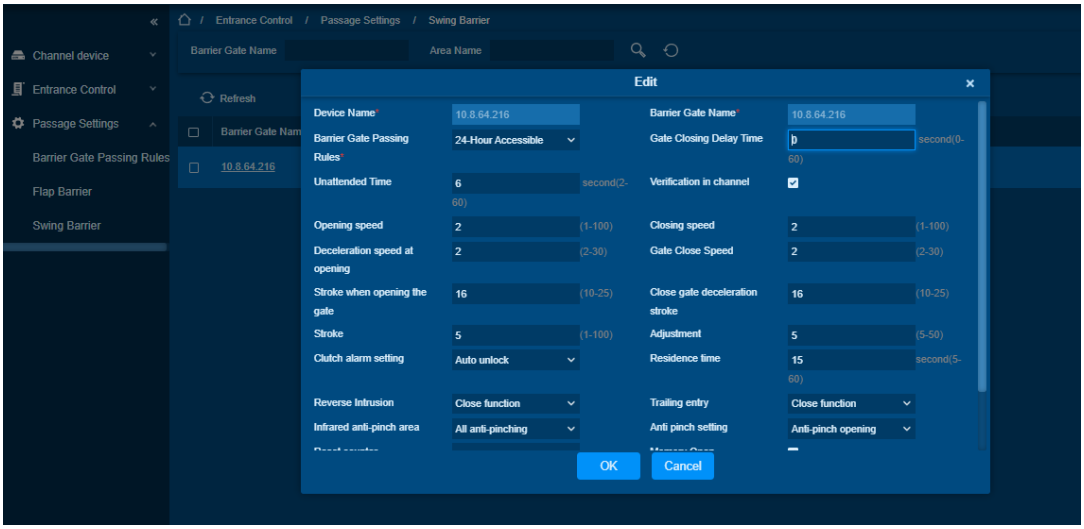
7.4.2 Swing Barrier

The Swing Barrier section explains the steps for configuring swing barrier parameters in the software, including editing settings and supported devices.

Steps:

- Navigate to **[Entrance Control] > [Passage Settings] > [Swing Barrier].**
- Locate the swing barrier name in the list and click the **[Edit]** button under the "Operations" column. This action will open the parameter editing interface.

Copyright © 2024 ARMATURA LLC. All rights reserved



After making the required adjustments to the swing barrier parameters, click **[OK]** to save the changes.

Device Name	Remark
SBT2011S	Only use as Access controller
SBT2022S	Only use as Access controller
SBTL7011	Only use as Access controller
SBTL7022	Only use as Access controller
SBTL9000	Access controller and turnstile gates controller.
SBTL9011	Access controller and turnstile gates controller.
SBTL9022	Access controller and turnstile gates controller.
SBTL9200	Access controller and turnstile gates controller.
SBTL9211	Access controller and turnstile gates controller.
SBTL9222	Access controller and turnstile gates controller oller.
Mars Pro-S1000	Access controller and turnstile gates controller.
Mars Pro-S1011	Access controller and turnstile gates controller.
Mars Pro-S1022	Access controller and turnstile gates controller.
Mars Pro-S1200	Access controller and turnstile gates controller.
Mars Pro-S1211	Access controller and turnstile gates controller.
Mars Pro-S1222	Access controller and turnstile gates controller.
Mars Pro-F1011	Only use as Access controller
Mars Pro-F1022	Only use as Access controller

Copyright © 2024 ARMATURA LLC. All rights reserved

MarsPro-F1211	Only use as Access controller
Mars Pro-F1222	Only use as Access controller
Mars-B1011	Only use as Access controller
Mars-B1022	Only use as Access controller
Mars-B1211	Only use as Access controller
Mars-B1222	Only use as Access controller
Mars-S1011	Only use as Access controller
Mars-S1022	Only use as Access controller
Mars-S1211	Only use as Access controller
Mars-S1222	Only use as Access controller
Mars-F1011	Only use as Access controller
Mars-F1022	Only use as Access controller
Mars-F1211	Only use as Access controller
Mars-F1222	Only use as Access controller

7.5 Channel Reports

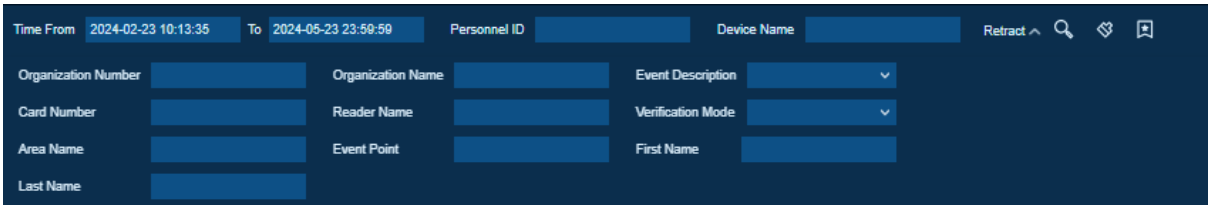
The Channel Reports feature provides users with the ability to query and manage various access control data sets. These reports include All Transactions, Today's Events, Person's Last Access Location, and All Exception Events. Users can query, export, or clear records as needed.

7.5.1 All Transactions

The All-Transactions section allows users to view and manage comprehensive records of all transaction data in the system. This includes querying data, exporting results, and clearing transaction reports.

Steps:

- Navigate to **[Entrance Control] > [Channel Reports] > [All Transactions].**
- In the **All Records** interface, enter the query criteria in the relevant fields.
- Click the **[More]** symbol to refine or expand your query. The queried data will appear in the results table.

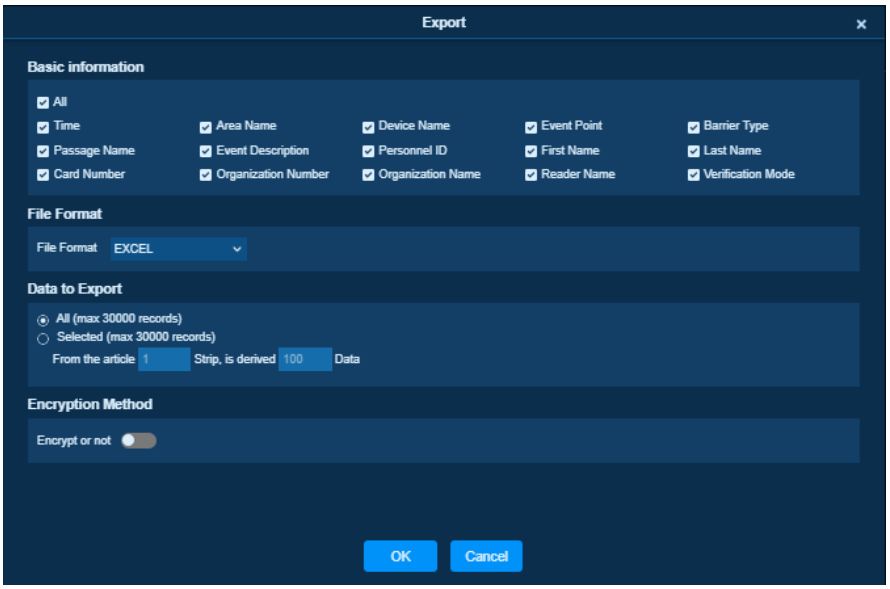


Copyright © 2024 ARMATURA LLC. All rights reserved

Export Records

Steps:

- In the **All-Transactions** interface, click **[Export].**
- When prompted, enter the **user password** for security verification, and click **[OK].**
- Choose the export format (e.g., **Excel**, **PDF**, or **CSV**) and determine whether to encrypt the file.
- Select the destination folder to save the file.

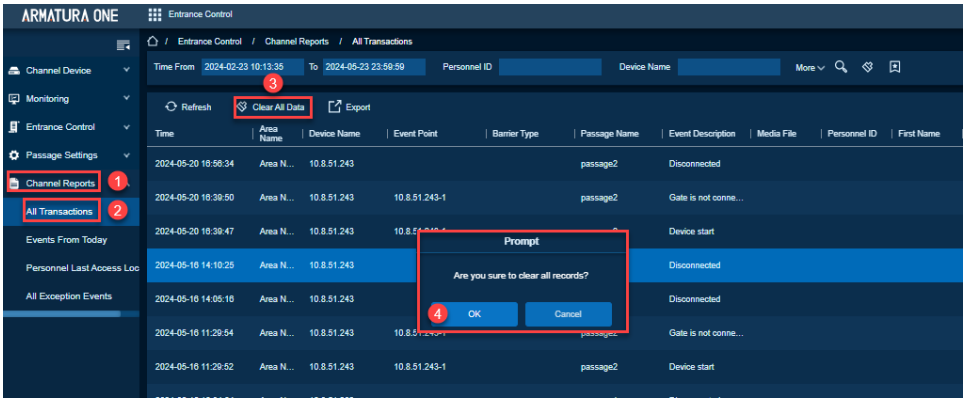


- Click **[OK]** to complete the export.

Clear All Data

Steps:

- In the **All-Transactions** interface, click **[Clear All Data].**
- A confirmation prompt will appear; click **[OK]** to confirm and clear all transaction records from the system.



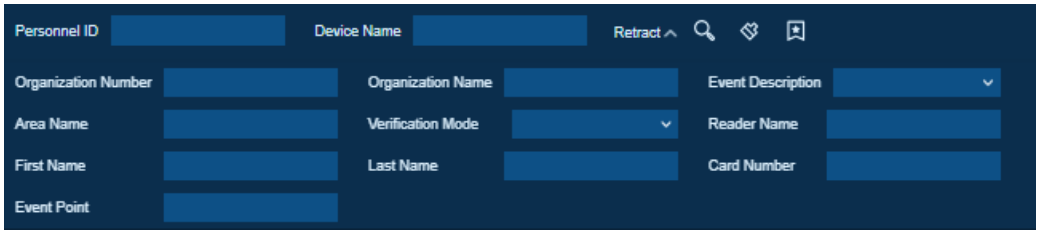
Copyright © 2024 ARMATURA LLC. All rights reserved

7.5.2 Events from Today

The Events from Today section provides a detailed display of all access records generated within the current day. Users can query specific events, export data, or clear today's records.

Steps:

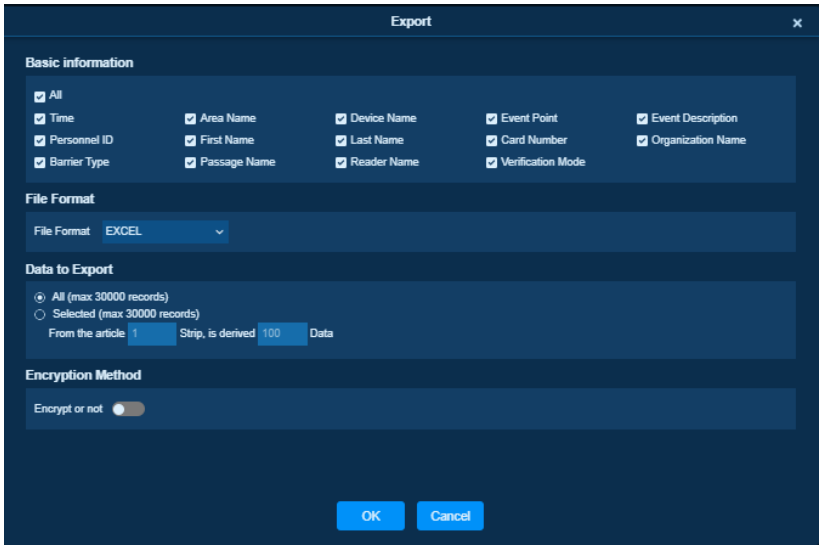
- Navigate to **[Entrance Control] > [Channel Reports] > [Events from Today].**
- In the **Today's Access Record** interface, enter the query criteria in the relevant fields.
- Click the **[More]** symbol to refine or expand your query. The queried access records will appear in the results table.



Export Records

Steps:

- In the **Today's Access Record** interface, click **[Export].**
- When prompted, enter the **user password** for security verification, and click **[OK].**
- Choose the export format (**Excel**, **PDF**, or **CSV**) and determine whether to encrypt the file.



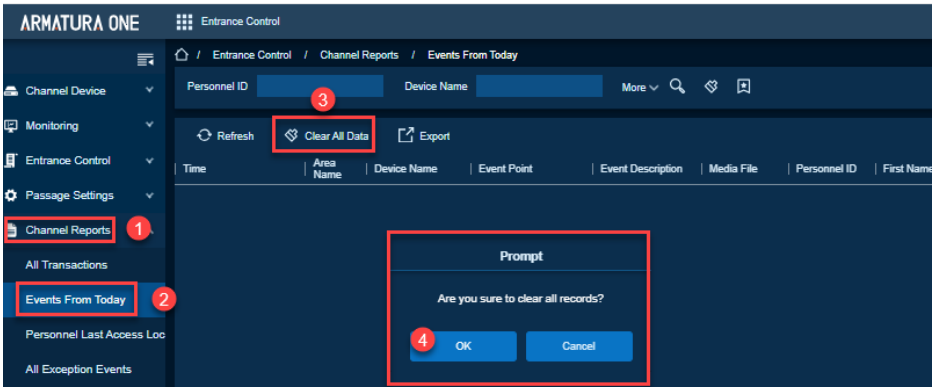
- Select the destination folder where the file will be saved.
- Click **[OK]** to complete the export.

Copyright © 2024 ARMATURA LLC. All rights reserved

Clear All Data

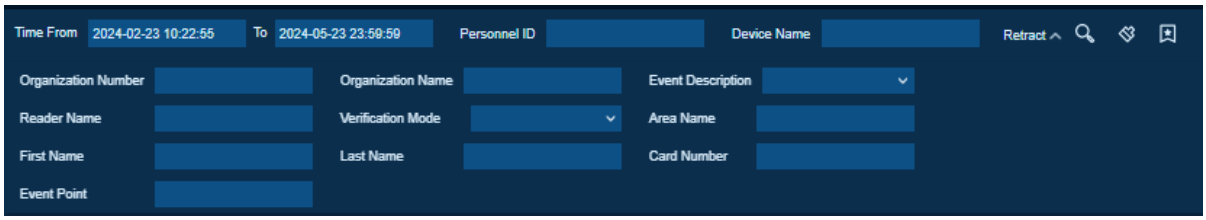
Steps:

- In the **Today's Access Record** interface, click **[Clear All Data].**
- A confirmation prompt will appear; click **[OK]** to permanently clear all access records from the current day.



7.5.3 Personnel Last Access Location

The Personnel Last Access Location report enables users to view the most recent access location of authorized personnel. This functionality helps administrators quickly locate personnel within the system. Navigate to **[Entrance Control] > [Channel Reports] > [Personnel Last Access Location].** In the **Personnel Last Access Location** interface: Enter the relevant query criteria in the provided fields. Click the **[More]** symbol to refine the query or expand the search parameters. Review the generated results to see the most recent access location details for personnel.

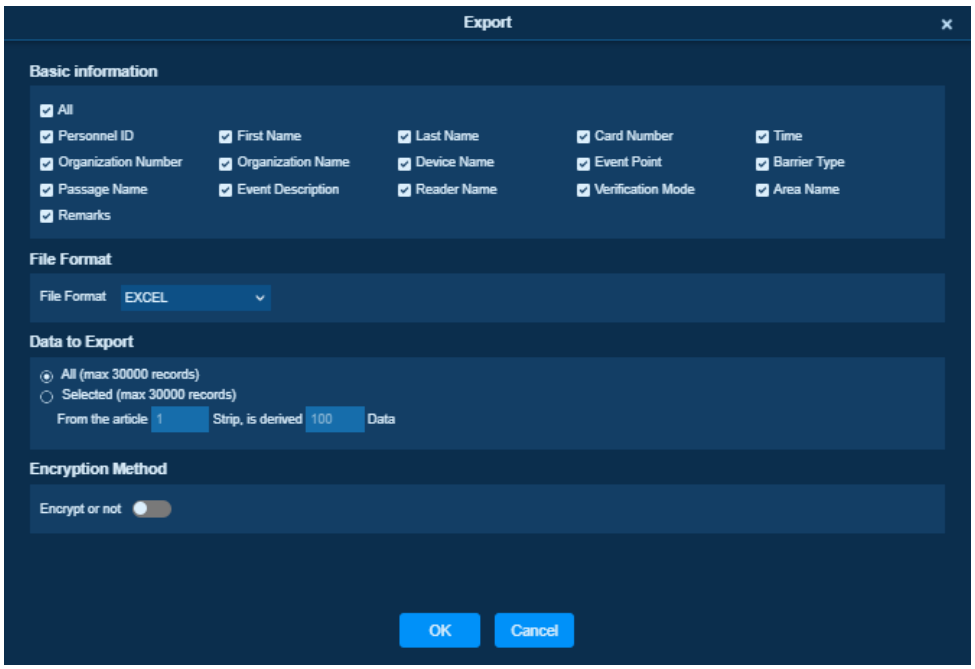


Export Records

Steps:

- In the **Personnel Last Access Location** interface, click **[Export].**
- A security verification prompt will appear: Enter your **user password** and click **[OK].**

Copyright © 2024 ARMATURA LLC. All rights reserved

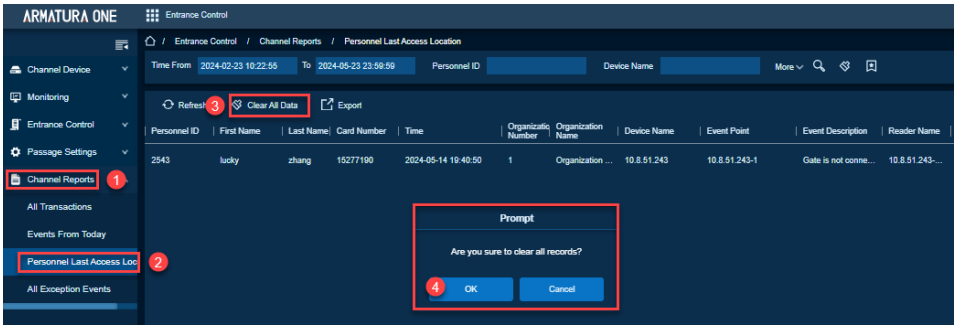


- Select the desired export format (**Excel**, **PDF**, or **CSV**) and decide whether to encrypt the file for added security.
- Choose the destination folder for the exported file.
- Click **[OK]** to finalize the export.

Clear All Data

Steps:

- In the **Personnel Last Access Location** interface, click **[Clear All Data].**
- A confirmation prompt will appear; click **[OK]** to permanently delete all recorded last access location data.



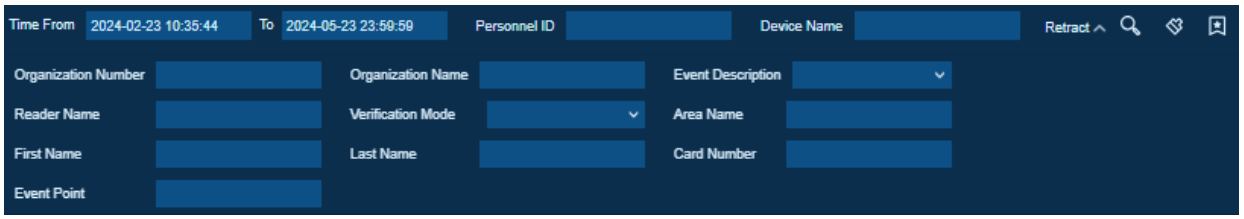
7.5.4 All Exception Events

The All Exception Events report displays records of abnormal events, such as unregistered personnel attempting access, illegal entries, gate operation timeouts, or server connection failures. These events are logged under specified query conditions for monitoring and analysis.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

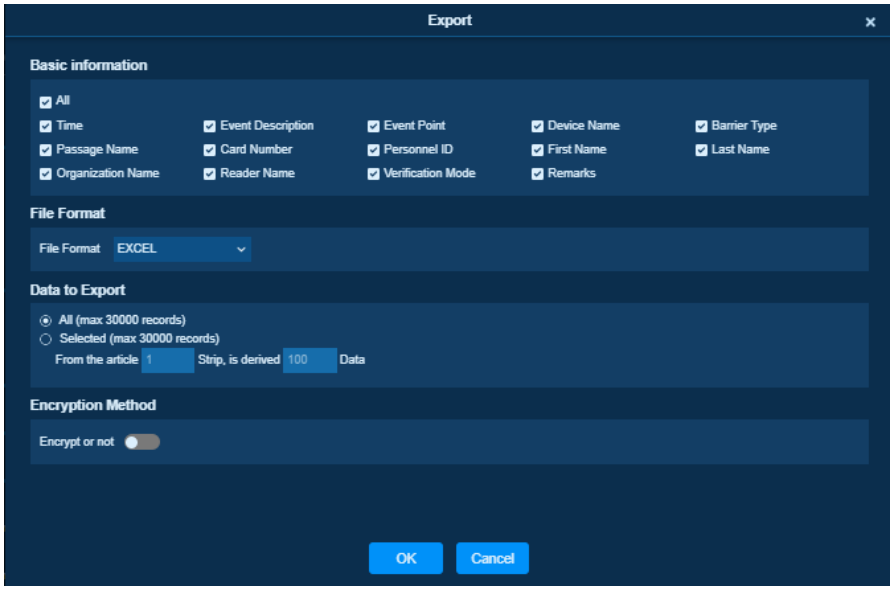
- Navigate to **[Channel Reports] > [All Exception Events]** in the **Entrance Control** module.
- In the **All Exception Events** interface: Enter the necessary query parameters in the provided fields. Click the **[More]** symbol to refine or expand the query results.
- Review the displayed records to analyze the exception events.



Export Exception Events

Steps:

- In the **All Exception Events** interface, click **[Export].**
- A **security verification prompt** will appear: Enter your **user password** and click **[OK].**
- Select the desired export format (**Excel**, **PDF**, or **CSV**) and specify whether to encrypt the file for additional security.



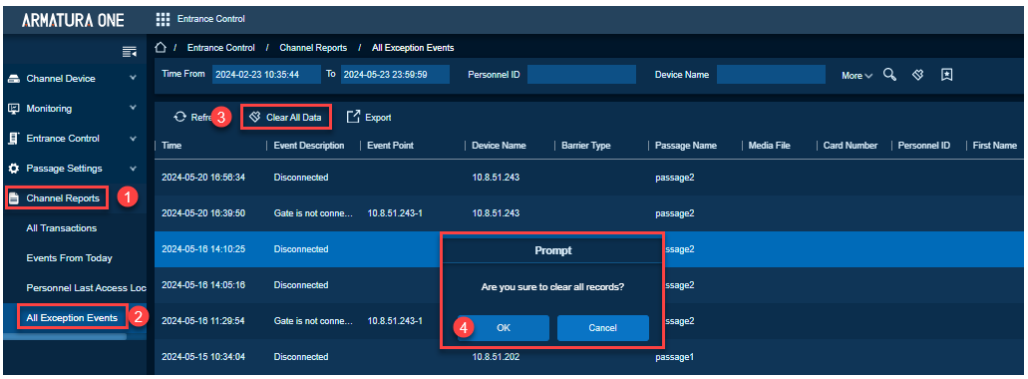
- Choose the destination folder where the exported file will be saved.
- Click **[OK]** to complete the export process.

Clear All Data

Steps:

- In the **All Exception Events** interface, click **[Clear All Data].**
- A confirmation prompt will appear:
- Click **[OK]** to permanently delete all exception event records.

Copyright © 2024 ARMATURA LLC. All rights reserved



Copyright © 2024 ARMATURA LLC. All rights reserved

8 Elevator Control Management

The Elevator Control System enables efficient management of elevator devices, personnel access, and real-time supervision of events. The system ensures that only authorized users can access specific floors during designated time periods, improving security and operational efficiency. This manual provides details on managing online elevator control. If you are using offline elevator control, refer to the respective guide.

The system currently supports integration with KONE, Mitsubishi, Mitsubishi ELSGW, Hitachi, and Schindler elevators.

8.1 Elevator Settings

The Elevator Settings menu includes several functions for configuring elevator parameters, managing access, and monitoring events. Below is the list of functionalities:

Function List

Functions	Description
Buildings	Manage building data, including adding, editing, deleting, and searching for building information.
Devices	Perform operations such as adding, deleting, exporting, searching, enabling/disabling, restarting devices, upgrading firmware, modifying IP addresses, synchronizing data/time, and more.
Readers	View and edit elevator reader configurations.
Floors	Manage floors, perform remote operations like locking/unlocking, enabling/disabling normal open settings, and configuring release buttons.
Auxiliary Inputs	View the status and details of auxiliary input devices.
Event Types	View and manage event types specific to elevator control devices.
Monitoring	Monitor real-time elevator events, remotely release buttons, and perform lock/unlock operations.
Elevator Groups	Configure elevator groups corresponding to the buildings and devices in the system.

Copyright © 2024 ARMATURA LLC. All rights reserved

Elevator Cars	Manage elevator cars and their associated floor settings assign devices to specific areas, and set up monitoring filters.
I/O Board	Manage I/O boards for elevators, including configuration protocol types, device names, and ports.

8.1.1 Buildings

Function Description

The **Buildings** module enables the configuration and management of building-related information, including assigning areas, floors, and integrating with third-party elevator control platforms. This functionality is essential for managing personnel and visitor permissions and verifying elevator operations.

Add Building

Function Description

Define building parameters, configure floor information, and integrate with third-party elevator systems to manage personnel permissions for elevator use.

Prerequisites for Use

Ensure the system allows for setting and selecting the corresponding areas.

Usage Scenarios

Configure elevator control devices to manage personnel access and initiate elevator operations.

Enable remote elevator calls after verifying access permissions through a third-party integrated platform.

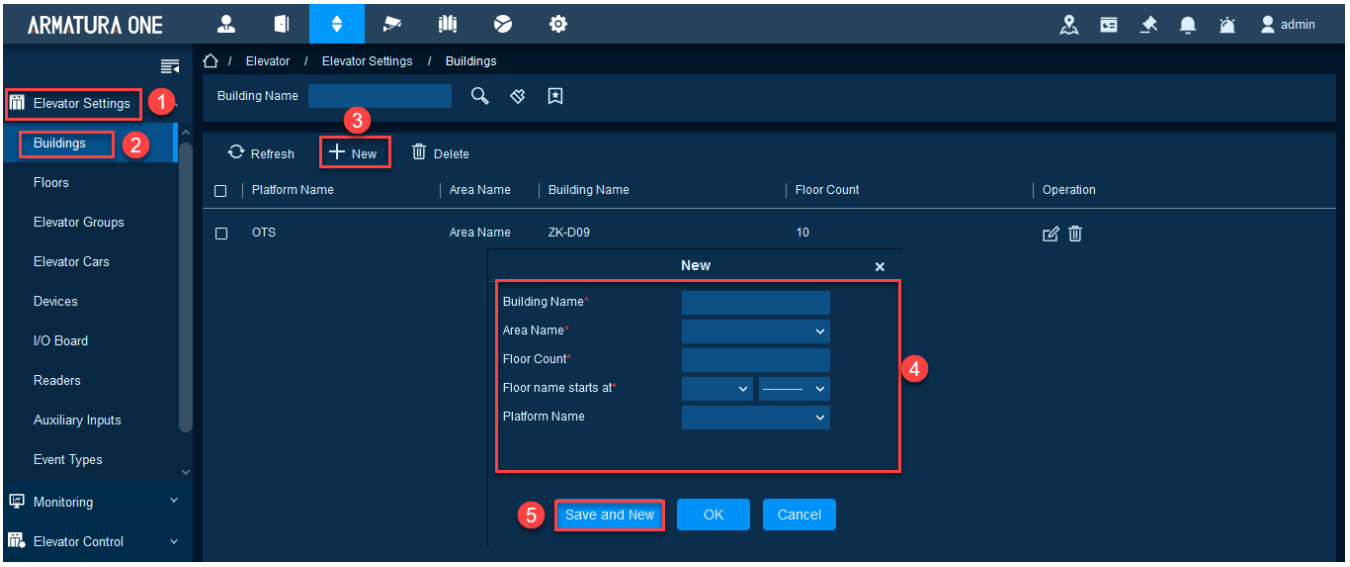
Trigger Result

Adding a building automatically creates floors based on the configured number of floors, along with the corresponding floor information.

Steps:

- Click **[Elevator Settings] > [Buildings] > [New]** from the Action Menu.

Copyright © 2024 ARMATURA LLC. All rights reserved



Building Name: Enter a name or title for the building.

Area Name: Define the area where the building is located.

Floor Count: Specify the number of floors in the building.

Platform Name: Choose the third-party elevator control platform to integrate with.

Floor Name Starts At: Assign a floor code name and number for the elevator system.

- Click **[OK]** to save and add the building. The system will automatically generate floor information based on the entered details.

Edit Buildings

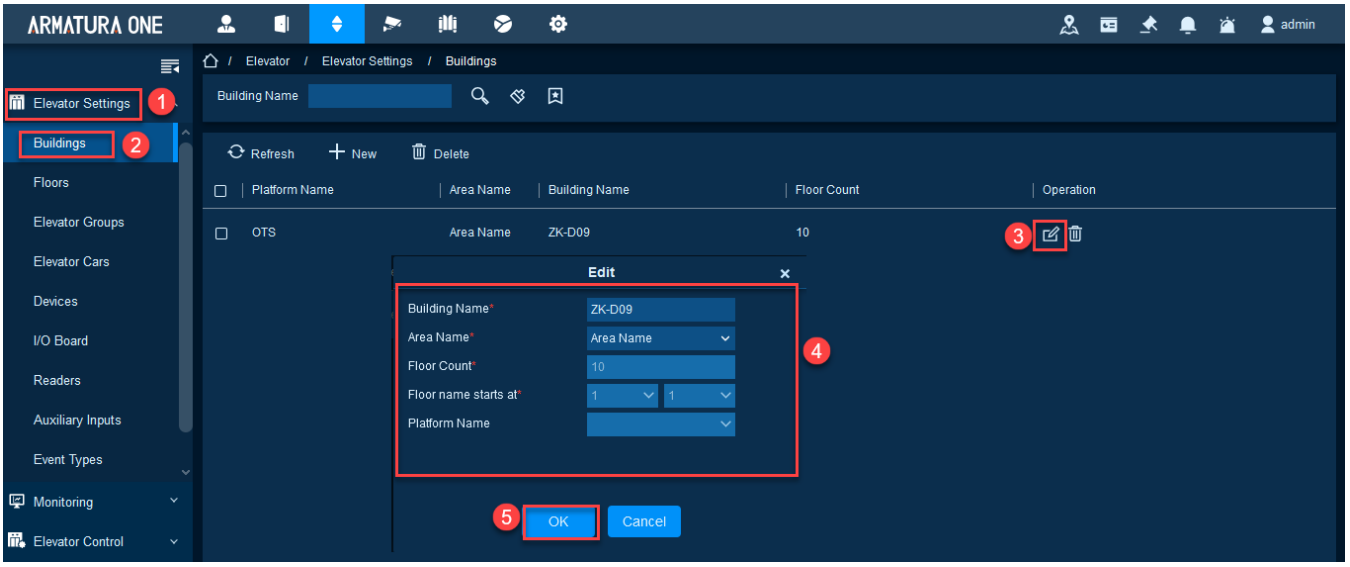
Function Description

Modify the details of an existing building, such as its name, associated area, or number of floors.

Steps:

- Click **[Elevator Settings]** > **[Buildings]** > **[Edit]** from the Action Menu.
- Update building name, area, floor count, or platform name as needed.
- Click **[OK]** to confirm and save the modifications.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Buildings

Function Description

Remove a building and its associated floor information when no longer needed or incorrectly configured.

Prerequisites for Use

Ensure that the building has been successfully added.

Verify that the building's floors are **not bound** to:

Elevator settings - External Reader

Elevator settings - Internal Reader

Usage Scenarios

The number of floors or other building details are incorrectly configured.

The building is no longer in active use.

Trigger Result

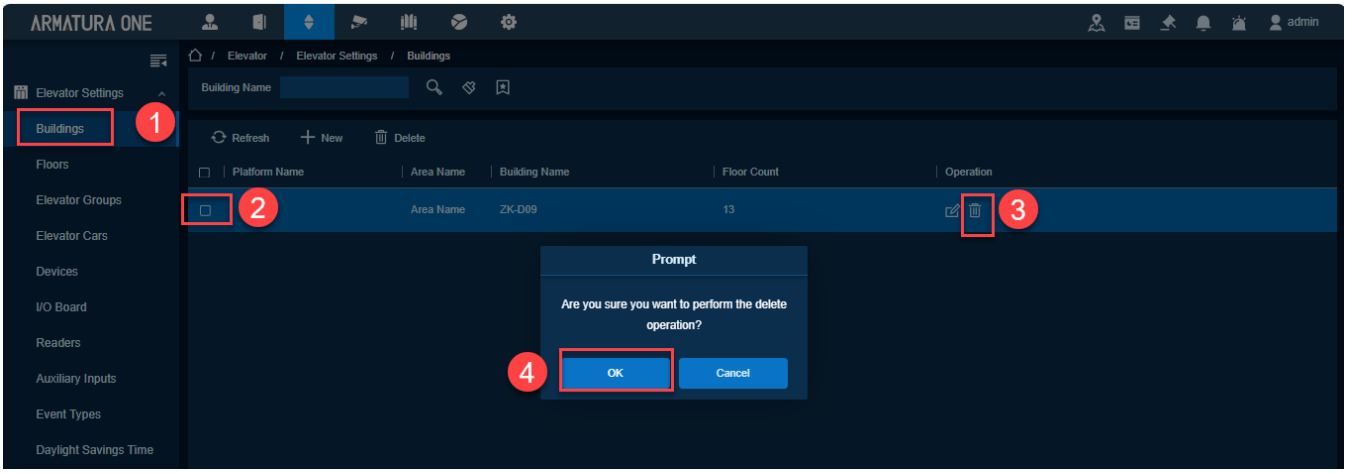
Deletes the selected building's information.

Deletes the corresponding floor information for that building.

Steps:

- Select the Platform Name: Navigate to **[Elevator Settings] > [Buildings].**
- Delete the Building: Click **[Delete]** next to the selected building name and confirm the action by clicking **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



8.1.2 Floors

Function Description

The **Floors** section allows users to manage and configure floor-related settings for elevator control devices. This includes editing floor parameters, releasing or locking buttons, and managing time zones for passage modes.

Edit Floors

Prerequisites for Use

Building data must be added, and floor information must be properly configured.

Usage Scenarios

Modify floor parameters, such as floor name, time zone settings, operation intervals, and button open durations.

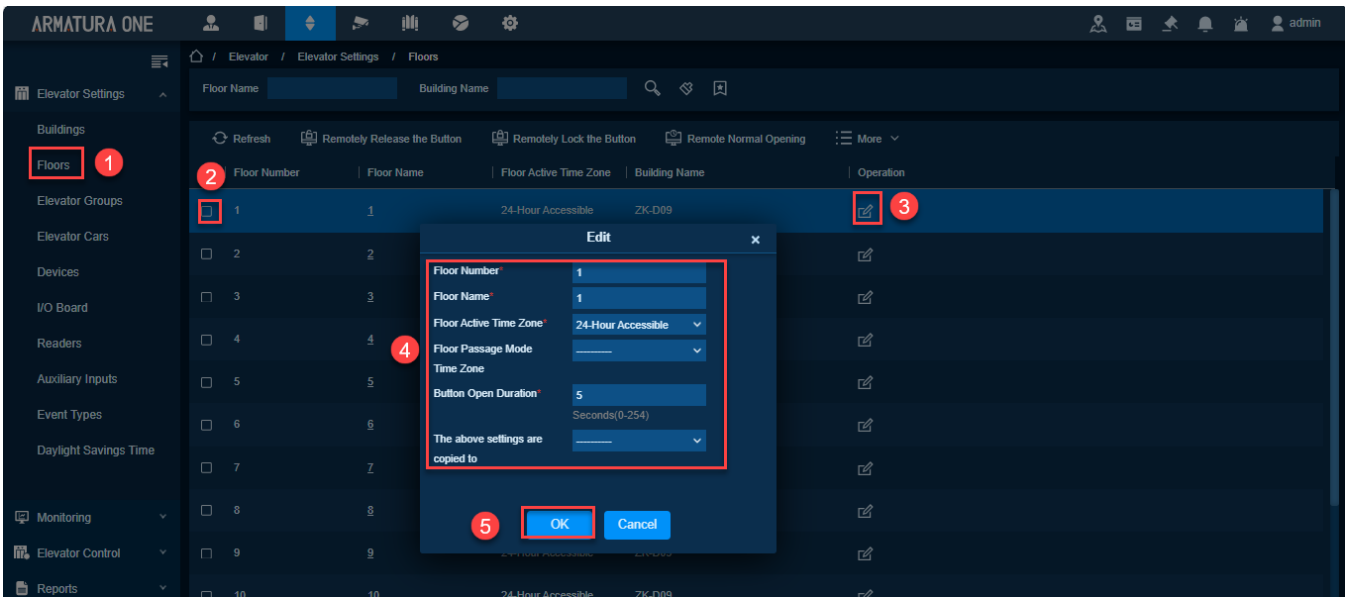
Trigger Result

Updates the relevant parameter information of the selected floor.

Steps:

- Click **[Elevator Settings] > [Floors]**.
- Choose the floor number to edit and click **[Edit]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Floor Number: Auto-generated based on the number of relays.

Floor Name: Default is “Device Name – Floor Number”; editable (max 30 characters).

Floor Active Time Zone: Select the active time zone for the floor.

Floor Passage Mode Time Zone: Specify a passage mode time zone.

Button Open Duration: Control how long the floor button remains active after verification (default: 5 seconds, range: 0–254 seconds).

All Floors in Current Device: Apply changes to all floors of the selected elevator device.

All Floors in All Devices: Apply changes to all floors within the user's access level.

- Click **[OK]** to finalize edits.

Remote Release Button

Prerequisites for Use.

The floor must be connected to a functioning elevator control device.

Usage Scenarios

Temporarily release button controls for a floor to allow operation within a specified time.

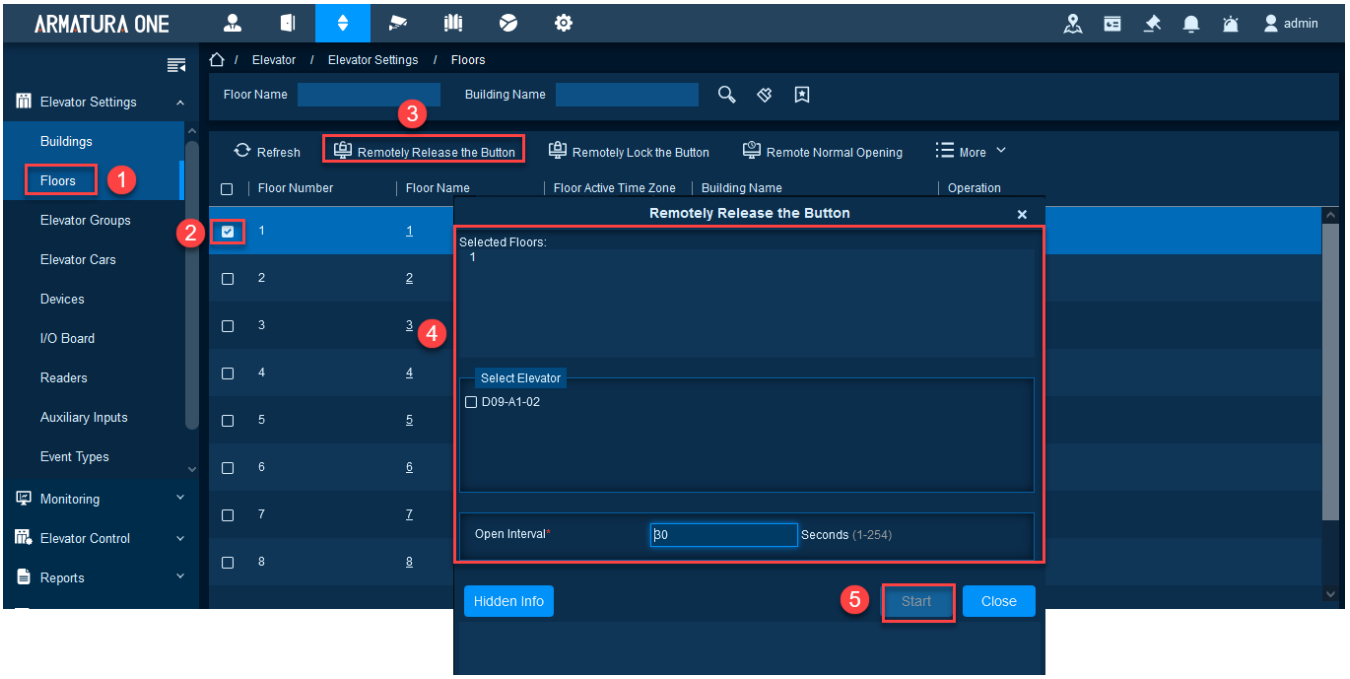
Trigger Result

Floor buttons can be operated within the set duration.

Steps:

- Click **[Elevator Settings] > [Floors] > [Remotely Release the Button]**.
- Enter the duration for button release.
- Enter the password and click **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Remote Lock the Button

Prerequisites for Use

The floor must be connected to a functioning elevator control device.

Usage Scenarios

Lock the floor button to prevent unauthorized operations.

Trigger Result

Floor button operations are disabled.

Steps:

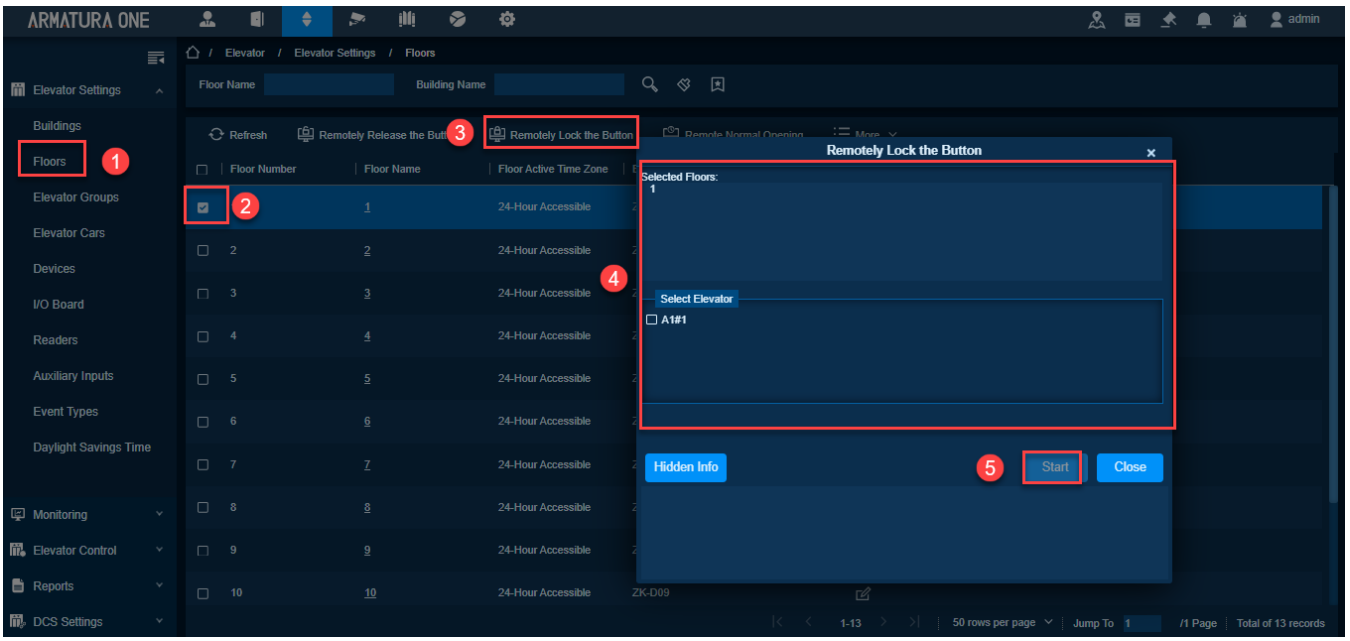
- Click **[Elevator Settings] > [Floors] > [Remotely Lock the Button]**.
- Enter the password and click **[OK]**.

Note:

This function remotely locks the floorboard permissions of the elevator device. Once confirmed, the user will be unable to operate the button until it is unlocked. Confirm the lock by entering the password.

Only the selected floor from the device supports this operation.

Copyright © 2024 ARMATURA LLC. All rights reserved



Remote Normal Opening

Prerequisites for Use

The floor must be connected to a functioning elevator control device.

Usage Scenarios

Keep the floor button in an unlocked state for unrestricted use.

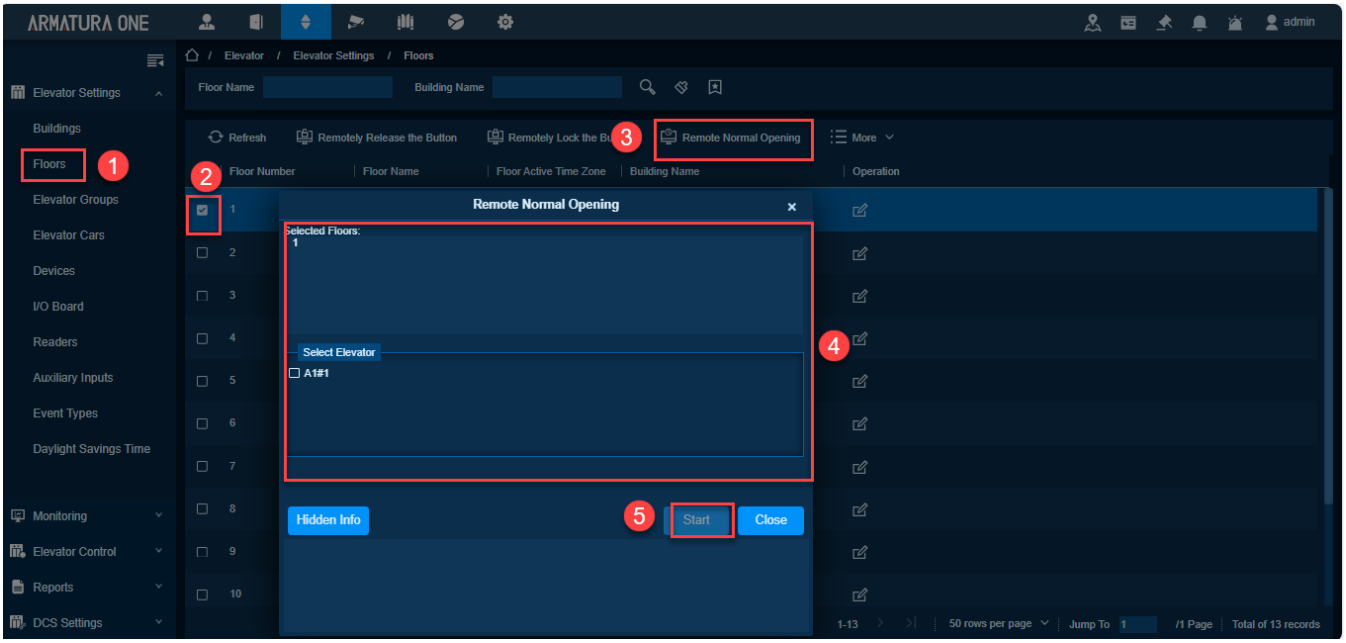
Trigger Result

Floor buttons remain operable without verification.

Steps:

- Click **[Elevator Settings] > [Floors] > [Remotely Normal Opening]**.
- Enter the password and click **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Enable Intraday Passage Mode Time Zone

Prerequisites for Use

The floor must be connected to a functioning elevator control device.

Usage Scenarios

Activate a preset time zone for the floor to remain open.

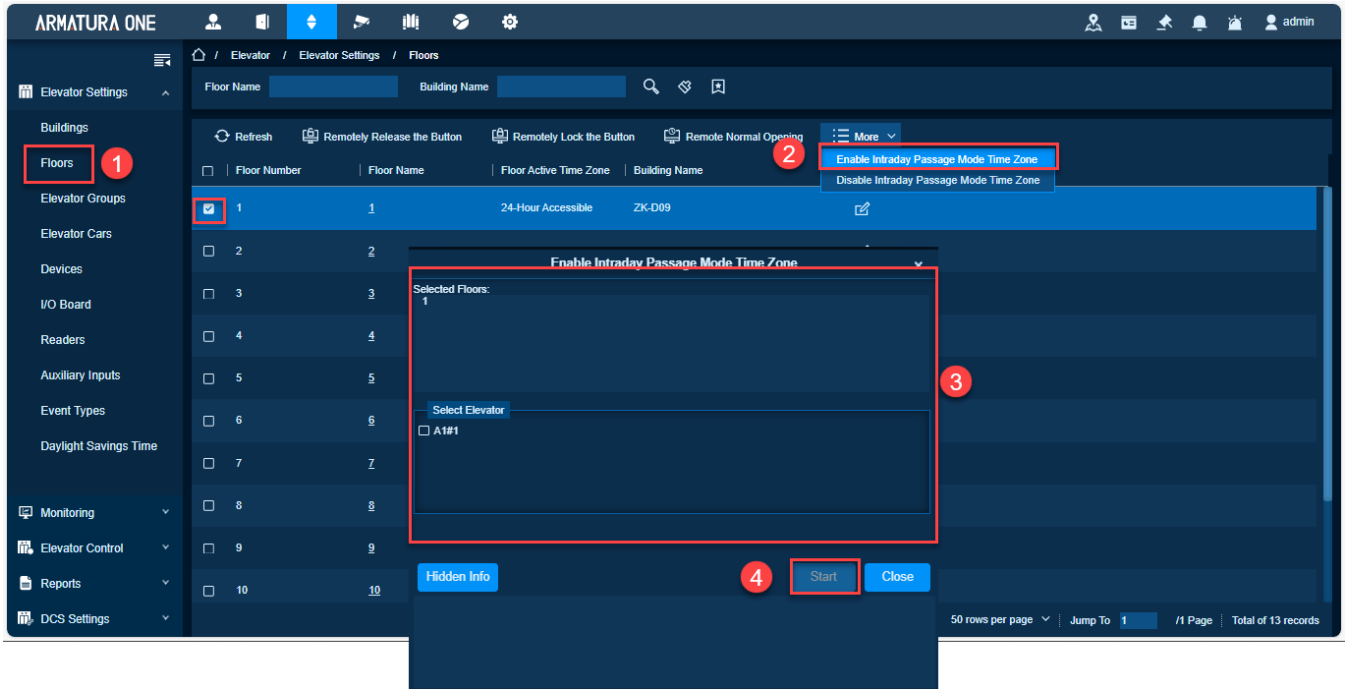
Trigger Result

Activates the normally open time zone for the floor.

Steps:

- Click **[Elevator Settings] > [Floors] > [Enable Intraday Passage Mode Time Zone]**.
- Enter the password and click **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Disable Intraday Passage Mode Time Zone

Prerequisites for Use

The floor must be connected to a functioning elevator control device.

Usage Scenarios

Deactivate the normal open time zone for the floor.

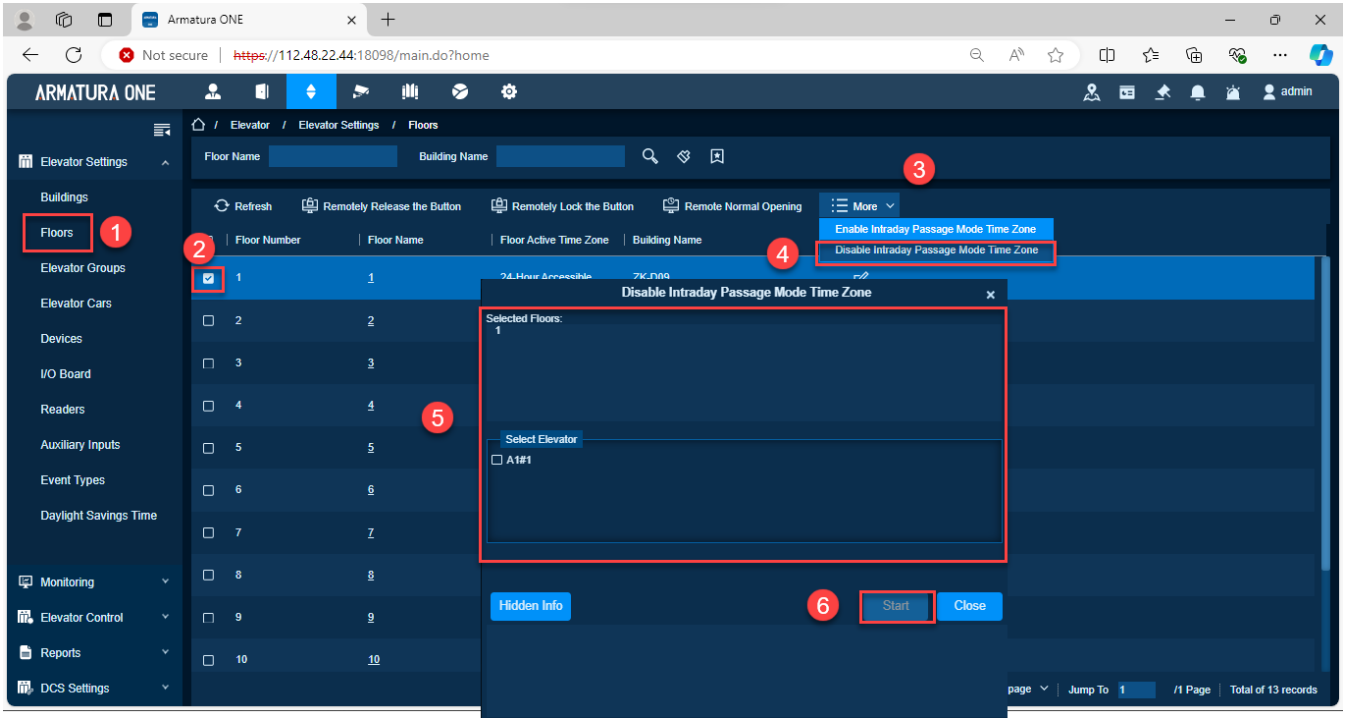
Trigger Result

Disables the preset normal open time for the floor.

Steps:

- Click **[Elevator Settings] > [Floors] > [Disable Intraday Passage Mode Time Zone]**.
- Enter the password and click **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



8.1.3 Elevator Groups

Function Description

Elevator groups represent the grouping of elevator control devices bound to a specific building. This configuration ensures streamlined management of elevator operations and facilitates integration with third-party systems.

Add Elevator Groups

Prerequisites for Use

The system must be configured with corresponding areas and allow area selection.

Usage Scenarios

To assign elevator control devices for personnel permissions and manage elevator operations.

To enable remote elevator calling by verifying personnel access authority through third-party integrations.

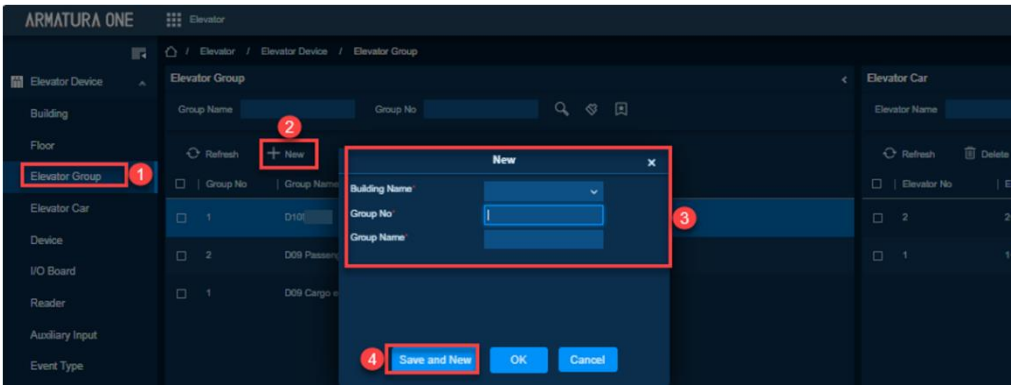
Trigger Result

When a building is added, the number of floors associated with the elevator is also configured.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Elevator Settings] > [Elevator Groups] > [New]**.
- Complete the necessary fields in the displayed interface, such as:
  - **Building Name:** Specify the name of the building.
  - **Group No.:** Assign a unique identifier to the group.
  - **Group Name:** Provide a descriptive name for the group.
- Click **[OK]** to finalize the group addition.



Edit Elevator Groups

Prerequisites for Use

A building and its associated group must already exist and be configured.

Usage Scenarios

Modify default parameters like the building name, group number, or group name.

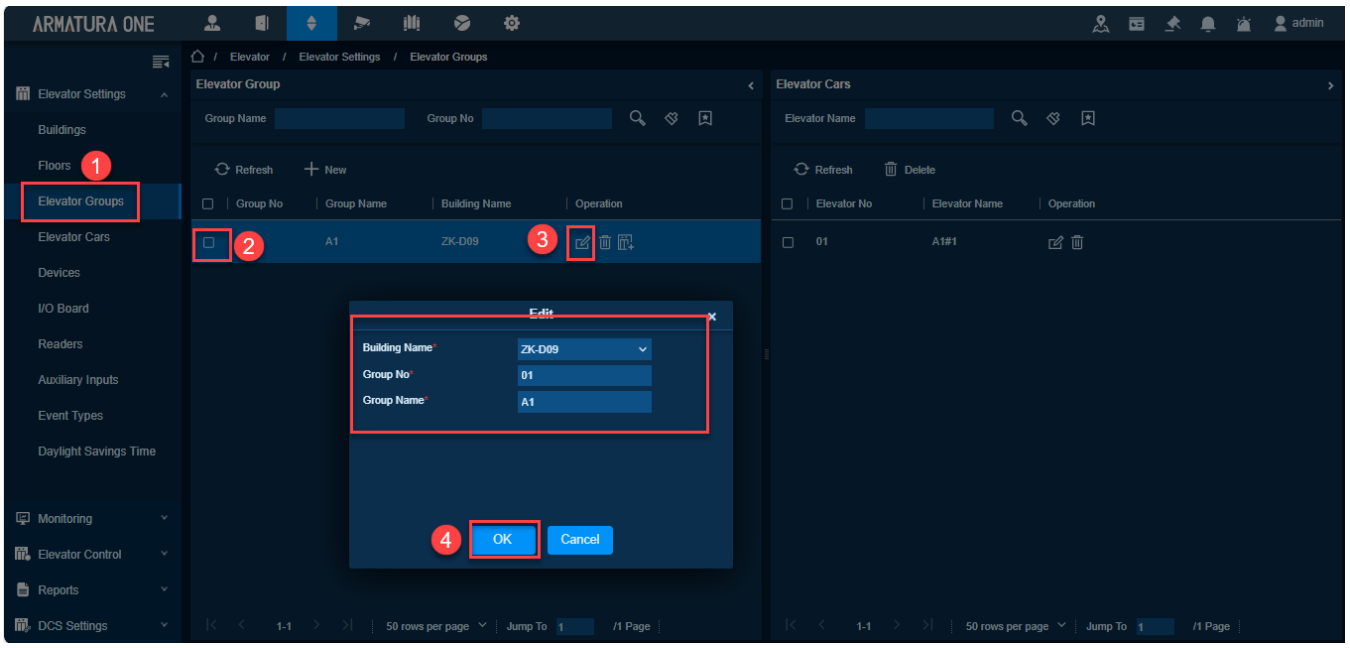
Trigger Result

Updates the building and group information with new parameters.

Steps:

- Select the group to edit.
- Click **[Edit]** and modify the relevant details.
- Click **[OK]** to save changes.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete

Prerequisites for Use

The elevator group must not be in use or bound to other functions.

Usage Scenarios

When an elevator group or its building is no longer needed.

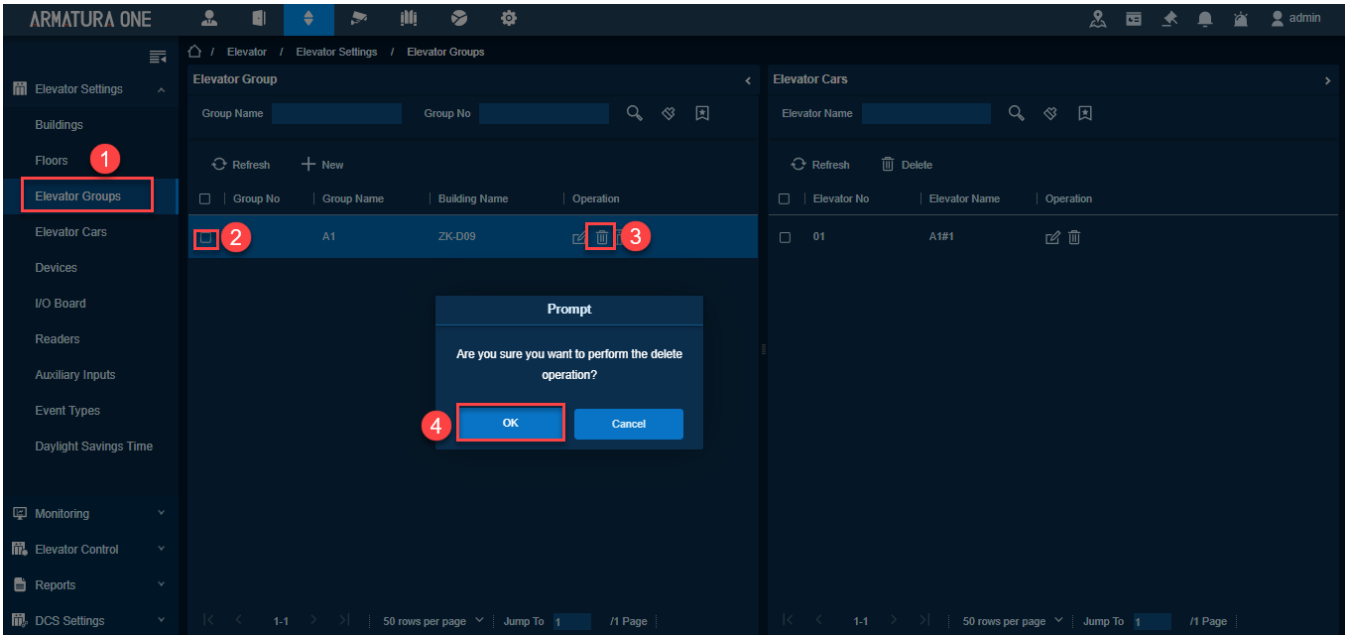
Trigger Result

Deletes the specified elevator control group.

Steps:

- Select the group to delete.
- Click **[Delete]**.
- Confirm the operation in the pop-up window by clicking **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



New elevator

Prerequisites for Use

The elevator must be linked by its name and group function.

Usage Scenarios

To assign elevators to a specific group with identifiers like elevator number and name.

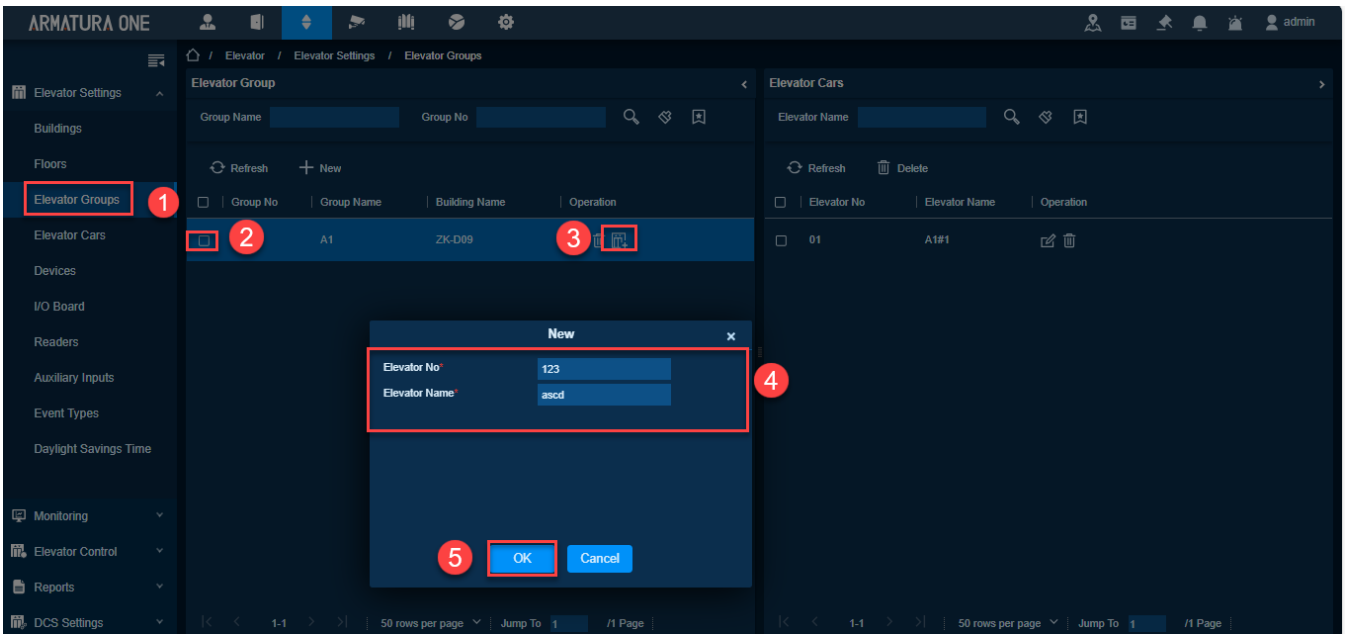
Trigger Result

Adds a new elevator to the selected group.

Steps:

- Select the group where the elevator will be added.
- Click **[New Elevator]**.
- Provide the required details in the pop-up window and click **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Edit Elevator Cars

Prerequisites for Use

The elevator must be linked by its name and car function.

Usage Scenarios

Updates the information of the elevator car in the group.

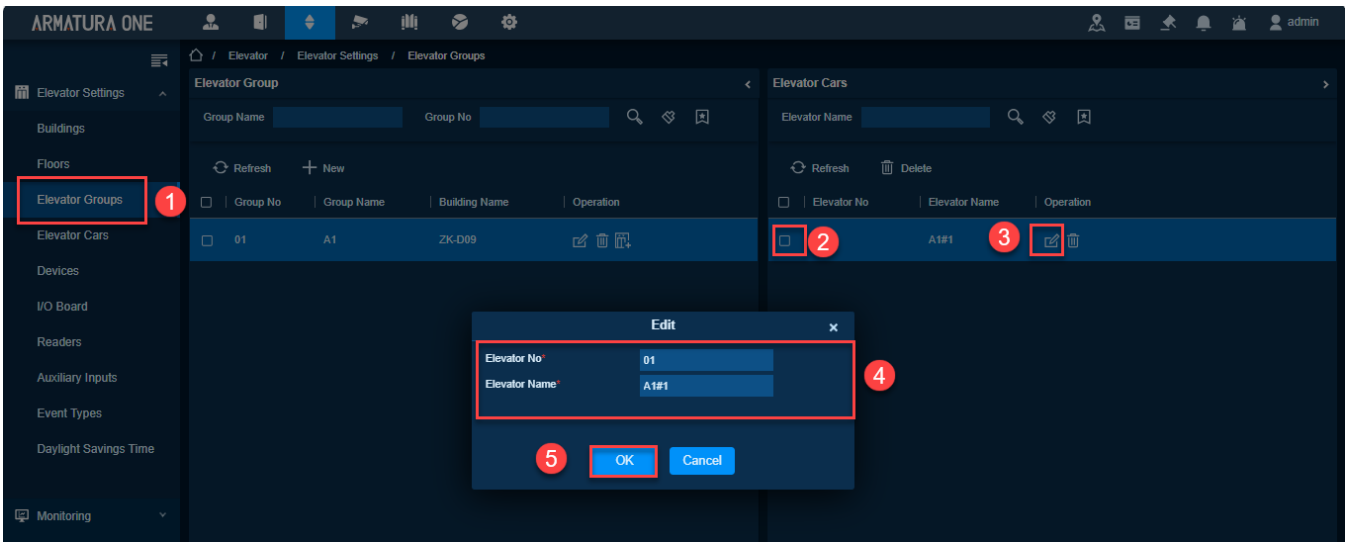
Trigger Result

Updates the information of the elevator car in the group.

Steps:

- Select the corresponding group.
- Click **[Edit Elevator]**.
- Make the necessary modifications.
- Confirm the changes in the pop-up window by clicking **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete

Prerequisites for Use

The elevator must be linked by its name and group function.

Usage Scenarios

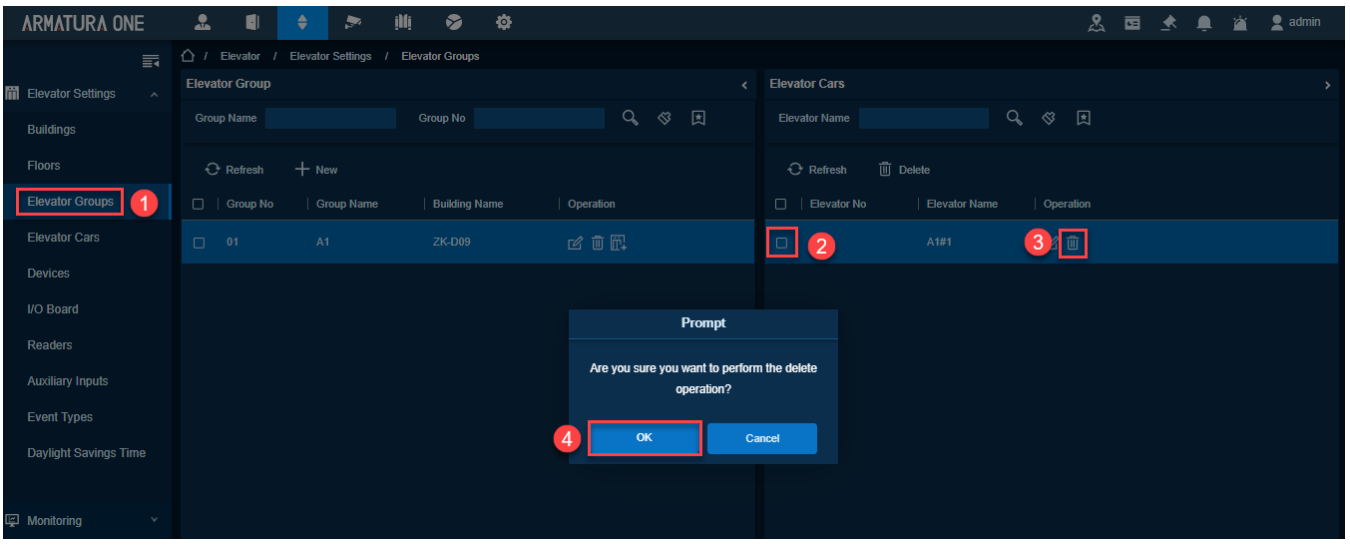
To remove an elevator from a group when it is no longer required.

Trigger Result

Clears the selected elevator from the current elevator control group.

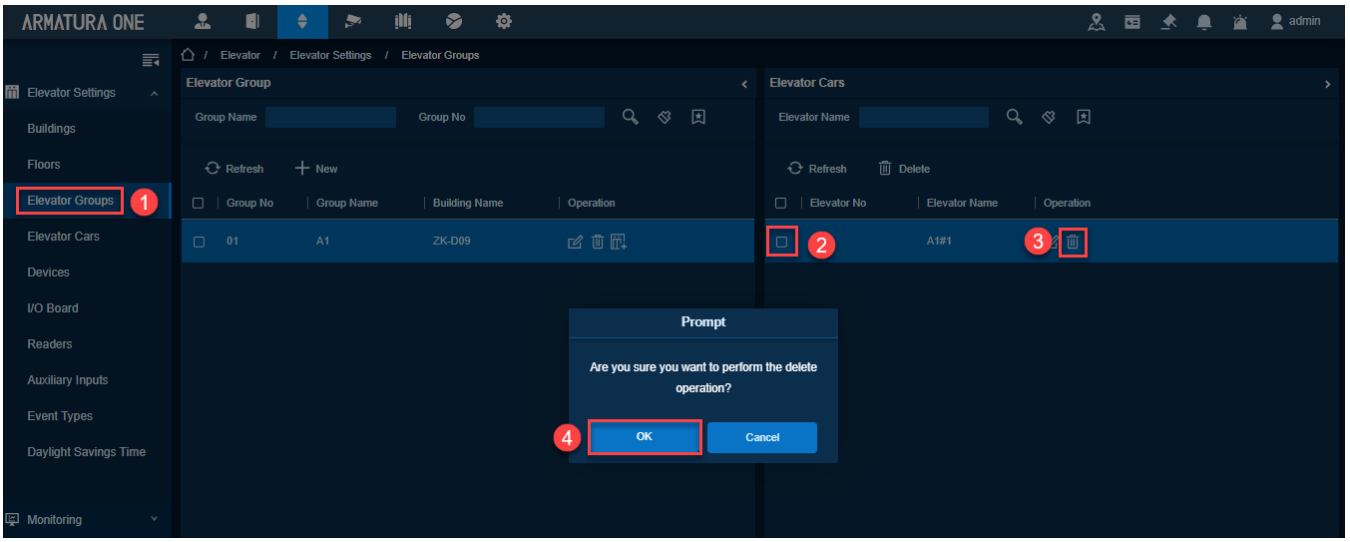
Steps:

- Select the group containing the elevator.
- Click **[Delete Elevator]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

- Confirm the deletion in the pop-up window by clicking **[OK]**.



8.1.4 Elevator Cars

Function Description

Elevator car information corresponds to the floor information of elevator control devices bound to specific areas. This enables real-time monitoring and allows devices (such as doors) to be filtered by area.

View Elevator Car

Prerequisites for Use

Elevator floor details are correctly displayed in the system.

Usage Scenarios

Modify the default parameters of buildings, elevator cars, floors, and groups.

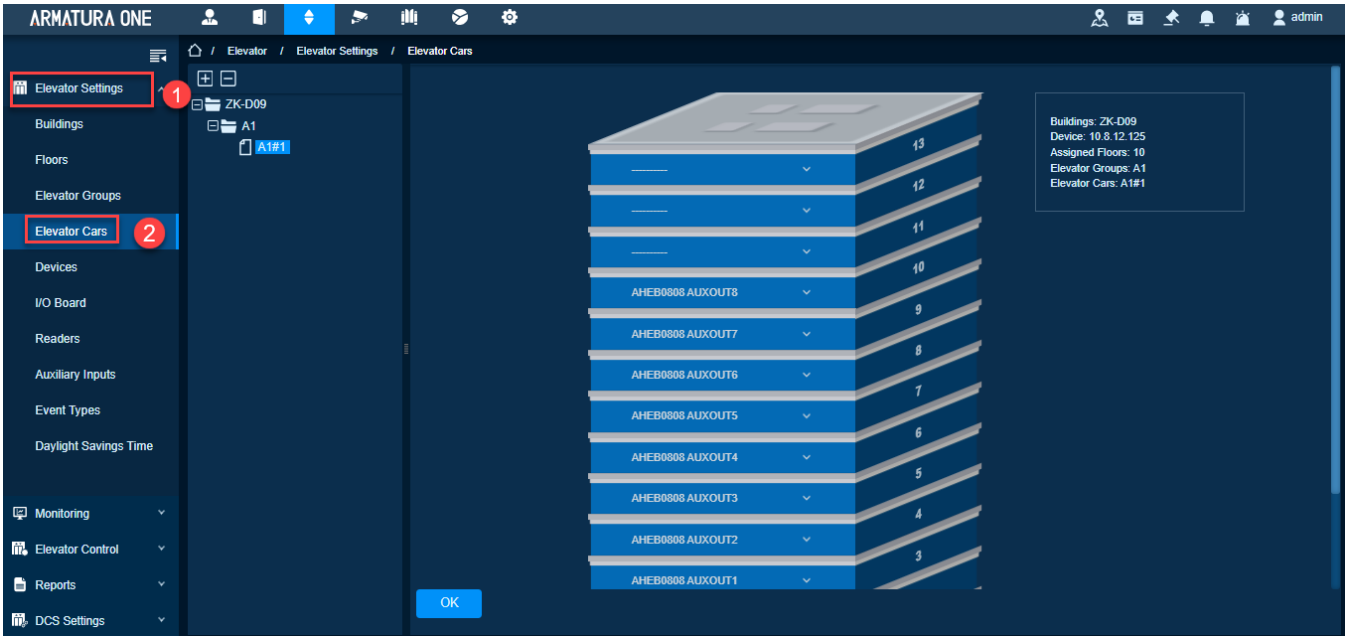
Trigger Result

Updates the relevant parameter information of the elevator car.

Steps:

- Navigate to **[Elevator Settings] > [Elevator Cars]**.
- View the details of the elevator cars, including floor assignments and group associations.

Copyright © 2024 ARMATURA LLC. All rights reserved



8.1.5 Devices

Function Description

This section manages elevator control devices, supporting operations such as adding, deleting, updating parameters, and obtaining data. It facilitates personnel permissions and elevator operations.

Search Device

Prerequisites for Use

The elevator control device communicates normally and is added to the system.

Usage Scenarios

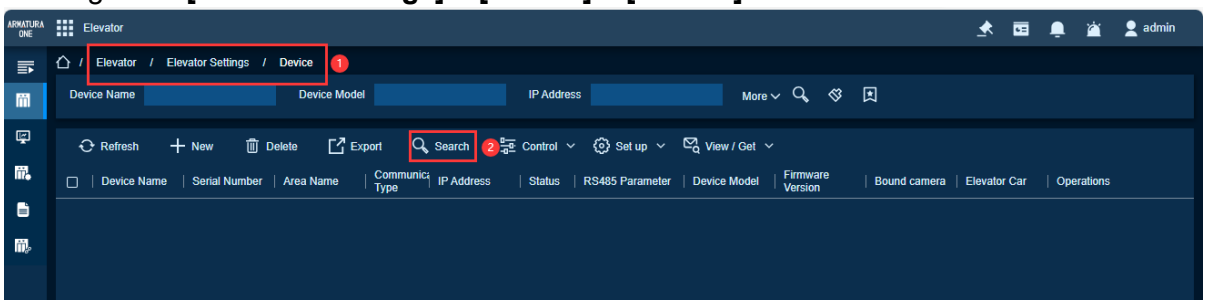
Locate and add an elevator control device to the system.

Trigger Result

Adds the elevator control device to the system.

Steps:

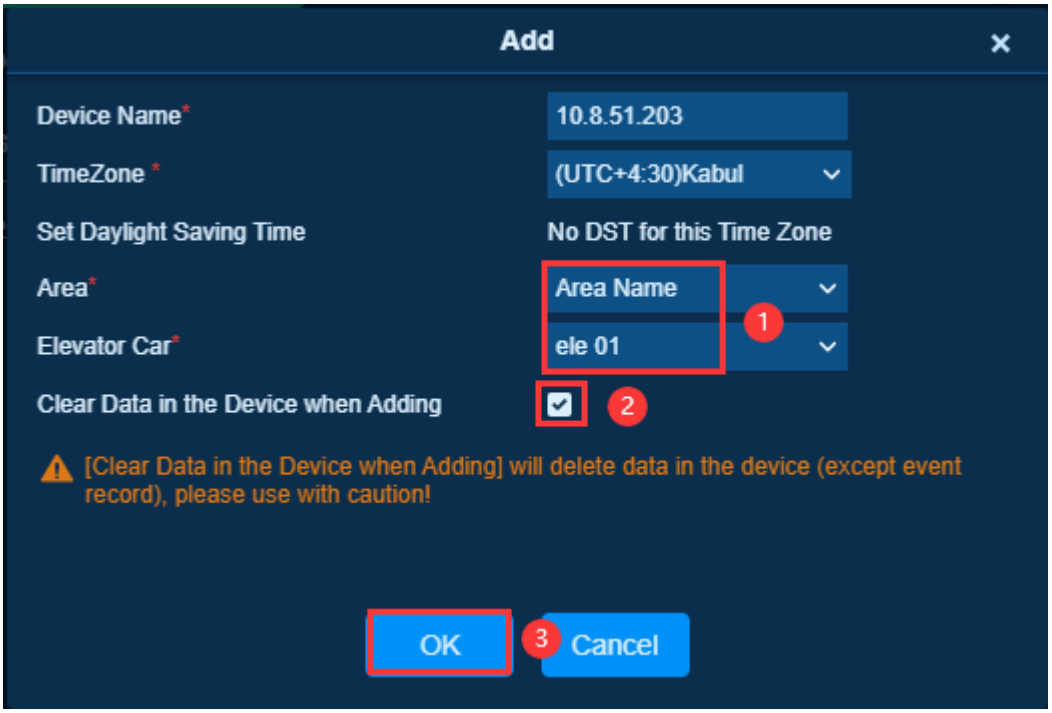
- Navigate to **[Elevator Settings] > [Device] > [Search]**.



- Click **[Search]**. After the search completes, locate the desired device and click the **[+]** icon to add it.

Copyright © 2024 ARMATURA LLC. All rights reserved

- Assign an area and elevator car to the device. Optionally, check **[Clear Data in the Device when Adding]**.
- Click **[OK]** to save the settings.



Add Devices

Prerequisites for Use

The system must include configured area information.

Usage Scenarios

Add elevator control devices for personnel to access elevators.

Trigger Result

Adds elevator control device information and enables device operations.

Steps:

- Navigate to **[Elevator Settings] > [Device] > [New]**.

Copyright © 2024 ARMATURA LLC. All rights reserved

- Fill in the required parameters:

Device Name: Enter the name of the device.

Communication Type: Select the type of communication (e.g., TCP/IP).

IP Address: Enter the device's IP address.

Communication Port: Default is 4370.

Communication Password: Up to 6 characters, including letters and numbers. Leave blank for new factory devices or after initialization.

Number of Expansion Boards: Specify the expansion boards the device controls.

Baud Rate: Select the baud rate.

Elevator Car: Assign the elevator car.

Area: Assign the device to an area.

Clear Data in the Device when Adding: Optionally clear all device data except event logs.

- Click **[OK]**. The system will connect to the device and retrieve extended parameters.

Delete Device

Prerequisites for Use

The device is not in use or bound to other functions.

Usage Scenarios

Remove devices that are damaged or no longer needed.

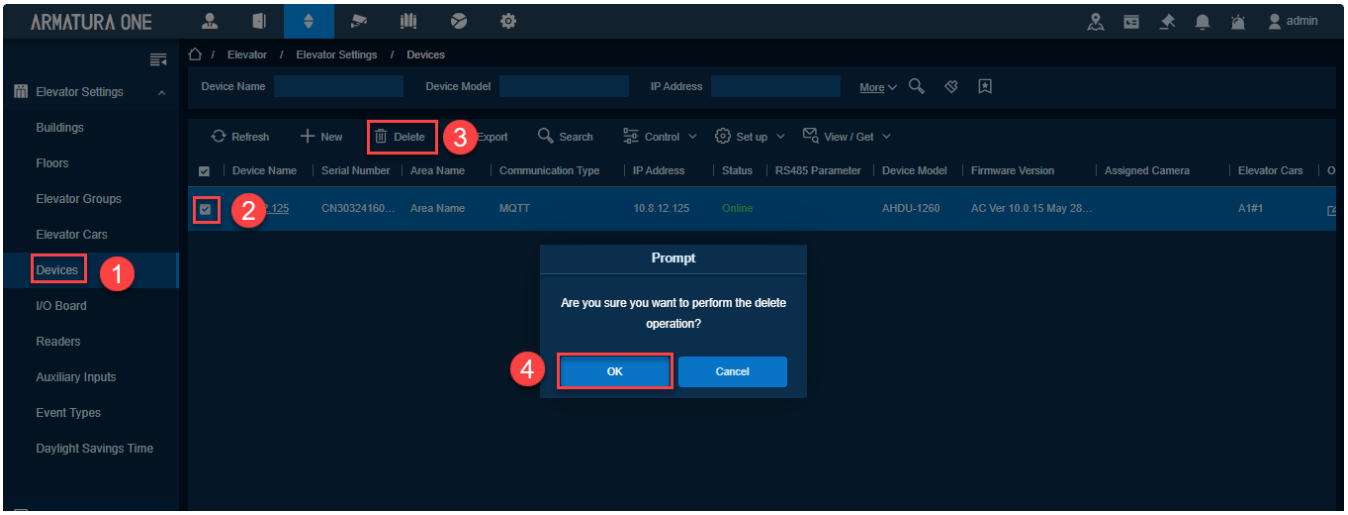
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Deletes the device and clears its associated data.

Steps:

- Select the device from the list.
- Click **[Delete]**.
- Confirm the operation by clicking **[OK]** in the pop-up window.



Export Device

Usage Scenarios

Export device data for review.

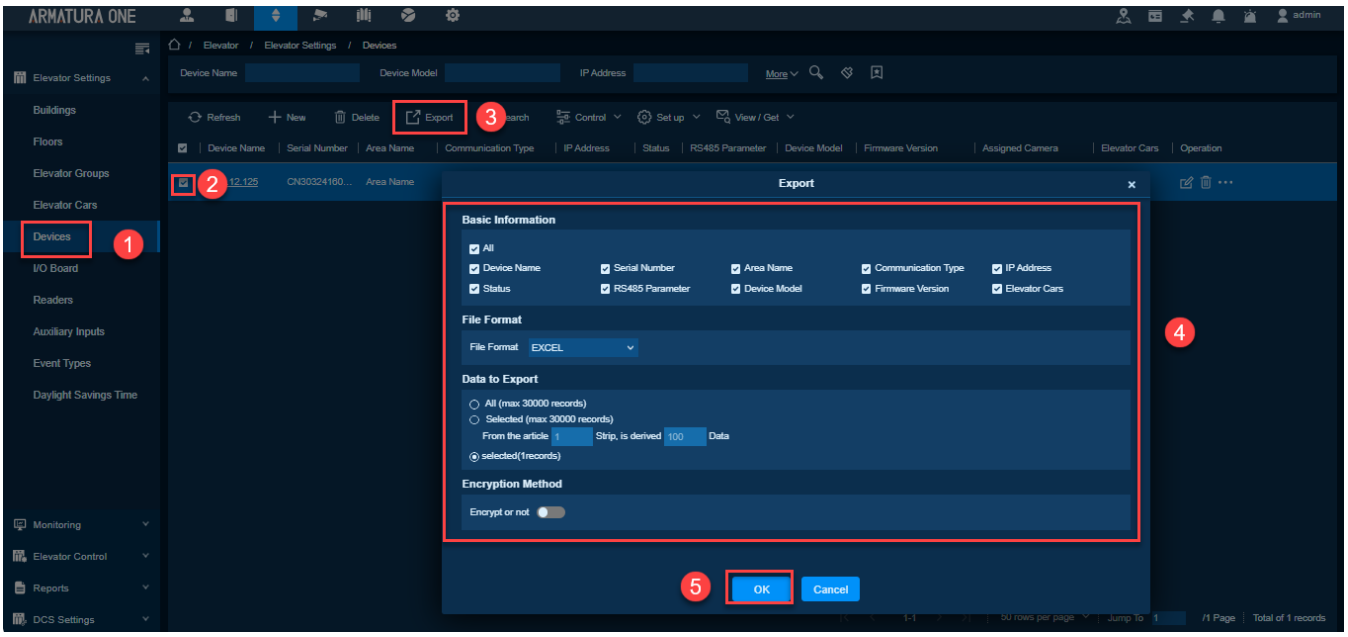
Trigger Result

Saves device data as an Excel, PDF, or CSV file.

Steps:

- Select the data to export.
- Click **[Export]** and set export conditions.
- Click **[OK]** to download the file.

Copyright © 2024 ARMATURA LLC. All rights reserved



Control Functions

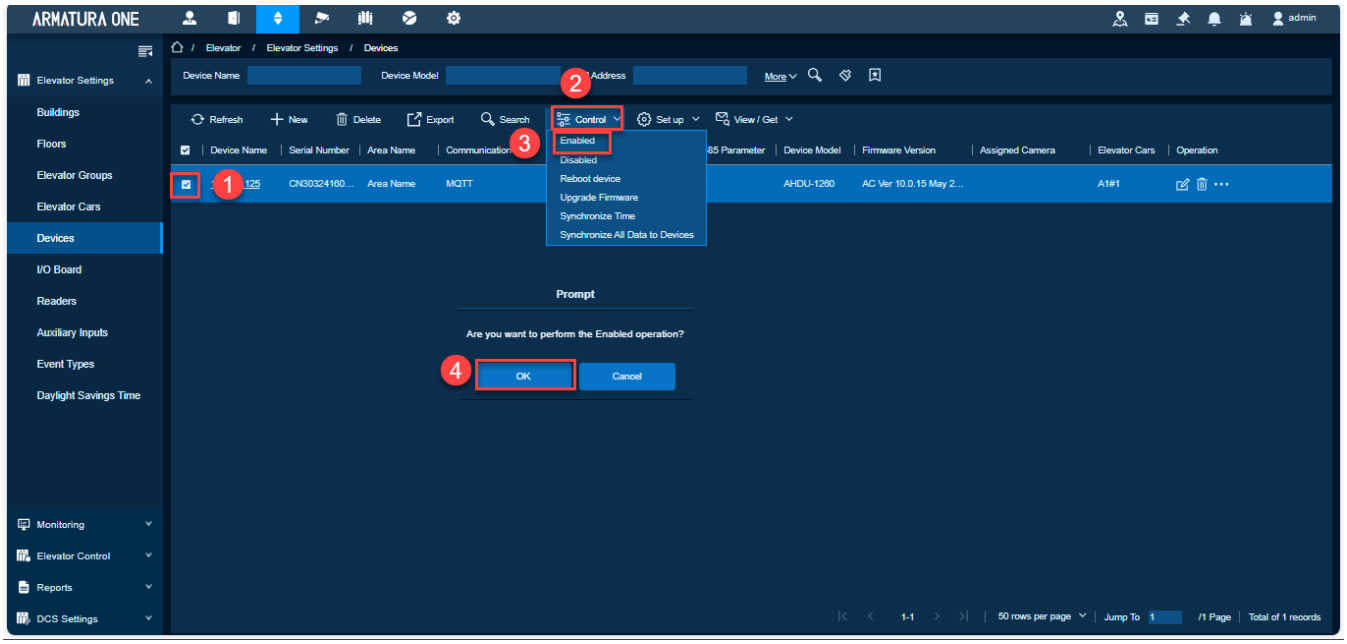
Enable

Prerequisites for Use: The device communicates normally and is added to the system.

Usage Scenario: Enable a disabled device.

Trigger Result: The device becomes operational.

Steps: Select the device, click **[Enable]**, and confirm with **[OK]**.

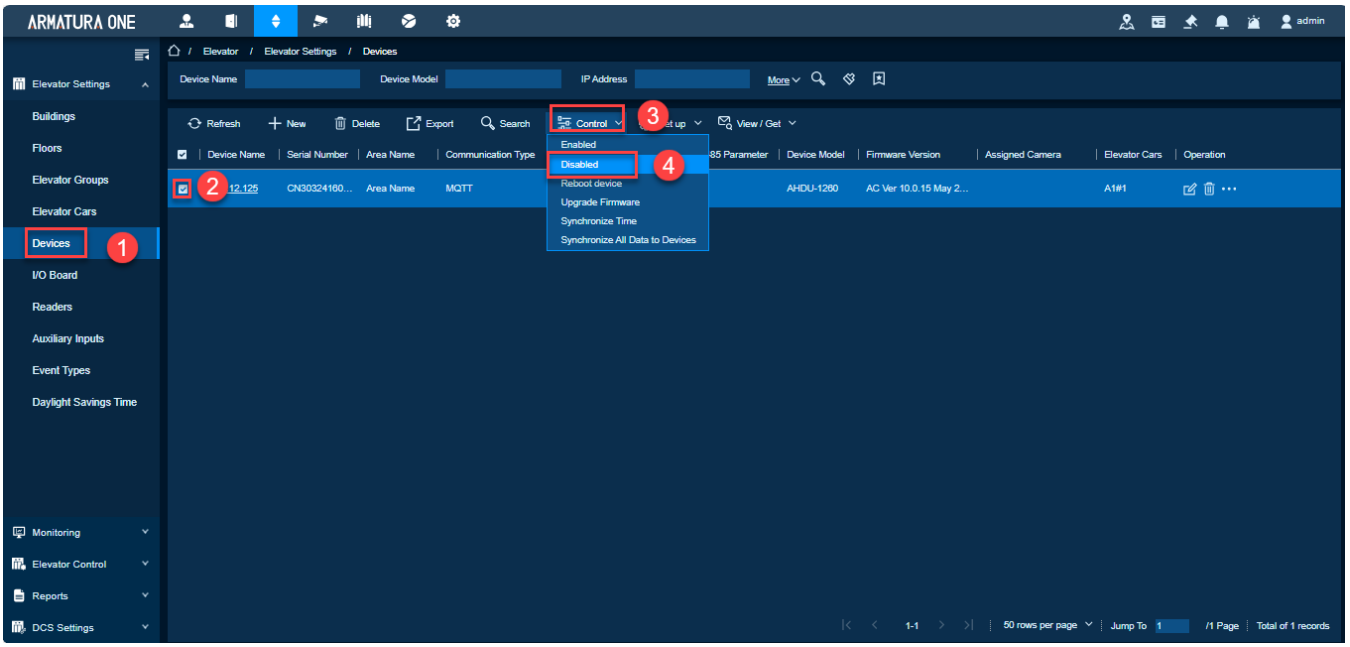


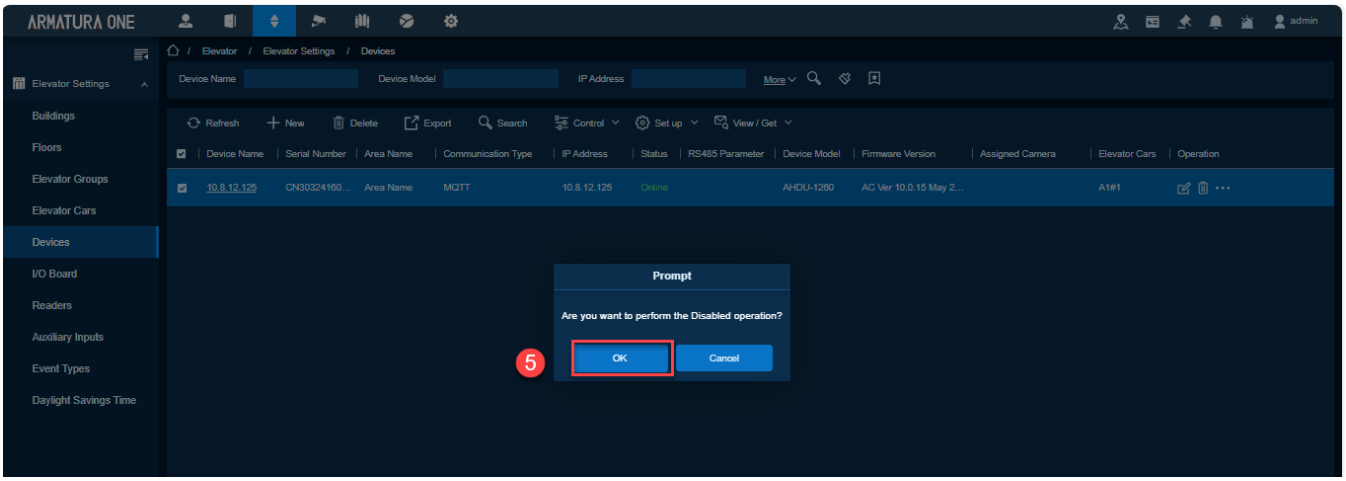
Copyright © 2024 ARMATURA LLC. All rights reserved

Disable

Usage Scenario: Disable a device to prevent its operation.

Steps: Select the device, click **[Disable]**, and confirm with **[OK]**.



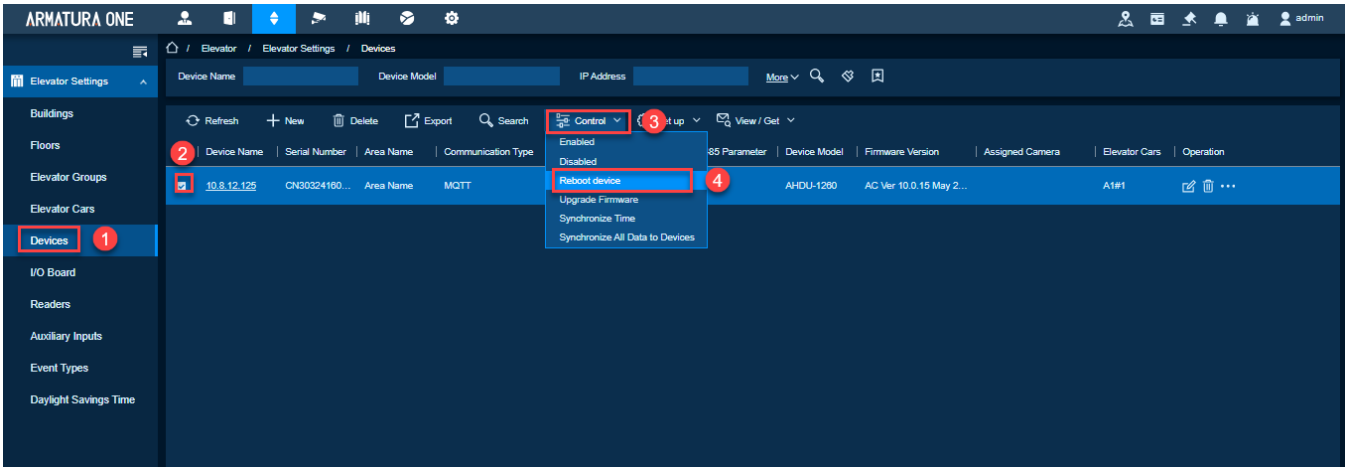


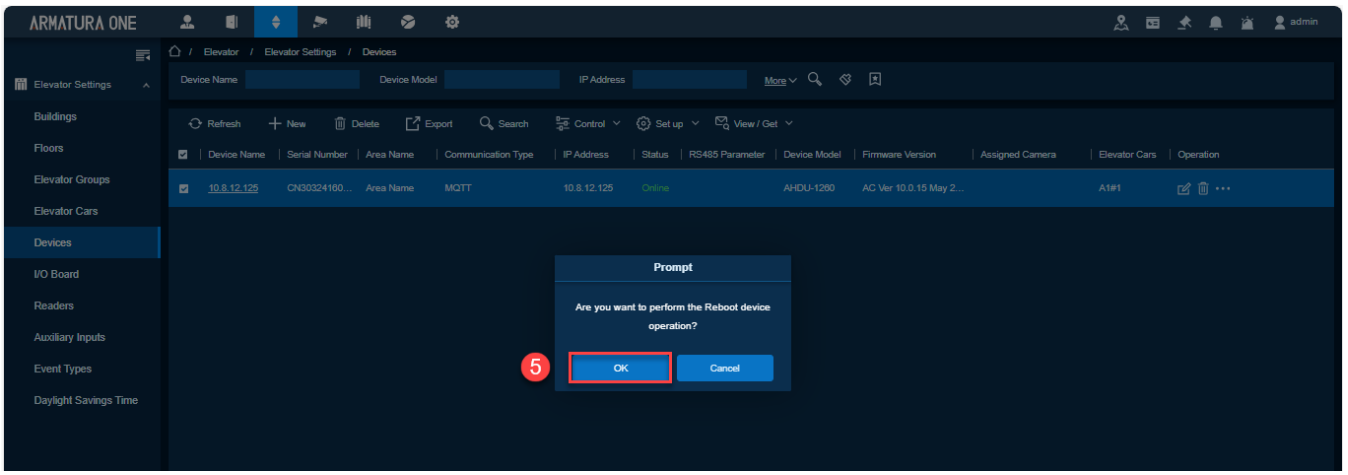
Reboot Device

Usage Scenario: Restart a device for maintenance.

Steps: Select the device, click **[Reboot Device]**, and confirm with **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved

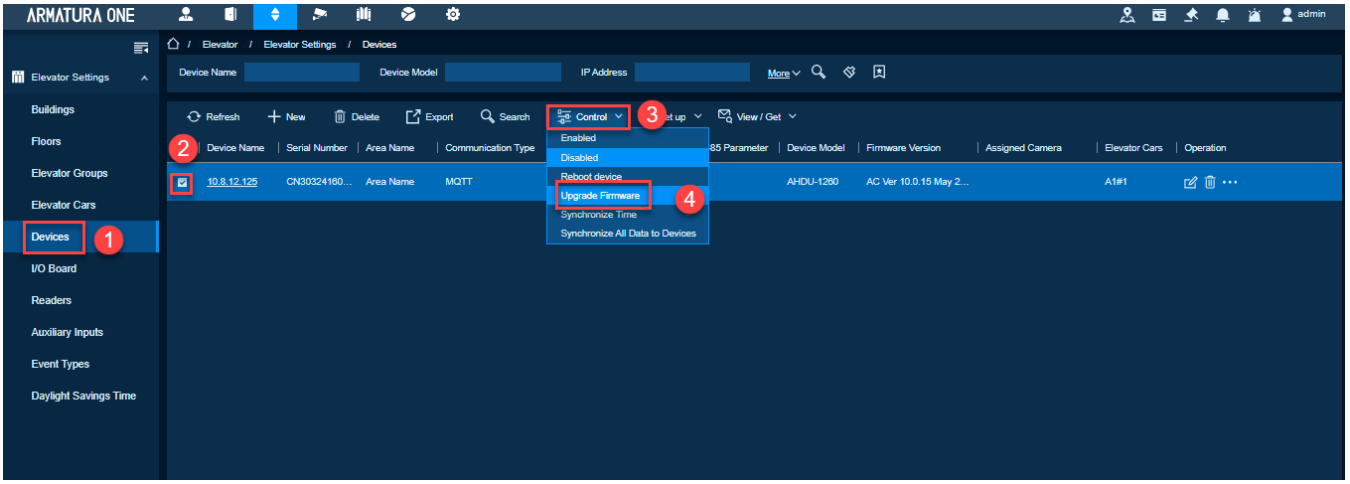




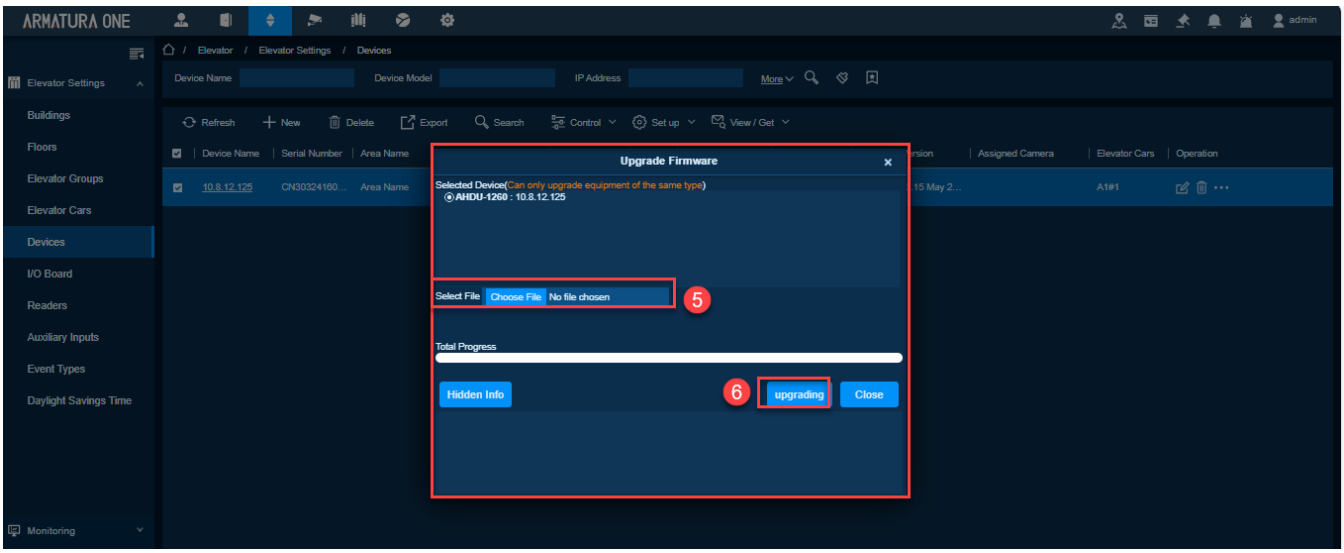
Upgrade Firmware

Usage Scenario: Update the firmware version.

Steps: Select the device, click **[Upgrade Firmware]**, upload the firmware file, and confirm the update.



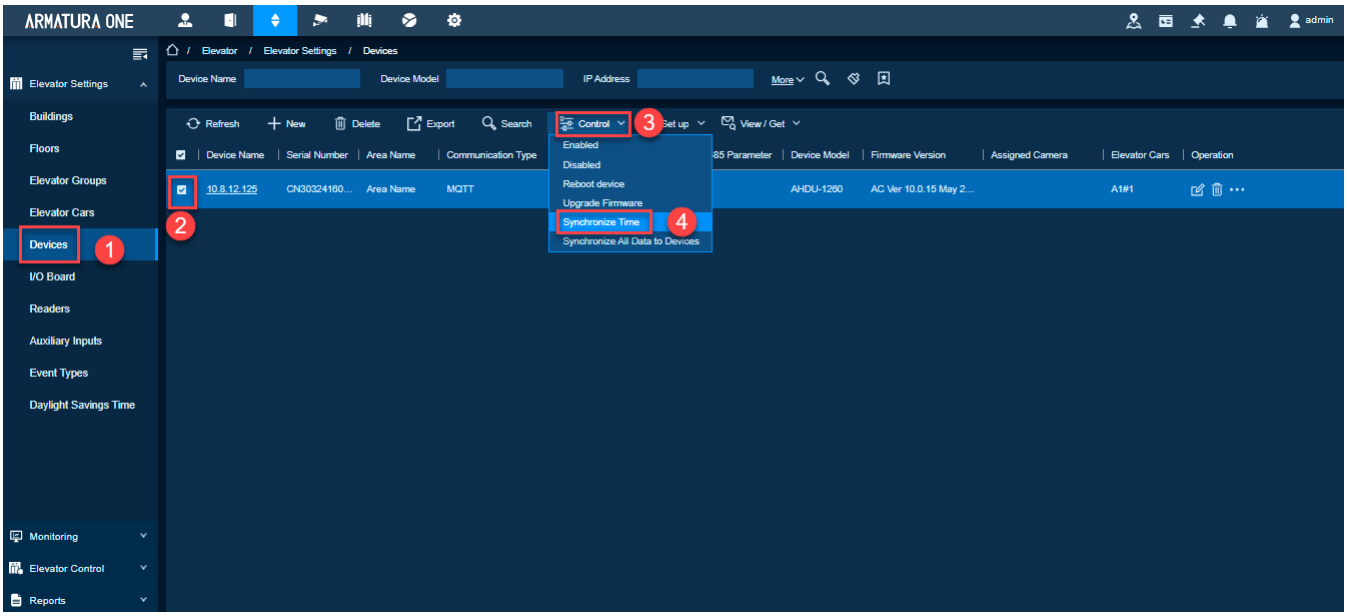
Copyright © 2024 ARMATURA LLC. All rights reserved



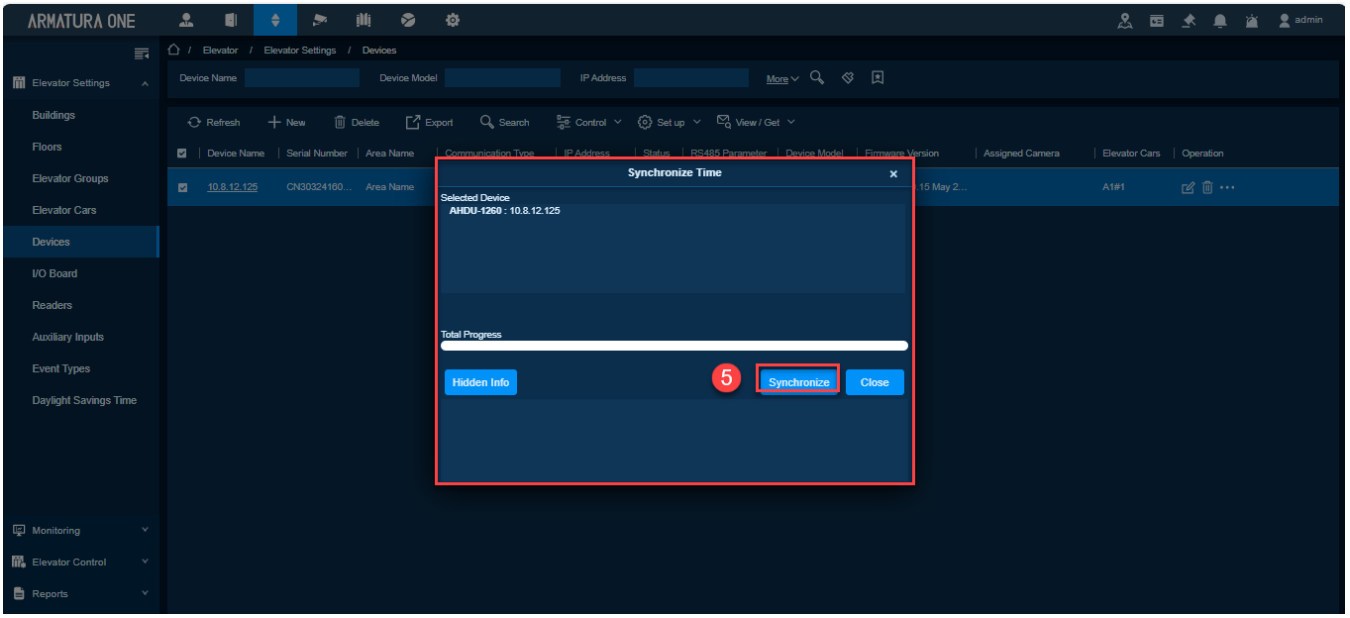
Synchronize Time

Usage Scenario: Align device time with the system.

Steps: Select the device, click **[Synchronize Time]**, and confirm.



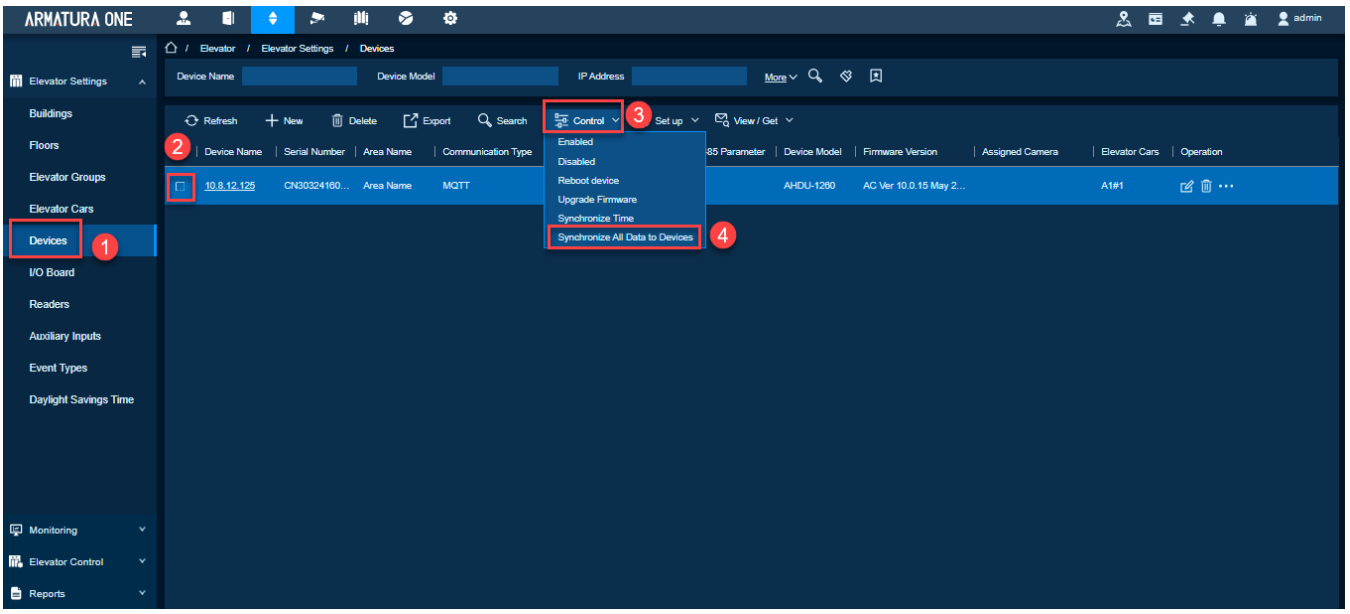
Copyright © 2024 ARMATURA LLC. All rights reserved



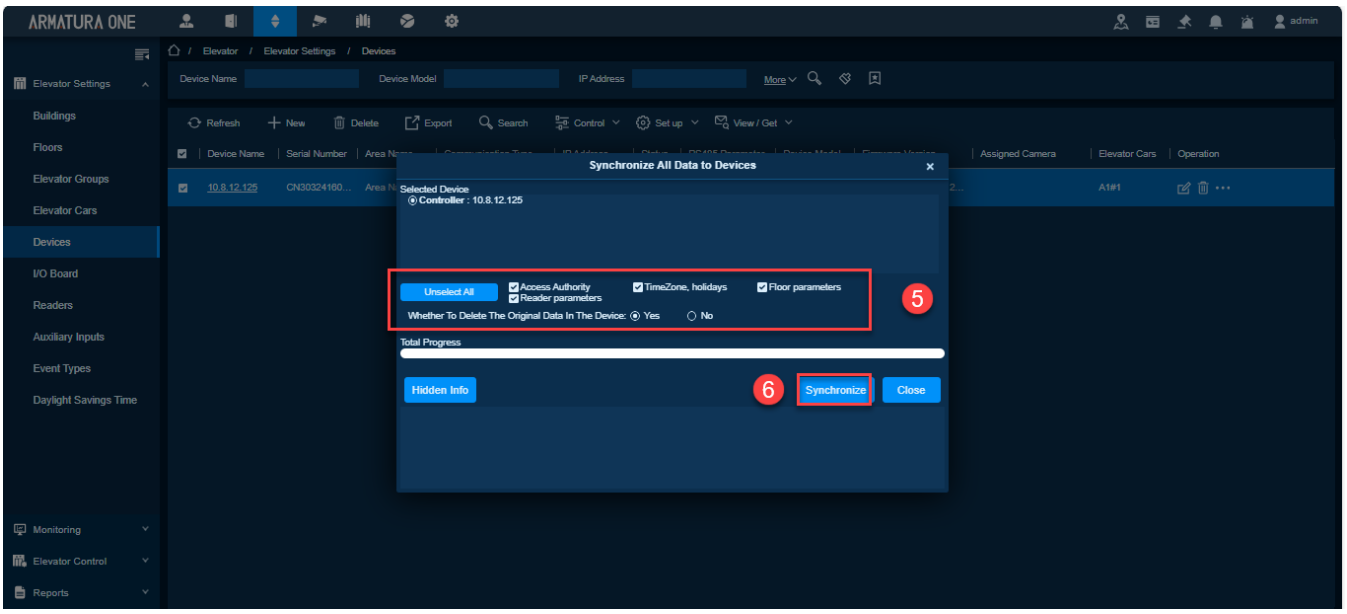
Synchronize All Data

Usage Scenario: Send configuration data to the device.

Steps: Select the device, click **[Synchronize All Data]**, and confirm.



Copyright © 2024 ARMATURA LLC. All rights reserved



Setup Functions

Modify IP address

Prerequisites for Use

The elevator control device must be functioning normally and integrated into the system.

Usage Scenarios

Resolve IP conflicts or other network issues by modifying the elevator control device's IP address.

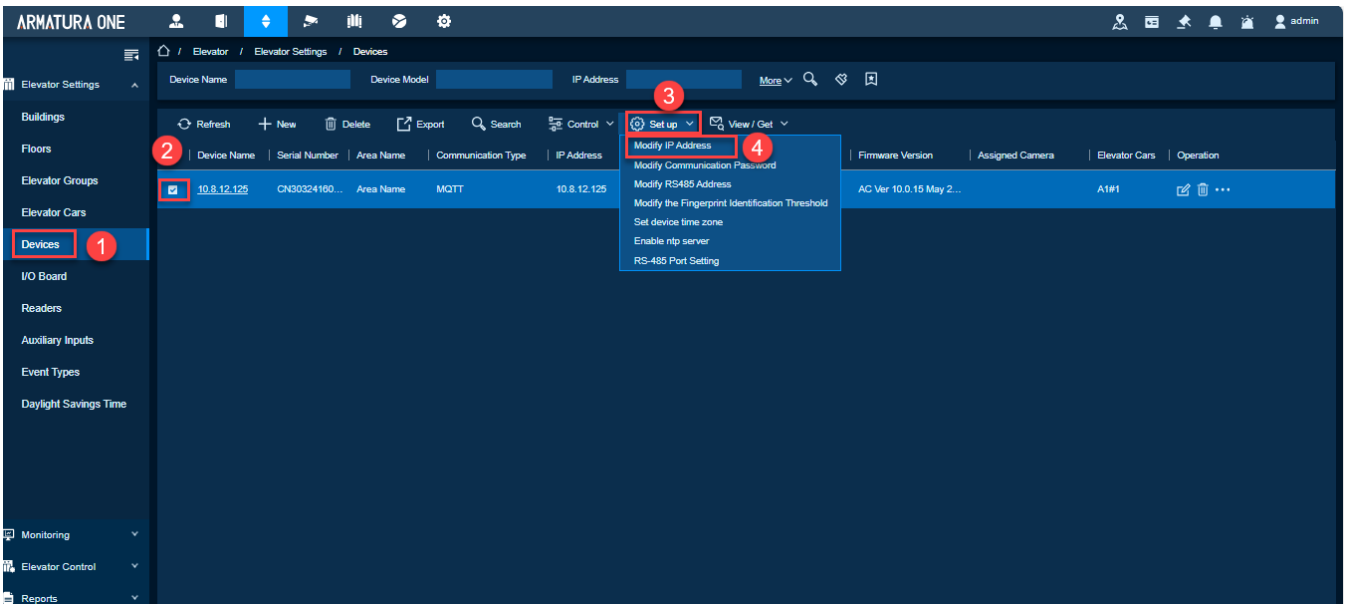
Trigger Result

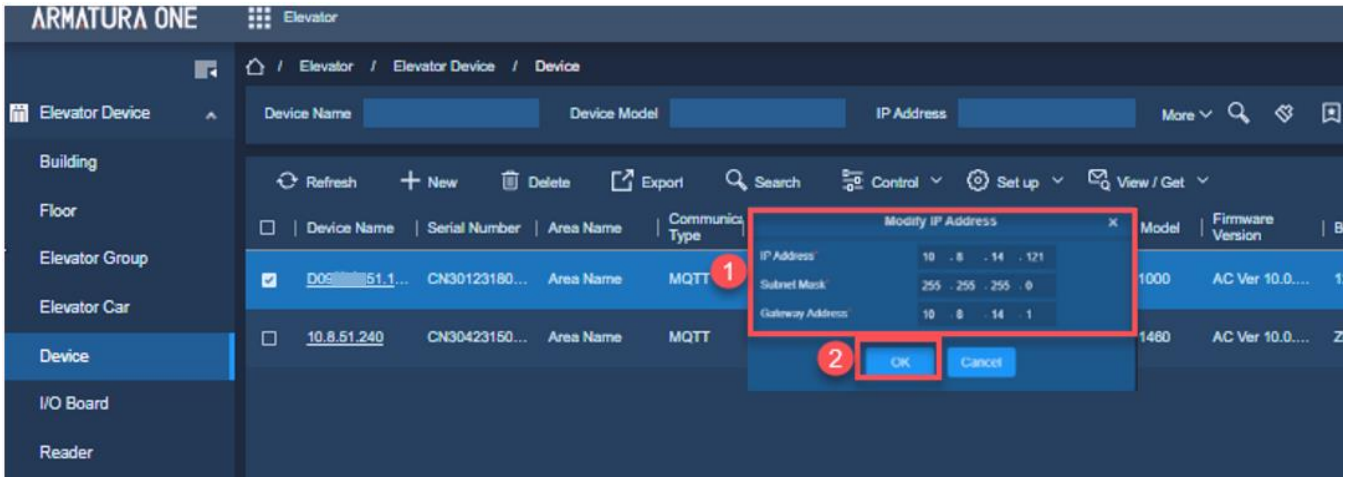
The IP address of the elevator control device is successfully updated.

Steps:

- Select the Elevator Control Device.
- Click the **[Modify IP Address]** button.
- In the pop-up window, modify the IP address, subnet mask, and gateway parameters.
- Click **[OK]** to save the changes.

Copyright © 2024 ARMATURA LLC. All rights reserved





The field description are as follows:

IP Address: Enter the device's IP address.

Subnet Mask: Enter the subnet mask.

Gateway Address: Enter the gateway address.

Settings-Modify Communication Password

Prerequisites for Use

The elevator control device must be communicating normally and integrated into the system.

Usage Scenarios

Protect the Elevator Control Device by requiring password authentication to establish communication.

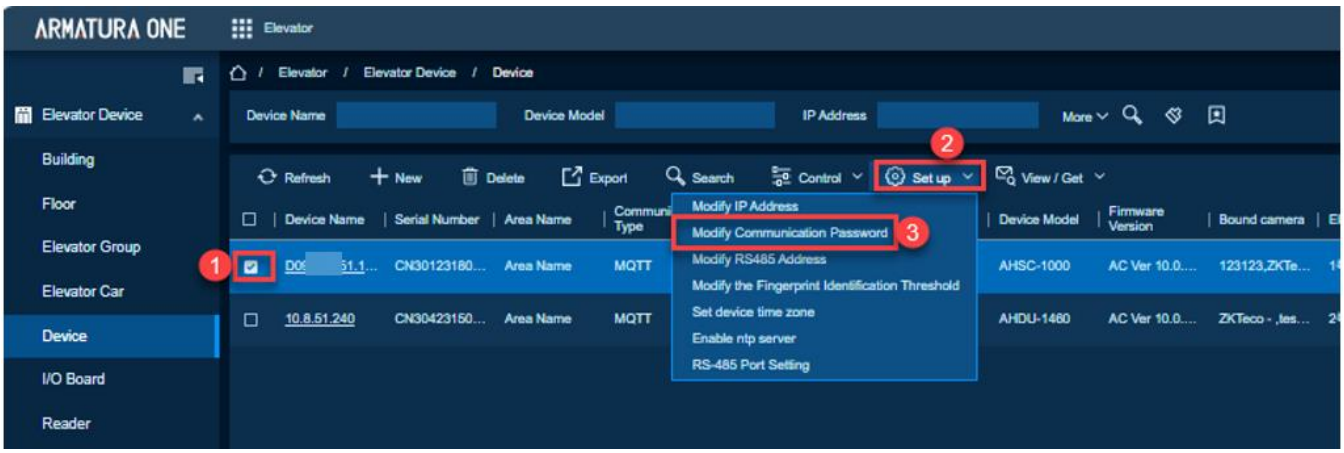
Trigger Result

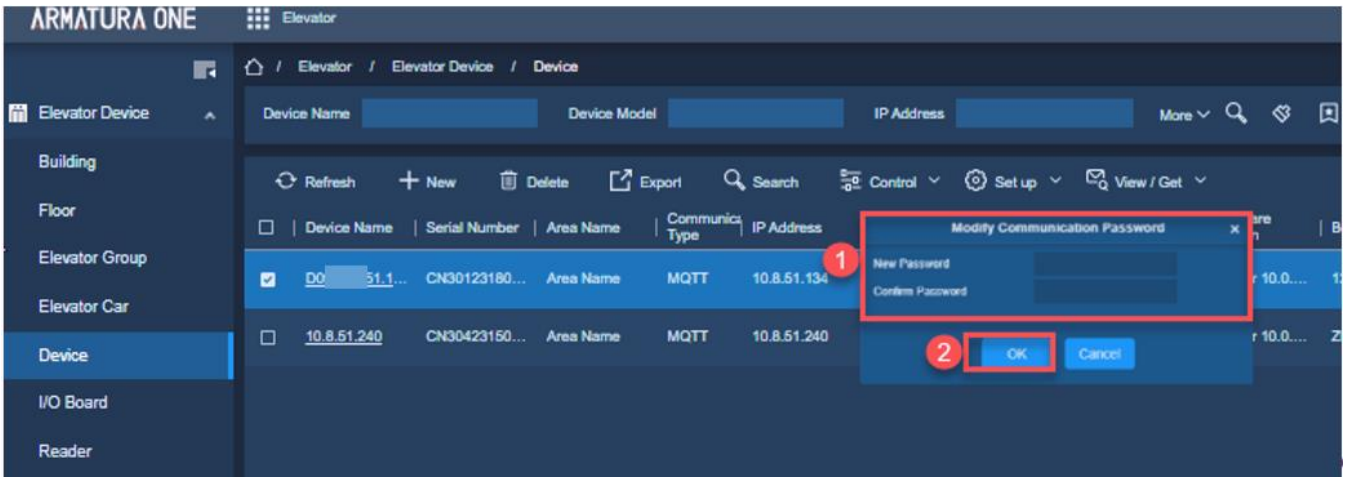
A new communication password is set for the device.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Select the Elevator Control Device.
- Click the **[Modify Communication Password]** button.
- In the pop-up window, enter the new password and confirm it (both fields must match).
- Click **[OK]** to save.





The field description are as follows:

New Password: Enter the new password.

Confirm Password: Re-enter the password for confirmation.

Settings-Modify RS485 Address

Prerequisites for Use

The elevator control device must be communicating normally and integrated into the system.

Usage Scenarios

Update the RS485 address when the reader dial code changes.

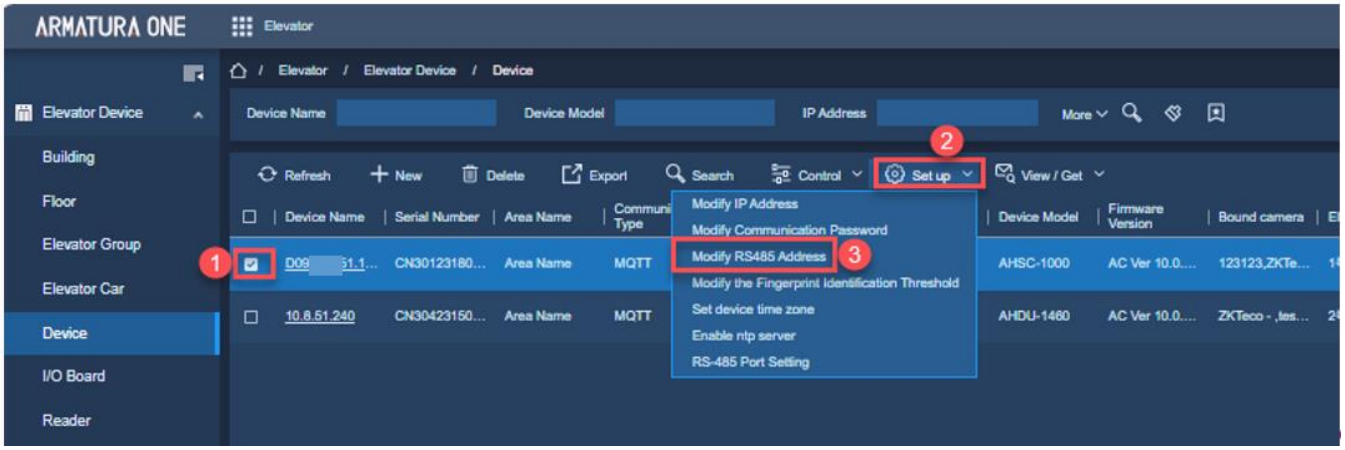
Trigger Result

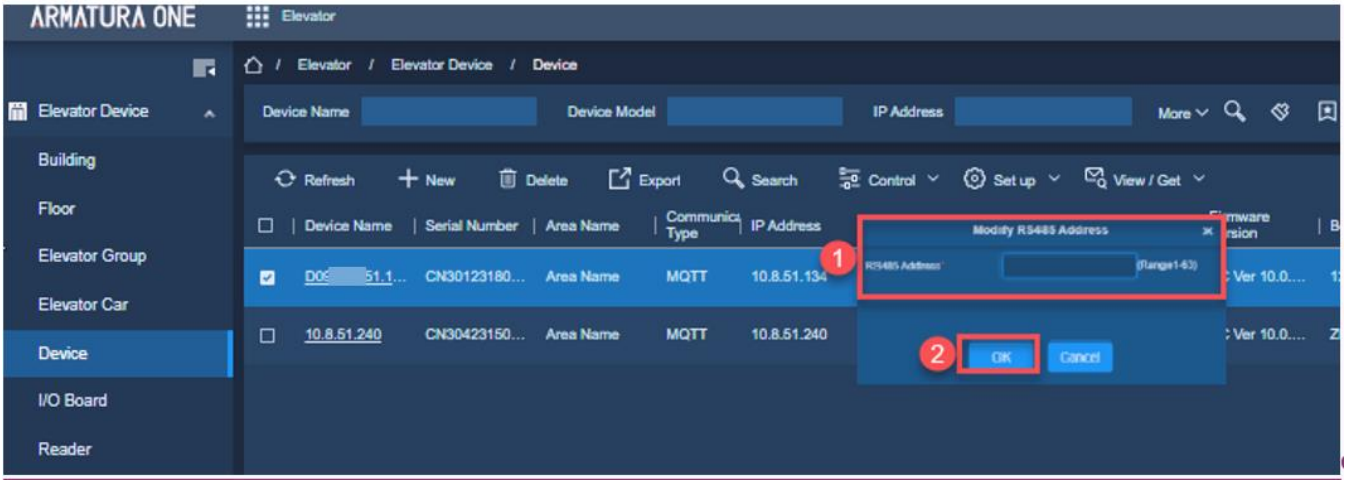
The RS485 address is successfully updated.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Select the Elevator Control Device.
- Click the **[Modify RS485 Address]** button.
- In the pop-up window, enter the new RS485 address.
- Click **[OK]** to confirm.





The field description are as follows:

RS485 Address: Enter the RS485 address.

Settings-Modify Fingerprint Comparison Threshold

Prerequisites for Use

The elevator control device must support fingerprint reading and verification.

It must be communicating normally and added to the system.

Usage Scenarios

Adjust the threshold level for fingerprint comparison during elevator control verification.

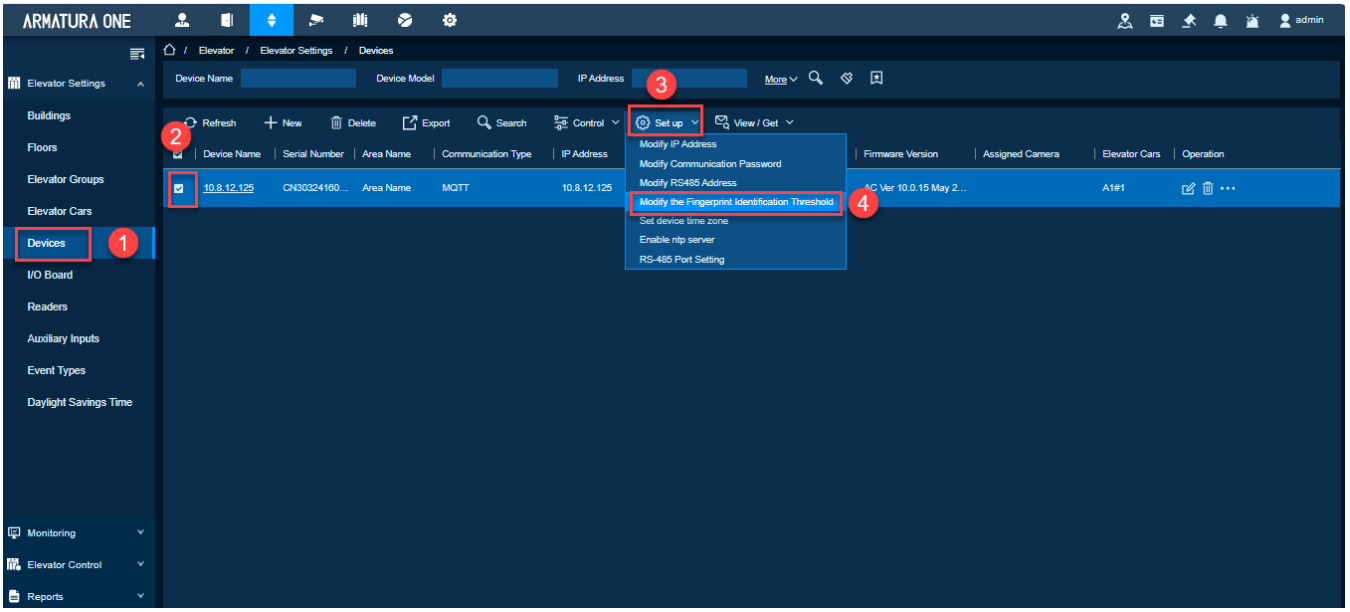
Copyright © 2024 ARMATURA LLC. All rights reserved

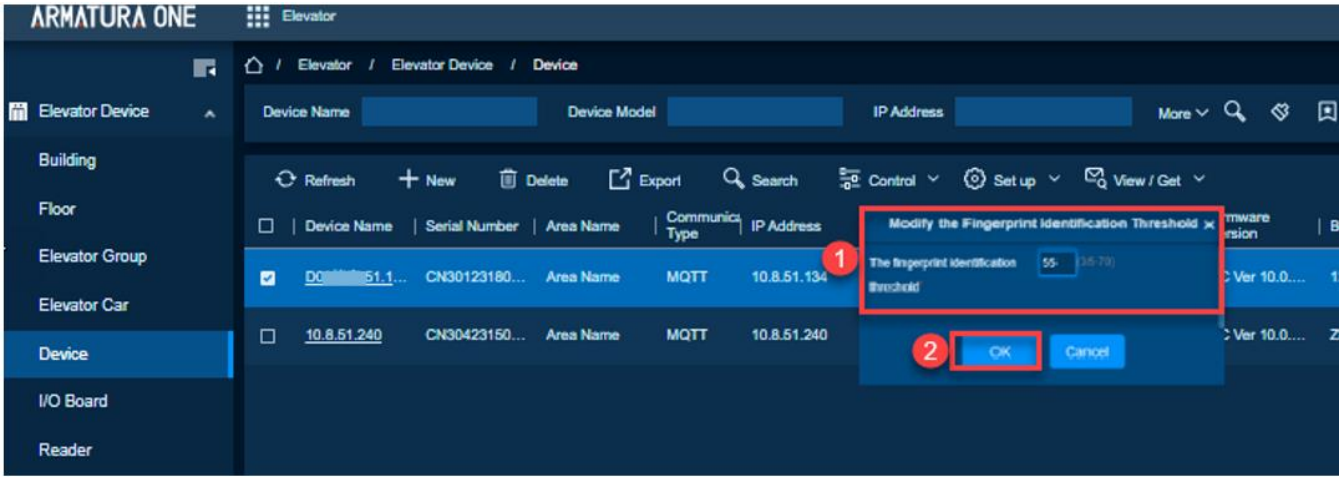
Trigger Result

The fingerprint comparison threshold is successfully updated.

Steps:

- Select the Elevator Control Device.
- Click **[Modify the Fingerprint Identification Threshold]**.
- In the pop-up window, adjust the threshold value.
- Click **[OK]** to confirm.





The field description are as follows:

Fingerprint Identification Threshold: Enter the desired threshold value.

Set device time zone

Prerequisites for Use

The elevator control device must support timezone configuration and be integrated into the system.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

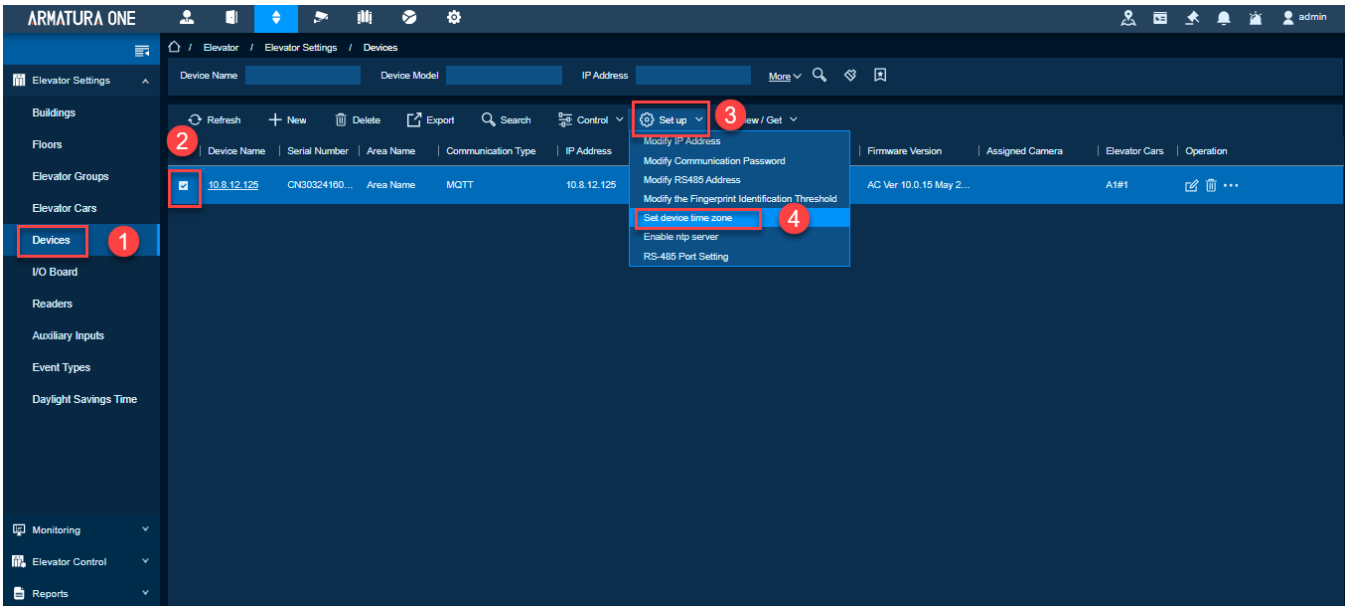
Set the elevator device's timezone with local time.

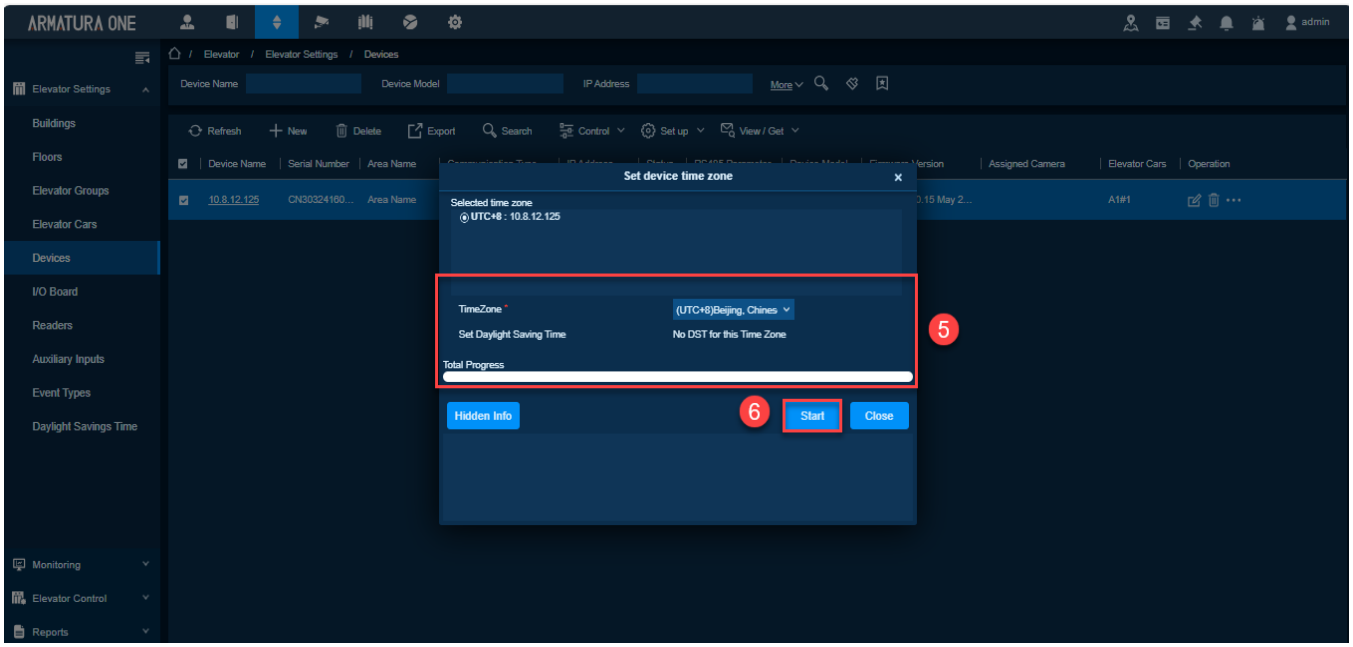
Trigger Result

The device's timezone is updated.

Steps:

- Select the Elevator Control Device.
- Click **[Set Device Time Zone]**.
- In the pop-up window, select the appropriate timezone.
- Click **[OK]** to save the changes.





Copyright © 2024 ARMATURA LLC. All rights reserved

Enable NTP Server

Prerequisites for Use

The elevator control device must support NTP server settings and be integrated into the system.

Usage Scenarios

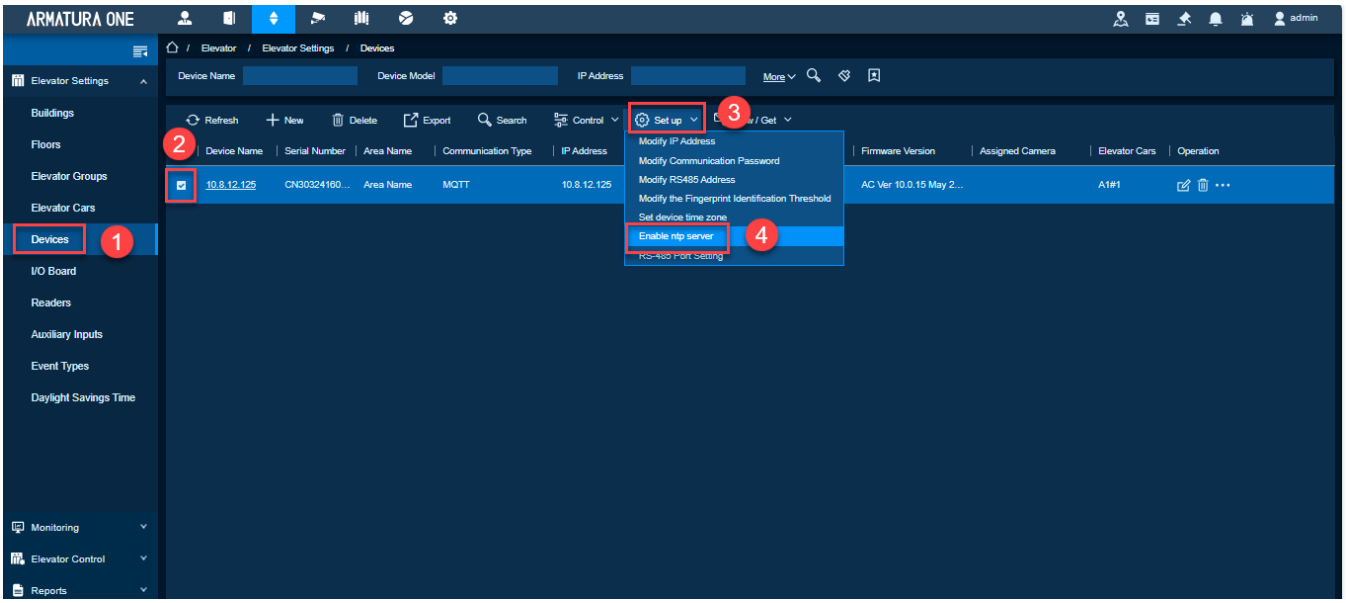
Configure or enable the NTP server for time synchronization.

Trigger Result

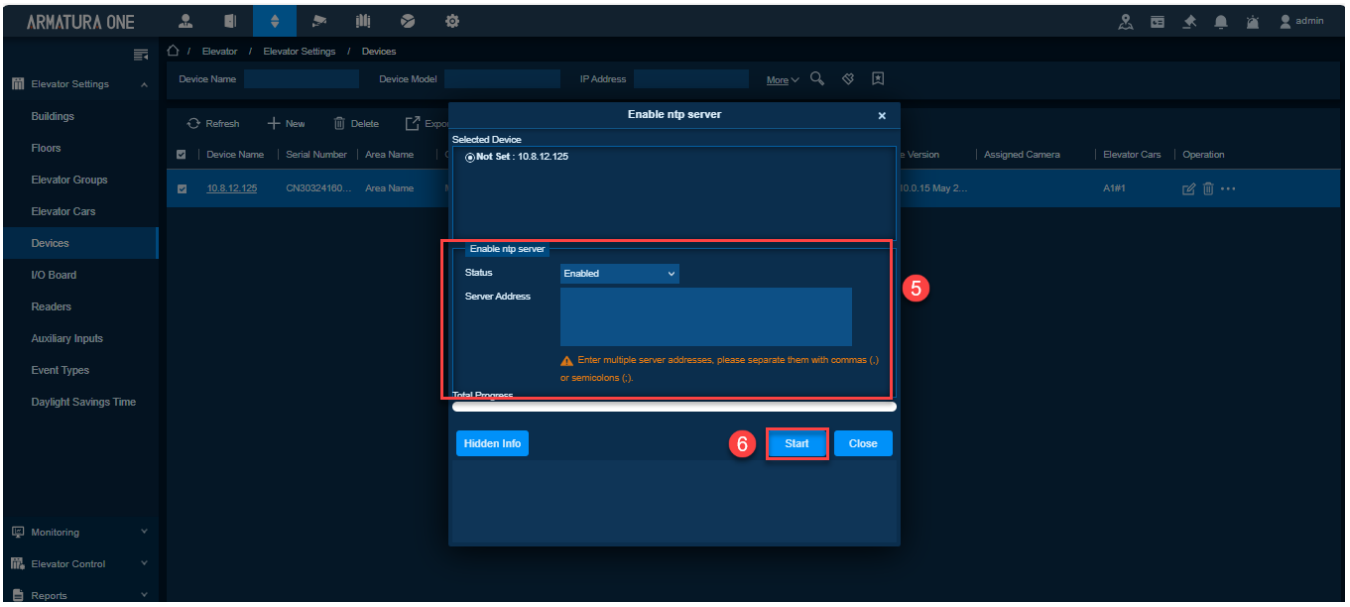
NTP server settings are updated.

Steps:

- Select the Elevator Control Device.
- Click **[Set NTP Server]**.
- Enter the server address and modify the status as needed.
- Click **[OK]** to confirm.



Copyright © 2024 ARMATURA LLC. All rights reserved



RS-485 Port Setting

Prerequisites for Use

The elevator control device must support RS-485 port and baud rate settings.

Usage Scenarios

Modify the RS-485 port and baud rate.

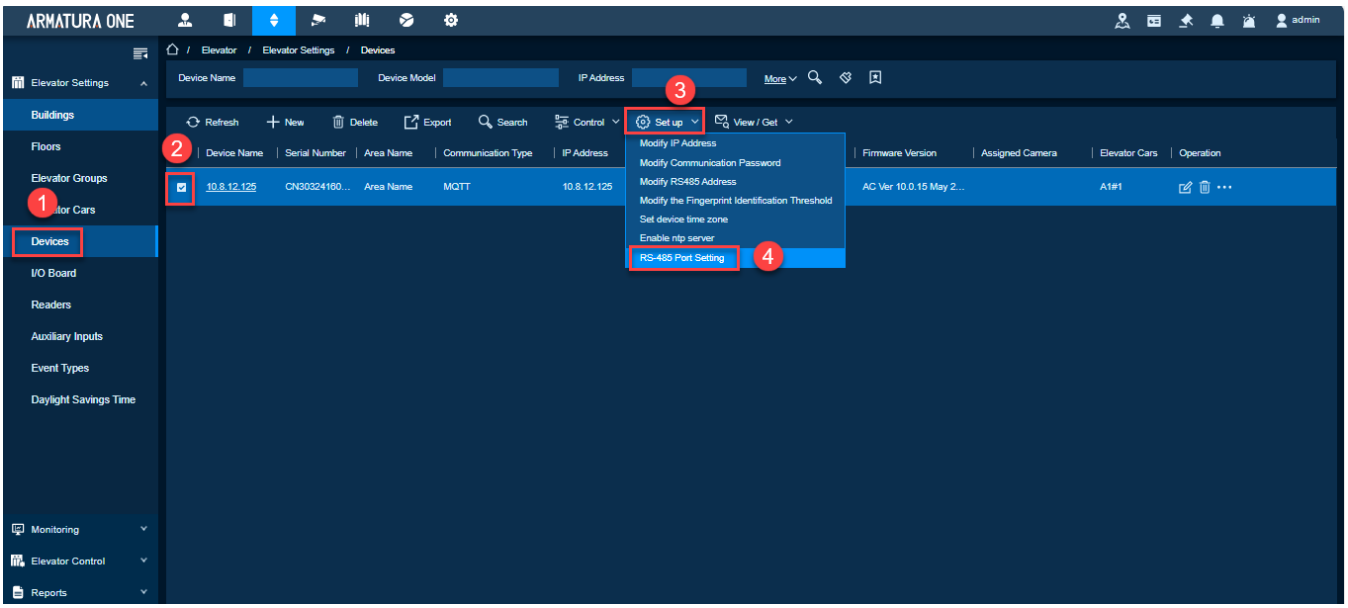
Trigger Result

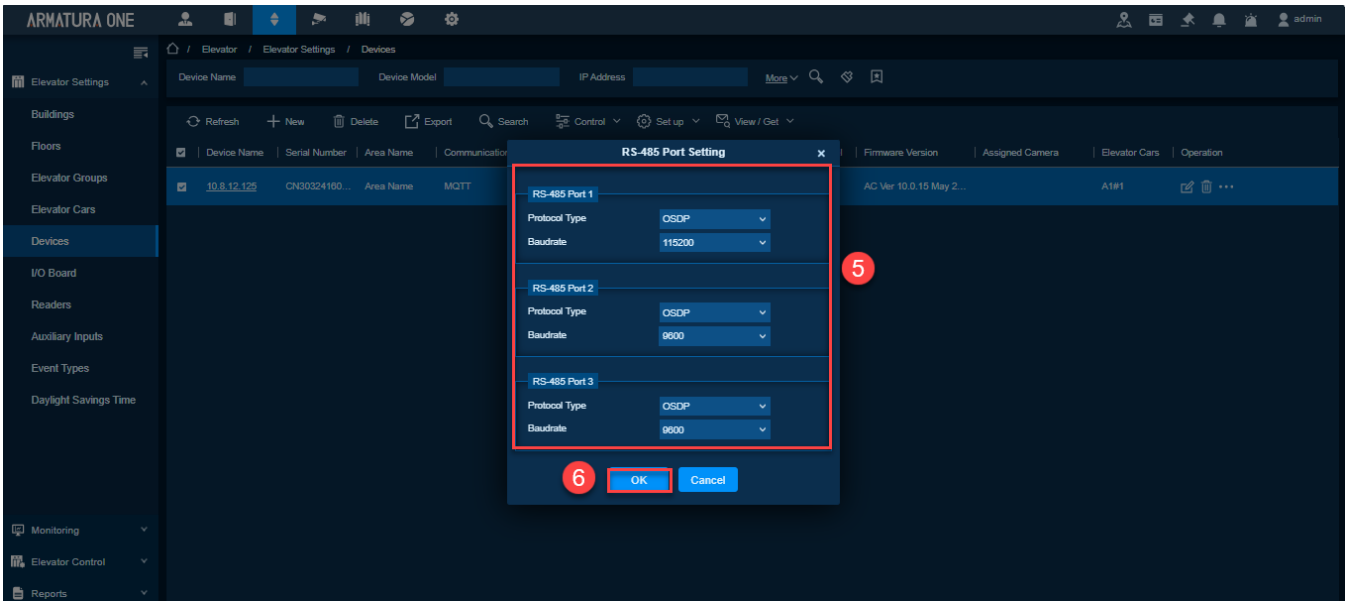
RS-485 port settings are updated.

Steps:

- Select the Elevator Control Device.
- Click **[RS-485 Port Setting]**.
- Configure the protocol type and baud rate in the pop-up window.
- Click **[OK]** to save the changes.

Copyright © 2024 ARMATURA LLC. All rights reserved





The field description are as follows:

Protocol Type: Choose the RS-485 protocol type.

Baud Rate: Select the communication speed.

View and Get Functions

Prerequisites for Use

The elevator control device must be integrated into the system and functioning normally.

Usage Scenarios

Retrieve the current parameters from the elevator control device to ensure synchronization with the system.

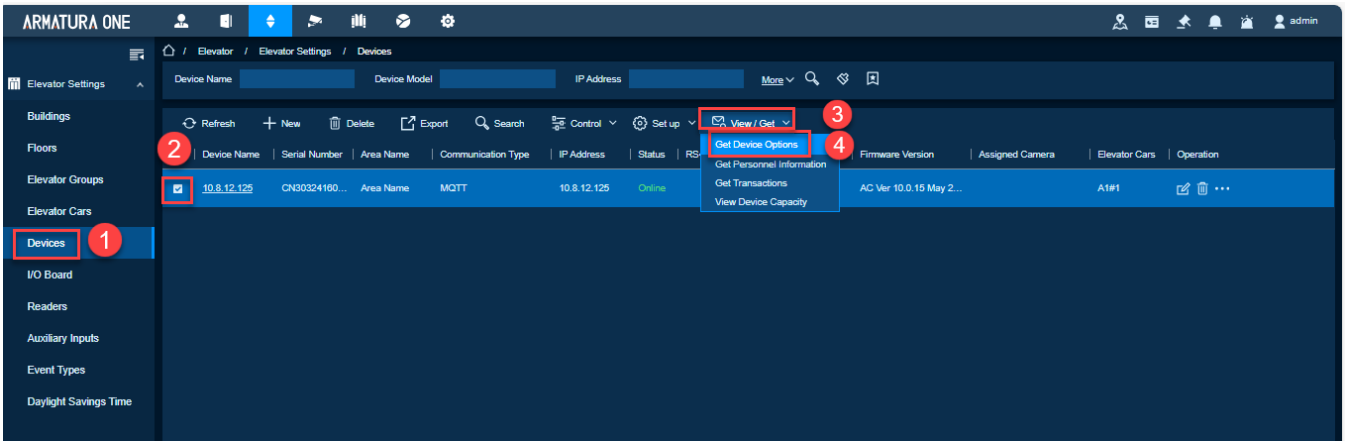
Copyright © 2024 ARMATURA LLC. All rights reserved

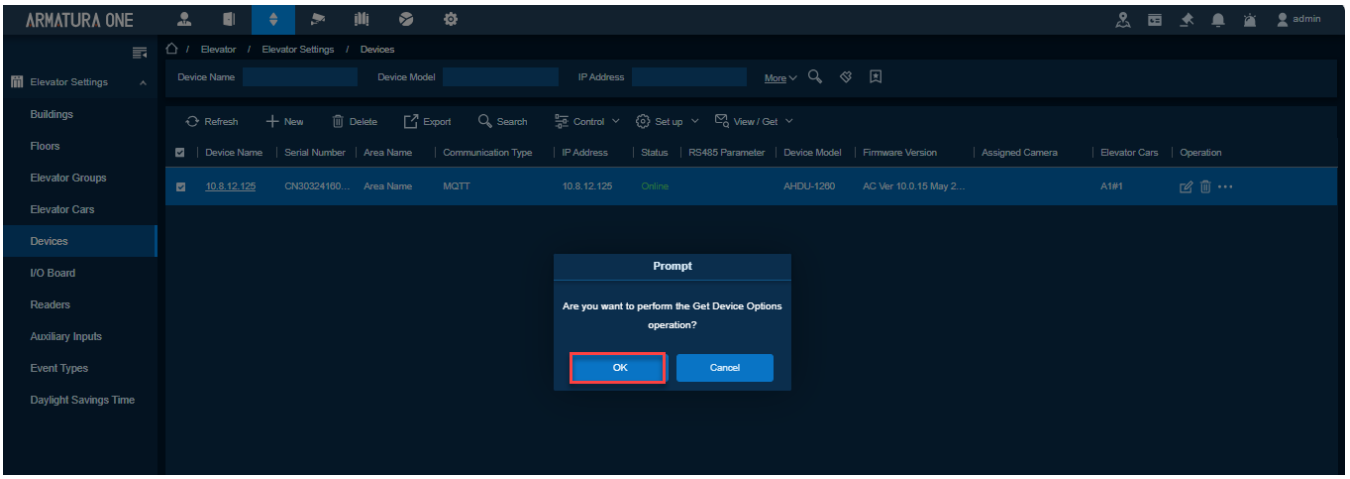
Trigger Result

The system synchronizes the elevator control device parameters.

Steps:

- Select the Elevator Control Device.
- Click **[Get Device Option]**.
- In the pop-up window, click **[OK]** to fetch and display the device parameters.





Get Personnel Information

Prerequisites for Use

The elevator control device must be communicating normally and integrated into the system.

Usage Scenarios

Retrieve personnel data stored on the elevator control device to synchronize with the system.

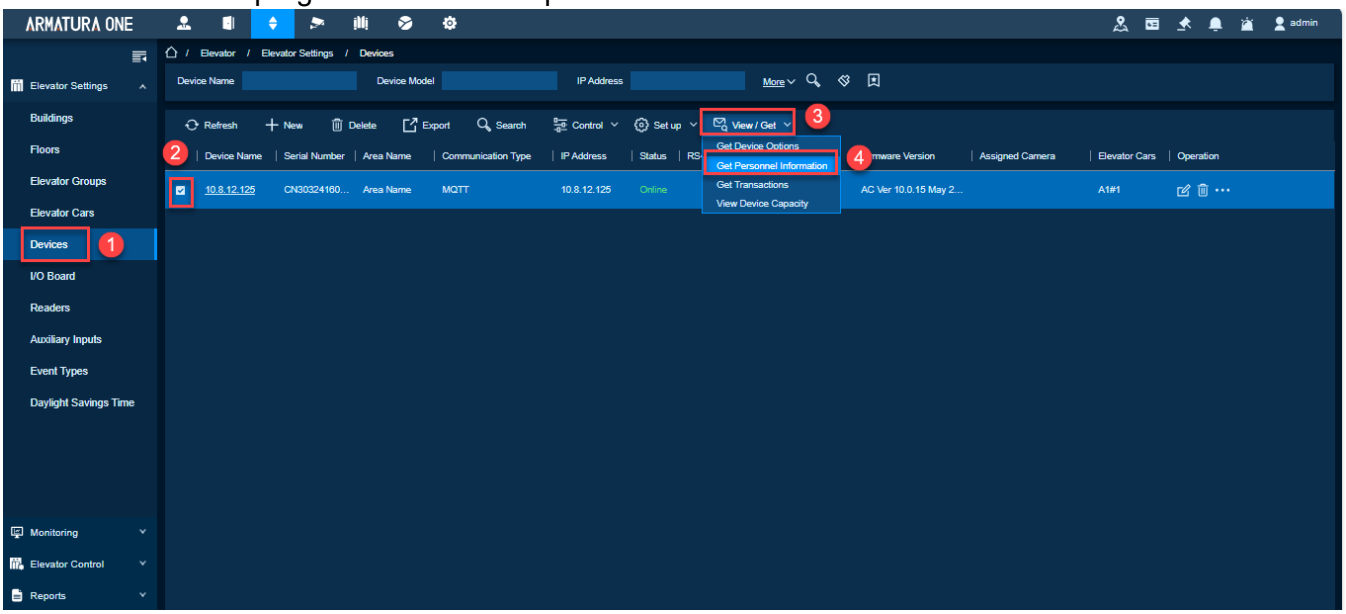
Trigger Result

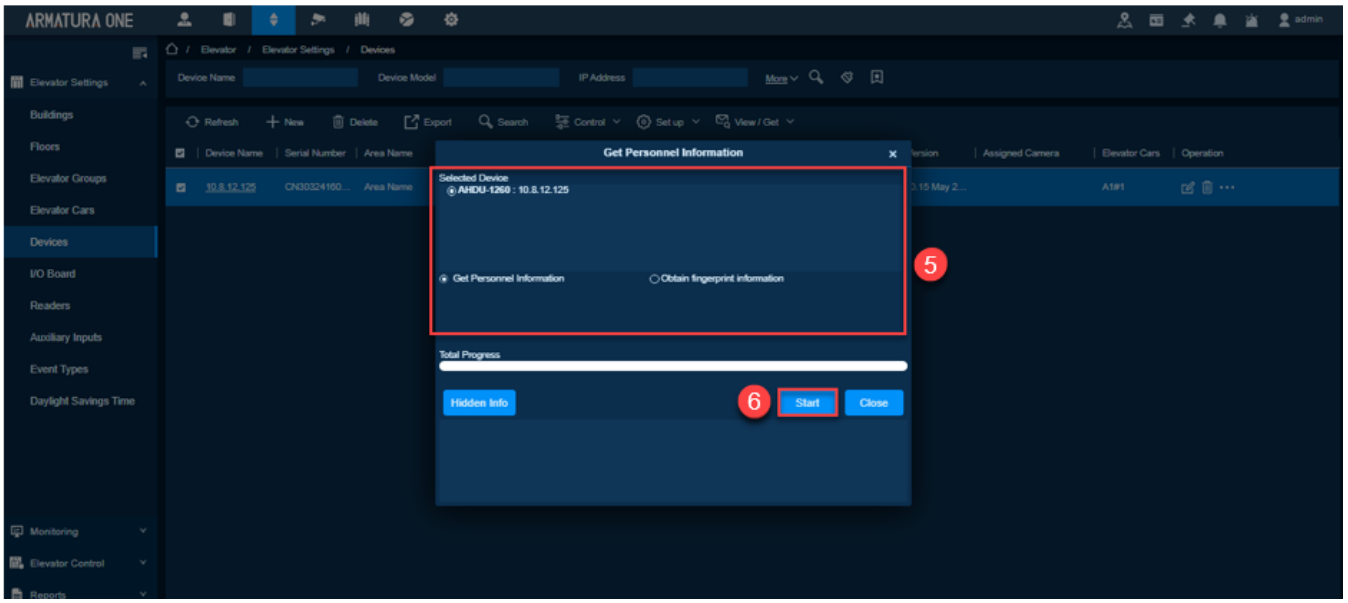
Personnel information is synchronized with the system.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Select the Elevator Control Device.
- Click **[Get Personnel Information]**.
- In the pop-up window, click **[Start]** to initiate the process.
- Monitor the progress bar until completion.





Get Transactions

Prerequisites for Use

The elevator control device must be integrated into the system and function normally.

Usage Scenarios

Fetch all event transaction data from the elevator control device.

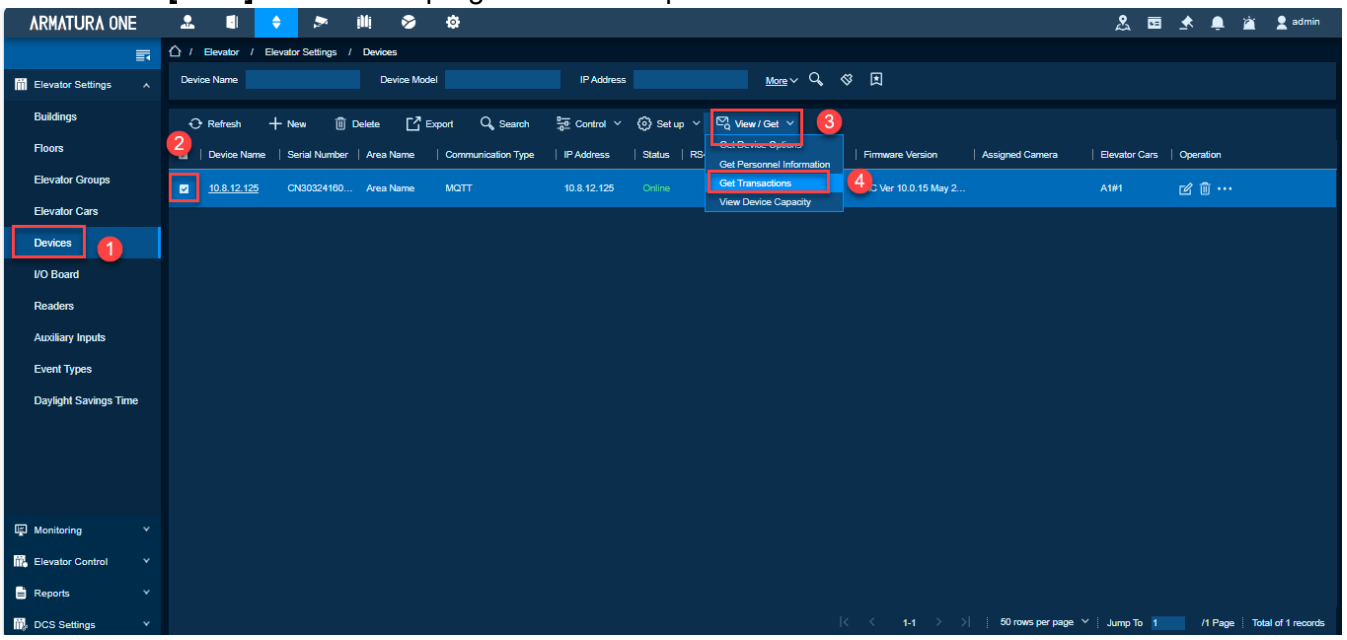
Copyright © 2024 ARMATURA LLC. All rights reserved

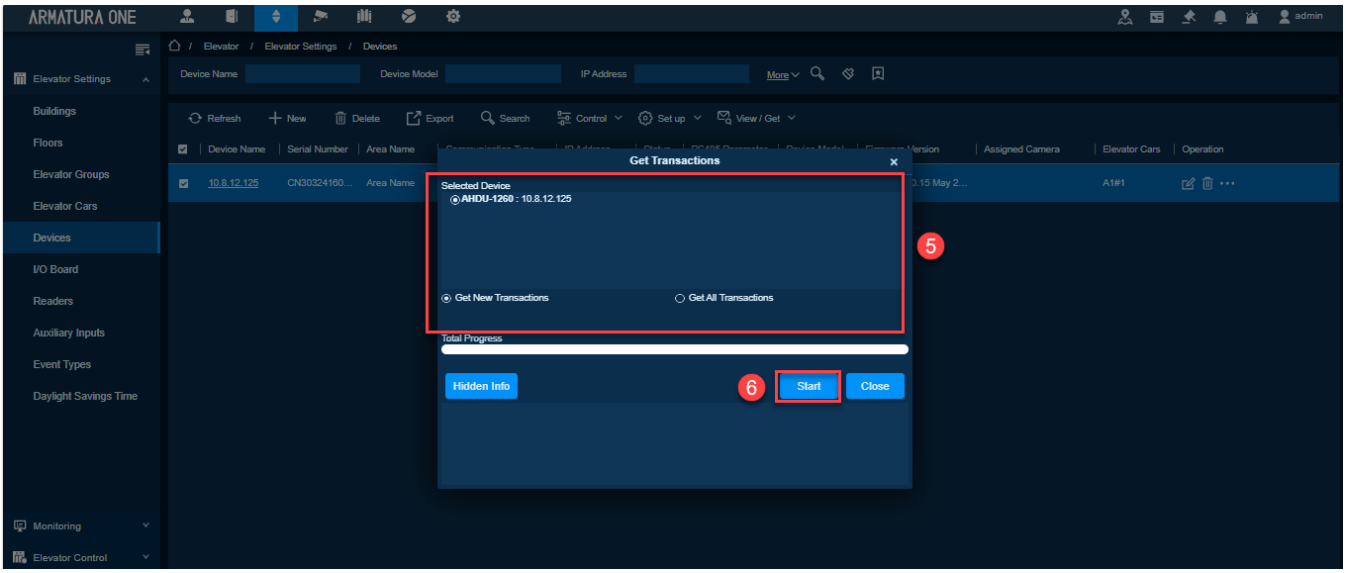
Trigger Result

Transaction data is retrieved and saved in the system.

Steps:

- Select the Elevator Control Device.
- Click **[Get Transactions]**.
- Choose between retrieving new records or all records in the pop-up window.
- Click **[Start]** and monitor progress until completion.





Copyright © 2024 ARMATURA LLC. All rights reserved

View Device Capacity

Prerequisites for Use

The elevator control device must be communicating normally and integrated into the system.

Usage Scenarios

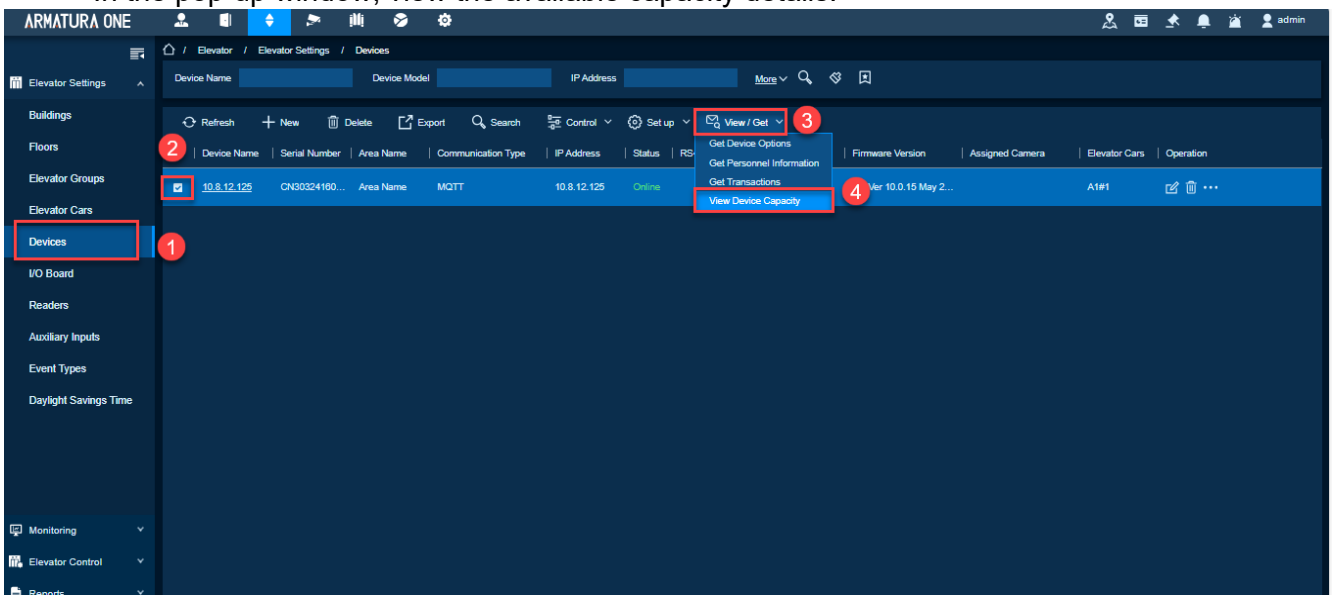
Review the capacity information of the elevator control device.

Trigger Result

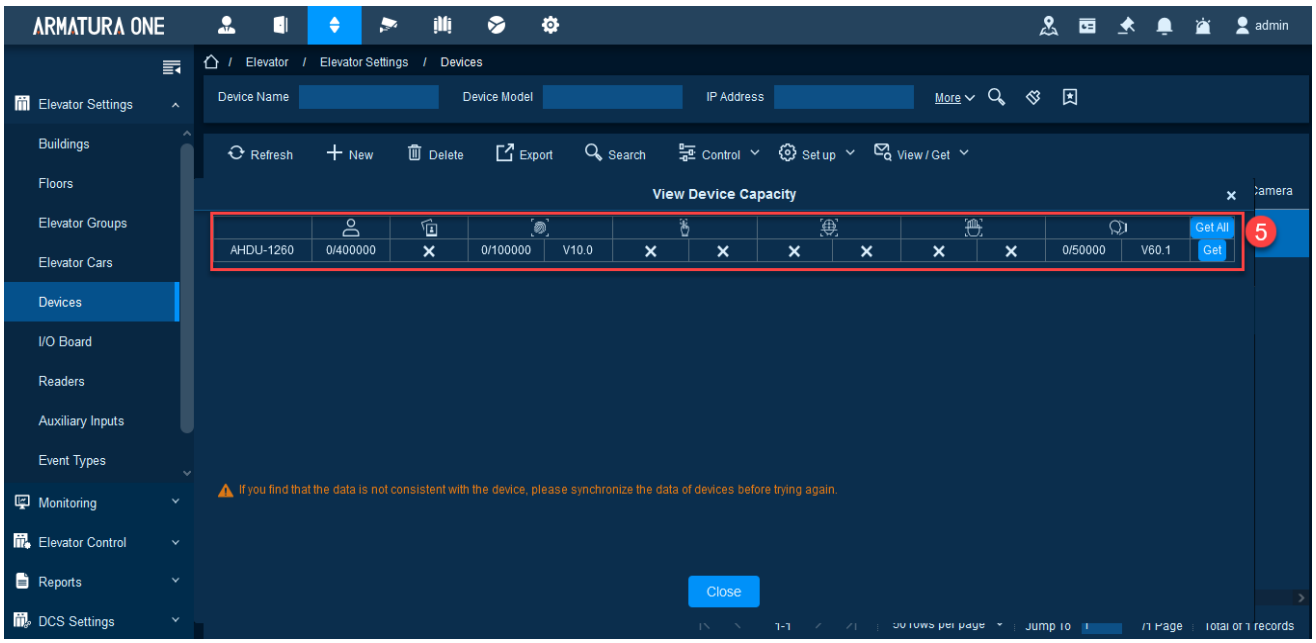
The system displays capacity details for the device.

Steps:

- Select the Elevator Control Device.
- Click **[View Device Capacity]**.
- In the pop-up window, view the available capacity details.



Copyright © 2024 ARMATURA LLC. All rights reserved



8.1.6 I/O Board

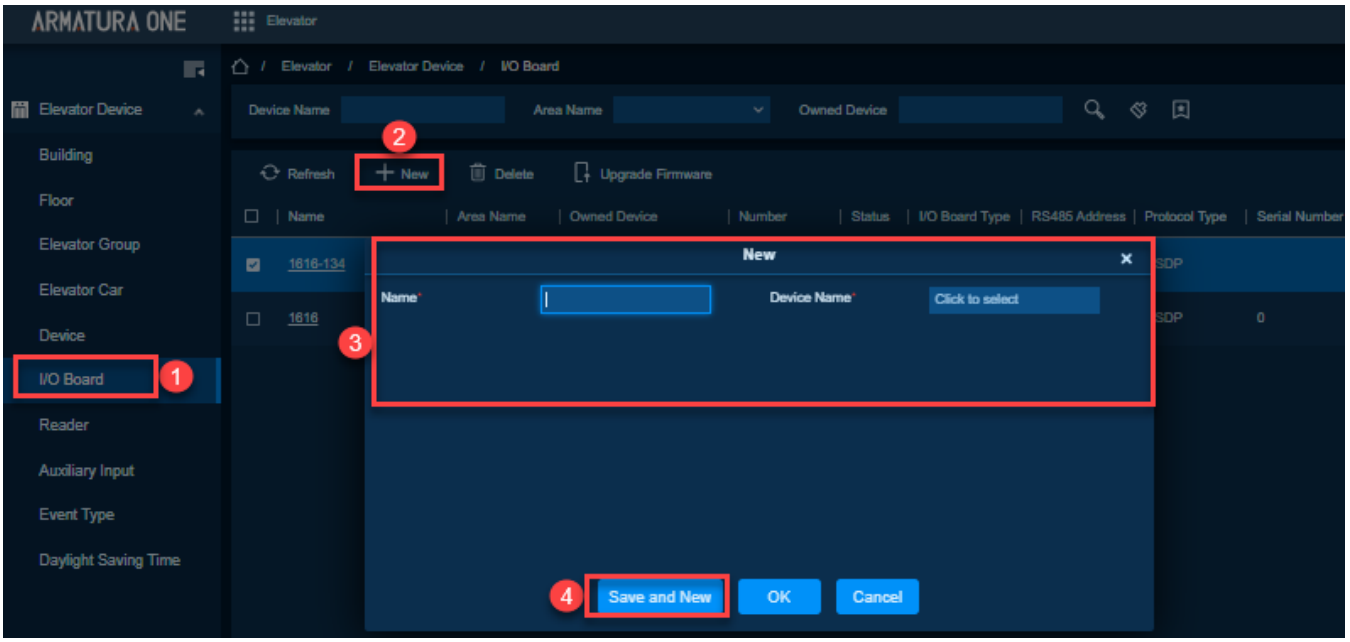
Function Description

The I/O Board section provides detailed configuration and management options for elevator devices. Each I/O board is associated with a device name, protocol type, and port.

Add New I/O Board

Steps:

- Navigate to **[Elevator Settings] > [I/O Board] > [New]**.
- Enter the required details in the provided fields.
- Click **[Save and New]** to submit the information.



Copyright © 2024 ARMATURA LLC. All rights reserved

Field Description:

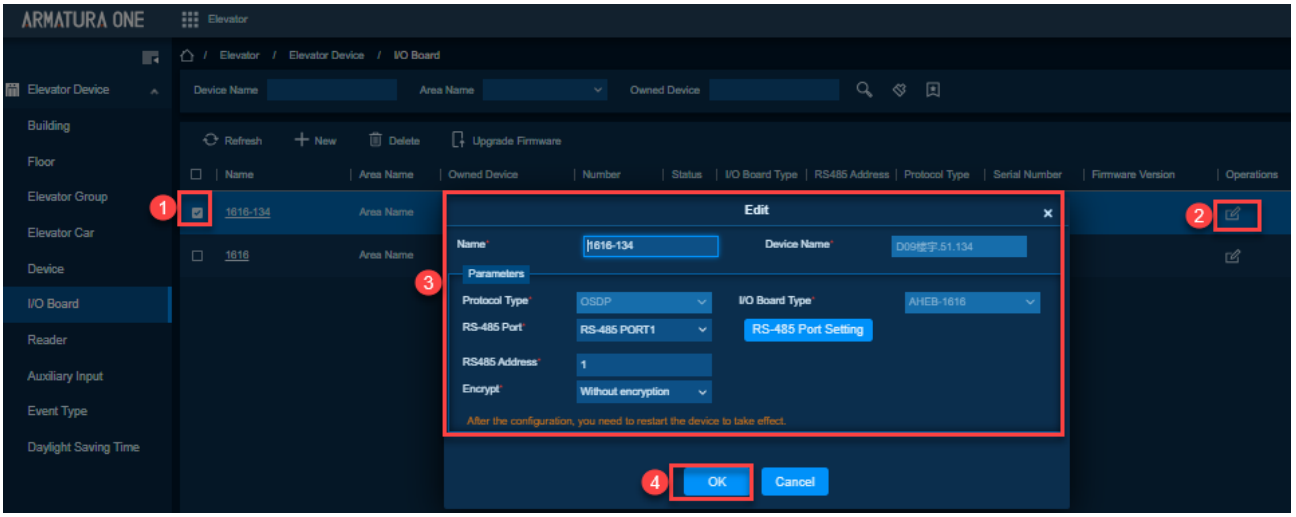
Name: Specify the name of the I/O board.

Device Name: Select the corresponding device name from the list.

Edit I/O Board

Steps:

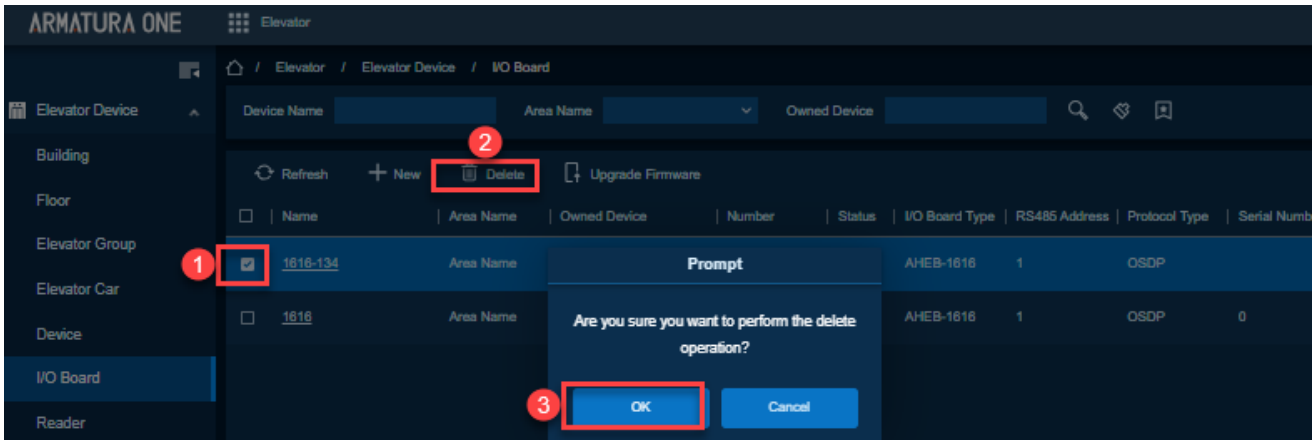
- Navigate to **[Elevator Settings] > [I/O Board] > [Edit]**.
- Modify the necessary details in the provided fields.
- Click **[OK]** to save the changes.



Delete I/O Board

Steps:

- Navigate to **[Elevator Settings] > [I/O Board]** and select the I/O board to be deleted.
- Click the **[Delete]** button.
- Confirm the action by clicking **[OK]** in the pop-up confirmation window.

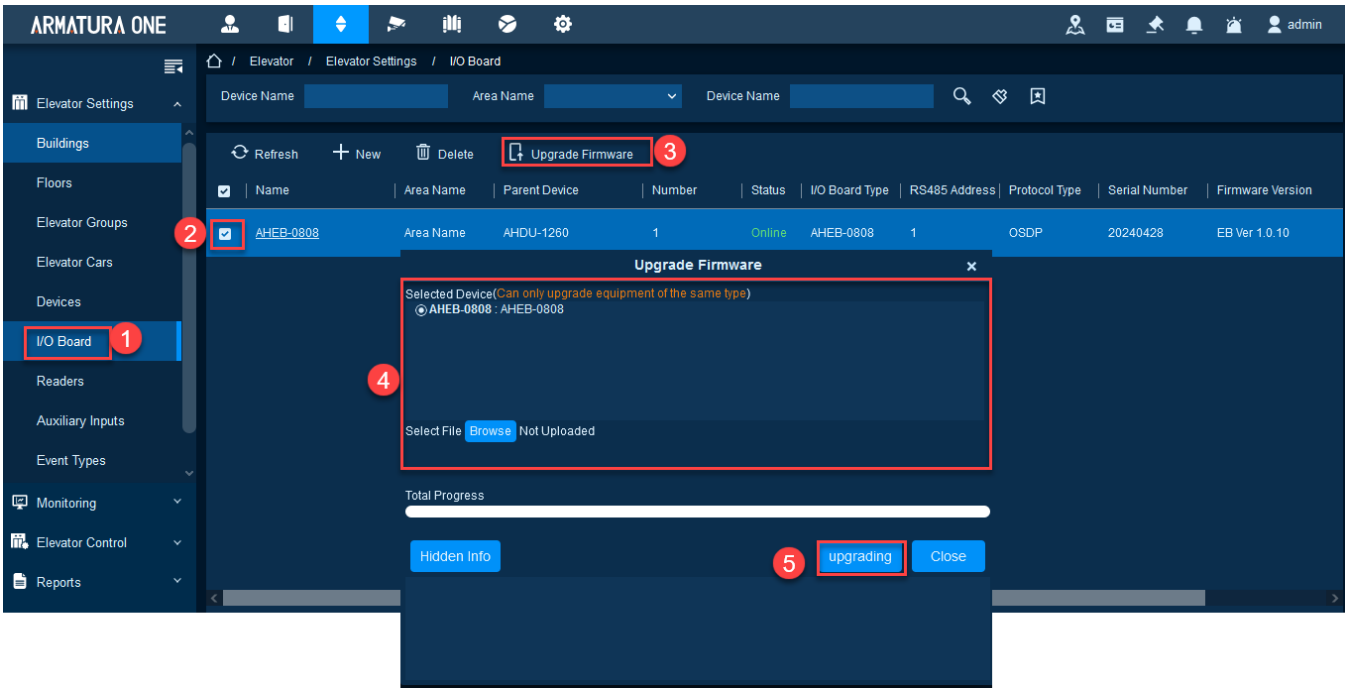


Upgrade Firmware

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Elevator Settings] > [I/O Board] > [Upgrade Firmware]**.
- Select the required firmware file from your system.
- Click **[Upgrade Firmware]** to initiate the upgrade process.



8.1.7 Readers

Function Description

Each elevator control device is equipped with a reader port. The reader's information, such as operation interval and verification methods, can be configured or modified as needed.

Edit

Prerequisites for Use

The elevator control devices must be successfully added to the system.

Each elevator control device automatically generates default reader information.

Usage Scenarios

Modify the reader's operation interval.

Change the verification method to suit the security and operational requirements.

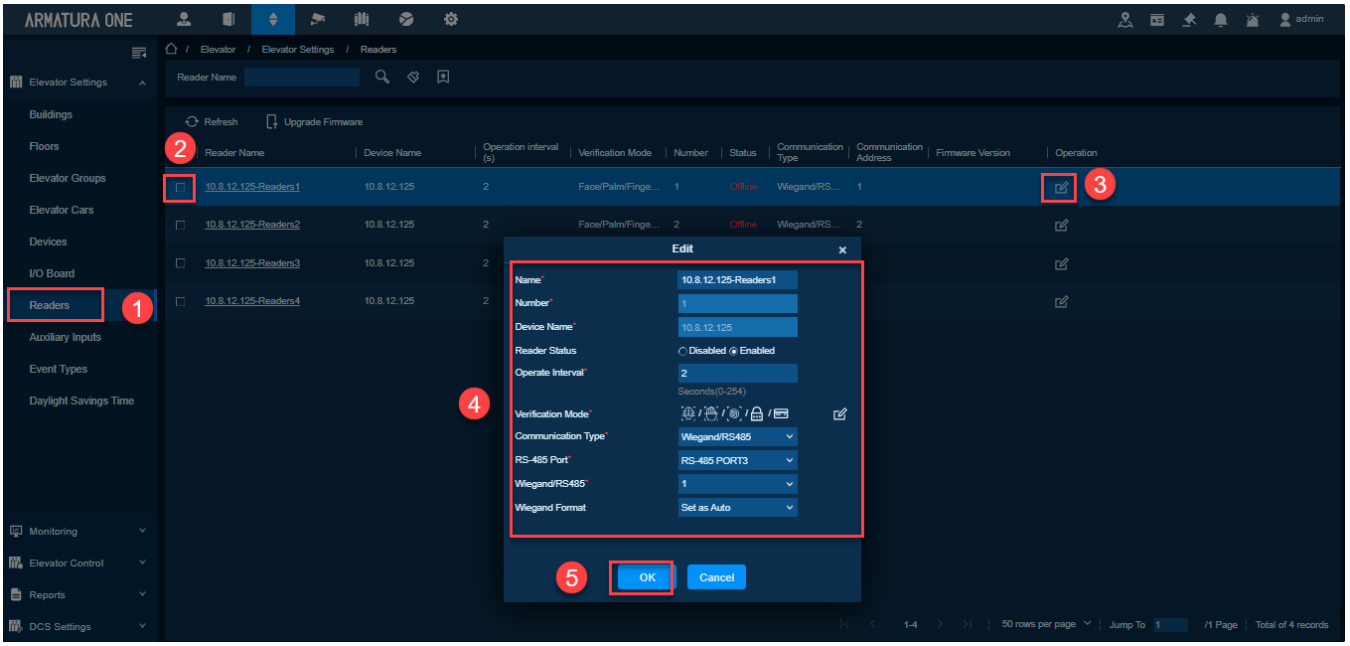
Trigger Result

Updates the operation interval and verification method for the selected reader in the elevator control device.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Navigate to **[Elevator Settings] > [Reader] > [Edit]**.
- Select a reader from the list.
- Modify the necessary parameters in the fields provided.
- Click **[OK]** to save and exit.



Field Descriptions:

Name: Displays the name of the reader.

Number: Displays the number of the reader.

Owned Device: Displays the associated device (not editable).

Reader Status: Displays the current operational status of the reader.

Operate Interval: The time interval between two verification attempts. Default is 2 seconds; range is 0–254 seconds.

Verification Mode: Specifies the mode of verification. Options vary depending on the reader type:

- **Wiegand Reader:**
  - "Only Card"
  - "Only Password"
  - "Card or Password"
  - "Card and Password"
  - "Card or Fingerprint"
- **RS485 Reader:**

Copyright © 2024 ARMATURA LLC. All rights reserved

- "Card or Fingerprint"

- **Note:** Ensure the reader has a keypad when using "Card and Password" mode.

Communication Type: Select the communication mode for the reader.

RS-485 Port: Specify the RS485 port.

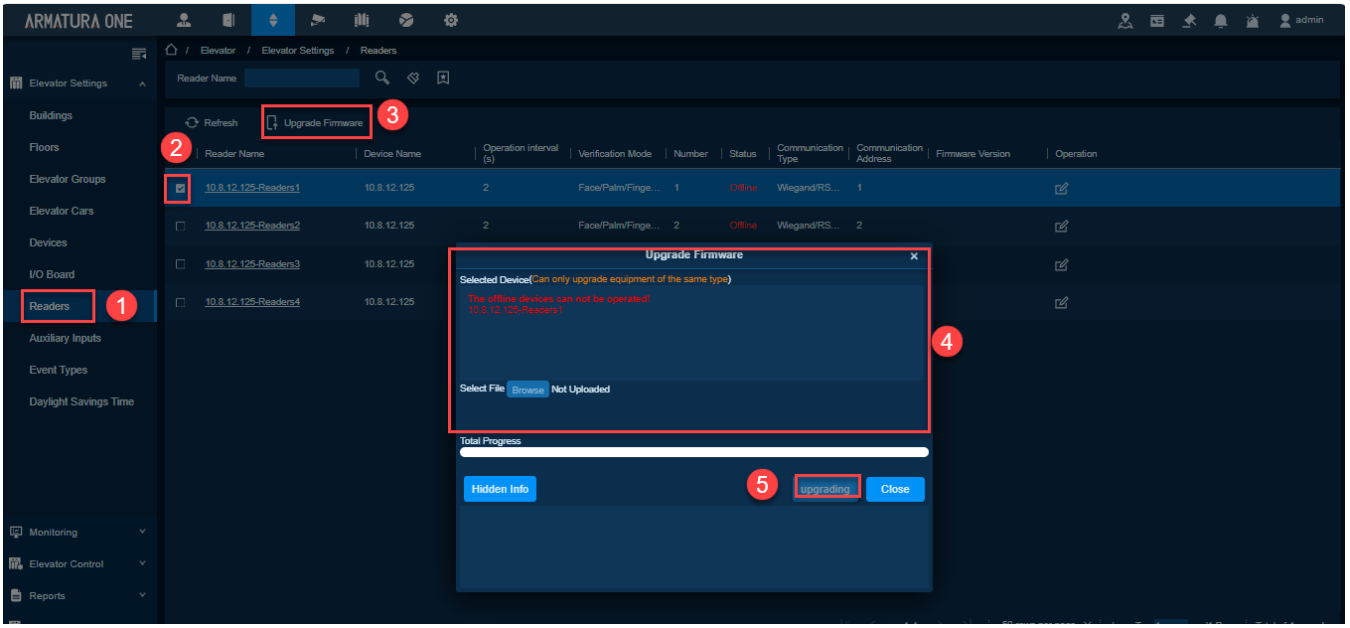
WiegandRS485: Choose the Wiegand number for the reader.

Wiegand Format: Specify the Wiegand format.

Firmware Upgrade

Steps:

- Navigate to **[Elevator Settings] > [Reader] > [Firmware Upgrade]**.
- Select the firmware upgrade file from your system.
- Click **[Upgrade Firmware]** to initiate the upgrade process.



8.1.8 Auxiliary Inputs

Function Description

Auxiliary Inputs are primarily used to connect devices like infrared sensors, smoke detectors, or other auxiliary devices. These inputs enable additional functionality for elevator control systems.

Edit Auxiliary Input

Prerequisites for Use

The elevator control devices must be successfully added to the system.

Usage Scenarios

Modify the default name of the auxiliary input to suit user preferences or operational requirements.

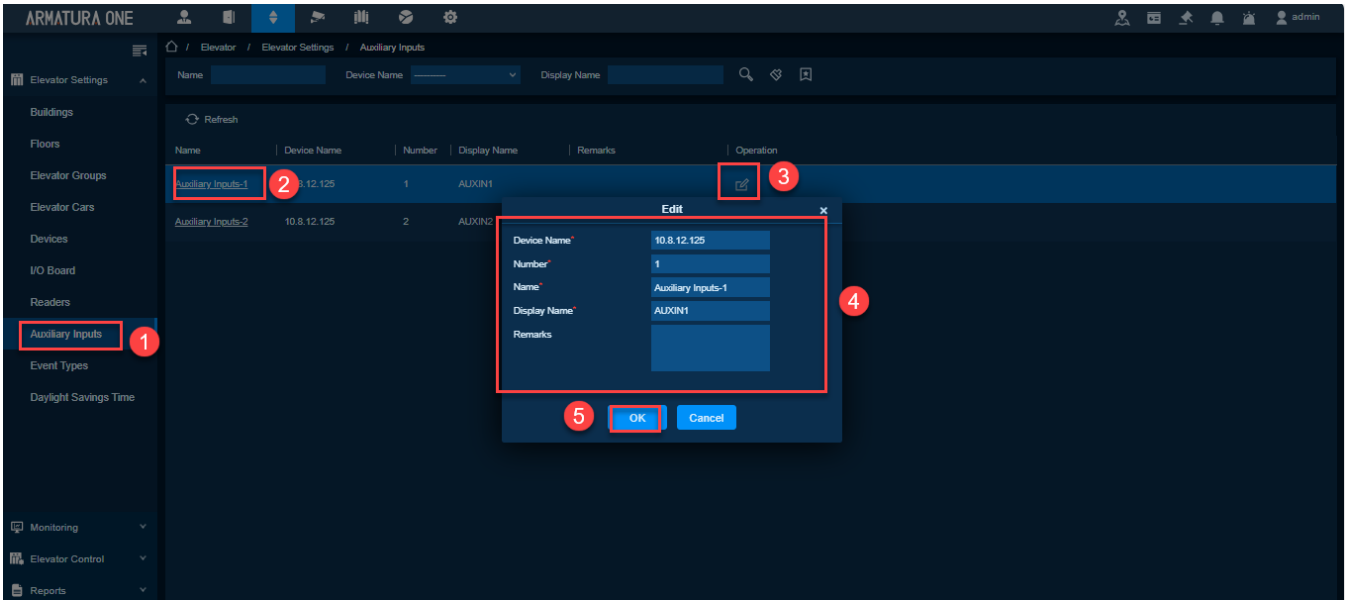
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Updates the name and remarks associated with the auxiliary input.

Steps:

- Navigate to **[Elevator Settings] > [Auxiliary Input]** on the Action Menu.
- Select the auxiliary input from the list to access its settings.
- Click **[Edit]** to modify the relevant fields.
- Make the required changes and click **[OK]** to save the updated details.



The fields are as follows:

Owned Device: Displays the IP address of the associated elevator control device. (Not editable.)

Number: Displays the number of the auxiliary input associated with the device. (Not editable.)

Name: Allows customization of the auxiliary input name based on user preference.

Printed Name: Displays the printed name on the hardware (e.g., IN9). (Not editable.)

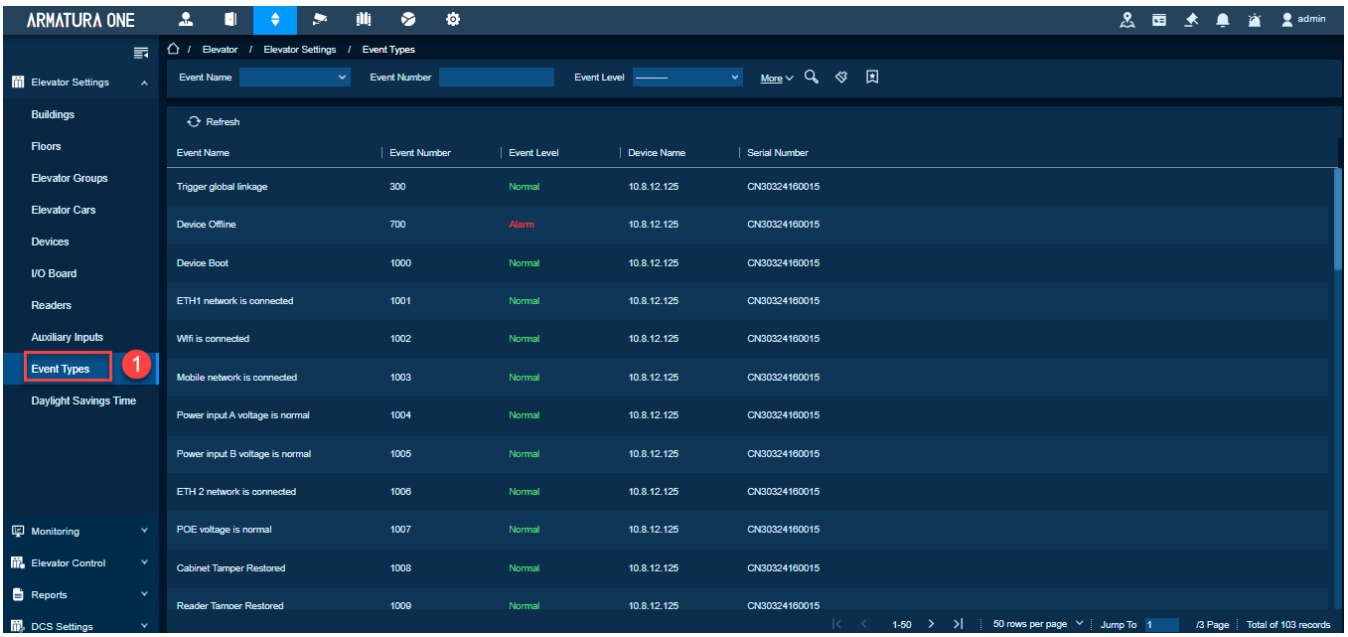
Remarks: Enter additional remarks or descriptions for the auxiliary input.

8.1.9 Event Types

Function Description

The **Event Types** feature allows users to view and manage various event types associated with elevator control devices.

Copyright © 2024 ARMATURA LLC. All rights reserved



8.1.10 Daylight Savings Time

Function Description

The **Daylight Savings Time (DST)** feature allows users to configure and manage time zone adjustments for elevator control devices. It ensures that elevator operations follow the correct time during periods when DST is in effect.

Usage Scenarios

Automatically adjust elevator operations for time changes during Daylight Savings periods.

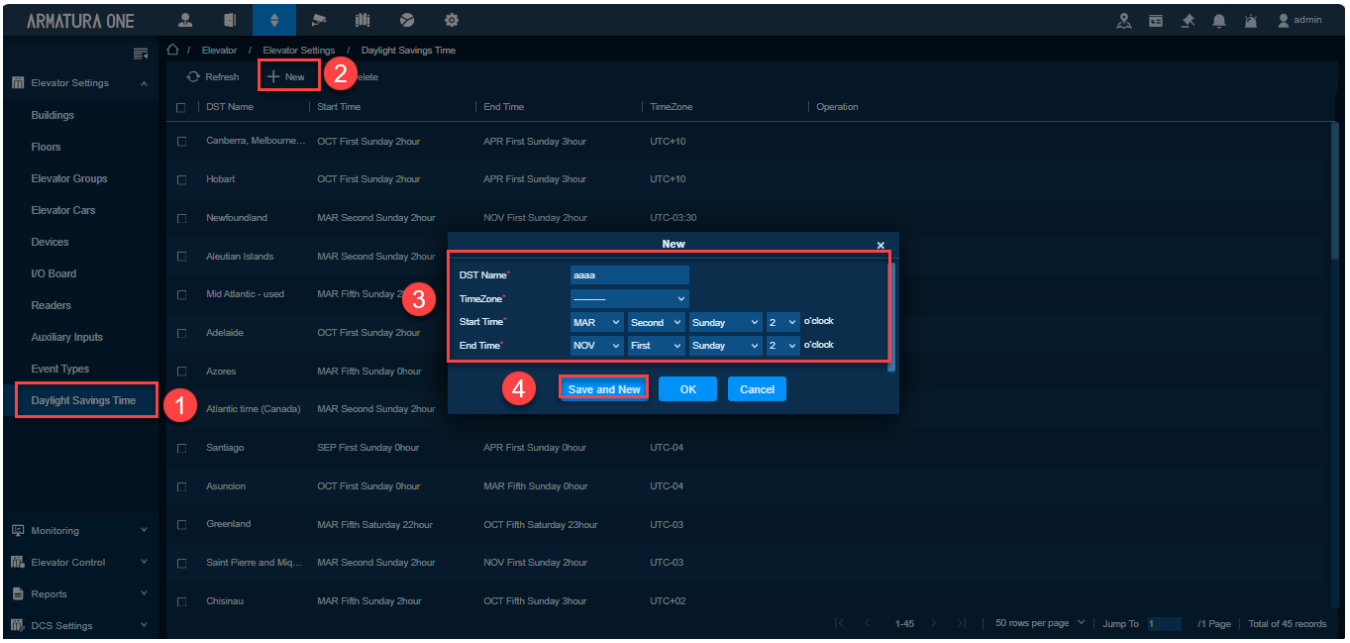
Ensure accurate scheduling and synchronization across connected elevator control devices.

New (Add)

Steps:

- Navigate to **[Elevator Settings] > [Daylight Savings Time]** in the Action Menu.
- Click **[New]** to open the configuration interface.
- Fill in the following parameters:
  - **DST Name:** Enter a unique name or title for the DST configuration.
  - **Timezone:** Select or define the timezone associated with the elevator device.
  - **Start/End Time:** Specify the start and end times for Daylight Savings adjustments.
- After entering the details, click **[Save and New]** to finalize the configuration or continue adding additional entries.

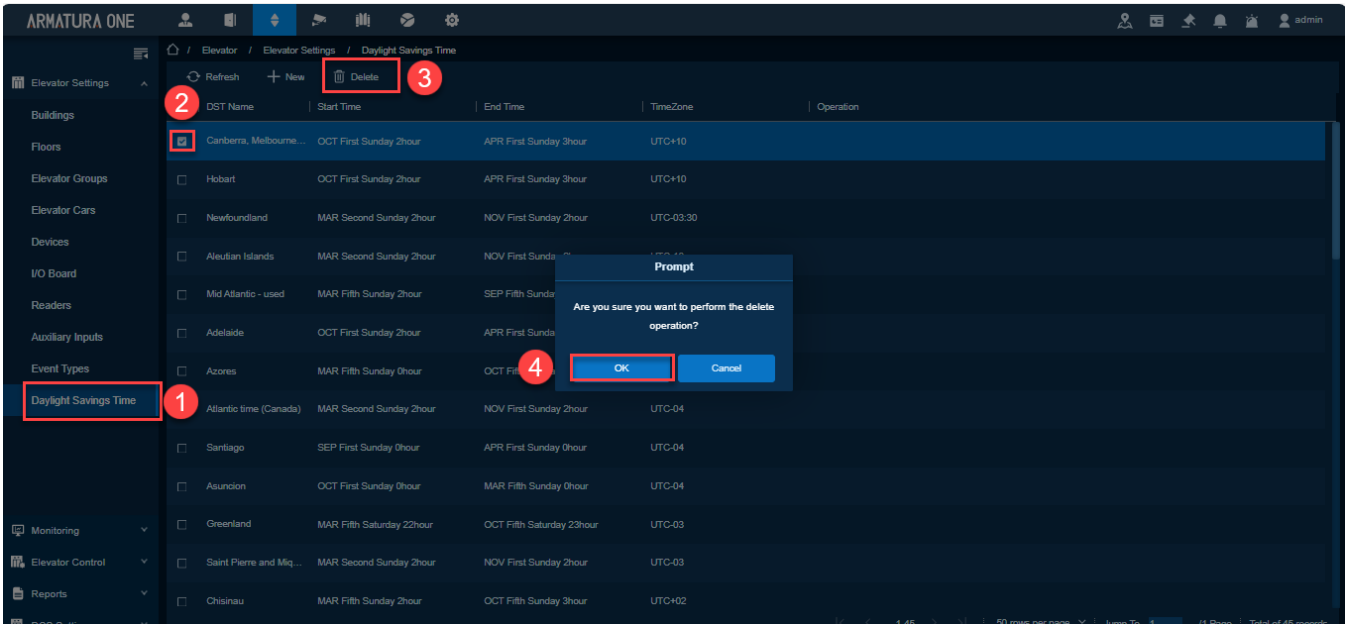
Copyright © 2024 ARMATURA LLC. All rights reserved



Delete

Steps:

- Navigate to **[Elevator Settings] > [Daylight Savings Time]** in the Action Menu.
- Select the DST configuration you wish to delete.
- Click **[Delete]** to remove the entry.
- Confirm the action by clicking **[OK]** in the confirmation prompt.



Copyright © 2024 ARMATURA LLC. All rights reserved

8.2 Monitoring

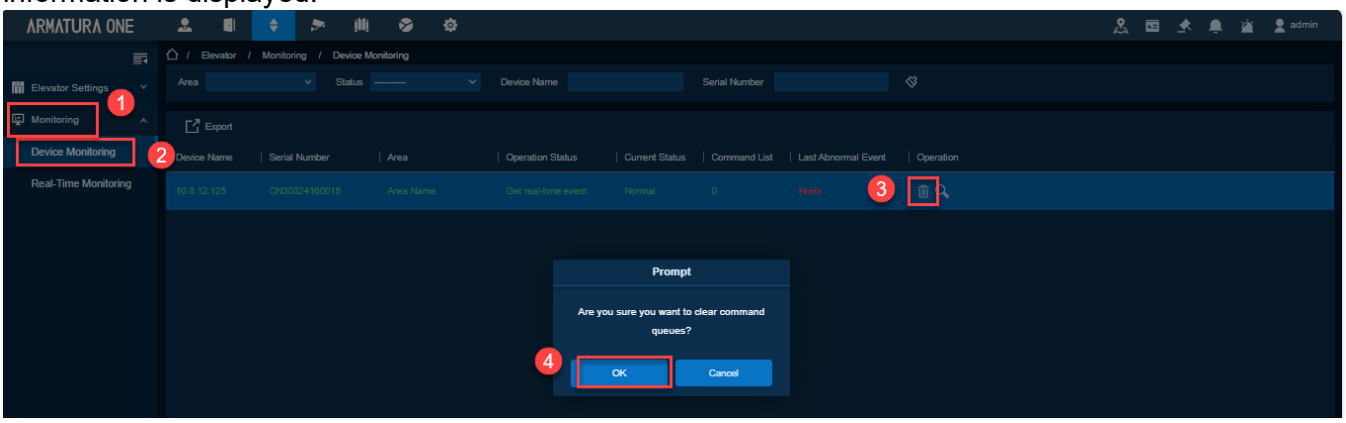
Function List

Functions	Description
Device Monitoring	Monitors elevator control device operations, including statu and commands.
Real- Time Monitorin	Displays real-time events from elevator control devices, wit options to remotely release or lock buttons.

8.2.1 Device Monitoring

Function Description

The **Device Monitoring** interface allows users to oversee the operational status and details of elevator control devices. By default, all devices within the user's access level are monitored, and key information is displayed.



Key Operations

Clear Commands

Purpose: Remove pending commands for a selected device.

Steps:

- Locate the target device in the **Device Monitoring** interface.
- Click **[Clear Command]** next to the corresponding device.
- Confirm the operation by clicking **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved

Note:

After clearing commands, execute the **Synchronize All Data to Devices** operation to re-synchronize software data with the device.

This operation cannot be performed if the device's **user capacity** and **fingerprint capacity** are fully utilized. If capacity is insufficient:

- Replace the current device with a higher-capacity model.
- Remove access rights for some personnel assigned to the device.
- Reattempt the synchronization.

Additional Information

1. **Operate State**
    - Displays the current communication status of the device, which is primarily used for debugging.
2. **Pending Commands**
    - If the **number of commands to be executed** is greater than 0, it indicates that data has not yet been synchronized to the device.
    - Wait for synchronization to complete before proceeding.

Export Functionality

Prerequisites for Use

The **Device Monitoring** interface must contain data to export.

Usage Scenarios

Export monitoring data for further processing, analysis, or record-keeping on a local system.

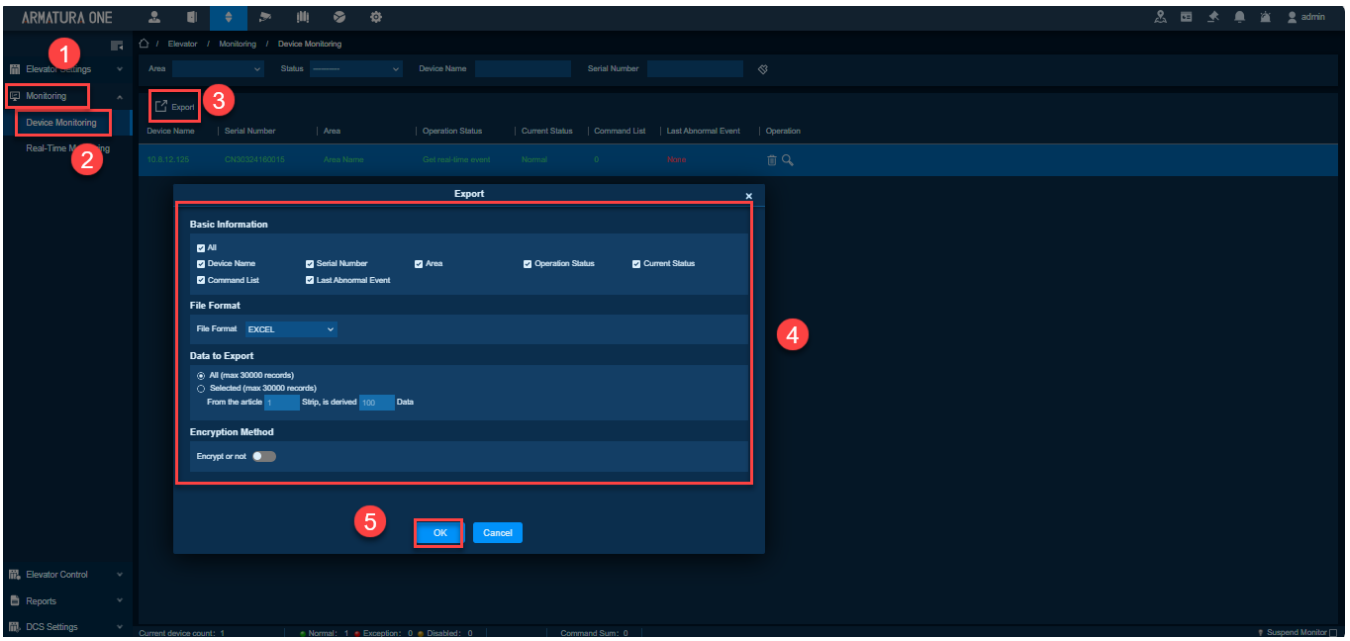
Triggered Result

Generates a file (Excel, PDF, or CSV) containing the exported data.

Steps:

- Navigate to **[Monitoring] > [Device Monitoring]**.
- Click the **[Export]** button.
- Choose the desired export format (Excel, PDF, or CSV).
- Save the file to a specified location on your local computer.

Copyright © 2024 ARMATURA LLC. All rights reserved

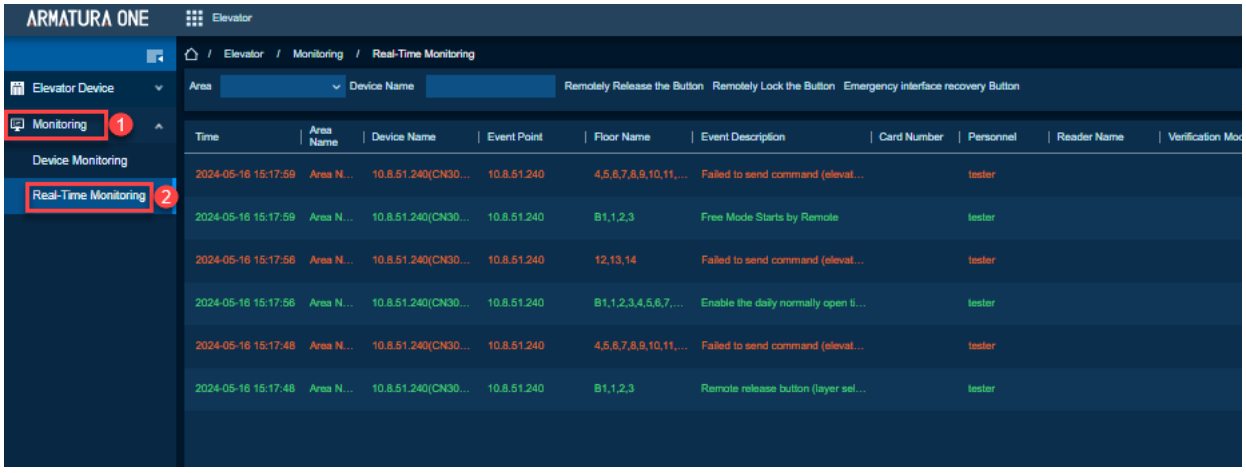


8.2.2 Real-Time Monitoring

Function Description

The **Real-Time Monitoring** feature allows users to monitor the live status and events of elevator controllers. This includes details such as **Time**, **Area**, **Event Point**, **Floor**, **Card Number**, **Personnel**, **Reader**, and **Verification Mode**.

To access this feature, navigate to **[Monitoring] > [Real-Time Monitoring]**. The Real-Time Monitoring interface provides a comprehensive view of elevator controller activity.



Copyright © 2024 ARMATURA LLC. All rights reserved

Event Monitoring

System Behavior

- The system automatically retrieves and displays **up to 200 event records** by default, including both normal and abnormal elevator events.
- **Event Color Coding**:
  - **Green**: Normal events.
  - **Red**: Alarm events.
  - **Orange**: Other abnormal events.
- **Filter Options**

Users can refine the monitoring focus by specifying:

- **Area**
- **Status**
- **Device Name**
- **Serial Number**
- **Photo Display**
- If a monitored event involves a person, the system displays the individual's photo.
- If no photo is registered, a default image is shown.
- The interface also displays the **event name**, **time**, and **personnel name**.

Remotely Release the Button

Allows the selected floor's button to be temporarily unlocked for operation.

Steps:

- Click **[Remotely Release Button]**.
- Select the desired floor.
- Set the release duration (default: **15 seconds**) or choose **Enable Intraday Passage Mode Time Zone** for extended access.
- Click **[Start]** to apply the operation.

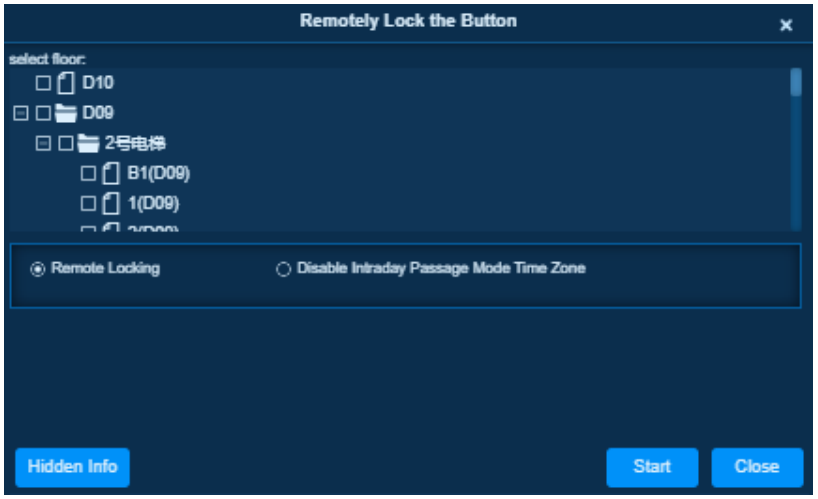
Copyright © 2024 ARMATURA LLC. All rights reserved

Remotely Lock the Button

Locks the button for a specific floor, preventing further use until unlocked.

Steps:

- Click **[Remotely Lock Button]**.
- Select the target floor.
- Click **[Start]** to apply the lock.



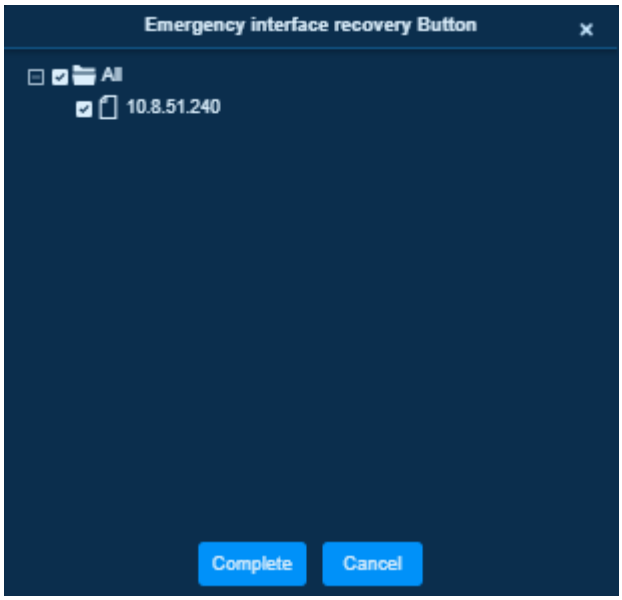
Emergency Interface Recovery Button

Allows resetting the device to its default operational state during emergencies.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Click **[Emergency Interface Recovery Button]**.
- Select the corresponding emergency number.
- Click **[Complete]** to finalize recovery.



The fields are as follows:

Remote Release:

Purpose: Temporarily unlock the button for a specific floor.

Customization:

- Set a release duration (default: **15 seconds**).
- Enable **Intraday Passage Mode Time Zone** to allow unrestricted access during specified times.
- Configure continuous release for unrestricted 24/7 access, bypassing restrictions like:
  - **Floor Active Time Zone**
  - **Floor Passage Mode Time Zone**
  - **Button Open Duration**

Normally Release Button: Set the floor button to continuous release, allowing unrestricted operation. Select **Disable Intraday Passage Mode Time Zone** to deactivate continuous release to disable.

Emergency Interface Recovery Button: Access recovery mode by holding the reset button while powering up the device.

Copyright © 2024 ARMATURA LLC. All rights reserved

Note:

If repeated failure messages occur during remote release operations, check for disconnected devices in the device list. Verify network connections and resolve any communication issues.

8.3 Elevator Control

The Elevator Control module allows configuration and management of elevator access, including time zones, holidays, levels, and permissions for personnel or organizations. Each function is designed to ensure smooth, secure, and customizable elevator operations.

Function List

Functions	Description
Time Zones	Define elevator floor access by time intervals.
Holidays	Manage holiday-specific elevator access rules.
Elevator Levesls	Configure, edit, delete, and bind elevator levels to syste floor operations.
Set Access by Lev	Manage access rights for specific elevator levels.
Set Access by Person	Assign or revoke elevator access for individual personn
Set Access by Organization	Assign elevator access permissions to personnel by organization.
Default floor	Set the default floor for the elevator.
Global Linkages	Define event-triggered operations within the elevator system.
Parameters	Set methods for obtaining elevator event records and configure real-time photo display sizes.

8.3.1 Time Zones

Function Description

Time zones define specific time intervals when users can access elevator floors. Permissions outside these intervals are restricted.

Add Timetable

Prerequisites for Use

Time zones must be added for elevator control.

Usage Scenarios

Create custom elevator control schedules for floors.

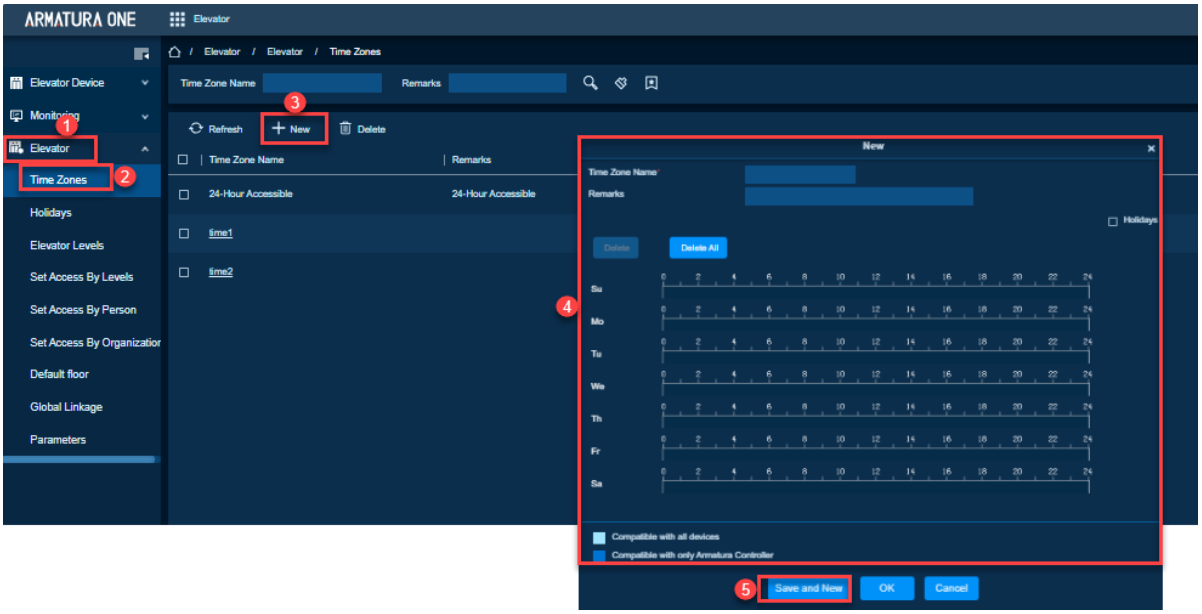
Copyright © 2024 ARMATURA LLC. All rights reserved

Triggered Result

New time zone data is added to the system.

Steps:

- Navigate to **[Elevator Control] > [Time Zones] > [New]** to access the time zone setting interface.



Parameters:

Time Zone Name: Enter up to 30 characters.

Remarks: Provide a detailed description (up to 50 characters) of the time zone and its applications.

Interval and Start/End Time: Define up to 3 intervals per day and for holidays. Ensure intervals do not overlap or extend across days.

Setting: If the interval is Normal Open, just enter 00:00-23:59 as interval 1, and 00:00-00:00 as the interval 2/3. If the interval is Normal Close: All are 00:00-00:00. If only using one interval, user just needs to fill out the interval 1, and the interval 2/3 will use the default value. Similarly, when only using the first two intervals, the third interval will use the default value. When using two or three intervals, user needs to ensure two or three intervals have no time intersection, and the time shall cross over to 2nd day, or the system will prompt error.

Holiday Type: Set specific holiday intervals. Optional—default values will apply if not specified.

Copy on Monday: Quickly copy Monday's settings to other days of the week.

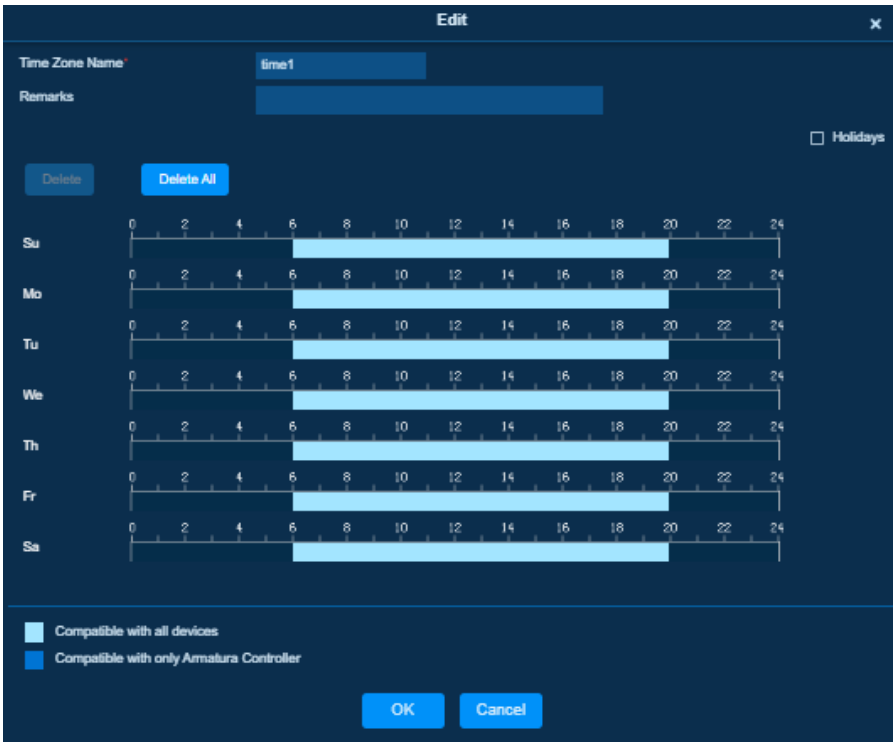
After filling in all required fields, click **[OK]** to save. The time zone will appear in the list.

Maintenance of Elevator Time Zones

Edit Timetable

Copyright © 2024 ARMATURA LLC. All rights reserved

- Click the **[Edit]** button in the operations column to modify time zone details. After editing, click **[OK]** to save the changes.



Delete Timetable

Prerequisites for Use

Ensure the selected time zone is not in active use.

Usage Scenarios

Delete time zones that are obsolete or no longer required.

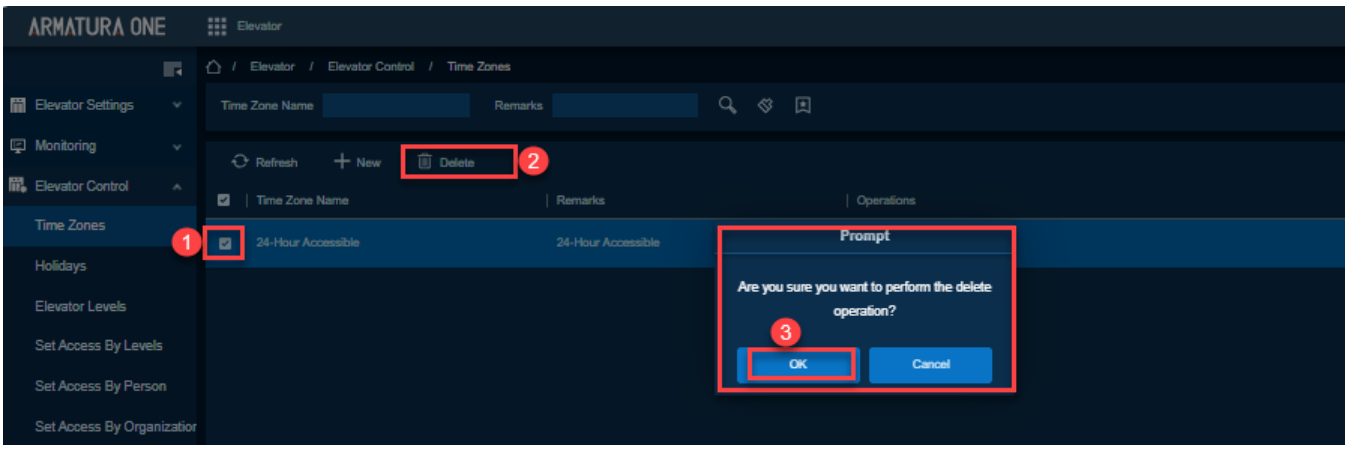
Triggered Result

Deletes the selected time zone data.

Steps:

- Select the desired time zone and click **[Delete]**.
- Confirm by clicking **[OK]**. If a time zone is in use, it cannot be deleted.

Copyright © 2024 ARMATURA LLC. All rights reserved



Note:

You can also select multiple time zones by ticking their checkboxes and clicking **[Delete]** above the list.

8.3.2 Holidays

Function Description

The **Holidays** module provides configuration for elevator access control during holidays, which may differ from regular weekdays. This ensures that holiday-specific schedules are managed effectively. The system supports adding, editing, and deleting holiday records.

Add Holidays

Prerequisites for Use

Ensure the system allows adding new holidays for configuration.

Usage Scenarios

To manage holiday-specific elevator access times and avoid scheduling conflicts.

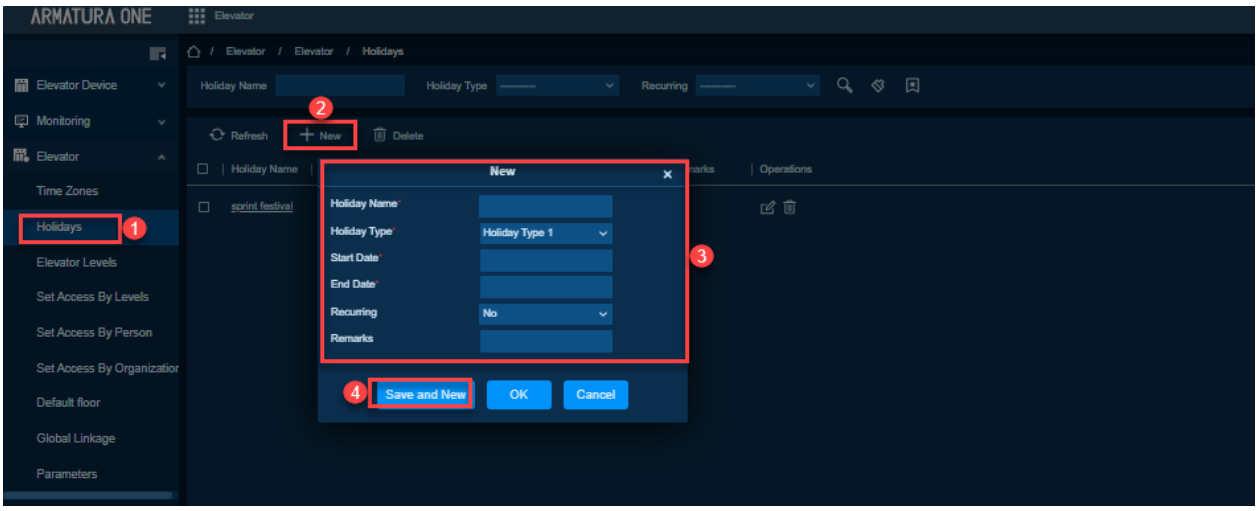
Triggered Result

Adds holiday data and links it to the relevant time settings for elevator control, which take effect on the specified holiday.

Steps:

- Click **[Elevator Control] > [Holidays] > [New]** to open the new holiday interface.

Copyright © 2024 ARMATURA LLC. All rights reserved



Fields are as following:

Holiday Name: Enter up to 30 characters.

Holiday Type: Choose from **Type 1**, **Type 2**, or **Type 3**. Each type can include up to 32 holidays.

Start/End Date: Enter the start and end dates in the format YYYY-MM-DD. The start date cannot be later than the end date. Holidays cannot span years.

Recurring: Specify if the holiday recurs annually. Select **Yes** for fixed-date holidays like January 1 (New Year's Day). Select **No** for variable dates like Mother's Day.

Remarks: Add descriptive notes about the holiday for future reference.

Example: For New Year's Day on January 1, 2010:

- Holiday Type: 1
- Start/End Date: January 1, 2010
- Recurring: Yes
- Remarks: "Applies to New Year's Day annually."

After completing the fields, click **[OK]** to save the new holiday.

Edit Holidays

Prerequisites for Use

Existing holiday data must be available for editing.

Usage Scenarios

Update holiday configurations to reflect changes in schedules or details.

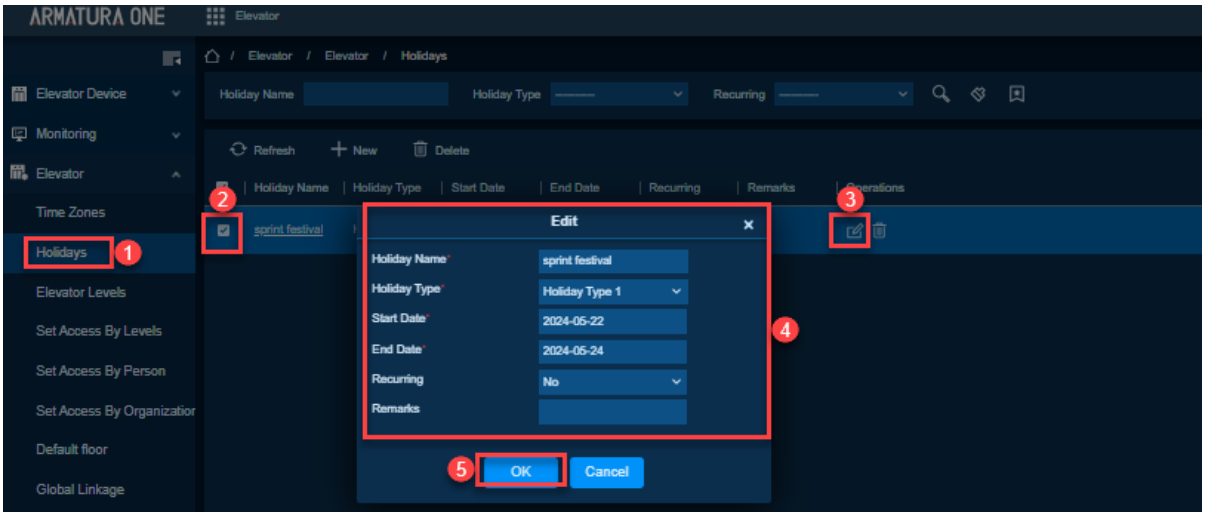
Triggered Result

The system applies the edited holiday data.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Select the desired holiday record and click the **[Edit]** button in the operations column.
- Modify the required fields in the holiday interface.
- Click **[OK]** to save the changes.



Delete Holidays

Prerequisites for Use

Existing holiday data must be selected.

A holiday in active use cannot be deleted.

Usage Scenarios

Remove holiday records that are no longer required.

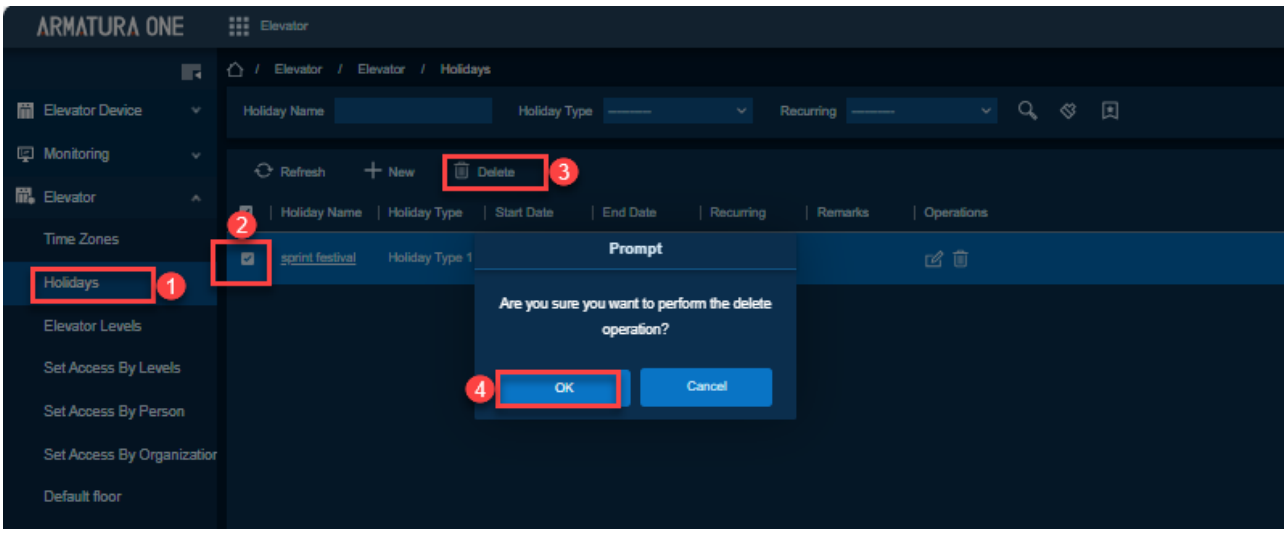
Triggered Result

Deletes the selected holiday record from the system.

Steps:

- In the **Access Control Holiday List**, select the holiday to be deleted.
- Click the **[Delete]** button in the operations column.
- Confirm the deletion by clicking **[OK]**. Click **[Cancel]** to abort the operation.

Copyright © 2024 ARMATURA LLC. All rights reserved



8.3.3 Elevator Levels

Function Description

Elevator levels define the floors or doors that can be accessed through the verification of a multi-person combination within a specified time zone. This combination is configured in the **Personnel Access Level** settings, ensuring secure and restricted access.

Add Permission Group

Prerequisites for Use

Time zones and data must be added beforehand.

Usage Scenarios

To configure authority groups for elevator control floors, ensuring precise access permissions.

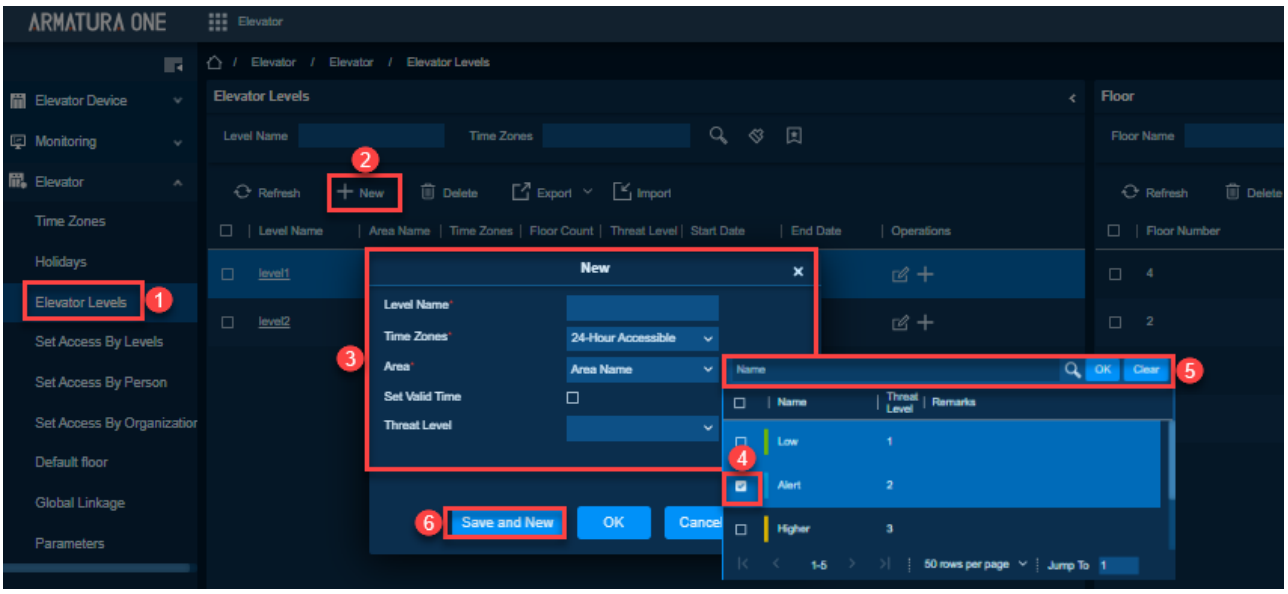
Triggered Result

Adds access level configurations that bind authorized floors to specific elevator levels.

Steps:

- Navigate to **[Elevator Control] > [Elevator Levels] > [New]** to open the **Add Levels** interface.

Copyright © 2024 ARMATURA LLC. All rights reserved

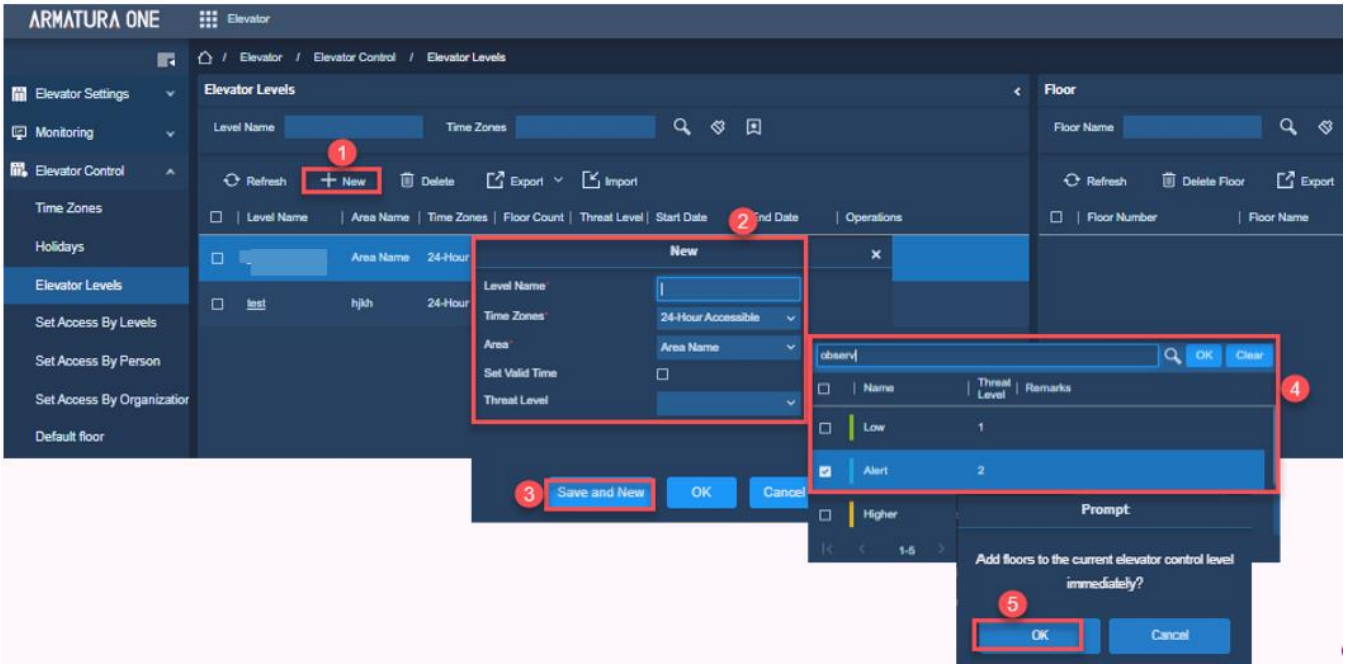


Parameter: Level Name (unrepeatable), Time Zone and Area.

- **Level Name:** Enter a unique name for the elevator level (up to 30 characters).
- Time Zones: Select the time zone applicable for the elevator level.
- Area: Specify the area to associate with the elevator level.
- Set Valid Time: Define the start and end date & time for the elevator level.
- Threat Level: Set the security threshold for each level to determine its operational importance or sensitivity.

Click **[OK],** a prompt will appear: **"Add floors to the current elevator control level immediately"**

Choose **[OK]** to add floors or **[Cancel]** to return to the elevator levels list.



Copyright © 2024 ARMATURA LLC. All rights reserved

Delete Permission Group

Prerequisites for Use

Identify the elevator levels to be deleted.

Usage Scenarios

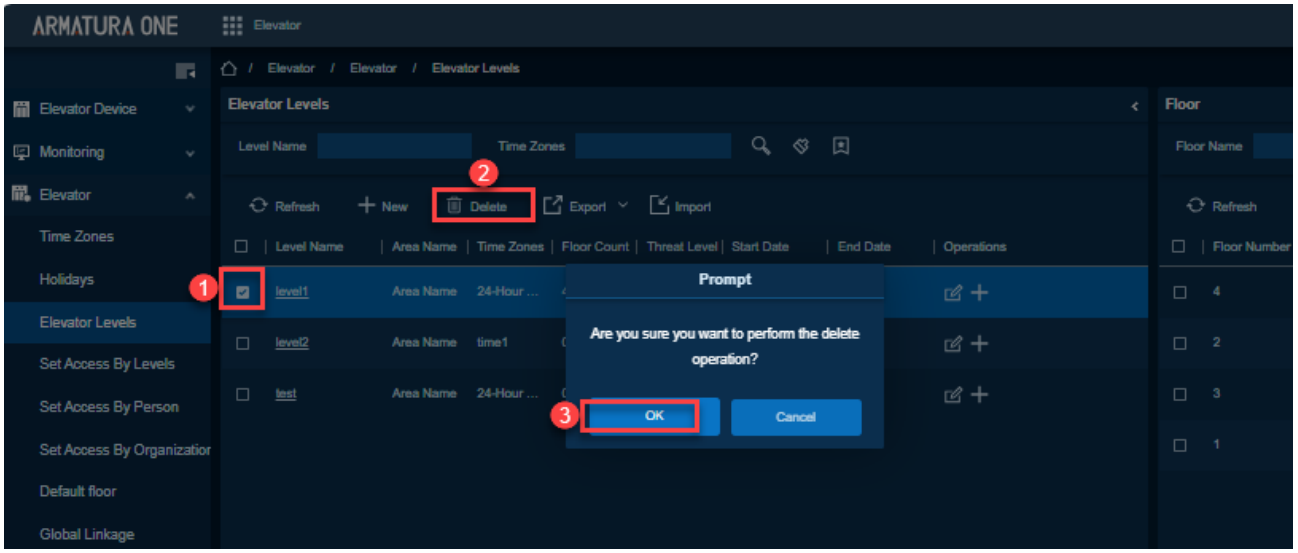
Remove elevator levels that are no longer in use.

Triggered Result

Deletes the selected elevator levels.

Steps:

- Select the relevant elevator level data.
- Click the **[Delete]** button.
- Confirm the deletion by clicking **[OK]** in the pop-up window.



Add Floor

Prerequisites for Use

Elevator levels must exist in the current system.

Usage Scenarios

Bind a specific floor to an elevator level to grant access.

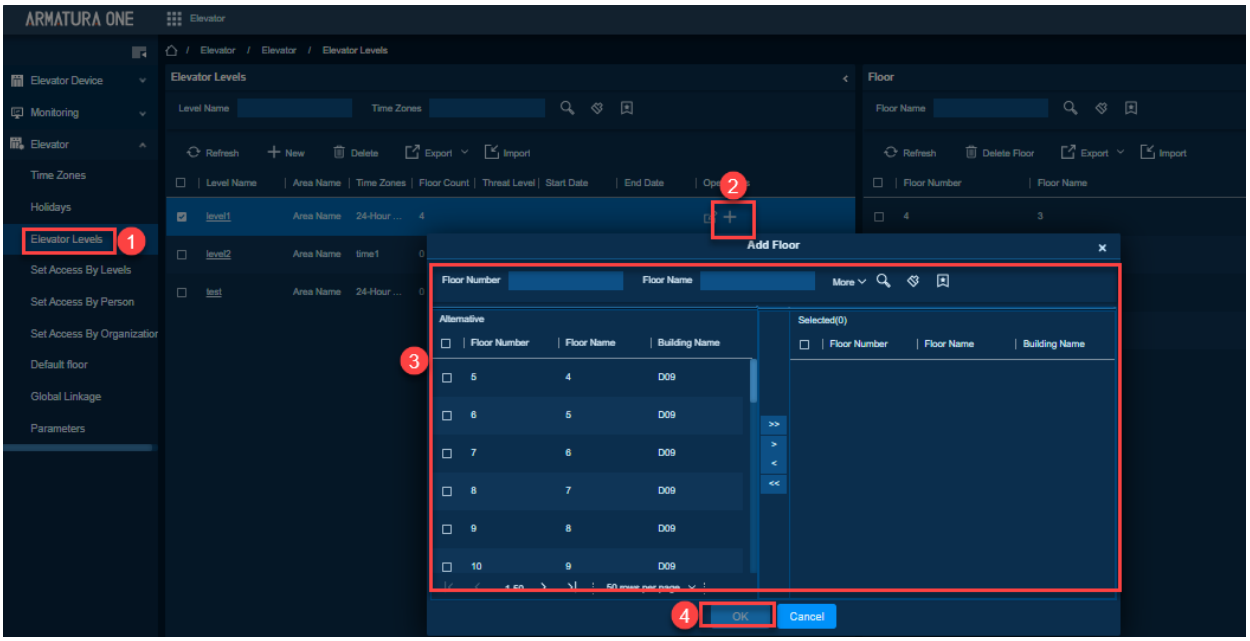
Triggered Result

Links elevator control floors with the selected elevator level.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Go to **[Elevator Control]** > **[Elevator Levels]** and select an elevator level from the left list.
  - The personnel with access to this level will appear on the right list.
- In the left list, click **[Add Personnel]** to open the Add Personnel window.
- Select multiple personnel and move them to the right list using the arrow icon.
- Click **[OK]** to save and complete the process.



Delete Floor

Prerequisites for Use

The elevator level must already have floor data added.

Usage Scenarios

Remove a floor from the associated elevator level.

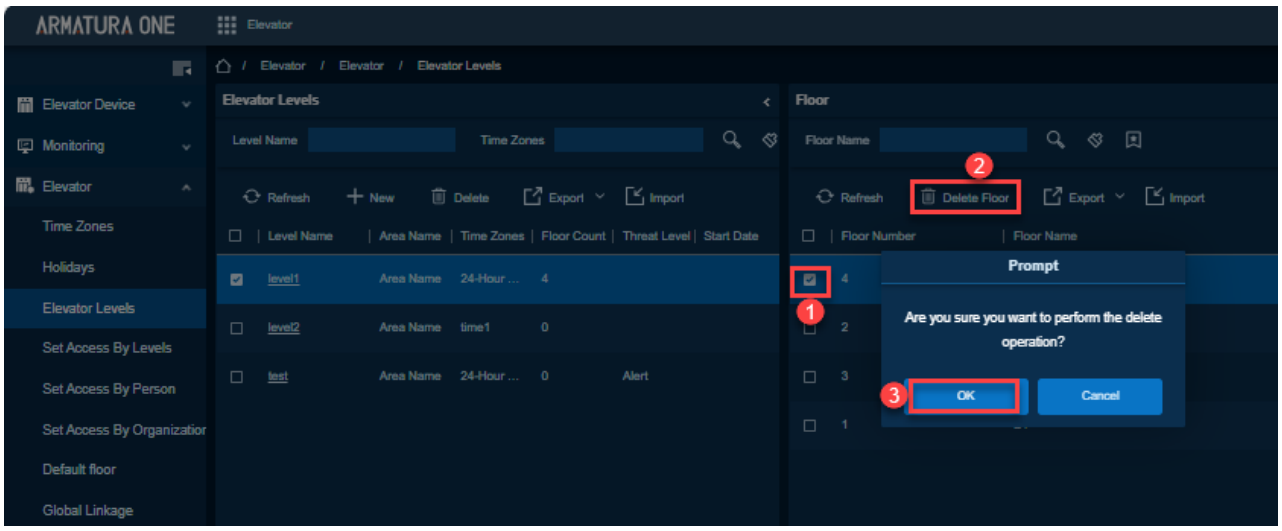
Triggered Result

Releases the binding relationship between the elevator level and its floors.

Steps:

- Select the elevator level to view the associated personnel in the right list.
- Select the personnel to remove and click **[Delete Personnel]** above the right list.
- Confirm the deletion by clicking **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export Elevator Data

Prerequisites for Use

The system must contain elevator control event records.

Usage Scenarios

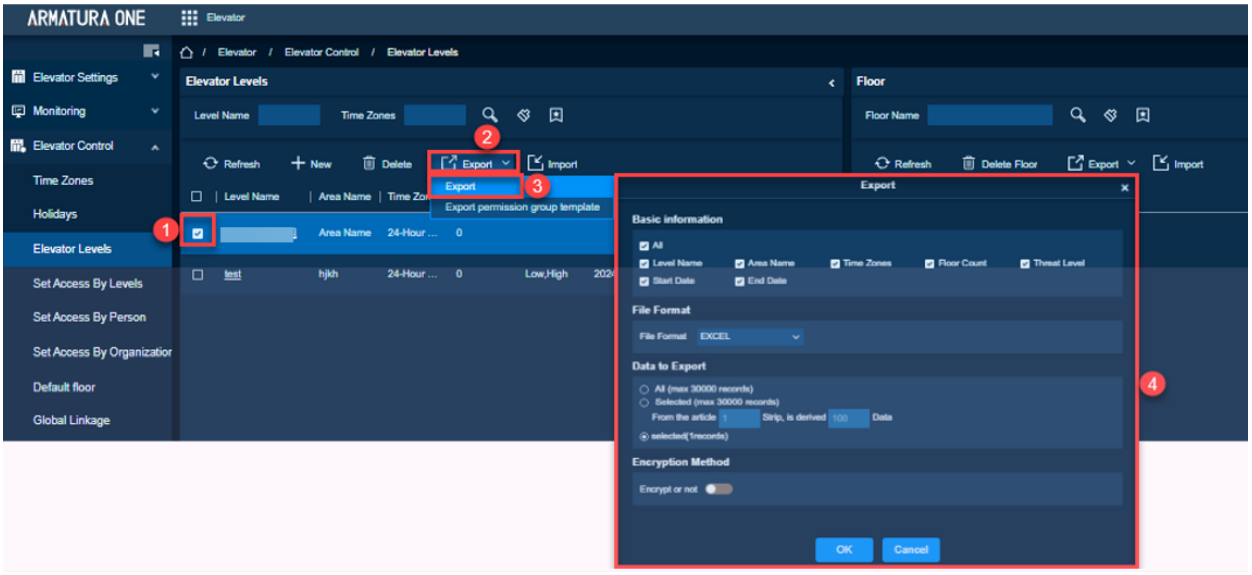
Export elevator control data for analysis or record-keeping.

Triggered Result

Generates a file containing the exported data.

Steps:

- Select **[Export]** to generate files in Excel, PDF, or CSV format.



Copyright © 2024 ARMATURA LLC. All rights reserved

Export permission group template

Prerequisites for Use

Elevator control event records must be available in the system.

Usage Scenarios

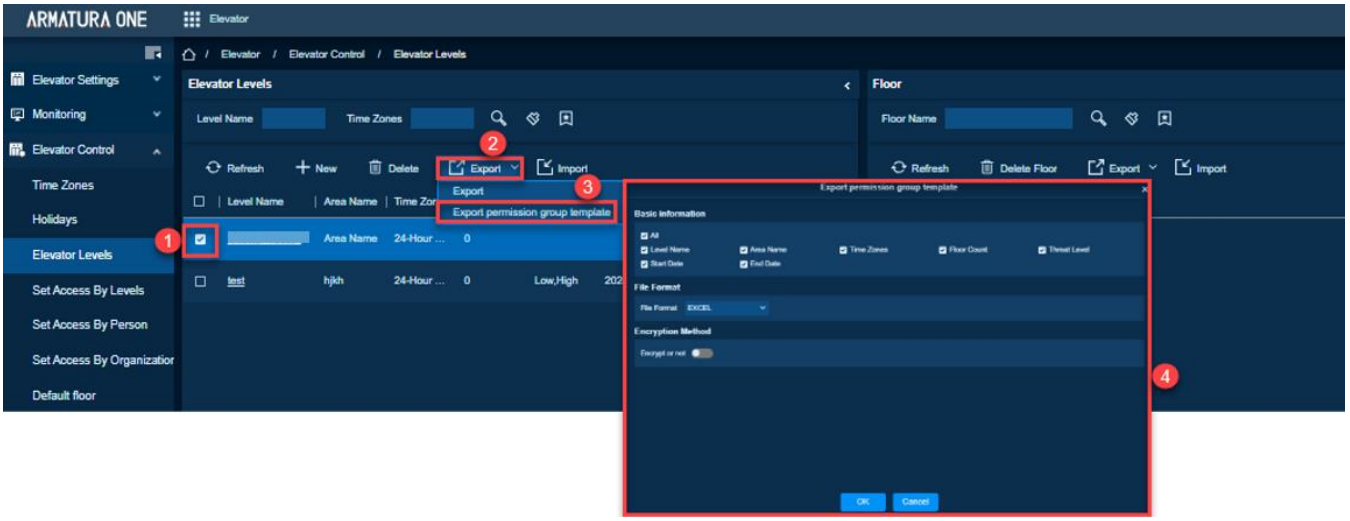
Export the permission group template for record-keeping or modifications.

Triggered Result

Produces an exported file in the chosen format.

Steps:

- User can export all elevator permission group template in Excel, PDF, CSV format.



Note:

Exporting floor data works the same way as exporting elevator details.

Import Elevator Data

Prerequisites for Use

Elevator control event records must exist in the system.

Usage Scenarios

Upload elevator-related data for analysis or integration.

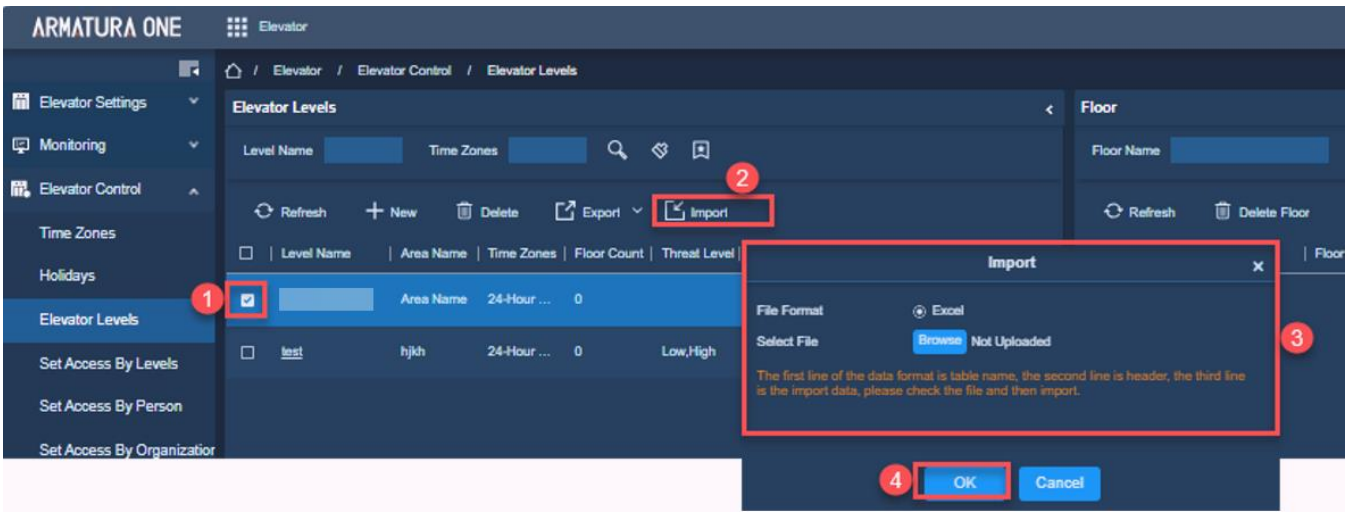
Triggered Result

Imports elevator control data from an Excel file into the system.

Steps:

- Use the **[Import]** button to upload an Excel file containing elevator control data.

Copyright © 2024 ARMATURA LLC. All rights reserved



Note:

Importing floor data works the same way as importing elevator details.

8.3.4 Set Access By Levels

Function Description

This feature allows the addition of selected personnel to elevator levels or the removal of personnel from specific elevator levels, granting or restricting their access to certain floors.

Add Personnel

Prerequisites for Use

The system must have the corresponding elevator levels added.

Usage Scenarios

To configure appropriate elevator control permissions for personnel, enabling them to operate the elevator and access specific floors.

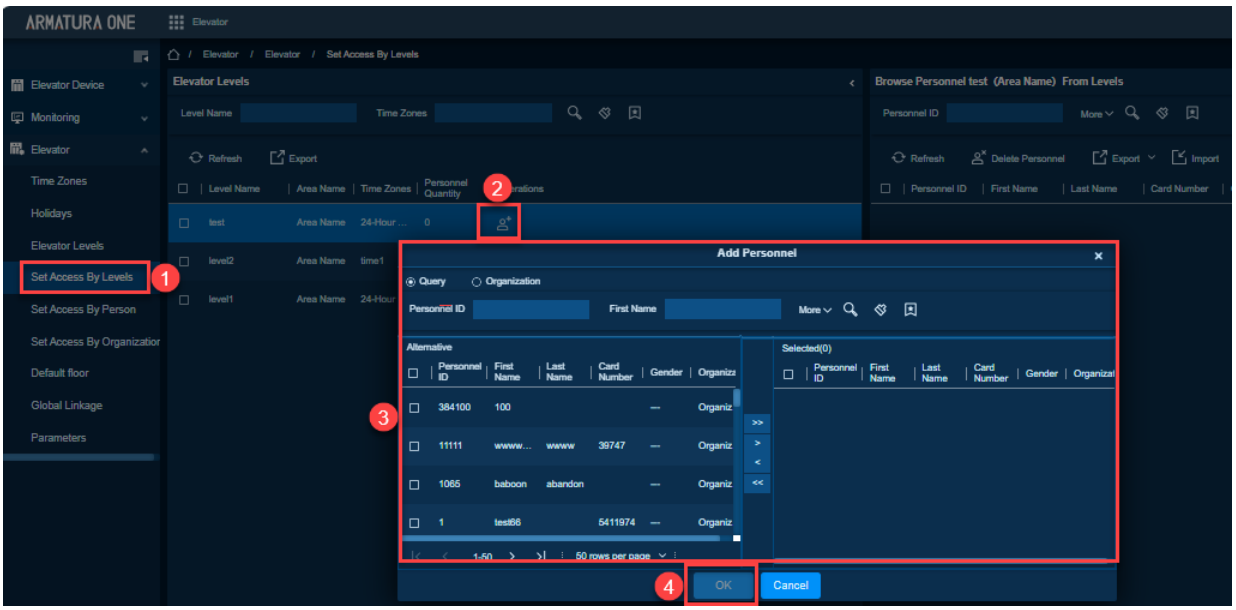
Triggered Result

Personnel are granted the authority of the selected elevator level, allowing them to access specified floors via the elevator.

Steps:

- Navigate to **[Elevator Control] > [Set Access By Levels] > [Add Personnel]**.
- Click an employee to view the levels they are associated with in the right list.
- Click **[Add Personnel]** under operations to open the **Add to Levels** window.
- Select one or more levels and move them to the selected list using the arrow.
- Click **[OK]** to save and complete the configuration.

Copyright © 2024 ARMATURA LLC. All rights reserved



The fields are as follows:

Personnel ID: Enter the unique ID of the personnel.

First Name: Enter the person's first name.

Last Name: Enter the person's last name.

Card Number: Enter the personnel's card number.

Organization Name: Specify the name of the organization.

Gender: Select the gender of the personnel.

Export Personnel Data

Prerequisites for Use

The current system must contain elevator control event records.

Usage Scenarios

Export data for analysis, record-keeping, or processing on a local computer.

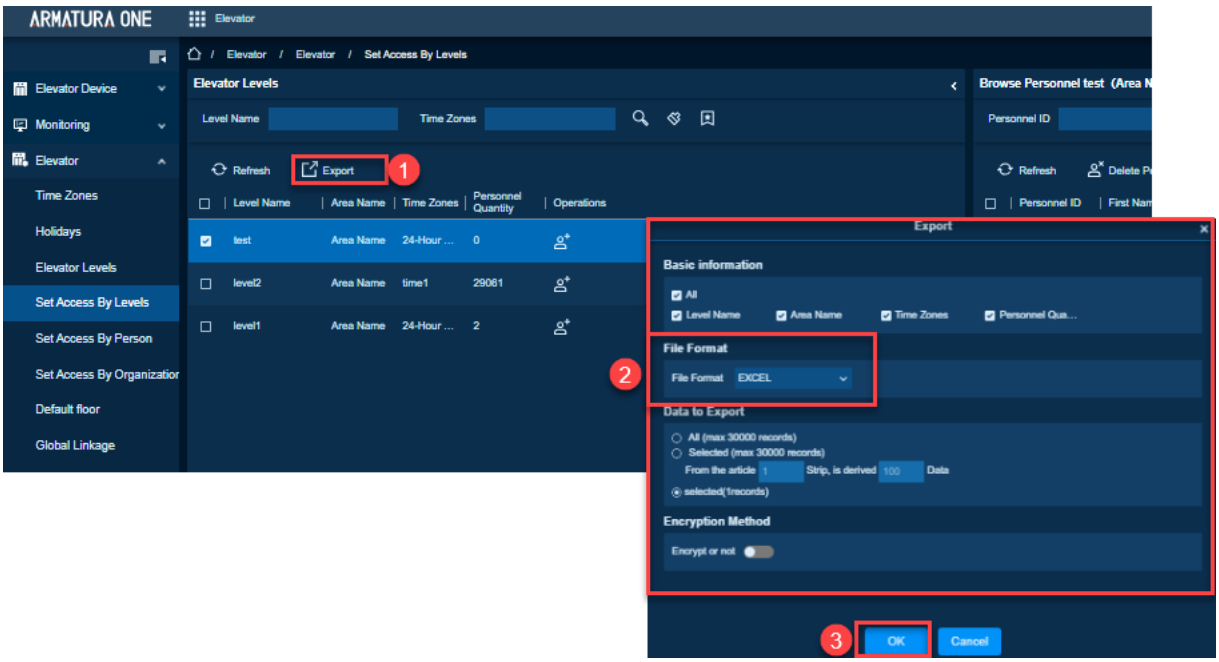
Triggered Result

An Excel, PDF, or CSV file is generated containing the exported data.

Steps:

- Select **[Export]** and choose the desired format (Excel, PDF, or CSV).
- Follow the prompts to complete the export process.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Personnel

Prerequisites for Use

Personnel must be associated with an elevator level.

Usage Scenarios

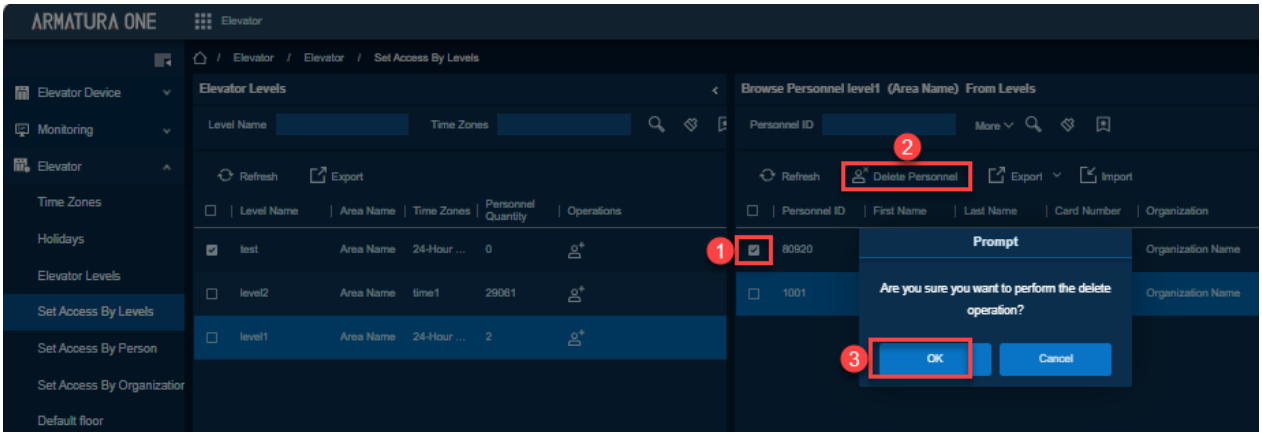
Remove elevator level permissions from personnel to restrict their access.

Triggered Result

Personnel lose access to the elevator levels, preventing them from reaching corresponding floors.

Steps:

- Select one or more levels from the right list.
- Click **[Delete from Levels]** above the list.
- Confirm the deletion by clicking **[OK]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

Export Levels

Export

Prerequisites for Use

The system must contain elevator level data.

Usage Scenarios

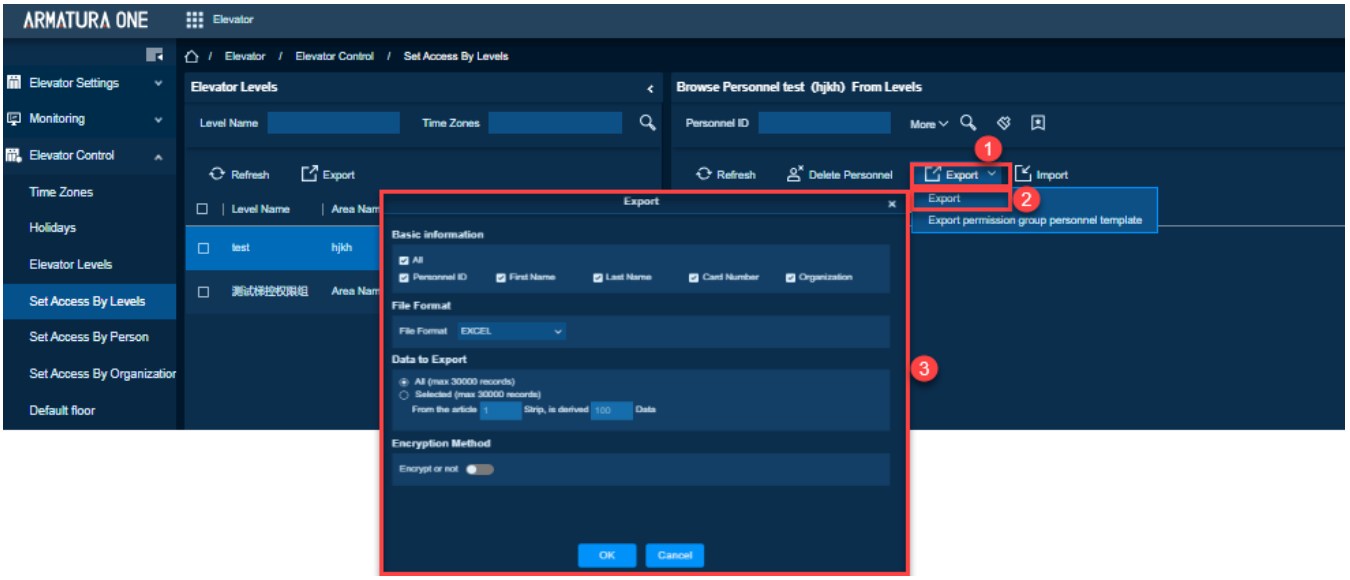
Export elevator level data for local processing or record-keeping.

Triggered Result

Generates an Excel, PDF, or CSV file with exported level data.

Steps:

- Navigate to **[Export]** and choose the desired format.
- Follow the prompts to complete the export process.



Export permission group personnel template

Prerequisites for Use

The system must contain elevator control event records.

Usage Scenarios

Export a permission group personnel template for record-keeping or modifications.

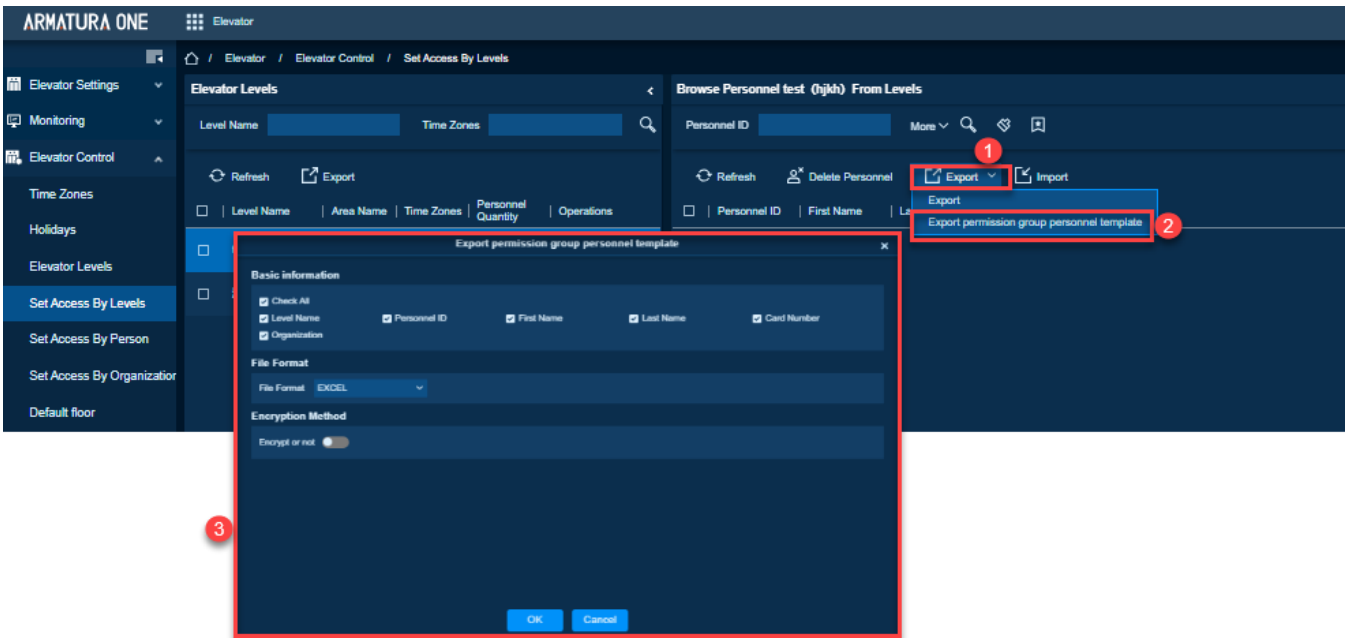
Triggered Result

Generates an Excel file containing the template data.

Steps:

- Select **[Export Permission Group Personnel Template]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Import Levels

Prerequisites for Use

The system must contain elevator level records.

Usage Scenarios

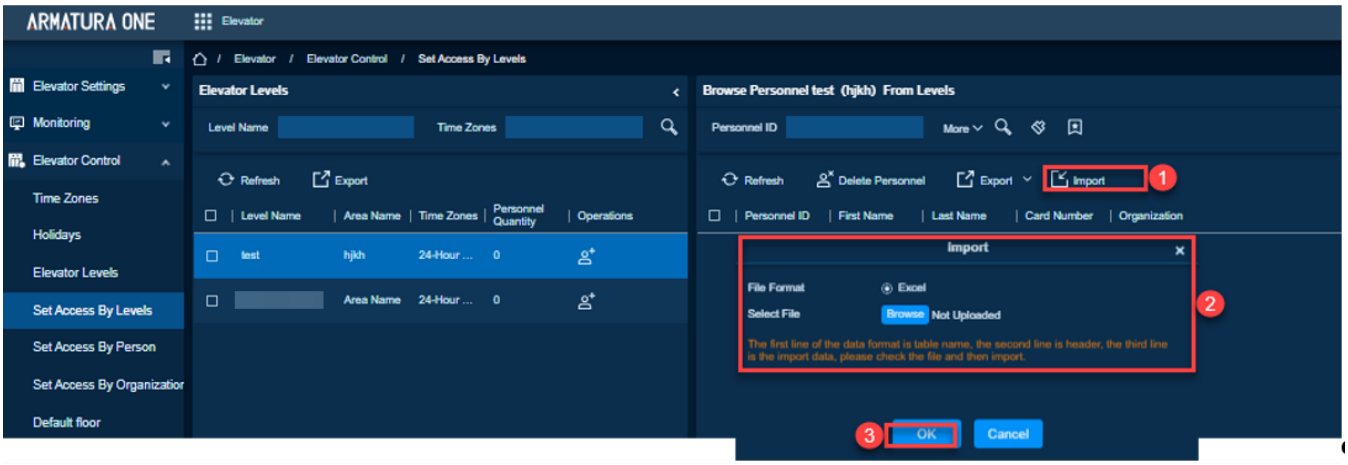
Upload level data for processing or analysis.

Triggered Result

The system processes and integrates the uploaded level data.

Steps:

- Select **[Import]** to upload an Excel file containing level data.



Copyright © 2024 ARMATURA LLC. All rights reserved

8.3.5 Set Access By Person

Function Description

This feature allows assigning or revoking elevator access permissions for individuals. Users can configure authority groups for personnel, assign super administrator rights, or manage elevator level access for specific individuals.

Elevator Control Settings

Prerequisites for Use

Personnel must be selected for the operation.

Usage Scenarios

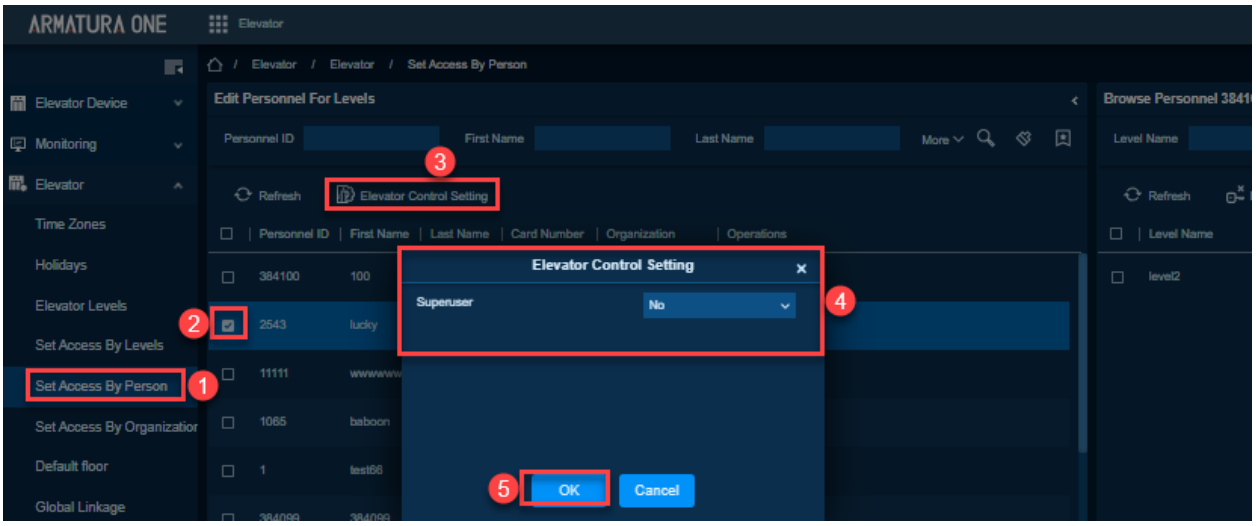
Assign super administrator authority to an individual. Set effective access times for an individual.

Triggered Result

The selected individual is granted super administrator authority or has their effective access times configured.

Steps:

- Select a person from the list on the left.
- Click **[Elevator Control Setting]** to open the configuration page.
- Configure the elevator control parameters as required and click **[OK]** to save.



Parameters:

Superuser: Select **Yes** or **No** to assign superuser rights.

Add Permission Group

Prerequisites for Use

Personnel to be assigned permissions must be selected.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

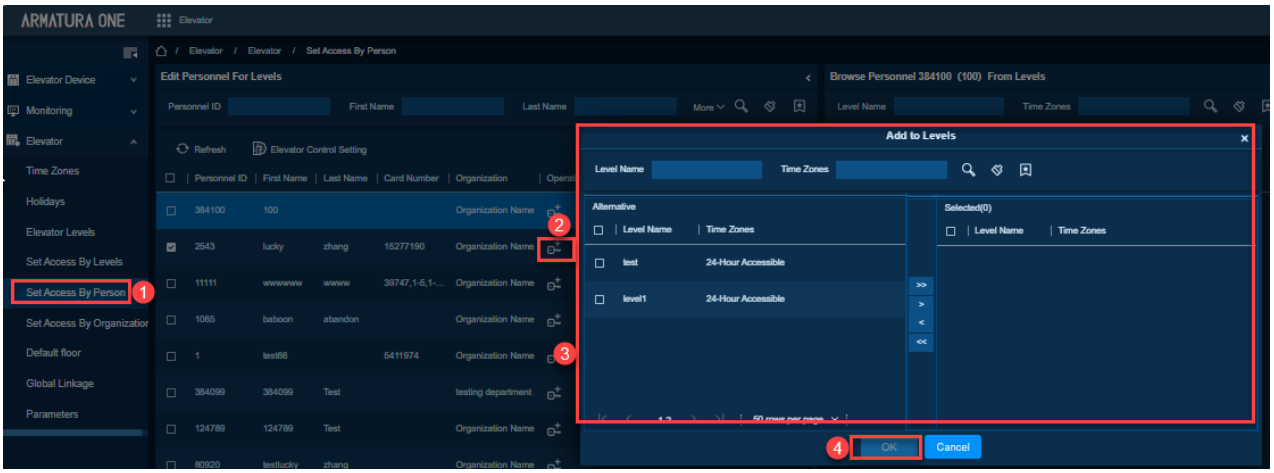
Add authority group configurations to personnel, granting them access to elevator levels within the group.

Triggered Result

Establish a binding relationship between the individual and the selected elevator levels.

Steps:

- Click **[Add Permission Group]**.
- In the pop-up window, select the appropriate elevator levels.
- Click **[OK]** to save the changes.



Delete Permission Group

Prerequisites for Use

Personnel must already be bound to elevator levels.

Usage Scenarios

Revoke access to elevator levels for personnel by removing them from the associated authority group.

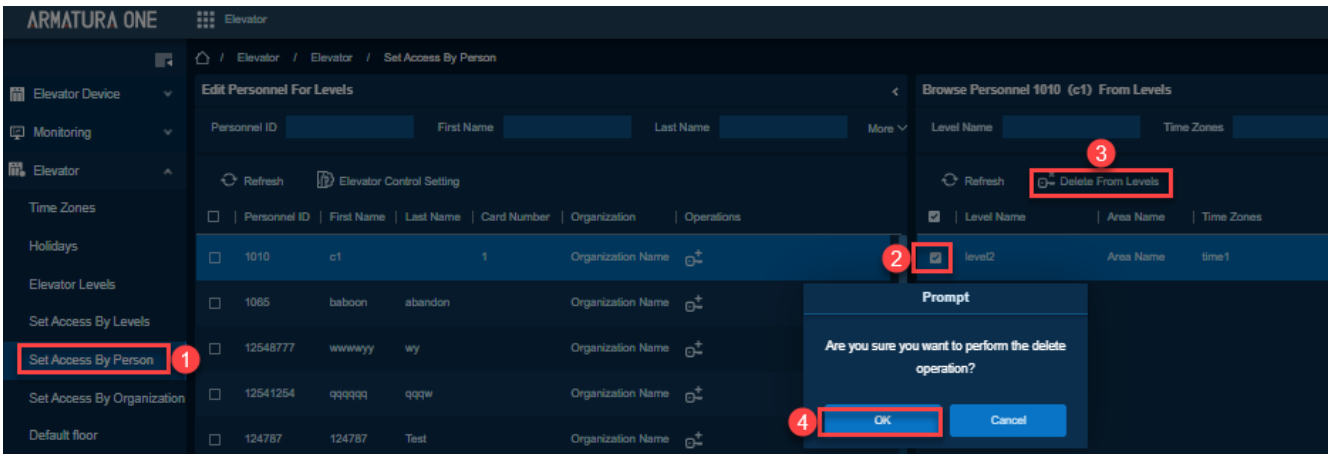
Triggered Result

Remove the binding relationship between the individual and the elevator levels, revoking their access.

Steps:

- Select the corresponding authority group from the personnel list.
- Click **[Delete]** to remove the individual from the group.
- Confirm the deletion in the pop-up window by clicking **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



8.3.6 Set Access By Organization

Function Description

This feature allows assigning or revoking elevator level permissions for an entire organization or department. Users can configure access levels for all personnel in a department or remove access as necessary.

Add Default Levels

Prerequisites for Use

No specific prerequisites.

Usage Scenarios

Assign elevator level permissions to all personnel within the selected organization or department.

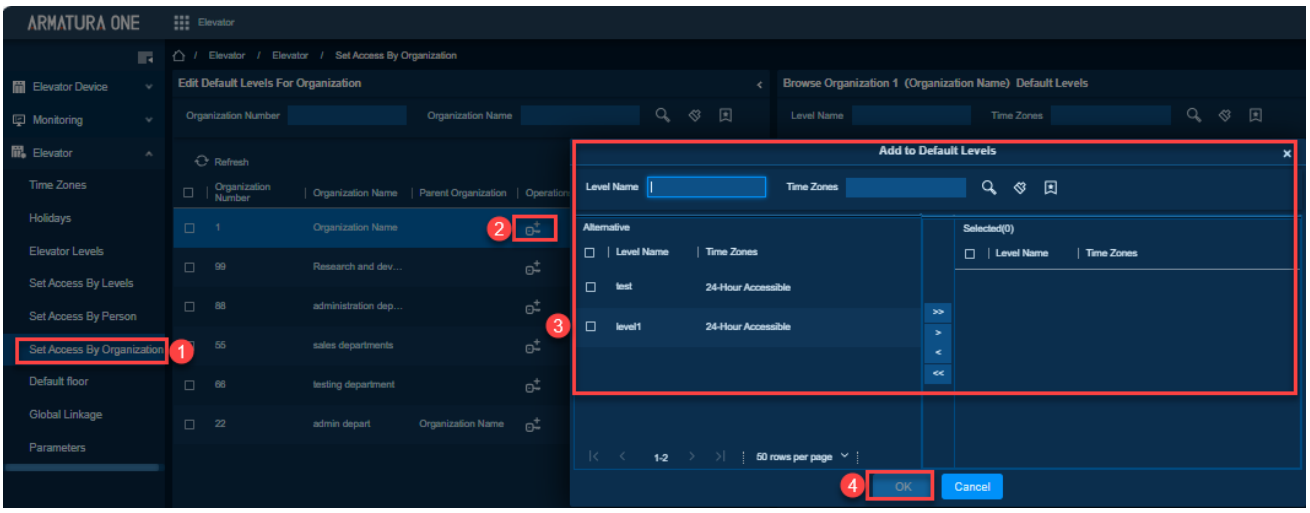
Triggered Result

All members of the department gain access to the designated elevator levels.

Steps:

- Click **[Add Default Levels]**.
- In the pop-up window, select the relevant elevator levels.
- Click **[OK]** to confirm and save the settings.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Default Permission Group

Prerequisites for Use

The organization must have previously been assigned elevator levels.

Usage Scenarios

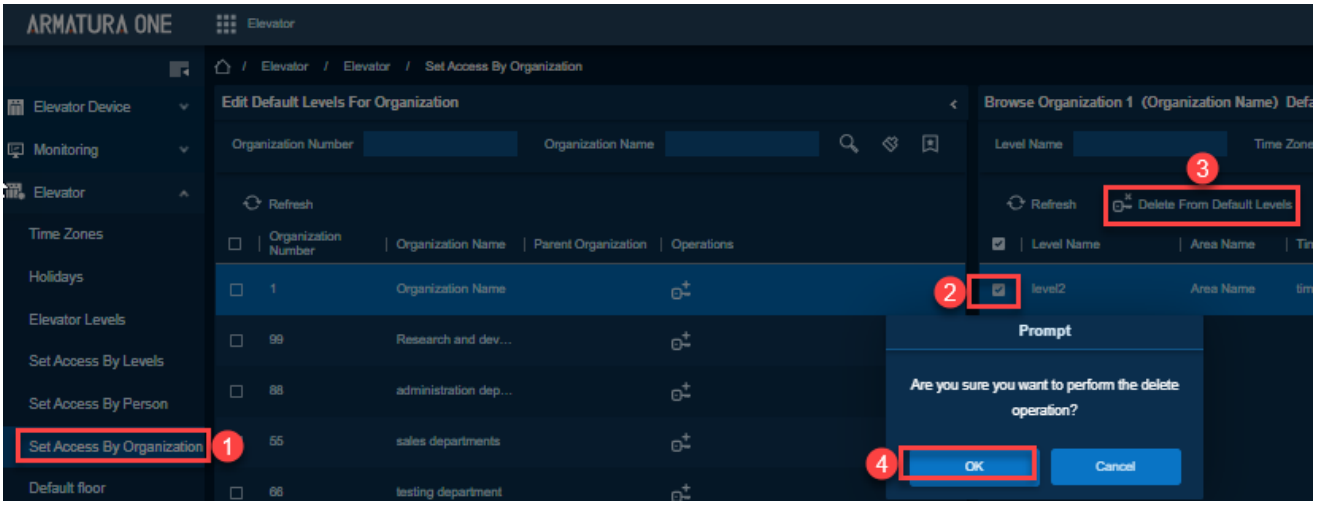
Revoke elevator level permissions for all personnel within the organization.

Triggered Result

All personnel in the department lose access to the elevator levels associated with the deleted permissions.

Steps:

- Select the permission group to delete.
- Click the **[Delete]** button.
- In the confirmation window, click **[OK]** to finalize the removal.



Copyright © 2024 ARMATURA LLC. All rights reserved

8.3.7 Default Floor

Function Description

The **Default Floor** functionality allows users to assign a default floor to an elevator control device. This setting can trigger corresponding system events such as video linkage, email notifications, and other configured responses.

Add default Floor

Prerequisites for Use

Select the appropriate floor for the elevator.

Usage Scenarios

The elevator control system triggers events or responses such as:

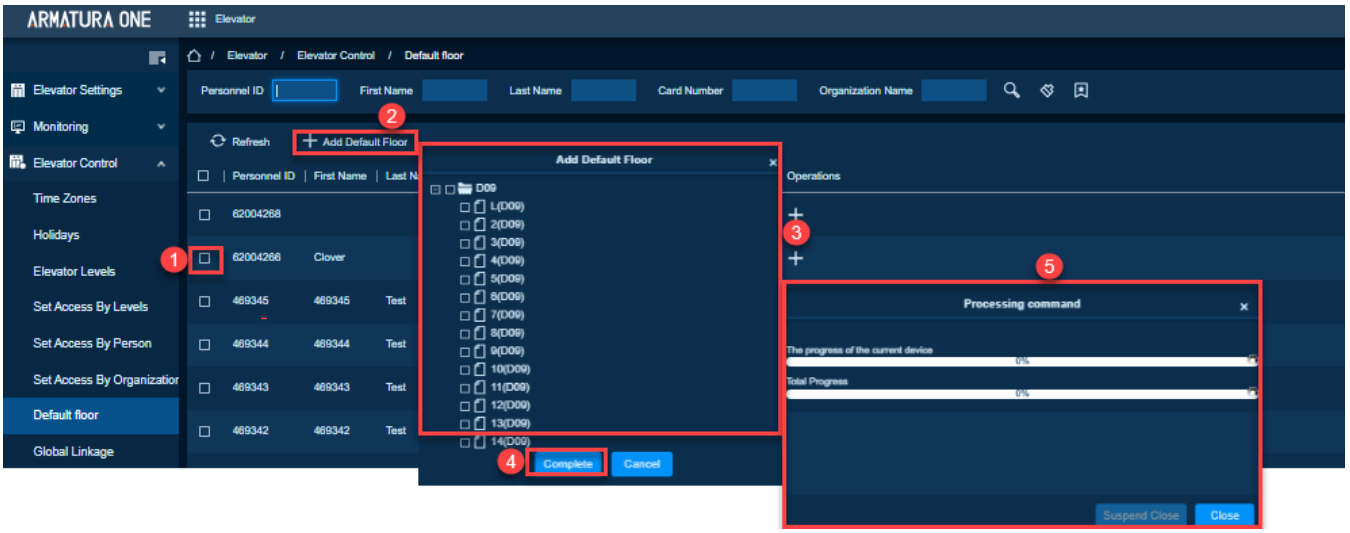
- Binding a camera to capture snapshots or initiate a pop-up video.
- Sending emails or notifications with relevant information.
- Executing other configuration-based actions tied to the default floor.

Triggered Result

The system assigns a default floor to the elevator, enabling configured responses.

Steps:

- Navigate to **[Elevator Control]** > **[Default Floor]** > **[New]**.
- In the pop-up interface, configure the necessary parameters for the default floor.
- Click **[OK]** to save the settings.



Copyright © 2024 ARMATURA LLC. All rights reserved

8.3.8 Global Linkages

Function Description

The **Global Linkage** feature enables users to configure system-wide data connections across elevator control devices. This includes setting up event-triggered actions, video monitoring integrations, email alerts, and other custom configurations.

Add

Prerequisites for Use

An elevator control device must be added to the system.

The device must have defined event types.

Usage Scenarios

The elevator control device triggers system events for linkage processing.

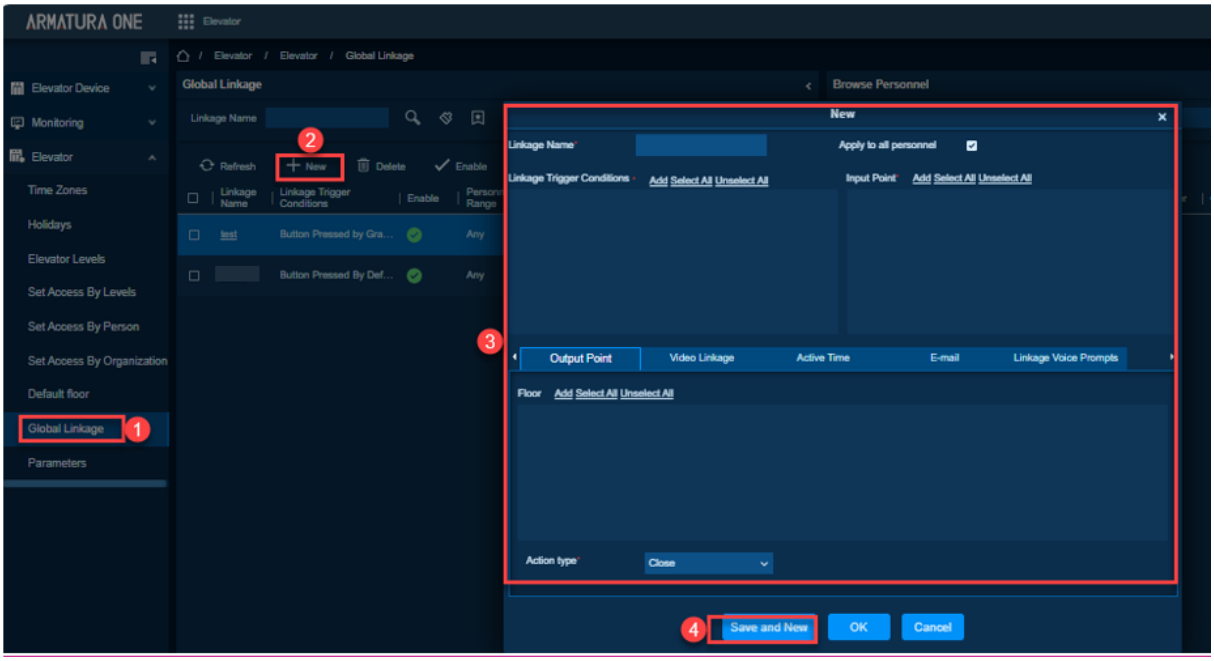
Configurations may include binding cameras for snapshots, pop-up video previews, email notifications, and more.

Triggered Result

Adds a new linkage configuration to the system.

Steps:

- Navigate to **[Elevator] > [Elevator Control] > [Global Linkages] > [New]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

- **Fields:**

Linkage Name: Assign a name to the linkage configuration.

Linkage Trigger Condition: Set the event type that triggers the linkage (e.g., Device Start, Enable/Disable Auxiliary Output).

Input Point: Select an input point (e.g., Door 1, Auxiliary Input 1-12).

Output Point: Select an output point (e.g., Lock 1, Auxiliary Output 1-10).

Linkage Action: Set action type: Close, Open (with delay), or Normal Open.

Video Linkage: Configure video-related settings: pop-up previews, video recording, snapshot capture, and display time.

Delay: Specify delay duration (1-254 seconds) for actions triggered.

Active Time: Choose the time zone during which the linkage is active.

Start/End Date: Define the date range for the linkage.

Email Address: Input the email address to send notifications.

Linkage Voice Alarm: Set a voice alarm for the linkage event.

Note:

Input and output points cannot share the same settings.

Multiple trigger conditions can be defined for a single linkage configuration.

Logical linkage across devices is permitted.

Delete

Prerequisites for Use

Select existing linkage configuration data.

Usage Scenarios

Remove outdated or unused linkage configurations.

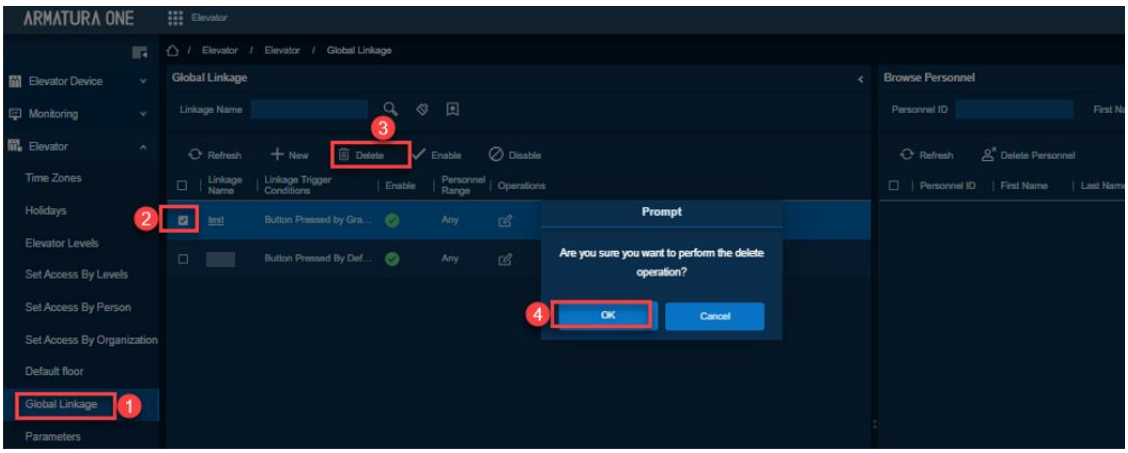
Triggered Result

Deletes the specified linkage configuration.

Steps:

- Select the linkage configuration to delete.
- Click **[Delete]**.
- On the confirmation window, click **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Enable

Prerequisites for Use

Select an added linkage configuration.

Usage Scenarios

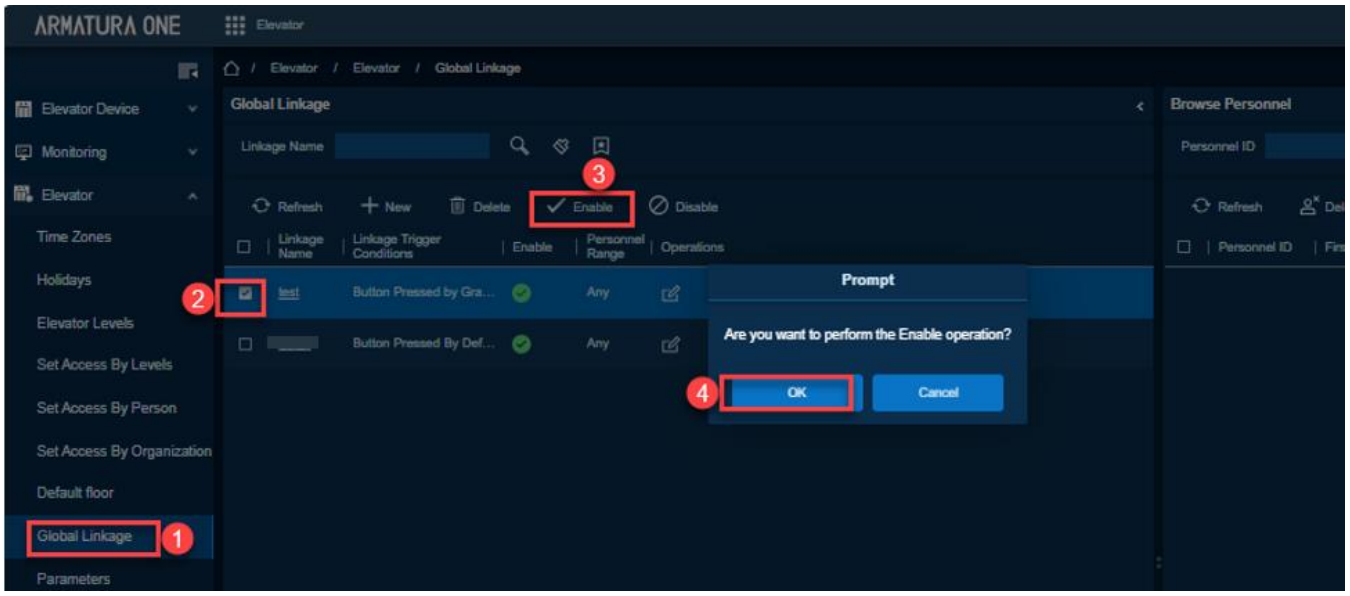
Activate linkage configurations to execute triggers.

Triggered Result

Executes linkage configurations, such as sending emails or triggering camera actions.

Steps:

- Select the linkage configuration.
- Click **[Enable]**.
- Confirm the operation in the pop-up window by clicking **[OK]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

Disable

Prerequisites for Use

Select the linkage configuration that has been added.

Usage Scenarios

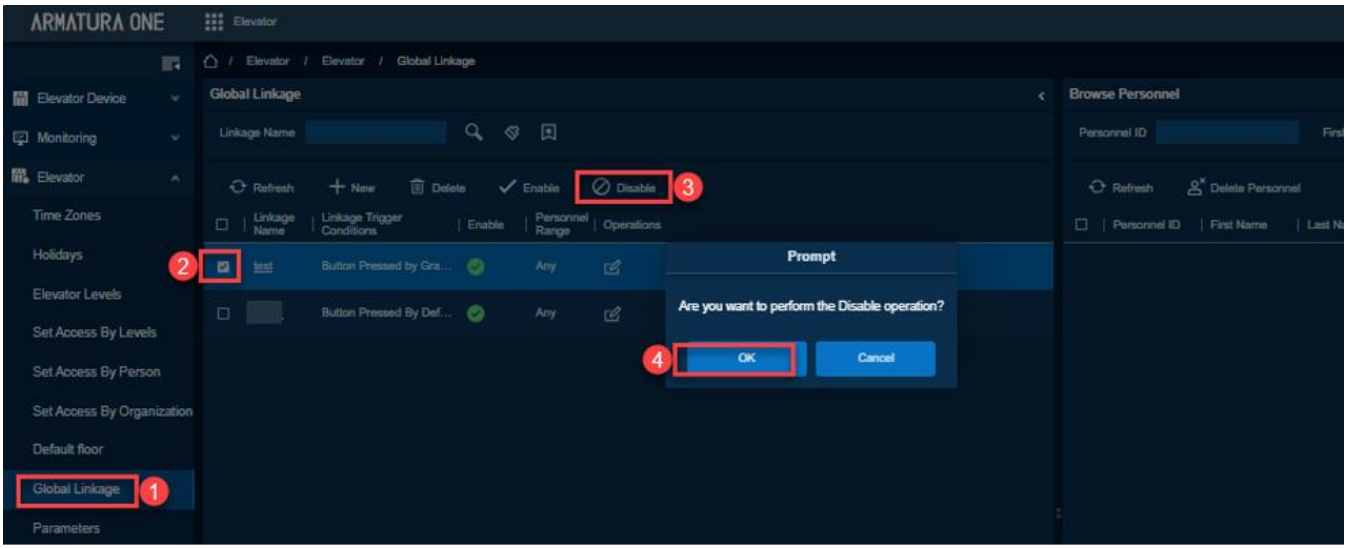
Deactivate the linkage configuration and stop executing the current linkage settings.

Triggered Result

The linkage has been disabled, and the configuration will not be executed.

Steps:

- Select linkage configuration, click **[Disable]**.
- Click **[OK]**.



Add Personnel

Prerequisites for Use

The range of linkage configuration personnel is the selection type.

Usage Scenarios

Set up linkage configuration for certain people.

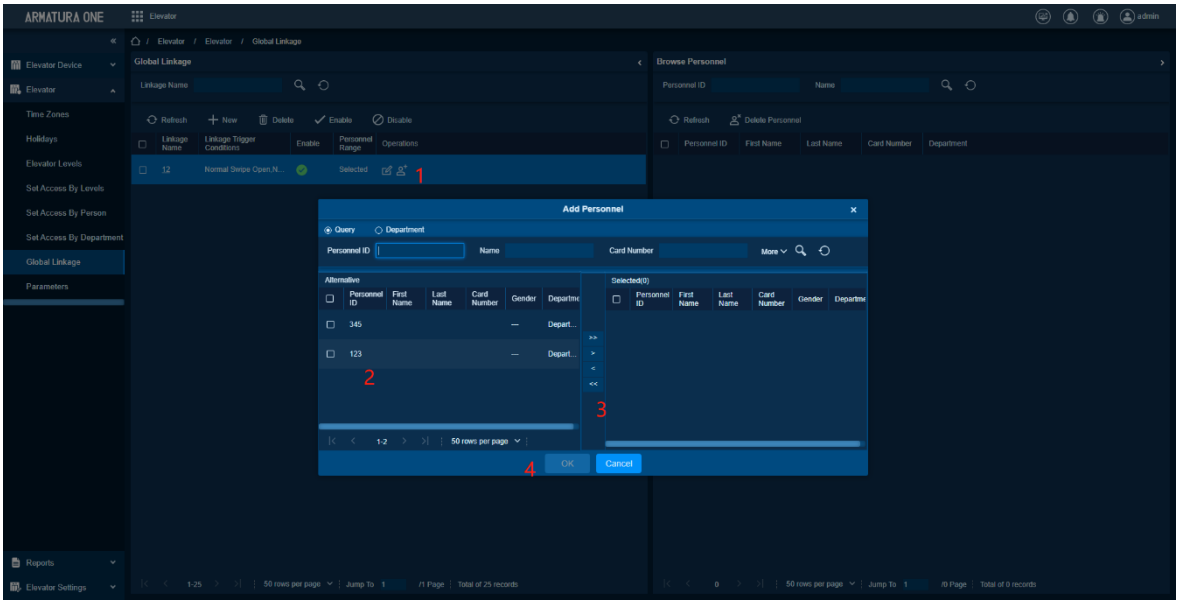
Triggered Result

Linkage configuration to add designated personnel.

Steps:

- Click Add Personnel button, a window will pop up to select the corresponding personnel information, click **[OK].**

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete Personnel

Prerequisites for Use

The range of personnel for the linkage configuration is based on the selected type. Linkage configuration has been added personnel.

Usage Scenarios

Delete linkage of designated personnel.

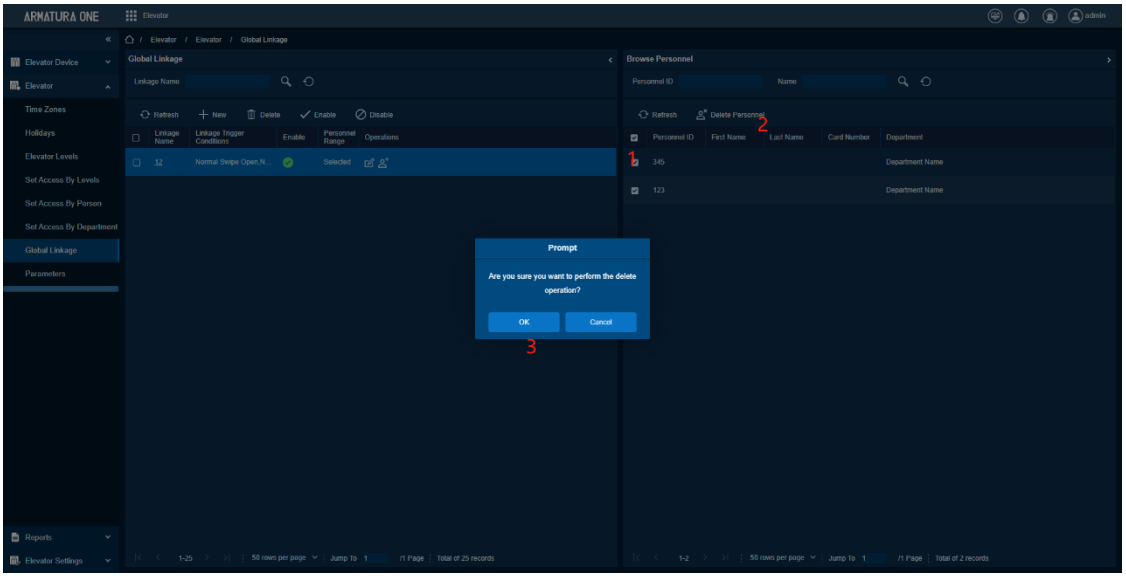
Triggered Result

Delete the association between personnel and linkage configuration.

Steps:

- Select Personnel, click **[Delete]**.
- A confirmation window pops up, click **[OK].**

Copyright © 2024 ARMATURA LLC. All rights reserved



8.3.9 Parameters

Function Description

The guest module uses parameter configuration.

Prerequisites for Use

Set custom parameters.

Usage Scenarios

Modify the default method of obtaining event records or modify the height of the photo pop-up window on the real-time monitoring page.

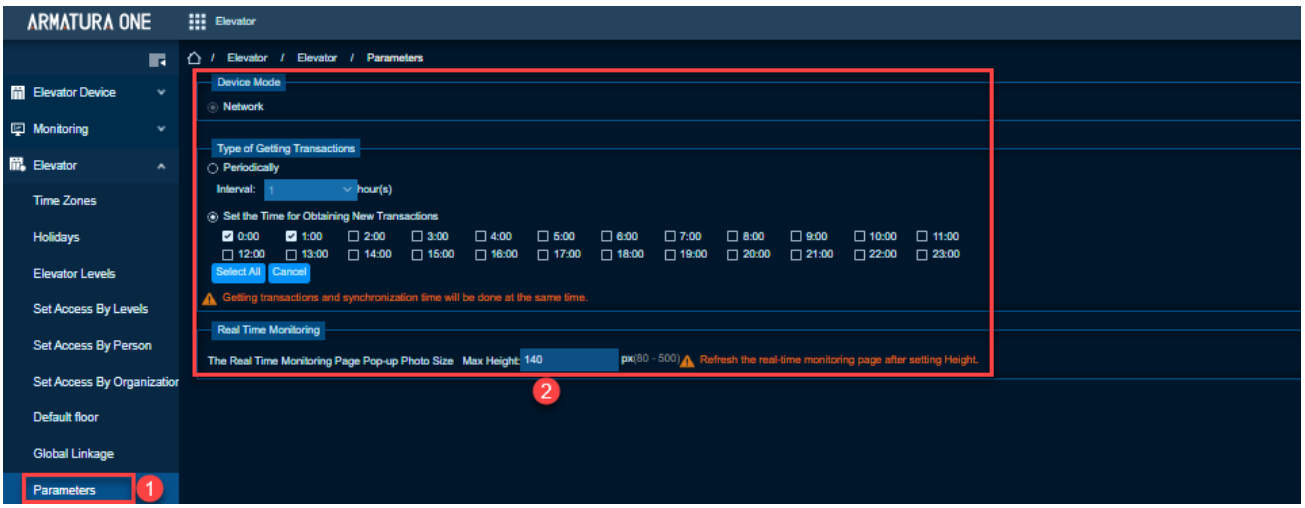
Triggered Result

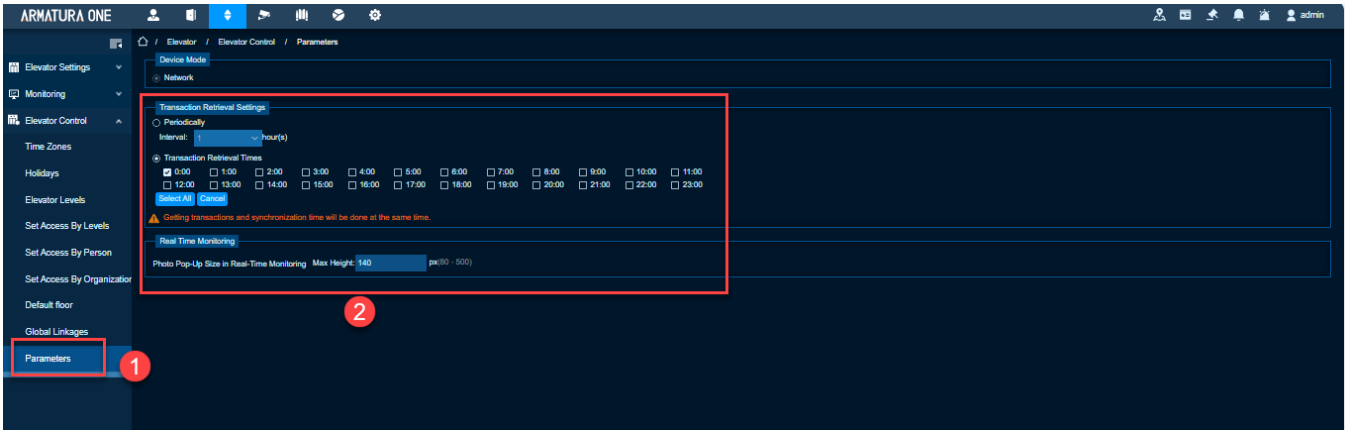
Modify the default method of obtaining event records to custom or modify the height of the photo pop-up window on the real-time monitoring page to custom.

Steps:

- Click **[Elevator] > [Elevator Control] > [Parameters].**

Copyright © 2024 ARMATURA LLC. All rights reserved





Transaction Retrieval Settings:

Periodically

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

Set the Transaction Retrieval Times

The selected time is up, the system will attempt to download new transactions automatically.

The Real Time Monitoring Page Pop-up Staff Photo Size: When an access control event occurs, the personnel photo will pop up, set the size of the pop-up photos, the range is 80-500px.

Copyright © 2024 ARMATURA LLC. All rights reserved

8.4 Report

Function List

Functions	Description
All Transactions	View elevators control all records, clear data, and export function.
All Exception Events	All abnormal record management of elevator control, data can be cleared and export operation.
Access Rights By Personnel	View the personnel in the corresponding permission list of the floor and be able to export the corresponding personnel list information.
Access Rights By Floor	View system personnel's corresponding floor permissions and be able to export corresponding personnel floor information.

8.4.1 All Transactions

Function Description

View the records of all events generated by the current system elevator control module, support clearing data and exporting data. Because the data size of elevator access control event records is large, user can view elevator access control events as specified condition when querying. By default, the system displays the latest three months' transactions.

Clear Data

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Clear historical data.

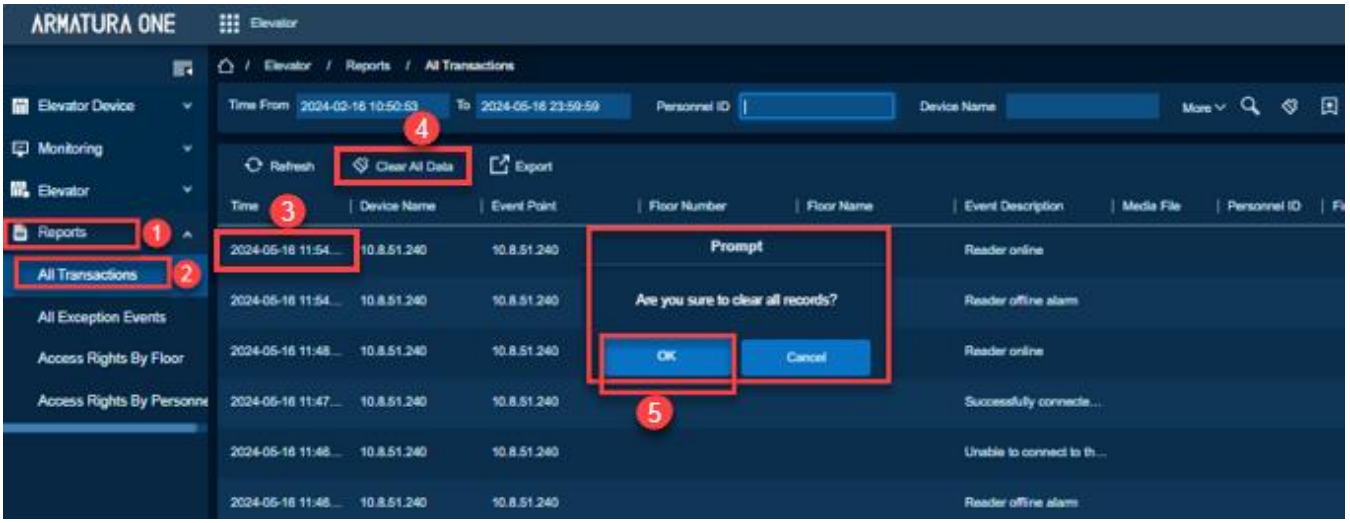
Triggered Result

Clear all event records of elevator control in the current system.

Steps:

- Click **[Clear All Data]** to pop up window and click **[OK]** to clear all transactions.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export

Prerequisites for Use

The current system elevator control event record has data.

Usage Scenarios

Export data to a local computer for viewing or processing.

Triggered Result

The local computer generates an Excel table, and the content of the table is exported data.

Steps:

- User can export all transactions in Excel, PDF, CSV format.

All Transactions

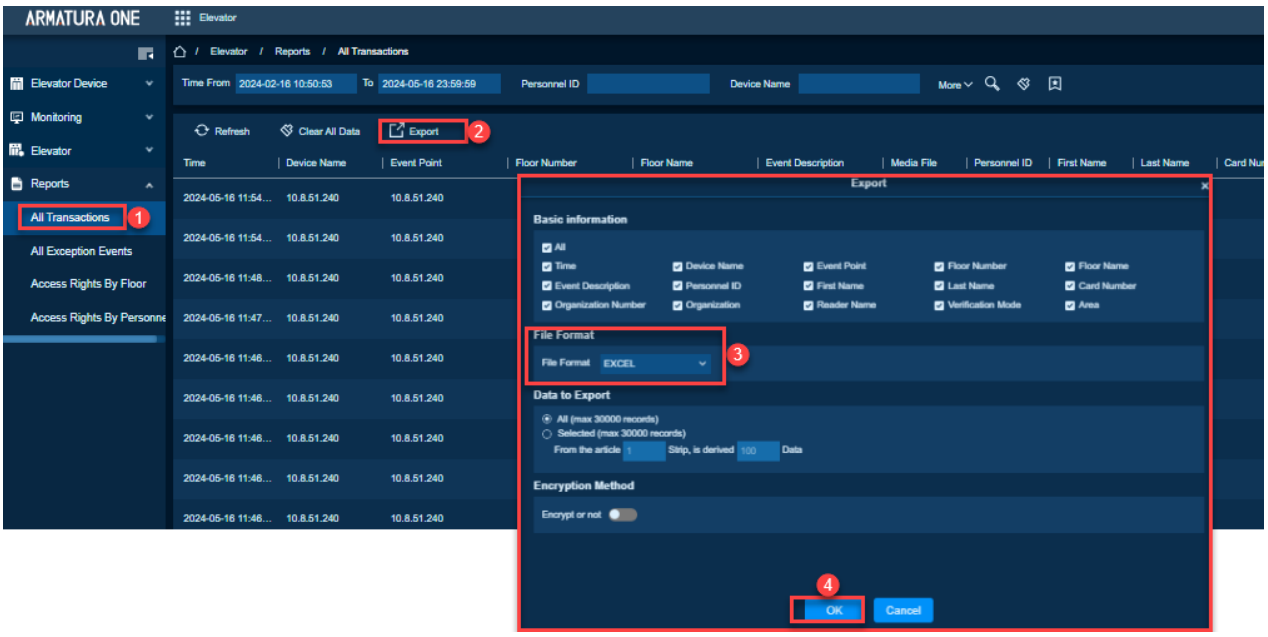
Time: 2017-09-18 00 : 00 : 00 - 2017-12-18 23 : 59 : 59

Time	Device	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department	Reader Name	Verification Mode	Area	Remark
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-8	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-5	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-9	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-1	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-4	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-3	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-2	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-8	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-10	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-9	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-7	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-6	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-8	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-7	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-5	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:51	192.168.218.65	192.168.218.65-5	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:51	192.168.218.65	192.168.218.65-8	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:	192.168.218.65	192.168.218.65-6	Normal Punch	2940	Sherry	Yang	4461253	General	192.168.218.65-	Card or Fingerprint	Area Name	

Created on: 2017-12-18 16:01:27

Created from ZKBioSecurity software. All rights reserved. 1/3

Copyright © 2024 ARMATURA LLC. All rights reserved

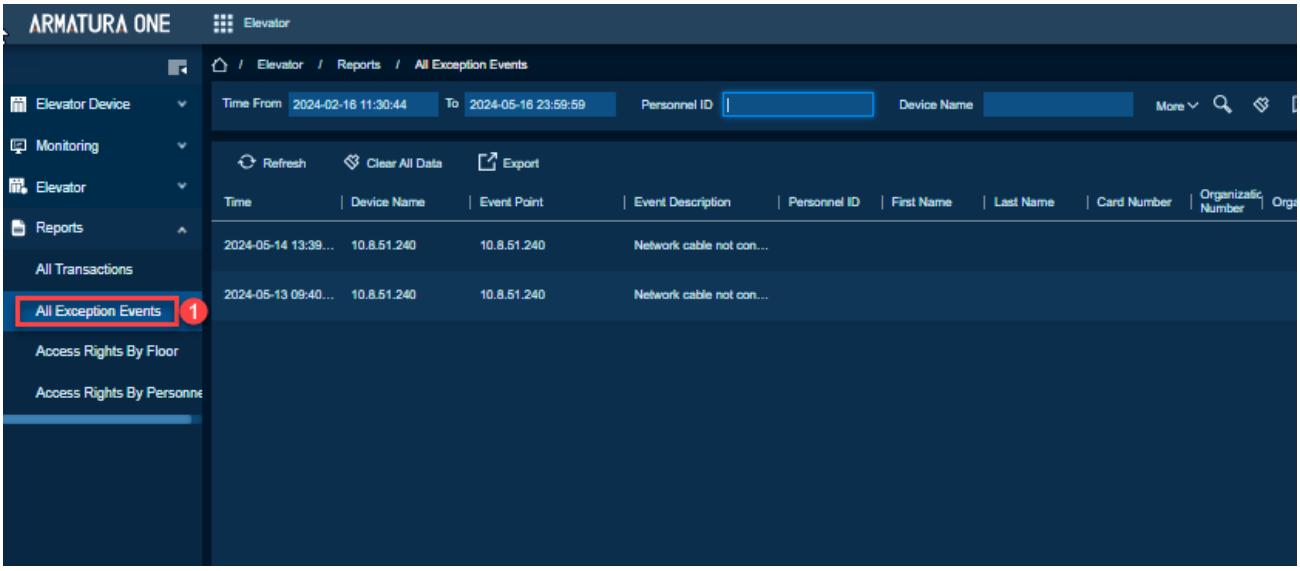


8.4.2 All Exception Events

Function Description

Steps:

- Click **[Reports] > [All Exception Events]** to view exception events in specified condition. The options are same as those of **[All Transactions].**



Clear Data

Prerequisites for Use

Log into the system using an account with the required permissions. Ensure that the current system elevator control event record contains data.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

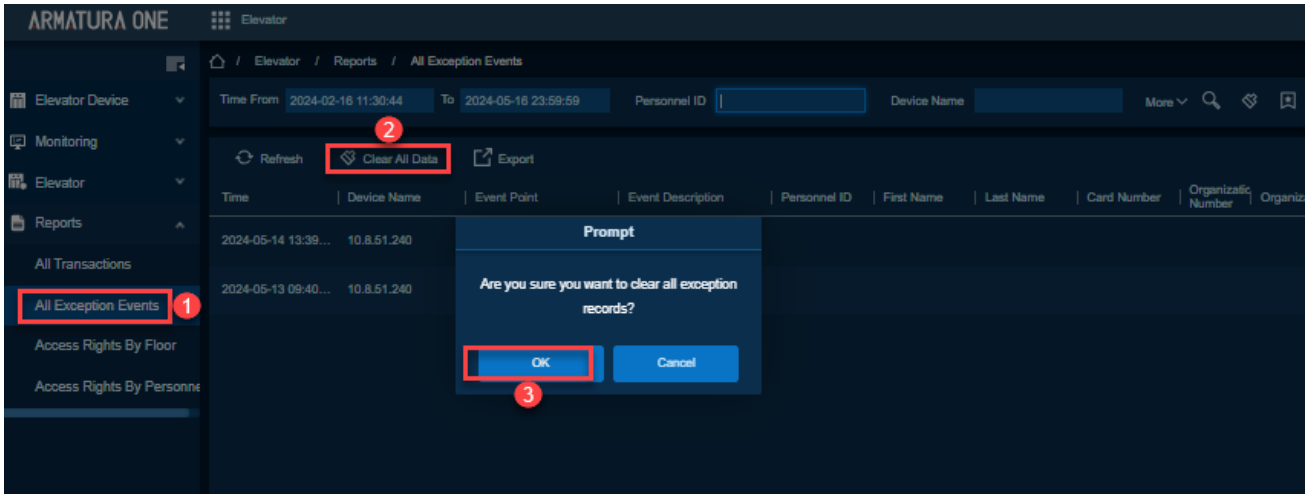
Clear historical data.

Triggered Result

Clear all event records of elevator control in the current system.

Steps:

- Click **[Clear All Data]** to pop up window, click **[OK]** to clear all exception events.



Export

Prerequisites for Use

The current system elevator control event record has data

Usage Scenarios

Export data to a local computer for viewing or processing.

Triggered Result

The local computer generates an Excel table, and the content of the table is exported data.

Steps:

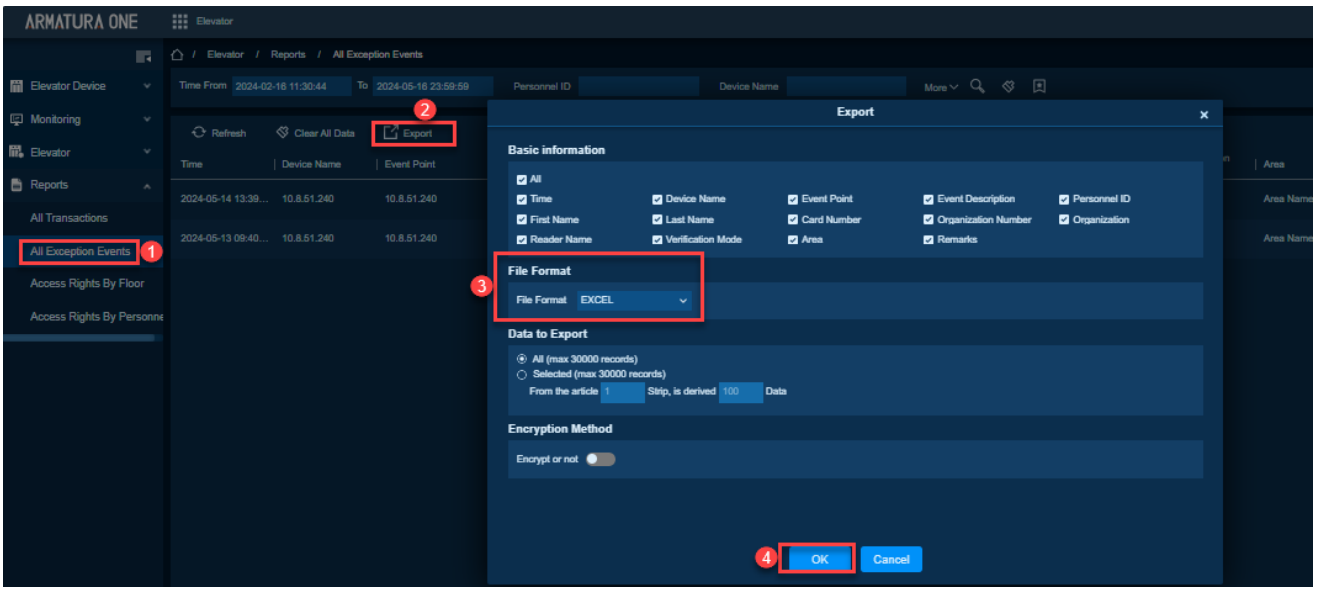
- User can export all exception events in Excel, PDF, CSV format.

All Exception Events

Time: 2017-09-18 00 : 00 : 00 - 2017-12-18 23 : 59 : 59

Time	Area	Device	Event Point	Event Description	Card Number	Personnel ID	First Name	Last Name	Department	Reader Name	Verification Mode	Remark
2017-12-15 10:29:11	Area Name	192.168.218.65	192.168.218.65-Reader	Disabled Card	9505930	1	Jerry	Wang	General	192.168.218.65-Reader	Card or Fingerprint	
2017-12-15 10:29:14	Area Name	192.168.218.65	192.168.218.65-Reader	Disabled Card	4461253	2940	Sherry	Yang	General	192.168.218.65-Reader	Card or Fingerprint	
2017-12-15 10:29:09	Area Name	192.168.218.65	192.168.218.65-Reader	Disabled Card	13260079	3	Leo	Hou	General	192.168.218.65-Reader	Card or Fingerprint	
2017-12-15 10:29:09	Area Name	192.168.218.65	192.168.218.65-Reader	Operate Interval too Short	13260079	3	Leo	Hou	General	192.168.218.65-Reader	Card or Fingerprint	

Copyright © 2024 ARMATURA LLC. All rights reserved



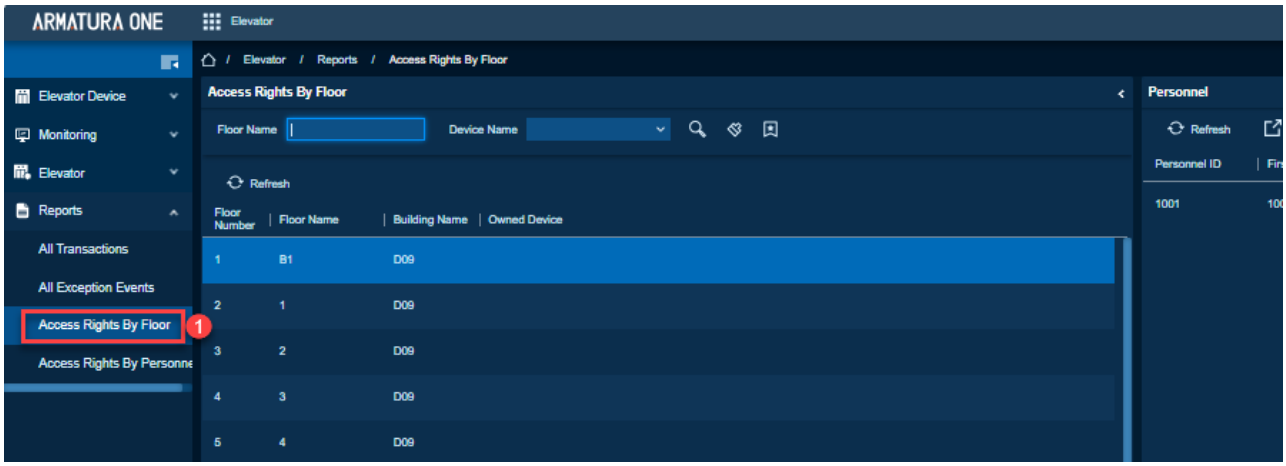
8.4.3 Access Rights By Floor

Function Description

View related access levels by door.

Steps:

- Click **[Reports] > [Access Rights by Floor],** the data list in the left side shows all floors in the system, select a floor, the personnel having access levels to the floor will display on the right data list.



Export

Prerequisites for Use

Query personnel floor access rights.

Usage Scenarios

Export data associated with elevator control floors and personnel information to local.

Copyright © 2024 ARMATURA LLC. All rights reserved

Triggered Result

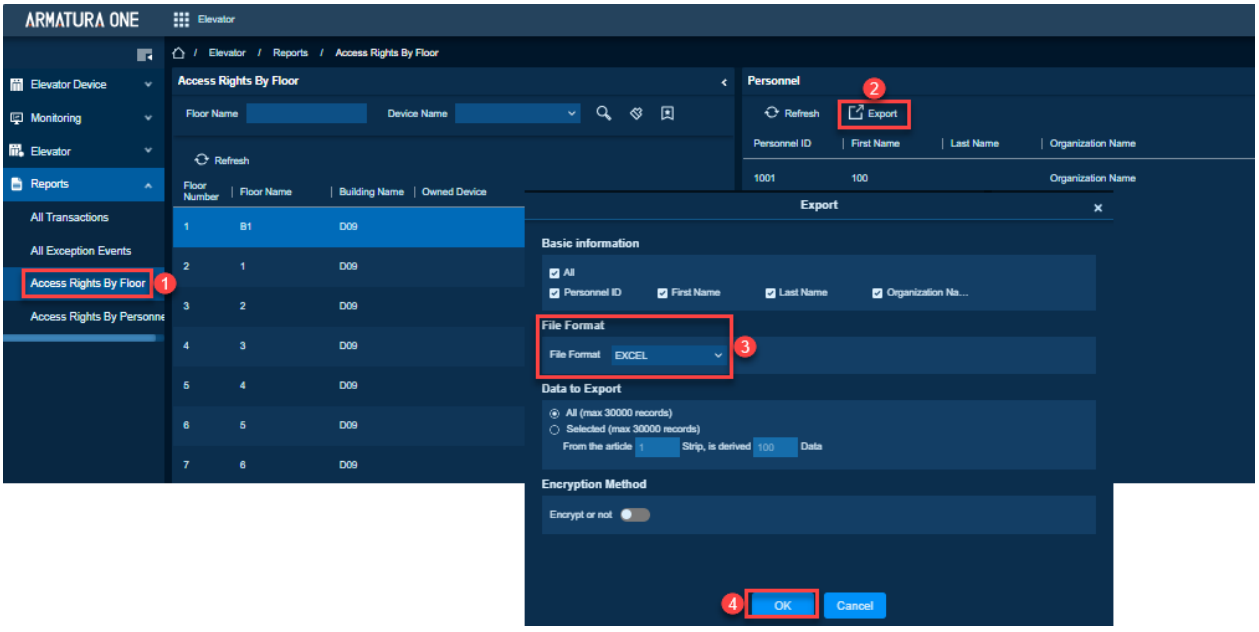
Save locally generated files.

Steps:

- User can export all the personnel having access levels to the floor data in Excel, PDF, CSV format.

192.168.218.65-1(1) Opening Personnel

Personnel ID	First Name	Last Name	Department
2940	Sherry	Yang	Hotel
1	Jerry	Wang	General
2	Lucky	Tan	Development Department
3	Leo	Hou	Financial Department
5	Necol	Ye	Marketing Department
6	Amber	Lin	Financial Department
8	Glori	Liu	Marketing Department
9	Lilian	Mei	Development Department

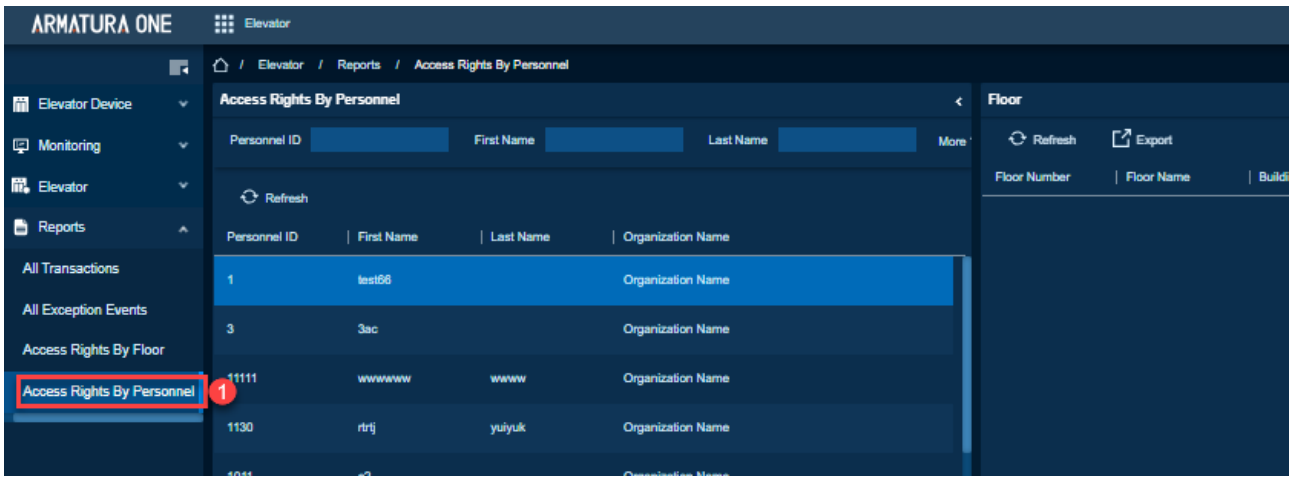


8.4.4 Access Rights By Personnel

Function Description

Click **[Reports] > [Access Rights by Personnel],** the data list in the left side shows all doors in the system, select personnel, the personnel having access levels to the door will display on the right data list.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export

Prerequisites for Use

Personnel have corresponding floor authority.

Usage Scenarios

Export the floor information corresponding to the personnel to the local computer.

Triggered Result

Generate export data files locally.

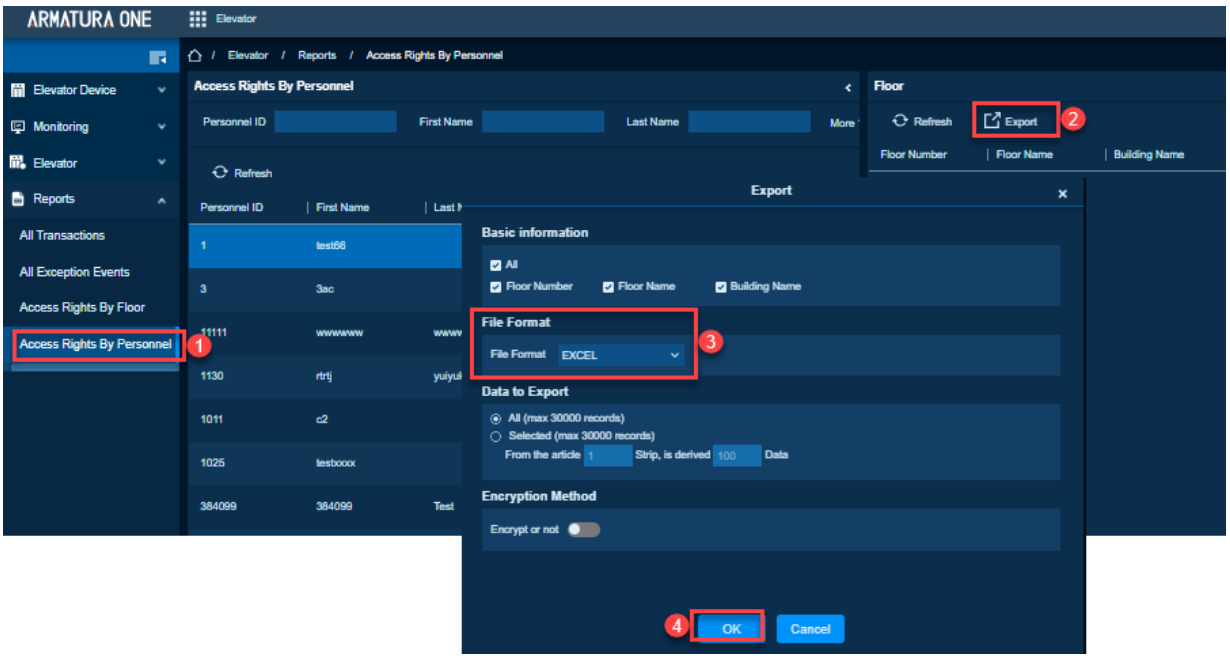
Steps:

- User can export all the floor information in Excel, PDF, CSV format.

2940(Sherry) Having Level to Access

Floor Number	Floor Name
1	192.168.218.65-1
2	192.168.218.65-2
3	192.168.218.65-3
4	192.168.218.65-4
5	192.168.218.65-5
6	192.168.218.65-6
7	192.168.218.65-7
8	192.168.218.65-8
9	192.168.218.65-9
10	192.168.218.65-10

Copyright © 2024 ARMATURA LLC. All rights reserved



8.5 DCS Settings

Function List

Functions	Description
Integrated Device	Add and delete access control device integrated elevator control module.
External Readers	Add, edit, delete reader, configure template, clear templat
Internal Readers	Add, edit, delete reader, configure template, clear templat
Operation Lo	View operation records with third-party elevator control systems.

8.5.1 Integrated Device

Function Description

Add access control device to the elevator control module and provide the elevator control locking to verify the access control authority to use the elevator function.

Add

Prerequisites for Use

Add Access Control Device.

Usage Scenarios

The door of the access control device is bound with external reader or internal reader for access control permission verification, and then directly call the elevator to take the elevator.

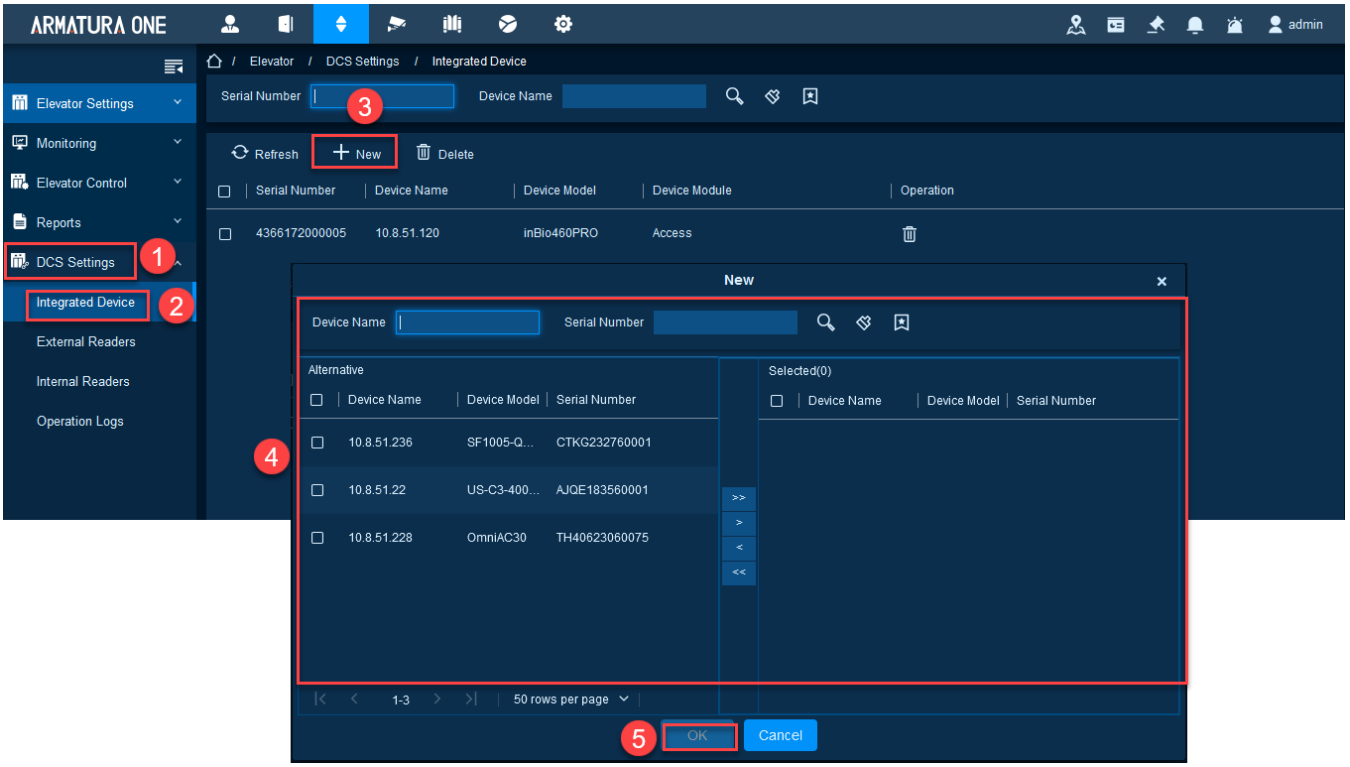
Copyright © 2024 ARMATURA LLC. All rights reserved

Triggered Result

Add the access control device to the current menu.

Steps:

- Click **Add**, a double list pops up to select the access control device.
- Select the corresponding access control device, click **OK.**



Copyright © 2024 ARMATURA LLC. All rights reserved

Delete

Prerequisites for Use

The system requires selection of an Access Control Device where door information is not bound to any external or internal readers.

Usage Scenarios

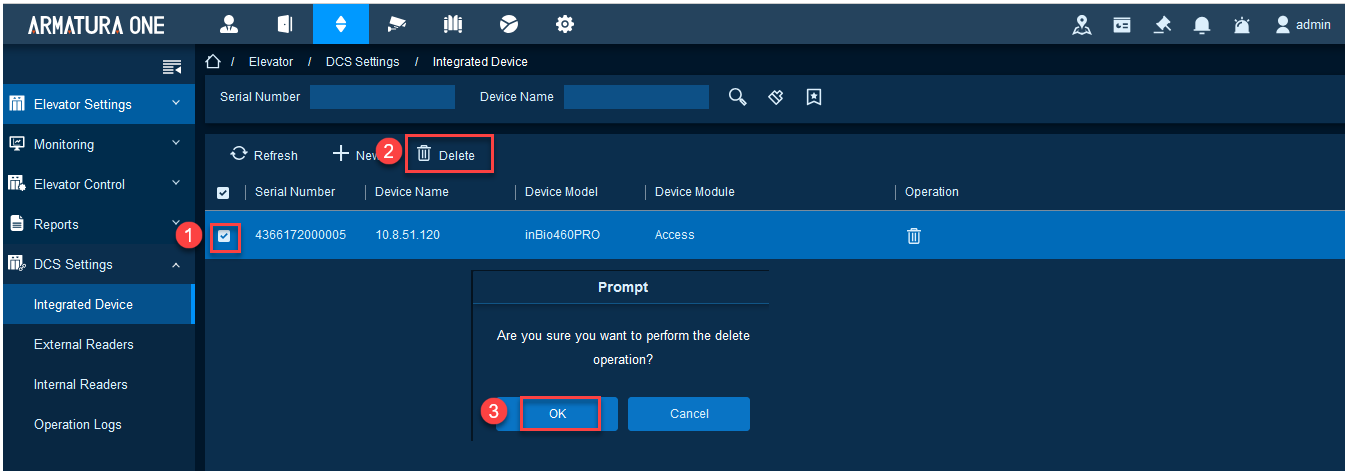
Access control device is not used.

Triggered Result

Delete the associated information of the selected access control device and elevator control module.

Steps:

- Select the device, click **[Delete]** button.
- On the pop-up interface, click **[OK].**

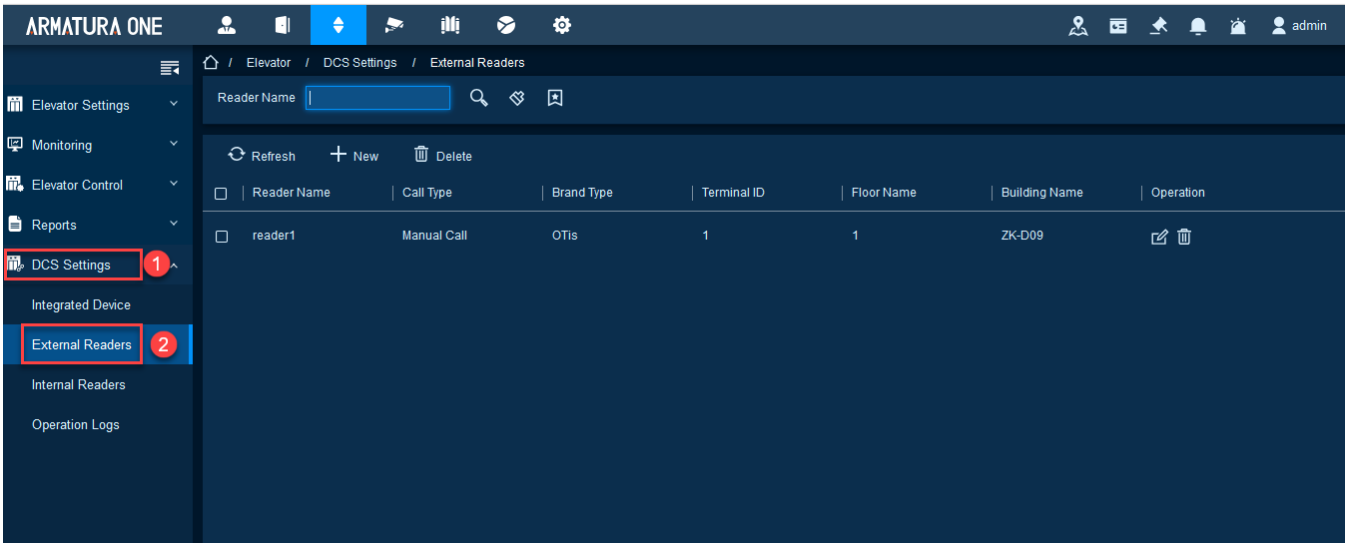


8.5.2 External Readers

Function Description

Click **[Elevator Settings] > [External Readers]**. The edited external read page displayed on the current page. Using the system, user can manage and edit the connection between external reader and buildings and set the default floor and call mode. Each elevator call type is different from the building to which it is bound.

Copyright © 2024 ARMATURA LLC. All rights reserved



Add External Readers

Prerequisites for Use

The system requires an added access control device, selected door reader, and configured building floor information.

Usage Scenarios

Add the information associated with the access control device to from external reader.

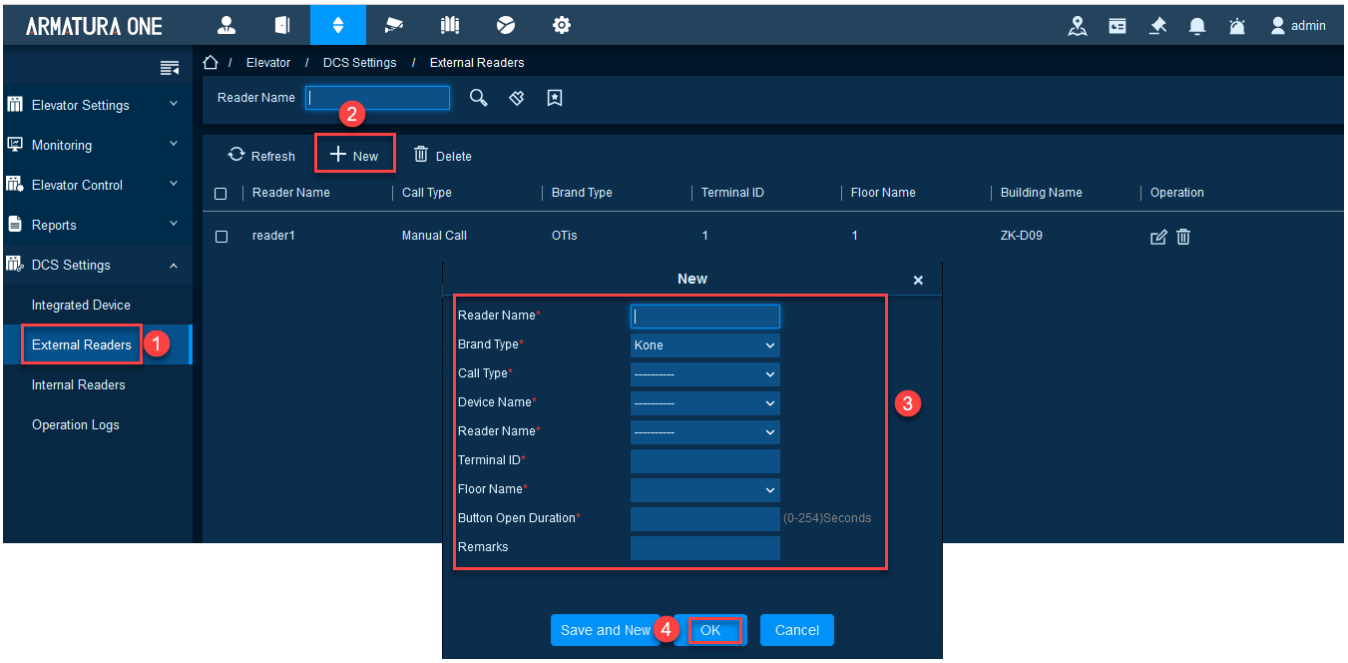
Triggered Result

Generate an external reader data message.

Steps:

- Click **[Elevator Settings]** > **[External Readers]** > **[New]** to add new external reader.

Copyright © 2024 ARMATURA LLC. All rights reserved



Reader Name: Name of the external reader displayed on the list page.

Brand Type: Select different elevator brands and the corresponding brand names will be listed. such as KONE, Mitsubishi, Hitachi, Schindler, Otis.

Call Type: Depending on the brand type of elevator chosen, there are different call types.

Elevator T	Type of Call	Description
KONE	Normal Call	Normal call
	RCGIF Call	DOP Side
Mitsubishi	Manual Call	Manual call (for the VIP or the everyman)
	Auto Call	Automatic call (for the disabled)
Hitachi	Manual Call	Manual call (for the VIP or the everyman)
	Auto Call	Automatic call (for the disabled)

Device Name: Select the added integration device.

Reader Name: Select the reader from integration device.

Terminal ID: Set the terminal ID. Each elevator brand type must have a non-repeatable terminal ID and a significant number that can only range from 1 to 255.

Floor Name: Select the floor in the bound building.

Button Open Duration: It is used to control the time to press floor button after verification. The default value is 5 seconds; the range is 0 to 254 seconds.

Copyright © 2024 ARMATURA LLC. All rights reserved

Remark: Add the remark**.**

Delete External Readers

Prerequisites for Use

Delete an external reader.

Usage Scenarios

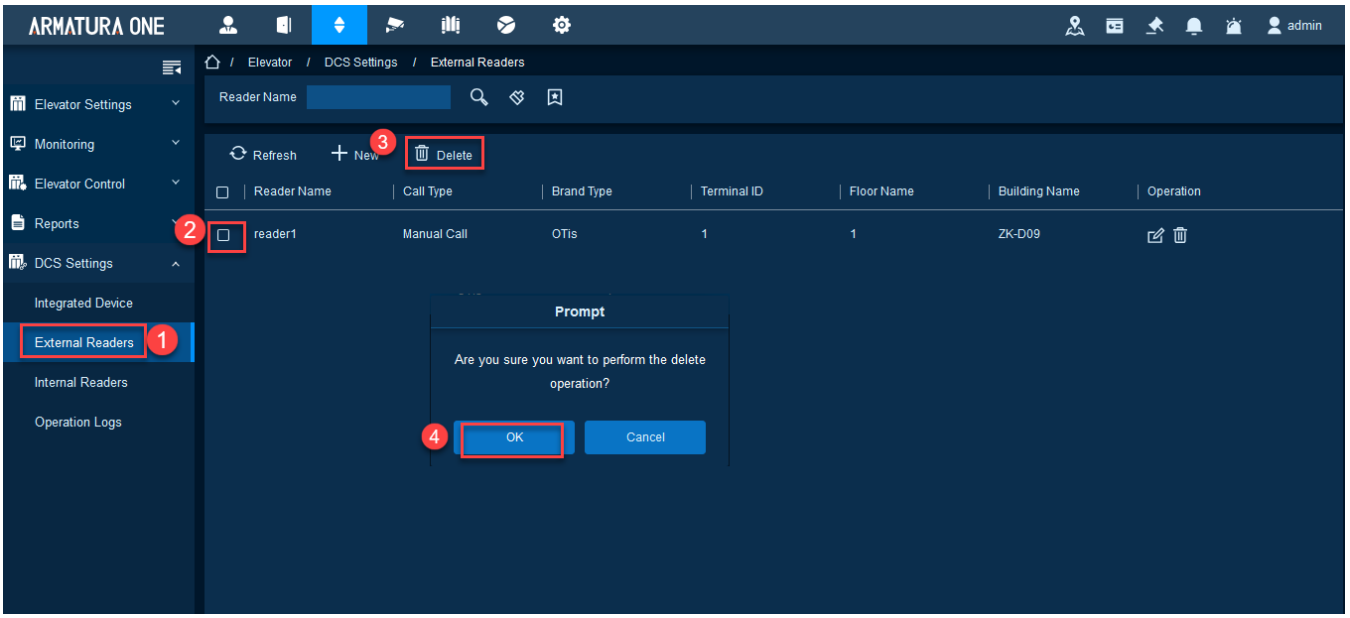
Currently external reader is not used or requires delete.

Triggered Result

Delete the currently selected external reader information.

Steps:

- Click the delete button of the list data, a confirmation window pops up, click **[OK]**, the operation is complete.



Edit Readers

Prerequisites for Use

Add external reader information.

Select the external reader information that needs to be configured.

Usage Scenarios

Set the external reader to configure the opening and closing status of the door before and after arriving on the floor and support the configuration of the online and offline status settings of the device.

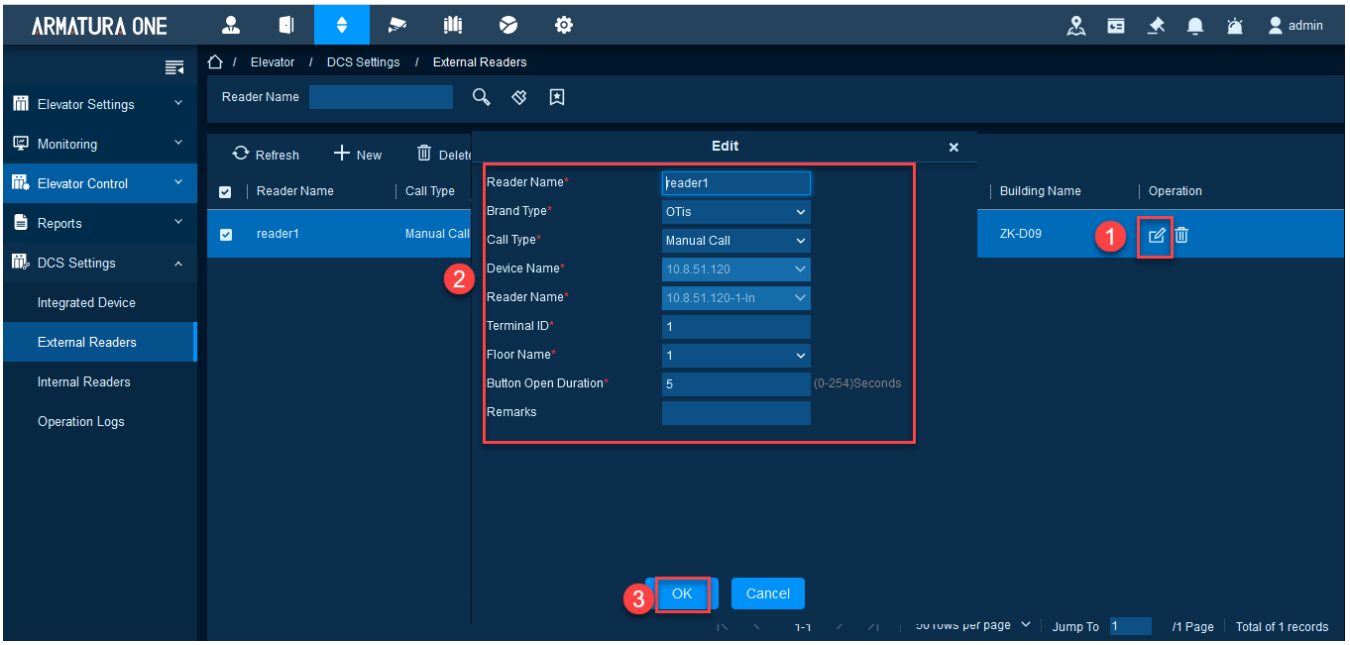
Copyright © 2024 ARMATURA LLC. All rights reserved

Triggered Result

Set the open status of the front and rear doors on the arrival floor when the current external reader is online and offline and send it to the third-party elevator control system.

Steps:

- Select the Reader name, click **[Edit].**
- After editing the data, on the pop-up window, click **[OK]**.

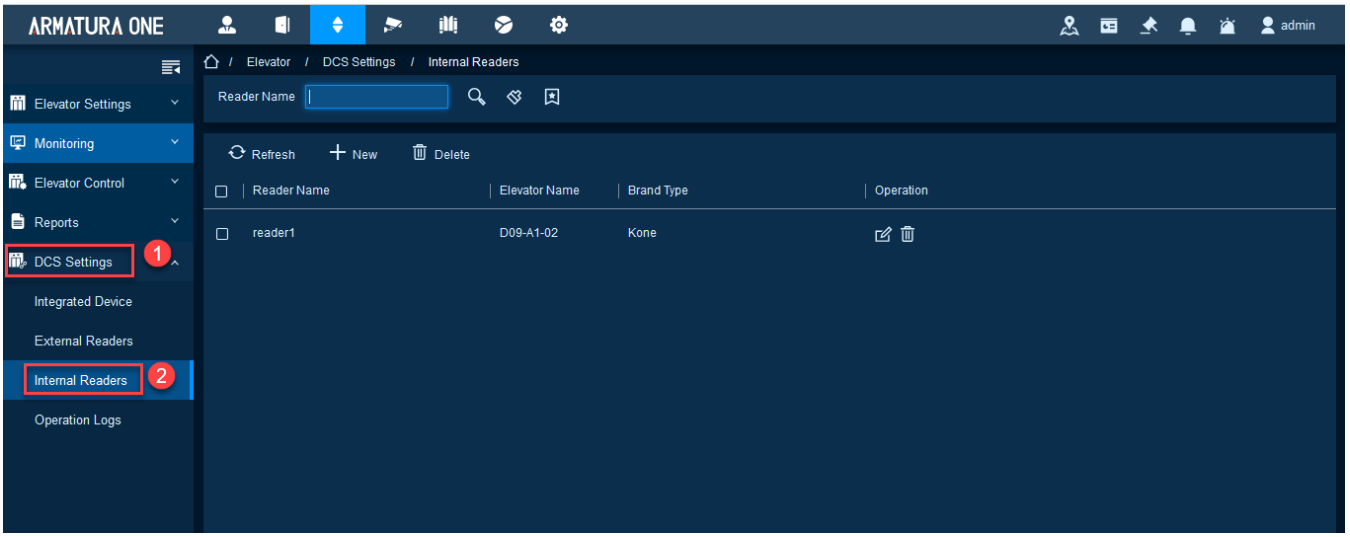


8.5.3 Internal Readers

Function Description

This feature allows user to bind the internal reader inside the elevator to the corresponding elevator in the Elevator Group.

Copyright © 2024 ARMATURA LLC. All rights reserved



Add Internal Readers

Prerequisites for Use

The system requires configured elevator data, added access control device, and selected door reader information.

Usage Scenarios

This function associates access control device and elevator data with internal reader configurations.

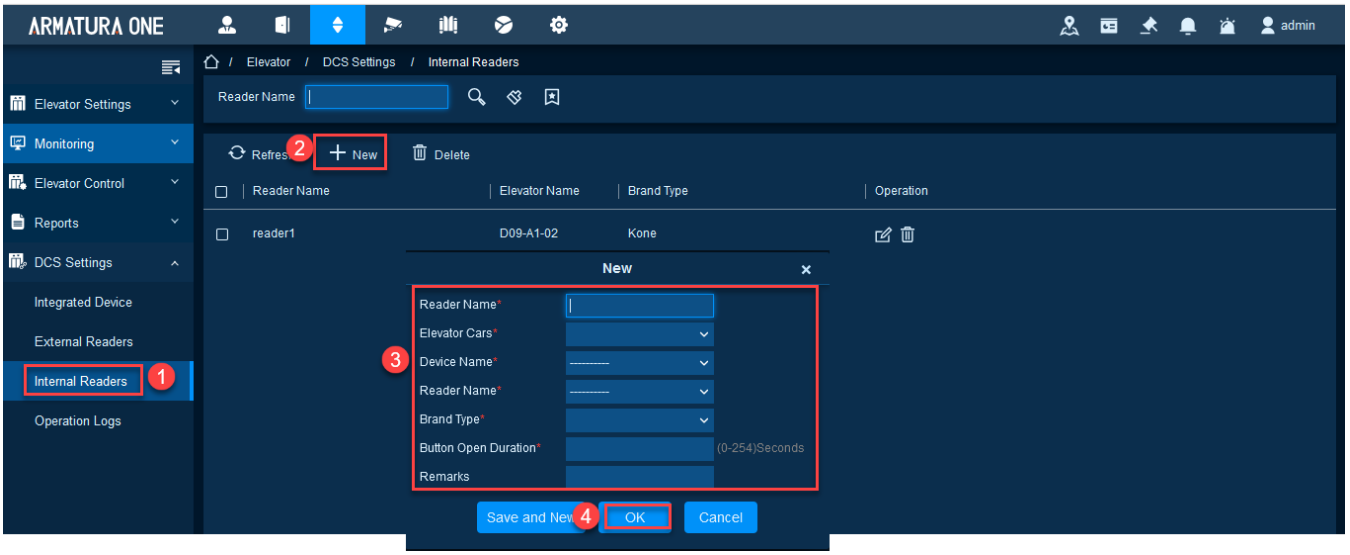
Triggered Result

Add an internal readers data message.

Steps:

- Click **[Elevator Settings] > [Internal Readers] > [New]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Reader name: Name of the Internal reader displayed on the list page.

Elevator Cars: The data source comes from the corresponding elevator group and elevator added to the elevator group.

Device Name: The device name is derived from the integration device and is obtained by adding the integration device.

Reader Name: Select the reader from device.

Brand Type: Set brand type as Kone, Mitsubishi, Hitachi, Schindler, Otis and so on.

Button Open Duration: It is used to control the time to press floor button after verification. The default value is 5 seconds; the range is 0 to 254 seconds.

Remark: Add the remark**.**

Delete Internal Readers

Prerequisites for Use

No specific prerequisites required.

Usage Scenarios

This function removes obsolete or unnecessary internal reader configurations from the system.

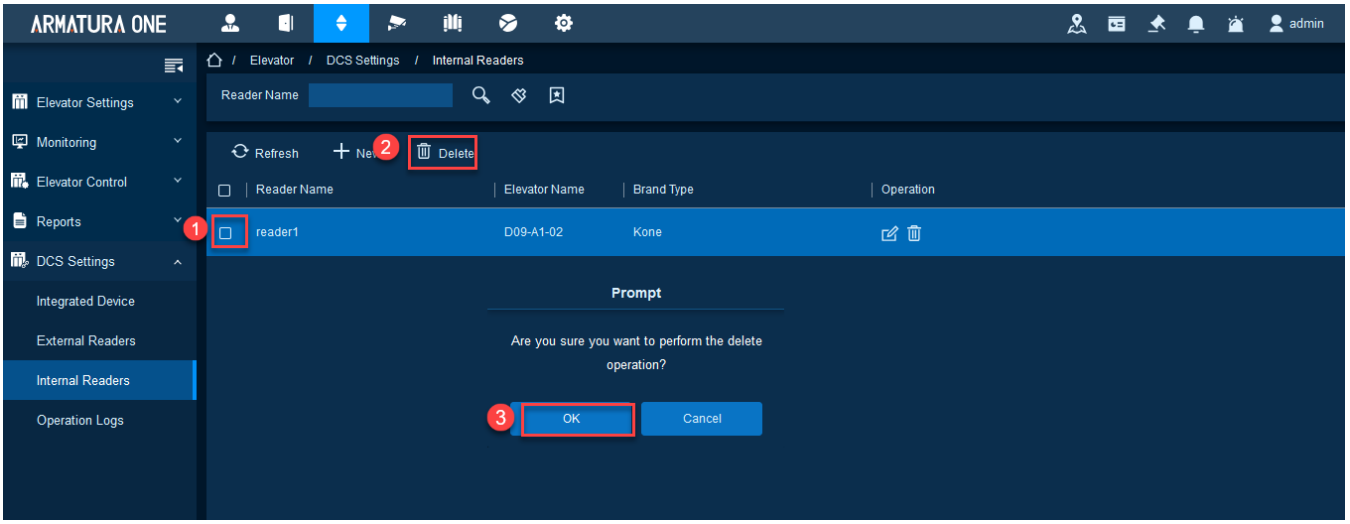
Triggered Result

Removes the selected internal reader configuration.

Steps:

- Select the Reader name, click **[Delete].**
- On the pop-up interface, click **[OK]**.

Copyright © 2024 ARMATURA LLC. All rights reserved



Edit Readers

Prerequisites for Use

Add internal reader information.

Usage Scenarios

Set the internal reader to configure the opening and closing status of the door before and after arriving on the floor and support the configuration of the online and offline status settings of the device.

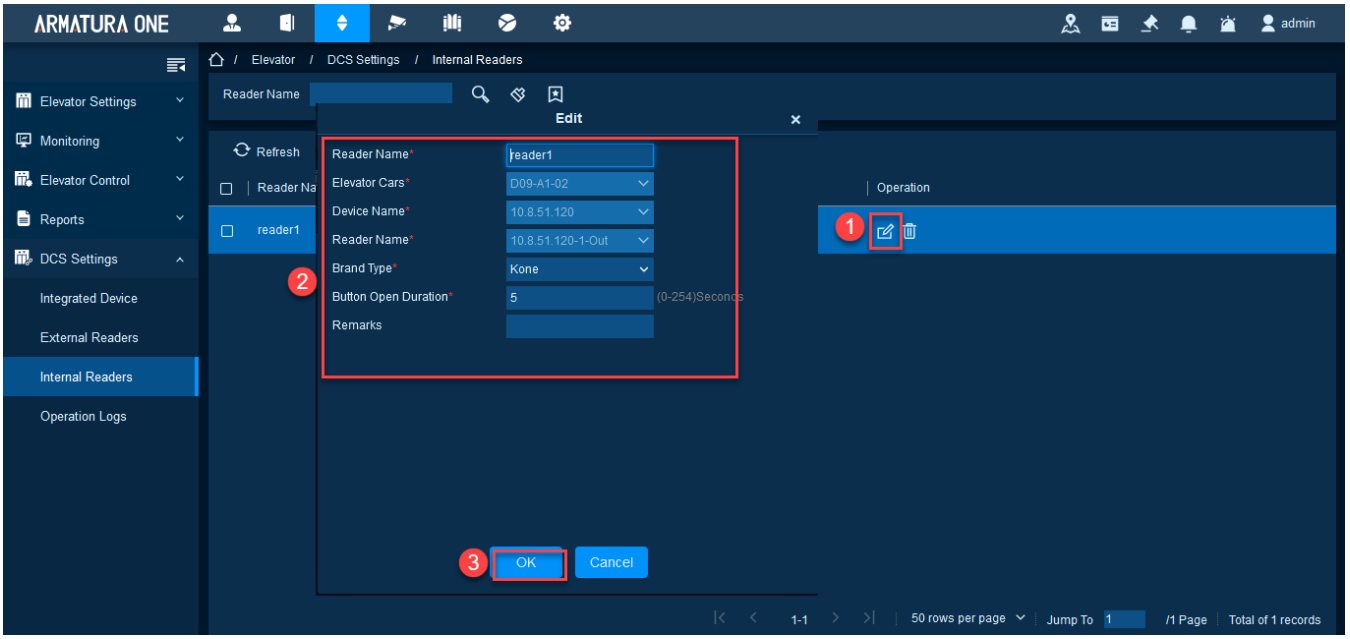
Triggered Result

Set the open status of the front and rear doors of the arrival floor when the current internal reader is online and offline and send it to the third-party elevator control system.

Steps:

- Select the Reader Name and click **[Edit].**
- After editing the reader details, click on, click **[OK]** to save the edit.

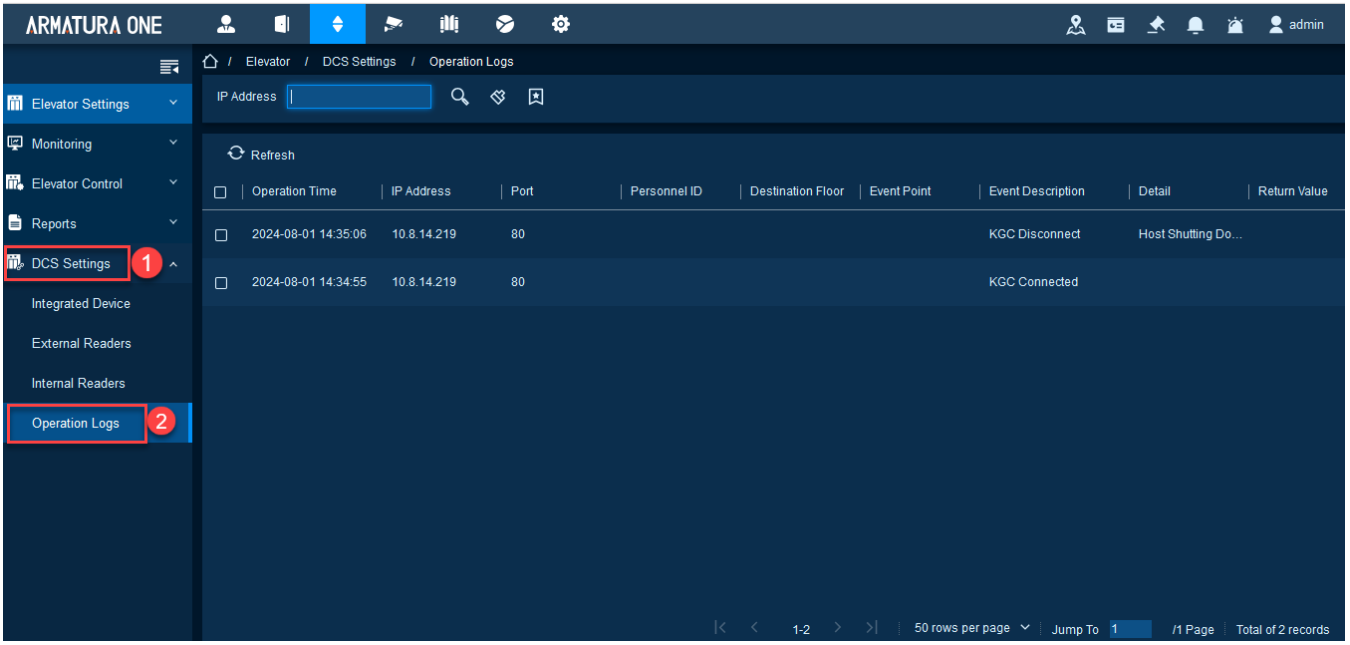
Copyright © 2024 ARMATURA LLC. All rights reserved



8.5.4 Operation Logs

Function Description

- Click **[Elevator Settings] > [Operation Logs]** to query and view all operation records of elevator equipment (such as heartbeat check, device connection status, elevator arrival to default floor, etc.)



Copyright © 2024 ARMATURA LLC. All rights reserved

9 Video

The Video Module enables comprehensive video management by integrating with Hanwha Vision's Wave VMS. Users can perform real-time video previews and playback for authorized devices, providing immediate access to visual security data. It also allows users to configure recording schedules, ensuring critical moments are captured and archived effectively.

Additionally, the module supports integration with Arteco's OMNIA software through a configurable connector. This integration enables access control data from Armatura One to be transmitted to Arteco OMNIA, allowing the data to be displayed directly within the OMNIA interface. This feature enhances the synchronization between access control and video management systems, delivering a unified visual security solution.

9.1 Video Management

Function List

Operations	Descriptions
Video Device	Unified management of video device.
Video Preview	It can view the monitoring screen which is connected to t video device in real time and can remotely control the PT functions.
Video Playback	It is possible to replay the recorded content of the camer searching for the specified time and specifying the camer

9.1.1 Device

Function Description

Unified Management of video device.

Device List

Prerequisites for Use

For third-party integrated systems, the parameter configuration must be properly connected and enabled.

Usage Scenarios

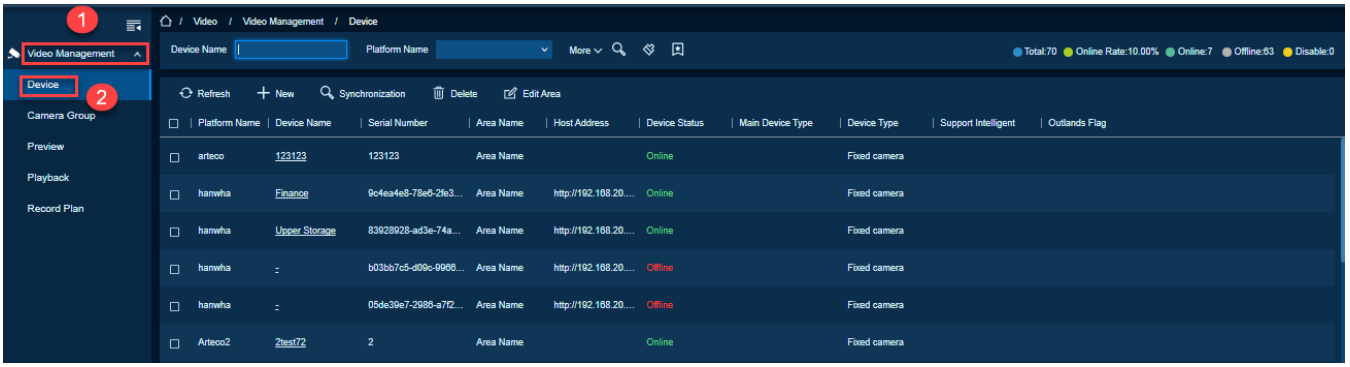
View device information.

Trigger Result

Operations	Descriptions
Enter the Page	View devices and status

The page directly displays the device list data according to the conditions and counts. The status of the device is as follows.

Copyright © 2024 ARMATURA LLC. All rights reserved



New (Add Devices)

Usage Scenarios

Add the required devices.

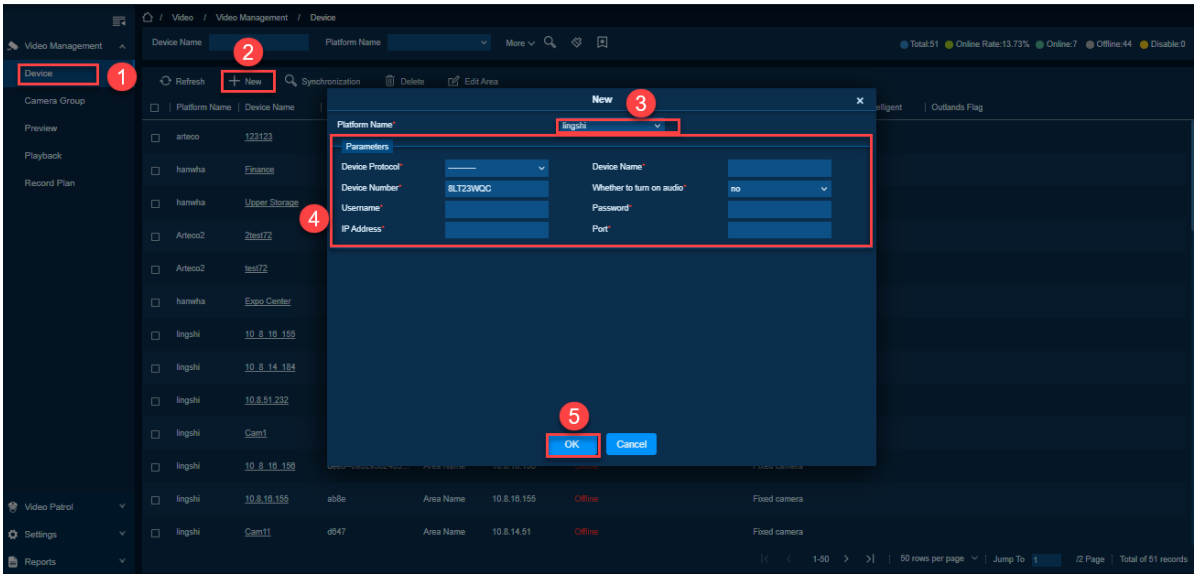
Trigger Result

Operations	Description
New	Add the devices by selecting platform name and parameters.

Platform Name: Drop down to select the platform name, Type the platform name in search bar or select the platform name from list then click **[OK]**.

Parameters: After choosing platform name enter the parameters details then click **[OK]**.

To Add the Device, click **[New]** then it will go to new interface.



Copyright © 2024 ARMATURA LLC. All rights reserved

Synchronization

Prerequisites for Use

For third-party integrated systems, the parameter configuration must be properly connected and enabled.

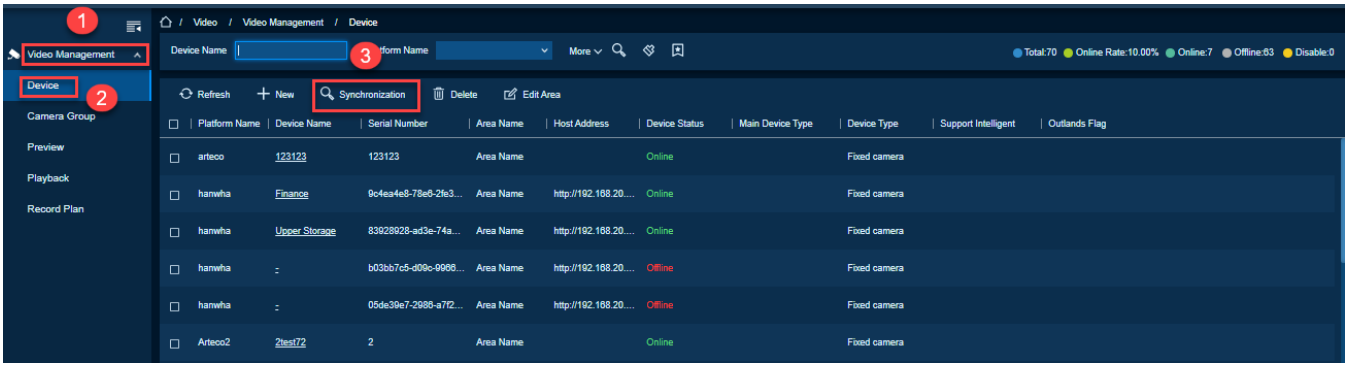
Usage Scenarios

Parameter configuration account permission switch when device data is inconsistent.

Trigger Result

Operations	Descriptions
Synchronize Device	The device data under the account authority will be synchronized.

After completing the parameter configuration, click the **[Synchronization]** button, and device list will be generated automatically.



Edit Area

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Change the camera's area.

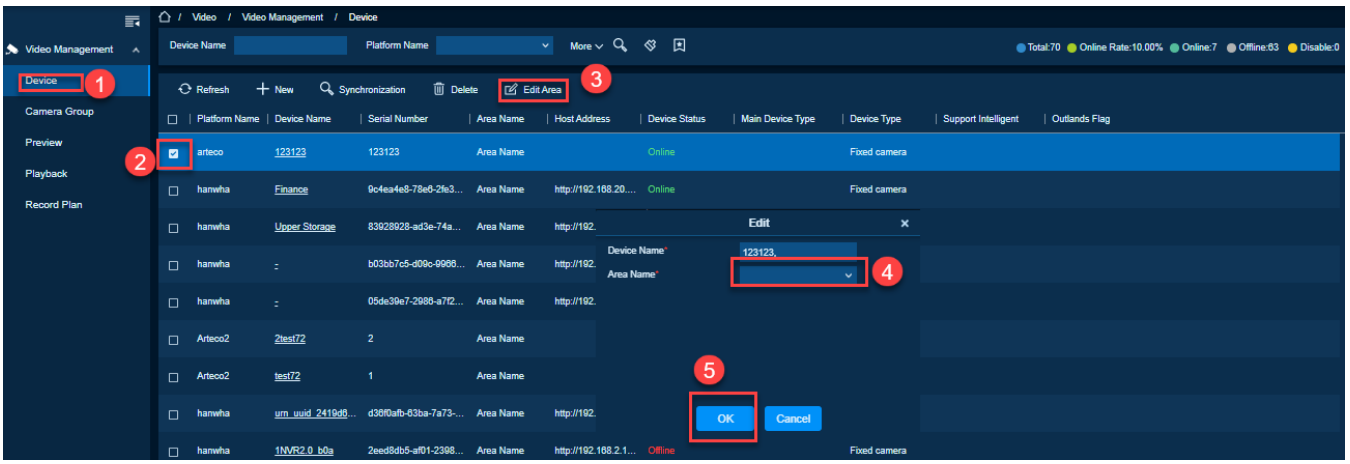
Trigger Result

Operations	Description
Edit Area	Modify the camera's area and details.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Check the video device that needs to be adjusted and click the **[Edit Area]** button.



Device Name: The designated identifier for the camera, which can be modified as required.

Area Name: A dropdown menu for selecting an area, referencing preconfigured settings.

- Click **[OK]** to complete the device area adjustment.

Delete Connector

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

The controller is no longer needed, or it requires reinstallation.

Trigger Result

Operations	Description
Delete Connector	Delete the connector

Steps:

- Check the connector to be deleted and click **[Delete]** button.
- Click **[OK]** to complete delete.

9.1.2 Preview

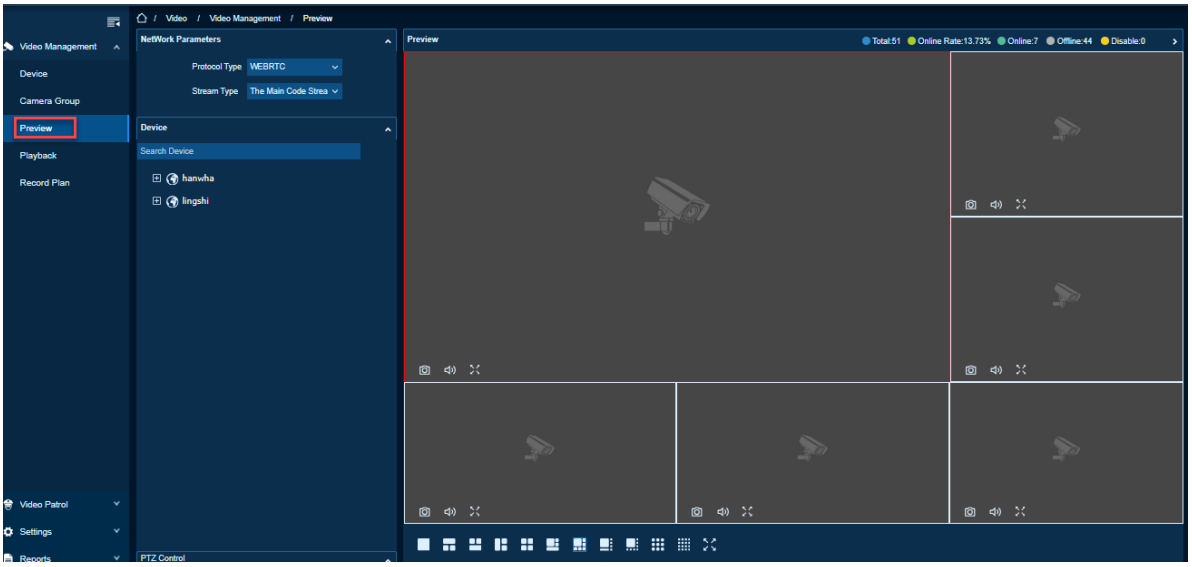
Function Description

This menu allows users to view real-time monitoring screens from connected video equipment and remotely operate PTZ (Pan-Tilt-Zoom) devices.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

Click **[Video Management]** > **[Preview]** to view the preview interface: the interface is divided into 5 windows.



Network Parameters

Prerequisites for Use

Third-party integrated systems require proper connection and authentication setup. During initial use, users must authenticate via the third-party VMS interface with valid credentials to enable video preview functionality.

Usage Scenarios

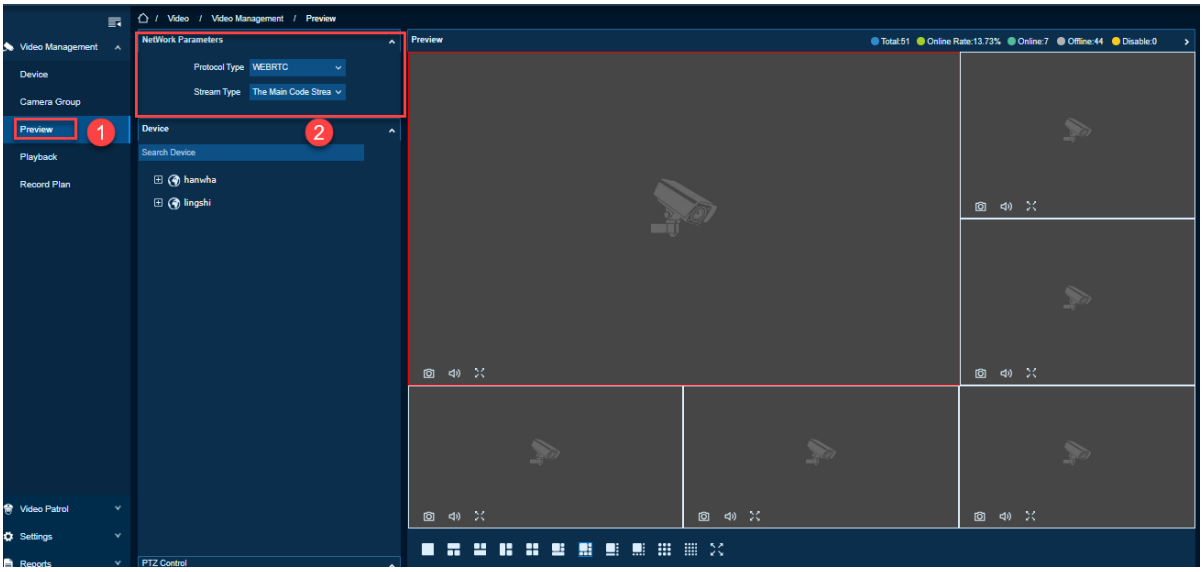
This function allows users to adjust viewing and network settings to resolve video streaming issues.

Trigger Result

Operations	Description
Modify network parameters	Parameters used for video preview

Set the parameters for video preview.

Copyright © 2024 ARMATURA LLC. All rights reserved



Protocol Type: Select the TCP or UDP protocol depending on the type of connected device, such as WebSocket, WebRTC, or HTTP FLV. The default protocol is TCP.

Stream Type: The selectable options include **[Don't Assign]**, **[Main Stream]**, **[Sub Stream 1]**, and **[Sub Stream 2]**.

Device List

Prerequisites for Use

For third-party integrated systems, the parameter configuration must be properly connected and enabled.

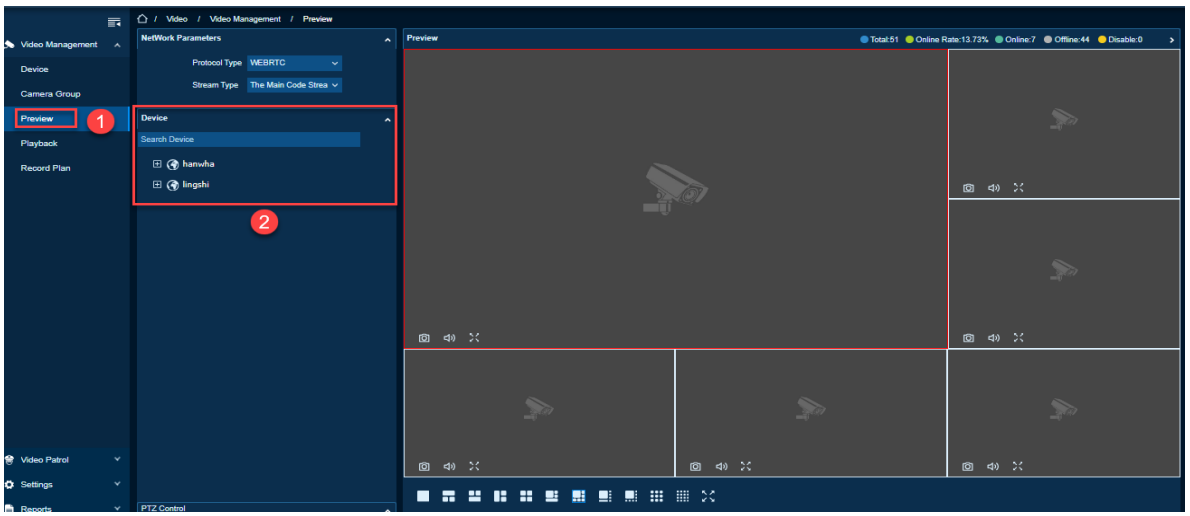
Usage Scenarios

To view the current device information, double-click the camera in the list to preview its details.

Trigger Result

Operations	Description
Double-click the device list	In the video preview window, select the pane to play and preview the video.

Copyright © 2024 ARMATURA LLC. All rights reserved



Device list: The device list is organized in a tree structure by area. Device status is represented by icon colors: gray for offline devices, white for online devices, and green for devices currently in preview. To locate a specific device quickly, use the search box to enter its name.

PTZ Control Panel

Prerequisites for Use

For third-party integrated systems, ensure parameter configurations are properly set and enabled. No additional player plugins are required. Upon first use, the third-party VMS webpage will prompt users to enter their VMS account credentials for authentication. Video content can only be previewed normally after successful authentication. Additionally, the camera must support the necessary playback functionality to display the video stream.

Usage Scenarios

Users can utilize the PTZ (Pan-Tilt-Zoom) controls to adjust or reposition the camera view as needed.

Trigger Result

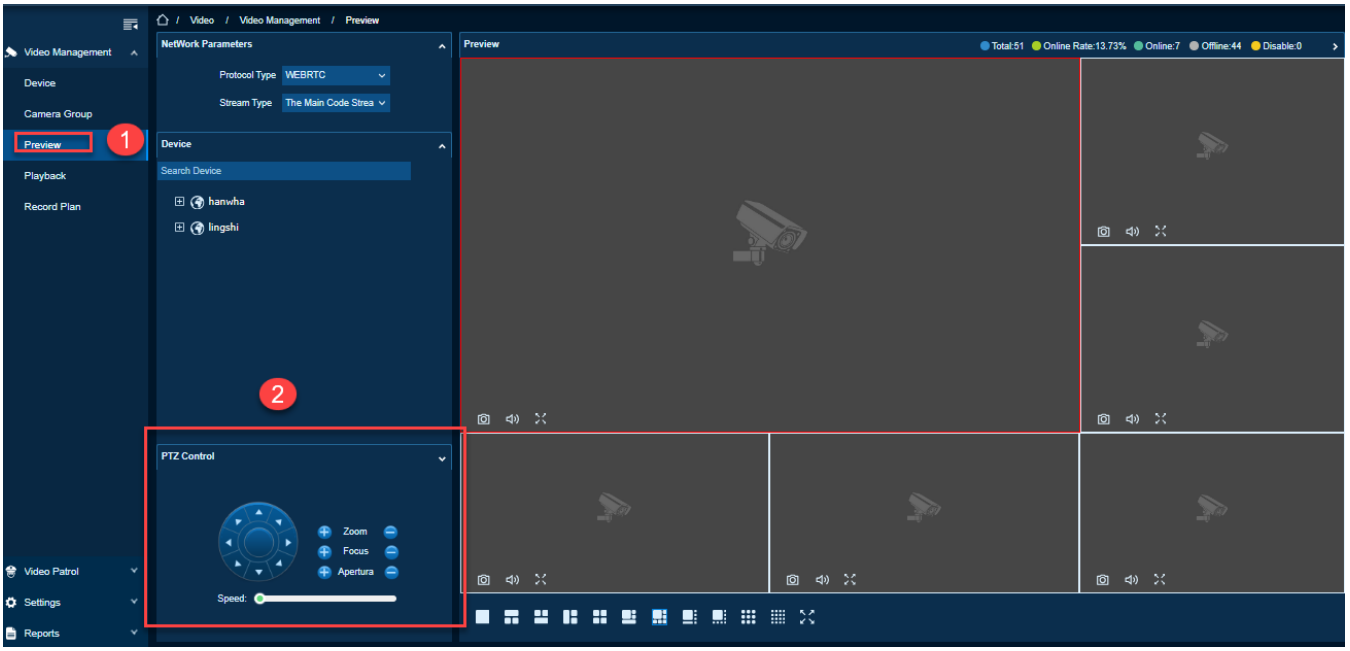
Operations	Description
PTZ Control	While the video is playing, users can adjust the camera's vertical and horizontal angles using tl Pan-Tilt-Zoom controls.

PTZ control panel:

- Select the camera that supports PTZ control in the preview box on the right to control the camera in the PTZ panel.
- The direction adjustment button allows user to change the camera's viewing angle in 8 different directions.
- The lens adjustment button allows user to zoom in and out the lens distance.

Copyright © 2024 ARMATURA LLC. All rights reserved

- The focal length adjustment button allows user to adjust the clarity of the lens by zooming in and out.
- The Apertura adjustment button allows user to adjust the image sharpness and it controls exposure, amount of light that enters user camera.
- The speed bar controls the lens viewing angle's movement speed, which is useful for both large-scale movement and fine-scale fine-tuning.



Device Status Bar

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

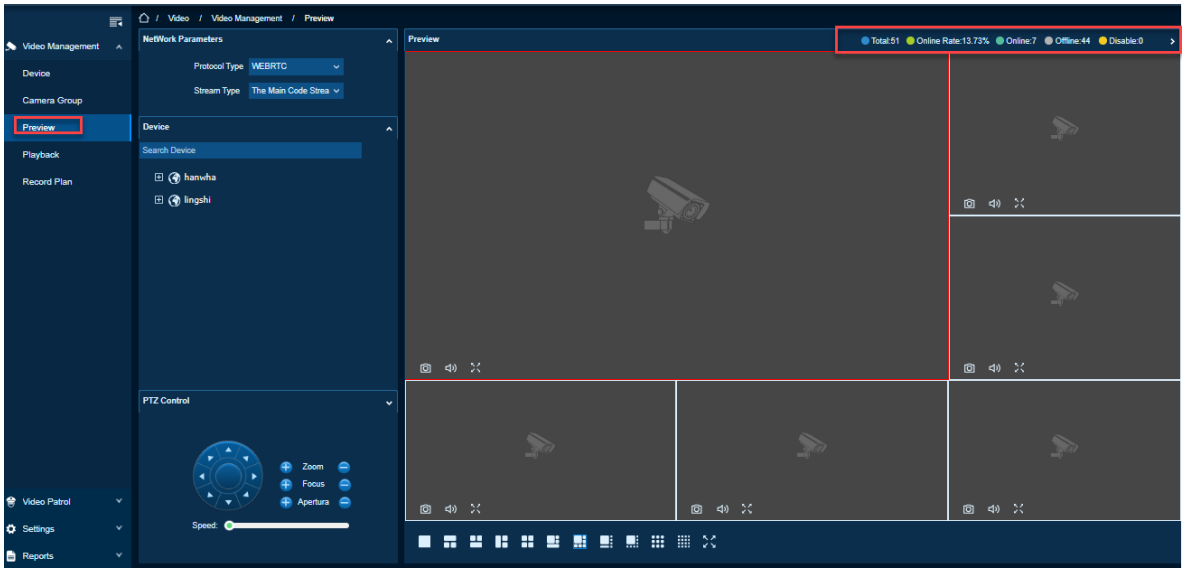
Checking the status of the device.

Trigger Result

Operations	Description
Enter the Page	View statistics about the online status of the devi

It displays the basic conditions and statistics of all connected devices.

Copyright © 2024 ARMATURA LLC. All rights reserved



Preview Window

Prerequisites for Use

For third-party integrated systems, ensure that parameter configuration is correctly set up and enabled. No additional player plugins are required. Upon first use, a third-party VMS webpage will prompt users to enter their VMS account credentials for authentication. Video content can only be previewed after successful authentication.

Usage Scenarios

Users can view and play camera feeds, including across multiple windows.

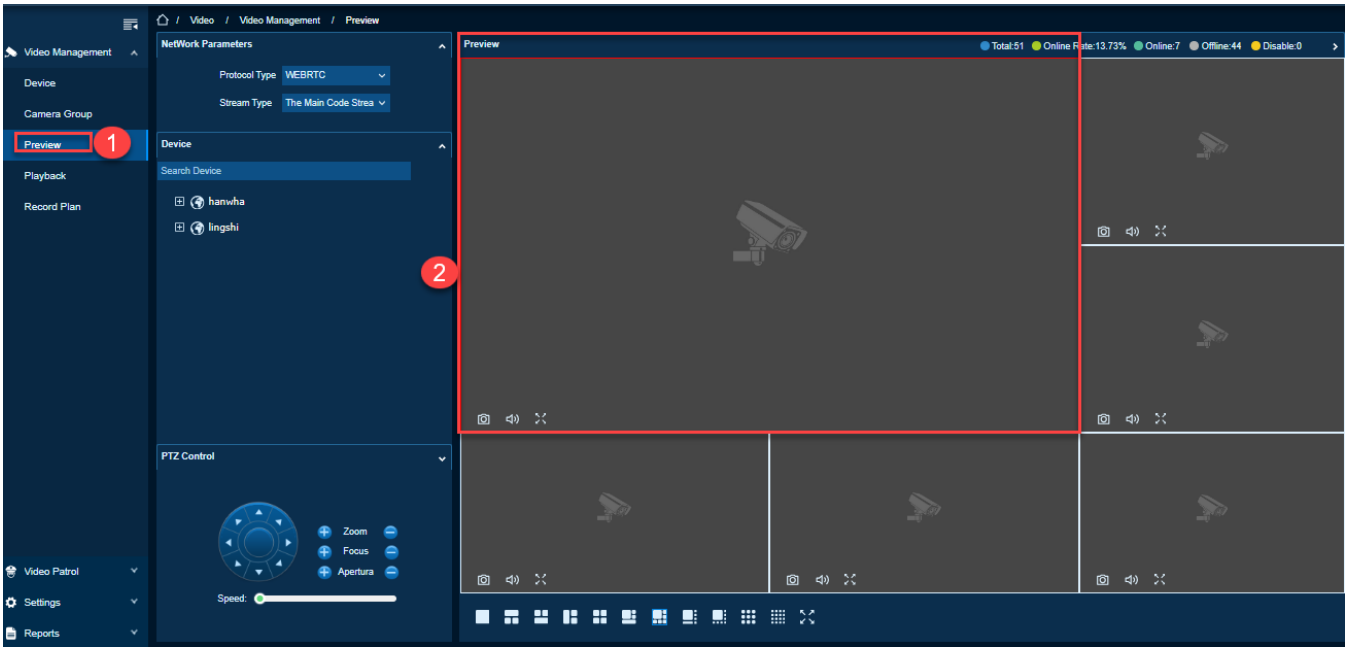
Trigger Result

Operations	Description
Close pane	Video preview stopped
Multi-pane switching	Video preview pane adjustment

Preview window:

- Play and select the desired camera for preview.
- Control the number of video panes displayed simultaneously, with support for adjustments ranging from 1 to 16 panes.
- Use the full-screen button to display the preview window in full-screen mode.
- The preview pane supports screen capture, and PTZ cameras can be controlled using the PTZ direction adjustment buttons on the playback pane.

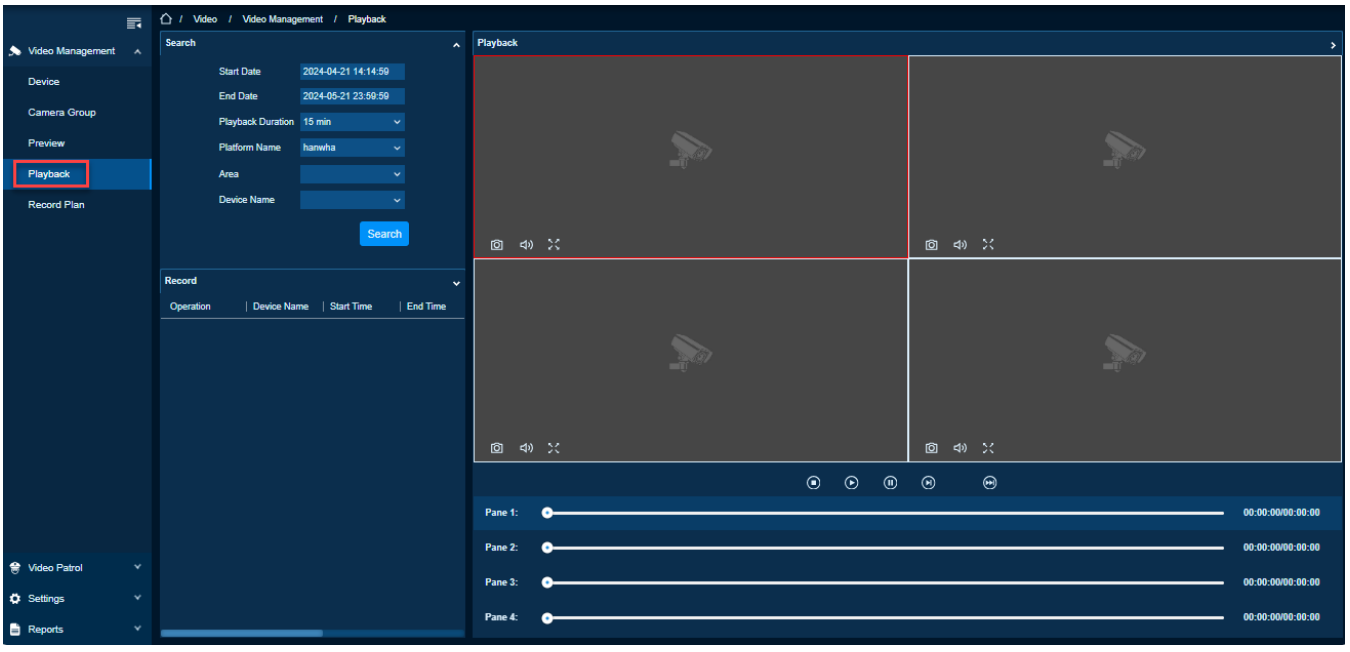
Copyright © 2024 ARMATURA LLC. All rights reserved



9.1.3 Playback

Function Description

Recorded content can be played back by retrieving videos based on the specified time and camera under this menu option. Click **[Video Management] > [Playback]** to access the playback interface, which is composed of three parts.



Search Window

Prerequisites for Use

For third-party integrated systems, ensure that parameter configuration is correctly set up and enabled. No additional player plugins are required. Upon first use, a third-party VMS webpage will prompt users

Copyright © 2024 ARMATURA LLC. All rights reserved

to enter their VMS account credentials for authentication. Video content can only be previewed after successful authentication.

Usage Scenarios

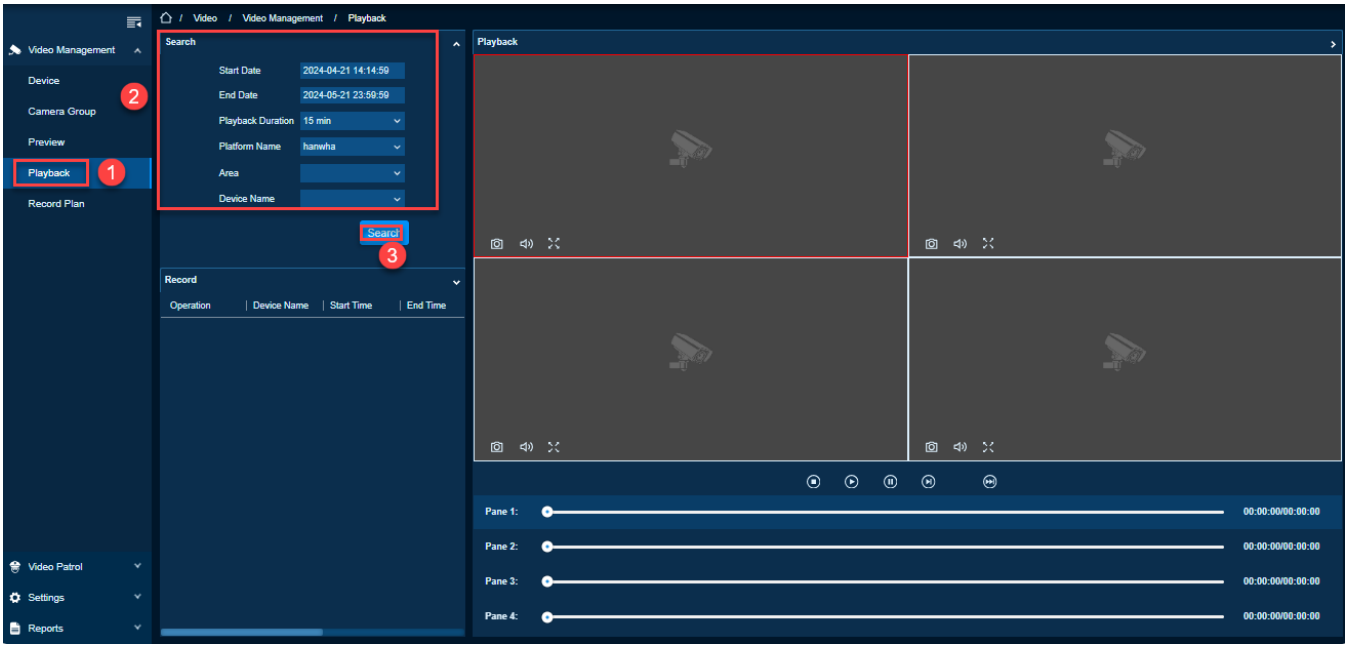
Users can search video recordings using specific conditions to locate footage quickly.

Trigger Result

Operations	Description
Search	Retrieve recording data that matches the specified conditions.

Search Window:

- Select the start and end time of the playback video.
- Select the playback duration.
- Select the platform to view. Supports multiple selection and one-click selection.
- Select the area and device name that the user wants to view.
- The video mode allows selection between platform video and front-end video content. The choice is based on the video storage mode defined in the Video Plan, with platform video set as the default.



- After configuring the parameters, click the **[Search]** button to display the search results in the video record pane.

Copyright © 2024 ARMATURA LLC. All rights reserved

Video Recording Pane

Prerequisites for Use

For third-party integrated systems, ensure that parameter configuration is correctly set up and enabled. No additional player plugins are required. Upon first use, a third-party VMS webpage will prompt users to enter their VMS account credentials for authentication. Video content can only be previewed after successful authentication.

Usage Scenarios

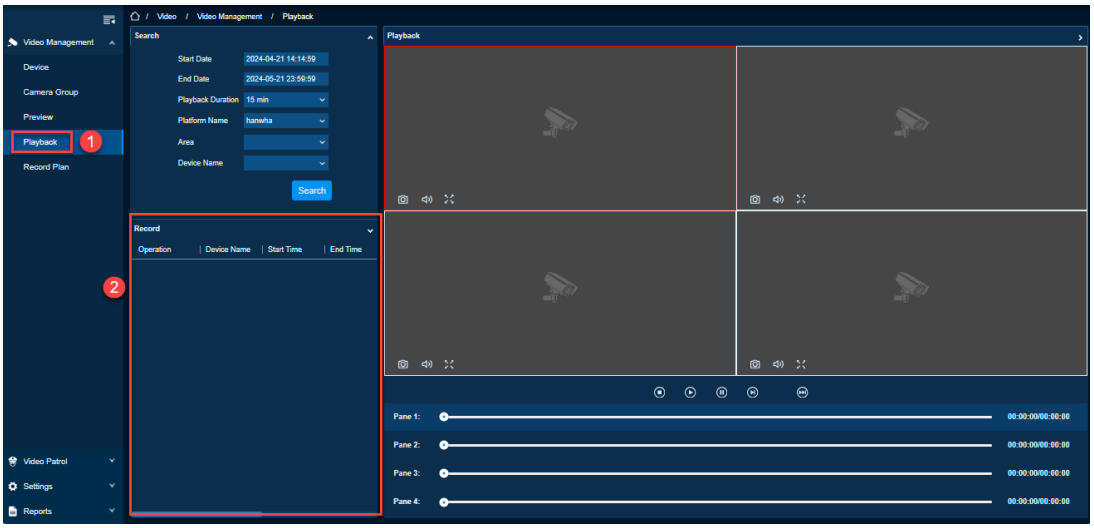
Playback and video download operations need to be performed on the retrieved video.

Trigger Result

Operations	Description
Video playback	Play back the recorded video.
Video download	Download the video recording

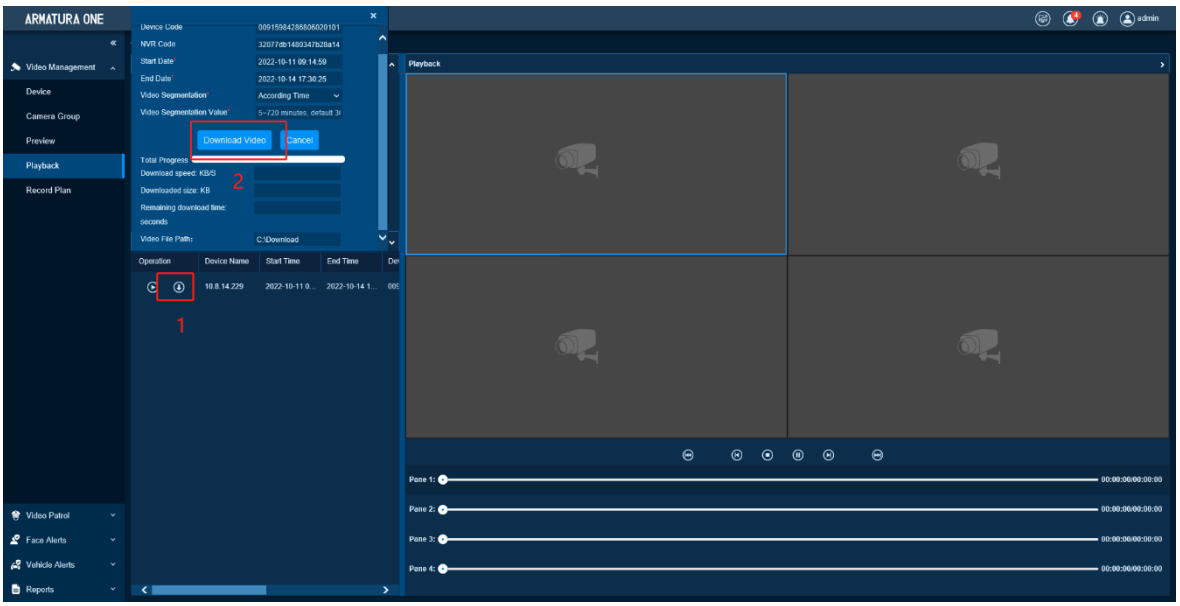
Video record pane:

- Click the **[Search]** button to display the current records.



- Click the **[Download Video]** button to open the video download interface.

Copyright © 2024 ARMATURA LLC. All rights reserved



Video Download Interface: Displays the information of the video record.

Video Segmentation: Allows users to download videos based on time length. The default duration is 30 minutes, with options ranging from 5 to 720 minutes.

Videos can be downloaded based on storage size, with a default size of 2048 MB. Users can choose sizes ranging from 200 MB to 3072 MB.

Click the **[Download Video]** button to start downloading the video. The download progress will be displayed below the playback window.

Video Playback Pane

Prerequisites for Use

For third-party integrated systems, ensure that parameter configuration is correctly set up and enabled. No additional player plugins are required. Upon first use, a third-party VMS webpage will prompt users to enter their VMS account credentials for authentication. Video content can only be previewed after successful authentication.

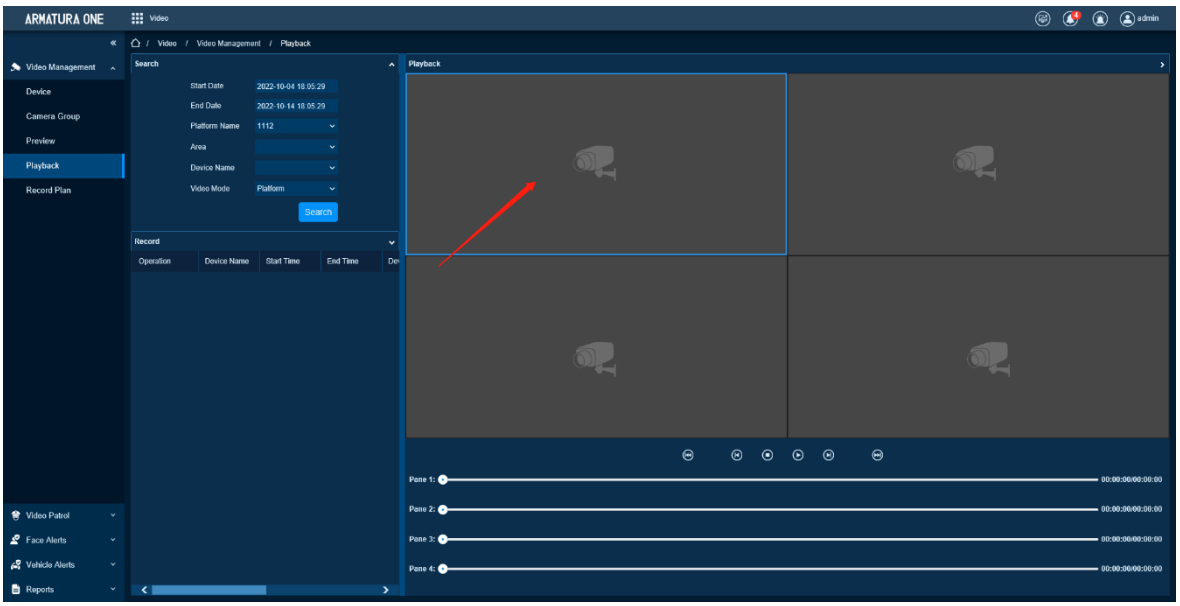
Usage Scenarios

Control video playback and enable viewing in multiple panes.

Trigger Result

Operations	Description
Playback	Control the video playback.

Copyright © 2024 ARMATURA LLC. All rights reserved



Video Playback Pane: Supports simultaneous playback of up to 4 video channels.

Control Bar: Control video playback speed with the following options: slow rewind and slow forward playback at a minimum speed of 1/32x, fast rewind and fast forward playback at a maximum speed of 32x, pause, and stop playback.

Progress Bar: Displays the current playback time and total duration of the video, with support for dragging to fast forward or rewind playback.

9.2 Settings

Configuration and management of the connection interface with Arteco's OMNIA software.

Function List

Operations	Description
Arteco Connector	View all connector names and IDs

9.2.1 Arteco Connector

Function Description

View the data for all connector names, IDs, and Web device IDs.

Arteco Connector

Prerequisites for Use

Arteco connector data must be available.

Usage Scenarios

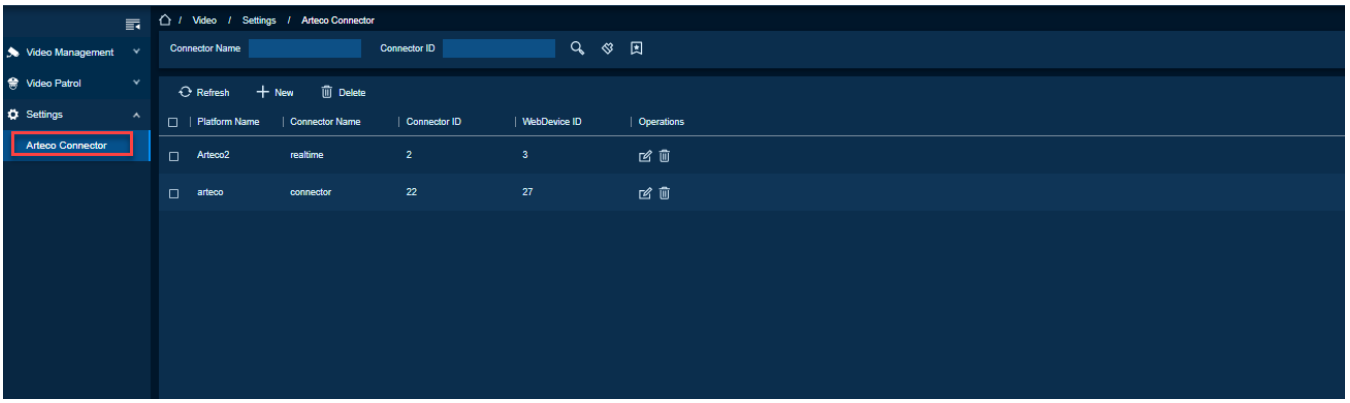
When querying Arteco connector data is required

Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Operations	Description
Enter the Page	Display Arteco Connector data.

Click **[Arteco Connector]** button to view the detailed data of the Arteco Connector.



Add Connector

Usage Scenarios

Add the required connector.

Trigger Result

Operations	Description
Add connectors	Add the required connectors

Platform Name: Use the drop-down menu to select the platform name. Alternatively, type the platform name in the search bar or choose it from the list. Once selected, click **[OK]**.

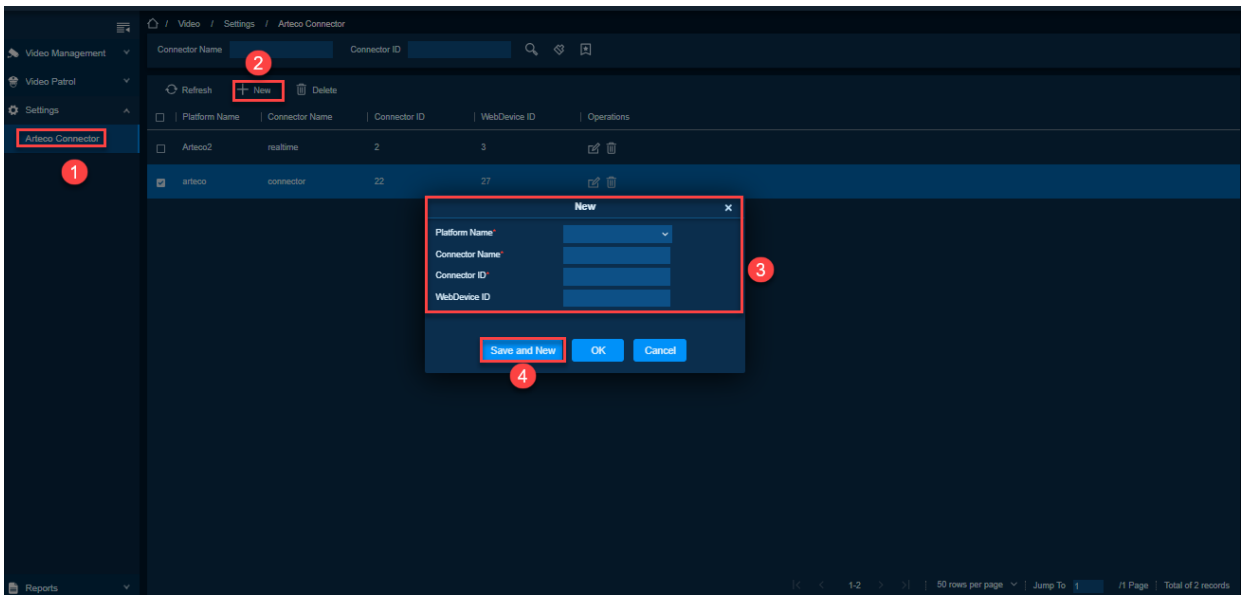
Connector Name: Enter the connector name.

Connector ID: Enter the connector ID.

Web Device ID: Enter the Web Device ID.

1. To add a connector, click **[New]**, and a new window will pop up.

Copyright © 2024 ARMATURA LLC. All rights reserved



2. In the pop-up window, select **[Arteco]** from the **[Platform Name]** dropdown menu.
3. Enter the connector's name and its corresponding Connector ID, ensuring that it matches exactly with the Connector ID listed in Arteco Omnia.
4. Once the user has completed these steps, click the **[OK]** button to save the settings

Delete Connector

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

Remove unused connectors and delete their associated data.

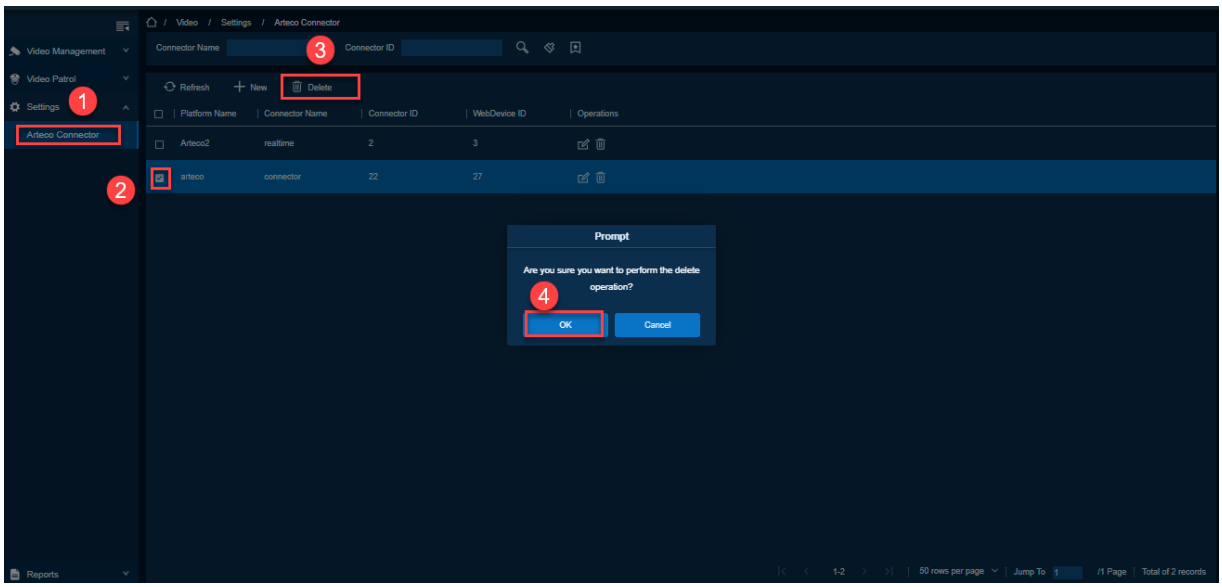
Trigger Result

Operations	Description
Delete Connector	Delete the Arteco connector

Steps:

- Select the connector to be deleted and click the **[Delete]** button.
- Click **[OK]** to delete.

Copyright © 2024 ARMATURA LLC. All rights reserved



9.3 Reports

Function List

Operations	Description
Video Event Recording	View the related records of video snapshots and videos.
Camera Alarm Record	View all video alarm records, manually add, and export alarm records.
Patrol Report	View the patrol records of the patrol staff.
Patrol Warning	View the information reported during the patrol.

Copyright © 2024 ARMATURA LLC. All rights reserved

9.3.1 Video Event Record

Function Description

View related records of video equipment's snapshots and videos.

Video Event Recording List

Prerequisites for Use

The equipment has snapshot data.

Usage Scenarios

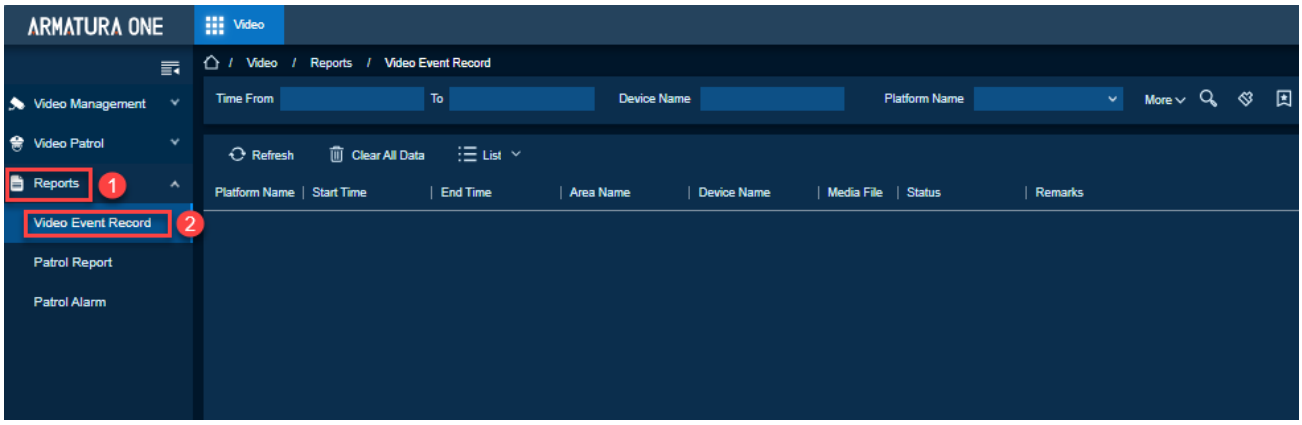
Querying video event recording data.

Trigger Result

Operations	Description
Enter the Page	Display the event recording data.

Copyright © 2024 ARMATURA LLC. All rights reserved

View the related records of video snapshots and video footage.



Introduction of media file classification:

: Indicates that in the linkage settings of access control or elevator control, the selected video linkage type is 'Recording.' Click to download the video.

: Indicates that in the linkage settings of access control or elevator control, the selected video linkage type is 'Capture.' Click to preview the image file.

Note:

If the user selects both 'Video' and 'Capture' at the same time, two separate records will be generated. For the specific setting method, please refer to the Linkage Settings and Global Linkage sections above.

Copyright © 2024 ARMATURA LLC. All rights reserved

10 Data Monitor

Contains data analysis for each module, including statistics for basic report types and report data analysis. Through statistical charts, events can be visualized, and the chart data can be further analyzed.

10.1 Data Chart

Function List

Functions	Description
Data Chart	View, export and download chart-related data for acce control, visitor, office, personnel, video, and system modules

10.1.1 Base Chart

Function Description

View the chart data for the access control, visitor, office, personnel, video, and system modules, with the data graphically displayed in chart form. By clicking on the event list on the left or right, the chart for the corresponding event will be displayed. You can also export, download, or close the data for each chart.

Access Chart

Prerequisites for Use

Log into the system using an account with the required permissions.

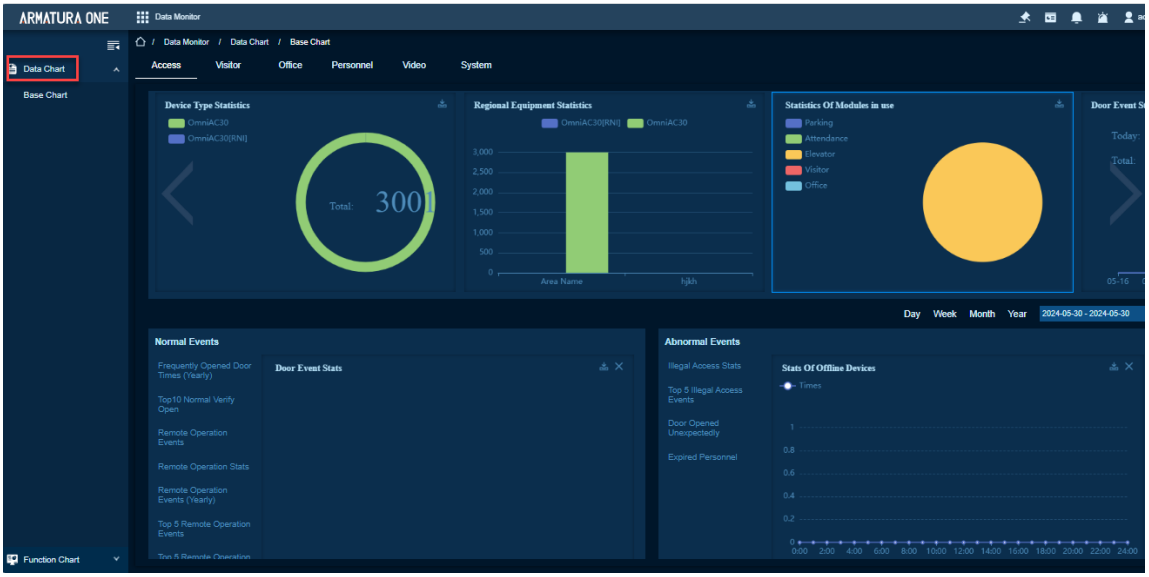
Usage Scenarios

Administrators or users need to view the overall data of the corresponding module.

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Access]** in the Action Menu to display the following interface:

Copyright © 2024 ARMATURA LLC. All rights reserved



- **Overview:** The charts in the overview represent the key and generalized data for the entire access control module and include the following charts:

Device Type Statistics: Displays statistics on the various device types added to the access control module.

Regional Equipment Statistics: Displays statistics on the types of equipment across different regions.

Statistics of Modules in Use: Displays statistics on devices added to the access control module that are used in other modules.

Door Event Statistics: Displays statistics on door openings for the last 15 days.

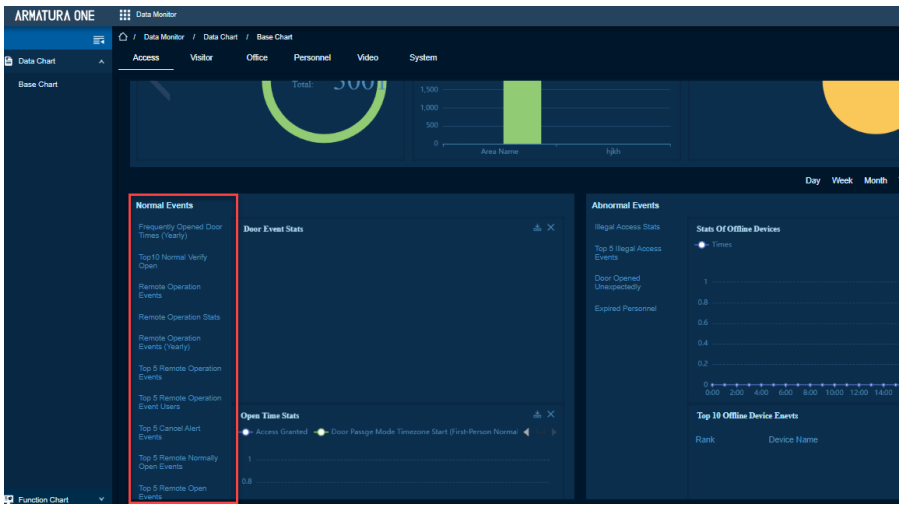
Remote Operation Statistics: Displays statistics for remote operations over the last 15 days.

Normal Events: Normal events can be selected using the time control for day, week, month, or year, or based on the normal access control event data graph for the corresponding timetable.

Steps:

- Click **[Data Monitor] > [Data Chart] > [Base Chart] > [Access]** in the Action Menu, and the chart will be displayed at the top of the normal class of events. Before the chart is moved down, the remaining chart functions remain the same, as shown in the figure.

Copyright © 2024 ARMATURA LLC. All rights reserved



Door Opening Event Statistics: Displays the proportion of each door opening event in the timetable, including normal verification to open the door, first person to open the door, multiple people opening the door, door button activation, emergency password access, and remote door opening.

Door Opening Statistics: Displays statistics on the number of individual door opening events within the timetable.

Number of Openings: Statistics comparing the number of door openings in the current timetable with the previous timetable.

Top 5 Door Opening Devices: Statistics on the top five devices with the highest number of door openings in the current timetable.

Top 5 Low-Frequency Door Openings: Statistics on the top five devices with the lowest frequency of door openings in the current timetable.

Normal Verification Door Opening Frequency: Statistics on the frequency of normal verification door openings in the current timetable.

Top 10 Normal Verification Door Openings: Statistics on the top 10 devices with the most normal verification door openings in the current timetable.

Number of Remote Operations: Statistics on the total number of remote operations in the current timetable, including remote open, close, lock, and unlock.

Remote Operation Statistics: Statistics on the percentage of remote operations in the current timetable.

Remote Operation Comparison: Statistics comparing the number of remote operations in the current timetable to the previous timetable.

Top 5 Remote Operations Devices: Statistics on the top five devices with the most remote operations in the current timetable.

Top 5 Remote Operation Users: Statistics on the top five users performing remote operations in the current timetable.

Top 5 Cancelled Alarms: Statistics on the top five devices with the highest number of cancelled alarms in the current timetable.

Copyright © 2024 ARMATURA LLC. All rights reserved

Top 5 Remote Normally Open Devices: Statistics on the top five devices with the most remote normally open operations in the current timetable.

Top 5 Remote Door Openings: Statistics on the top five devices with the highest number of remote door openings in the current timetable.

Regional Equipment Alarms & Handling: Statistics on the number of equipment alarms and the number of alarms handled by system personnel in the current timetable.

Top 10 Permission Group Configurations: Statistics on devices with the most permission groups configured in the current timetable.

Unauthorized Devices: Statistics on devices that are not configured with permission groups in the current timetable.

- **Abnormal Events:** Abnormal events can be selected using time controls for day, week, month, or year, or by using the abnormal access control event data graph for the corresponding timetable. This includes the following:

Offline Statistics: Counts the total number of times the device has gone offline during the current timetable.

Top 10 Offline Devices: Statistics on the top ten devices with the most offline occurrences during the current timetable. Devices with frequent offline issues can be recommended for maintenance or regular checks.

Excessive Temperature Statistics: Statistics on instances of excessive temperature in the current timetable.

Overheated Individuals: Statistics on individuals with high body temperature during the current timetable.

Illegal Access Statistics: Statistics on instances of illegal access within the current timetable.

Top 5 Illegal Access: Statistics on the top five individuals involved in illegal access during the current timetable.

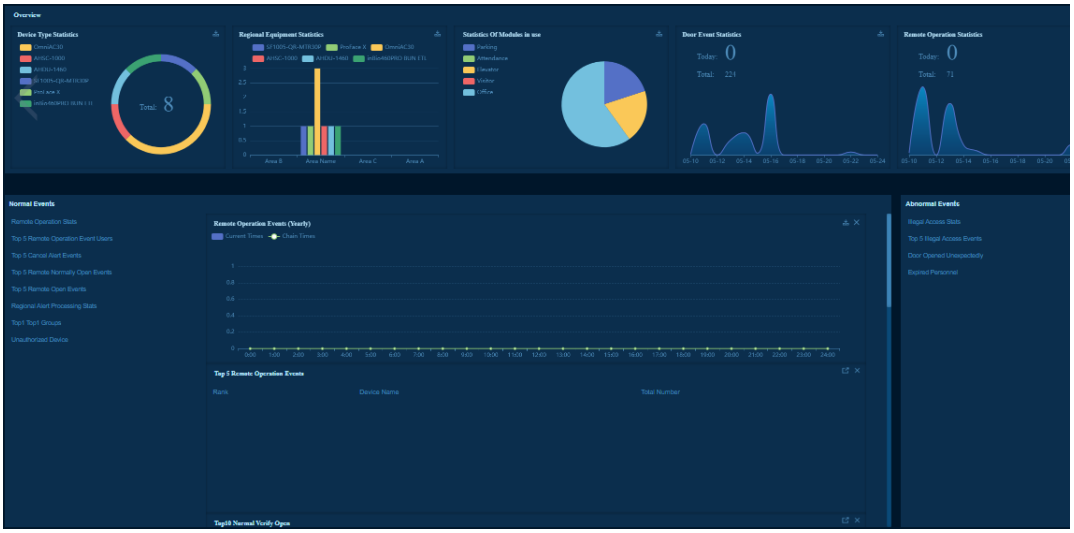
Accidental Door Openings: Statistics on the number of accidental door openings during the current timetable.

Expired Personnel: Statistics on personnel whose access has expired in the current timetable, making it easier for administrators to take action.

Close Chart

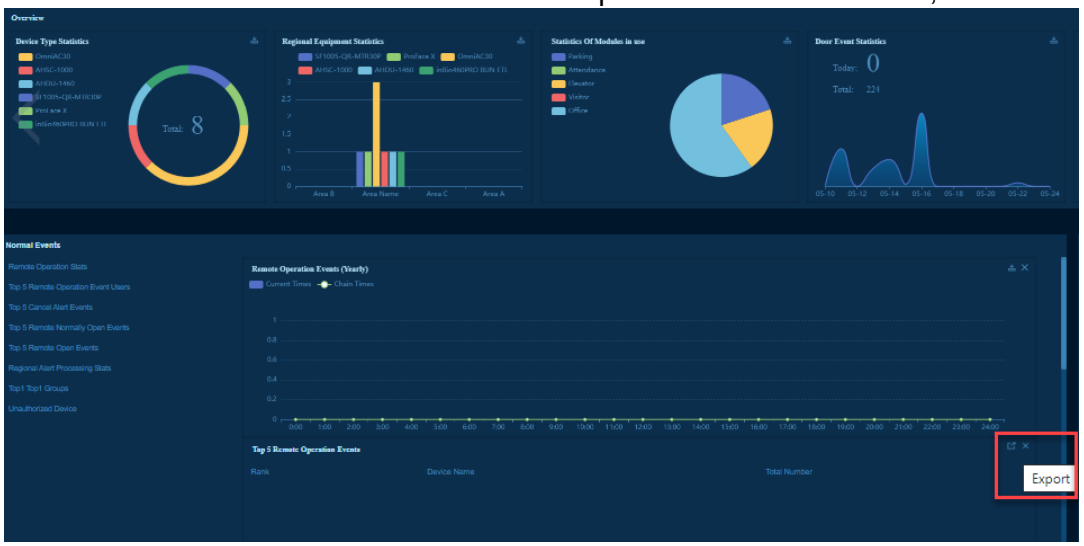
- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Access]**, and the following interface will be shown.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export

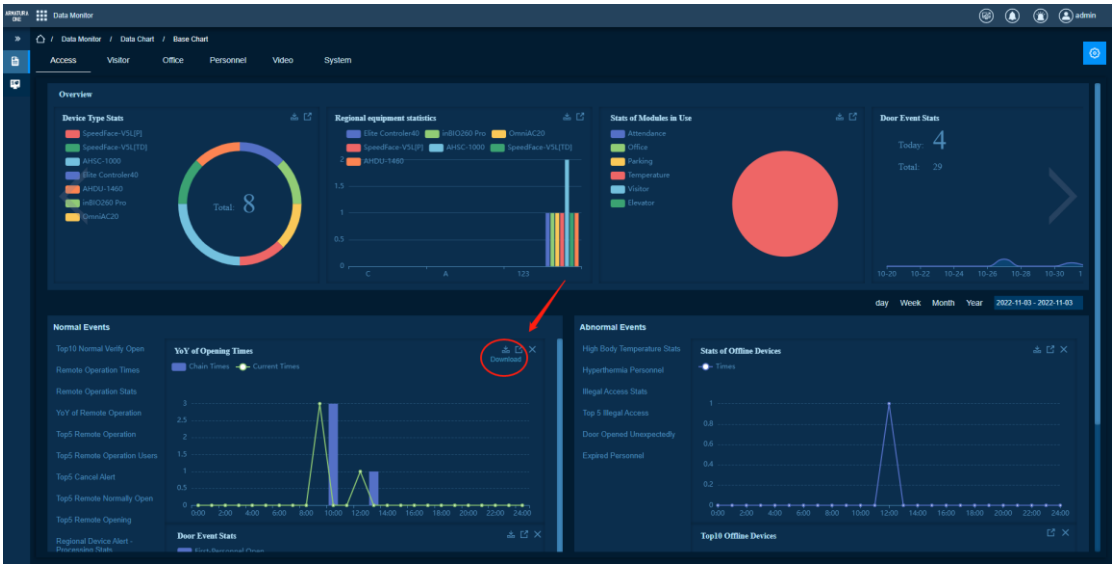
- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Access]**, and the export button in the chart retrieves the data source for this chart and presents it in tabular form, as shown below.



Download

- Click **[Data Monitor]** > **[Data Chart]** > **[Access]**, and the download button in the chart will allow you to download the chart in PNG format, as shown in the figure.

Copyright © 2024 ARMATURA LLC. All rights reserved



Visitor Chart

Prerequisites for Use

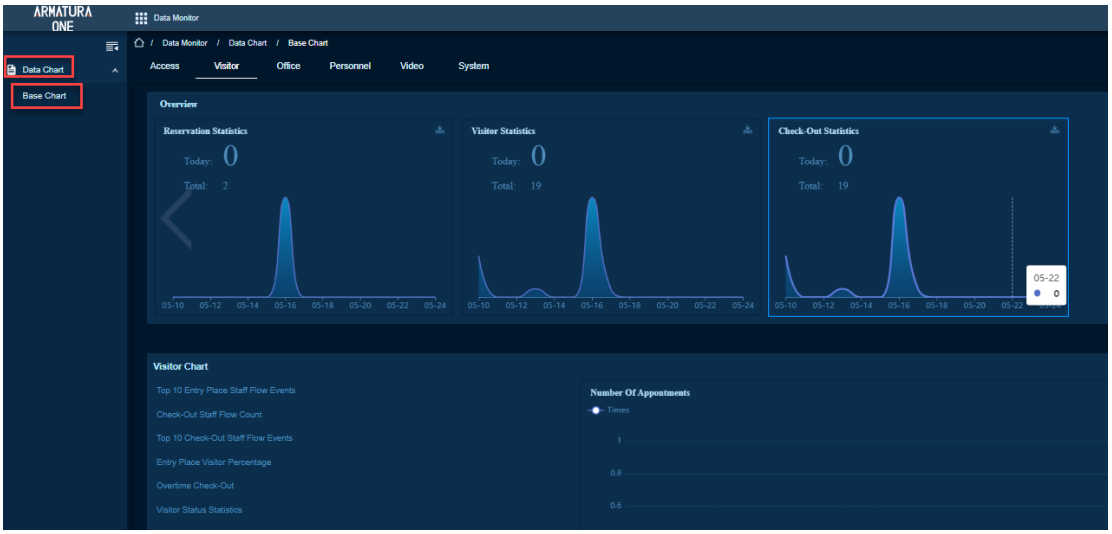
Log into the system using an account with the required permissions.

Usage Scenarios

Administrators or users need to view the overall data for the corresponding module.

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Visitor]** in the Action Menu, the following interface will be shown:



- **Overview:** The charts in the overview provide the most important and generalized data for the entire visitor module, including the following charts.

Reservation Statistics: Displays the number of reservations made in the last 15 days and today.

Visitor Statistics: Shows the number of visitors in the last 15 days and today.

Copyright © 2024 ARMATURA LLC. All rights reserved

Check-Out Statistics: Displays the number of sign-outs in the last 15 days and today.

- **Visitor Chart:** Visitor charts can be selected using time controls for daily, weekly, monthly, yearly, or corresponding timetable visitor event data charts. These include the following:

Number of Appointments: Statistics on the number of appointments made by visitors during the timetable.

Visitor Statistics: Statistics on the number of visitors during the timetable.

Top 10 Entry Place Staff Events: Information on the top 10 entry places for staff events in the statistical timetable.

Top 10 Check-Out Locations by Traffic Flow: The top 10 sign-out locations based on the number of sign-outs during the timetable.

Top 10 Registered Locations by Visitor Traffic: Information on the top 10 registered locations based on the number of visitors during the statistical timetable.

Sign-Out Location Traffic: Statistics on the number of people signing out during the timetable.

Sign-Out Timeout Personnel: Statistics on personnel who have exceeded the sign-out time within the timetable.

Visitor Status Statistics: Statistics on the number of registered, signed-out, and remaining unsigned-out individuals during the timetable.

Office

Prerequisites for Use

Log into the system using an account with the required permissions.

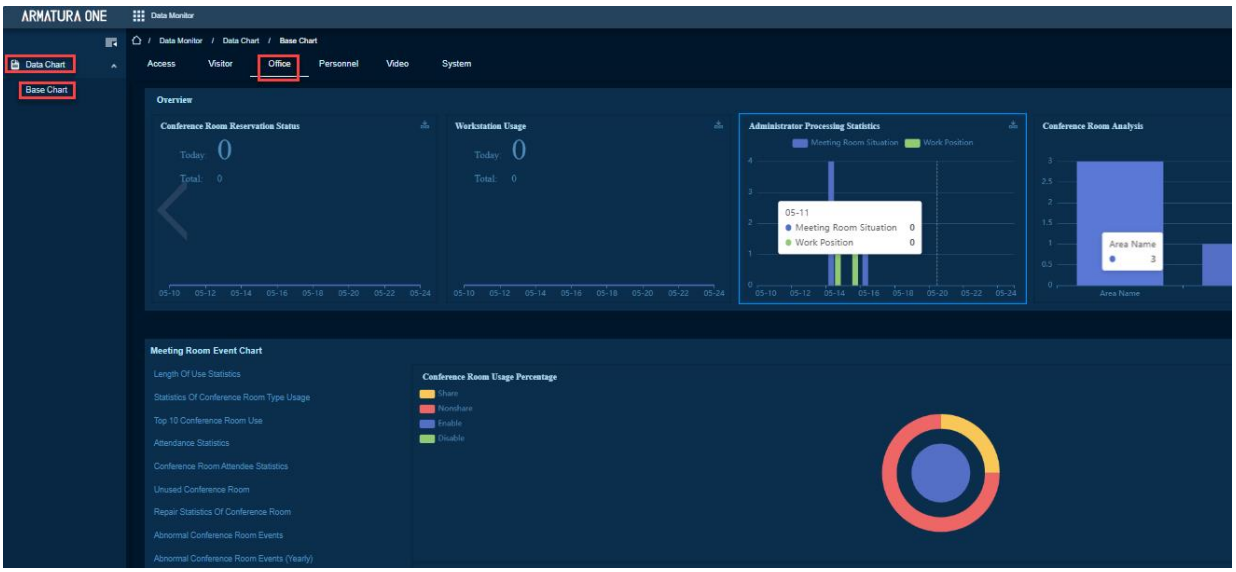
Usage Scenarios

Administrators or users need to view the overall data of the corresponding module.

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Office]** in the Action Menu, the following interface will be shown.

Copyright © 2024 ARMATURA LLC. All rights reserved



- **Overview:** The charts in the overview provide important and general data for the entire office module, including the following charts:

Meeting Reservation Status: Counts the number of meeting rooms reserved in the last 15 days and today.

Station Usage: Statistics on the usage of stations in the last 15 days and today. Usage is counted from the moment of occupation.

Manager Processing Statistics: Statistics comparing the processing of repair reports in conference rooms with the processing of repair reports by station area administrators.

Conference Room Statistics: Counts the number of conference rooms in each region.

Station Statistics: Counts the number of stations in each region.

- **Meeting room event Chart:** The meeting room event chart allows you to select day, week, month, year, or corresponding timetable meeting room event data through time control. This includes the following:

Proportion of Meeting Room Usage: Counts the number of available/unavailable meeting rooms, and the number of shared/non-shared meeting rooms.

Conference Room Reservation Statistics: Counts the number of reservations for each conference room within the timetable.

Usage Time Statistics: Tracks the usage time of each meeting room within the timetable (excluding the day, with usage starting from the beginning of the week and from the moment of occupation).

Conference Room Type Usage Statistics: Statistics on the usage time of shared/non-shared conference rooms within the statistical timetable (usage is calculated weekly, excluding days).

Top 10 Meeting Room Usage: Lists the top ten most used meeting rooms in the statistical timetable.

Participants Statistics: Counts the number of participants during the statistical timetable (including both participants and reservations).

Copyright © 2024 ARMATURA LLC. All rights reserved

Conference Room Participant Statistics: Tracks the number of participants in each conference room during the statistical timetable.

Unused Meeting Rooms: Lists information on unused meeting rooms during the statistical timetable.

Conference Room Repair Report Statistics: Counts the number of repair reports for meeting rooms during the statistical timetable.

Timetable Repair Report Statistics: Statistics on the repair report status of each conference room during the timetable.

Abnormal Meeting Rooms: Information on meeting rooms under repair or maintenance within the statistical timetable.

Repair Report Statistics for Abnormal Meeting Rooms: The total number of repairs reported for meeting rooms during the statistical timetable, and the ratio of repairs compared to the previous period.

Top 10 Repair Request Handlers: The top ten administrators who processed meeting room repair requests during the statistical timetable.

- **Workstation event Chart:** The station event chart can be used to select the day, week, month, year, or the station event data chart in the corresponding Timetable through the time control, including the following content:

Proportion of station usage: the number of station usage in each area during the statistical Timetable (counted once from the start of activation).

Usage time statistics: Statistics on the usage time of stations in the Timetable (calculated once from the beginning of occupation).

Usage time statistics: Statistics on the usage time of stations in the Timetable (calculated once from the beginning of occupation).

Station repair statistics: Count the number of station repair requests during the statistical Timetable.

Abnormal workstations: Information about workstations that are in repair or maintenance within the statistical Timetable.

Top 10 of the workstation repair application handles: information about the top ten administrators in the number of processing times after the workstation repair application within the statistical Timetable.

Personnel

Prerequisites for Use

Log into the system using an account with the required permissions.

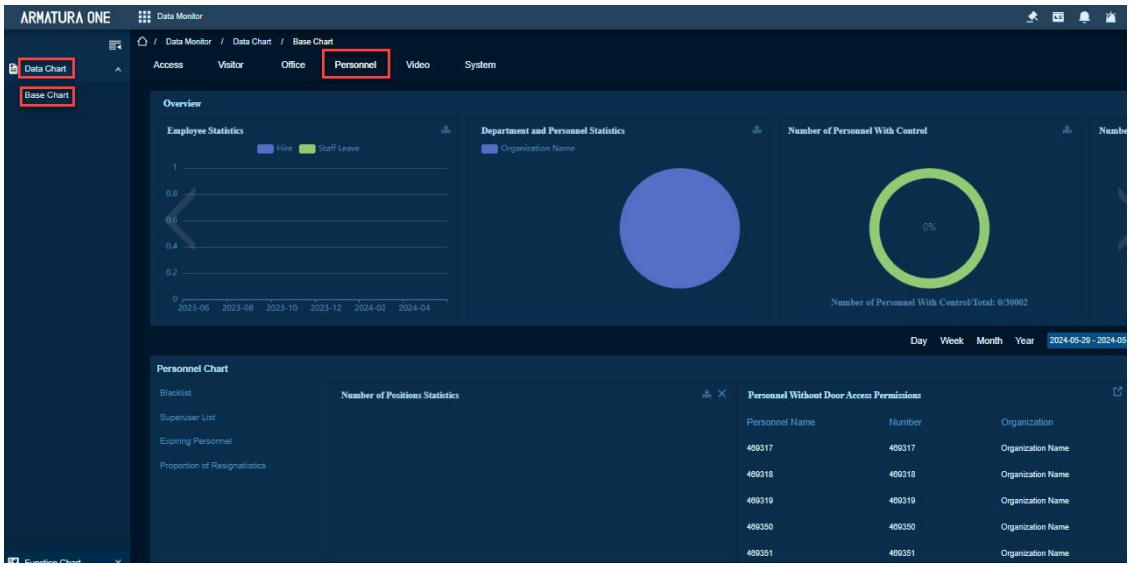
Usage Scenarios

Administrators or users need to view the overall data of the corresponding module.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Personnel]** in the Action Menu, the following interface will be shown.



- **Overview:** The charts in the overview provide important and general data for the entire personnel module, including the following charts:

Statistics of Recruited and Resigned Personnel: Counts the number of recruits and resignations within the last month.

Department and Population Statistics: Shows the proportion of people in each department.

Number of Deployed Controls: Counts the number of deployed controls relative to the total number of people.

Number of Background Verifiers: Displays statistics on the number of background verifiers relative to the total number of people.

Proportion of Men and Women by Age Group: Shows the proportion of men and women in each age group.

Employee's Working Age Ratio: Compares the ratio of men to women across different working age groups.

- **Personnel Chart:** The personnel event chart can be selected using time controls for day, week, month, year, or corresponding timetable personnel event data. This includes the following:

Persons Without a Card: Information on individuals without an authorized card number during the statistical timetable.

Persons Without Photos: Information on individuals without face avatars in the statistical timetable.

Banned Persons: Information on individuals on the banned list during the statistical timetable.

Super User List: Information on super users during the statistical timetable.

Copyright © 2024 ARMATURA LLC. All rights reserved

Persons Who Are About to Expire: A list of personnel whose credentials are about to expire (within five days) during the statistical timetable, sorted by the most recent expiration.

Proportion of Resignation Types: The proportion of resignation types during the statistical period, including resignation, dismissal, transfer, and self-resignation.

Persons Without Access Control Authority: Information on individuals without access control authority during the statistical timetable.

Video

Prerequisites for Use

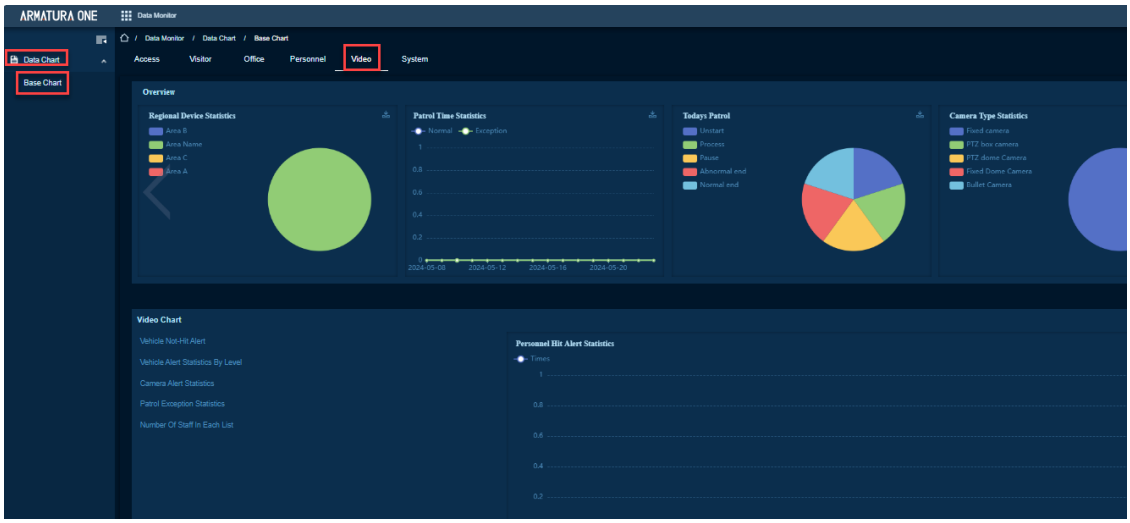
Log into the system using an account with the required permissions.

Usage Scenarios

Administrators or users need to view the overall data of the corresponding module.

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Video]** in the Action Menu, the following interface will be shown.



- **Overview:** The charts in the overview provide important and general data for the entire video module, including the following charts:

Regional Equipment Statistics: Counts the amount of equipment in each area.

Patrol Statistics: Counts the number of video patrols within the last 15 days (excluding today).

Today's Patrol Status: Displays statistics on today's patrol status, including not started, in progress, suspended, normal end, and abnormal end.

Camera Type Statistics: Counts the number of each camera type.

Personnel and Vehicle Alarm Statistics: Counts the number of personnel hit/non-hit and vehicle hit/non-hit alarms.

Copyright © 2024 ARMATURA LLC. All rights reserved

- **Video:** The video event chart allows you to select day, week, month, year, or the corresponding timetable video event data through time control. This includes the following:

Personnel Hit Alarm Statistics: The number of personnel hit alarms during the statistical timetable.

Personnel Non-Hit Alarm Statistics: The number of personnel non-hit alarms during the statistical timetable.

Alarm Statistics by Personnel Level: The number of alarms for each alarm level during the statistical timetable.

Vehicle Hit Alarm Statistics: The number of vehicles hit alarms during the statistical timetable.

Vehicle Non-Hit Alarm Statistics: The number of vehicle non-hit alarms during the statistical timetable.

Vehicle Alarm Statistics by Level: Statistics of the number of vehicle alarms for each alarm level during the statistical timetable.

Camera Alarm Statistics: Statistics on the number of each alarm type during the statistical timetable.

Abnormal Patrol Statistics: The number of incidents of no patrol, patrol alarms, and patrols not clocking in during the statistical timetable.

List Type Statistics: The number of individuals on each list (banned, allowed, red list) during the statistical timetable.

System

Prerequisites for Use

Log into the system using an account with the required permissions.

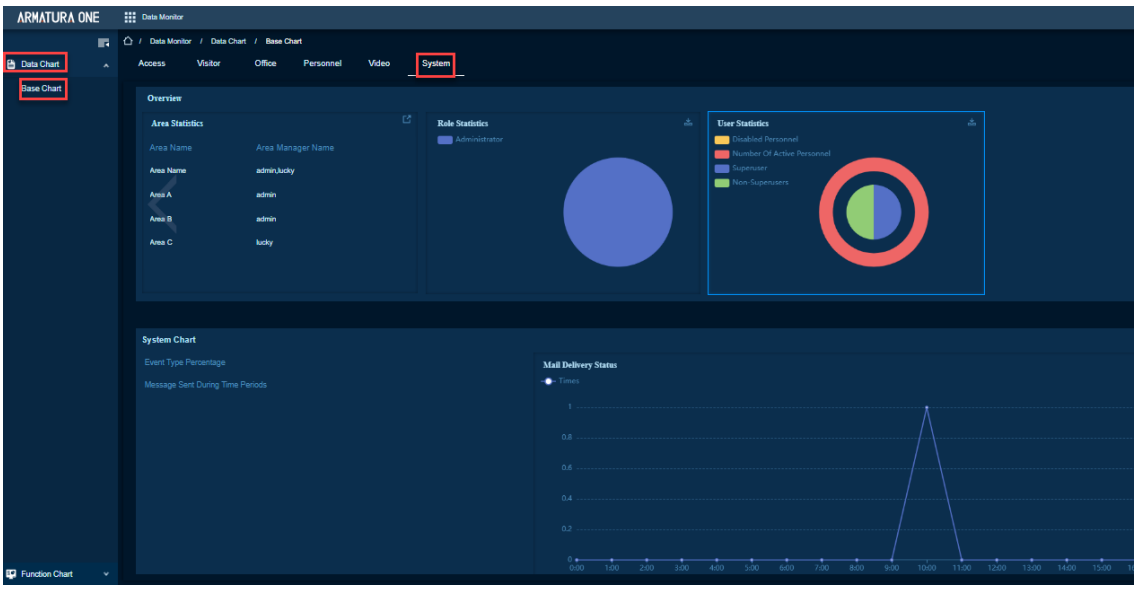
Usage Scenarios

Administrators or users need to view the overall data situation of the corresponding module.

Steps:

- Click **[Data Center]** > **[Data Chart]** > **[Base Chart]** > **[System]** in the Action Menu, the following interface will be shown.

Copyright © 2024 ARMATURA LLC. All rights reserved



- **Overview:** The charts in the overview provide important and general data for the entire system module, including the following charts:

Regional Statistics: Statistics on all the regions within the system module and their corresponding regional administrators.

System Roles: Counts the types of system roles and the number of corresponding personnel.

System User Statistics: Statistics on the number of disabled/non-disabled users and super users/non-super users.

- **System:** The system event chart allows you to select day, week, month, year, or corresponding timetable system event data through time control. This includes the following:

Mail Delivery Status: Counts the number of emails sent during the timetable.

Top 5 Email Subjects: Displays the top five email subjects in the statistical timetable.

Proportion of Platform Types Used: Counts the number of platforms used during the statistical timetable.

Message Status: Displays the number of each message status in the statistical timetable.

Proportion of Event Types: Statistics on event types from each module in the timetable. Click on a different module to display the event types for that module.

Number of Messages in Timetable: The number of system messages from each module during the statistical timetable.

10.2 Function Chart

Function List

Functions	Description
Alarm Manageme	Displays the system's alarm information in real-time usir charts.

Copyright © 2024 ARMATURA LLC. All rights reserved

10.2.1 Alarm Management

Function Description

View various alarms and alarm details, including access control alarms, face alert alarms, vehicle alert alarms, intrusion detection, tripwire detection, loitering detection, area entry detection, area exit detection, and fast movement detection, and perform alarm processing operations.

Overview

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

View all types of alarms in real-time.

Time Range

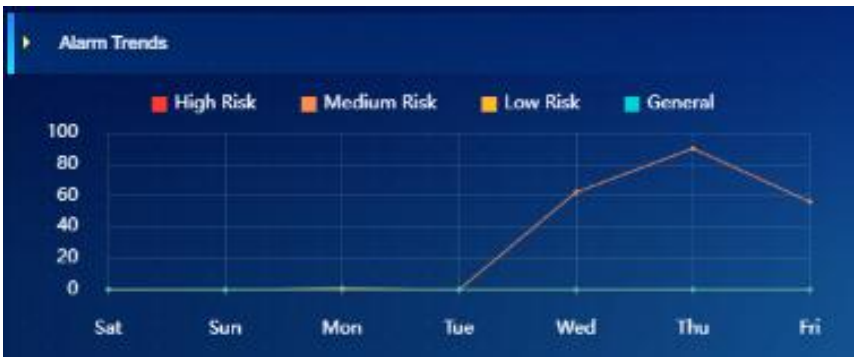
Select a different time period to set a custom time range for each chart.

The time period can be set to Week, Month, Season, or user-defined.

Alarm Trends

View the trend graph of alarms by different levels over the selected time range.

Copyright © 2024 ARMATURA LLC. All rights reserved



Alarm Type Statistics

Displays the number and percentage of different types of alarms for comparison.

Classification Statistics

Displays the number of different types of alarms. Hover over each alarm to view the components of each trigger event and their respective numbers.

Total Alarm

Displays the total number of alerts generated, pending, and processed.

Copyright © 2024 ARMATURA LLC. All rights reserved

Region Statistics

View the distribution of alarms across each area of the system.

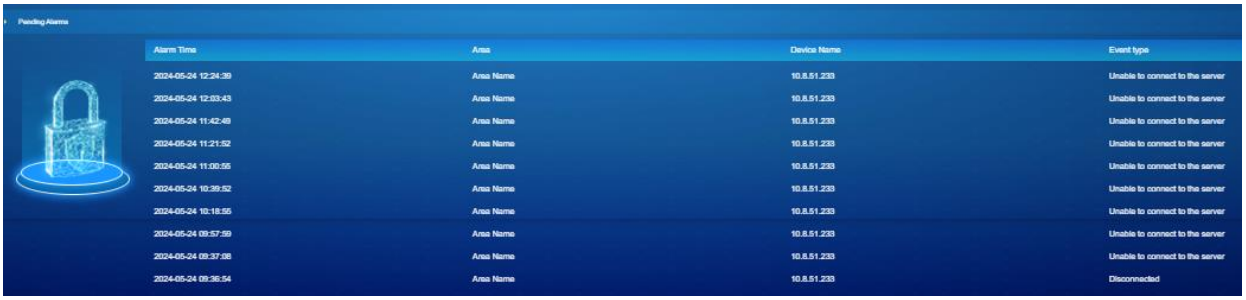
Type Statistics

Displays the different types of alarms by level.

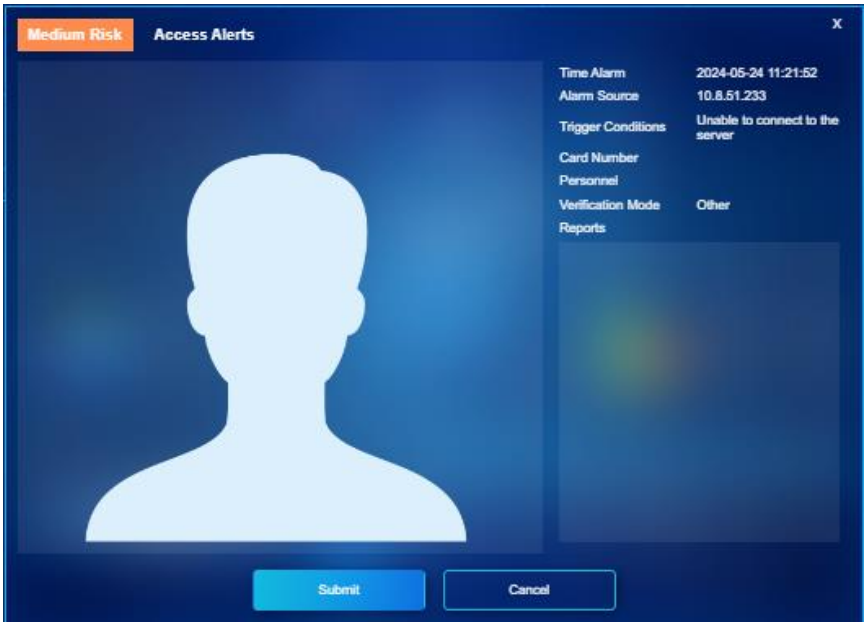
Pending Alarms

View pending alarms and their details.

Copyright © 2024 ARMATURA LLC. All rights reserved



Click **[Detail]** to view alarm details, enter text content, and click **[Submit]** to confirm the alarm.



Access Alert

Prerequisites for Use

Log into the system using an account with the required permissions.

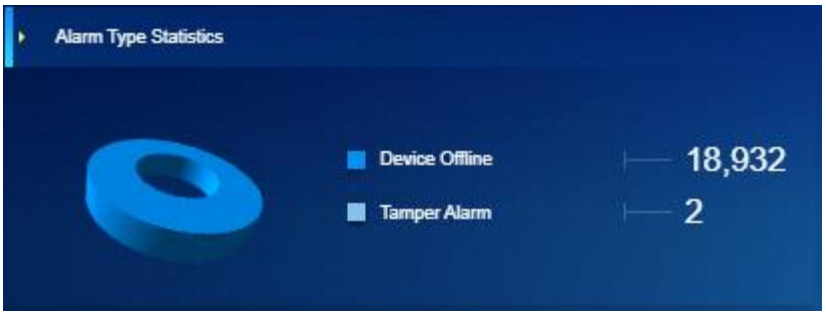
Usage Scenarios

View access alarms in real-time.

Copyright © 2024 ARMATURA LLC. All rights reserved

Alarm Type Statistics

View the composition and quantity of different access alarm types.



Type Statistics

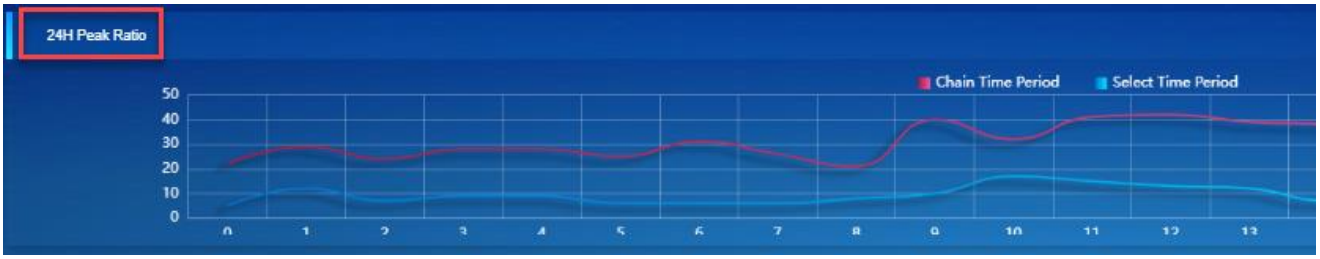
Display the types of each alarm level in the access control system.

Region Statistics

Display the number of access alarms in different areas of the system.

24H Peak Ratio

A graph comparing the number of alerts per hour over a period of time.



Copyright © 2024 ARMATURA LLC. All rights reserved

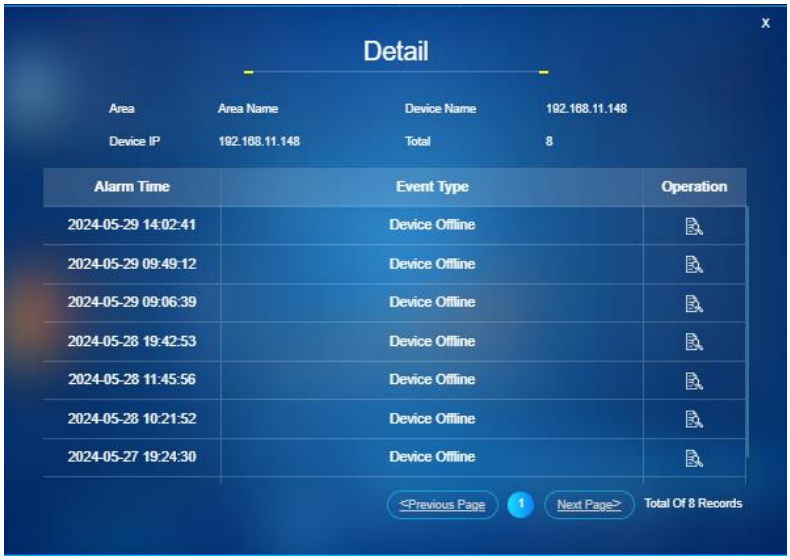
Time Period Peak

A graph comparing different access alarm levels over a specified period of time.

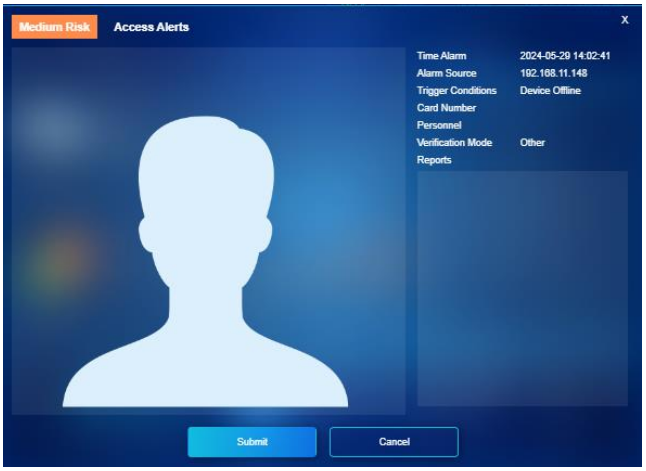
Device Alarm Status

View access alarm status, quantity, and details of the device.

Click **[Detail]** to view alarm details. In the detail prompt, click the " " under operations, enter the text content, and click **[Submit]** to confirm the alarm



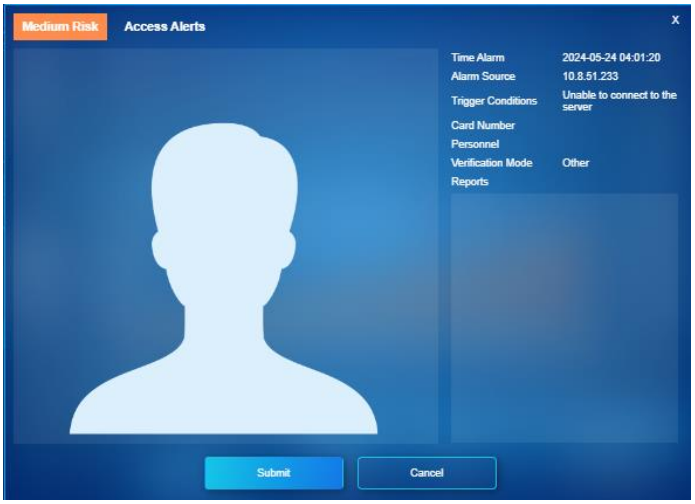
Copyright © 2024 ARMATURA LLC. All rights reserved



Pending Alarm

View pending access alarm status and details.

Click **[Detail]** to view the alarm details, enter the text content, and click **[Submit]** to confirm the alarm.



Face Alert

Prerequisites for Use

Log into the system using an account with the required permissions.

Function Usage Scenarios

View Face alert alarms in real time.

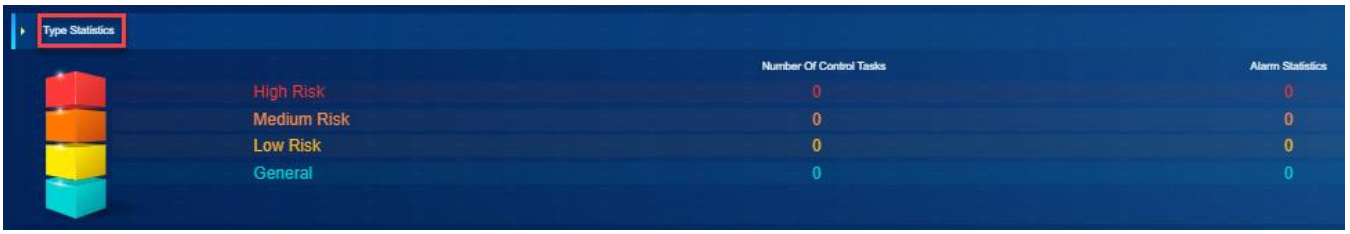
Copyright © 2024 ARMATURA LLC. All rights reserved

Control Details

Display the data situation of Face Alert and alarms that have been generated.

Type Statistics

Displays the number of alarms that have been set for each level of Face Alert and the number of alarms generated by each level.



Region Statistics

Display the number of face alert alarms in different areas of the system.

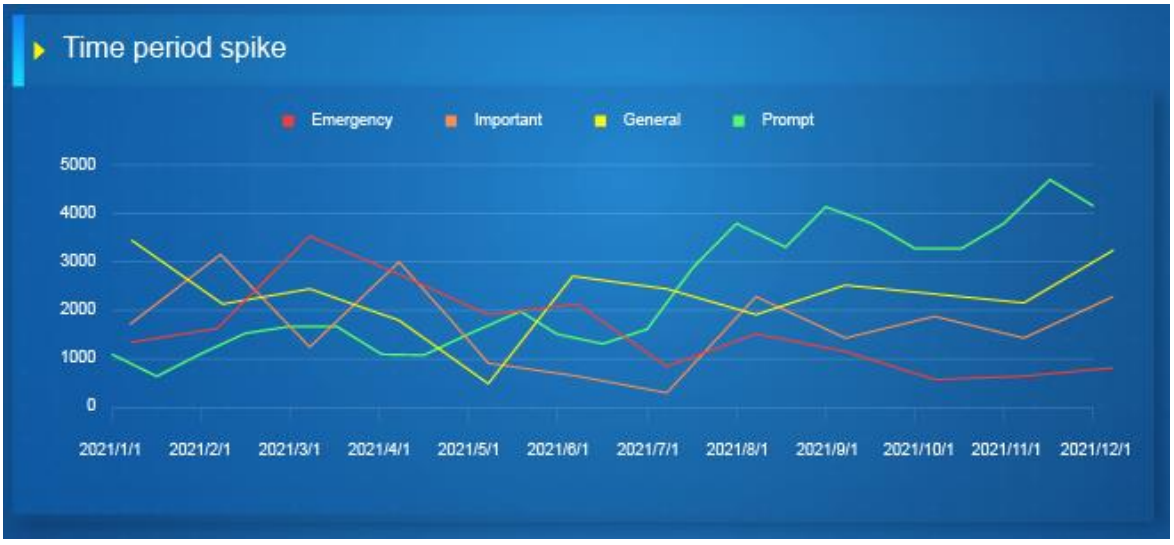
Copyright © 2024 ARMATURA LLC. All rights reserved

24H Peak Ratio

A graph comparing the number of alerts per hour over a period of time.

Time Period Peak

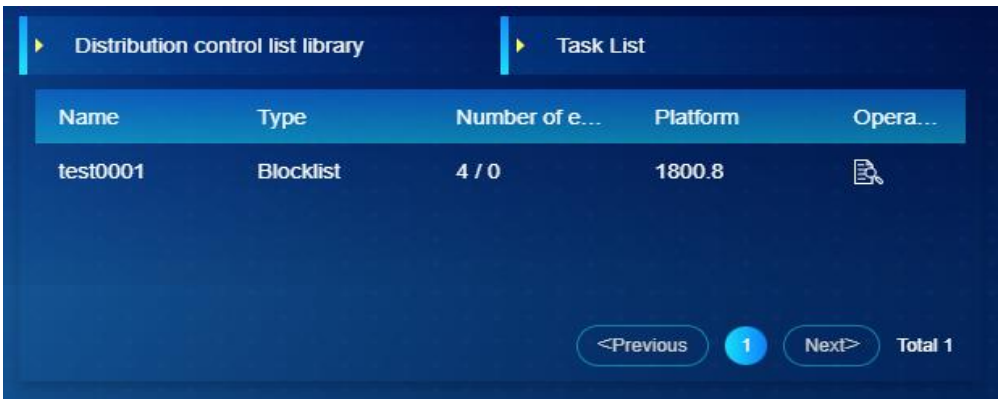
A graph comparing different face alert alarm levels over a period of time.



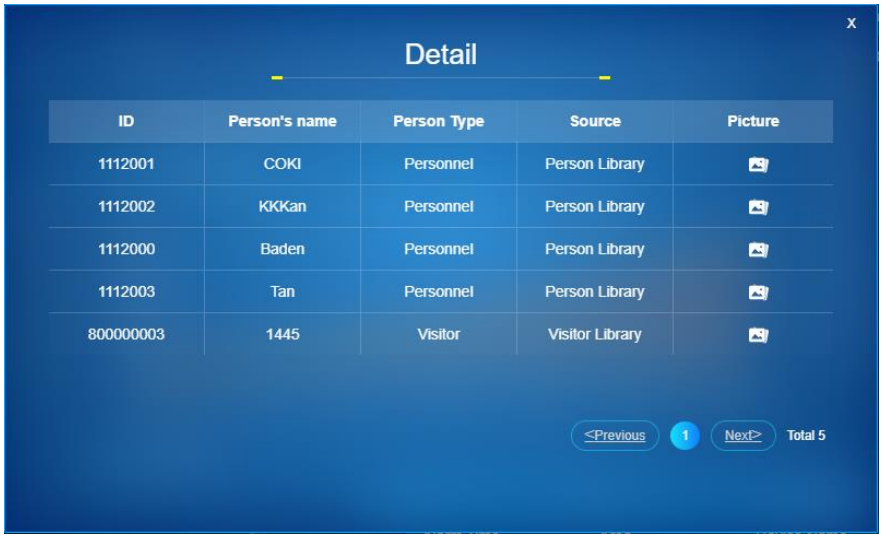
Distribution Control List Library

Display the face alert list library and the details of the list personnel that have been deployed.

Copyright © 2024 ARMATURA LLC. All rights reserved

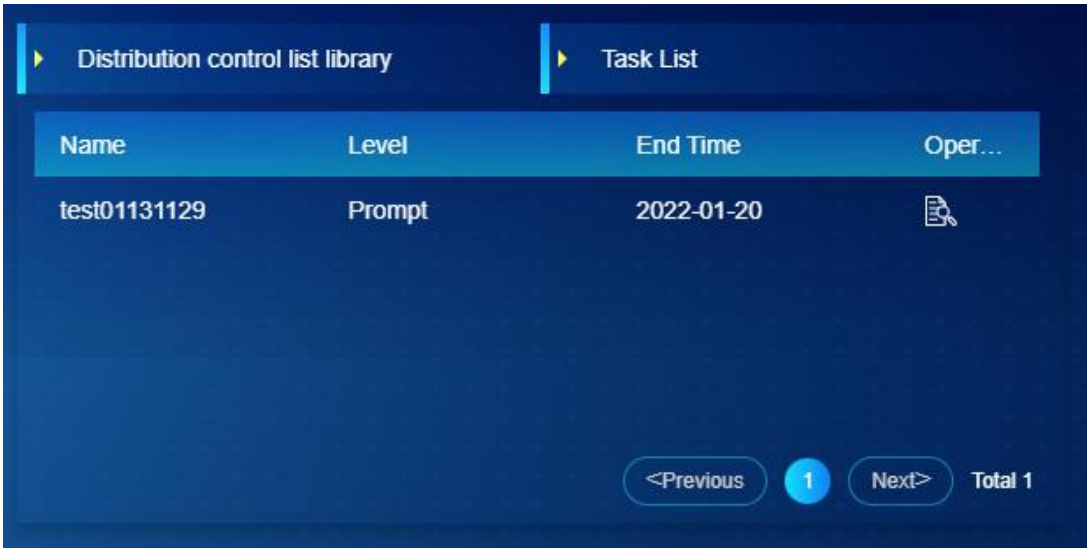


Click **[Detail]** to view the composition of the library.



Task List

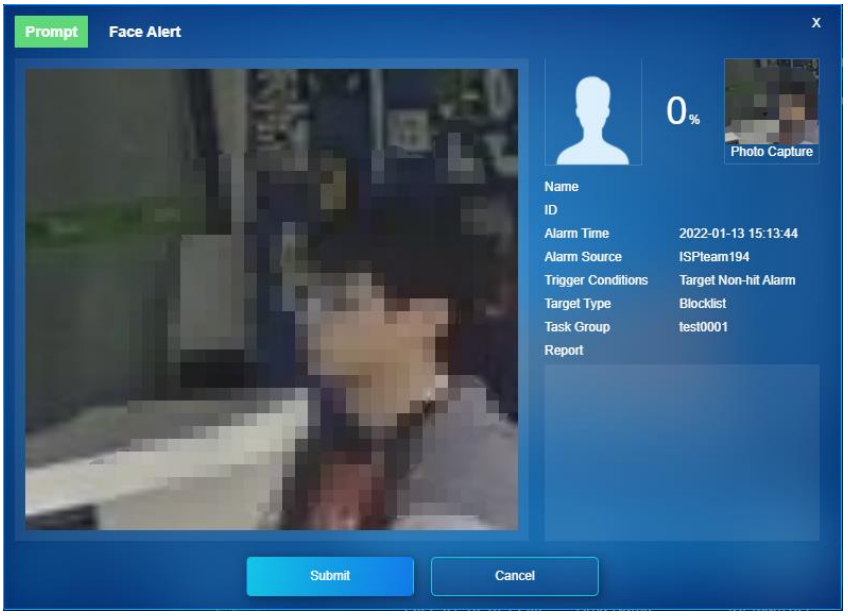
View the face alert task, and task details and the historical alarm records.



Copyright © 2024 ARMATURA LLC. All rights reserved

Click **[Detail]** to view Task detail and history alarm records.

Click **[Detail]** to view alarm detail and make a text content and click **[Submit]** to confirm an alarm.

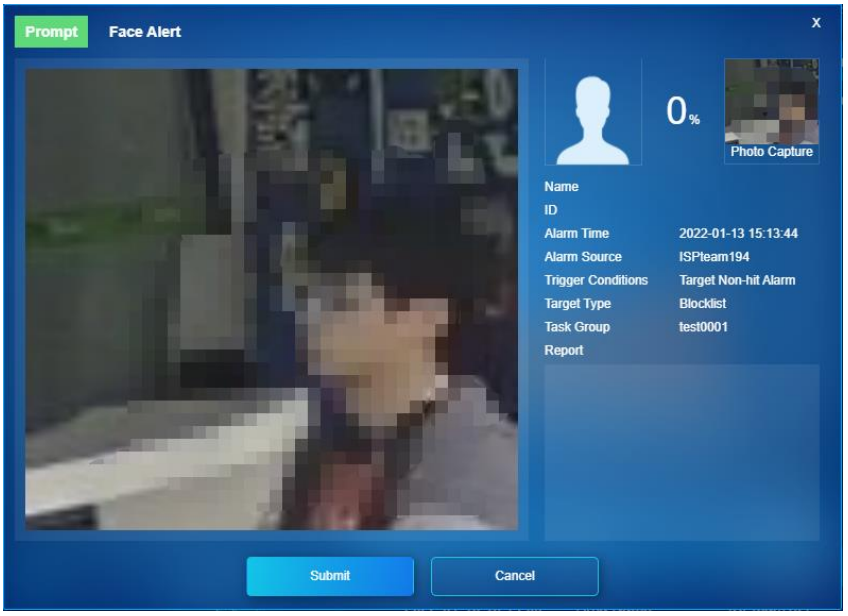


Pending Alarm

View pending face alert alarm status and details.

Copyright © 2024 ARMATURA LLC. All rights reserved

Click **[Detail]** to view alarm detail and make a text content and click **[Submit]** to confirm an alarm.



Vehicle Alerts

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

View vehicle alert alarms in real time.

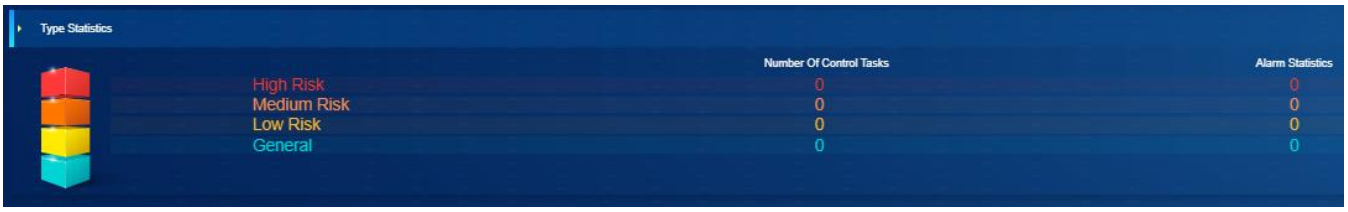
Copyright © 2024 ARMATURA LLC. All rights reserved

Control Details

Display the data situation of Vehicle Alert and alarms that have been generated.

Type Statistics

Displays the number of alarms that have been set for each level of Vehicle Alert and the number of alarms generated by each level.



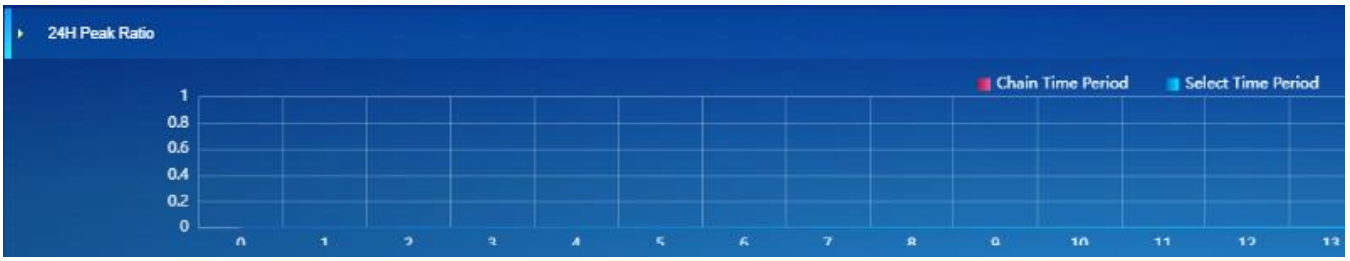
Region Statistics

Display the number of Vehicle alert alarms in different areas of the system.

Copyright © 2024 ARMATURA LLC. All rights reserved

24H Peak Ratio

A graph comparing the number of alerts per hour over a period of time.

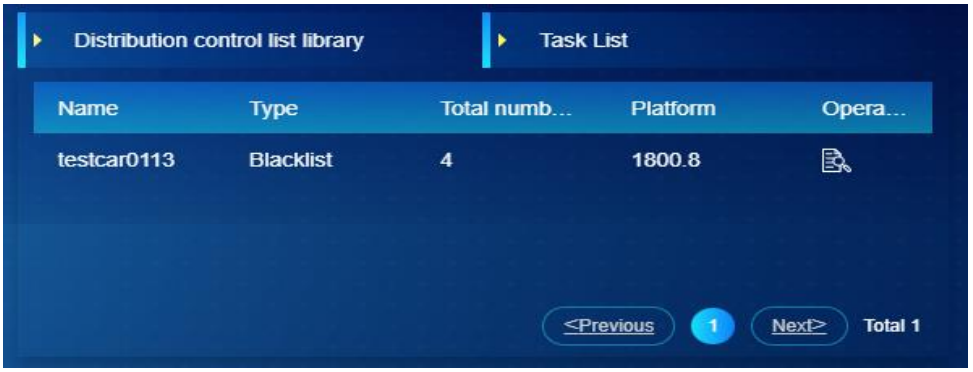


Time Period Peak

A graph comparing different face alert alarm levels over a period of time.

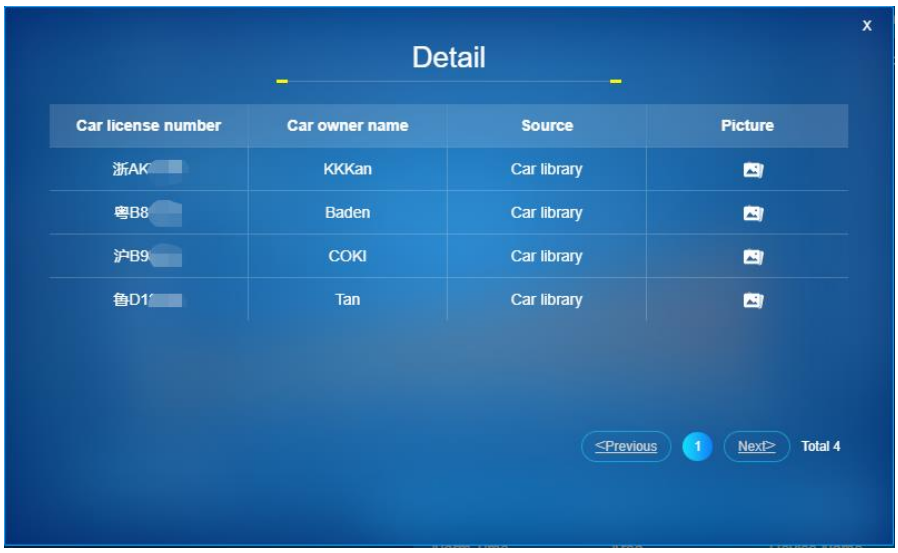
Distribution Control List Library

Display the vehicle alert list library and the details of the list personnel that have been deployed.

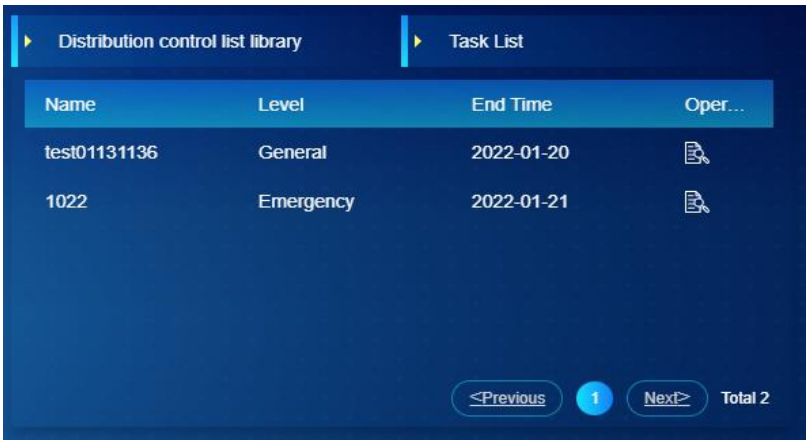


Click **[Detail]** to view the composition of the library.

Copyright © 2024 ARMATURA LLC. All rights reserved



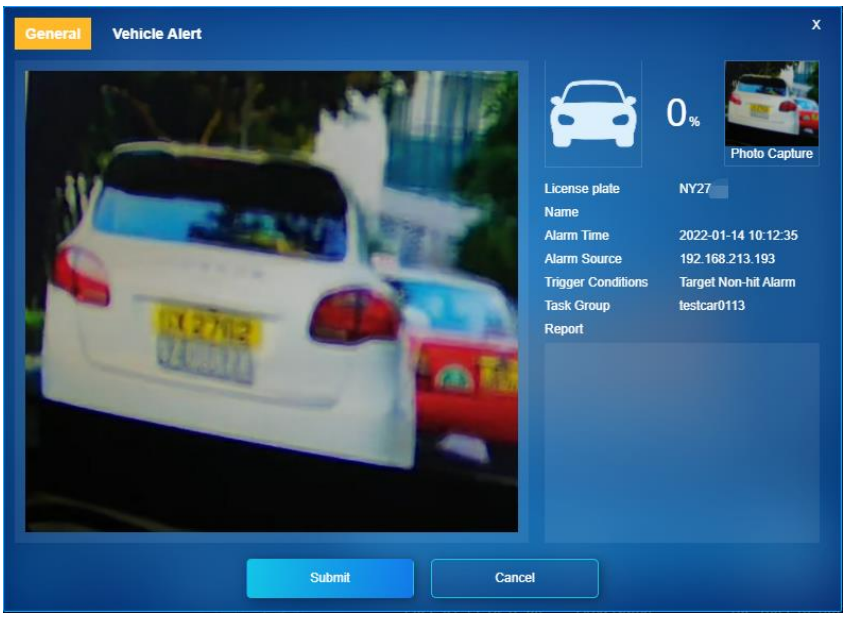
Task List



Click **[Detail]** to view Task detail and history alarm records.

Click **[Detail]** to view alarm detail and make a text content and click **[Submit]** to confirm an alarm.

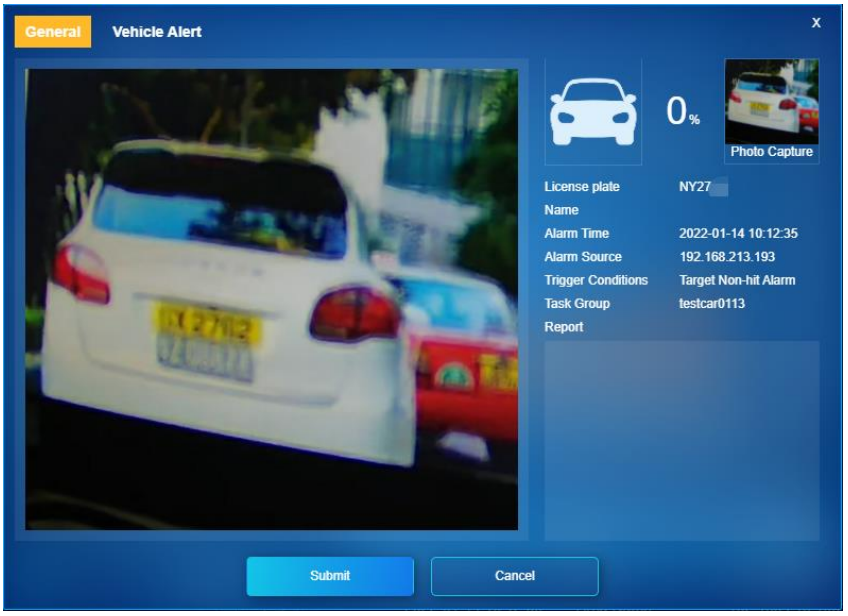
Copyright © 2024 ARMATURA LLC. All rights reserved



Pending Alarm

View pending vehicle alert alarm status and details.

Click **[Detail]** to view alarm detail and make a text content and click **[Submit]** to confirm an alarm.



Copyright © 2024 ARMATURA LLC. All rights reserved

Camera Alerts

Prerequisites for Use

Log into the system using an account with the required permissions.

Usage Scenarios

View camera alert alarms in real time.

Total Number of Cameras

View the total number of cameras and the number of subscriptions used as alerts and the number of idle.

Type Statistics

Displays the distribution of the number of generated camera alarms of different levels.

Copyright © 2024 ARMATURA LLC. All rights reserved

Region Statistics

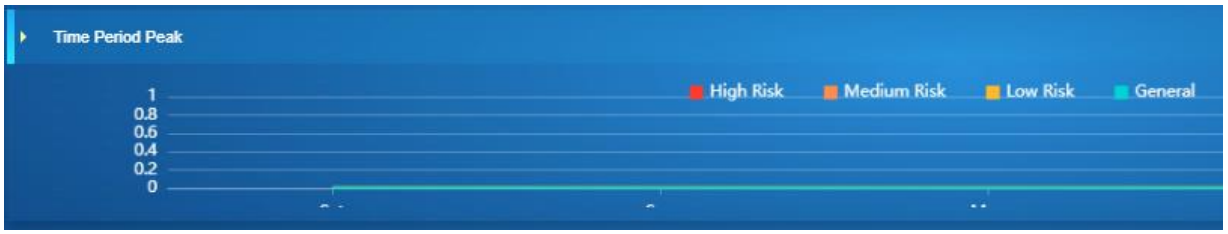
Display the number of camera alarms in different areas of the system.

24H Peak Ratio

A graph comparing the number of alerts per hour over a period of time.

Time Period Peak

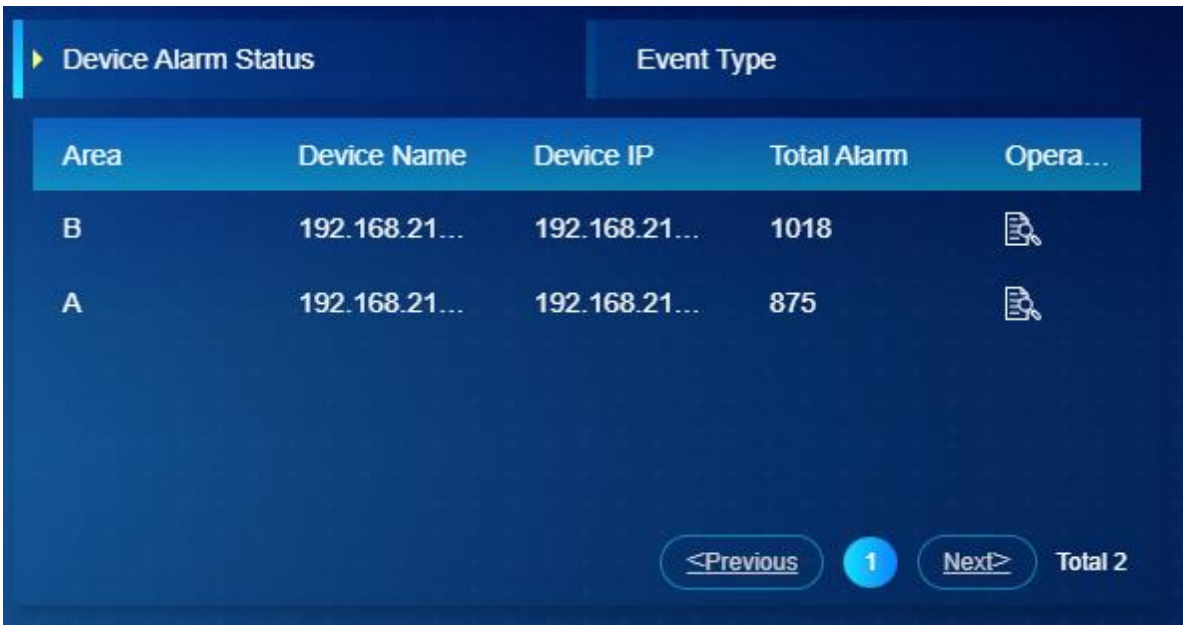
A graph comparing different face alert alarm levels over a period of time.



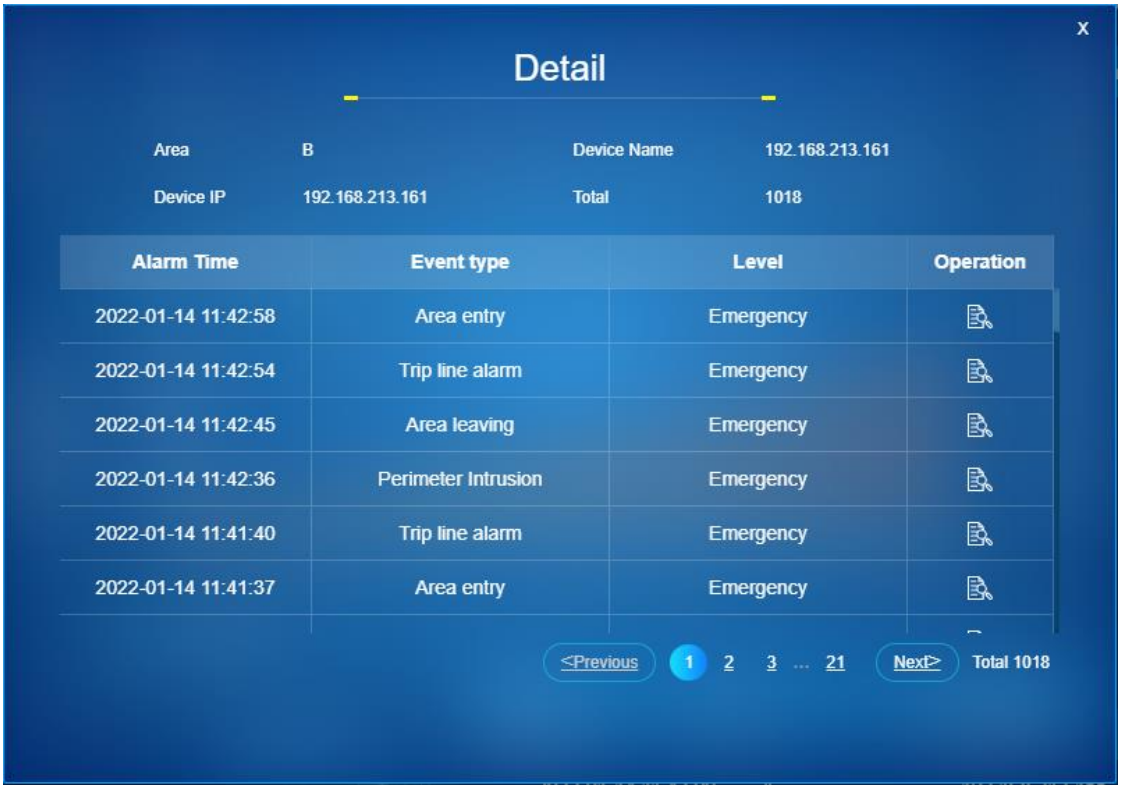
Device Alarm Status

Display the generated alarm devices and their alarm numbers and view the alarm details of the device.

Copyright © 2024 ARMATURA LLC. All rights reserved

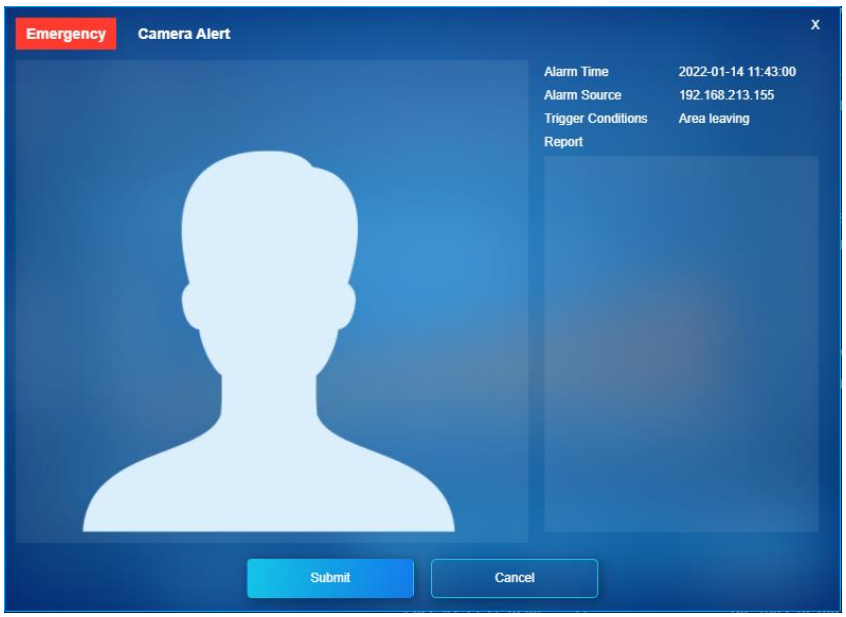


Click **[Detail]** to view device detail and alarm records.



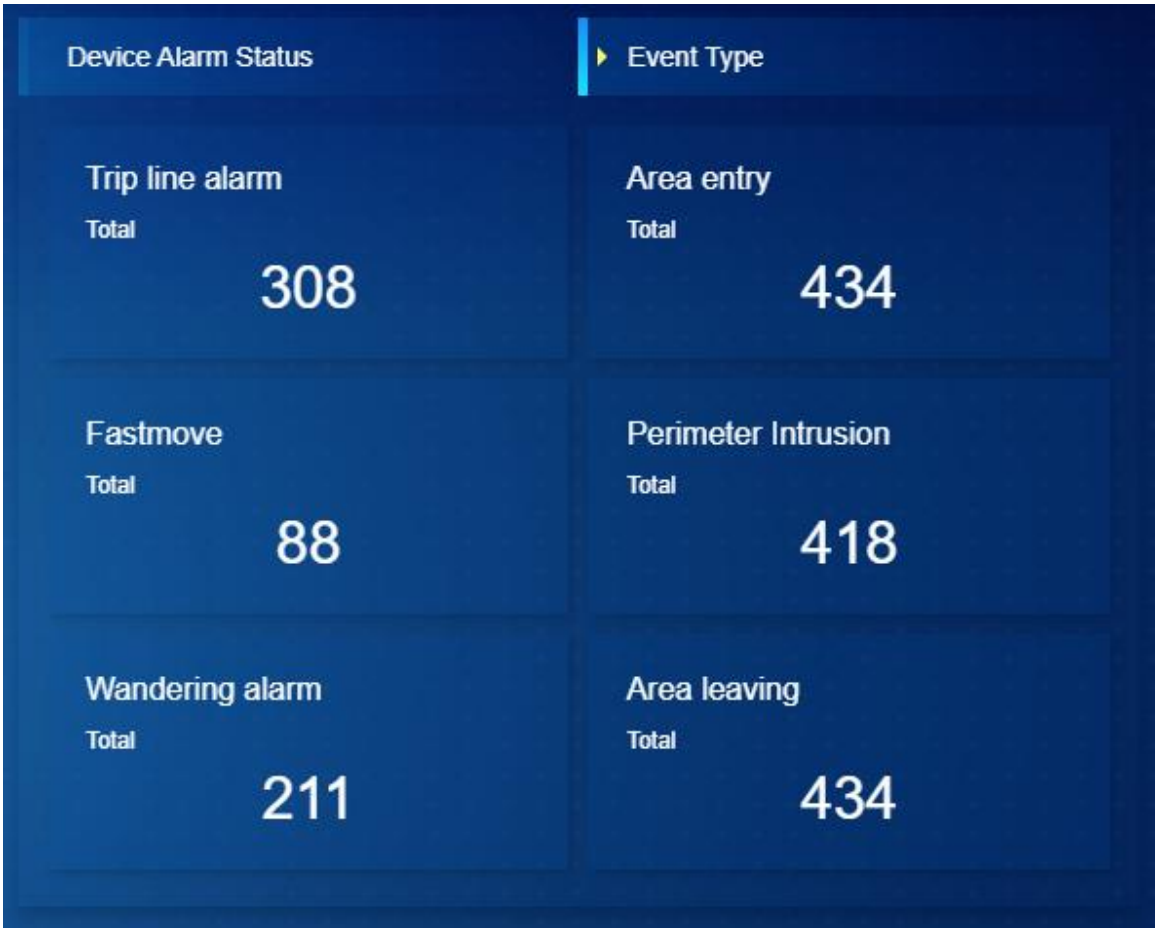
Click **[Detail]** to view alarm detail and make a text content and click **[Submit]** to confirm an alarm.

Copyright © 2024 ARMATURA LLC. All rights reserved



Event Type

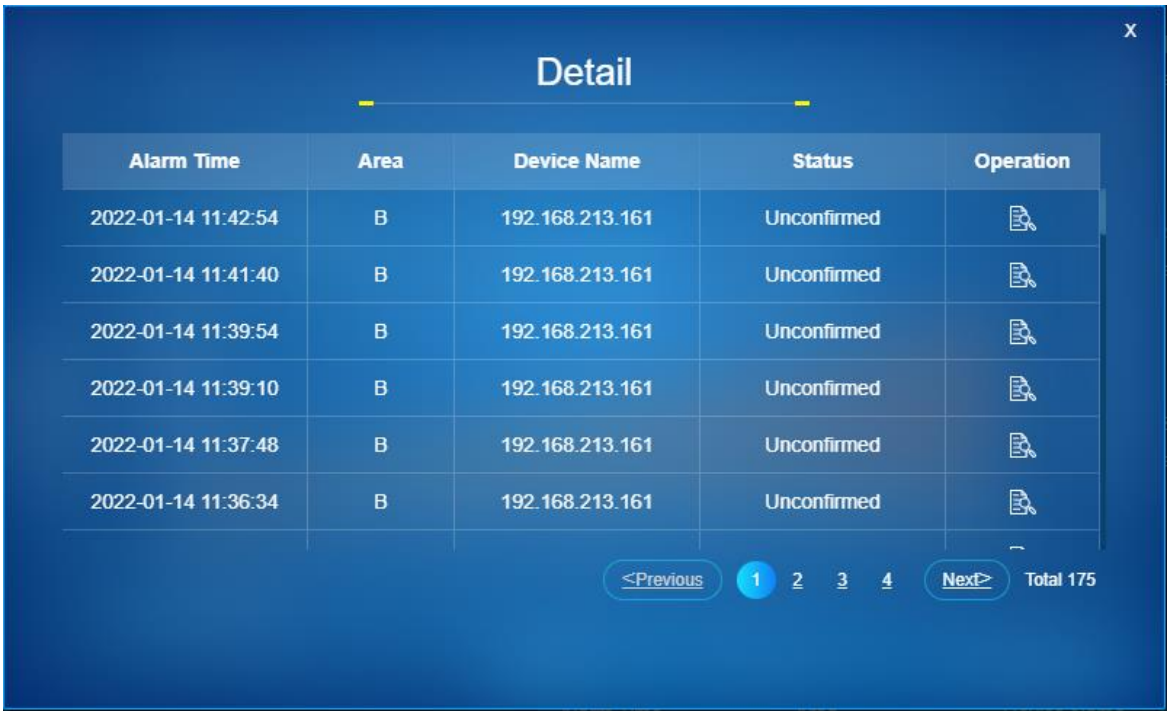
View the number of different camera alarm events and alarm details.



Click on an event to view the distribution of the number of different regions.

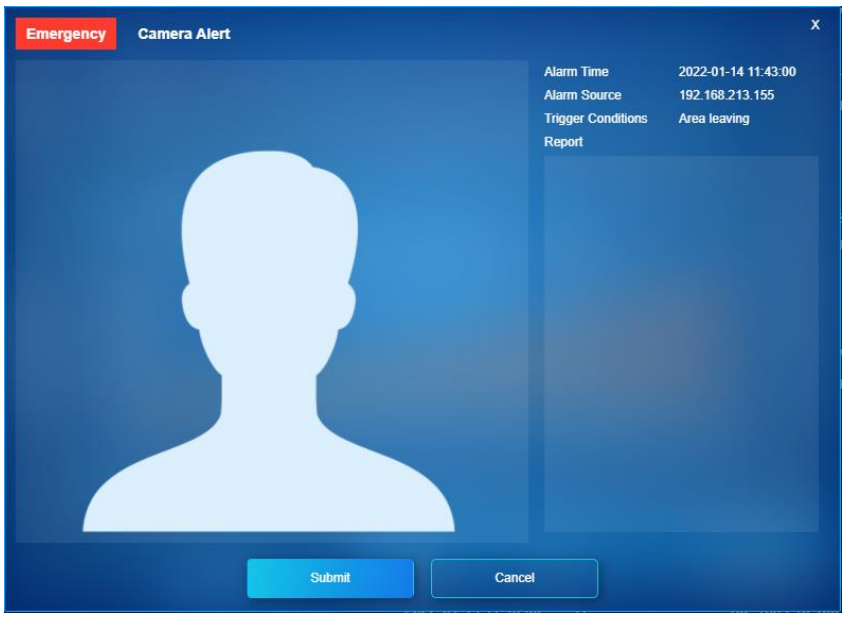
Copyright © 2024 ARMATURA LLC. All rights reserved

Click **[Detail]** to view the details of the alarms in the area.



Click **[Detail]** to view alarm detail and make a text content and click **[Submit]** to confirm an alarm.

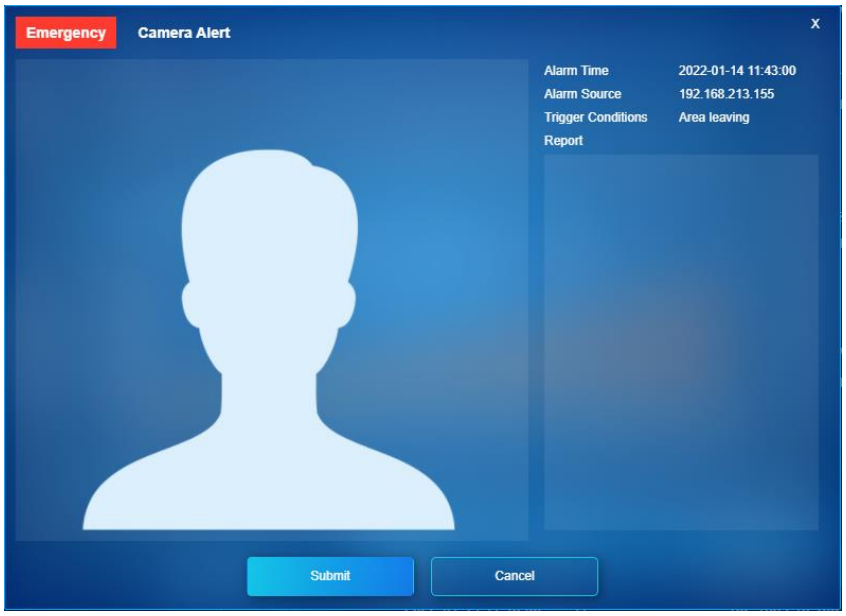
Copyright © 2024 ARMATURA LLC. All rights reserved



Pending Alarm

View pending camera alarm status and details.

Click **[Detail]** to view alarm detail and make a text content and click **[Submit]** to confirm an alarm.



Copyright © 2024 ARMATURA LLC. All rights reserved

11 System

System Settings acts as the central configuration hub for your access control system. Through this interface, administrators can manage user roles, including company management, registrars, and access control administrators. The system allows for comprehensive role configuration within the corresponding modules and provides tools for database management and system parameter adjustments. Additionally, administrators can monitor system usage through detailed operation logs, ensuring security and accountability in all system interactions.

11.1 General Settings

Function List

Operation	Description
Area Settings	Configure and manage physical spaces within your facility to organize and control devices effectively. Areas enable hierarchical organization of access points and simplified monitoring.
Organization	Create and manage organizational structure through departments and teams, enabling efficient personnel management and clear reporting hierarchies.
Certificate Types	Configure and manage the various security certificates and credentials supported by the system, ensuring proper authentication and access control.
Media Files	Manage audio files and other media resources used by the access control system. These files can be deployed to devices for announcements, alerts, and voice prompts.
Card Templates	Access system diagnostics and error code references. View detailed explanations of error messages and perform system health checks for troubleshooting.

11.1.1 Area Settings

Function Description

Areas allow you to organize and manage devices within specific physical spaces. This spatial organization helps you monitor and control access more effectively.

New (Add)

Prerequisites for Use

Administrator access with area creation permissions

Usage Scenarios

Implement when facility areas need to be organized or restructured for more efficient device management and monitoring.

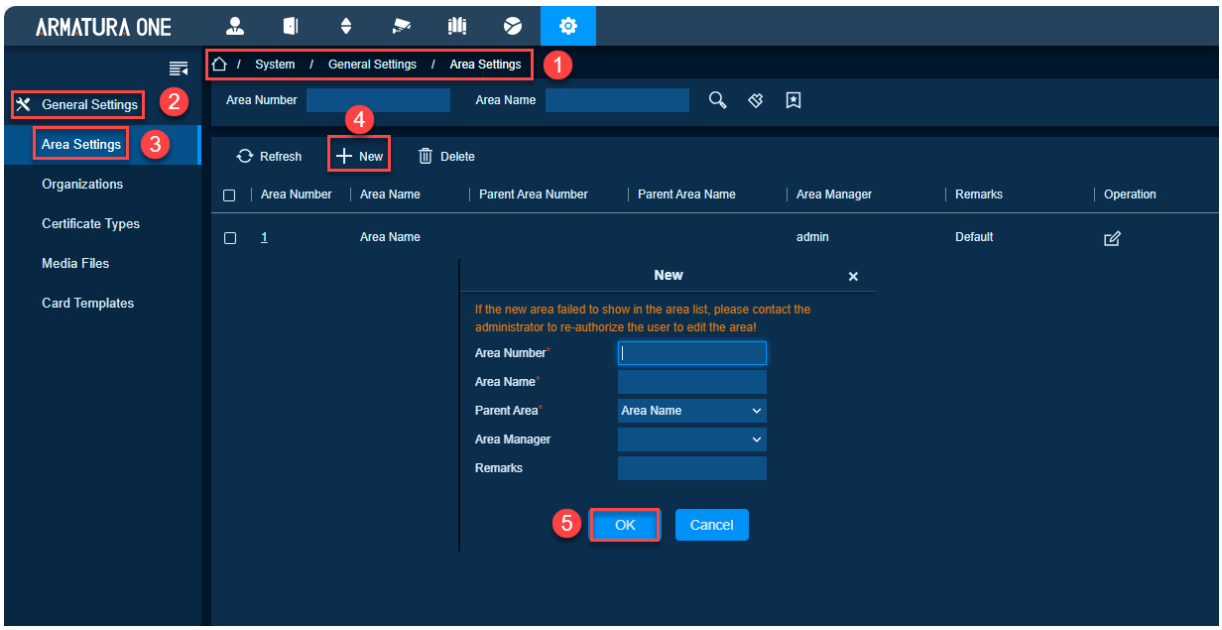
Trigger Result

Creates a new area entry in the system hierarchy with specified configurations and permissions.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Click **[New]** button to open the creation window.



- Complete all required fields. Fields marked with * are mandatory:

Area Number: Enter a unique identifier for the area.

Area Name: Assign a unique descriptive name for the area.

Parent Area: Select the hierarchical parent location for this area.

Area Manager: Designate the administrator responsible for this area.

Remarks: Add optional notes or additional information about the area.

- Click **[OK]** button to save the new area.

Delete

Prerequisites for Use

Administrator account with deletion permissions. Selected areas must be unlinked from all devices and configurations before deletion.

Usage Scenarios

Execute when an area becomes obsolete or requires decommissioning from the system.

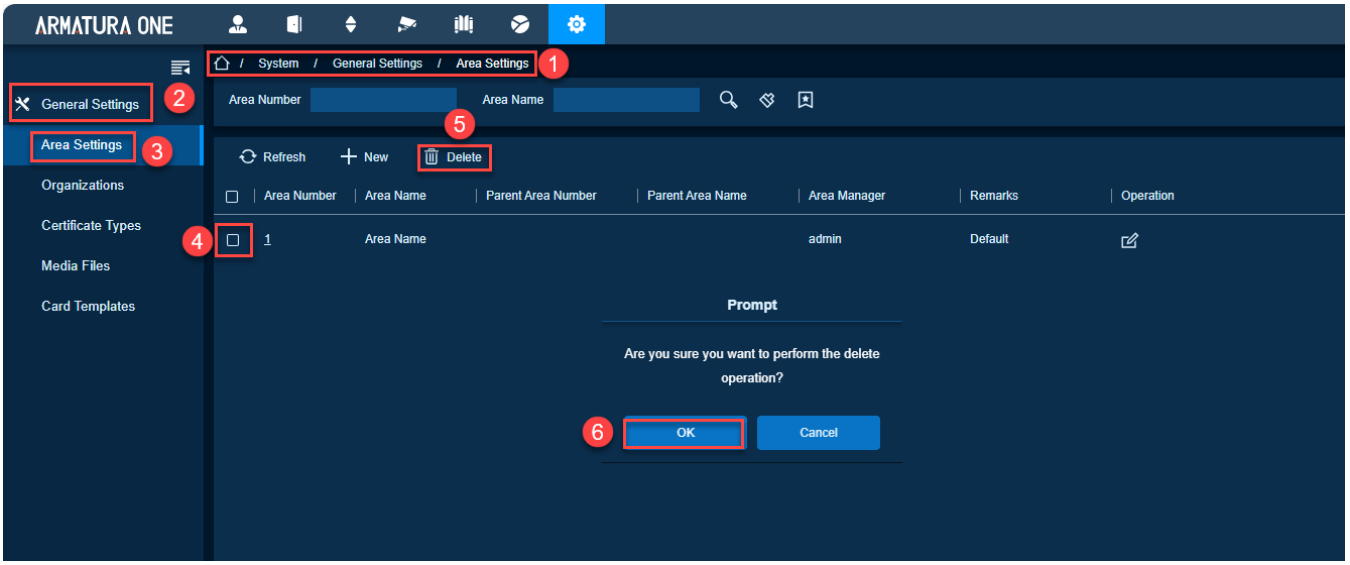
Trigger Result

Permanently removes the selected area from the system hierarchy.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Select the area for deletion.
- Click **[Delete]** button to initiate removal.
- Click **[OK]** in the confirmation prompt to permanently delete the area.



Edit

Prerequisites for Use

Administrator account with edit permissions and access to modifiable areas within the system.

Usage Scenarios

Perform when area configurations require updates or modifications.

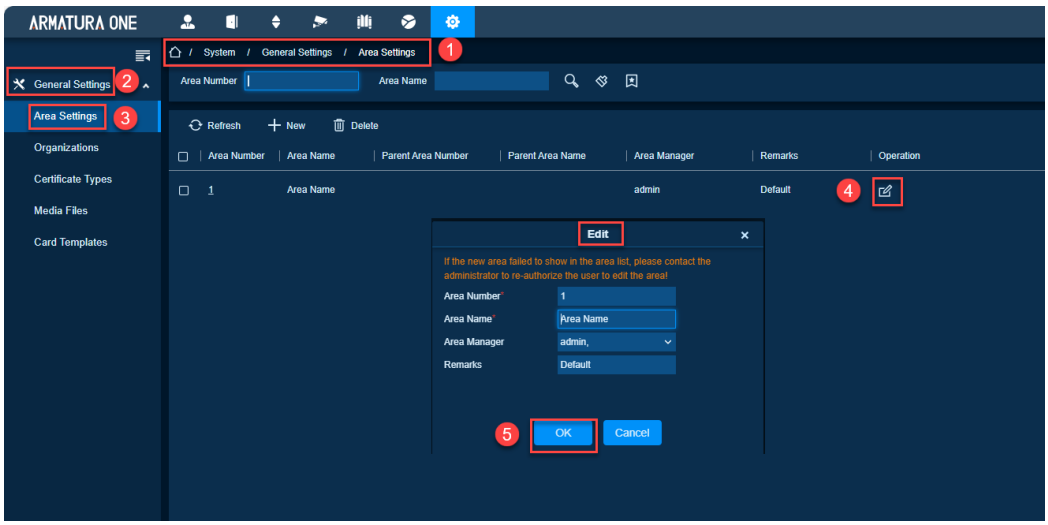
Trigger Result

Updates the selected area with modified configuration settings.

Steps:

- Select the target area for modification.
- Click **[Edit]** button to access area settings.
- Click **[OK]** to save the modified configuration.

Copyright © 2024 ARMATURA LLC. All rights reserved



11.1.2 Organizations

Function Description

Create and manage organizational structures to establish clear hierarchies, streamline personnel management, and define operational responsibilities across teams.

New (Add)

Prerequisites for Use

Administrator account with organization creation permissions. Each organization requires unique identifiers for both name and number.

Usage Scenarios

Implement when establishing new departments, restructuring teams, or refining organizational hierarchies.

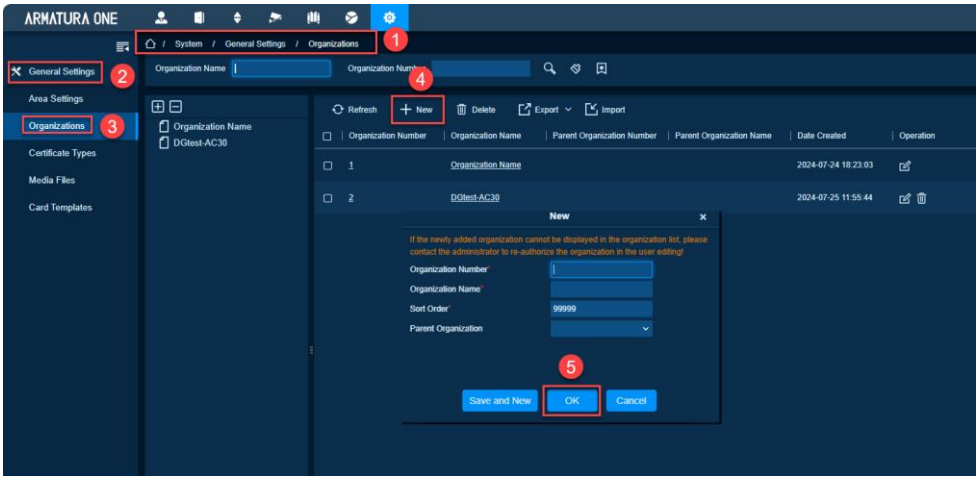
Trigger Result

Creates a new organizational unit in the system hierarchy.

Steps:

- Click **[New]** button to open the creation window.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Complete all required fields. Fields marked with * are mandatory:

Organization Number: Enter a unique identifier for the organization.

Organization Name: Assign a unique name for the organization.

Sort Order: Define the display priority in organizational listings.

Parent Organization: Select the hierarchical parent organization.

- Click **[OK]** button to save the new organization.

Delete

Prerequisites for Use

Administrator account with deletion permissions and access to removable organization entries.

Usage Scenarios

Execute when an organizational unit becomes obsolete or requires removal.

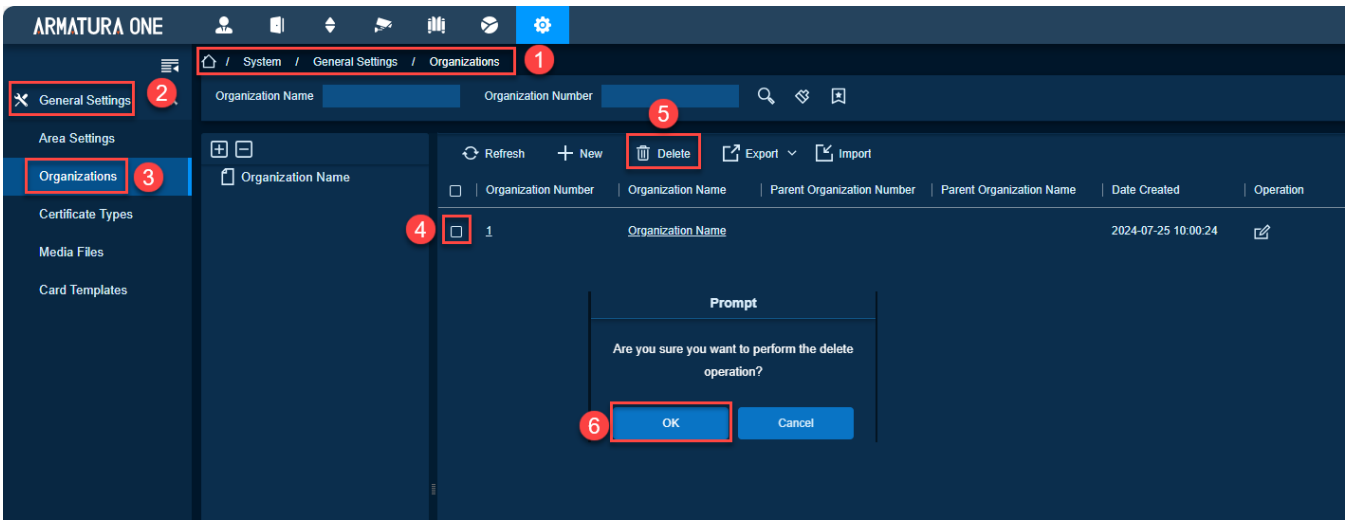
Trigger Result

Removes the selected organization from the system.

Steps:

- Select the target organization for deletion.
- Click **[Delete]** button to initiate removal.
- Click **[OK]** button in the confirmation prompt to complete deletion.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export Organization Information

Prerequisites for Use

Administrator account with data export permissions.

Usage Scenarios

Generate organizational data reports for analysis or record-keeping.

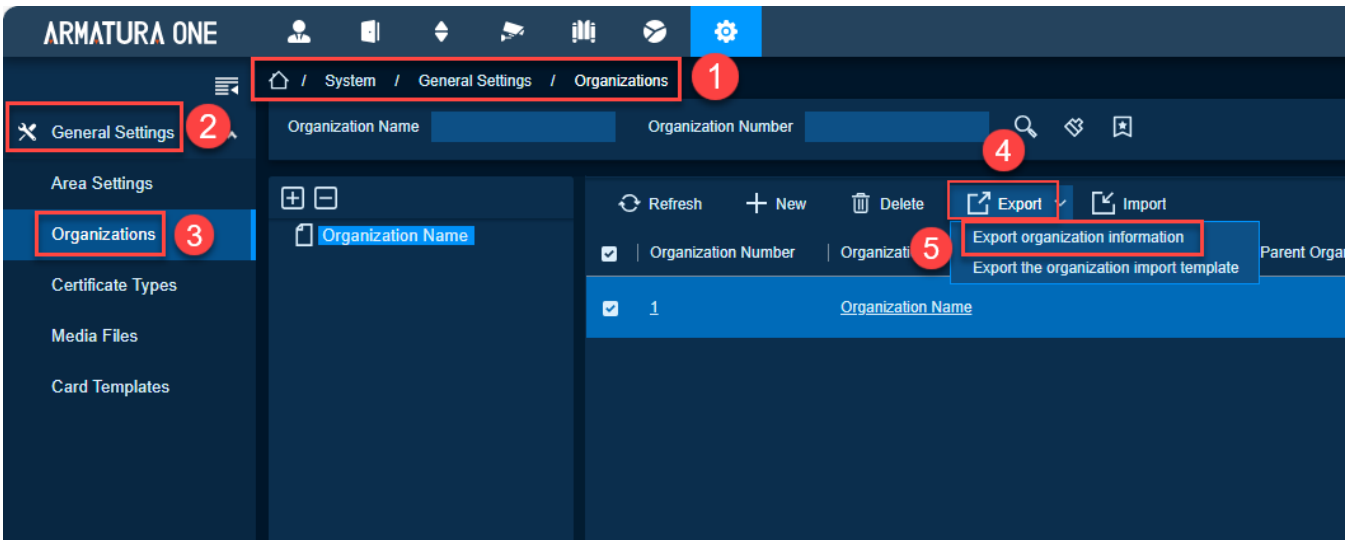
Trigger Result

Operations	Description
Select Excel	Generate organization data in EXCEL format
Select PDF	Generate organization data in PDF format
Select CSV	Generate organization data in CSV format
Select All Data	Export all organizational data
Select the amount of Data Export	Export specified portion of organizational data

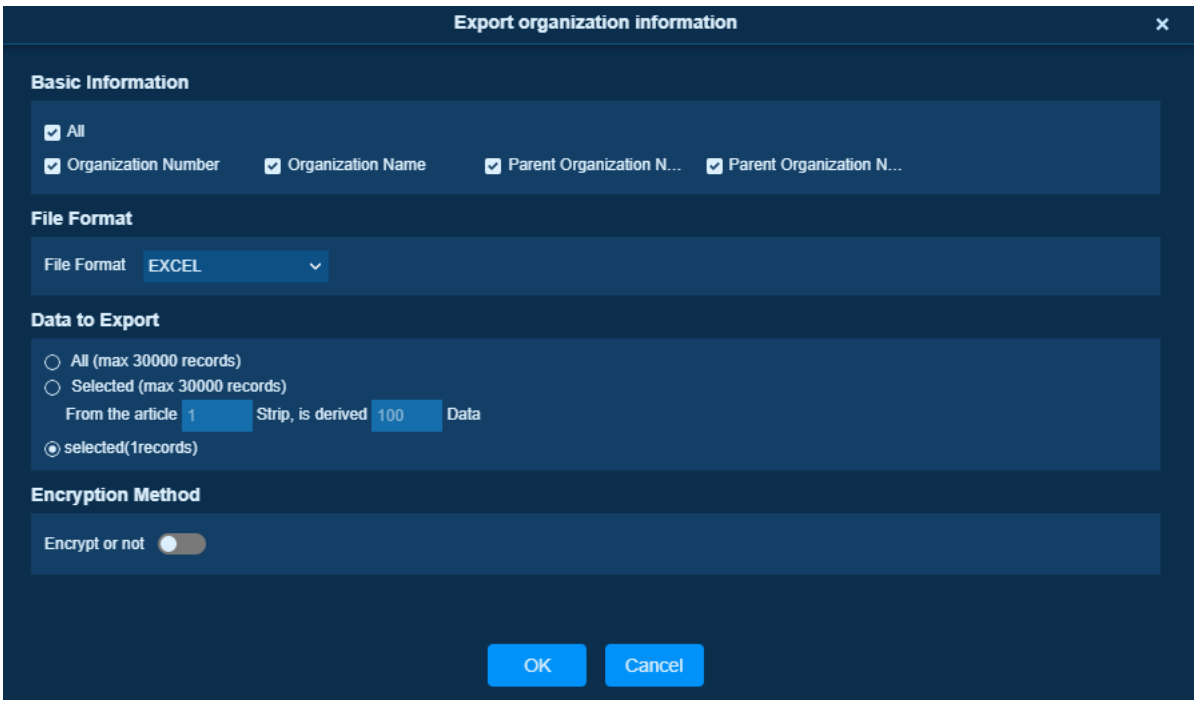
Steps:

- Select organizations for export.
- Click **[Export]** drop-down box.
- Select **[Export Organization information]** in the drop-down box.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Choose desired file format.
- Specify data range for export.
- Click **[OK]** to complete the export operation.



Export Organization Import Template

Prerequisites for Use

Administrator account with template export permissions.

Usage Scenarios

Generate template for bulk organization data imports via EXCEL format.

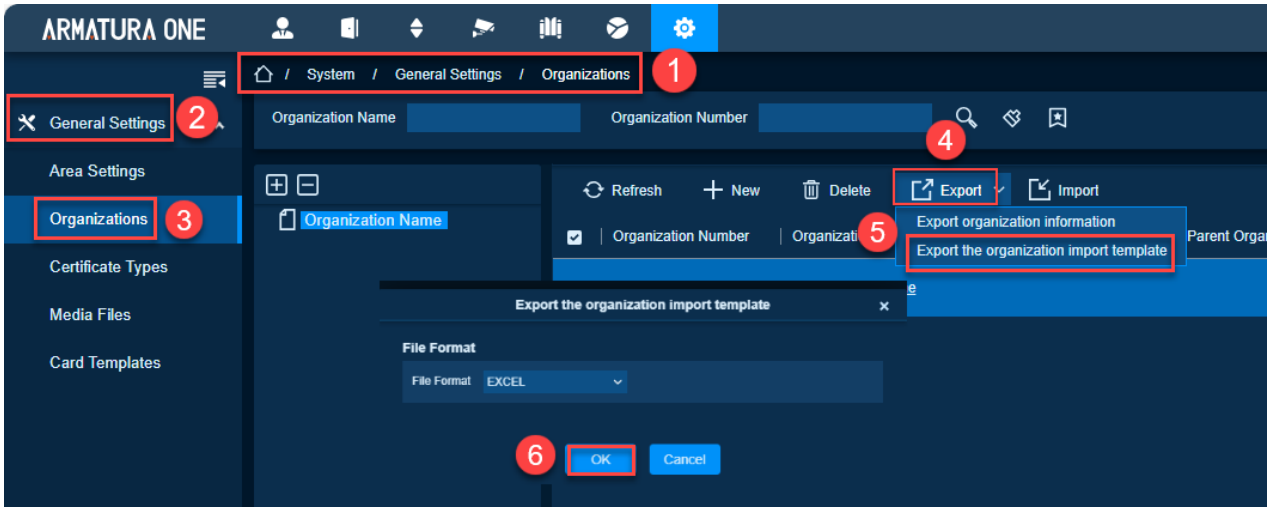
Trigger Result

Downloads organization import template in EXCEL format.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Click **[Export]** drop-down box.
- Select **[Export the Organization Import Template]** option.



- Confirm EXCEL format selection.
- Click **[OK]** button to download the template.

Import

Prerequisites for Use

Administrator account with import permissions and correctly formatted organization template.

Usage Scenarios

Perform bulk import of organizational data using completed EXCEL templates.

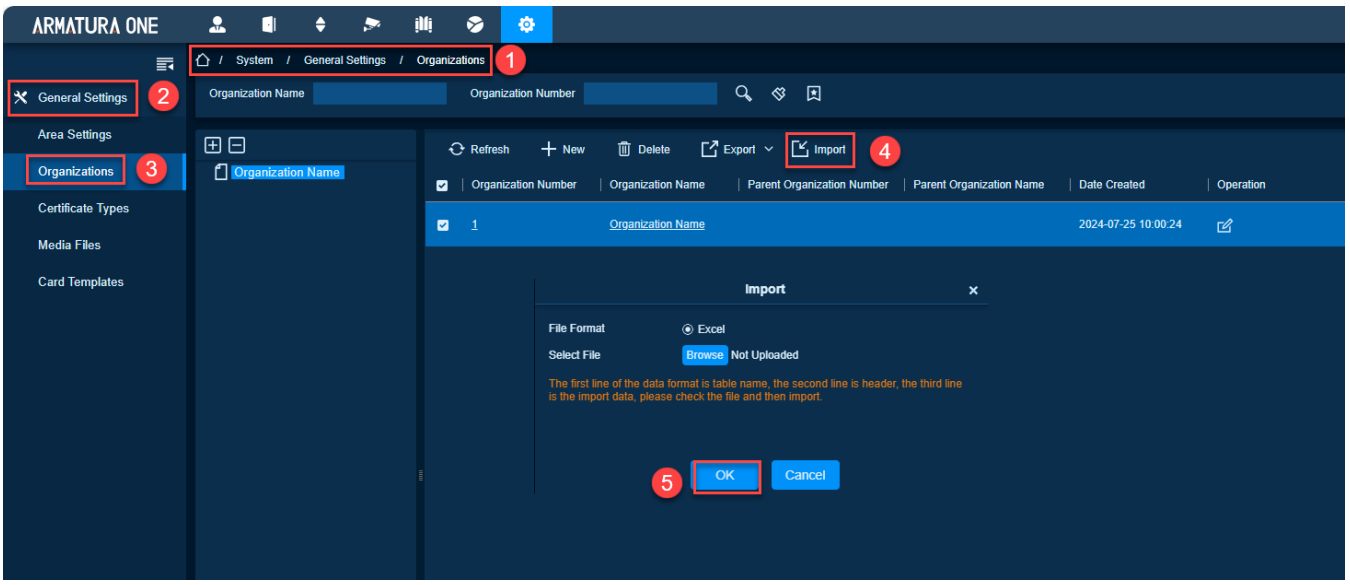
Trigger Result

Integrates organizational data from EXCEL file into the system.

Steps:

- Click **[Import]** button to launch import wizard.
- Click **[Browse]** to locate and select the completed template.
- Click **[OK]** button to process the import.

Copyright © 2024 ARMATURA LLC. All rights reserved



Edit

Prerequisites for Use

Administrator account with edit permissions and access to modifiable organizations.

Usage Scenarios

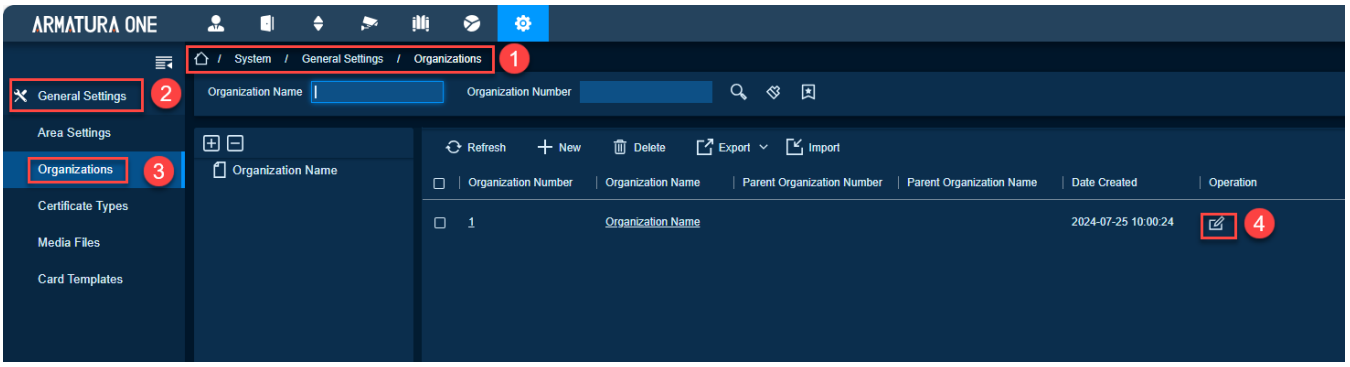
Perform when organizational details require updates or modifications.

Trigger Result

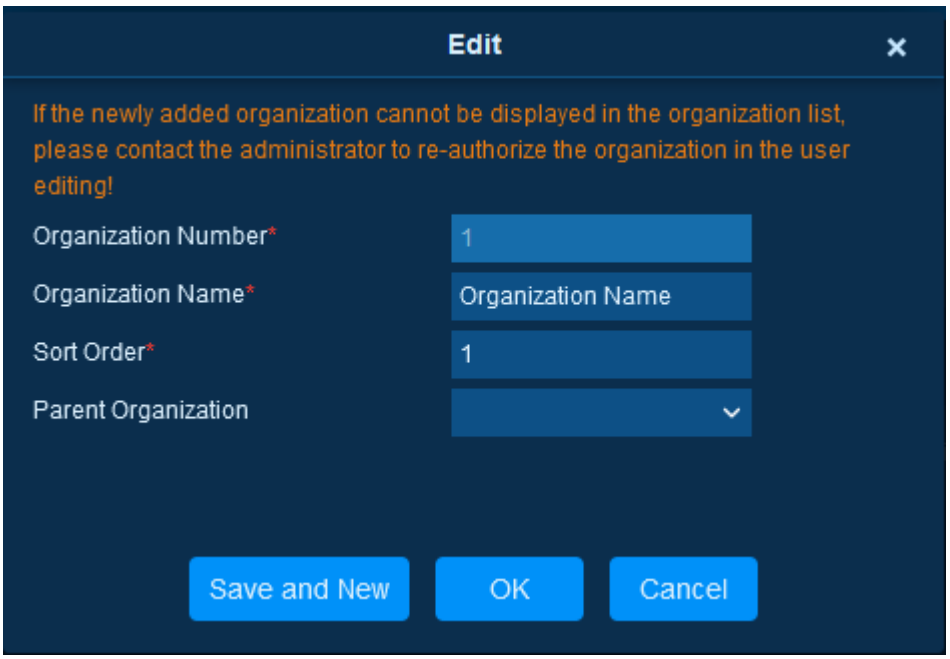
Updates the selected organization with modified information.

Steps:

- Select the target organization for modification.
- Click **[Edit]** button to access settings.
- Click **[OK]** to save the modified configuration.



Copyright © 2024 ARMATURA LLC. All rights reserved



11.1.3 Certificate Types

Function Description

Configure and manage the various types of security certificates and credentials recognized by the management system.

New (Add)

Prerequisites for Use

Administrator account with certificate type management permissions.

Usage Scenarios

Implement when new certificate types are required to support additional authentication methods or security protocols.

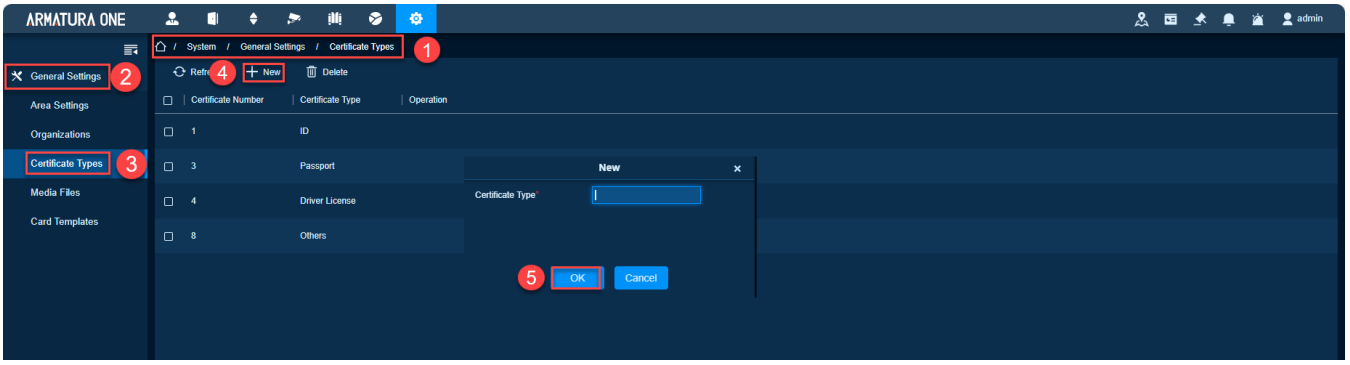
Trigger Result

Creates a new certificate type configuration in the system.

Steps:

- Click **[New]** button to open the creation window.
- Enter the name of the certificate type to add.
- Click **[OK]** button to save the new certificate type.

Copyright © 2024 ARMATURA LLC. All rights reserved



Delete

Prerequisites for Use

Administrator account with deletion permissions. System default certificate types cannot be removed.

Usage Scenarios

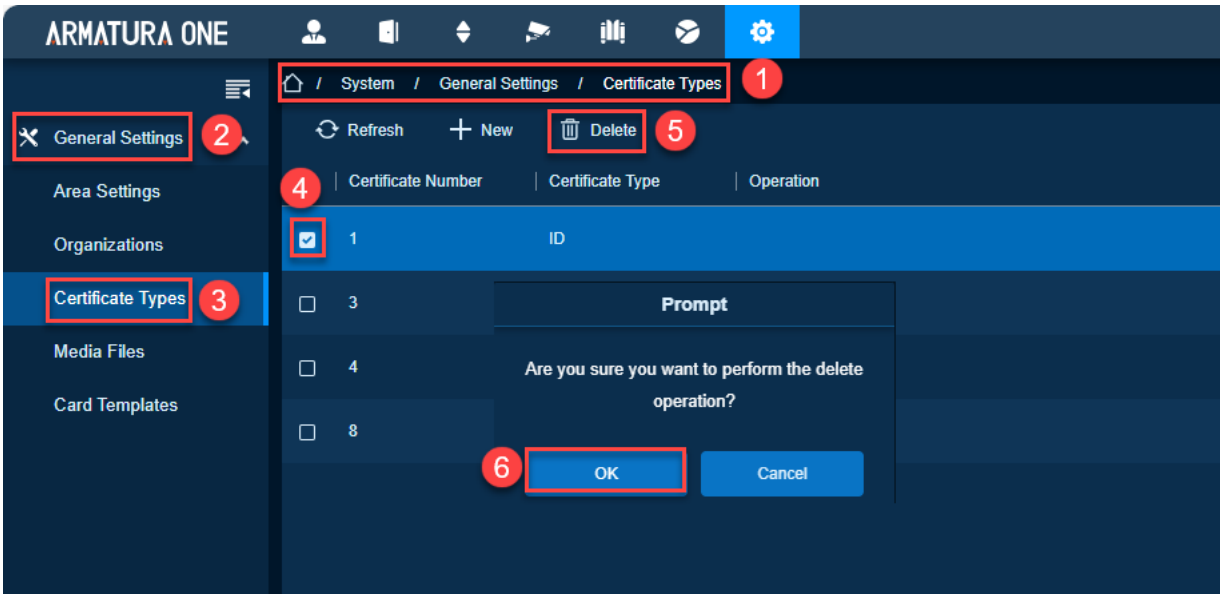
Execute when a custom certificate type becomes obsolete or requires removal.

Trigger Result

Removes the selected certificate type from the system.

Steps:

- Select the certificate type for deletion.
- Click **[Delete]** button to initiate removal.
- Click **[OK]** in the confirmation prompt to complete deletion.



Edit

Prerequisites for Use

Administrator account with edit permissions and access to modifiable certificate types.

Copyright © 2024 ARMATURA LLC. All rights reserved

Usage Scenarios

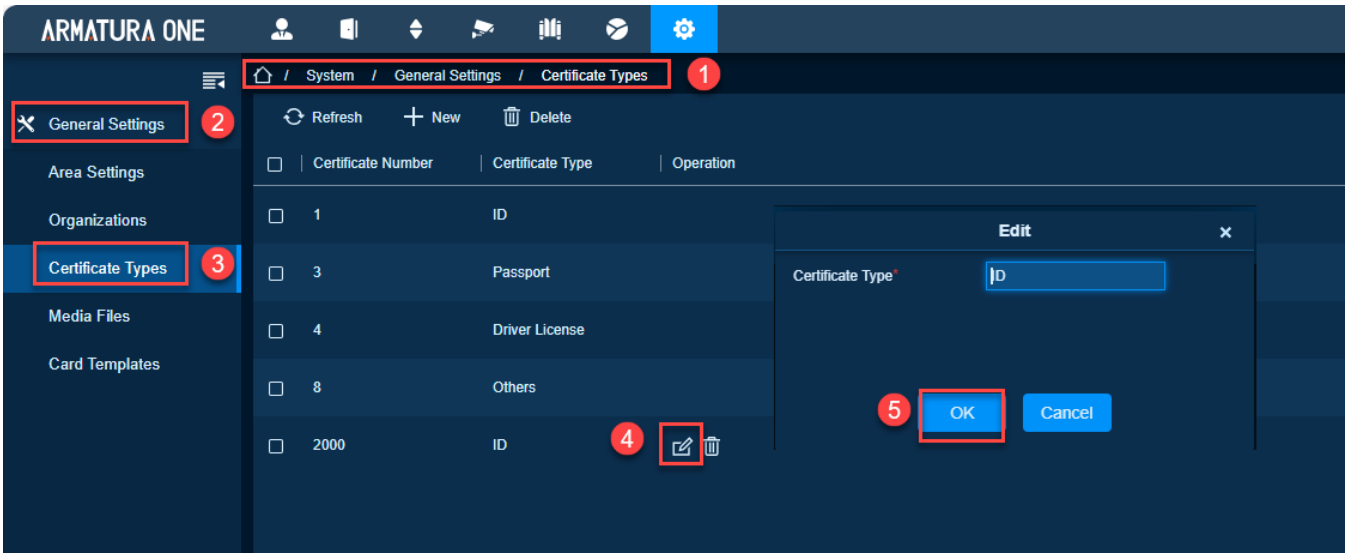
Perform when certificate type configurations require updates or modifications.

Trigger Result

Updates the selected certificate type with modified settings.

Steps:

- Select the target certificate type for modification.
- Click **[Edit]** button to access settings.
- Click **[OK]** to save the modified configuration.



11.1.4 Media Files

Function Description

Manage audio files used for access control system notifications and device voice prompts. These media files provide audio feedback for various system events and actions.

New (Add)

Prerequisites for Use

Administrator account with media file management permissions. Supported audio formats: MP3 and WAV only.

Usage Scenarios

Implement when new audio notifications or voice prompts are needed for devices or access control modules.

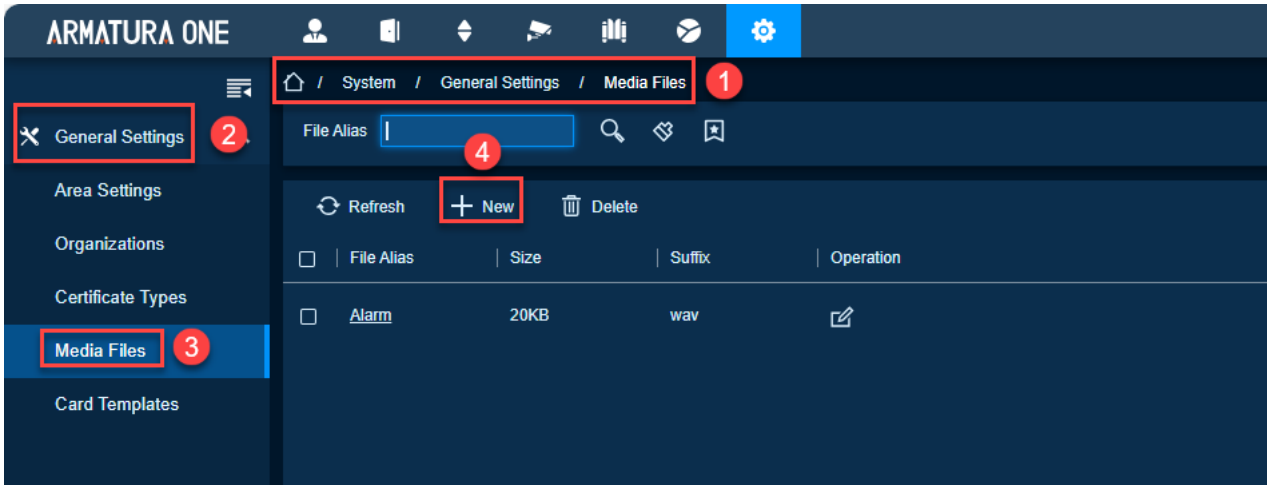
Trigger Result

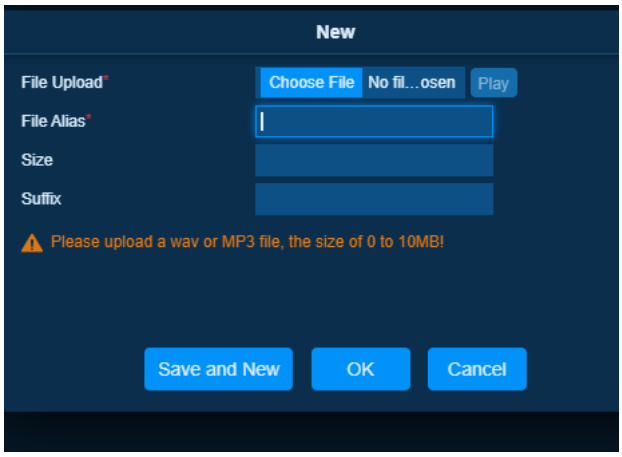
Adds a new audio file to the system's media library.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Click **[New]** button to open the upload window.
- Complete all required fields marked with (*).
- Click **[OK]** button to save the new media file.





The fields are explained as follows:

File Upload: Select the audio file from your local system.

File Alias: Define a descriptive name for the audio file.

Size: Displays the file size.

Suffix: Displays the file format extension (.mp3 or .wav).

Delete

Prerequisites for Use

Administrator account with deletion permissions. System default audio files cannot be removed. Selected files must not be in use by any system module.

Usage Scenarios

Execute when audio files become obsolete or require removal from the system.

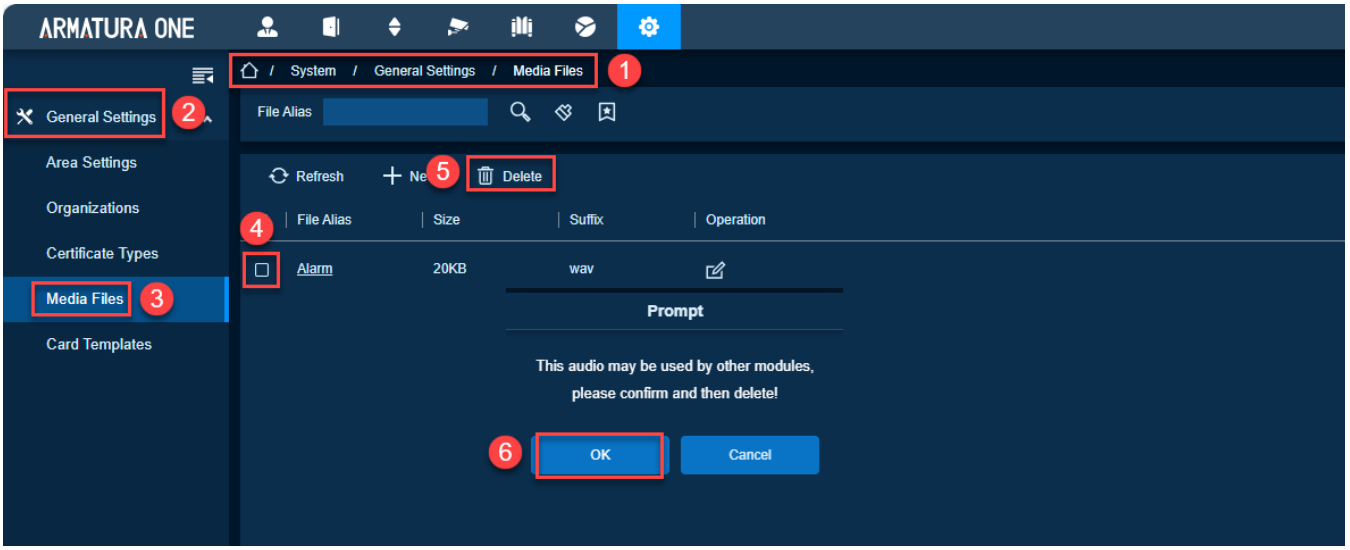
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Removes the selected audio file from the media library.

Steps:

- Select the audio file for deletion.
- Click **[Delete]** button to initiate removal.
- Click **[OK]** to confirm and complete deletion.



Edit

Prerequisites for Use

Administrator account with edit permissions. Selected files must not be system defaults or currently in use by other modules.

Usage Scenarios

Perform when audio file settings require updates or modifications.

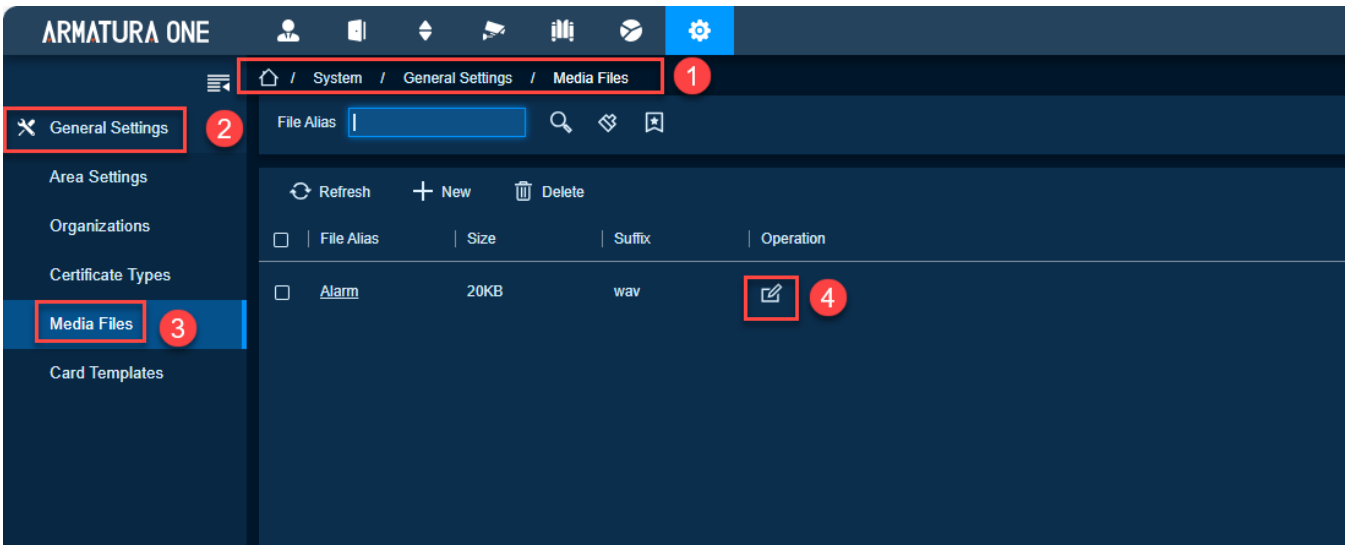
Trigger Result

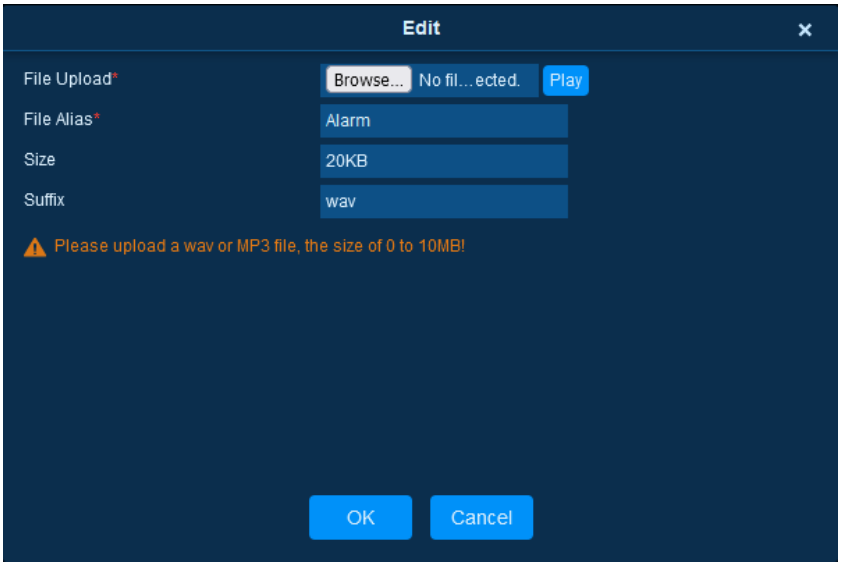
Updates the selected audio file's configuration.

Steps:

- Select the target audio file for modification.
- Click **[Edit]** icon to access settings.
- Click **[OK]** to save the modified configuration.

Copyright © 2024 ARMATURA LLC. All rights reserved





11.1.5 Card Templates

Function Description

Manage and customize employee card templates for card printing purposes.

New (Add)

Prerequisites for Use

Administrator must have permission to create card templates.

Usage Scenarios

Create a new card template when additional template designs are needed.

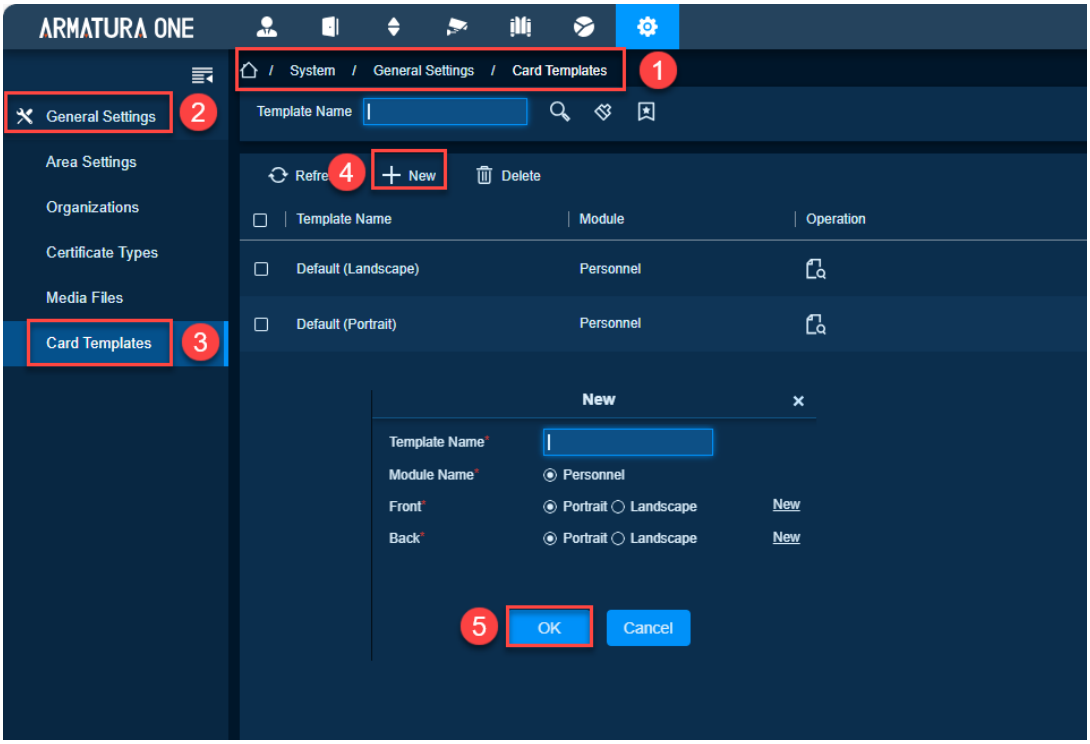
Trigger Result

Creates and saves a new card template in the system.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Click the **[New]** button to open the creation window.
- Enter all required template information.
- Click **[OK]** to save and create the template.



Delete

Prerequisites for Use

Administrator must have deletion permissions and at least one existing template must be available for removal.

Usage Scenarios

Remove obsolete or unnecessary card templates from the system.

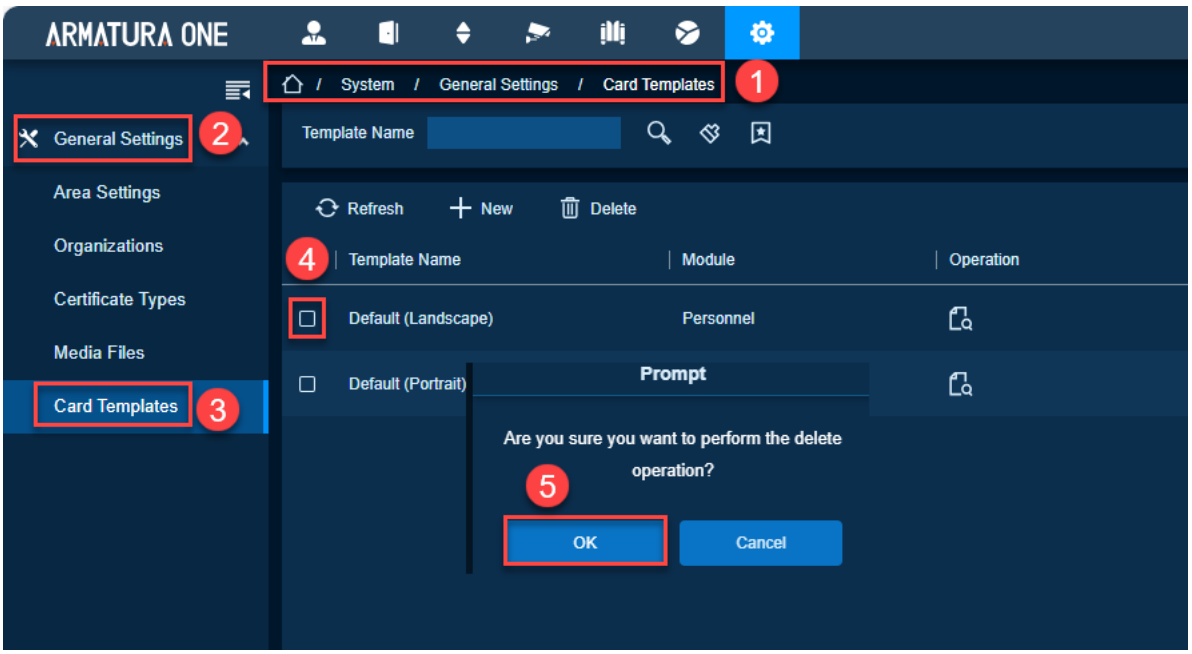
Trigger Result

Permanently removes the selected card template.

Steps:

- Select the desired card template for deletion.
- Click the **[Delete]** icon to display the confirmation window.
- Click **[OK]** in the confirmation window to permanently remove the template.

Copyright © 2024 ARMATURA LLC. All rights reserved



Edit

Prerequisites for Use

Administrator must have permission to modify existing card templates.

Usage Scenarios

Modify existing card templates when updates or changes are required.

Trigger Result

Updates the selected card template with new information.

Steps:

- Select the card template you wish to modify.
- Click the **[Edit]** icon to open the editing window.
- Click **[OK]** to save your changes to the template.

Preview

Prerequisites for Use

User must have permission to view card templates.

Usage Scenarios

Inspect the appearance and details of any card template before use.

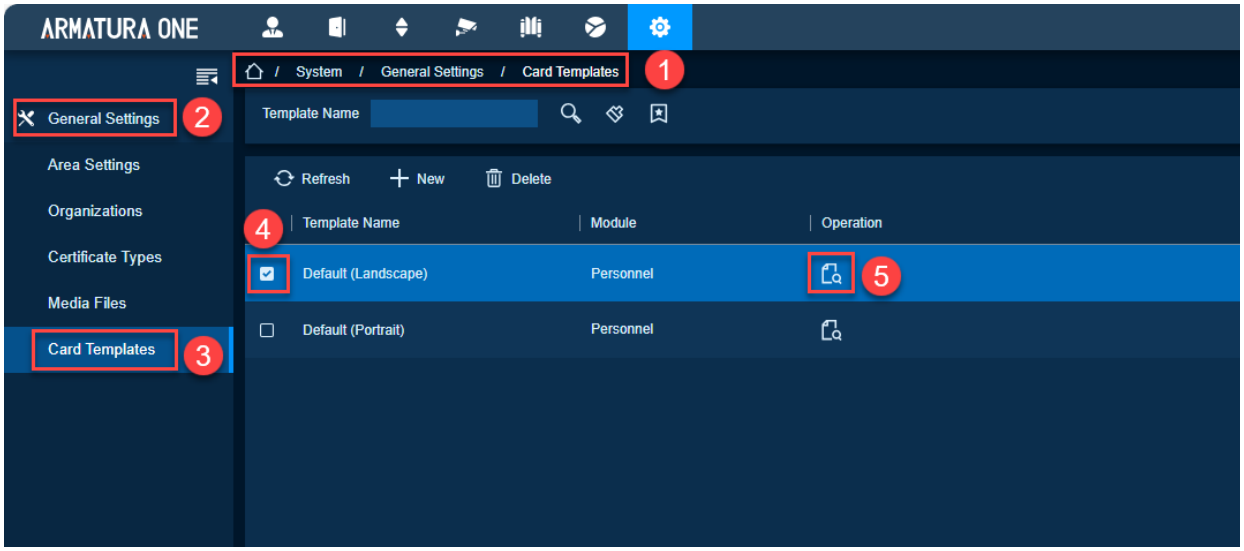
Trigger Result

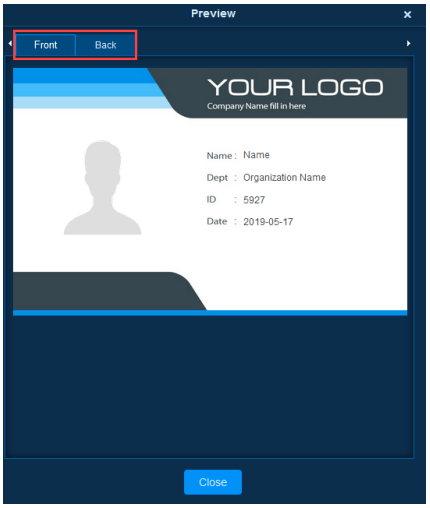
Displays a preview of the selected card template.

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Click the **[Preview]** icon to open the preview window and view the template details.





11.2 Data Management

Function List

Operation	Description
Operation Log	View and track all system operations and user activities through comprehensive logs.
Dictionary Management	Reference system for error codes and enables users to diagnose software issues through self-checks.
Database Management	Perform database maintenance tasks including refresh, backup, and scheduled operations.

Copyright © 2024 ARMATURA LLC. All rights reserved

Data Cleaning	Optimize server storage space by removing unnecessary data and maintaining efficient database size.
System Monitoring	Monitor and analyse server performance and resource utilization.
Event Types	Review and manage system events type.

11.2.1 Operation Logs

Export

Prerequisites for Use

User must have Administrator access with Operation Logs Export permissions.

Usage Scenarios

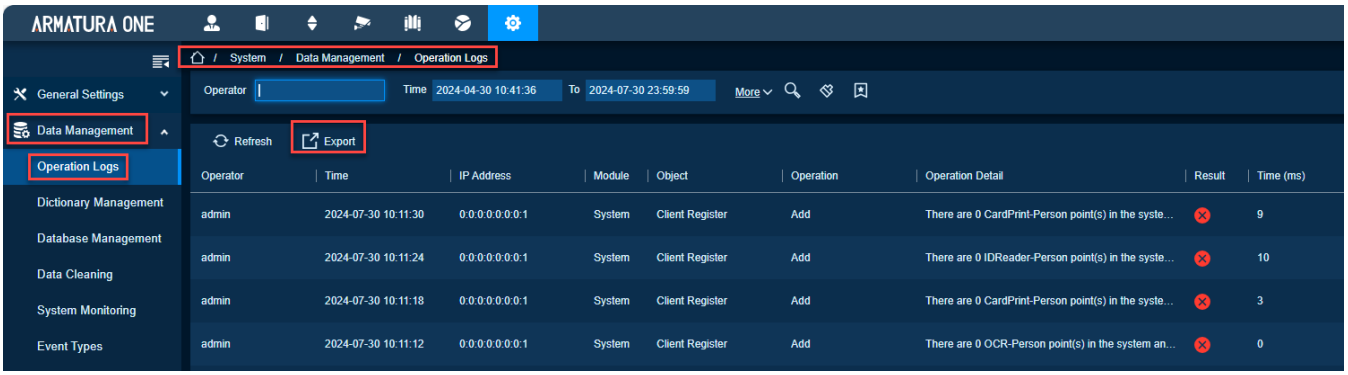
Export operation log data to your local computer.

Trigger Result

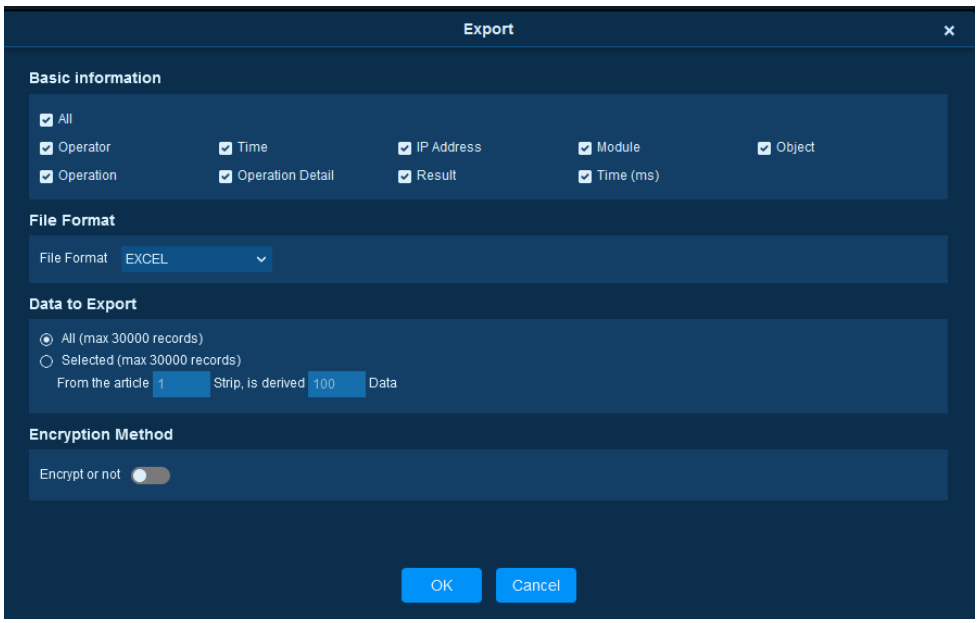
Operations	Description
Select Excel	Export data in Excel format
Select PDF	Export data in PDF format
Select CSV	Export data in CSV format
Select All	Export complete log history
Select Selected	Export logs within a specified date range

Steps:

- Click the **[Export]** button to open the export window.
- Choose your preferred file format.
- Specify the desired date range for export.
- Click **[OK]** to complete the export process



Copyright © 2024 ARMATURA LLC. All rights reserved

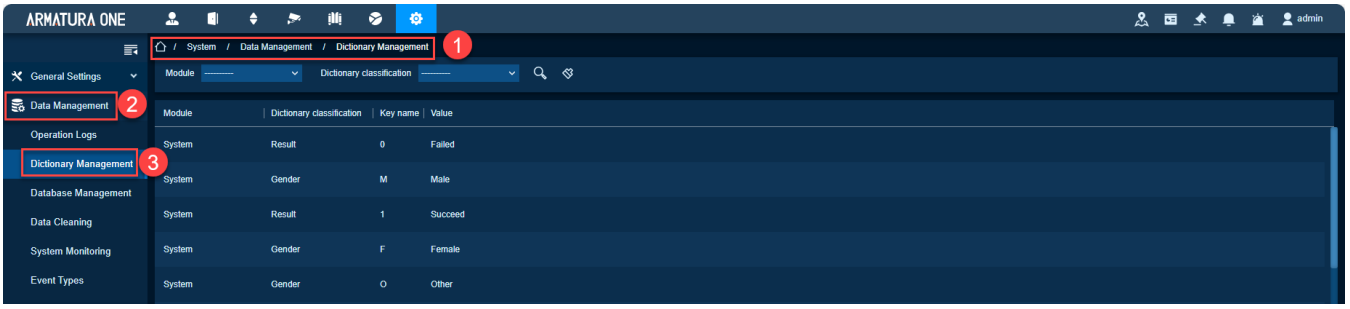


11.2.2 Dictionary Management

Function Description

Dictionary management provides a reference system for error codes and enables users to diagnose software issues through self-checks.

Interface Display



Module: Indicates the system module name

Dictionary classification: Shows the category of the dictionary entry

Key name: Displays the specific parameter name or identifier

Value: Contains the corresponding value or setting for the key

11.2.3 Database Management

Copyright © 2024 ARMATURA LLC. All rights reserved

Function Description

Display historical database backup operations and manage database functions including refresh, backup, and scheduled operations. Users can perform both manual and automated backups with optional FTP server integration.

Backup Now

Prerequisites for Use

User must have Administrator access with immediate backup permissions or backup permissions and FTP server access rights.

Usage Scenarios

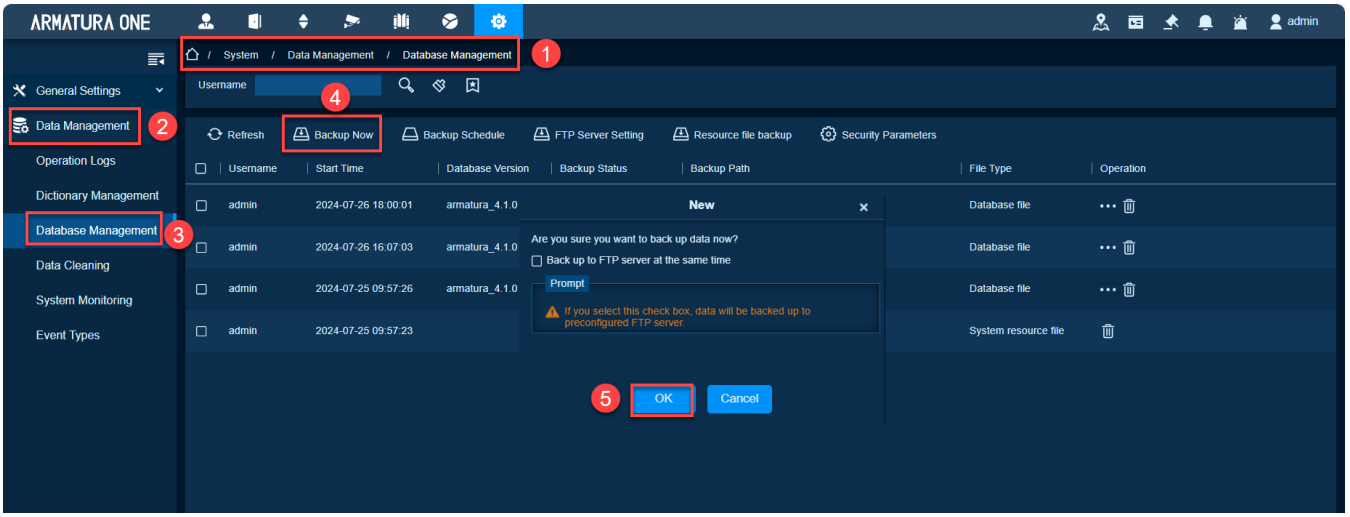
Perform immediate manual backup of the local network database and restore data from manual backups.

Trigger Result

Creates an immediate database backup and confirms successful data preservation.

Steps:

- Click **[Backup Now]** to open the backup window.
- Select whether to save to FTP server (optional).
- Click **[OK]** to initiate the backup process



Backup Schedule

Prerequisites for Use

User must have Administrator access with scheduled backup permissions.

Usage Scenarios

Configure automated database backups at specified intervals.

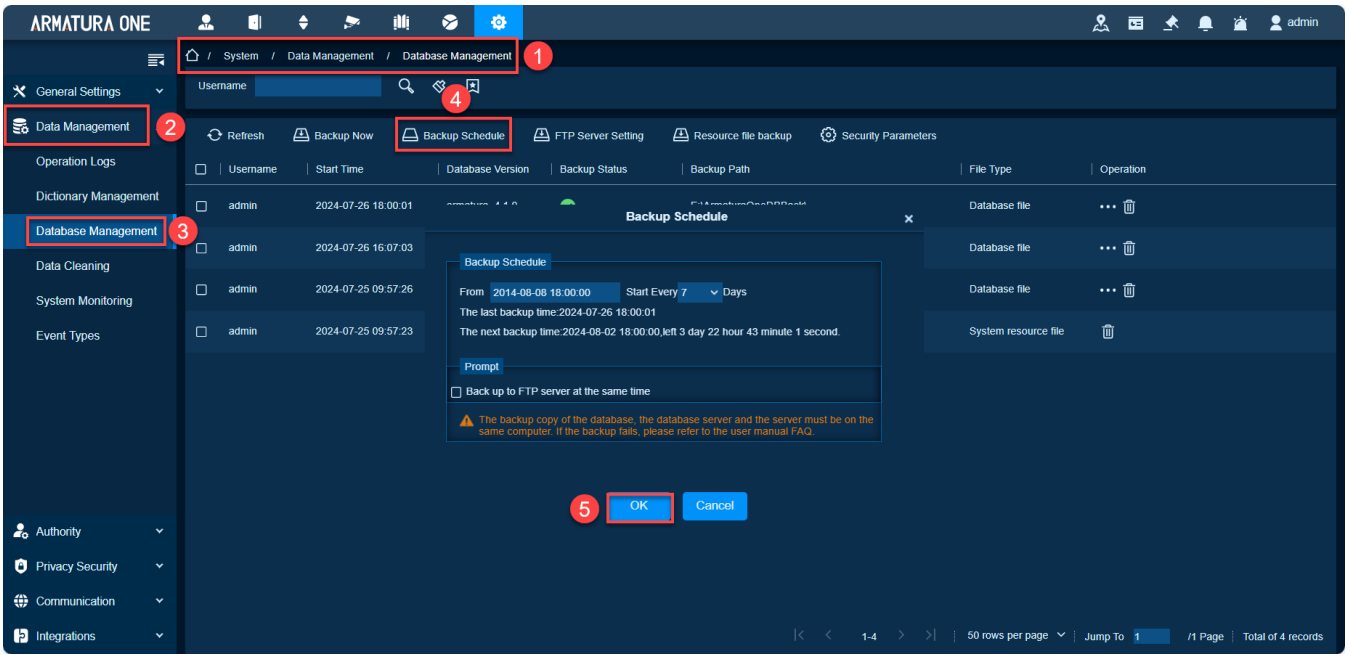
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Executes automatic backups according to the defined schedule.

Step:

- Click **[Backup Schedule]** to open the scheduling window.
- Configure the desired backup frequency and timing.
- Select whether to sync with FTP server (optional).
- Click **[OK]** to save the backup schedule.



FTP Server Setting

Prerequisites for Use

User must have Administrator access with FTP server configuration permissions.

Usage Scenarios

Configure FTP server settings required for remote backup storage.

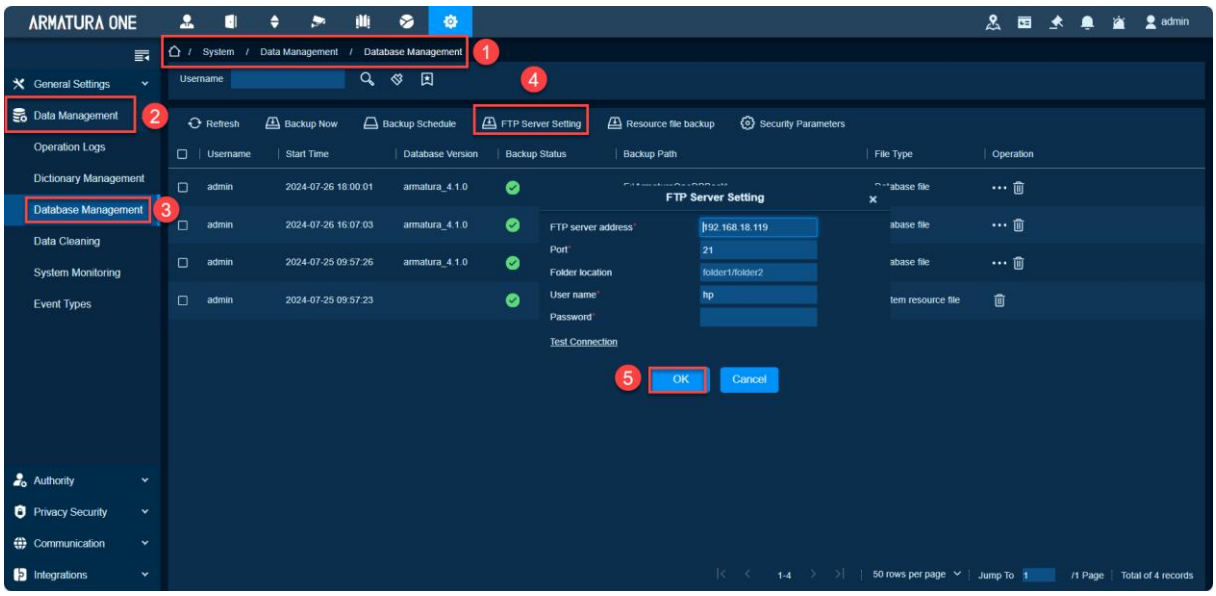
Trigger Result

Establishes FTP server connection for backup operations.

Steps:

- Click **[FTP Server Setting]** to open the configuration window.

Copyright © 2024 ARMATURA LLC. All rights reserved



- Enter the required information, fields marked with * are mandatory:

FTP Server Address: Enter the FTP server address

Port: Specify the connection port number

Folder Location: Define the backup storage path

Username: Enter FTP account username

Password: Enter FTP account password

- Click **[OK]** to save the FTP configuration

Resource File Backup

Prerequisites for Use

User must have Administrator access with system resource backup permissions.

Usage Scenarios

Backup system resource files in conjunction with database backups.

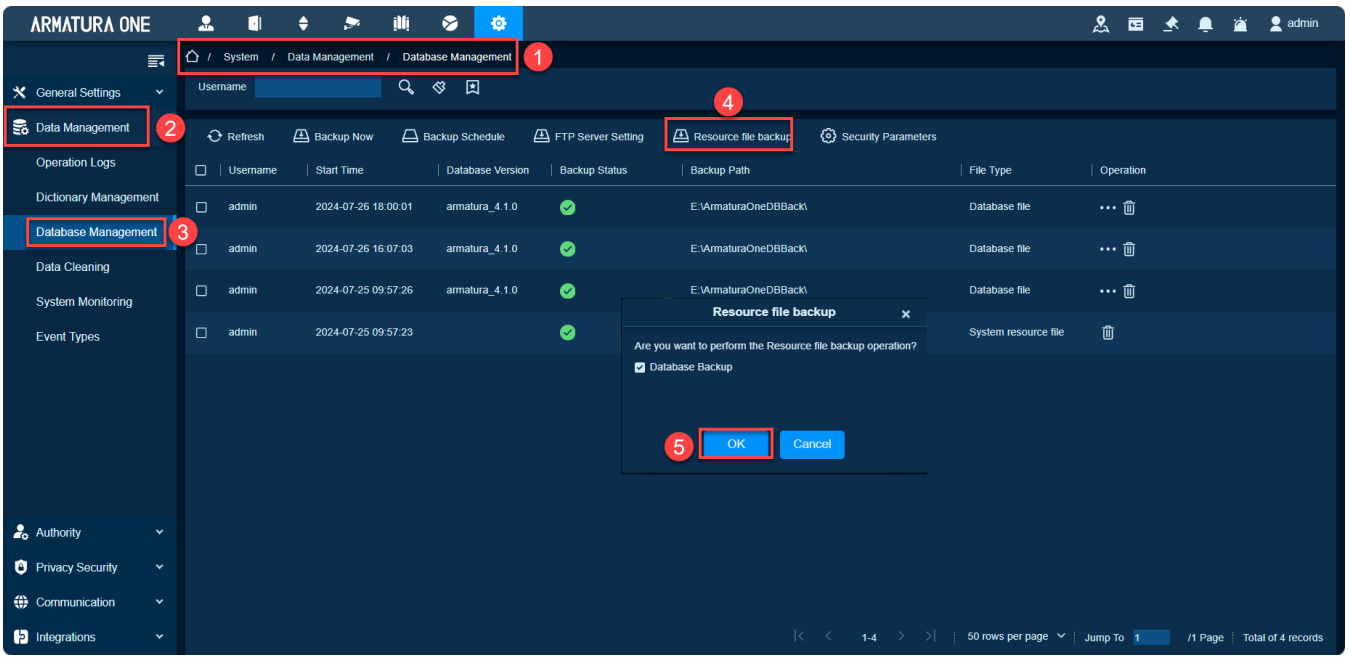
Trigger Result

Creates a backup of system resource files.

Steps:

- Click **[Resource File Backup]** to open the backup window.
- Click **[OK]** to initiate resource file backup.

Copyright © 2024 ARMATURA LLC. All rights reserved



Security Parameters

Prerequisites for Use

User must have Administrator access with security configuration permissions.

Usage Scenarios

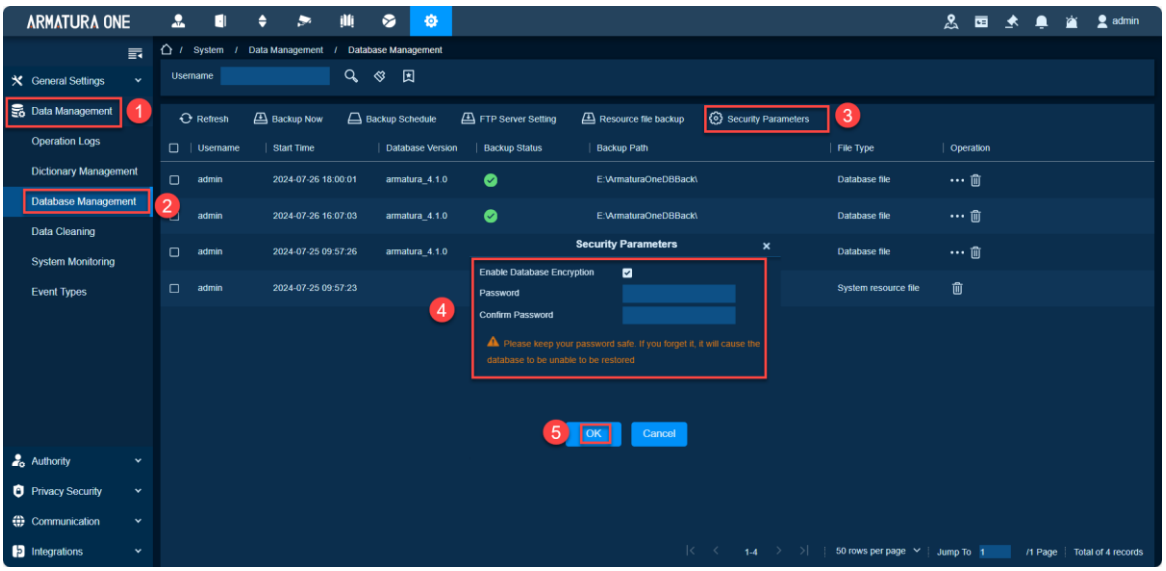
Configure database encryption settings for enhanced security.

Trigger Result

Enables database encryption with password protection.

Steps:

- Click **[Security Parameters]** to open the settings window.
- Enable database encryption, set password, and click **[OK]** to implement security settings.



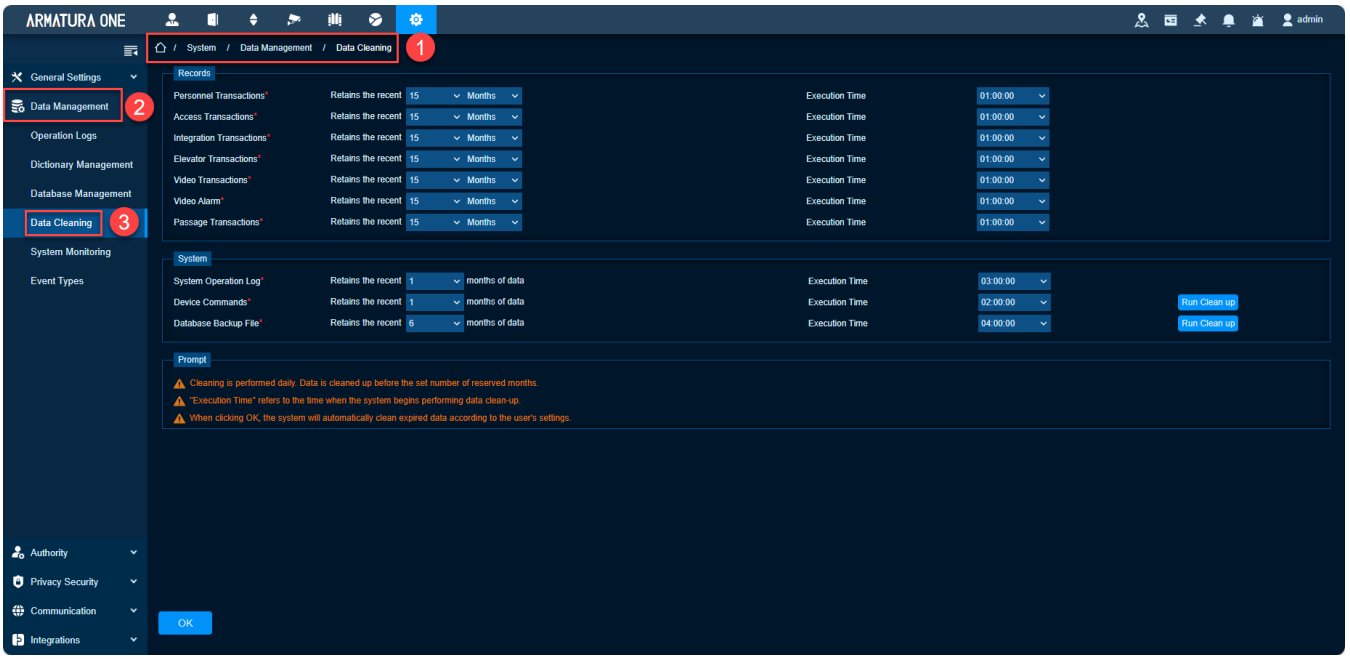
Copyright © 2024 ARMATURA LLC. All rights reserved

11.2.4 Data Cleaning

Function Description

The data cleaning feature optimizes server storage space by removing unnecessary data, ensuring efficient database management and preventing excessive server storage consumption.

Interface Display



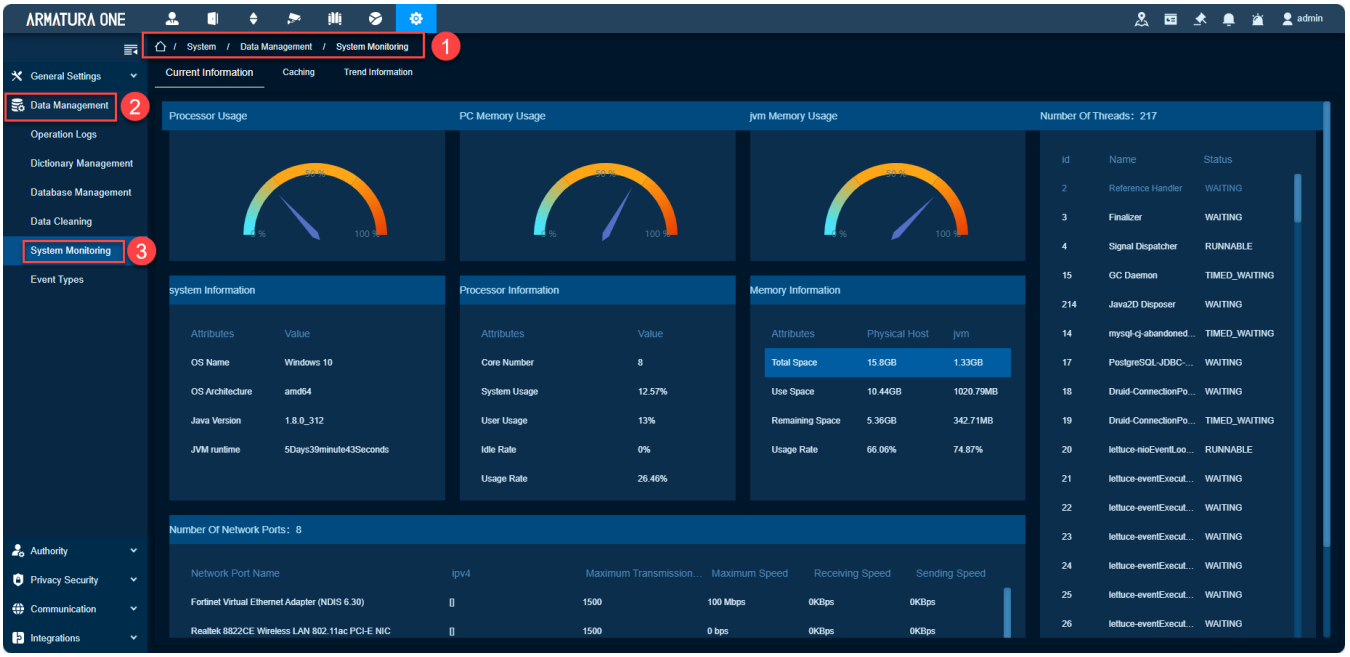
11.2.5 System Monitoring

Function Description

Monitor and analyse server load utilization in real-time.

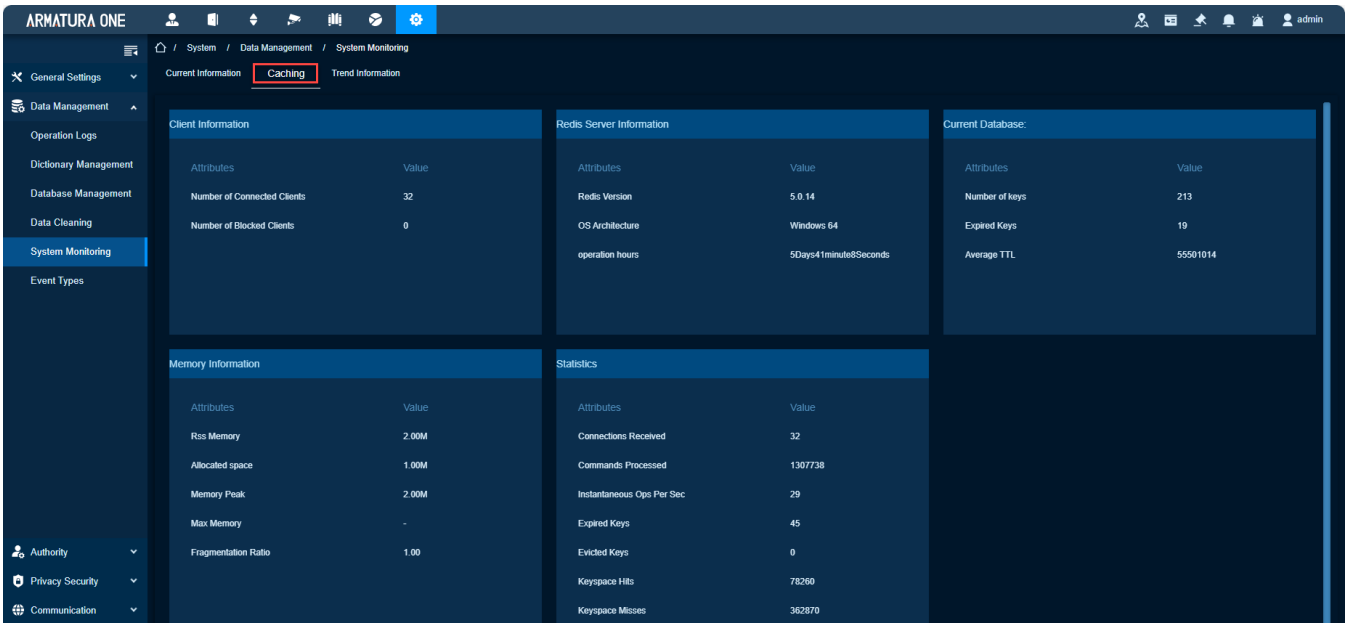
Copyright © 2024 ARMATURA LLC. All rights reserved

Function Page Display



Catching

Users can access comprehensive system information including Client details, Redis Server status, Current Database Memory usage, and detailed Statistics.



Trend Information

View detailed performance metrics through System Performance Trend and Thread Number Trend visualizations, providing insights into system behaviour over time.

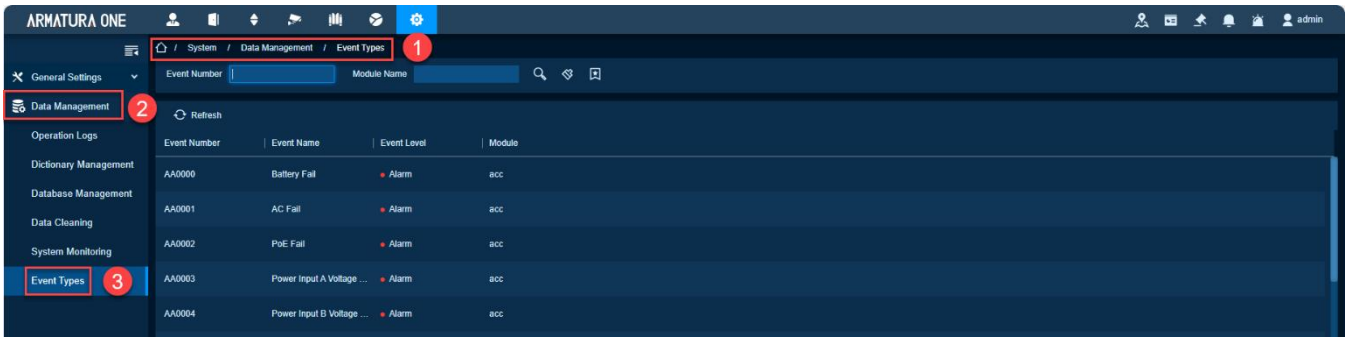
Copyright © 2024 ARMATURA LLC. All rights reserved

11.2.6 Event Types

Function Description

View and manage all configured event types within the system. This section provides access to the complete list of event classifications and their associated settings.

Function Page Display



11.3 Authority

The Authority section enables comprehensive management of the ARMATURA One system's security and access controls. Here you can administer user accounts, configure roles, and establish system security parameters.

Function List

Operations	Description
Users	Create, edit, and remove system user accounts
Users Online	Monitor active users and terminate sessions

Copyright © 2024 ARMATURA LLC. All rights reserved

Roles	Manage user roles and their associated permissi
Apps Management	Configure third-party application access
Security Parameters	Configure system security settings and policies
Threat Levels	Define and manage threat level configurations

11.3.1 Users

Function Description

Create new users in the system and configure their access levels.

Add

Prerequisites for Use

Administrator must have user creation permissions. Each username must be unique within the system.

Usage Scenarios

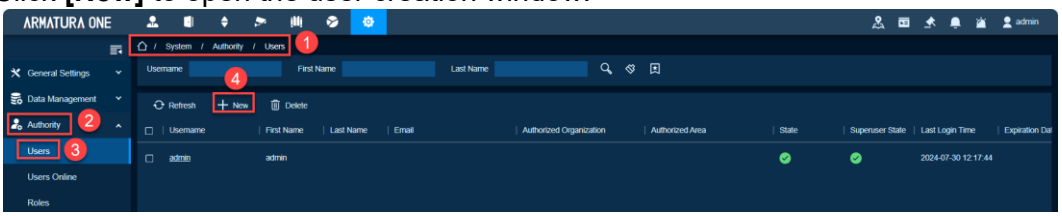
Creating new user accounts in the system.

Trigger Result

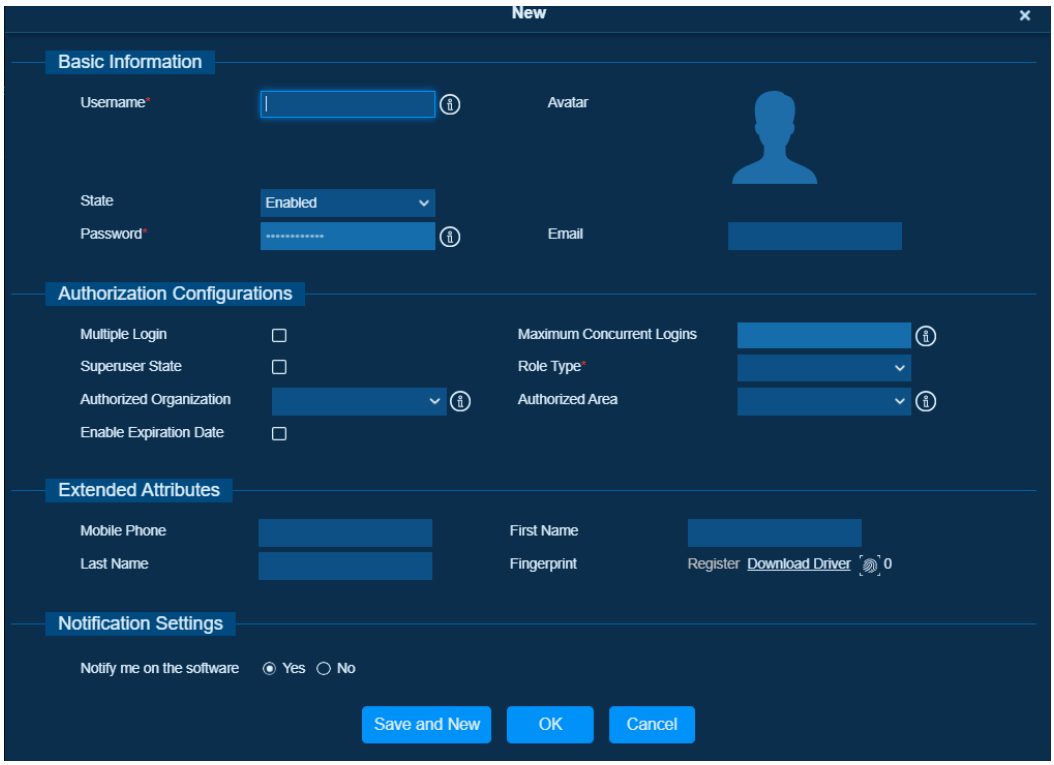
New user account is created in the system.

Steps:

- Click **[New]** to open the user creation window.



Copyright © 2024 ARMATURA LLC. All rights reserved



- Complete the required fields (marked with *). Field descriptions:

Username: User's login identifier

Avatar: User's profile image - click to browse and select

State: Account status

Password: User's login password (defaults to Admin)

Email: User's email address for password recovery

Multiple Login: Enable simultaneous login sessions

Maximum Number: Set limit for concurrent login sessions

Superuser State: Grant superuser administrator privileges

Role: Assign user role

Auth Department: Specify authorized department

Authorize Area: Define authorized access areas

Enabled expiration date: Set account validity period

Mobile Phone: User's contact number

First Name: User's given name

Last Name: User's family name

Fingerprint: Click **[Registration]** to enroll user's fingerprint

Copyright © 2024 ARMATURA LLC. All rights reserved

- Click **[OK]** to create the user

Delete

Prerequisites for Use

Administrator must have deletion permissions. Only initialization admin users cannot be deleted

Usage Scenarios

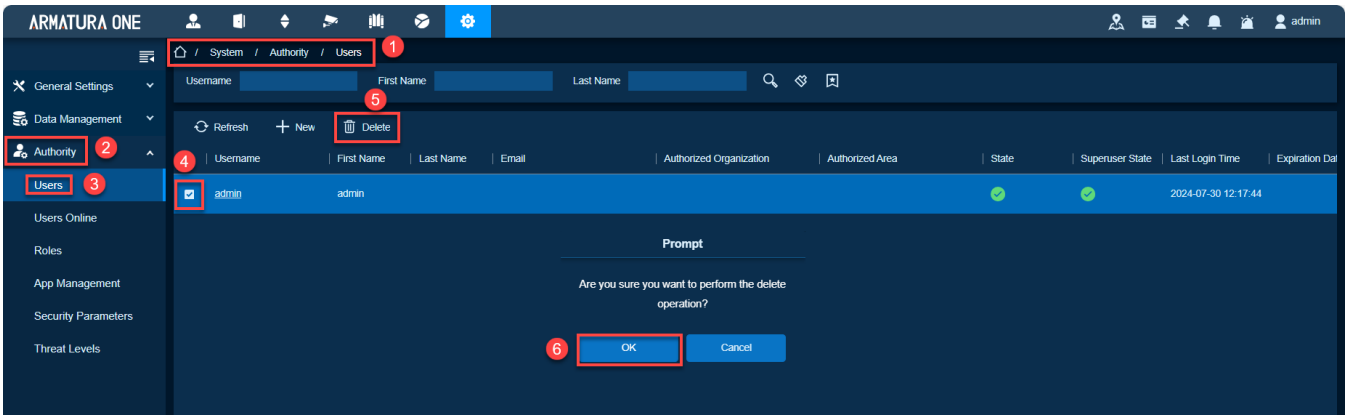
Remove obsolete or unnecessary user accounts.

Trigger Result

Selected user account is removed from the system.

Steps:

- Select target user account.
- Click **[Delete]** to open confirmation dialog.
- Click **[OK]** to confirm deletion



Edit

Prerequisites for Use

Administrator must have edit permissions.

Usage Scenarios

Modify existing user account information.

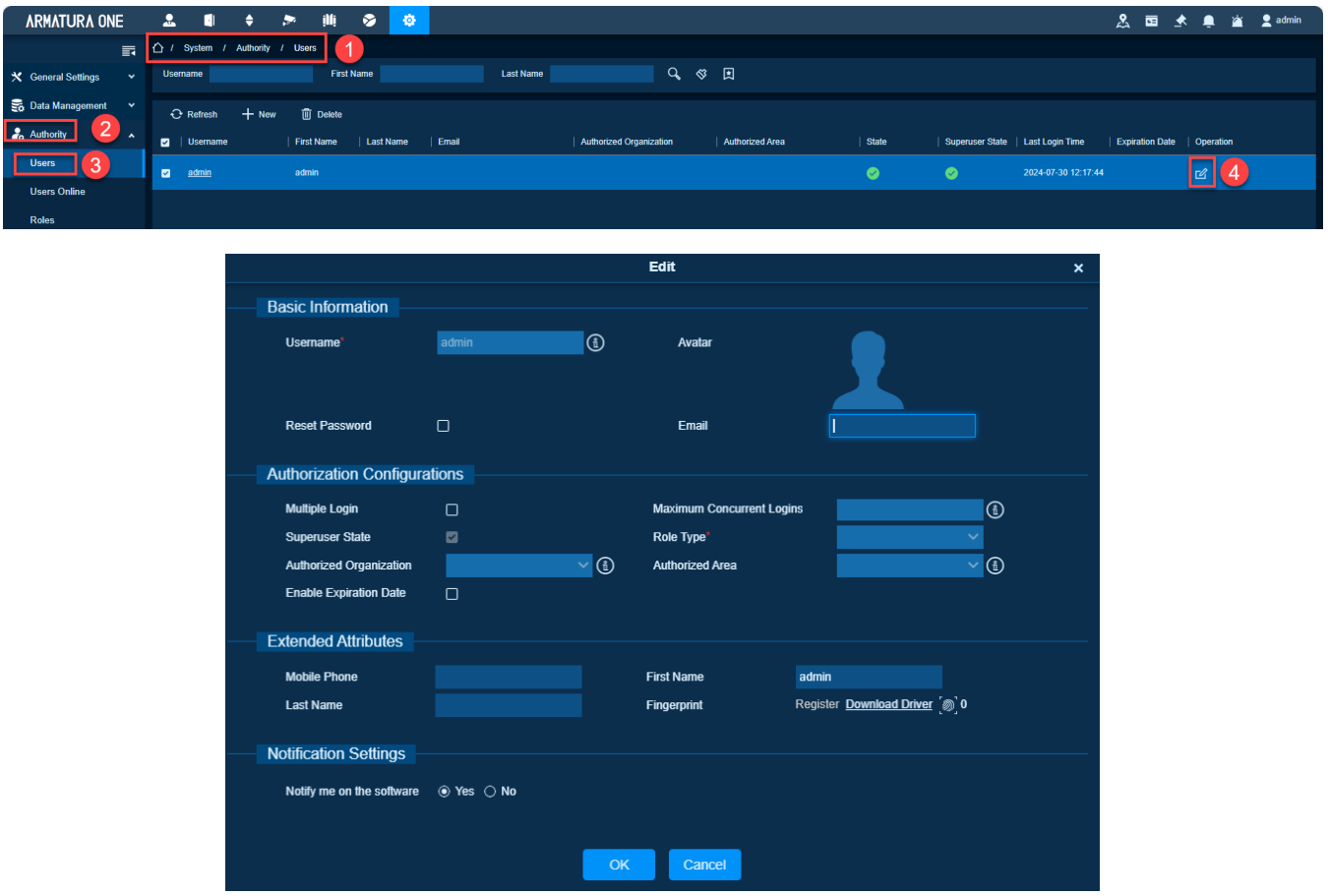
Trigger Result

Selected user account information is updated.

Steps:

- Select target user account.
- Click **[Edit]** to open modification window.
- Click **[OK]** to save changes.

Copyright © 2024 ARMATURA LLC. All rights reserved



11.3.2 Users Online

Function Description

Monitor active system users and manage their sessions in the ARMATURA One system, including the ability to terminate user sessions when necessary.

Force Logout

Prerequisites for Use

Only Administrator user accounts have permission to force logout other users.

Usage Scenarios

Terminate user sessions when required for security or system management purposes.

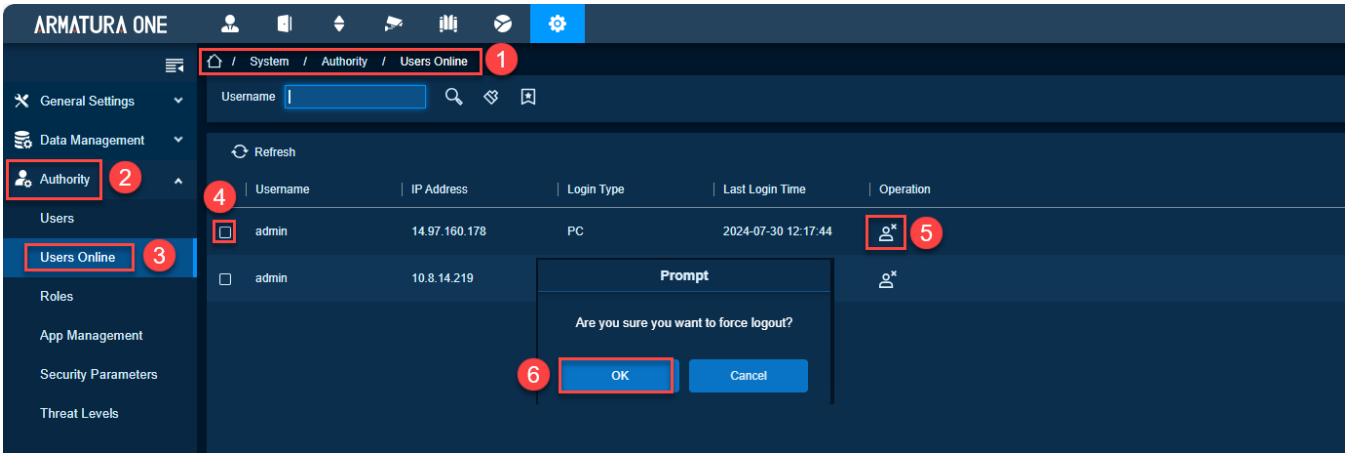
Trigger Result

User is logged out of the system immediately.

Step:

- Click **[Force Logout]**, confirm action in the popup window by clicking **[Ok]**

Copyright © 2024 ARMATURA LLC. All rights reserved



11.3.3 Roles

Function Description

Manage system roles and their associated permissions, including creation, modification, and removal of role definitions.

New (Add)

Prerequisites for Use

Administrator must have role creation permissions. Each role code must be unique.

Usage Scenarios

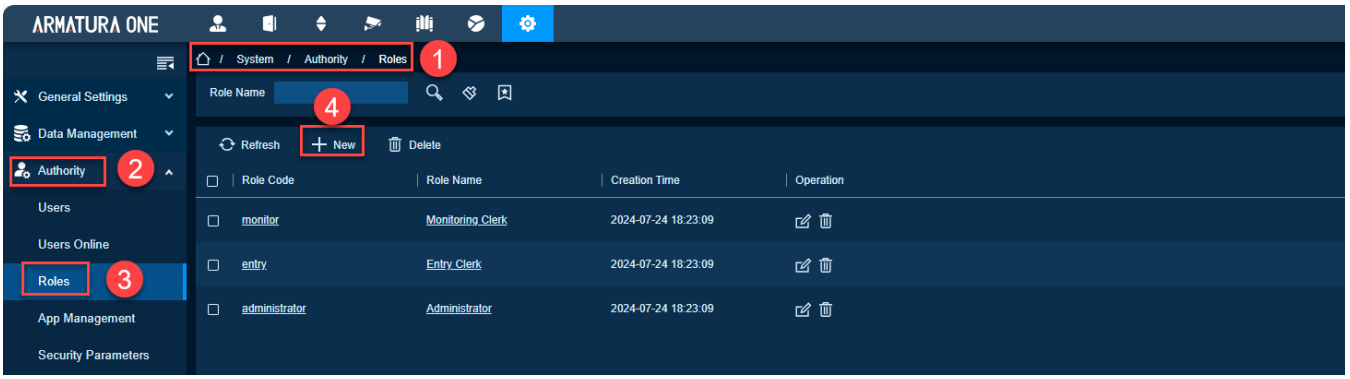
Create new roles when existing roles do not meet system requirements.

Trigger Result

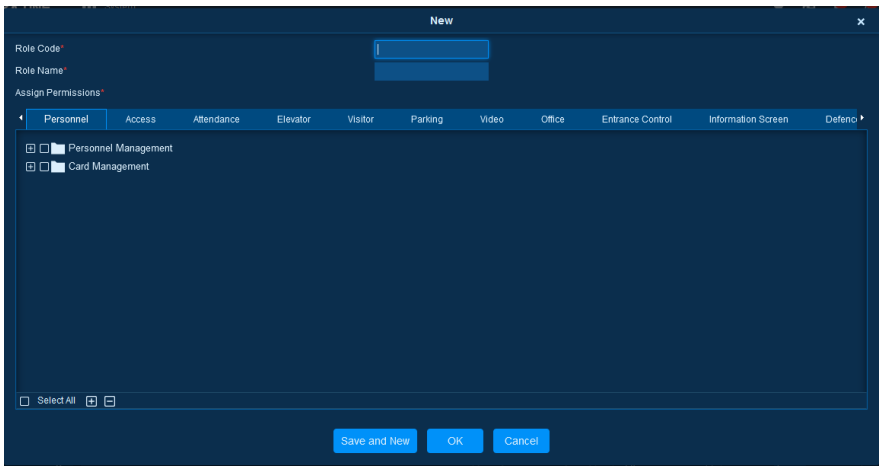
New role is created in the system.

Step:

- Click **[New]** to open role creation window.
- Enter required information:



Copyright © 2024 ARMATURA LLC. All rights reserved



Role Code: Unique identifier for the role

Role Name: Descriptive name for the role

- Select permissions to assign to the role.
- Click **[OK]** to create the role.

Delete

Prerequisites for Use

Administrator must have role deletion permissions. Only non-system roles can be deleted.

Usage Scenarios

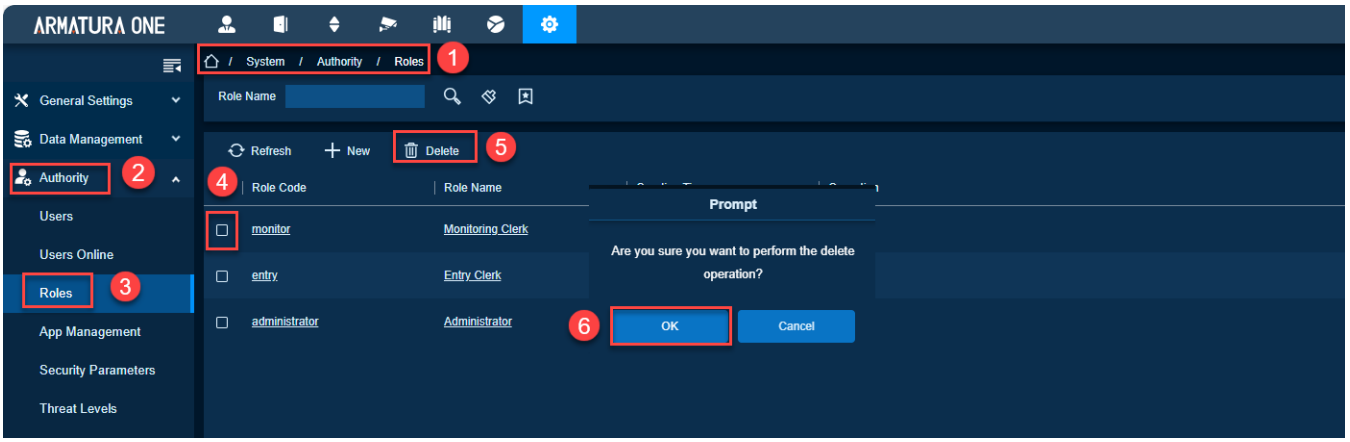
Remove obsolete or unnecessary roles from the system.

Trigger Result

Selected role is removed from the system.

Steps:

- Select target role.
- Click **[Delete]** to open confirmation dialog.
- Click **[OK]** to confirm deletion.



Copyright © 2024 ARMATURA LLC. All rights reserved

Edit

Prerequisites for Use

Administrator must have role modification permissions. Only non-system roles can be modified.

Usage Scenarios

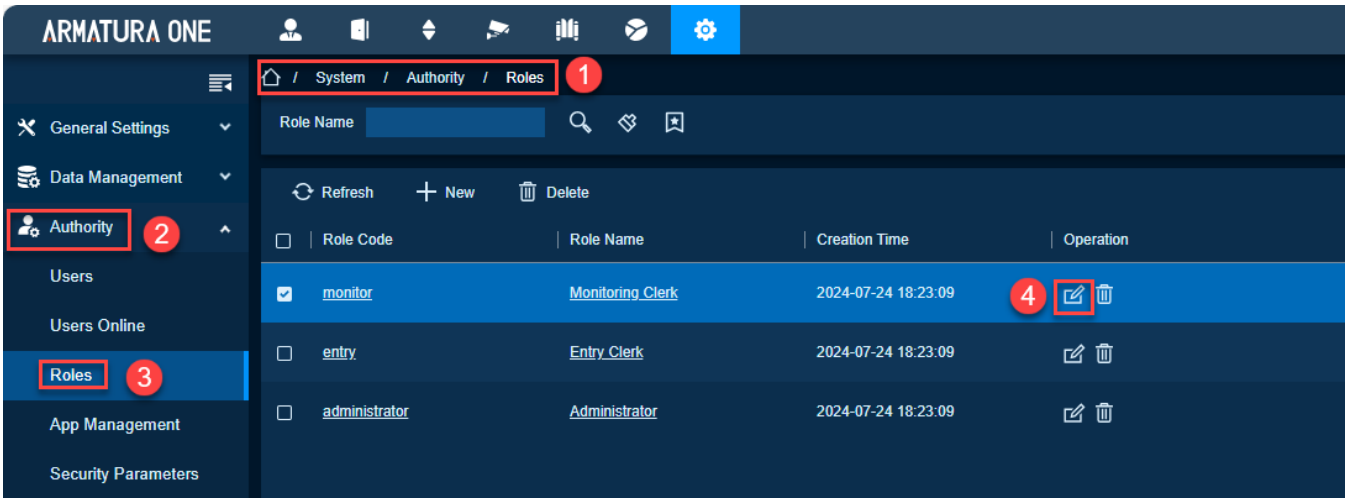
Modify existing role definitions and permissions.

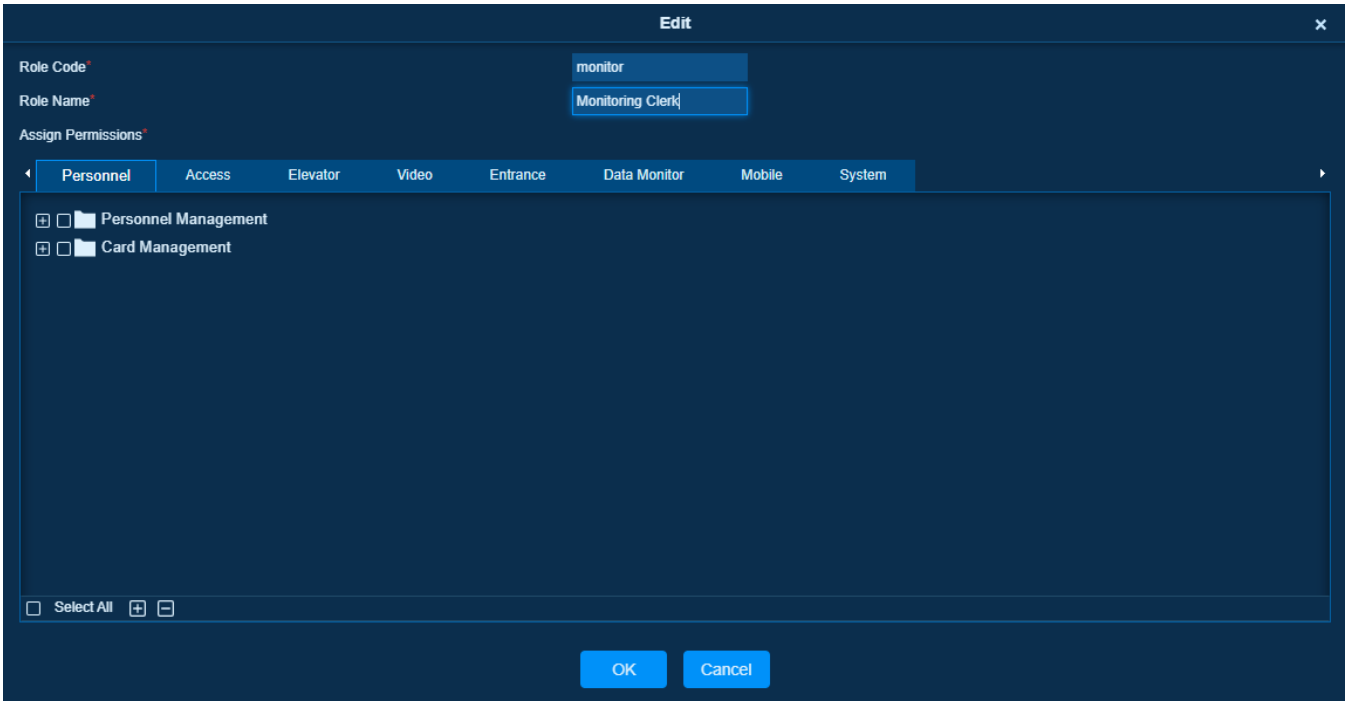
Trigger Result

Selected role configuration is updated.

Steps:

- Select target role.
- Click **[Edit]** to open modification window.
- Click **[OK]** to save changes.





Copyright © 2024 ARMATURA LLC. All rights reserved

11.3.4 App Management

Function Description

Manage application registrations within the system and generate registration codes for module functionality. The system controls access through allocated license points.

New (Add)

Prerequisites for Use

Administrator must have app registration permissions, and sufficient license points must be available for the desired modules.

Usage Scenarios

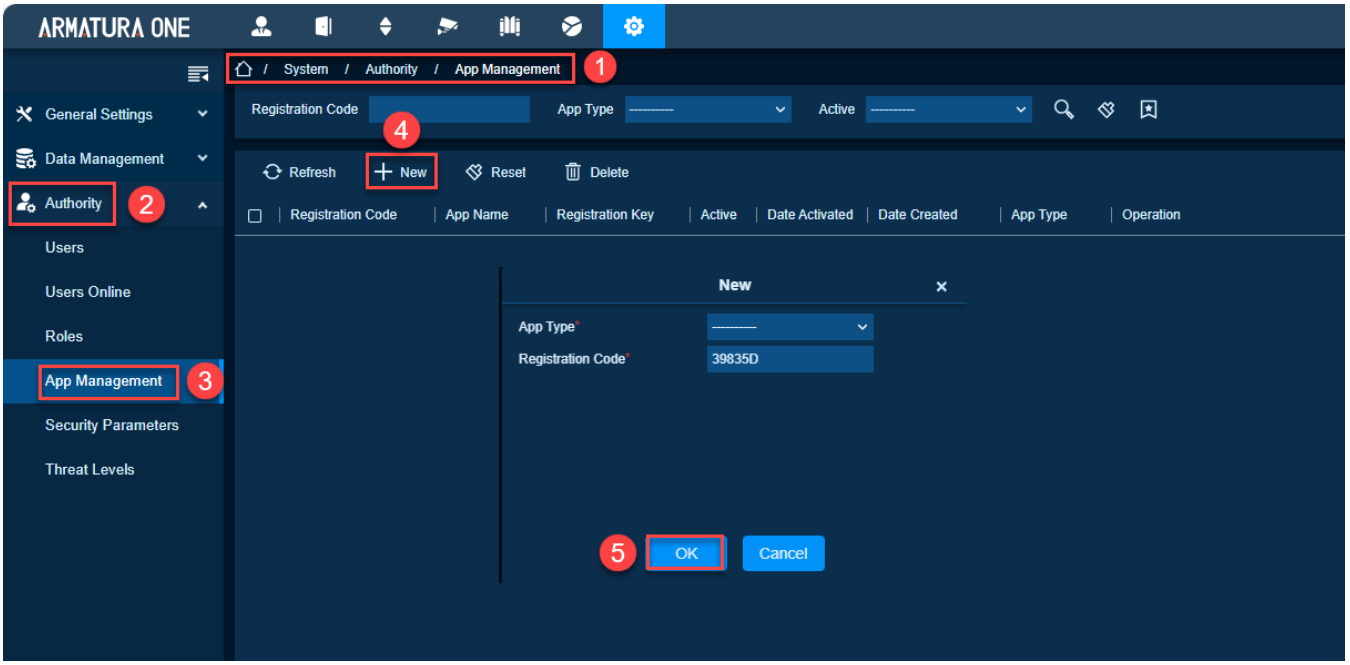
Register new devices to enable module functionality.

Trigger Result

New application registration is created.

Steps:

- Click **[New]** to open registration window.
- Select the desired application type or registration code.
- Click **[OK]** to complete registration.



Copyright © 2024 ARMATURA LLC. All rights reserved

Reset

Prerequisites for Use

Administrator must have reset permissions.

Usage Scenarios

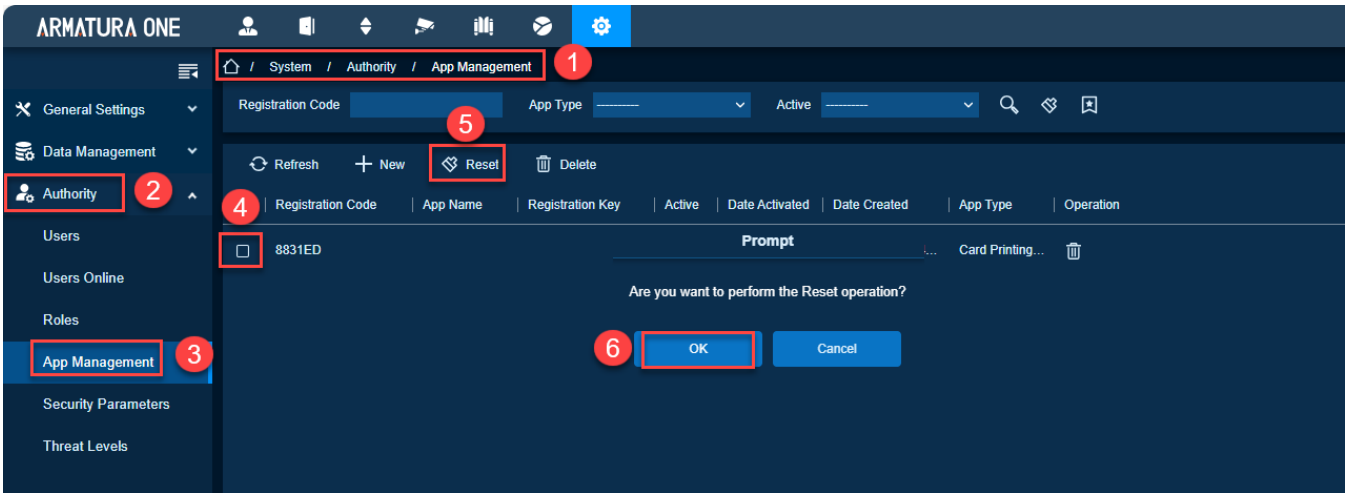
Reset client configurations when necessary.

Trigger Result

Selected client settings are restored to default.

Steps:

- Select target client.
- Click **[Reset]** to open confirmation dialog.
- Click **[OK]** to confirm reset.



Delete

Prerequisites for Use

Administrator must have client deletion permissions.

Usage Scenarios

Remove unnecessary or redundant client registrations.

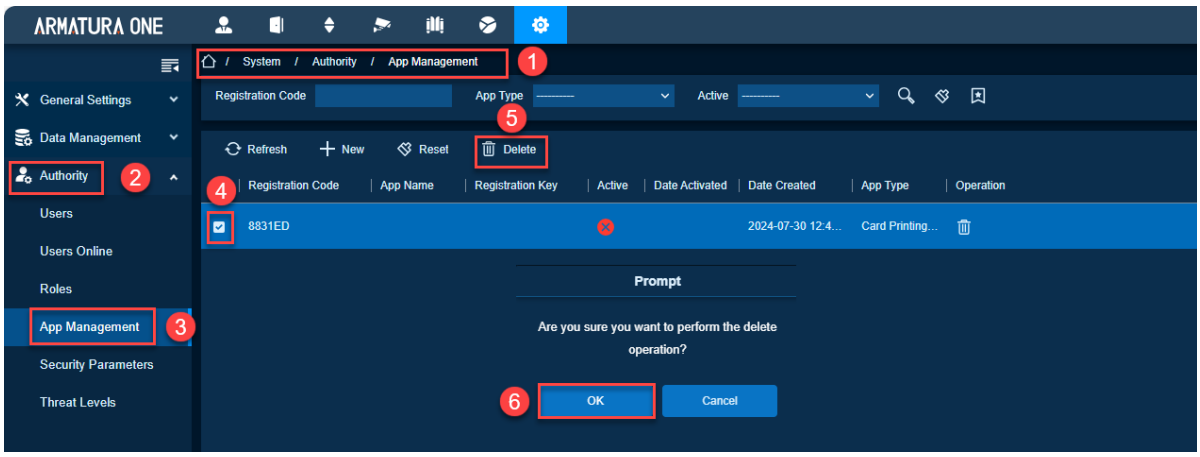
Trigger Result

Selected client registration is removed.

Steps:

- Select target client.
- Click **[Delete]** to open confirmation dialog.
- Click **[OK]** to confirm deletion.

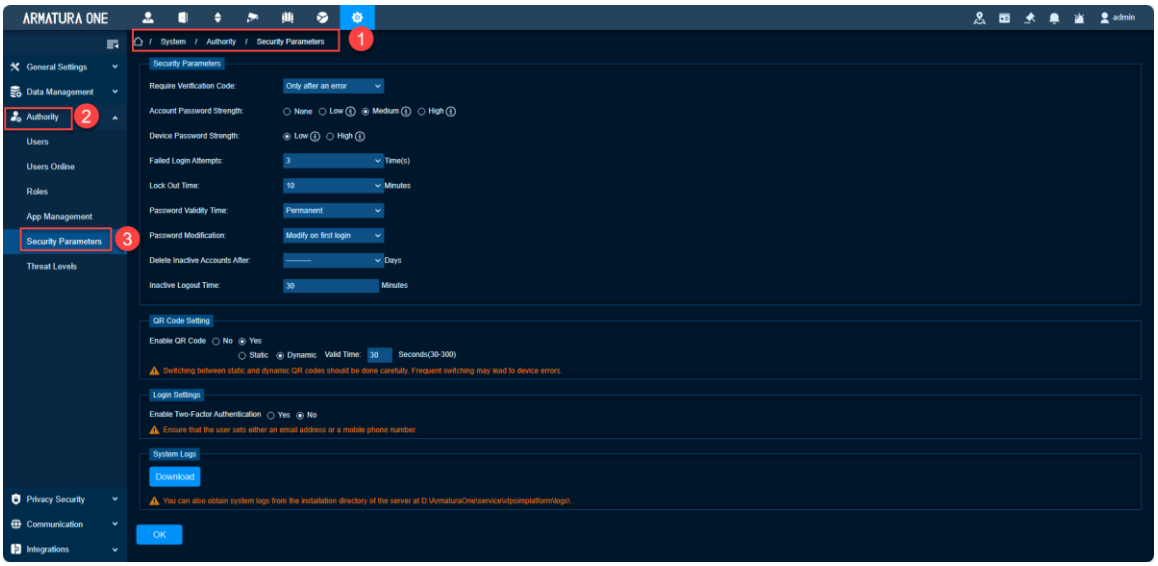
Copyright © 2024 ARMATURA LLC. All rights reserved



11.3.5 Security Parameters

Function Description

Configure system-wide security settings and authentication parameters.



Field Description

Login verification code: Configure verification code requirements during login

Default Password Strength: Define minimum password complexity requirements

Failed login: Set maximum number of failed logins attempts before account lockout

Account with lock: Configure account lockout duration and conditions

Password Valid Days (Day): Specify password expiration period

Password Modification: Define initial password change requirements

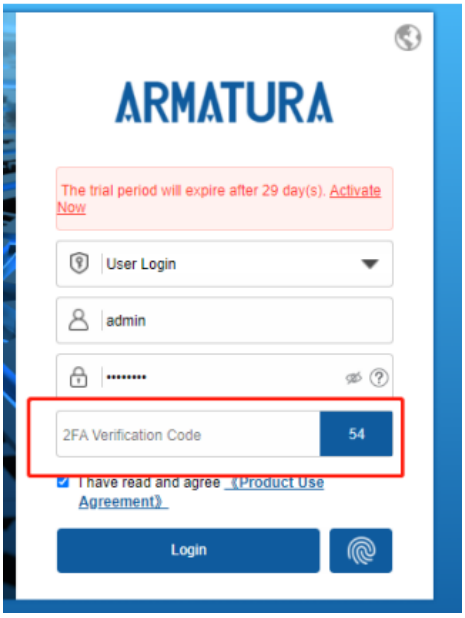
Delete Inactive Account: Set parameters for automatic removal of dormant accounts

Enable QR Code: Configure QR code authentication options including static or dynamic modes

Copyright © 2024 ARMATURA LLC. All rights reserved

Login Verification Settings: Configure two-factor authentication settings, requiring additional verification via SMS or email codes for enhanced security

System Logs: Access application logs including errors, warnings, and general information



11.3.6 Threat Levels

Prerequisites for Use

[Personnel Threat Level] and **[Access Level Threat Level]** must be configured first:

- Set Personnel Threat Level
- Set Access Level Threat Level

Add Threat Level

Usage Scenarios

Configure specialized access control restrictions for specific scenarios such as Threats, Robberies, and Fires. Administrators can define threat levels for both personnel and doors.

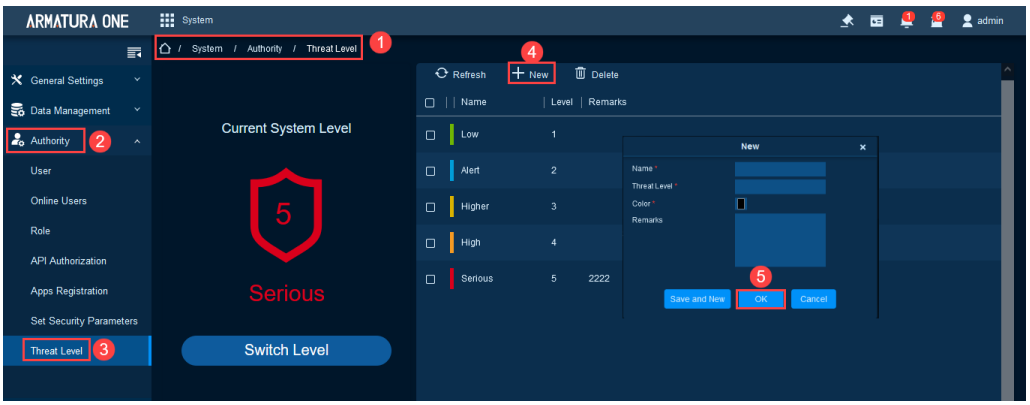
Trigger Result

New threat level is created in the system.

Steps:

- Click **[New]** to open creation window
- Click **[OK]** to save the threat level

Copyright © 2024 ARMATURA LLC. All rights reserved



Name: Descriptive identifier for the threat level

Threat Level: Numerical code between 1 and 254

Color: Any color supported by the system

Edit Threat Level

Prerequisites for Use

Administrator must have threat level modification permissions.

Usage Scenarios

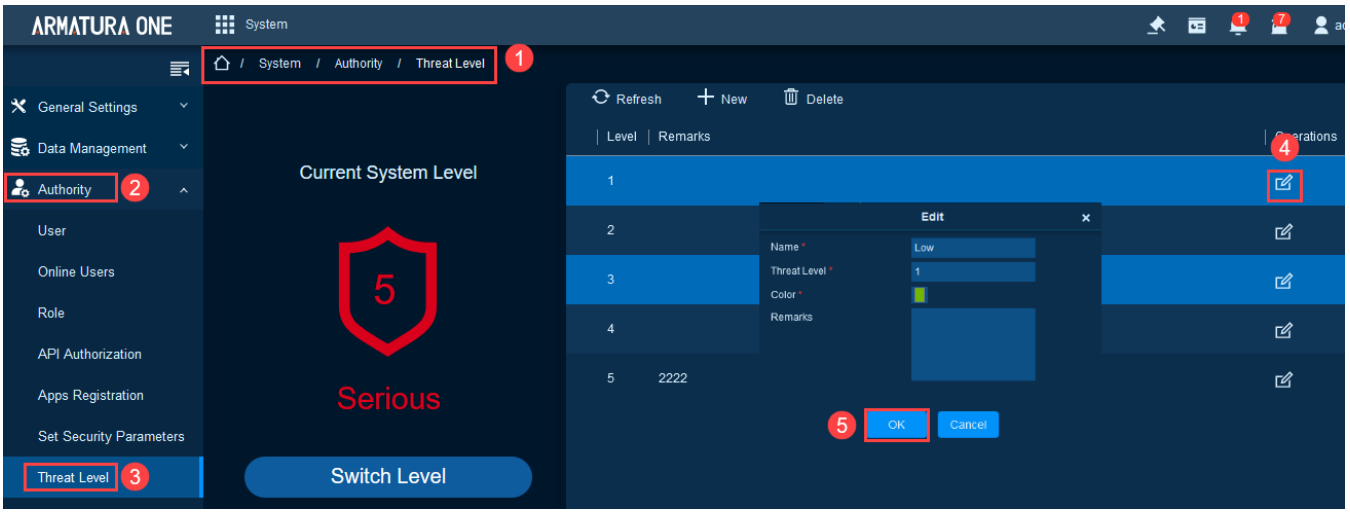
Modify existing threat level configurations.

Trigger Result

Selected threat level configuration is updated.

Steps:

- Select target threat level.
- Click **[Edit]** to open modification window.
- Click **[OK]** to save changes.



Name: Descriptive identifier for the threat level

Copyright © 2024 ARMATURA LLC. All rights reserved

Threat Level: Numerical code (cannot be modified during edit)

Color: Any color supported by the system

Delete Threat Level

Prerequisites for Use

Administrator must have threat level deletion permissions.

Usage Scenarios

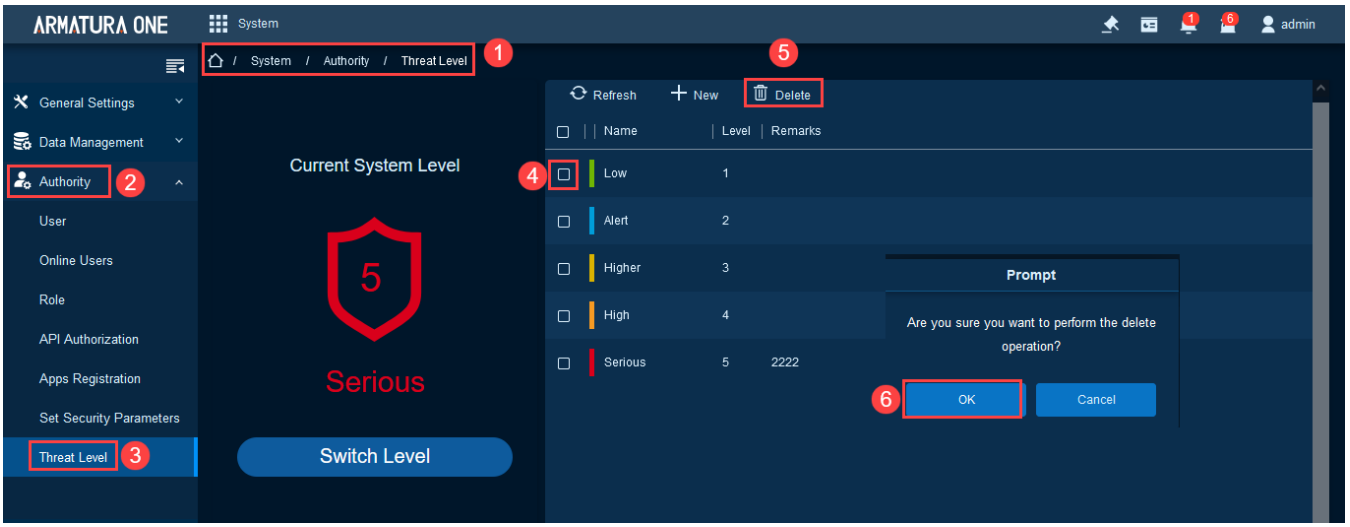
Remove unnecessary or redundant threat levels.

Trigger Result

Selected threat level is removed from the system.

Steps:

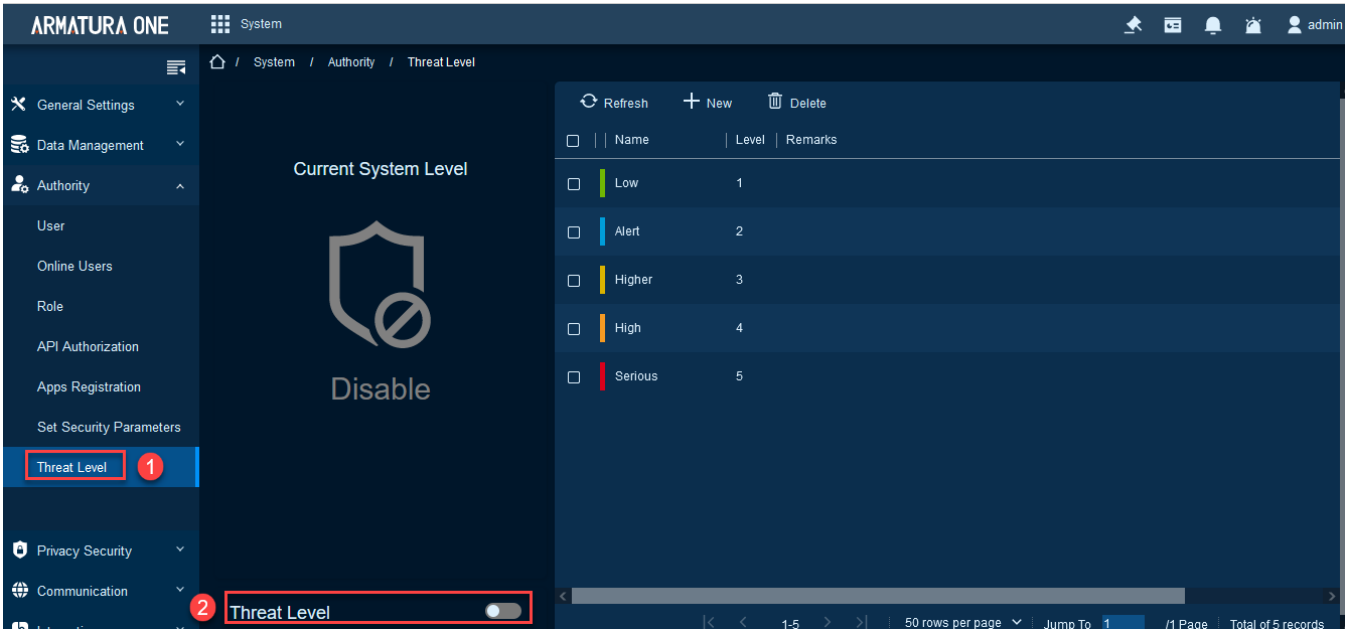
- Select target threat level.
- Click **[Delete]** to open confirmation dialog.
- Click **[OK]** to confirm deletion.



Switch Threat Level

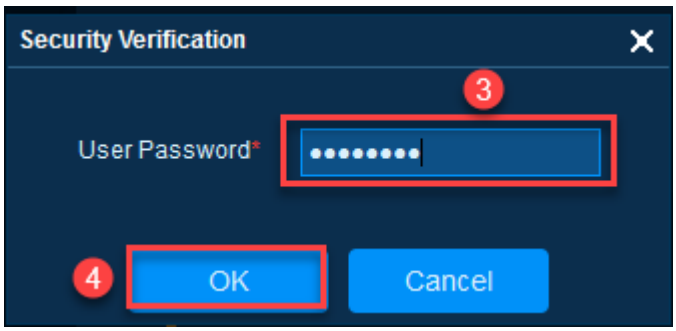
- Navigate to **[System] -> [Authority Management] -> [Manage Threat Levels]**

Copyright © 2024 ARMATURA LLC. All rights reserved



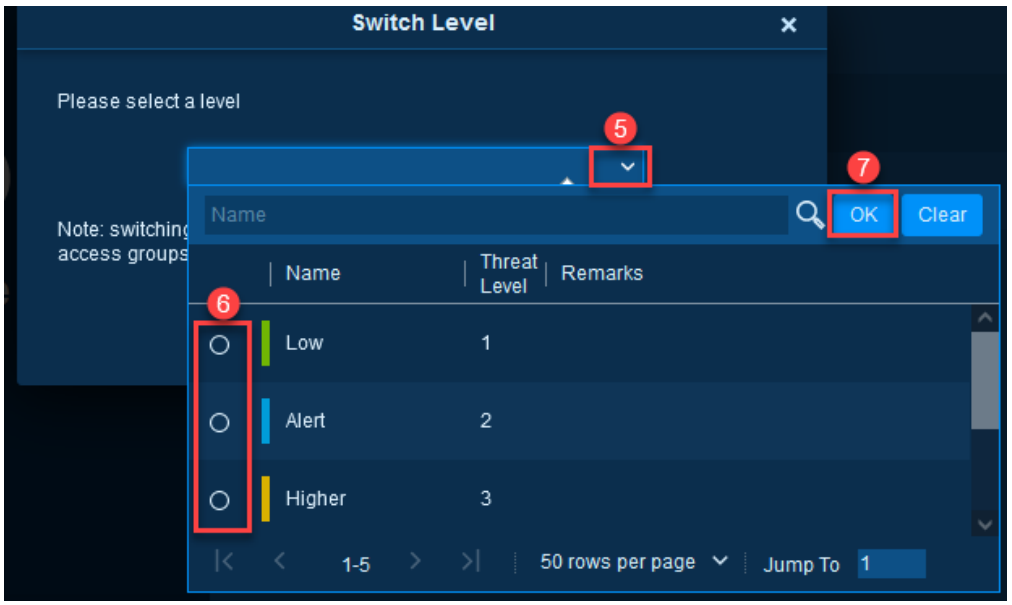
- Enable **Threat Level**

- Complete Security Verification



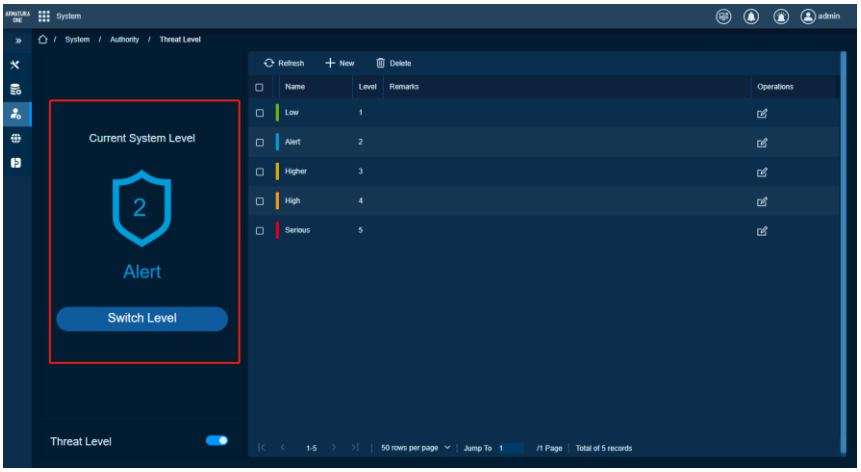
- Select different **System Threat Level**

Copyright © 2024 ARMATURA LLC. All rights reserved



Note:

Changing system threat level may invalidate certain user permissions and access groups. Active system threat level is displayed on the left side of the interface.



11.4 Privacy Security

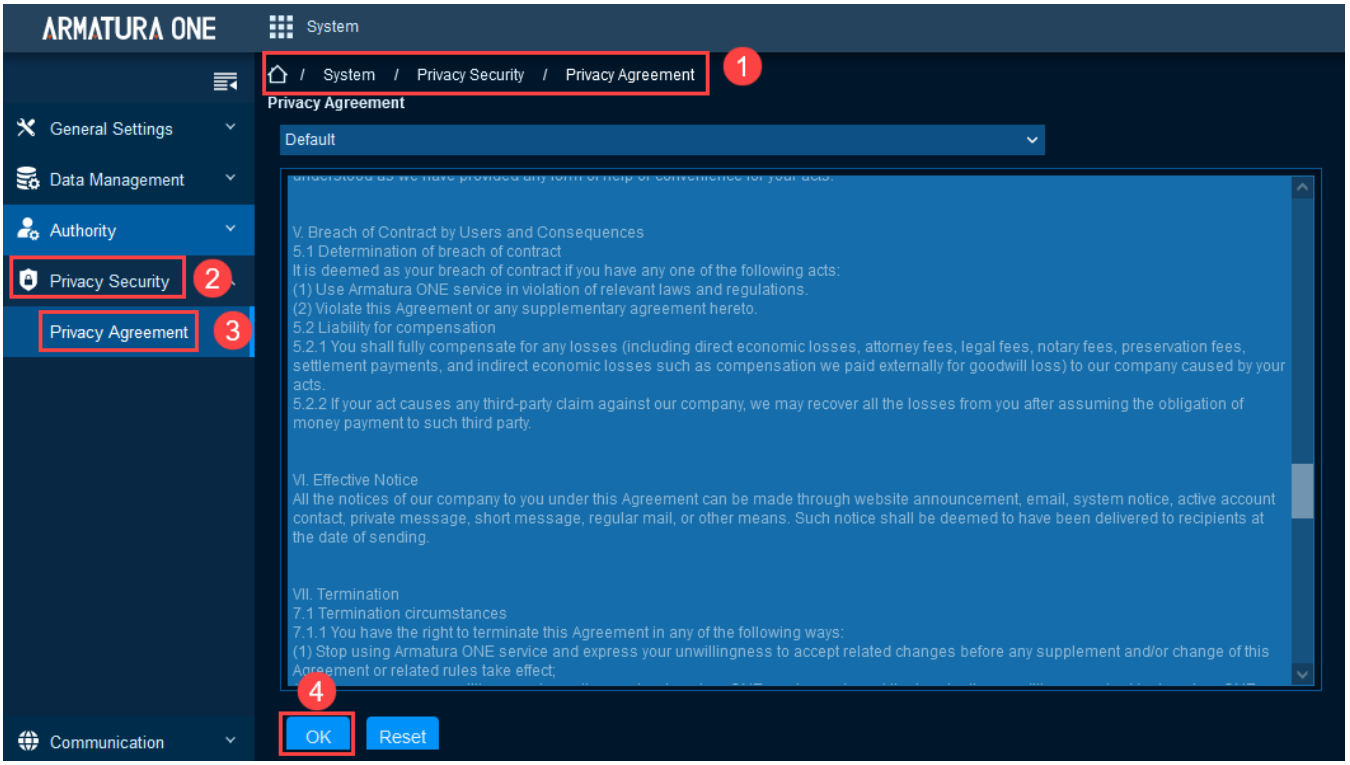
11.4.1 Privacy Agreement

Function Description

View the complete details of the system's Privacy Agreement and user data handling policies.

Copyright © 2024 ARMATURA LLC. All rights reserved

Function Page Display



11.5 Communication

Monitor and manage communication between software and hardware components, including device commands, connection status, product configurations, authorization settings, and communication services.

Function List

Operations	Description
Device Commands	View and export device command history f server
Communication Status	Monitor authorized device connections anc status
Product Definition	Create, modify, and remove product configurations
Authorized Management	Manage authorizations and export security files
Communication Services	Configure ADMS communication settings

Copyright © 2024 ARMATURA LLC. All rights reserved

11.5.1 Device Commands

Export

Prerequisites for Use

Administrator must have export permissions.

Usage Scenarios

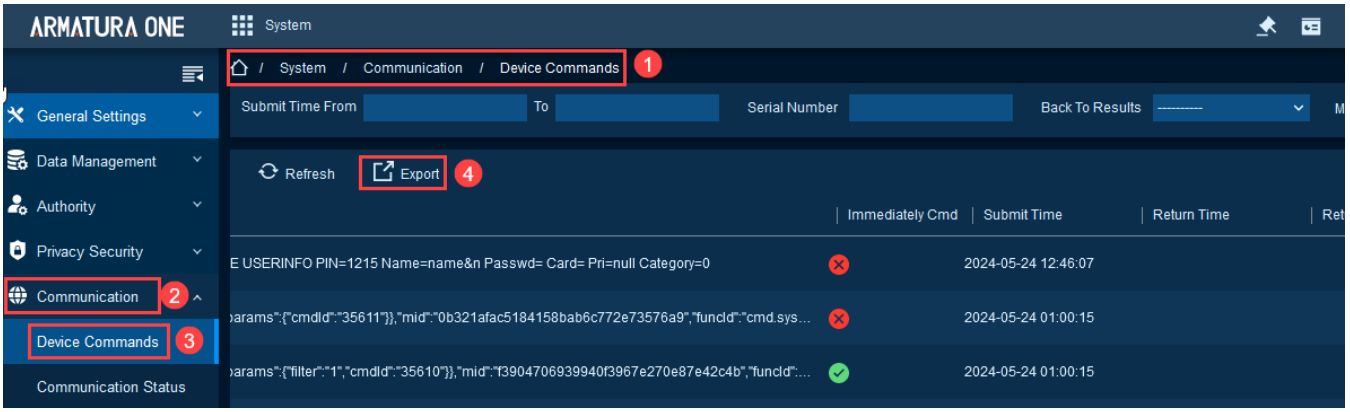
Export system data to local computer.

Trigger Result

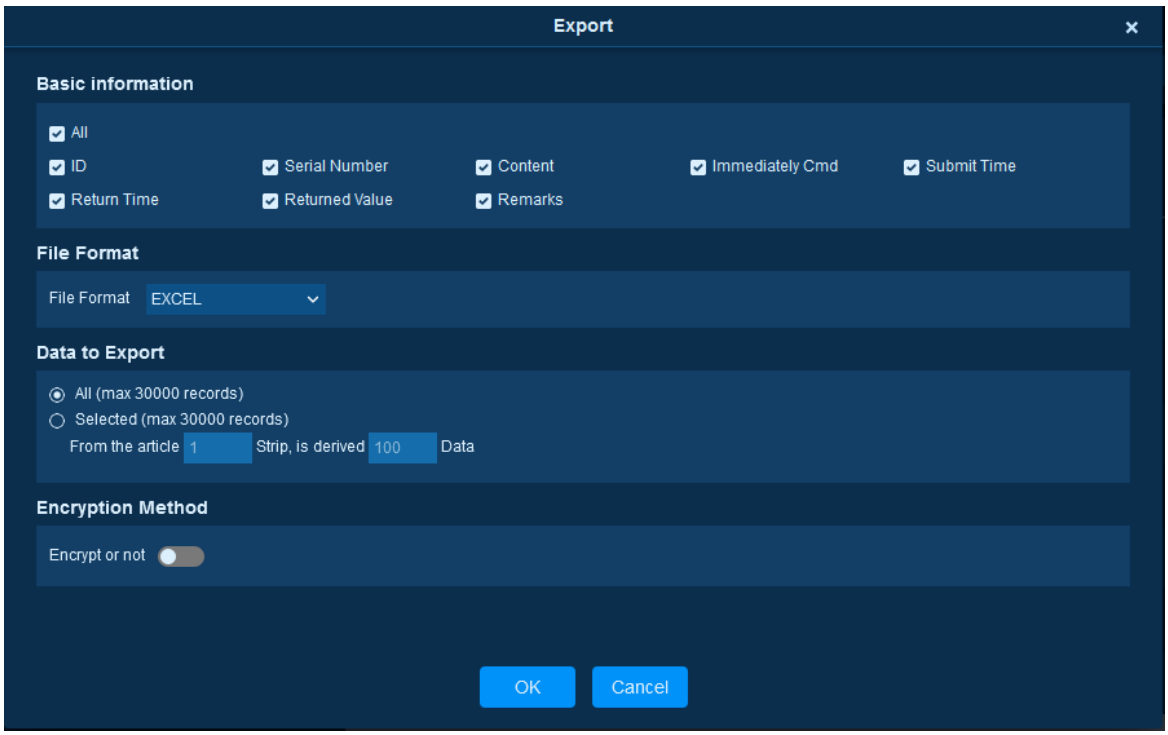
Operations	Description
Select Excel	Export data in Excel format
Select PDF	Export data in PDF format
Select CSV	Export data in CSV format
Select All	Export complete log history
Select Selected	Export logs within specified range

Steps:

- Click **[Export]** to open export window.
- Choose desired file format.
- Specify data range for export.
- Click **[OK]** to complete export.



Copyright © 2024 ARMATURA LLC. All rights reserved



11.5.2 Communication Status

Function Description

Monitor and view status of authorized devices in the system.

Prerequisites for Use

Administrator must have device monitoring permissions.

Usage Scenarios

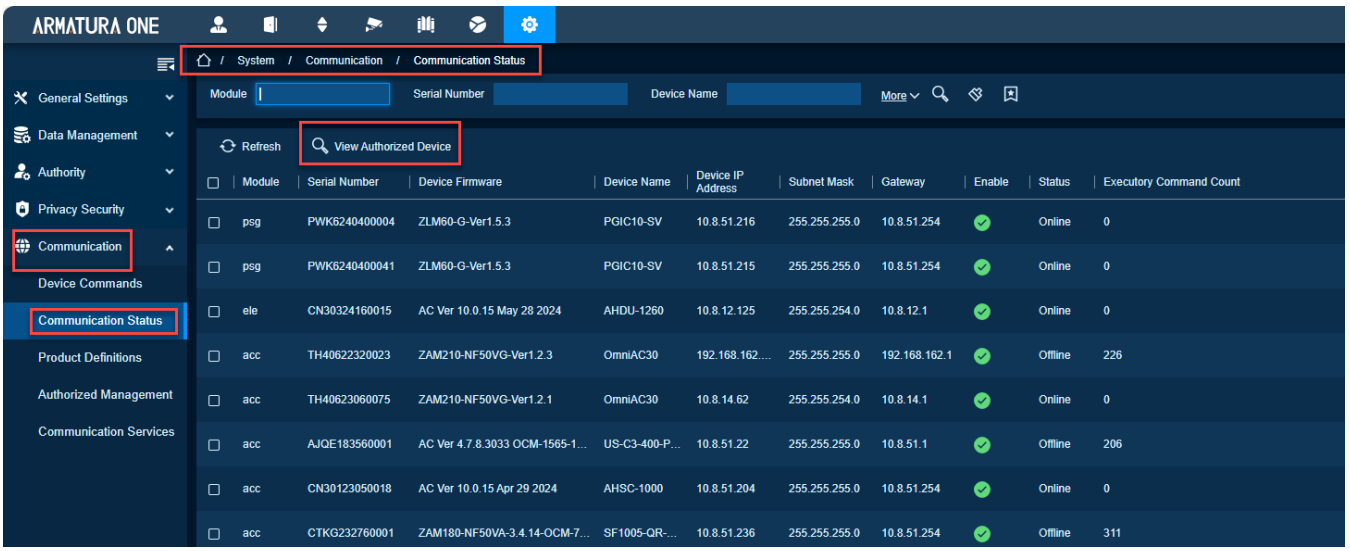
View status of authorized devices.

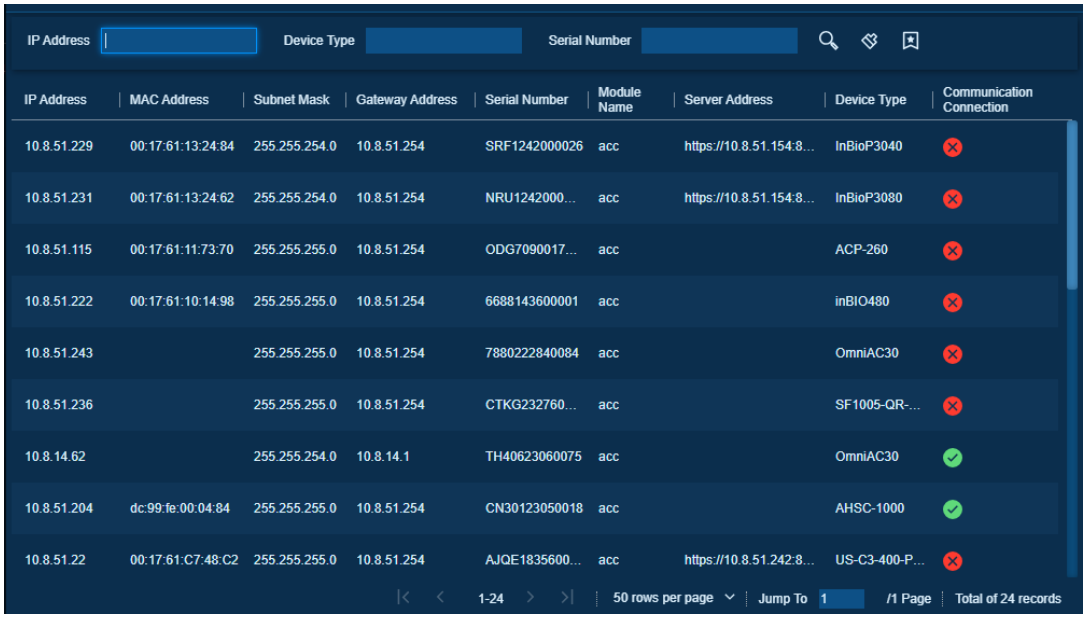
Trigger Result

View authorized device.

Click **[View Authorized Device]** to display list of authorized devices and their current status.

Copyright © 2024 ARMATURA LLC. All rights reserved





11.5.3 Product Definitions

Function Description

Manage system products including creation, modification, and removal of product configurations.

New (Add)

Prerequisites for Use

Administrator must have product creation permissions.

Usage Scenarios

Add new products to the system.

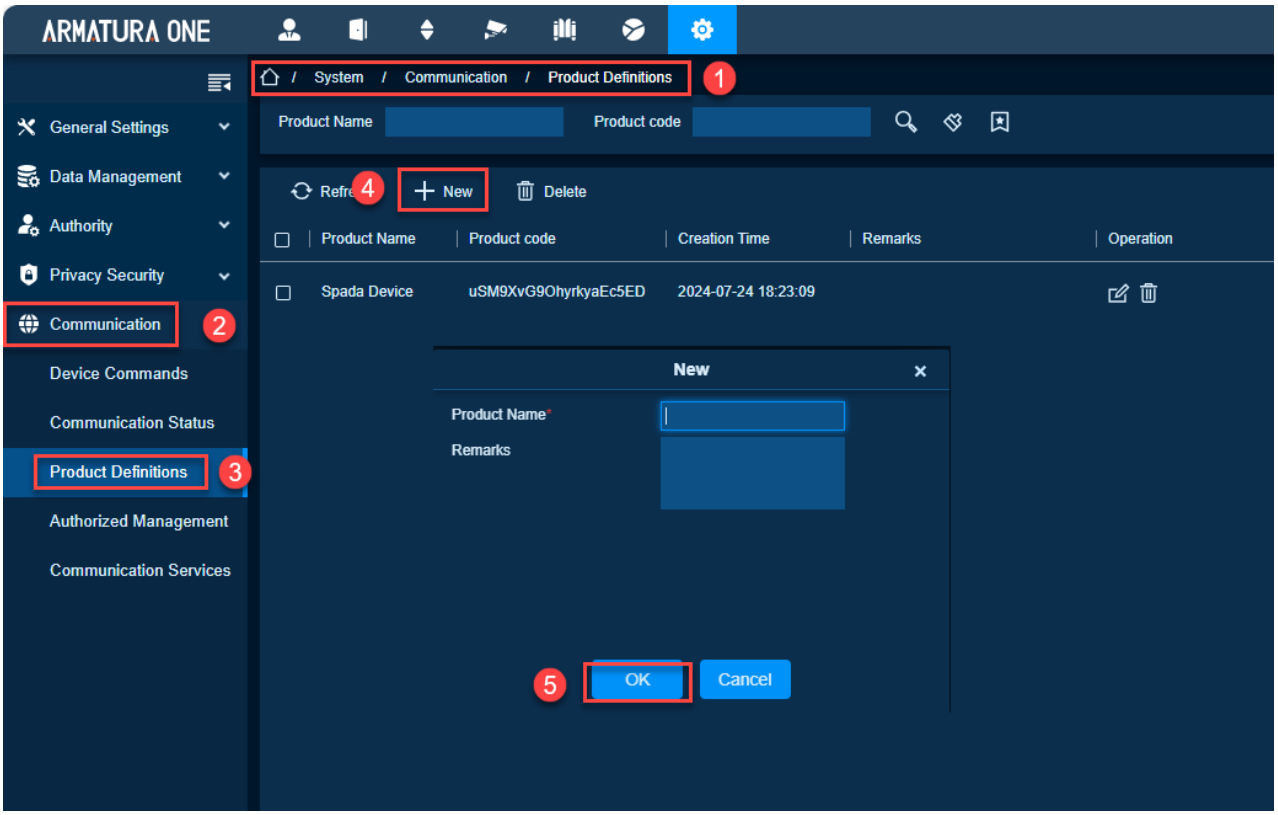
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

New product configuration is created.

Steps:

- Click **[Product Definition]** to open product management interface.
- Click **[New]**, complete configuration in popup window, then click **[OK].**



Delete

Prerequisites for Use

Administrator must have product deletion permissions.

Usage Scenarios

Remove obsolete or unnecessary product configurations.

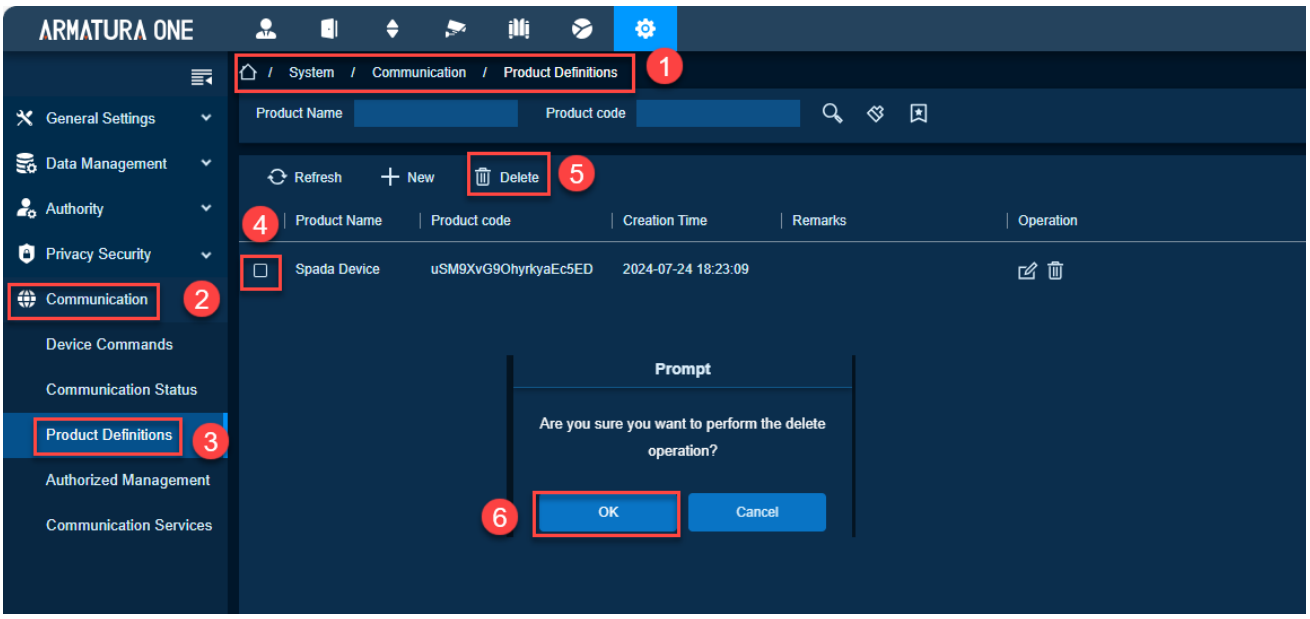
Trigger Result

Selected product is removed from the system.

Steps:

- Select target product.
- Click **[Delete]** to open confirmation dialog.

Copyright © 2024 ARMATURA LLC. All rights reserved



Edit

Prerequisites for Use

Administrator must have product modification permissions.

Usage Scenarios

Modify existing product configurations.

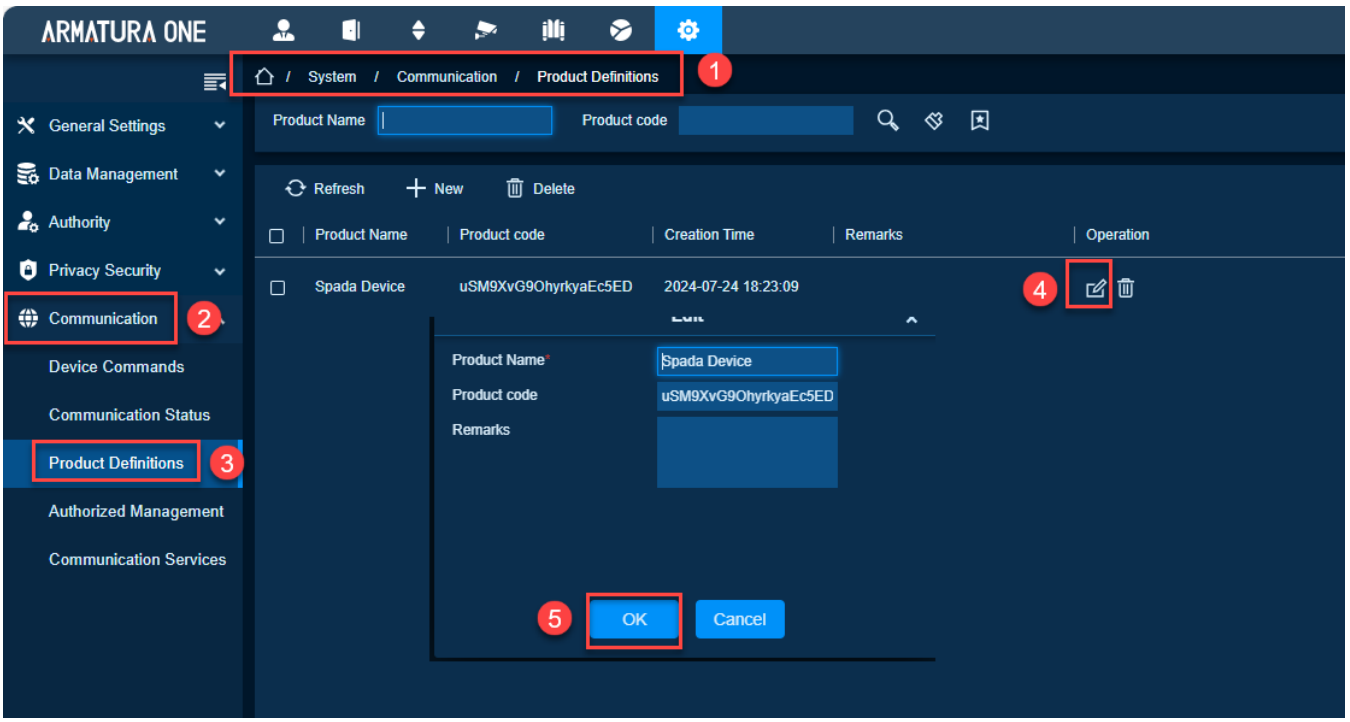
Trigger Result

Selected product configuration is updated.

Steps:

- Select target product.
- Click **[Edit]** to open modification window.
- Click **[OK]** to save changes.

Copyright © 2024 ARMATURA LLC. All rights reserved



11.5.4 Authorized Management

New

Prerequisites for Use

Administrator must have authorization management permissions.

Usage Scenarios

Create new device authorizations in the system.

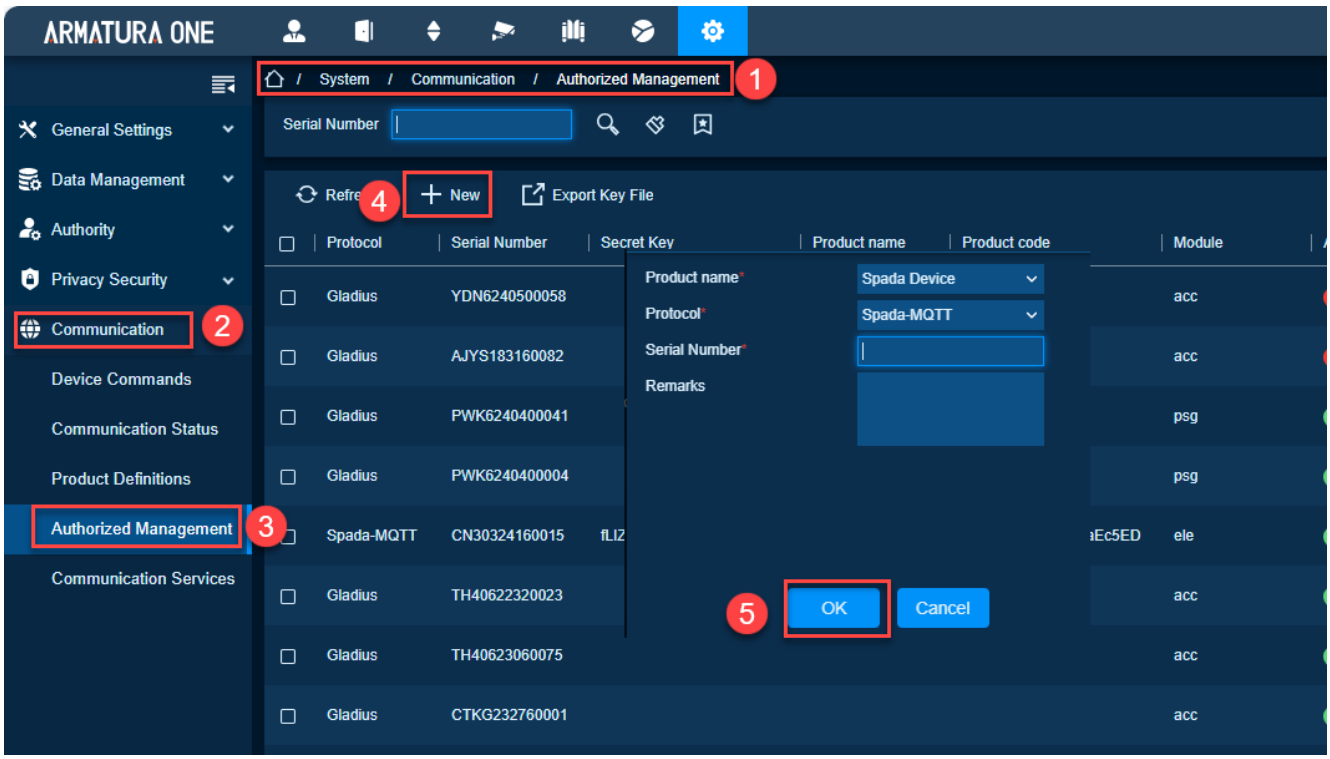
Trigger Result

New authorization is created.

Steps:

- Click **[Authorized Management]** to open authorization interface.
- Click **[New]**, select protocol and enter serial number, then click **[OK].**

Copyright © 2024 ARMATURA LLC. All rights reserved



Function List

Operations	Description
Product Name	Display product name
Protocol	Specify device communication protocol
Serial Number	Enter the serial number of the device.

Export key File

Prerequisites for Use

Administrator must have key file export permissions.

Usage Scenarios

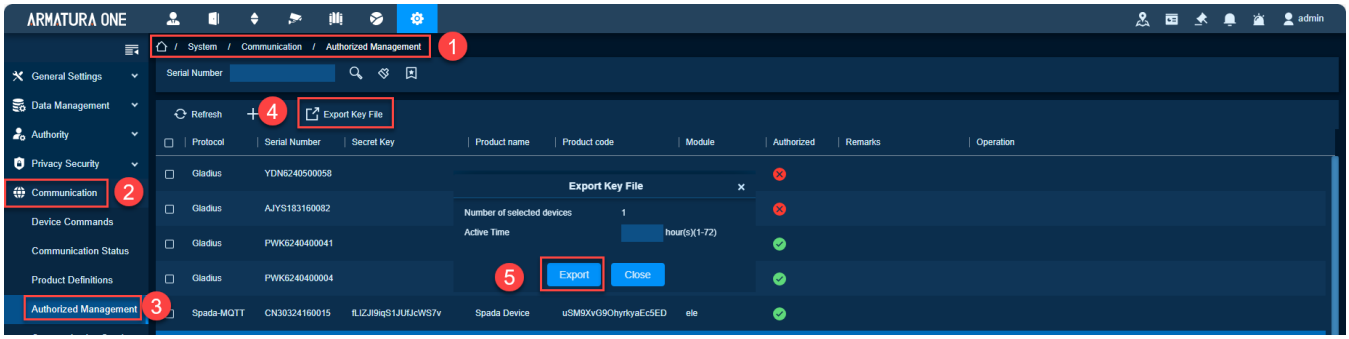
Export security key files to local computer.

Trigger Result

Steps:

- Click **[Export]** to open export window.
- Configure key activation period.
- Click **[OK]** to generate and export key file.

Copyright © 2024 ARMATURA LLC. All rights reserved



11.5.5 Communication Services

Function Description

Monitor ADMS communication ports and verify server internet connectivity status.

Prerequisites for Use

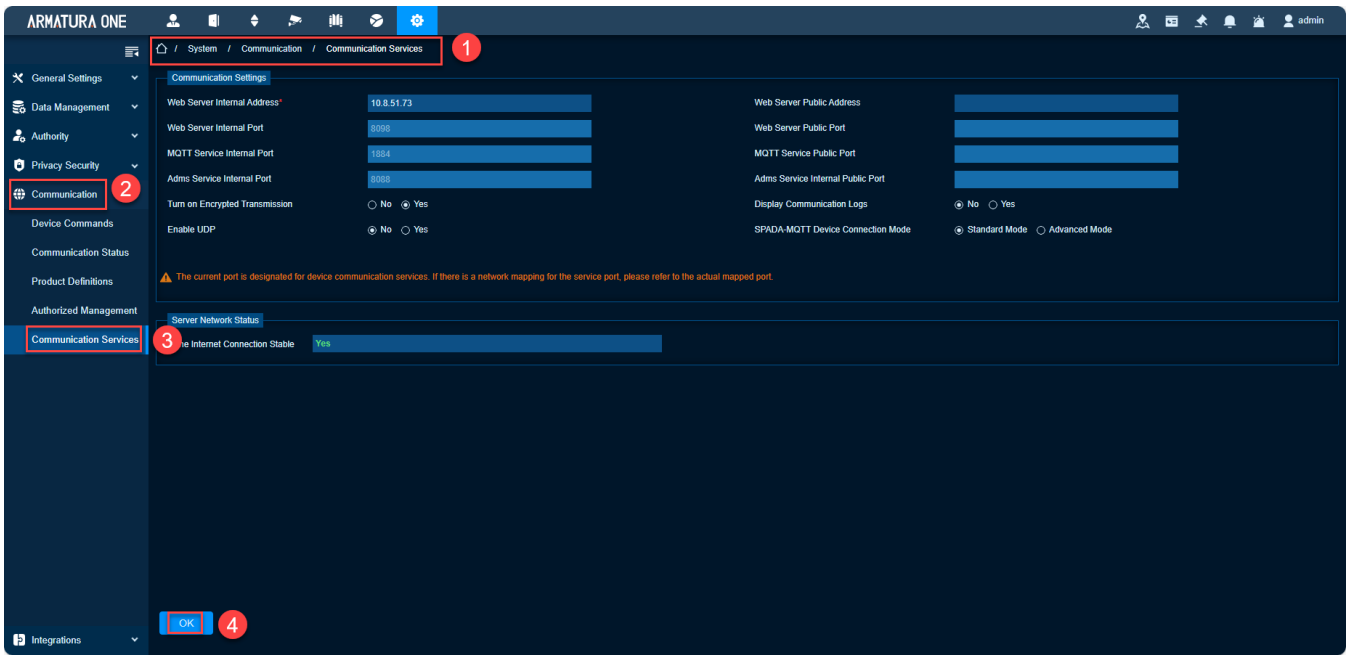
Administrator must have ADMS communication monitoring permissions.

Usage Scenarios

Monitor ADMS communication settings and connectivity.

Trigger Result

Advanced Mode enables full ADMS protocol configuration. **Standard Mode** automatically configures ADMS protocol with two default ports.



Copyright © 2024 ARMATURA LLC. All rights reserved

Field Description

ADMS Service Port: View configured ADMS service port number

Whether the Internet connection is normal: Display current internet connectivity status

11.6 Integration

Manage integrations between ARMATURA One and third-party systems, including configuration, monitoring, and data exchange settings.

- View the content of messages sent by the system.
- Query the content of the message notification in the system.
- Synchronize with Microsoft AD server.

Function List

Operations	Description
Platform Connections	Configure and manage third-party platform connectivity
E-mail Management	Manage system email communications and history
Message Management	Monitor message delivery status and timing
AD Management	Configure Microsoft Active Directory integration
System Message	View system message status and history
Map Configuration	Configure map integration settings
API Authorization	Manage data access through APIs

11.6.1 Platform Connections

Function Description

Configure and manage third-party platform integrations.

New (Add)

Prerequisites for Use

Administrator must have platform addition permissions and sufficient license points for the desired modules.

Usage Scenarios

Enable integration with external platforms for extended functionality.

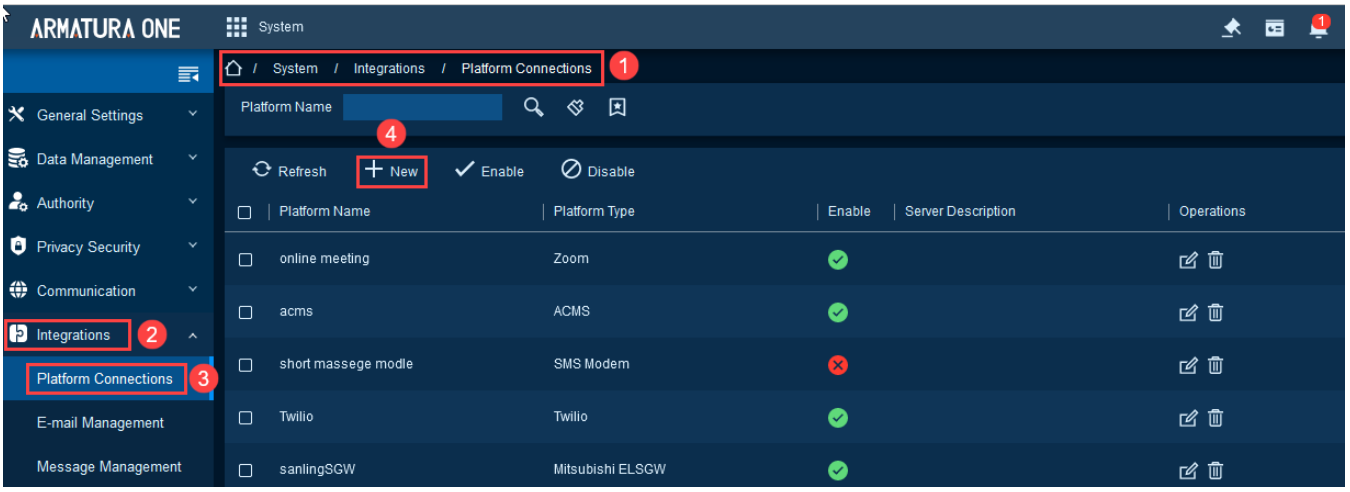
Trigger Result

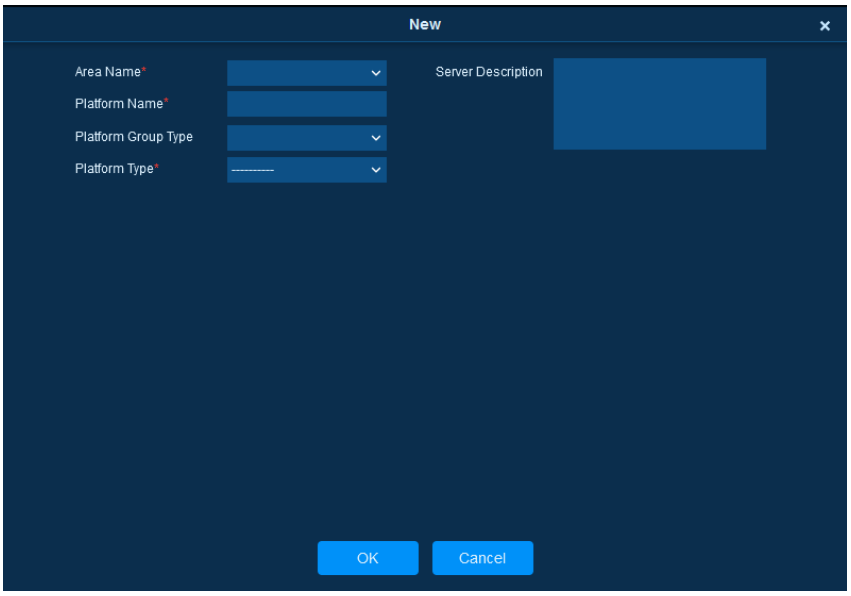
New platform integration is configured.

Steps:

- Click **[New]** to open configuration window.

Copyright © 2024 ARMATURA LLC. All rights reserved





- Complete required fields:

The field descriptions are as follows:

Parameter	How to set
Area Name	Select the area name.
Platform Name	Set the name of the platform
Platform Group Type	Select the platform group type
Platform Type	Select the platform type.
Server Description	Add server description

- Click **[OK]** to complete the Add configuration.

Copyright © 2024 ARMATURA LLC. All rights reserved

Add Zoom Platform

Prerequisites for Use

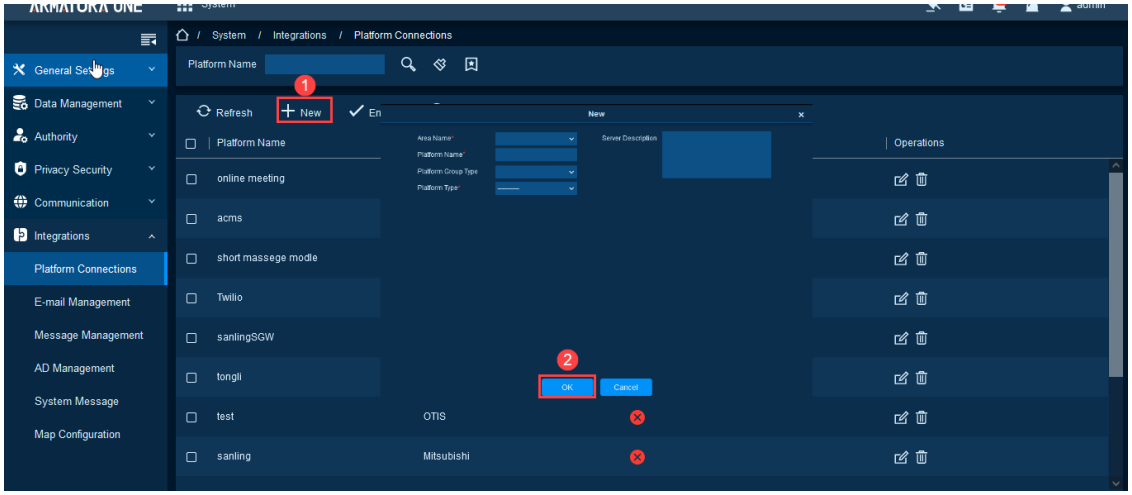
Administrator requires online meeting platform permissions.

Usage Scenarios

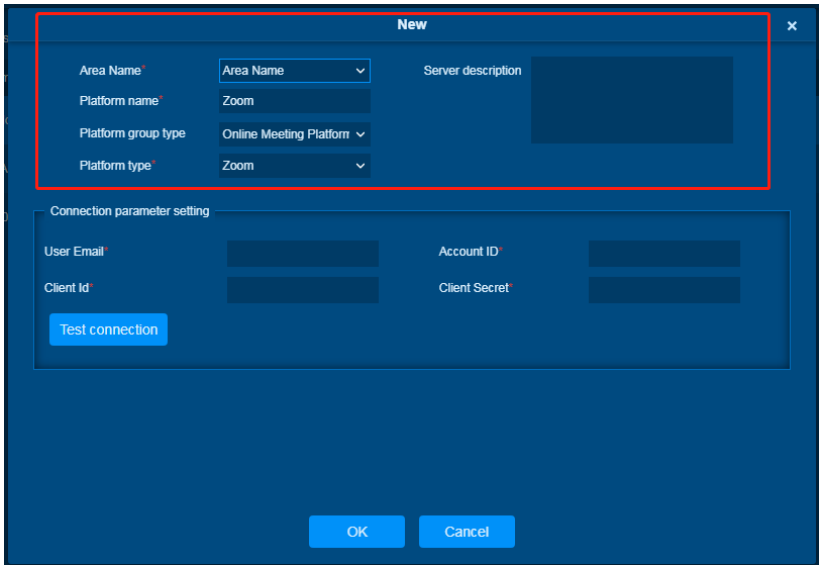
Enable virtual meeting capabilities for improved efficiency.

Steps:

- Click **[New]** to open configuration window.

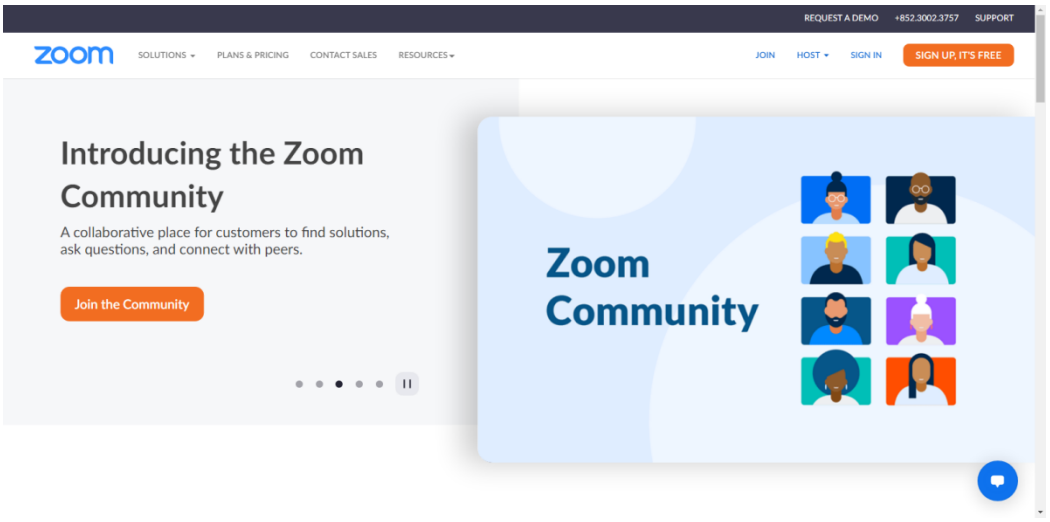


- Select **[Online Meeting Platform]** under **[Platform Group Type]**, then **[Zoom]** under **[Platform Type]**.

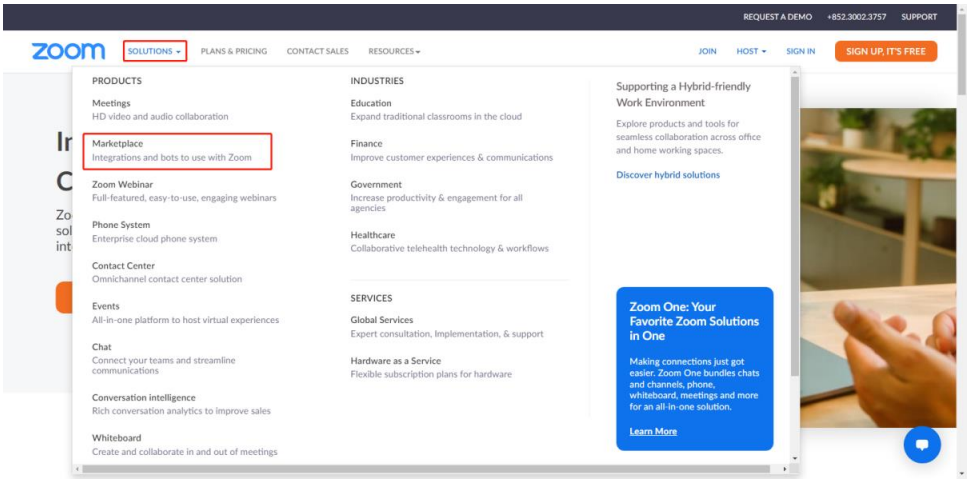


Copyright © 2024 ARMATURA LLC. All rights reserved

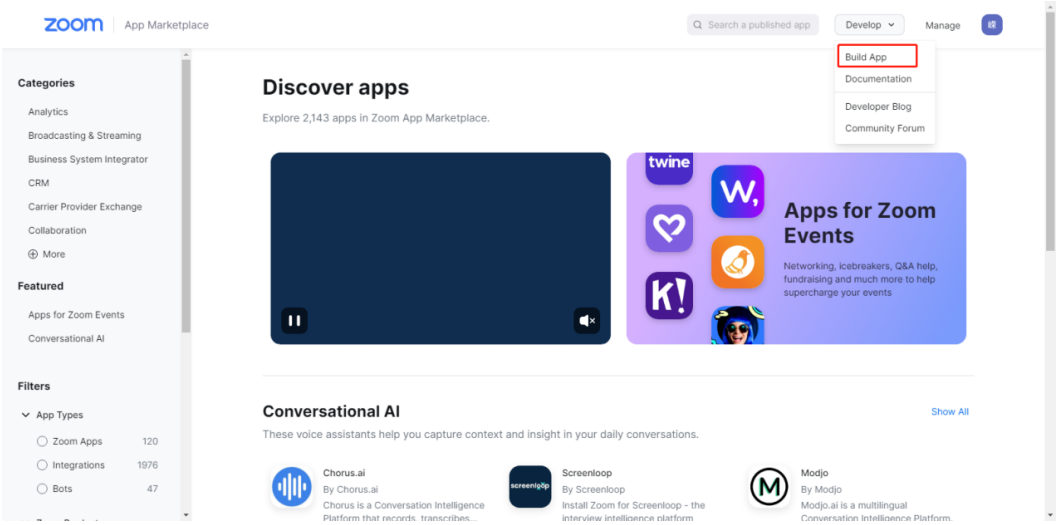
- Configure connection parameters.
- Log in to Zoom official website: https://zoom.us/.



- Click **[Marketplace]** in the **[SOLUTIONS]**.

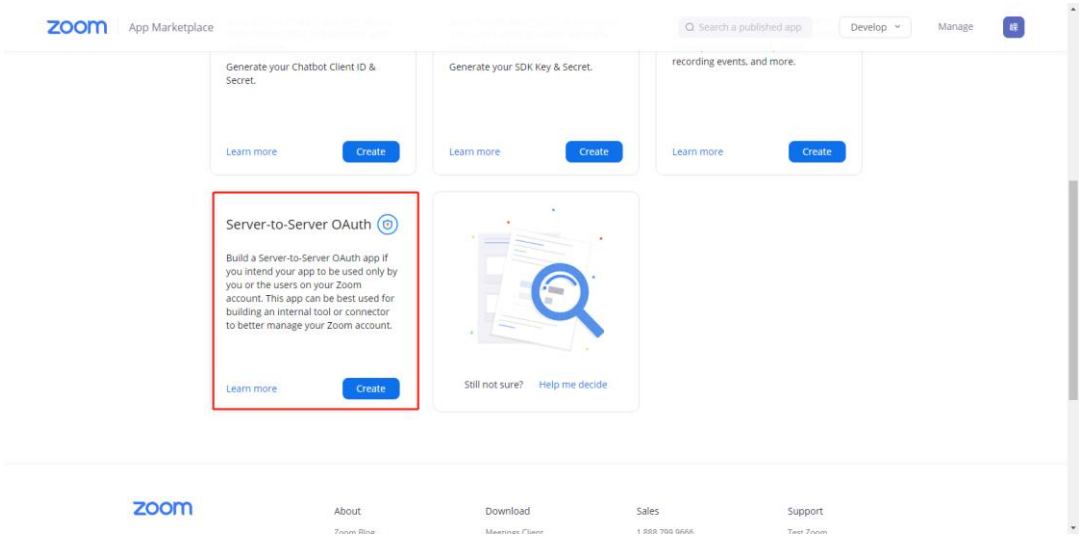


- Click **[Build App in the Develop]**.

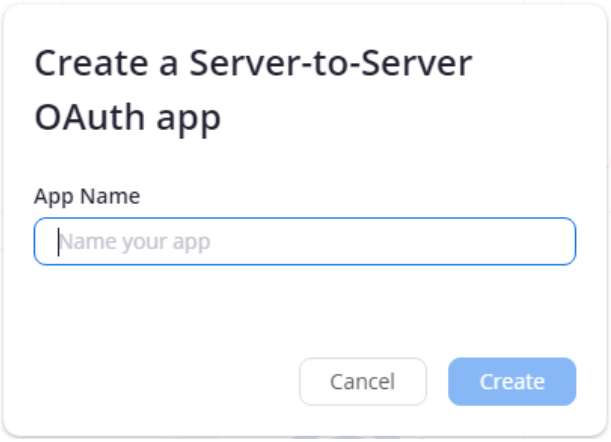


Copyright © 2024 ARMATURA LLC. All rights reserved

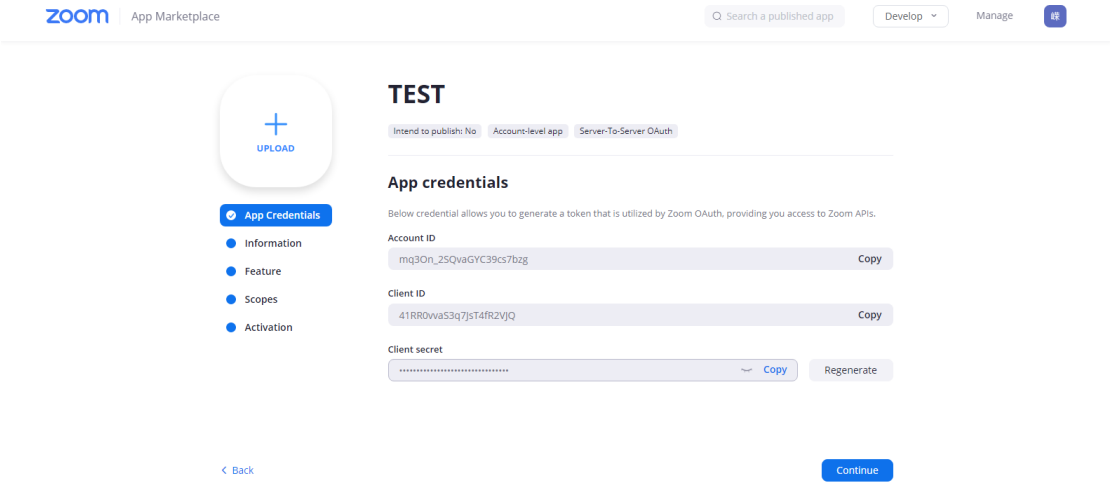
- Create Server-to-Server OAuth.



- Input the App name then click **[Create]**.

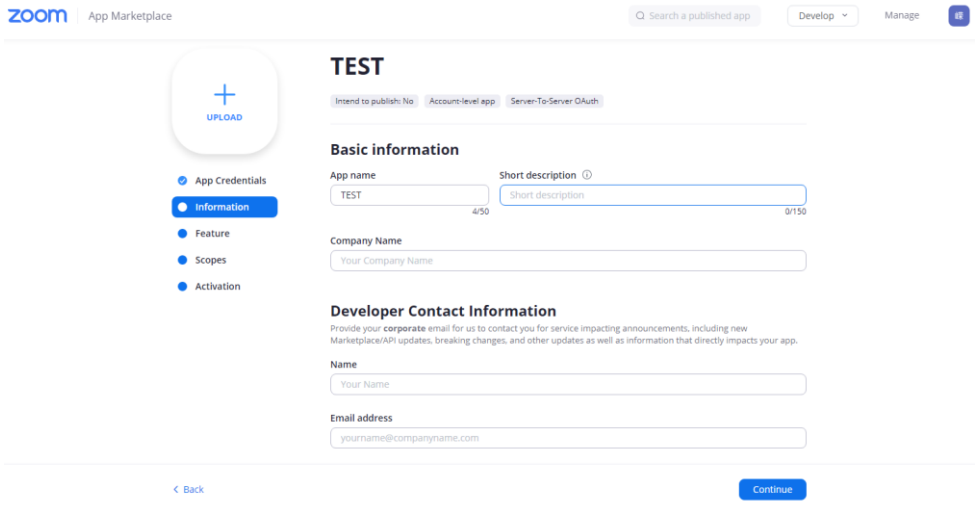


- Then will skip ahead to API configuration, click **[Continue]** skip to next step.

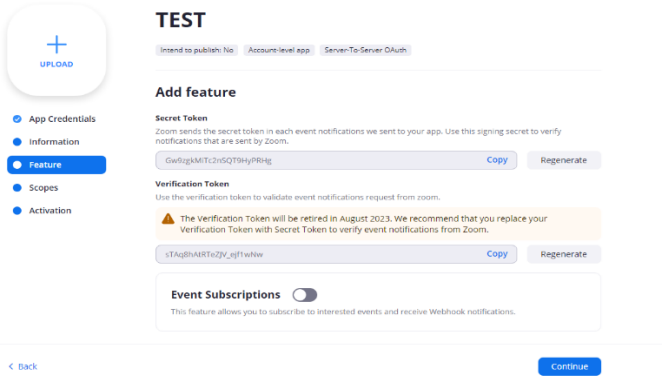


Copyright © 2024 ARMATURA LLC. All rights reserved

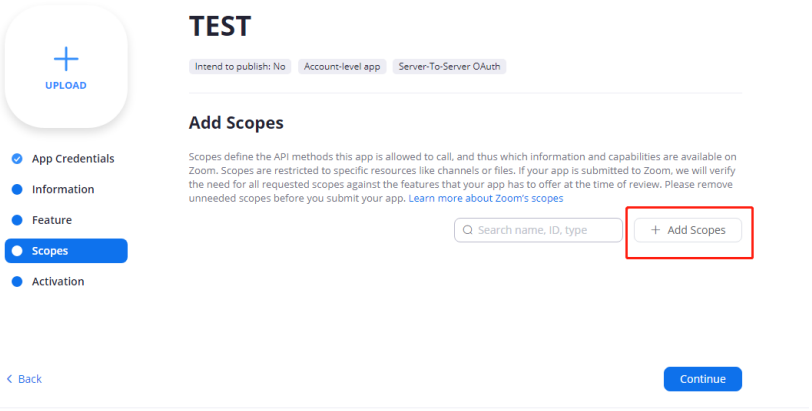
- Enter the basic information and developer contact information.



- Feature configuration is default, then click **[Continue]**.

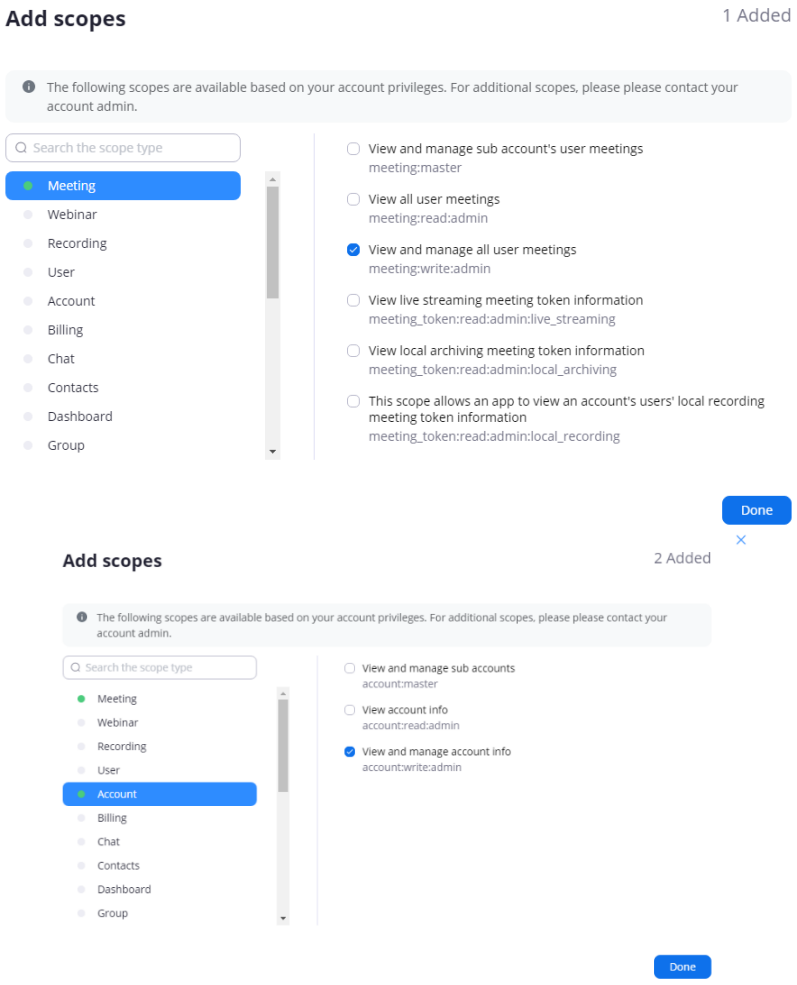


- Click **[Add Scopes]** to configure the scope.

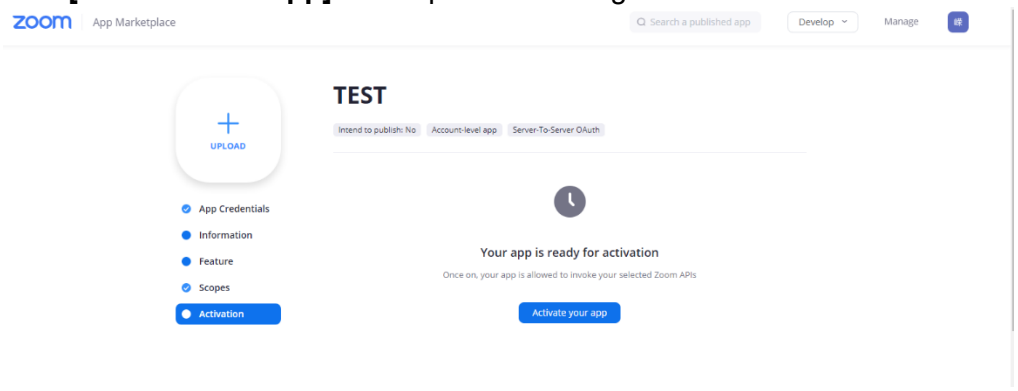


Copyright © 2024 ARMATURA LLC. All rights reserved

- Add required scopes: **[View and manage account info]** and **[View and manage all user meetings]**.

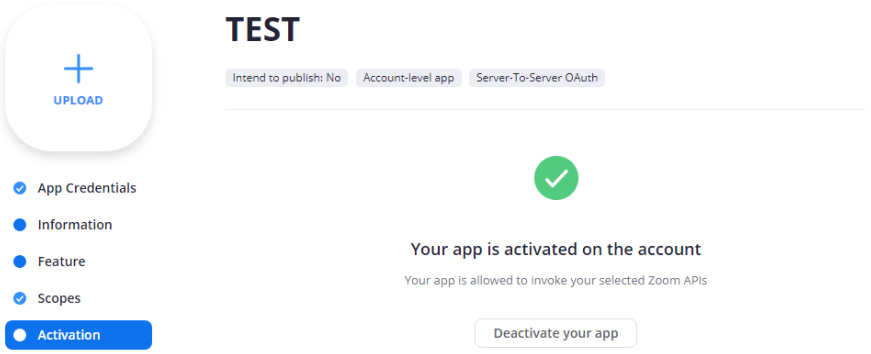


- Next click **[Activate user app]** to complete the configuration.

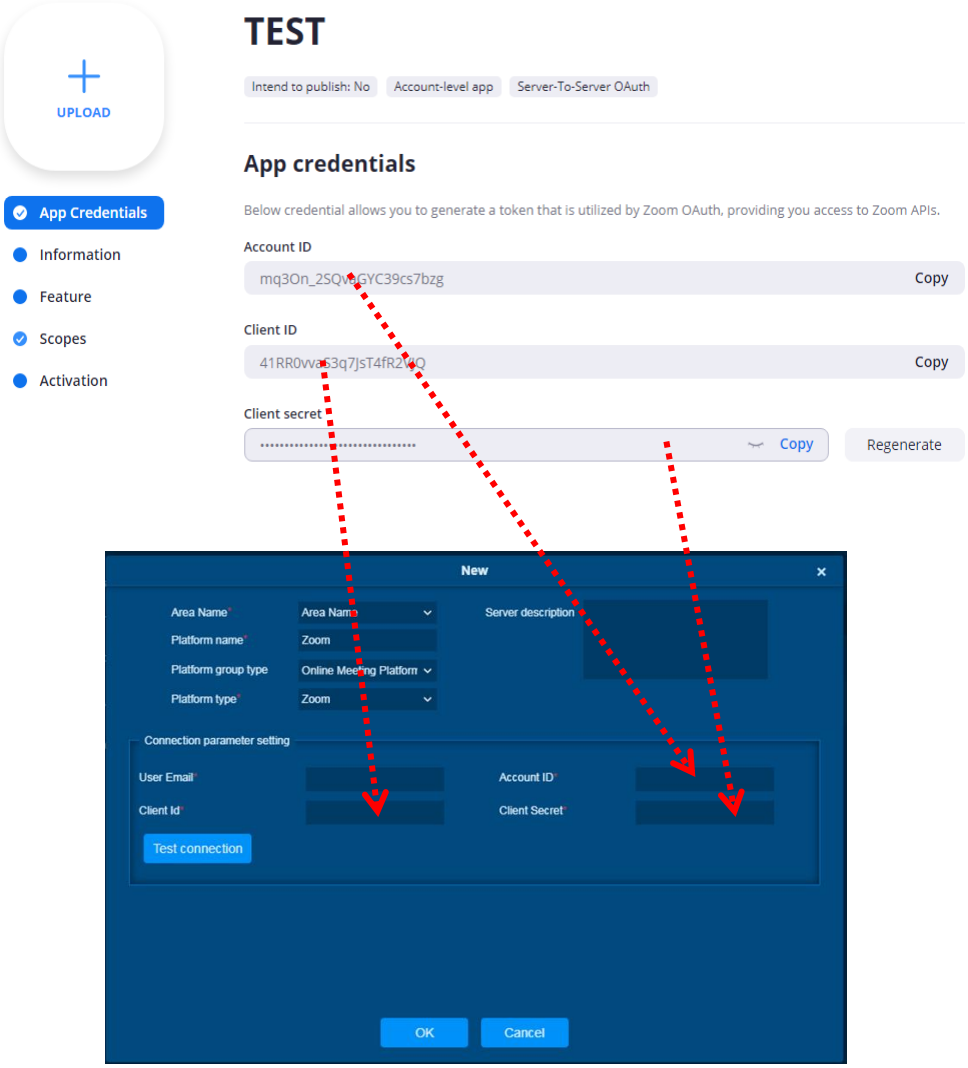


- When the prompt “User app is activated on the account” appears, it indicates that the Zoom connection parameter configuration has been successful.

Copyright © 2024 ARMATURA LLC. All rights reserved

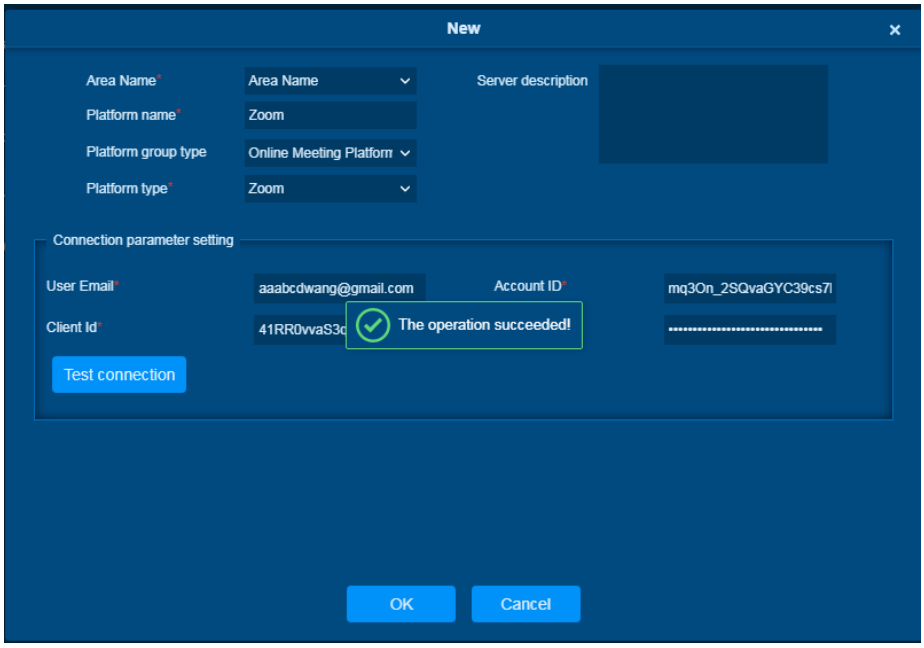


- Skip to **[App credentials]** and then put in the appropriate parameters in the Armatura One platform connection. The **[User Email]** is the same as the one used to sign up with Zoom. And the Account ID, Client Id, and Client Secret are derived from the **[App credentials]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

- After filling in the relevant parameters, click **[Test connection]**, if it appears “The operation successful” means platform connection is successful, vice versa.



- Click **[OK]**
- Finally, select the Zoom platform and click **[Enable]** to active the platform.

Enable

Prerequisites for Use

Administrator must have platform activation permissions.

Usage Scenarios

Activate disabled platforms when needed.

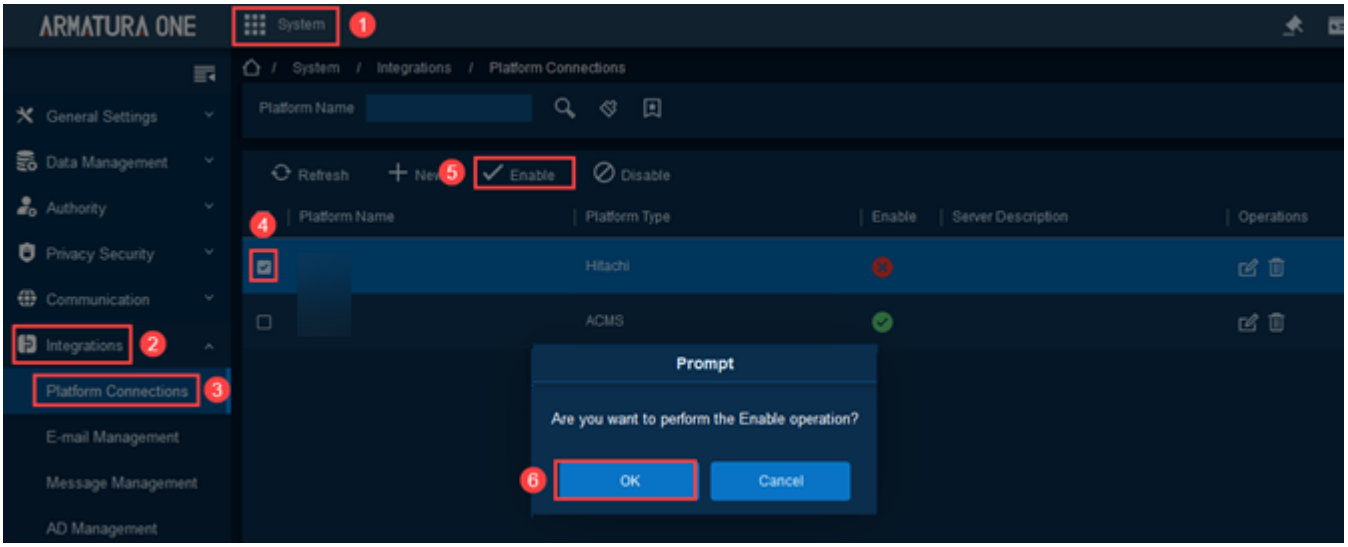
Trigger Result

Selected platform becomes active.

Steps:

- Select target platform.
- Click **[Enable]** to open confirmation dialog.
- Click **[OK]** to activate.

Copyright © 2024 ARMATURA LLC. All rights reserved



Disable

Prerequisites for Use

Administrator must have platform deactivation permissions.

Usage Scenarios

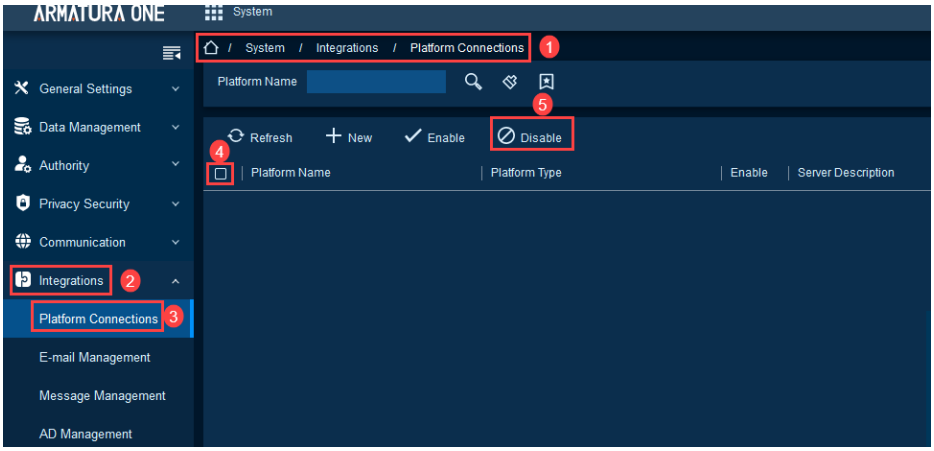
Temporarily suspend platform integration when not needed.

Trigger Result

Selected platform becomes inactive.

Steps:

- Select target platform.
- Click **[Disable]** to open confirmation dialog.
- Click **[OK]** to confirm deactivation.



Copyright © 2024 ARMATURA LLC. All rights reserved

11.6.2 E-mail Management

Function Description

Configure email server settings and manage email communications. Email templates and event linkages must be configured before sending emails.

Delete

Prerequisites for Use

Administrator must have email deletion permissions.

Usage Scenarios

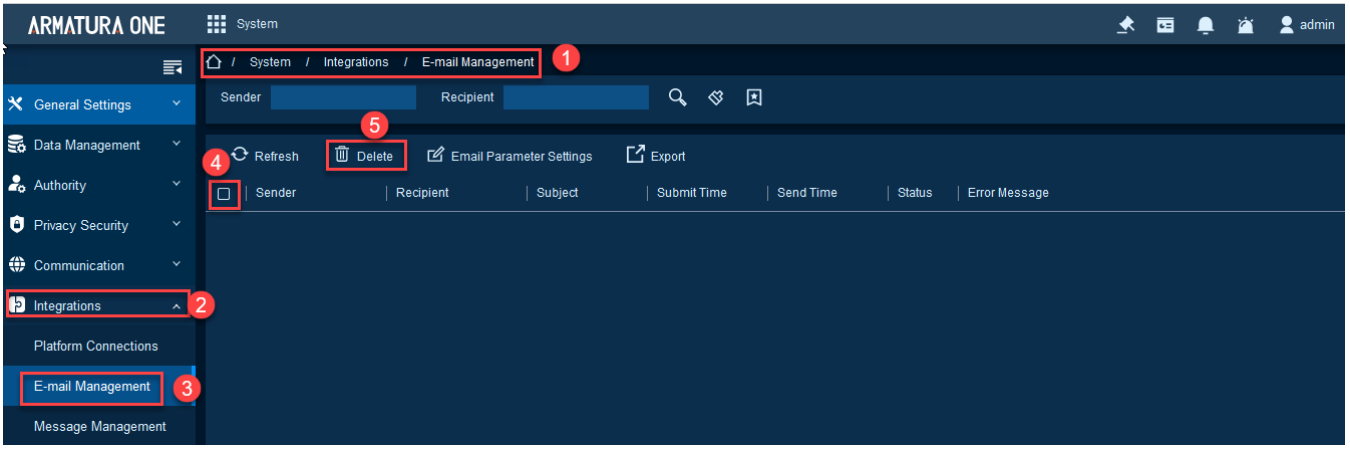
Remove unnecessary email records.

Trigger Result

Selected email records are removed.

Steps:

- Select target email records.
- Click **[Delete]** to open confirmation dialog.
- Click **[OK]** to confirm deletion.



Email Parameter Settings

Prerequisites for Use

Administrator must have email configuration permissions.

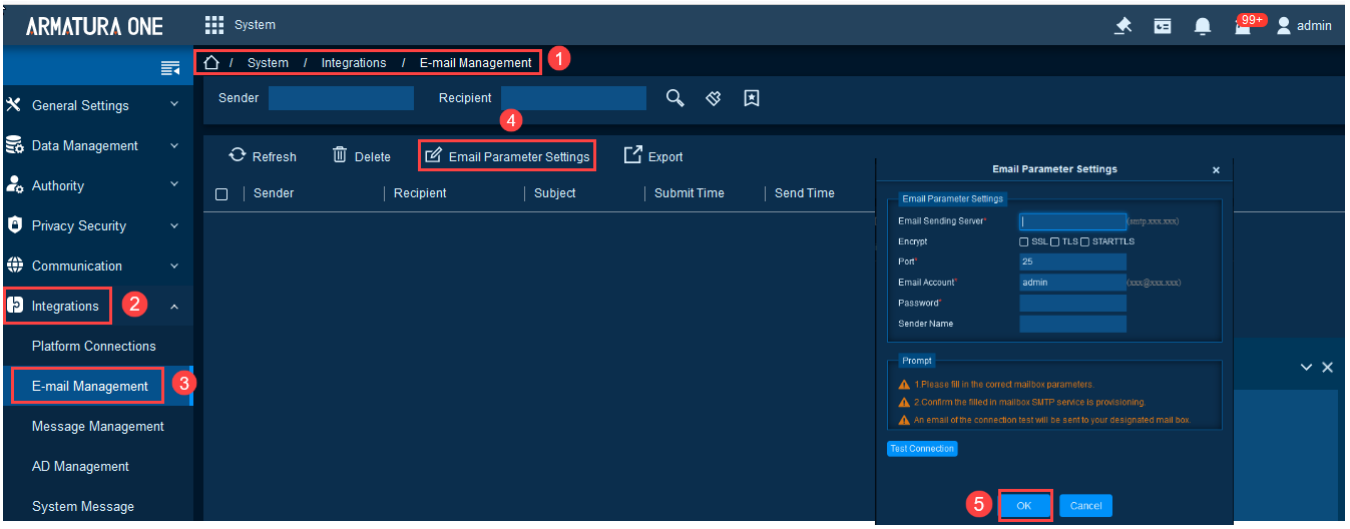
Usage Scenarios

Configure email server settings required for system email functionality.

Trigger Result

Email functionality becomes available after successful configuration.

Copyright © 2024 ARMATURA LLC. All rights reserved



Steps:

- Click **[Email Parameter Settings]** to open configuration window.
- Complete required fields (marked with *).
- Click **[Test Connection]** - successful test sends confirmation email.
- Click **[OK]** to save settings.

The fields are explained as follows:

Email Sending Server: SMTP server address

Port: SMTP Mail server port number

Email Account: Sender's email address

Password: Sender's email password

Sender Name: Display name for sender

Export

Prerequisites for Use

Administrator must have export permissions.

Usage Scenarios

Export email records to local computer.

Trigger Result

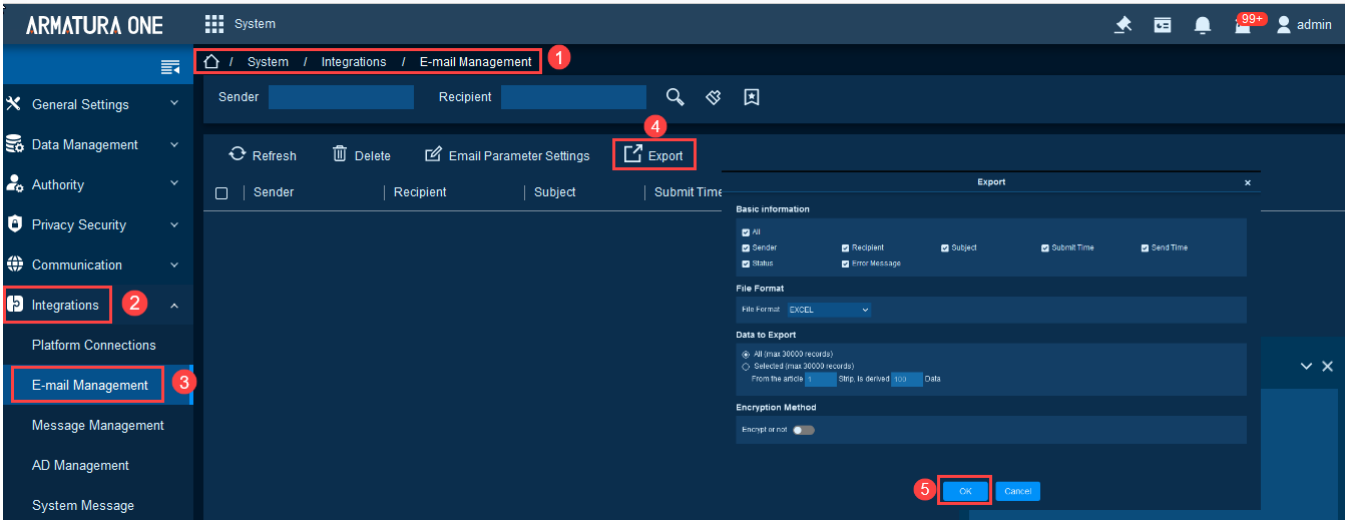
Operations	Description
Select Excel	Export in Excel format
Select PDF	Export in PDF format
Select CSV	Export in CSV format

Copyright © 2024 ARMATURA LLC. All rights reserved

Select all data	Export complete email history
Select the amount of data export	Export specified range of records

Steps:

- Click **[Export]** to open export window.
- Choose desired file format.
- Specify data range for export.
- Click **[OK]** to complete export.



11.6.3 Messages Management

Function Description

Manage messages integrated from third-party messaging platforms.

Delete

Prerequisites for Use

Administrator must have message deletion permissions.

Usage Scenarios

Remove obsolete or unnecessary message records.

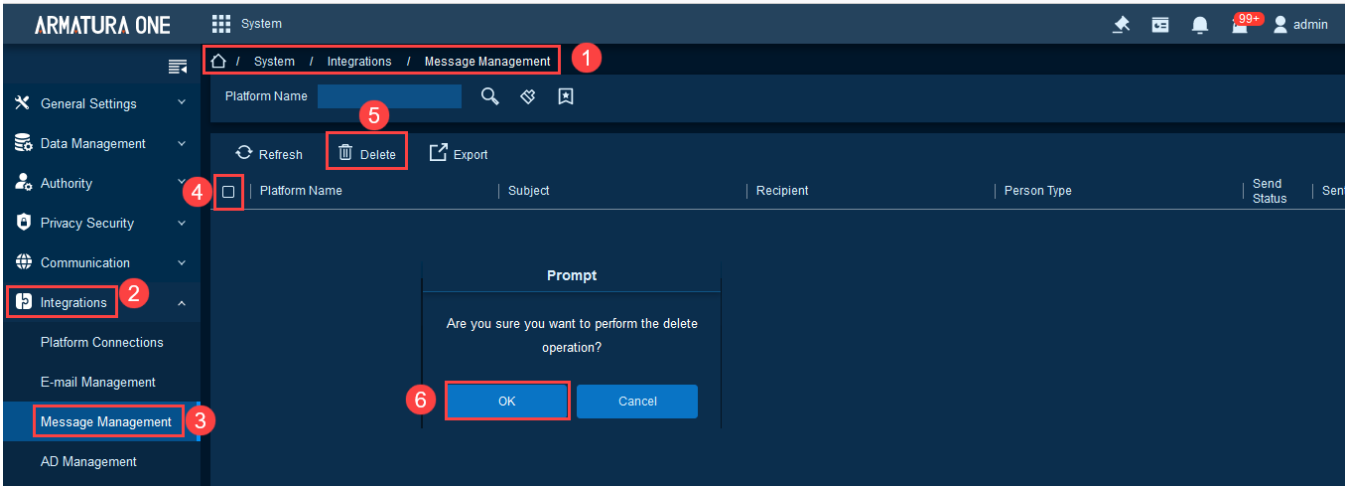
Trigger Result

Selected messages are removed.

Steps:

- Select target messages.
- Click **[Delete]** to open confirmation dialog.
- Click **[OK]** to confirm deletion.

Copyright © 2024 ARMATURA LLC. All rights reserved



Export

Prerequisites for Use

Administrator must have export permissions and available message data.

Usage Scenarios

Export message records to local computer.

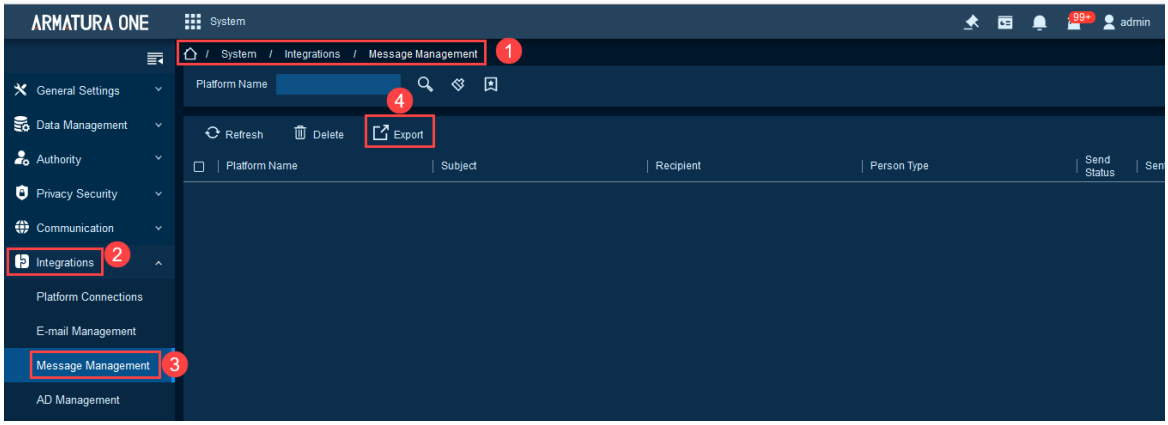
Trigger Result

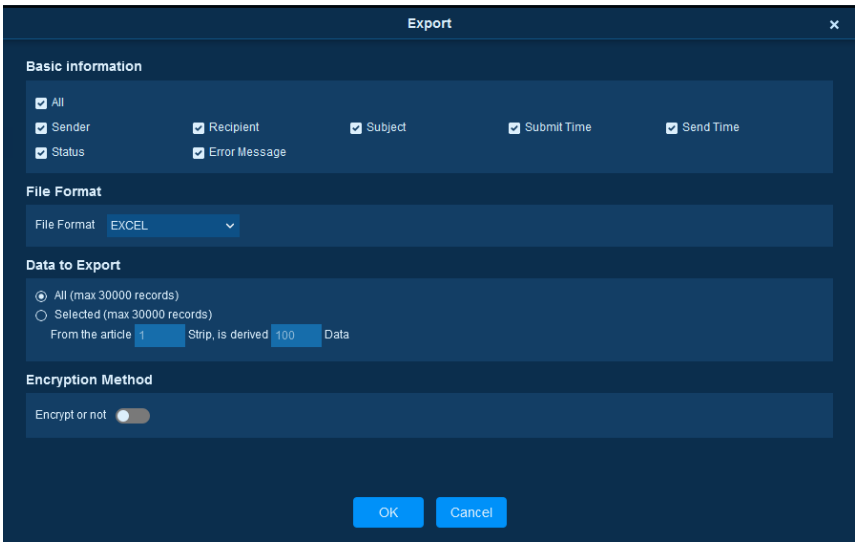
Operations	Description
Select Excel	Export in Excel format
Select PDF	Export in PDF format
Select CSV	Export in CSV format
Select All Data	Export complete message history
Select the Amount of Data Export	Export specified range of messages

Steps:

- Click **[Export]** to open export window.
- Choose desired file format.
- Specify data range for export.
- Click **[OK]** to complete export.

Copyright © 2024 ARMATURA LLC. All rights reserved



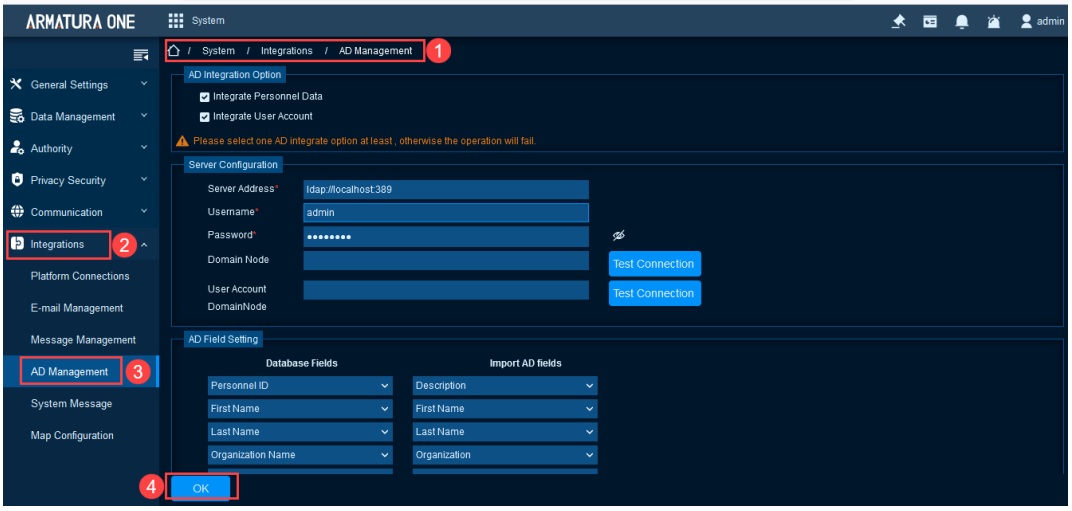


11.6.4 AD Management

Function Description

Configure Microsoft Active Directory integration for personnel data synchronization.

- Access via **[System Integration]** > **[AD Management]**.



Copyright © 2024 ARMATURA LLC. All rights reserved

Field Descriptions:

Server Address: Active Directory server location

Username: AD authentication username

Password: AD authentication password

Domain Node: Specify domain node path

AD Field Setting: Configure AD field mappings

Synchronization Permission Group: Enable permission group synchronization

Synchronize Members in Permission Group: Enable member synchronization within permission groups

Domain Node: Define access level domain node

Incremental Synchronization (minutes): Configure real-time user addition synchronization interval (addition only)

Global Synchronization: Set daily schedule for complete user synchronization (additions and removals)

11.6.5 System Message

Function Description

View and manage system message history.

Export

Prerequisites for Use

Administrator must have export permissions and available message data.

Usage Scenarios

Export system message records to local computer.

Trigger Result

Operations	Description
Select Excel	Export in Excel format
Select PDF	Export in PDF format
Select CSV	Export in CSV format
Select All Data	Export complete message history
Select the Amount of Data Export	Export specified range of messages

Copyright © 2024 ARMATURA LLC. All rights reserved

Steps:

- Click **[Export]** to open export window.
- Choose desired file format.
- Specify data range for export.
- Click **[OK]** to complete export.

11.6.6 Map Configuration

Function Description

Configure electronic maps by adding maps, placing devices, and managing map settings. Users can add doors, zoom in/out, save device locations, and monitor real-time door events on the map.

New Map

Prerequisites for Use

User must have appropriate system access permissions.

Usage Scenarios

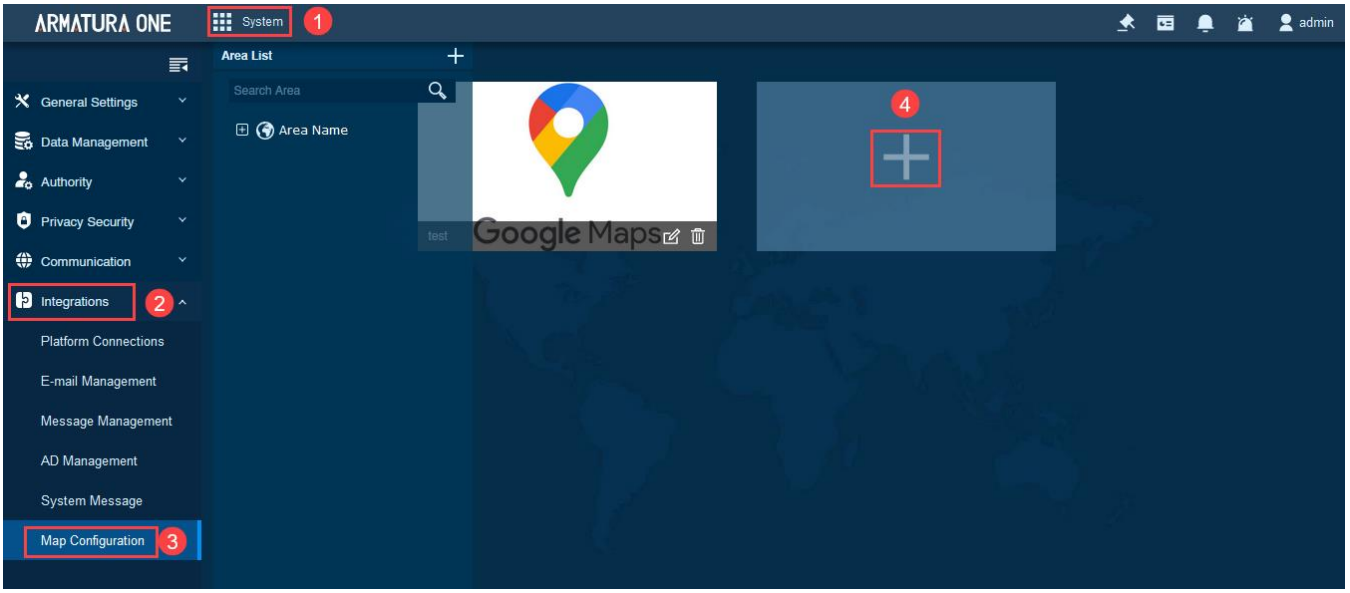
Configure maps for specific areas.

Trigger Result

Create new map with name, type, path, and area settings.

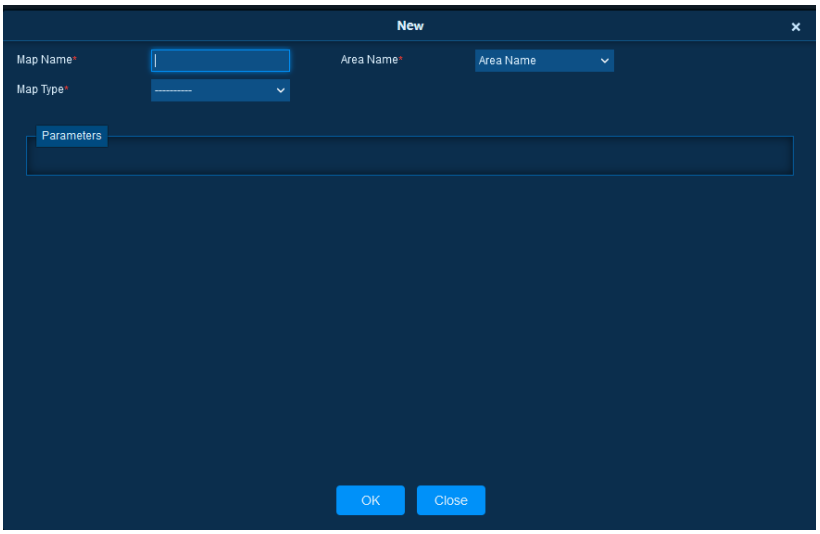
Steps:

- Navigate to **[System]** > **[Integrations]** > **[Map Configuration]** > **[+]** on the Action Menu.



Copyright © 2024 ARMATURA LLC. All rights reserved

Supported Map Types:



General Map

Upload local JPG/PNG image files

Google Maps

Integration using Google Cloud Platform API key (requires registration and billing)

Authority Control

1. Area selection required when adding levels
2. User access limited to authorized areas
3. Map area modification clears existing doors
4. Administrator can set user permissions for map operations.

Note:

Map name can be modified but not path

Multiple doors can be added simultaneously

Door icon margins must exceed 5 pixels when zoomed out

Recommended map size: 1120 * 380 pixels

GIS data provided by GIS provider

Google Maps requires valid API key.

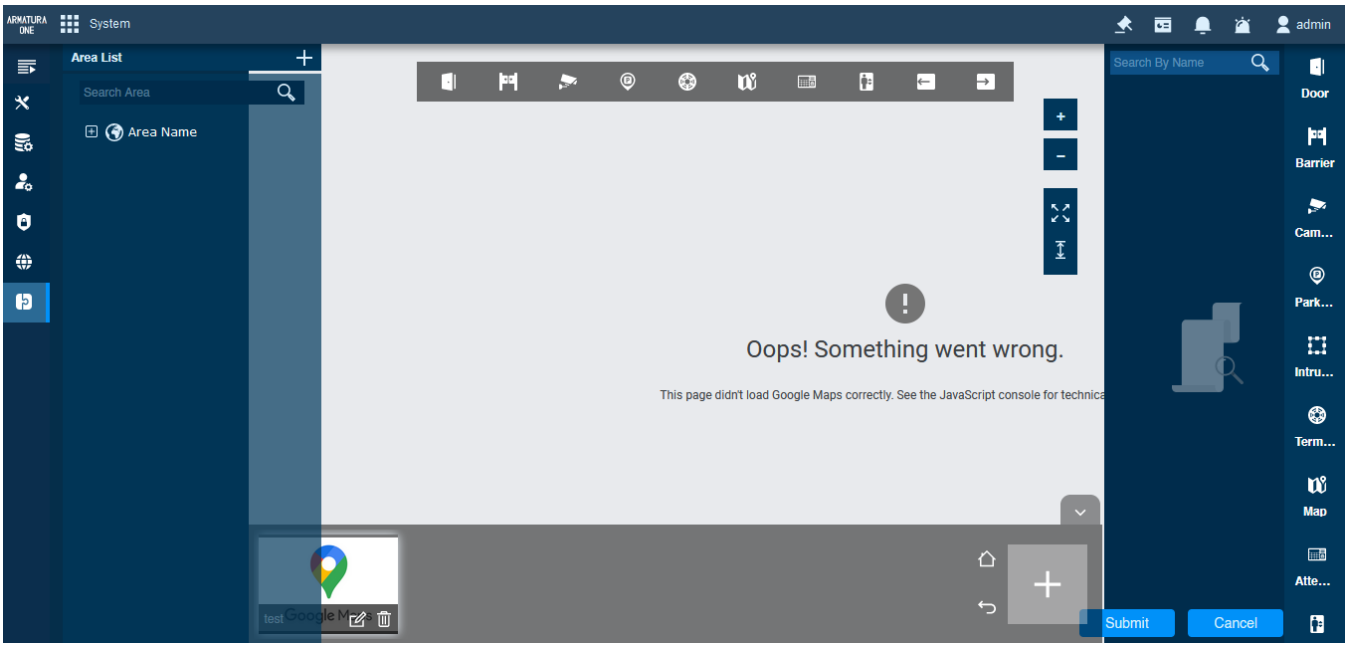
Adjust Map

Use the mouse scroll or toolbar controls (+/-) to zoom

Copyright © 2024 ARMATURA LLC. All rights reserved

Use the **[↑/↓]** icon for view height adjustment

Click **[Finish]** to lock view settings.



Add Devices

Use the **[+]** icon to add:

- Doors
- Cameras
- Fire Sensors
- Face Kiosks
- Attendance Devices
- Parking Devices

Drag devices from area list to map

Click submit to confirm placement

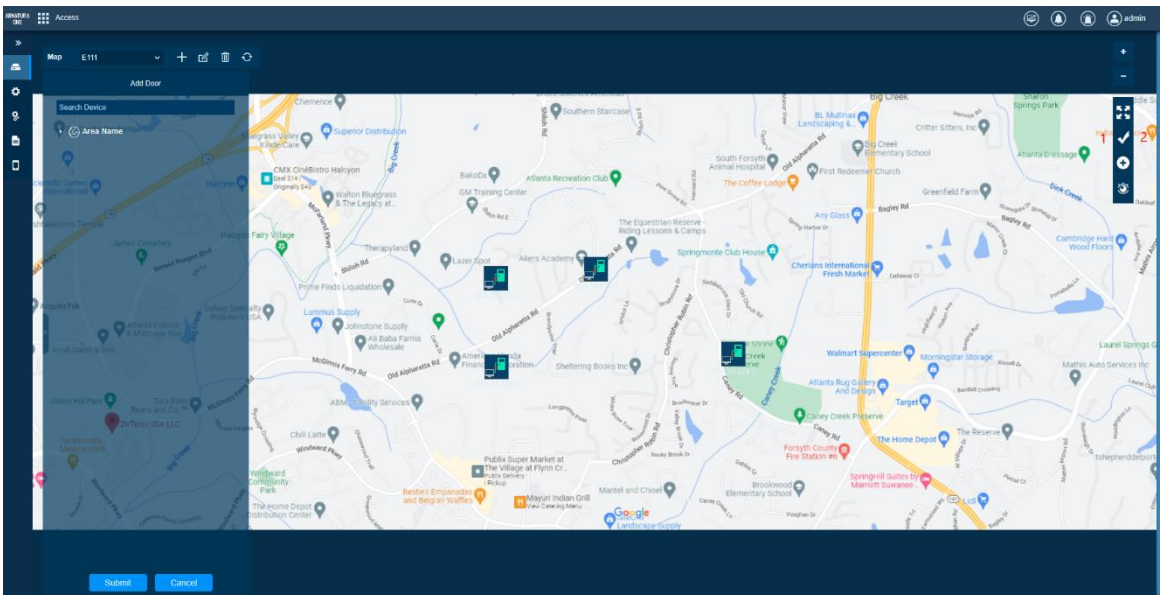
Change Device Location

Click **[✋]** icon

Drag device to new position

Click icon again to confirm

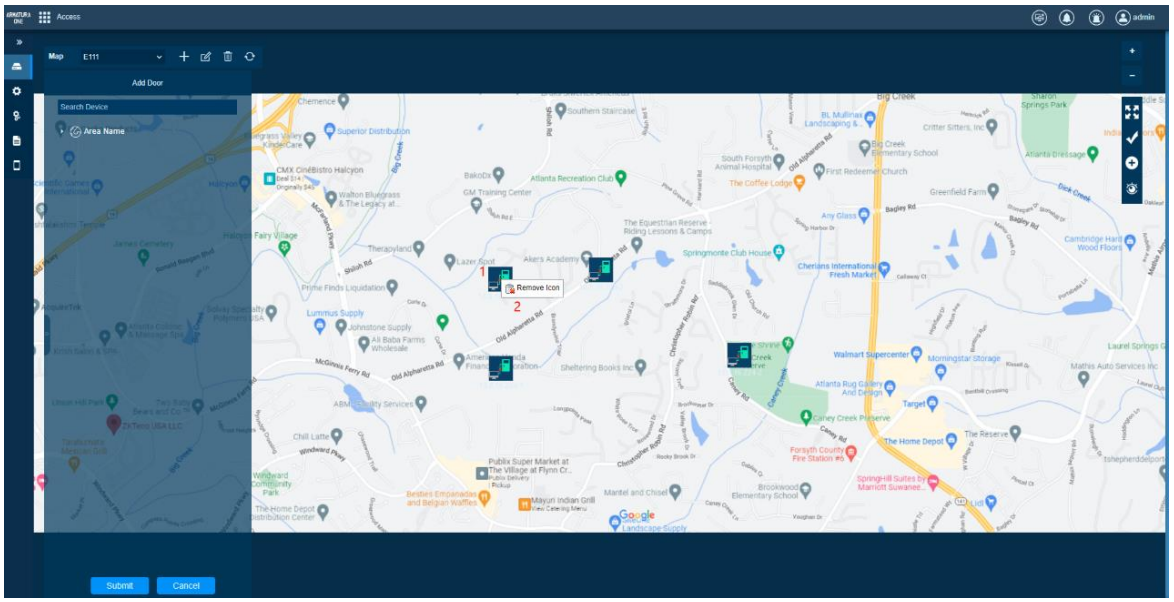
Copyright © 2024 ARMATURA LLC. All rights reserved



Click the button and drag the device icon on the map to wherever user want and finally click the button again to confirm operation.

Remove the Device

Right-click the device icon and select remove.



Edit Map Parameters

Prerequisites for Use

User must have appropriate permissions.

Usage Scenarios

Modify door and camera configurations in specific areas.

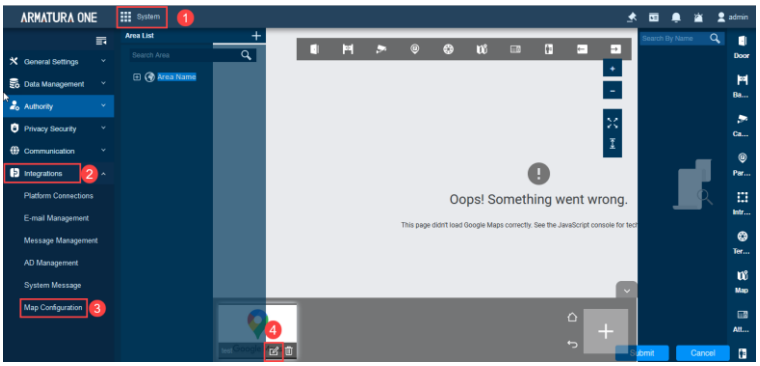
Copyright © 2024 ARMATURA LLC. All rights reserved

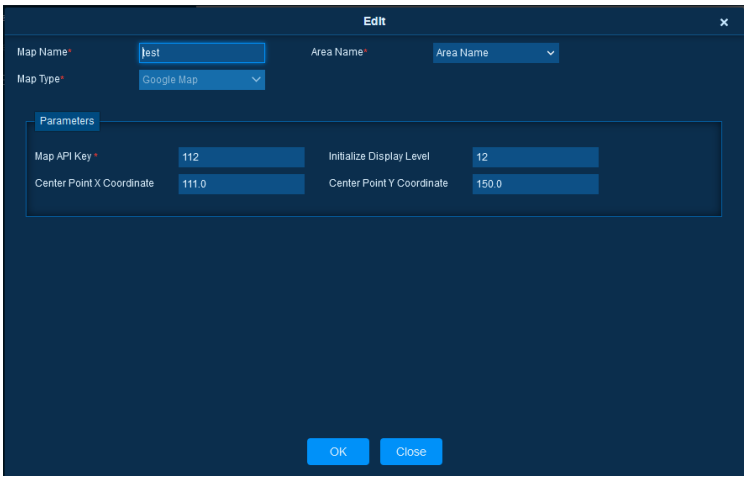
Trigger Result

Update map settings including name, key, and coordinates.

Steps:

- Navigate to **[System]** > **[Integrations]** > **[Map Configuration]** > [✎].
- Make desired changes.
- Refer to **[Adding Map]** for operation details.





Delete Map

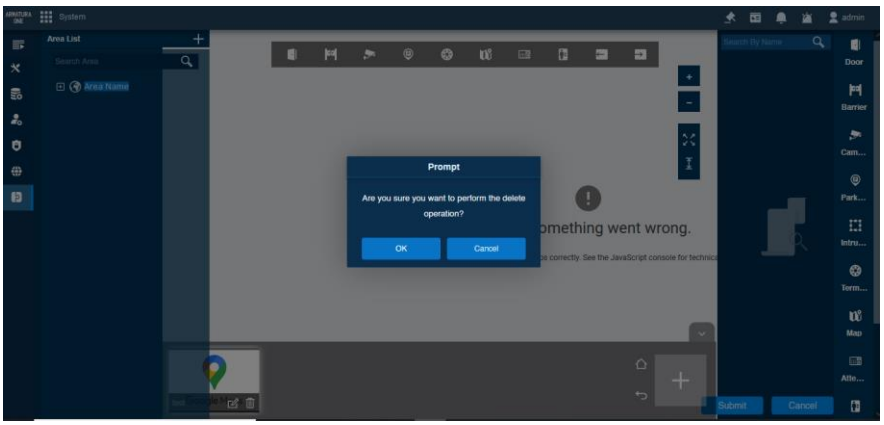
Trigger Result

Remove map and all associated devices.

Steps:

- Navigate to **[System]** > **[Integrations]** > **[Map Configuration]** > [🗑].
- Click **[OK]** to confirm deletion.

Copyright © 2024 ARMATURA LLC. All rights reserved



11.6.7 API authorization

Function Description

Manage API access credentials and permissions including creation, modification, and removal of API authorizations.

New (Add)

Prerequisites for Use

Administrator must have API creation permissions and valid API license activation.

Usage Scenarios

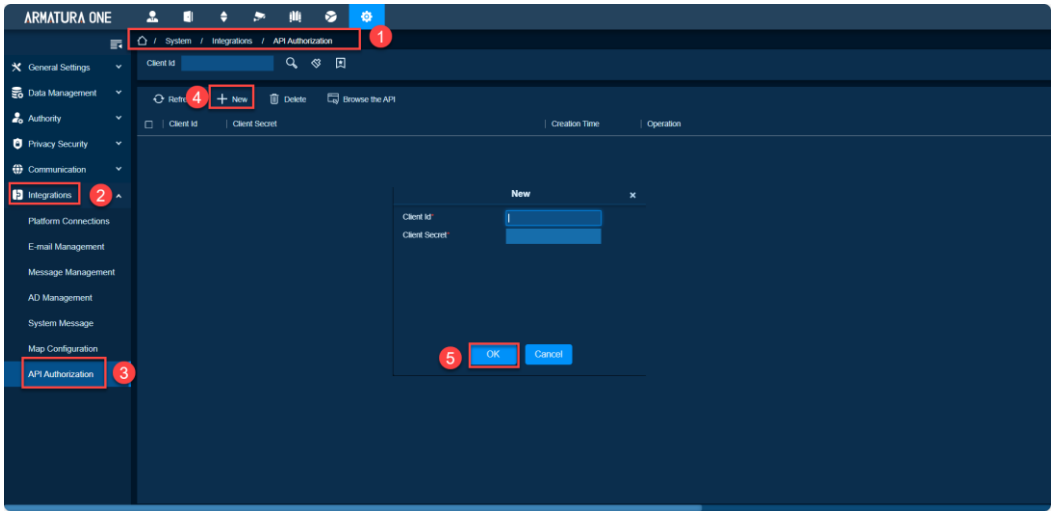
Create new API authorization credentials.

Trigger Result

New API authorization is created.

Steps:

- Click **[New]** to open configuration window.
- Complete required fields:



Copyright © 2024 ARMATURA LLC. All rights reserved

Client ID: Enter unique client identifier

Client Secret: System automatically generates based on Client ID

- Click **[OK]** to complete the add operation.

Delete

Prerequisites for Use

Administrator must have API deletion permissions.

Usage Scenarios

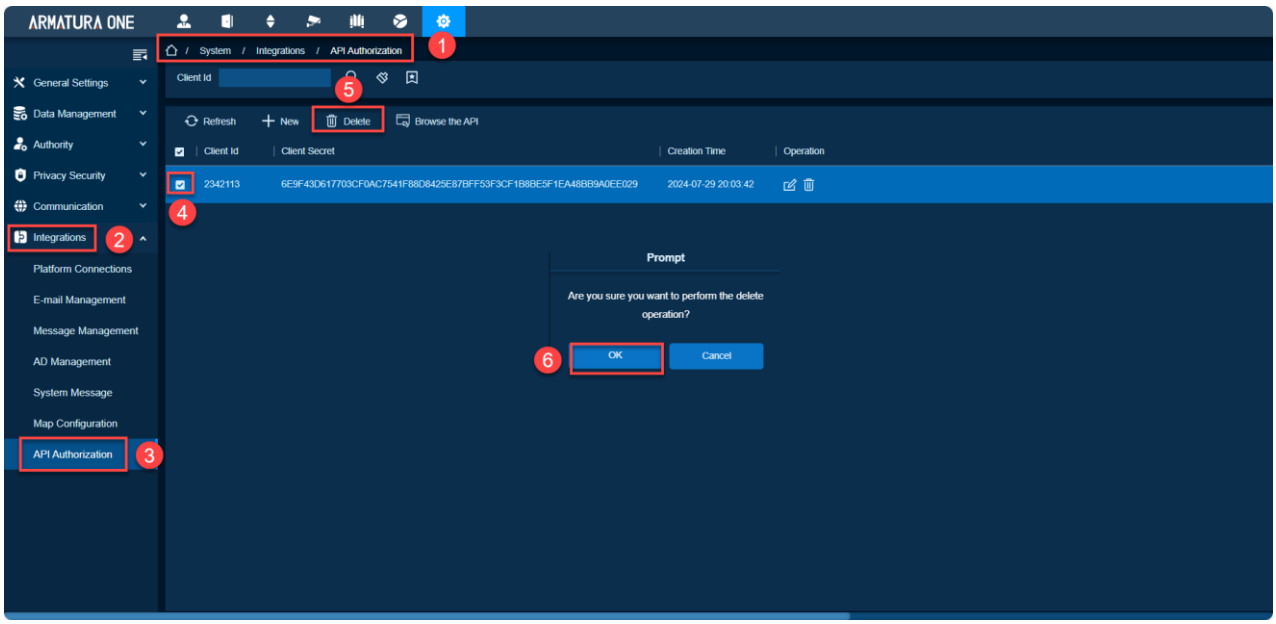
Remove unnecessary API authorizations.

Trigger Result

Selected API authorization is removed.

Steps:

- Select target API authorization.
- Click **[Delete]** to open confirmation dialog.
- Click **[OK]** to confirm deletion.



Browse the API

Prerequisites for Use

Administrator must have API viewing permissions and existing API configurations.

Usage Scenarios

View available API Swagger interface documentation.

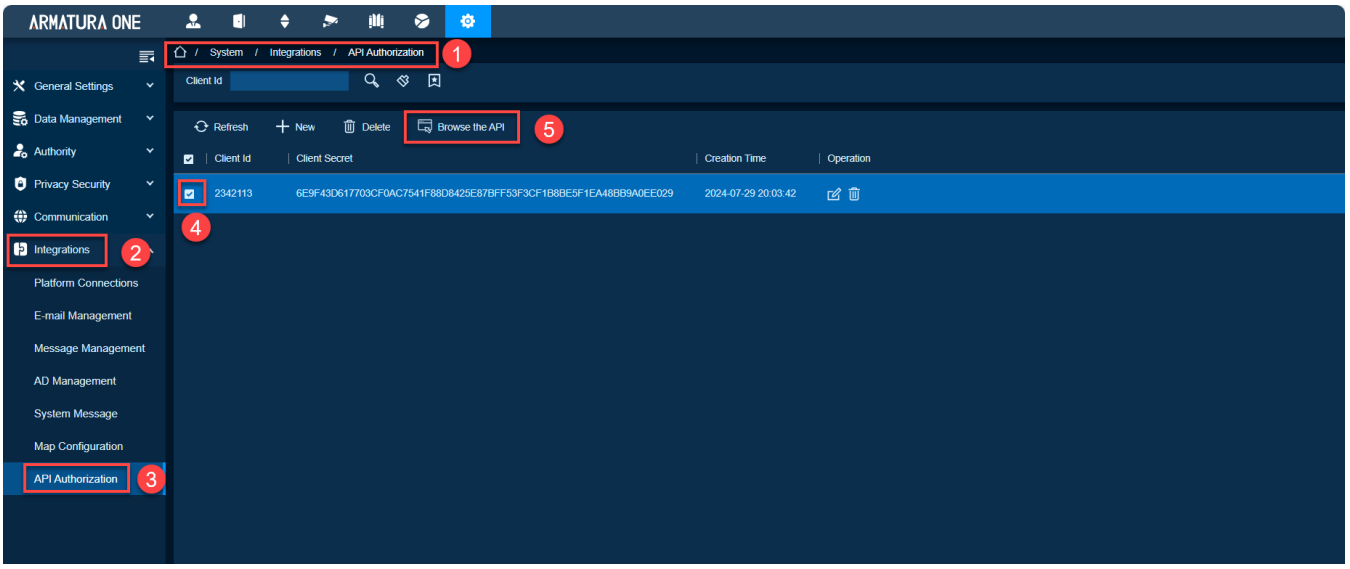
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

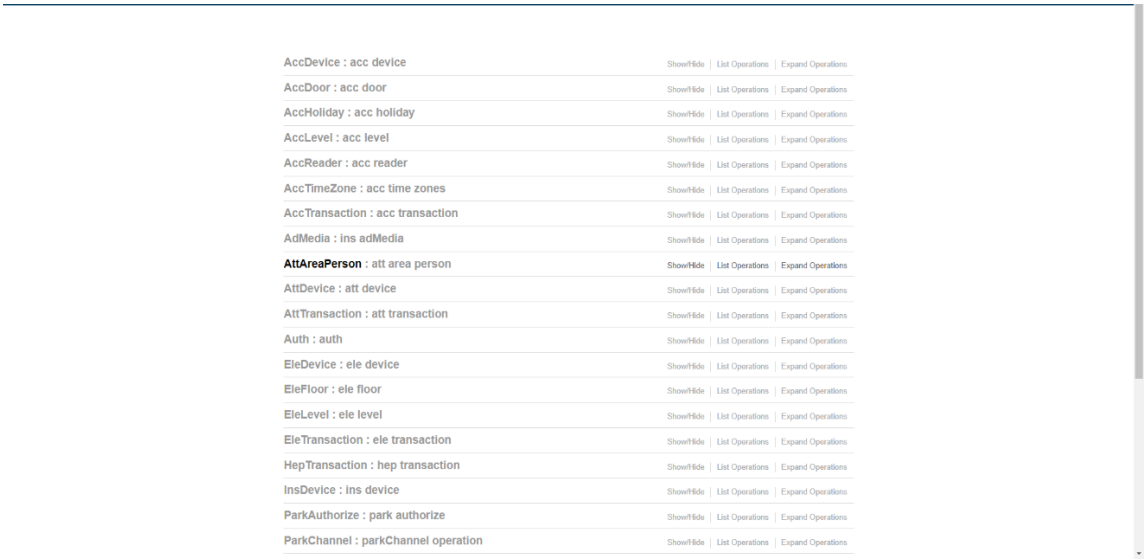
Access API Swagger documentation interface.

Steps:

- Click **[Browse the API]** to open documentation interface**.**



- Navigate to desired module documentation.



Edit

Prerequisites for Use

Administrator must have API modification permissions.

Usage Scenarios

Modify existing API authorization settings.

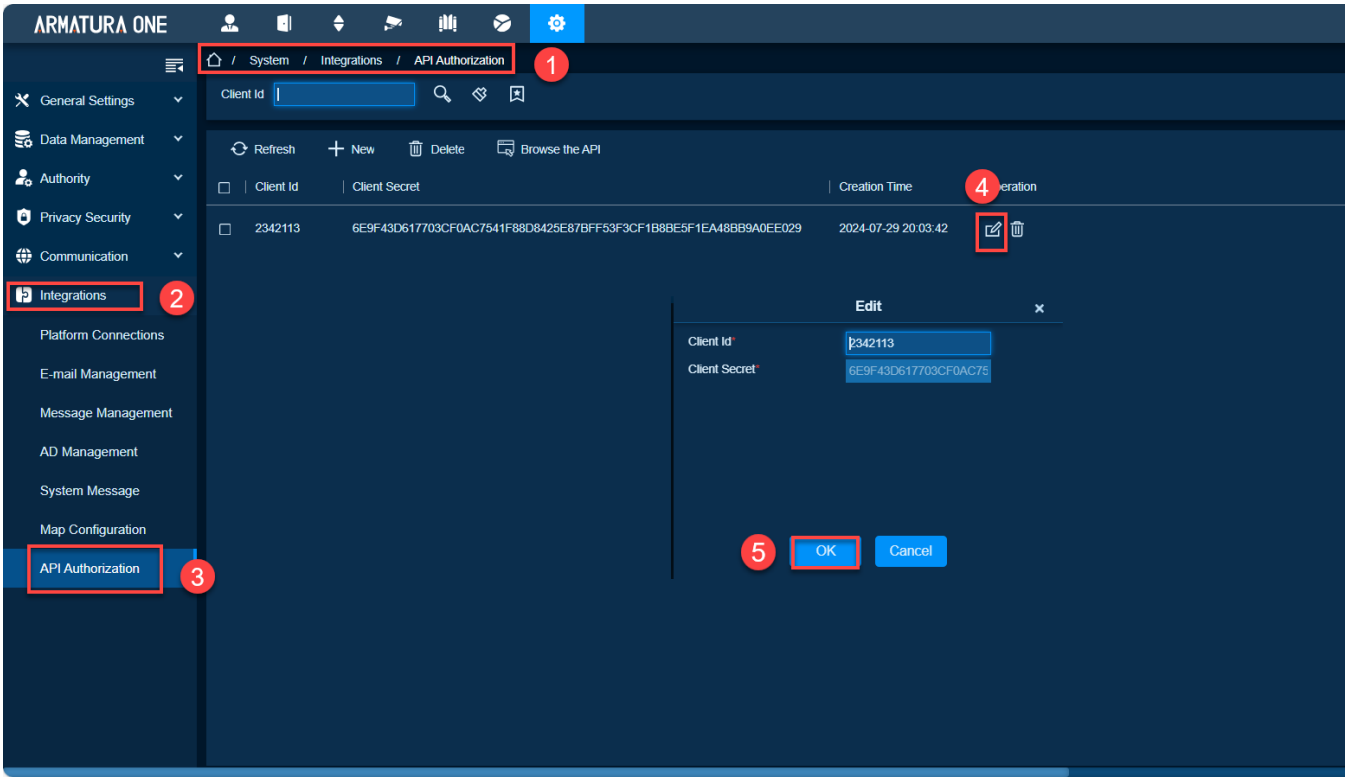
Copyright © 2024 ARMATURA LLC. All rights reserved

Trigger Result

Selected API configuration is updated.

Steps:

- Select target API authorization.
- Click **[Edit]** to open modification window.
- Click **[OK]** to save changes.



Copyright © 2024 ARMATURA LLC. All rights reserved

ARMATURA

ARMATURA LLC zktecousa.com E-mail:sales@zktecousa.com
Copyright© 2024 ARMATURA LLC. All rights reserved.