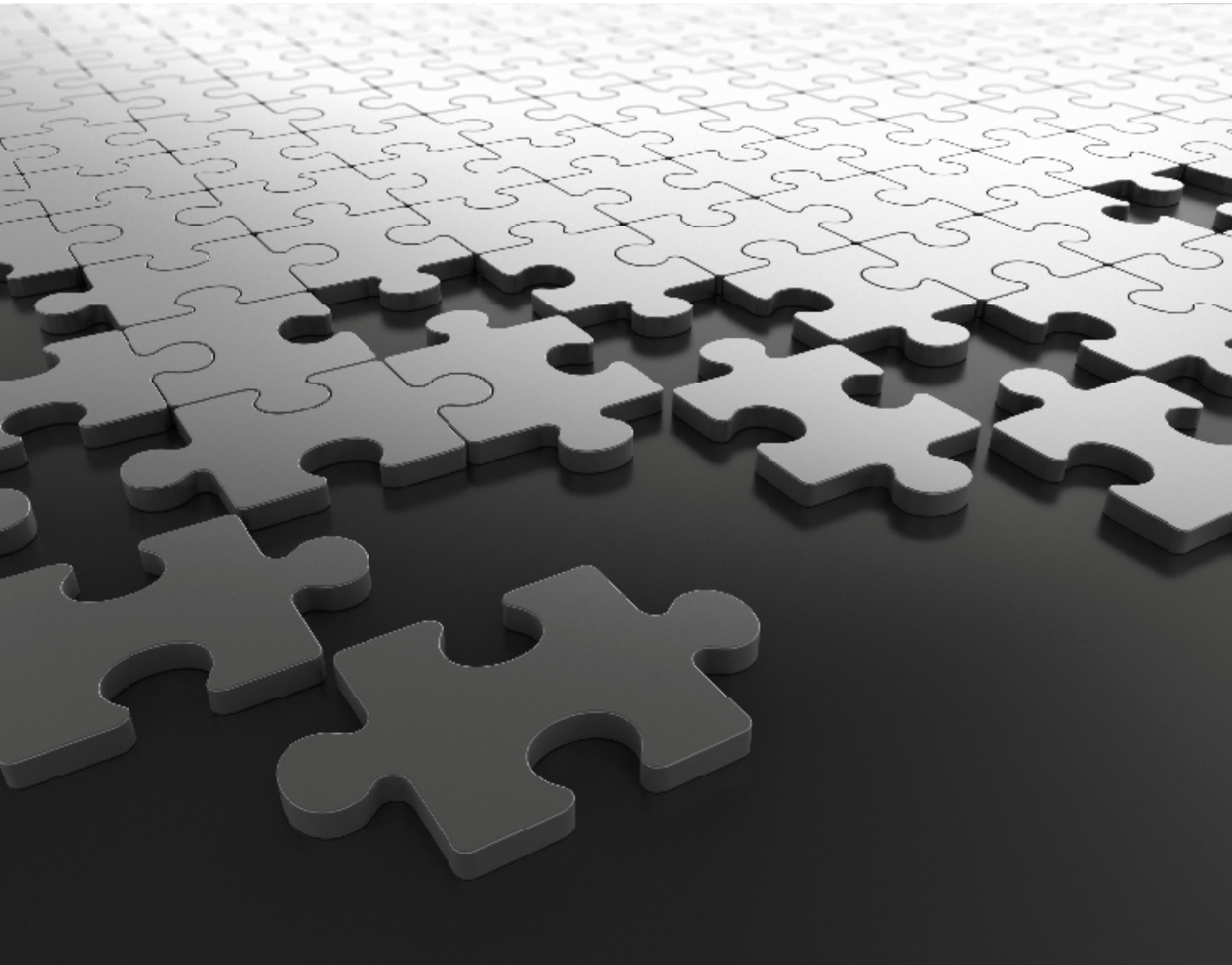


# **COSEC PANEL200**

## **System Manual**



## **COSEC PANEL200**

Multi-Door Panel for Seamless Access Control Management

### **System Manual**



# Documentation Disclaimer

Matrix Comsec reserves the right to make changes in the design or components of the product as engineering and manufacturing may warrant. Specifications are subject to change without notice.

This is a general documentation for all variants of the product. The product may not support all the features and facilities described in the documentation.

Information in this documentation may change from time to time. Matrix Comsec reserves the right to revise information in this publication for any reason without prior notice. Matrix Comsec makes no warranties with respect to this documentation and disclaims any implied warranties. While every precaution has been taken in the preparation of this system manual, Matrix Comsec assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Neither Matrix Comsec nor its affiliates shall be liable to the buyer of this product or third parties for damages, losses, costs or expenses incurred by the buyer or third parties as a result of: accident, misuse or abuse of this product or unauthorized modifications, repairs or alterations to this product or failure to strictly comply with Matrix Comsec operating and maintenance instructions.

## Warranty

For product registration and warranty related details visit us at:

<https://www.matrixcomsec.com/warranty/#access-control-time-attendance>

## Copyright

All rights reserved. No part of this system manual may be copied or reproduced in any form or by any means without the prior written consent of Matrix Comsec.

*Version 39*

*Release date: May 27, 2026*







# Contents

---

|                                        |            |
|----------------------------------------|------------|
| <b>Introduction .....</b>              | <b>1</b>   |
| <b>Know Your COSEC PANEL200 .....</b>  | <b>5</b>   |
| <b>Installing COSEC PANEL200 .....</b> | <b>13</b>  |
| <i>Connecting the PANEL200 .....</i>   | <i>15</i>  |
| <i>Configuring the PANEL200 .....</i>  | <i>17</i>  |
| <b>Quick Setup Wizard .....</b>        | <b>23</b>  |
| <b>Dashboard .....</b>                 | <b>29</b>  |
| <b>Panel Configuration.....</b>        | <b>37</b>  |
| <i>Basic Profile .....</i>             | <i>38</i>  |
| <i>Advanced Profile .....</i>          | <i>46</i>  |
| <i>Access Features .....</i>           | <i>58</i>  |
| <i>Special Functions .....</i>         | <i>64</i>  |
| <i>Input Output .....</i>              | <i>70</i>  |
| <i>Zone Configuration .....</i>        | <i>80</i>  |
| <i>Man Trap Door Group .....</i>       | <i>90</i>  |
| <i>Network Settings .....</i>          | <i>95</i>  |
| <i>Date and Time .....</i>             | <i>109</i> |
| <i>Server Settings .....</i>           | <i>111</i> |
| <i>CCC Settings .....</i>              | <i>119</i> |
| <b>Devices .....</b>                   | <b>121</b> |
| <i>Door Configuration .....</i>        | <i>122</i> |
| <i>Door Group .....</i>                | <i>149</i> |
| <i>Video Surveillance .....</i>        | <i>153</i> |
| <b>Masters .....</b>                   | <b>161</b> |
| <i>Card Format .....</i>               | <i>162</i> |
| <i>Card Personalization .....</i>      | <i>167</i> |
| <i>Wiegand Format .....</i>            | <i>172</i> |
| <b>Users.....</b>                      | <b>175</b> |
| <i>User Configuration .....</i>        | <i>176</i> |
| <i>Access Group .....</i>              | <i>190</i> |
| <i>Functional Group .....</i>          | <i>195</i> |
| <i>Blocked User .....</i>              | <i>197</i> |

|                                            |            |
|--------------------------------------------|------------|
| <b>Enrollment.....</b>                     | <b>199</b> |
| User .....                                 | 200        |
| Special Card .....                         | 205        |
| SI User .....                              | 207        |
| Authorization .....                        | 210        |
| <b>Access Policies.....</b>                | <b>213</b> |
| 2-Person Rule .....                        | 214        |
| Access Route .....                         | 218        |
| First-IN User Rule .....                   | 224        |
| Smart Card Access Route .....              | 228        |
| Time Zone .....                            | 232        |
| Access Cluster .....                       | 238        |
| Occupancy Control .....                    | 242        |
| Access Rule .....                          | 249        |
| <b>Access Schedule .....</b>               | <b>251</b> |
| Shifts and Schedules .....                 | 252        |
| Holiday Schedule .....                     | 259        |
| <b>Manage .....</b>                        | <b>263</b> |
| <b>Multi-Level Access.....</b>             | <b>271</b> |
| <b>Elevator Access Control .....</b>       | <b>283</b> |
| Elevator Configuration .....               | 285        |
| Elevator Floor Group .....                 | 289        |
| <b>Smart Elevator Access Control .....</b> | <b>297</b> |
| Elevator Facility .....                    | 300        |
| Smart Elevator Floor Group .....           | 306        |
| <b>Import, Export, Report.....</b>         | <b>315</b> |
| Import .....                               | 316        |
| Export .....                               | 318        |
| Reports .....                              | 322        |
| <b>Alerts.....</b>                         | <b>331</b> |
| Alert Message Configuration .....          | 332        |
| Alert Server Configuration .....           | 336        |
| <b>Account Management .....</b>            | <b>341</b> |
| Users .....                                | 342        |
| Password Policy .....                      | 344        |
| <b>SNMP Configuration .....</b>            | <b>347</b> |
| SNMP Configuration .....                   | 349        |
| <b>Change Password.....</b>                | <b>355</b> |
| <b>Storage Details.....</b>                | <b>357</b> |
| <b>About Device.....</b>                   | <b>359</b> |
| <b>Monitor &amp; Event Log.....</b>        | <b>361</b> |
| Monitor .....                              | 362        |
| Event Logs .....                           | 370        |
| <b>Appendix .....</b>                      | <b>375</b> |

|                                                                |            |
|----------------------------------------------------------------|------------|
| <i>Supported OSDP Commands and Responses .....</i>             | <i>375</i> |
| <i>Technical Specifications .....</i>                          | <i>392</i> |
| <i>Disposal of Products/Components after End-Of-Life .....</i> | <i>394</i> |



---

## Welcome

Thank you for choosing the Matrix COSEC PANEL200, the Multi-Door Access Control System!

We are sure you will be able to make optimum use of this product. Please read this document carefully to get acquainted with the product before installing and operating it.

## About this System Manual

This is a document providing detailed information and instructions for installing and configuring the COSEC PANEL200.

COSEC PANEL200 is an intelligent device used for access control application which operates in 3 modes — Standalone Mode, COSEC-Server Mode and Third Party-Server Mode. To know more about COSEC PANEL200, please refer [“Know Your COSEC PANEL200”](#).

The Manual is written for the Standalone Mode. All the configuration can be done from the Standalone Mode and the Third Party-Server Mode only. In the COSEC-Server Mode, all the applicable parameters will appear in read-only mode. However, specific pages can also be configured from the COSEC-Server Mode, these are specifically mentioned.

## Intended Audience

This System Manual is written for:

- **System Engineers**, who will install, maintain and support the COSEC PANEL200. System Engineers are persons who are responsible for configuring the PANEL200 to meet the requirements of the organization/ users. It is assumed that they are experienced in installing an Access Control System and are familiar with the cabling of such systems. They are expected to be aware of how it works, and the various technical terms and functions associated with it. The SE must have undergone training in the installation and configuration of the PANEL200. No one, other than the System Engineer is permitted to make any alterations to the configuration of the PANEL200.
- **System Administrators**, who are persons who will monitor and control the PANEL200 after installation. Generally, an employee of the IT/HR designation in an organization or establishment is selected as the System Administrator. It is assumed that the System Administrator has some previous experience in configuring and deploying a security cum Time and Attendance system. The System Administrators are not expected to setup and install the system hardware, but only the configuration of the system including its functionalities and features, defining the access levels for various users and the extraction of various reports.

- **Users**, persons/organizations who will use the PANEL200. They may be executives, include personnel of small and medium businesses, large enterprises, front desk and service staff of Hotels/Motels, hospitals, and other commercial and public organizations/institutions.

## Organization of this Document

This system manual contains the following important topics:

- **Introduction:** gives an overview of this document, its purpose, intended audience, organization, terms and conventions used to present information and instructions along with Dashboard of PANEL200.
- **Dashboard:** gives you an overview of all the users, doors and access rules.
- **Configuration:** describes the Basic and Advanced configuration — PANEL, Door, Users, Access Policies and other features, as well as instructions on how to manage the PANEL200.
- **Monitor:** provides the status overview of — Door, IO Link, Alarm, Live Events and Time Trigger.
- **Event Log:** provides the log of events based on different search criteria.
- **System Log:** allows you to enable the desired logs for troubleshooting.

## How to Read this System Manual

This document is organized in a manner to help you get familiar with the PANEL200, learn how to install it, connect it in various network topologies, connect the external devices, and power up the hardware systems. The manual also covers the installation and configuration of the PANEL200 and its dependent components.

This System Manual is presented in a manner that will help you find the information you need easily and quickly.

You may use the table of contents and the Index to navigate through this document to the relevant topic or information you want to look up.

### • Instructions

The instructions in this document are written in a step-by-step format, as follows. Each step, its outcome and indication/notification, wherever applicable, have been described.

### • Notices

The following symbols have been used for notices to draw your attention to important items.



**Important:** to indicate something that requires your special attention or to remind you of something you might need to do when you are using the system.



**Caution:** to indicate an action or condition that is likely to result in malfunction or damage to the system or your property.



**Warning:** to indicate a hazard or an action that will cause damage to the system and or cause bodily harm to the user.



**Tip:** to indicate a helpful hint giving you an alternative way to operate the system or carry out a procedure, or use a feature more efficiently.

## Terminology used in this System Manual

The technical terms and Acronyms used in this Manual are standard terms, commonly used in the Access Control and Time and Attendance industry. However, considering the broad group of intended users of this manual, wherever possible, use of jargon has been avoided.

The term PANEL, COSEC PANEL200, PANEL200 are used interchangeably but mean the same. Door refers to Panel Door including their variants. The features and functionalities of each door differ as per the variant.

Using this Manual in conjunction with the COSEC PANEL200 and Doors Quick starts, we hope, you will be able to set up, configure and make optimum use of this feature packed access control system.

## Getting Help

Our online help will provide you with immediate and context-related help.

- To get a more focused and context sensitive help, click **Help**  located on the upper right corner of the desired page.
- You can also download the entire System Manual. To do so, click **Download Manual**  . You can navigate to the relevant topic of interest in the System Manual.

## Technical Support

If you cannot find the answer to your question in this Manual or in the Help files, we recommend you contact your system installer. Your installer is familiar with your system configuration and should be able to answer any of your questions.

If you need additional information or technical assistance, contact our Technical Support Team.

|          |                               |
|----------|-------------------------------|
| Phone    | +91 (18002587747)             |
| Internet | www.MatrixComSec.com          |
| E-mail   | Tech.Support@MatrixComSec.com |





# ***Know Your COSEC PANEL200***

---

COSEC PANEL200 is a strong and scalable access controller made to manage multiple doors. It supports up to 255 doors for centralized monitoring and control. With features like real-time event alerts and data encryption, it ensures high security. PANEL200 is perfect for large businesses, factories, healthcare centers, and schools needing centralized access management.

PANEL200 is an intelligent device used for access control application. It works on 3 different modes — [“Standalone Mode”](#), [“COSEC-Server Mode”](#) and [“Third Party-Server Mode”](#).

There are different applications of PANEL200. For details refer to [“Applications of PANEL200”](#).

PANEL200 has an inbuilt SDK that supports the functionality of various features. PANEL200 having support of SDK1 can be upgraded with SDK2. However, PANEL200 with SDK2 cannot be downgraded to SDK1. To know the SDK Version, refer to [“About Device”](#). For upgrading the SDK version contact our Technical Support Team. However, if your PANEL200 is working on SDK1, certain features are not supported in the same. For detailed list of features, refer to [“Features not supported in SDK1”](#).

In Third Party-Server Mode, only SDK2 is supported.

## **Standalone Mode**

When in Standalone Mode, PANEL200 acts a site controller that offers advanced access control features. It also has an Embedded Web Server.

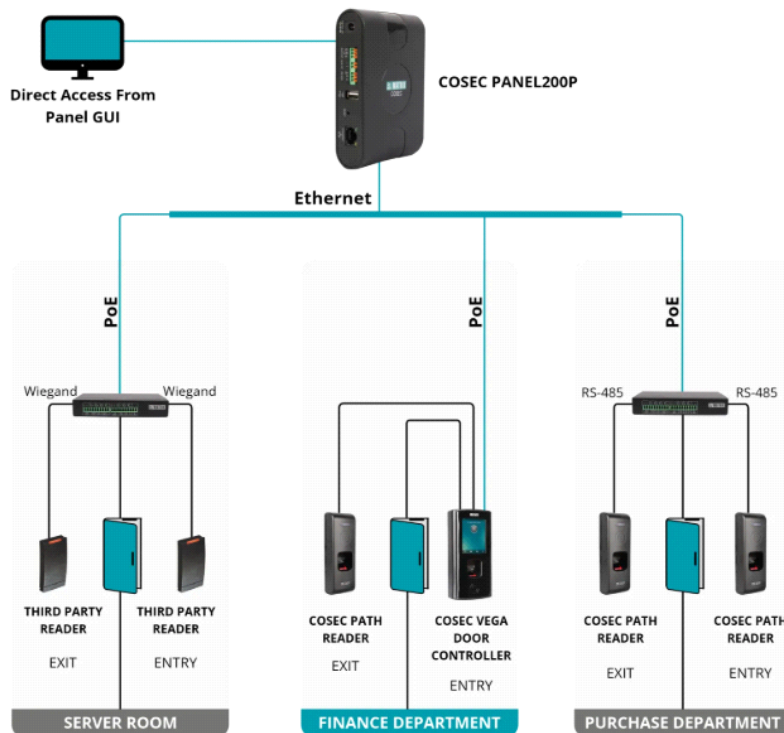
### **Features of Standalone Mode**

- **Access Controller with 25+ Advanced Access Features**
  - Man Trap, Dead Man Zone, Anti-Pass Back
  - 2-Person Rule, First-In User, Guard Tour
  - Elevator Access Control, Access Route, and Many More
  - Gain Full-fledged Access Control for Standalone Operations as well as Multi-Locations
- **The Access Controller supports Multiple Communication Options**
  - Built-in Bluetooth, Wi-Fi, USB, Ethernet, RS-485
  - Use Existing IT Infrastructures to Meet Future Needs
- **Better Control and Higher Storage Capacity**
  - Controls up to 255 Doors
  - Stores up to 25,000 User Profiles
  - Event Log Capacity of 5,00,000
- **Secured Communication:** PANEL200 Access Controller secures data transmission with SSL encryption, providing a highly reliable solution that is snoop-proof and hack-proof.

- **IP to Door:** Eliminate the need for long cables between the control panel, reader, and lock, reducing costs effectively with the innovative IP to Door technology.
- **Plug and Play:** Simplify installation and management with built-in web software and plug-n-play capability with no need for additional servers.
- **Auxiliary s Interface:** Allow seamless connection of fire alarm, as well as motion sensors and relay s via aux ports, eliminating the need for external integration hardware.
- **Compact Design:** Access controller features an innovative, compact design that seamlessly integrates above the door on a false ceiling, ensuring aesthetic appeal and a neat installation.
- **Push API:** Enable seamless communication with third-party software, allowing customers better control.
- Ethernet, Wi-Fi, Bluetooth and RS-485
- USB Port for Wi-Fi, 3G/4G/LTE and Data Transfer
- Auxiliary Input and Output Ports
- Events Storage up to 500,000
- Controls 255 Doors with 255 Exit and Entry Readers or 255 Doors with 255 Readers and 255 Exit Switches
- Supports 25,000 Users

In Standalone mode, PANEL200 (site controller) works independently without requiring a server for access control application.

### STANDALONE MODE OF OPERATION

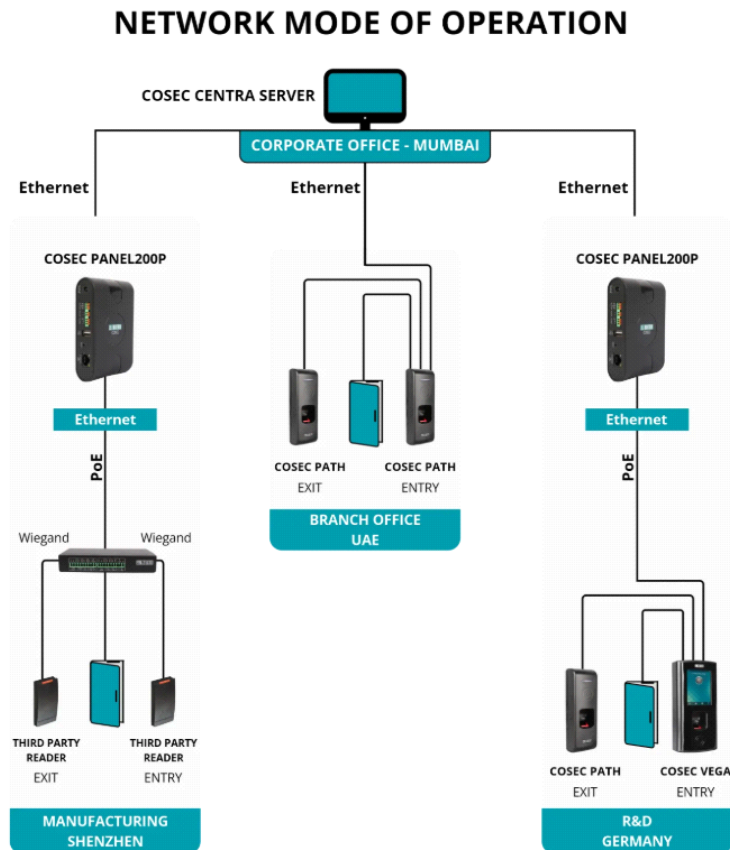


All Matrix COSEC biometric/face/card based doors are connected to the site controller for implementing advance access control features and restricting any unauthorized entry.

With its interactive and user friendly UI, it can manage 255 COSEC Doors and 25,000 users. This mode of operation is ideal for small and medium businesses, which need advance access control with minimum investment.

## COSEC-Server Mode

When in COSEC - Server Mode, PANEL200 manages multiple controllers and acts as a bridge between COSEC Application and COSEC Doors. COSEC biometric/face/card based doors are connected with PANEL200 using Ethernet or RS-485. PANEL200 is responsible for synchronizing all doors and implementing advanced access control features.



COSEC PANEL200 is required in Server Architecture —

- When Number of User Capacity Exceeds the Door's Capacity.
- For Advanced Access Control Features like Guard Tour, Man Trap, Dead-Man Zone, Duress Detection, Do Not Disturb, etc.



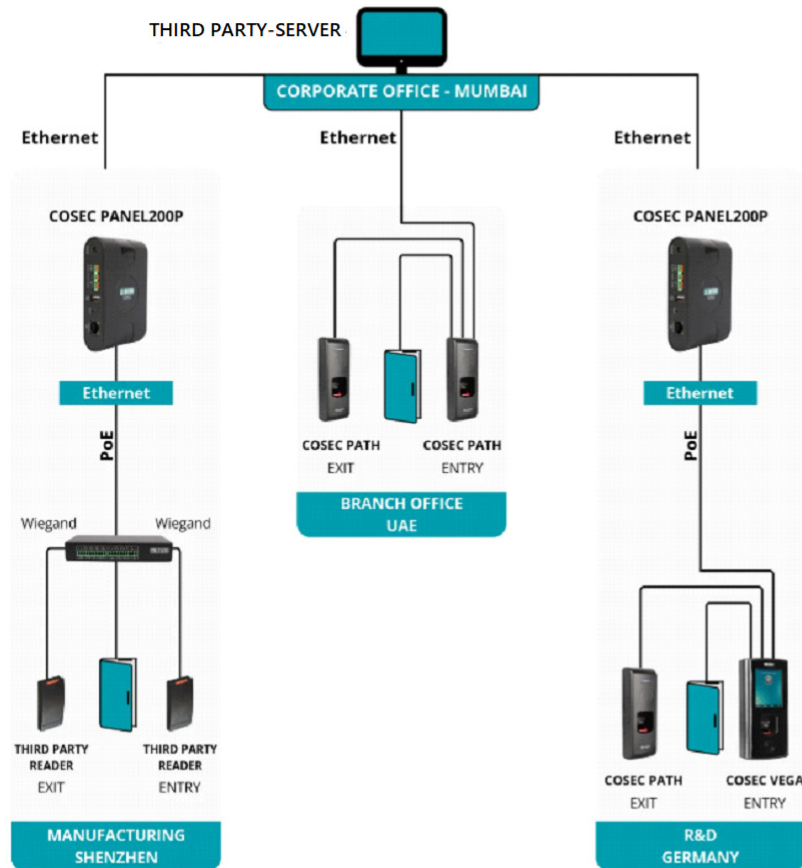
*If you are accessing the COSEC Server GUI, Device Module> Device Configuration > Click Add, there are three options related to PANEL, namely Panel, Panel Lite and Panel200.*

*Panel and Panel Lite are phased-out and are provided for maintenance purpose only. Please contact Matrix Technical Support for further details.*

## Third Party-Server Mode

Integrate PANEL200 with Third Party - Server, so that the Basic and Advance Access Control features of PANEL200 can be accessed by their unified software.

In this mode it supports all the features as mentioned in Standalone Mode. For details, refer to [“Standalone Mode”](#).



## Applications of PANEL200

| USE      | STANDALONE MODE/THIRD PARTY-SERVER MODE                                                                | SERVER MODE                                  |
|----------|--------------------------------------------------------------------------------------------------------|----------------------------------------------|
| For      | SMB, SME and SOHO                                                                                      | Enterprises and SME                          |
| Location | Single Location (Standalone Mode)<br>Multiple Location with multiple PANEL200-Third Party-Server Mode) | Multiple Location with COSEC CENTRA          |
| Software | Built-in with COSEC PANEL200                                                                           | Web-based with COSEC CENTRA                  |
| Capacity | Connect up-to 255 Doors with COSEC PANEL                                                               | Connects up-to 65000 Doors with COSEC CENTRA |
| Users    | 25000 Users with COSEC PANEL                                                                           | 1 million Users with COSEC CENTRA            |

## Features not supported in SDK1



*SDK1 is not applicable to Third Party-Server Mode.*

- ARGO FACE and ARGO FACE210 Door is not supported.
- Enrolled Face Count will not appear on Dashboard > [“Users Dashboard”](#).
- Following parameters will not be supported in Panel Configuration:
  - Panel Configuration > Basic Profile > [“General”](#)- Max. No. of Faces Per User (Standalone Mode).
  - Panel Configuration > Basic Profile > [“General”](#)- Face Validation Device.
  - Panel Configuration > Basic Profile > [“Panel Mode”](#)- Request Retry Timer (min).
  - Panel Configuration > Basic Profile > [“Panel Mode”](#)- Authentication Type and Authentication Algorithm.
  - Panel Configuration > Advanced Profile > [“Settings”](#)- Auto Add/Update Enrolled Face as Profile Photo.
  - Panel Configuration > Advanced Profile > [“Settings”](#)- Assign Doors to New Users.
  - Panel Configuration > Advanced Profile > Alarms and Timers > [“Alarms”](#)- Face Mask Compulsion, Duress and Tail-Gating for ARGO FACE and ARGO FACE210 Door.
  - Panel Configuration > Advanced Profile > [“Enrollment”](#)- Face as Enrollment Mode.
  - Panel Configuration > Advanced Profile > [“Enrollment”](#) - Max Number Of Faces.
  - Panel Configuration > [“Special Functions”](#) > Global Special Functions- Global Lock, Global Unlock, Global Normal, Global Arm and Global Disarm.
  - Panel Configuration > Zone Configuration > [“Basic Configuration”](#) > Face/ Face + PIN/ Face + Card as Access Mode in- Internal or Reader Group1 Mode.
  - Panel Configuration > Network Settings > [“LAN Settings”](#) > IP Assignment.
  - Panel Configuration > Network Settings > [“Advanced LAN Settings”](#) tab.
  - Panel Configuration > Network Settings > [“Wi-Fi Network Settings”](#) > DHCP (earlier Dynamic) under IP Assignment.
  - Panel Configuration > Network Settings > [“Wi-Fi Access Point Settings”](#)- Wi-Fi signal strength icon.
- Following parameters will not be supported in User Configuration:
  - Users > [“User Configuration”](#)- Face Images (Updated At) in User List for Standalone Mode.
  - Users > User Configuration > [“Basic Access Control”](#)- Enrolled Faces.
  - Users > User Configuration > [“Advanced Access Control 2”](#) - Smart Elevator Access Control.

- Users > User Configuration > “Face Recognition” tab.
- Following parameters will not be supported in Device Configuration:
  - Devices > Video Surveillance > “Built-In Camera” tab.
  - Devices > Door Configuration > “Basic Configuration” > Allowed/Denied Acknowledgment range 250ms-3000ms and Shortest option for LED-Buzzer range.
  - Devices > Door Configuration > “Readers” > RS-485 Interface Protocol, Matrix Reader Type and OSDP Parameters in ARC DC200.
  - Devices > Door Configuration > “Advance Configuration”> Pulse Timer range 0.1 to 65535.0 (sec).
  - Devices > Door Configuration > “Advance Configuration”> Duplicate Access Time Interval for ARGO, VEGA, ARGO FACE and ARGO FACE210 Door.
  - Devices > Door Configuration > “Advance Configuration 2” tab in COSEC-Server Mode.
  - Devices > Door Configuration > “Face Identification Settings” tab for Standalone Mode.
- Enrollment > “User”- Face as Enrollment Type and No. of Faces will not be supported.
- Enrollment > “Special Card” > Special Functions: Global Special Functions- Global Lock, Global Unlock, Global Normal, Global Arm and Global Disarm.
- Access Policies & Access Schedule > “First-IN User Rule” > Maximum limit of First-IN Users in a group 999.
- Access Policies & Access Schedule > “Shifts and Schedules” > Maximum limit of Shift creation 1402.
- Elevator Access Control > “Elevator Configuration”- Maximum limit of Elevator creation 64 and Floor addition 99 and Search bar will not be supported.
- Elevator Access Control > “Elevator Floor Group”- Maximum limit of Floor Group creation 999 and search bar will not be supported.
- The feature “Smart Elevator Access Control” will not be supported.
- Import, Export, Report > “Import”

The following parameters will not be supported while importing:

| Import Data          | Parameter                  | Action                              |
|----------------------|----------------------------|-------------------------------------|
| User Configuration   | Face Recognition           | Any values entered will be ignored. |
| Device Configuration | Device Type=21             | Import process will fail.           |
| Device Configuration | Face Mask Compulsion Alarm | Any values entered will be ignored. |

- Import, Export, Report > “Export”

The following parameters will not be supported while exporting:

| Template             | Parameter                  | Action                                                 |
|----------------------|----------------------------|--------------------------------------------------------|
| User Configuration   | Face Recognition           | Value will be 0.                                       |
| Device Configuration | Device Type=21             | Device Type=21 will not be present in the Export file. |
| Device Configuration | Face Mask Compulsion Alarm | Value will be NA.                                      |

- Import, Export, Report > Export > [“Templates”](#)

For User Configuration Template Type, Face Recognition field will not be supported in Field drop-down list.

For Device Configuration Template Type, Face Mask Compulsion will not be supported in Field drop-down list.

- Import, Export, Report > Reports > [“User”](#)- User Report will not contain Enrolled Faces count.
- Import, Export, Report > Reports > [“Event”](#)- in Source Type **User**, Credential Type, Credentials and Card Selection will not be displayed.
- Monitor & Event Log > [“Monitor”](#) > [“Live Events”](#)- the filters for — Device, Device Type, User ID, User Name, Credential, the columns —User ID, User Name, Credential and Entry/Exit in Live Events grid, Column Drop-down, Search Bar will not be displayed.
- Monitor & Event Log > [“Event Logs”](#)- Event Filters, the columns —User ID, User Name, Credential and Entry/Exit, Snapshot Image in Event Log grid, Column Drop-down, Search Bar will not be displayed.
- Following alerts will not be supported in Alert Message Configuration:
  - Alerts > [“Alert Message Configuration”](#)-
    - Event Type- System, Event- Captured Snapshot Count Full will not be displayed.
    - Event Type- Access Control, Event- User Allowed- Face Mask Not Detected will not be displayed.
    - Event Type- Access Control, Event- User Denied- Face Mask Not Detected will not be displayed.
- Storage Details > [“Captured Snapshot Details”](#) section will not be displayed.





---

## **Package Contents**

- COSEC PANEL200
- Power Adapter
- 2 Wall Mounting Screws and Screw grip

## **Things You Will Need**

- A Wire Stripper
- A Screw Driver Set
- Insulation Tape
- Access to the COSEC Server/Third Party Server, if wish to use it in the COSEC-Server Mode/Third Party Server mode
- A standalone Computer with a Web Browser to change the Network Settings of the PANEL200

## **Safety Instructions**

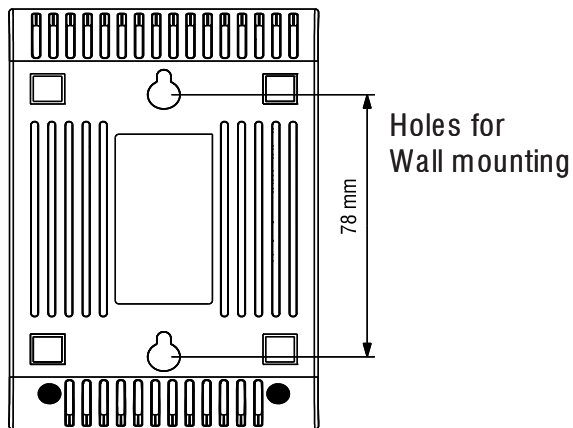
Do not install the device:

- On unstable surfaces.
- Where ferromagnetic field or noise is induced.
- Where static is created, such as desks made of plastic, carpets.
- Near volatile inflammable materials or inflammable goods such as drapes.
- Where volatile gas and/or inflammable gas is created.

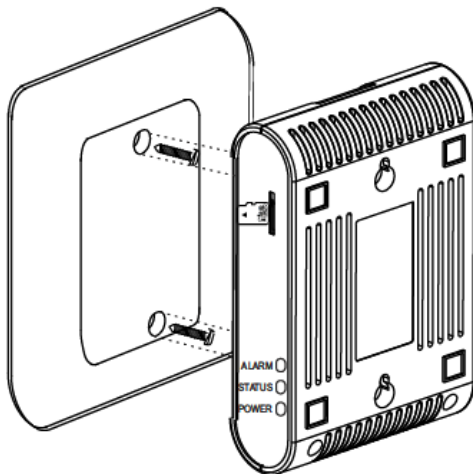
## **Mounting the PANEL200**

- Unpack the PANEL200 and check your package contents. If anything is missing or damaged, please contact your point of purchase.
- Select a suitable location for Wall mounting. Make sure the surface is flat. You can also Table Mount it.

- Drill holes as per the size of the screws provided and at the distance as shown below.



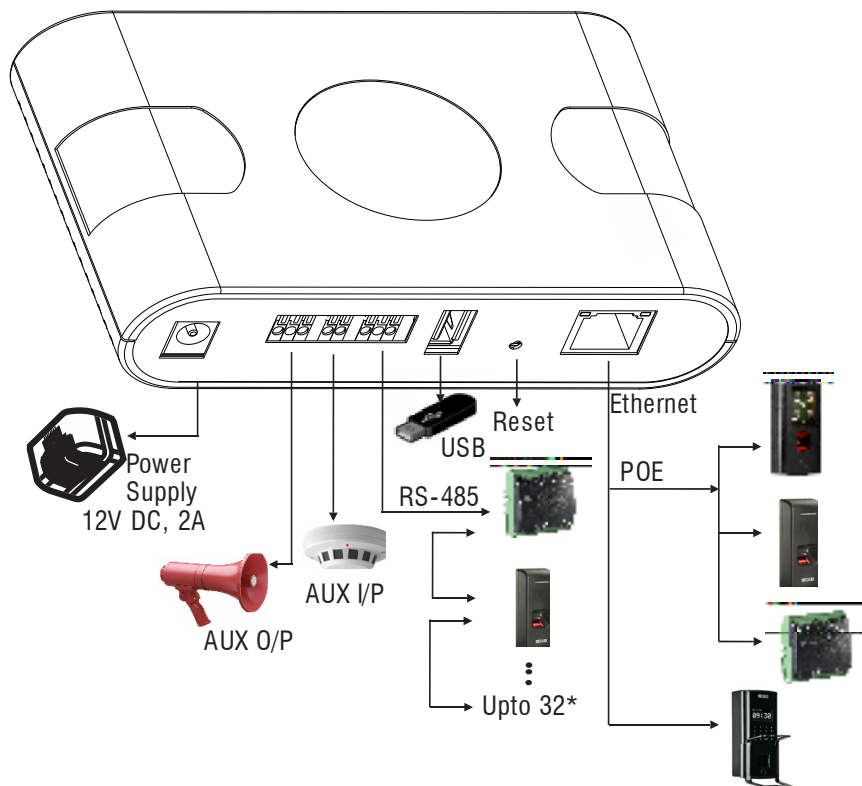
- Insert the screw grips in the holes you drilled.
- Drive the screws into the wall. Leave the screw heads protruding slightly (2 to 4 mm gap from the wall), enough for the keyhole slots of the PANEL to engage.



- Hold the product against the wall, aligning the larger openings of the keyhole slots with the screw heads. Slide the product downward or sideways (depending on slot orientation) until the screws sit securely in the narrow part of the keyhole slots.

# Connecting the PANEL200

---



## Connecting wires to AUX O/P/AUX I/P/RS-485 Ports

- Push back the orange lever of the connector of appropriate port, using a blunt pin or a small flat screw driver.
- Insert the stripped end of the wire into the opening of the connector.
- Release pressure on the levers. The wire will be held in place by spring clamp action.

## Connecting Doors

- Using RS-485, you can connect upto 32 doors in a loop.
- Using Ethernet, you can connect upto 255 doors through the Ethernet switch. The POE enabled doors will not require external power supply.

## Connecting Auxiliary Input

- You can connect a sensor for detecting alarm conditions. For this, connect the Auxiliary Input Port.
- For this connect the wire pair from the sensor to the Auxiliary Input Port.

## Connecting Auxiliary Output

- The Auxiliary Output port can be used for activating alarm s like hooter; energize some s; control annunciation s. For this connect the wires from the alarm s to the Auxiliary Output Port.

## USB

The USB port can be used for connecting Wi-fi Dongle or Mobile Broadband Dongle. It is used to download events directly from PANEL200 to USB memory.

## Reset

The Reset pin can be used to set the Password and Network settings of the PANEL200 to default.

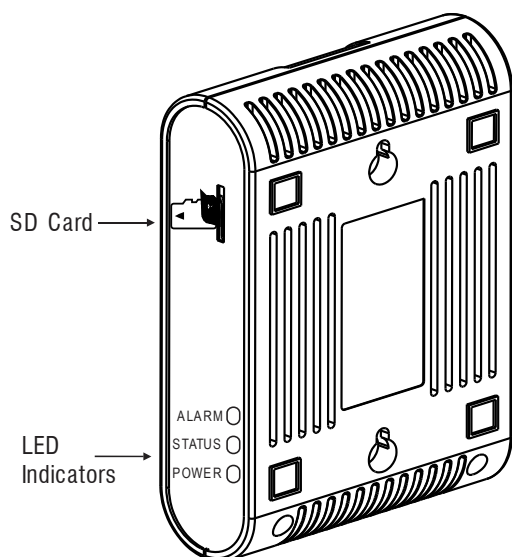
## SD Card

The SD card is used for the storage of internal processing data.

## Powering ON the PANEL200

Apply 12V DC,2A power supply to the PANEL200 and wait for the reboot cycle to complete. At the time of start up i.e. Bootloader state, the Power LED will glow in constant Red color.

The PANEL200 has 3 LEDs, that is, ALARM, STATUS and POWER. The table below shows some common indications.



## LED Status Indicators

| State                                 | Power LED | Status LED      | Alarm LED               |
|---------------------------------------|-----------|-----------------|-------------------------|
| Power ON Sequence                     | Red ON    | Orange blinking | Red Blinking            |
| Idle-Online (when online with Server) | Red ON    | Green blinking  | -                       |
| Idle-Offline                          | Red ON    | Red blinking    | -                       |
| Idle-Network Fault / Link Fail        | Red ON    | Orange blinking | -                       |
| Critical Alarm                        | -         | -               | Glows in Red till Reset |
| Minor and Major Alarms                | -         | -               | Red Blinking            |

# Configuring the PANEL200

---

PANEL200 provides an embedded web server with a Graphic User Interface (GUI), Jeeves, for configuration.

To access Jeeves, you will need to connect a computer to PANEL200.

## Connecting a Computer

You may connect a standalone computer to PANEL200 or grab any computer connected in the same LAN as PANEL200.

Connect a standalone computer to PANEL200, when installing the system for the first time. You may connect it to the LAN after you have finished installation and configuration of the system.

To connect a standalone computer,

- Plug one end of the Ethernet cable into the Ethernet Port of PANEL200. Plug the other end into the LAN Port of the computer.
- Make sure the IP Address of the computer and the Ethernet Port of PANEL200 do not conflict, and that both are in the same Subnet.

The default IP Address of the LAN Port of PANEL200 is: **192.168.50.1**

The default Subnet Mask of the LAN Port of PANEL200 is: **255.255.255.0**.

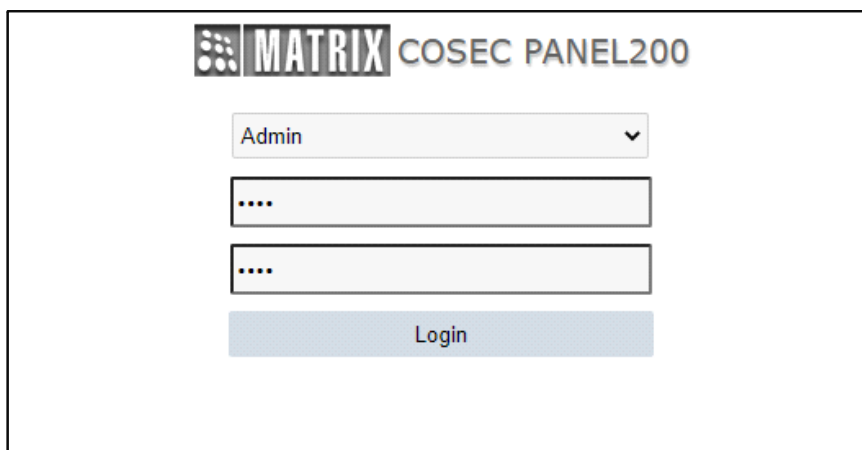
Change the Subnet of the computer, if necessary.

- Open the browser on the computer and enter the IP address of the PANEL200 (default: `http://192.168.50.1`), in the address bar of the browser and press the Enter key on your computer keyboard.
- You can use the PANEL200 in any of the following modes:
  - COSEC-Server Mode (default mode)
  - Standalone Mode
  - Third Party-Server Mode

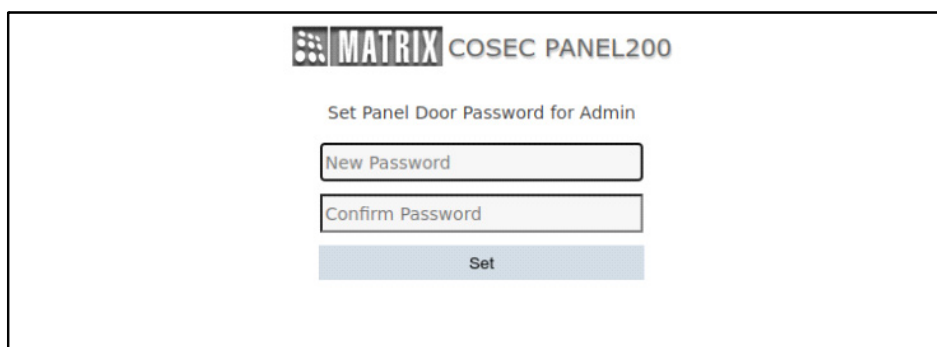
- The Login page appears. By default the PANEL200 is in the Server Mode and you need to change the Panel Mode to Standalone.



- Enter the login credentials of the PANEL200. Default User Name: Admin.
- You need to set the password. Configure the desired password in **New Password** and re-enter the same in **Confirm Password**.



- Click **Login**.
- The **Set Panel Door Password for Admin** page appears.

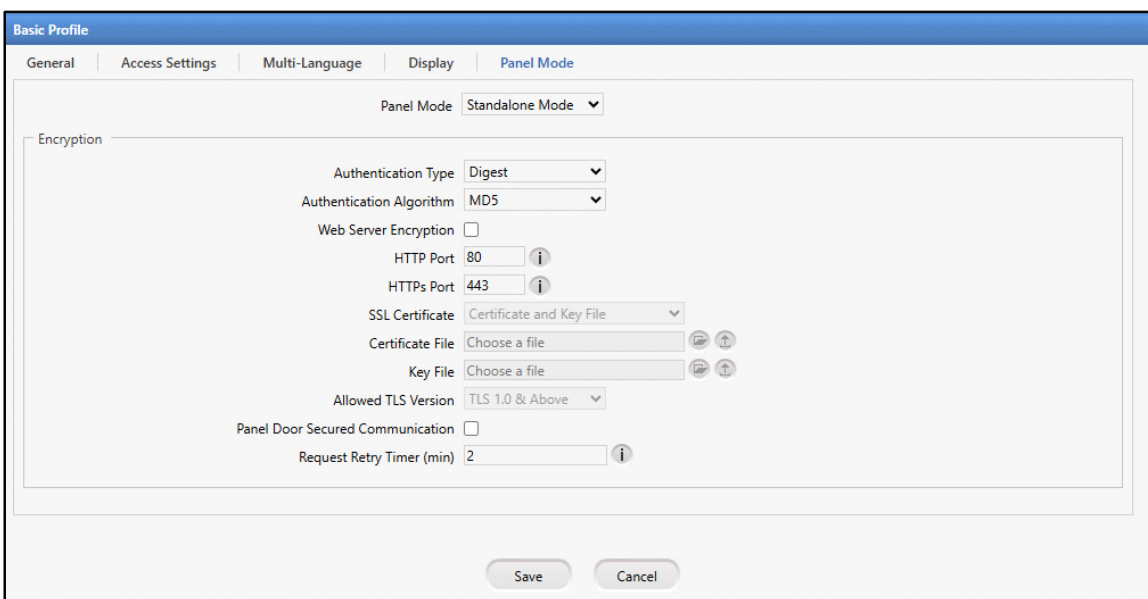


- Configure the desired password in **New Password** and re-enter the same in **Confirm Password**. Only numeric values are allowed.

- Click **Set**. The **Dashboard** page appears.



- To change the Panel Mode, click **Panel Configuration > Basic Profile > Panel Mode**. The Panel Mode page appears.

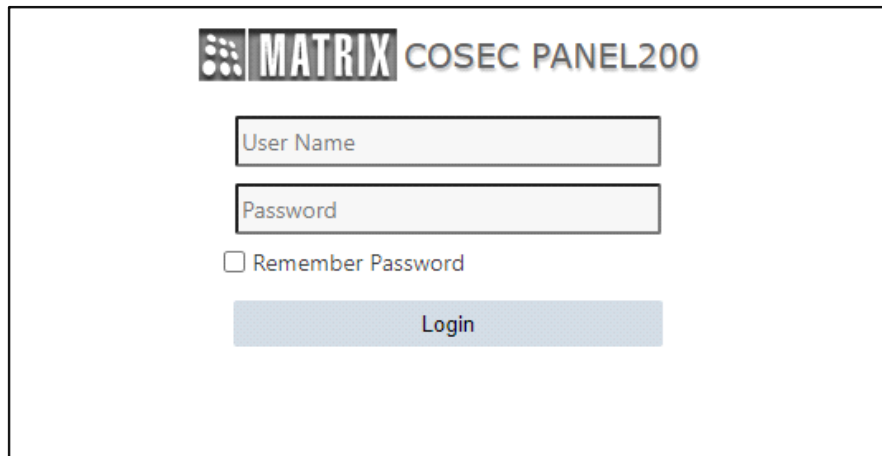


- Select the **Standalone Mode** from the drop-down list. The PANEL200 will reboot.



*If you wish to use the PANEL200 in Third Party-Server Mode, click **Panel Configuration > Basic Profile > Panel Mode** and select **Third Party Mode** from the drop-down list.*

- Click **Refresh**. The Login page appears.



MATRIX COSEC PANEL200

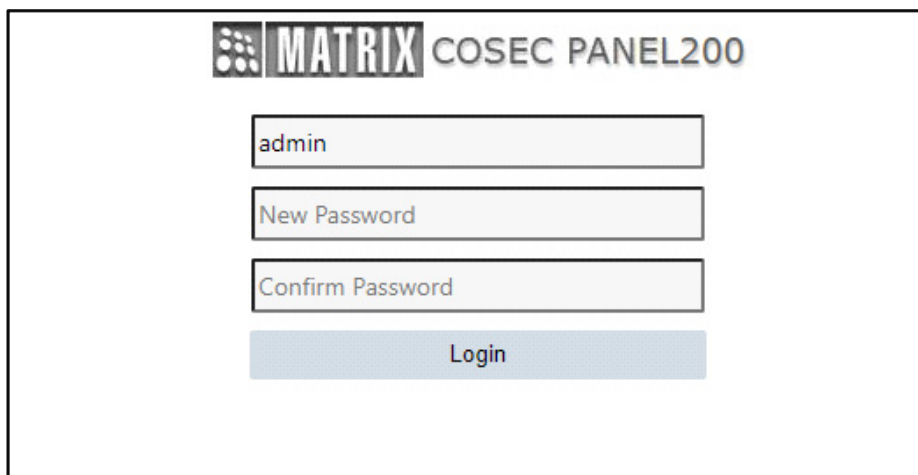
User Name

Password

☐ Remember Password

Login

- Enter the login credentials of the PANEL200.
- Configure the User Name as admin.



MATRIX COSEC PANEL200

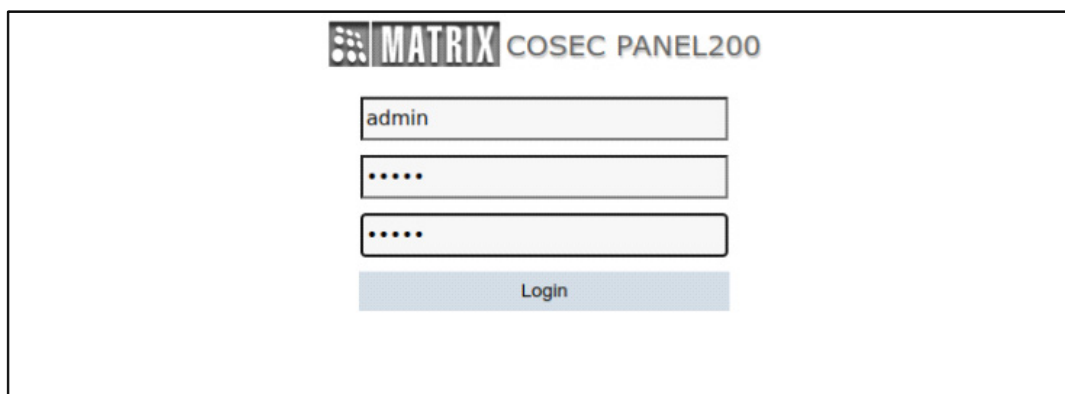
admin

New Password

Confirm Password

Login

- You need to set the password. Configure the desired password in **New Password** and re-enter the same in **Confirm Password**.



MATRIX COSEC PANEL200

admin

.....

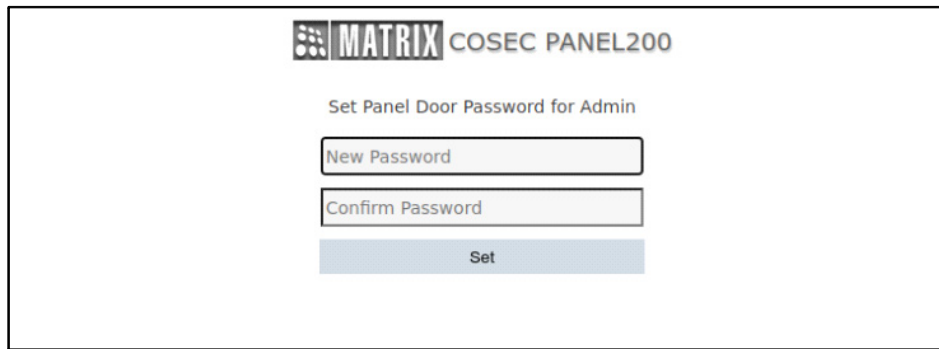
.....

Login

- Click **Login**.



- The **Set Panel Door Password for Admin** page appears.



- Configure the desired password in **New Password** and re-enter the same in **Confirm Password**. Only numeric values are allowed.
- Click **Set**. The **Quick Setup** pop-up appears. If you wish, you can configure the basic parameters using this Quick Setup.

**OR**

- You can **Quit** the Quick Setup and Selectively configure the parameters, by clicking the links in the left pane.

If you wish to configure the parameters at a later stage from the Wizard you can do so, Click the **Setup Wizard**  from the top right corner.

If you wish to configure the basic parameters using the Quick Setup, refer to [“Quick Setup Wizard”](#).

If you wish to selectively configure the parameters, click the desired link from the left pane.

You may use the Wizard or selectively configure the parameters, whichever works best for you.



*The [“Quick Setup Wizard”](#) is applicable only to the Standalone Mode. If you have configured the parameters using the wizard initially, the same configurations will be reflected in the respective pages when clicked from the left pane.*

*If you configure the parameters by clicking the desired links from the left pane and then click the **Setup***

**Wizard**  *the same configurations will be reflected in the respective tabs in the wizard. Now, if you make any changes again from the wizard, then these changes in configurations will be over-written in the respective pages when clicked from the left pane. Hence, we recommend you to use the Setup Wizard first to configure the basic parameters and then continue with selective configuration.*

*For COSEC-Server Mode and Third Party-Serve Mode, only selective configuration is applicable.*



---

Quick Setup Wizard is an easy and time saving configuration process for PANEL200, which enables you to configure basic parameters — Date & Time, Network Parameters, Scan Devices and Status of the Devices — step by step very quickly.

When you log into the PANEL200 in the Standalone Mode for the first time, the **Quick Setup** Wizard pop-up appears automatically.

You can navigate through the wizard to configure the basic parameters or quit the wizard. However, if you wish to configure the parameters at a later stage from the wizard, you can do so. Click the **Setup Wizard**  from the top right corner.



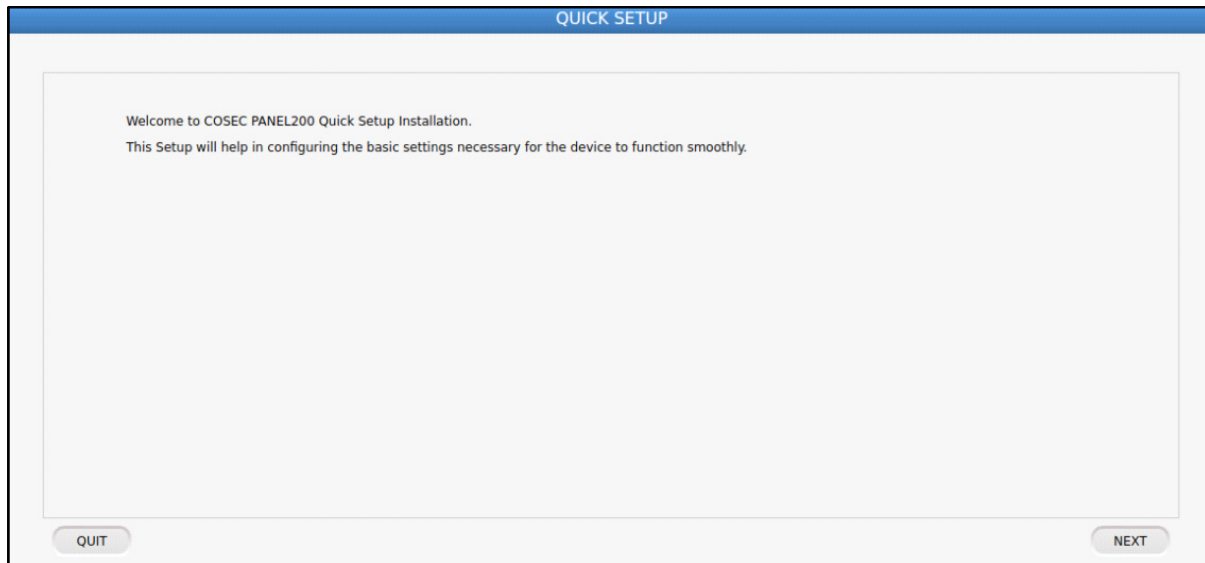
*The parameters configured from the Quick Setup Wizard can also be configured from the respective links in the left pane.*

*The Quick Setup Wizard is applicable only to the Standalone Mode. If you have configured the parameters using the wizard initially, the same configurations will be reflected in the respective pages when clicked from the left pane.*

*If you configure the parameters by clicking the desired links from the left pane and then click the **Setup***

**Wizard**  *the same configurations will be reflected in the respective tabs in the wizard. Now, if you make any changes again from the wizard, then these changes in configurations will be over-written in the respective pages when clicked from the left pane. Hence, we recommend you to use the Setup Wizard first to configure the basic parameters and then continue with selective configuration.*

When the Quick Setup Wizard pop-up appears automatically or you click **Setup Wizard**  , the Welcome page appears.



Get familiar with the functions of the following buttons of the Wizard before you begin to use them.

- **Next:** Takes you to the next page, saving the changes you made on the current page.
- **Back:** Returns you to the previous page.
- **Quit:** Enables you to exit the Wizard at any stage, saving changes you made before exiting.
- **Done:** Once all the configurations are completed, all the changes are saved and you can exit the wizard.

You can configure the following from the Wizard:

- "Date and Time"
- "Network"
- "Scan Devices"
- "Status"

## Date and Time

Configure the Date and Time parameters,

The screenshot shows the 'Date and Time' configuration window in the QUICK SETUP interface. The window has a blue header with 'QUICK SETUP' and four tabs: '1.Date and Time', '2.Network', '3.Scan Devices', and '4.Status'. The 'Date and Time' tab is active. The main area displays the current date and time: '01, August 2025 13:17:57'. Below this, there are several configuration options: 'Time Zone' (a dropdown menu showing '(GMT+05:30) Chennai, Kolkata, New Delhi, Mumbai'), 'Time Format' (a dropdown menu showing '24 hours'), 'Date' (a text field showing '01-08-2025' with a calendar icon), and 'Time' (a digital clock showing '13:17:42' with a reset icon). There are two checkboxes: 'Auto synchronize with NTP' (unchecked) and 'Daylight Saving Time' (unchecked). Below these, there is a 'Preferred NTP Server' text field containing 'time.windows.com'. At the bottom, there are four groups of settings: 'Forward Clock' (Month: January, Week: First, Day: Sunday, Time: 00:00), 'Reverse Clock' (Month: January, Week: First, Day: Sunday, Time: 00:00), and 'Duration' (00:00). At the very bottom, there are three buttons: 'QUIT', 'BACK', and 'NEXT'.

## Date and Time

- **Time Zone:** Select the time zone as per your region from the drop-down list.
- **Time Format:** Select a desired time format from the drop-down list — 12 hour, 24 hour.
- **Date & Time:** By default, the current Date and Time will be set automatically. You can change the same if required. To set the date, click the calendar and select the desired date. You can set the time in HH:MM:SS format. Click the desired box and use the up/down arrows to set the time.
- Click **Set Date and Time**  to save the changes.

## Auto Synchronize with NTP

If you want the Date and Time to automatically synchronize with the Preferred NTP Server (predefined or user-defined NTP Server Address), configure the following:

- **Auto Synchronize With NTP:** Select the check box to enable.
- **Preferred NTP Server:** Configure the Preferred NTP Server of your choice. Here, you can configure any one of the pre-defined NTP Servers or any other Server of your choice. The PANEL200 will first try to fetch the Date and Time from this configured Server Address. If it does not get the Date and Time in three tries; PANEL200 will check from the pre-defined NTP Servers. If you have entered one of the three pre-defined NTP Servers (ntp1.cs.wisc.edu, time.windows.com, time.nist.gov); then PANEL200 will first check that Server. If it receives the updates then, updated Date and Time will be reflected on door webpage and display screen. Valid Values: a-z A-Z 0-9 - . (dot).

If you do keep Preferred NTP Server blank, PANEL200 will check for Date and Time from the pre-defined NTP Server.

If you have manually entered the Date and Time, then these values will be reflected on the door webpage and display screen.

## Daylight Saving Time (DST)

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. The PANEL200 can be configured to be compatible with this procedure keeping the RTC of the PANEL200 updated with such changes.

Configure the following:

- **Daylight Saving Time:** Select the check box to enable.
- **Forward:** Select the desired month, week and day from the drop-down list and configure the desired time (HH:MM format) at which the clock is to be forwarded to increase the daylight time. For example, the clock is forwarded on the first Sunday of October at 6 am.
- **Reverse Clock:** Select the desired month, week and day from the drop-down list and configure the desired time (HH:MM format) at which the clock is to be reversed to normalize the time. For example, the clock is reversed on the first Sunday of January at 5 am
- **Duration:** Configure the time **Duration** (HH:MM format), by which the clock is to be forwarded or reversed. For example, the clock is forwarded and reversed by 1 hour. Now considering the day and time set in the above examples, the clock will be forwarded to 7 am and reversed to 4 am on the specified days.

## Network

Configure the following parameters:

The screenshot shows the 'QUICK SETUP' window with four tabs: '1.Date and Time', '2.Network', '3.Scan Devices', and '4.Status'. The '2.Network' tab is active. Below the tab bar, the 'Network' section contains the following fields:

|                 |                   |
|-----------------|-------------------|
| Panel Name      | Panel 127 RS-485  |
| IP Address      | 191.168.11.127    |
| MAC Address     | 00:1b:09:0f:1a:a1 |
| Subnet Mask     | 255.255.254.0     |
| Default Gateway | 191.168.11.1      |
| Preferred DNS   |                   |
| Alternate DNS   |                   |

At the bottom of the window, there are three buttons: 'QUIT' on the left, and 'BACK' and 'NEXT' on the right.

- **Panel Name:** Configure a name you wish to assign to the PANEL200.
- **IP Address:** This displays the default IP Address assigned to the PANEL200. You can change the same if required according to your network scenario.
- **MAC Address:** Displays the MAC Address of the PANEL200.

- **Subnet Mask:** This displays the default Subnet Mask assigned to the PANEL200. You can change the same if required according to your network scenario.
- **Default Gateway:** Configure the desired Default Gateway according to your network scenario.
- **Preferred DNS:** Configure the desired Preferred DNS, if required.
- **Alternate DNS:** Configure the desired Alternate DNS, if required.

## Scan Devices

Under the **Add Device to PANEL200** grid, the doors which are connected in the same network as the PANEL200, will be scanned automatically and displayed with their details — Door Type, Door Name, IP Address and MAC Address.

- Click the **Add Device** check box of the desired doors that you wish to add to the PANEL200.

| Sr.No. | Door Type    | Door Name        | IP Address      | MAC Address  | Add Device                          |
|--------|--------------|------------------|-----------------|--------------|-------------------------------------|
| 1      | PATH V2 DOOR | PATH V2 DOOR - 1 | 192.168.104.107 | 001b09070112 | <input checked="" type="checkbox"/> |
| 2      | VEGA DOOR    | VEGA DOOR - 2    | 192.168.104.85  | 001b090740cd | <input checked="" type="checkbox"/> |
| 3      | V3 DOOR      | V3 DOOR - 3      | 192.168.104.7   | 001b09053fe2 | <input type="checkbox"/>            |

- You can edit the **Door Name**, if required.
- Click **Scan Doors**  to check for new doors in the network.



*The grid displays a maximum of 255 doors.*

*The doors which are already added to the PANEL200 will not be displayed in the list.*

## Status

The status of the Doors you added is displayed here with their details — Door Type, Door Name, IP Address and MAC Address.

The screenshot shows the 'QUICK SETUP' window with the '4.Status' tab selected. It displays a table of door statuses with columns: Sr.No., Door Type, Door Name, IP Address, MAC Address, and Status. There are three rows of data. The first two rows have red dots in the Status column, indicating they are offline. The third row has a green dot, indicating it is online. Below the table are 'BACK' and 'DONE' buttons.

| Sr.No. | Door Type    | Door Name        | IP Address      | MAC Address  | Status  |
|--------|--------------|------------------|-----------------|--------------|---------|
| 1      | PATH V2 DOOR | PATH V2 DOOR - 1 | 192.168.104.107 | 001b09070112 | Offline |
| 2      | VEGA DOOR    | VEGA DOOR - 2    | 192.168.104.85  | 001b090740cd | Offline |
| 3      | V3 DOOR      | V3 DOOR - 1      | 192.168.104.7   | 001b09053fe2 | Online  |

Under **Status**, a Green dot denotes that the door is online and a Red dot denotes that the door is offline.

You can also filter the records according to — Door Type, Status, Door Group. As per set filter the records will be displayed.

Click **Done** and click **Close** to exit the Wizard.

After configuring the parameters from the Quick Setup Wizard, for advanced configuration you can move ahead with selective configuration, by clicking the desired link from the left pane under Configuration.

The screenshot shows the 'Configuration' window with the 'Basic Profile' tab selected. The left pane contains a list of configuration links. The main area shows settings for 'Panel123', including SD Card Status, Template Per Finger, Max. No. of Fingers Per User, Max. No. of Palms Per User, Max. No. of Faces Per User, Run PVR Door in Guide Mode, Auto Clear Alarm, Alarm Clear Timer, Override IO Linking and Time Triggered during Disarm, and Face Validation Device. There are 'Save' and 'Cancel' buttons at the bottom.

Panel Name: Panel123  
SD Card Status: Normal  
Template Per Finger: Single Template/Finger  
Max. No. of Fingers Per User: Two  
Max. No. of Palms Per User: Ten  
Max. No. of Faces Per User: Ten  
Run PVR Door in Guide Mode: ☐  
Auto Clear Alarm: ☐  
Alarm Clear Timer: 10 sec (10-65535)  
Override IO Linking and Time Triggered during Disarm: ☐  
Face Validation Device: S

Links in the Left Pane



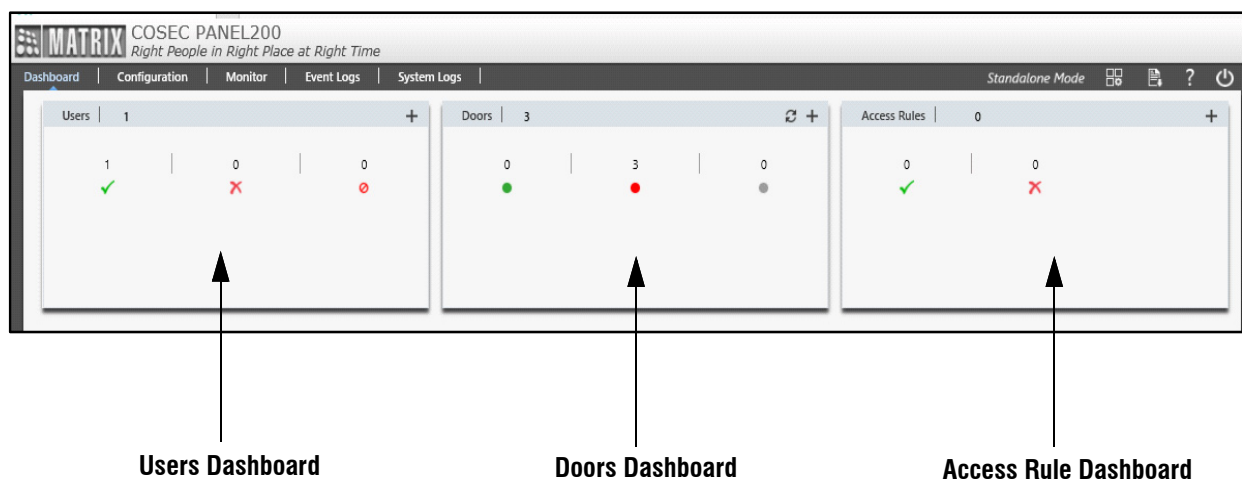
Dashboard enables you to Add/ Edit/ View— Users, Doors and Access Rules — easily and quickly by configuring their basic information.

To know more about the configurations of the User on Dashboard, refer [“Users Dashboard”](#).

To know more about the configurations of the Door on Dashboard, refer [“Doors Dashboard”](#).

To know more about the configurations of the Access Rules on Dashboard, refer [“Access Rules Dashboard”](#).

Dashboard displays the major configuration modules of the PANEL200 like **Users**, **Doors** and **Access Rules**.

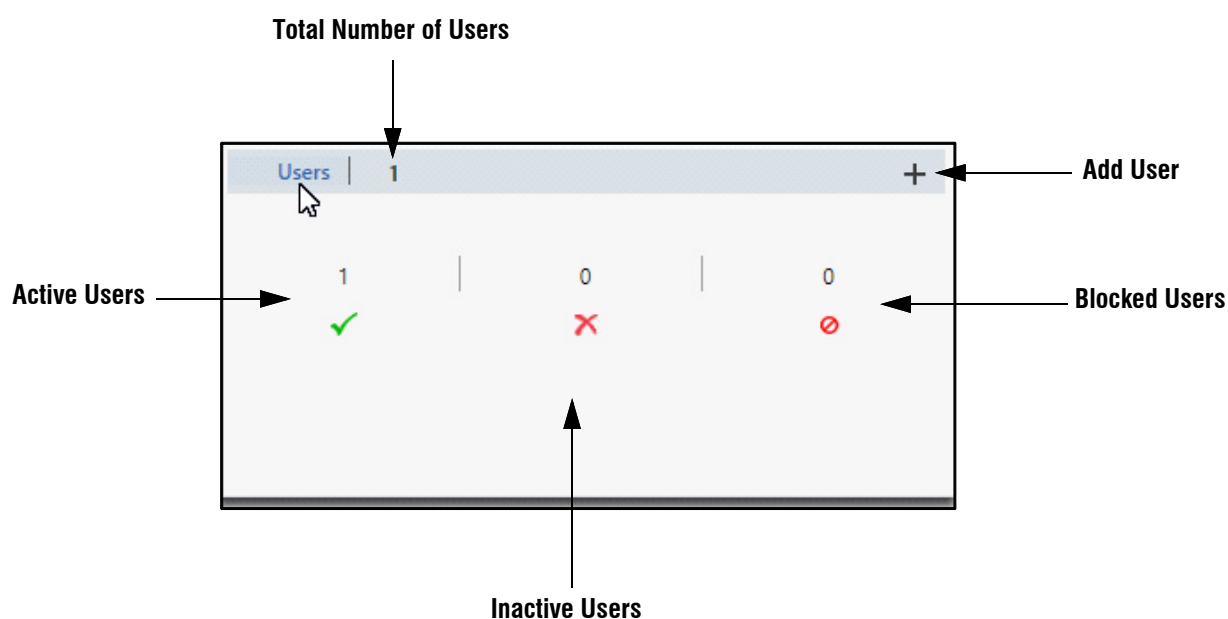


## Users Dashboard

Using the Users Dashboard, you can create a new user easily and quickly by configuring few basic user details.

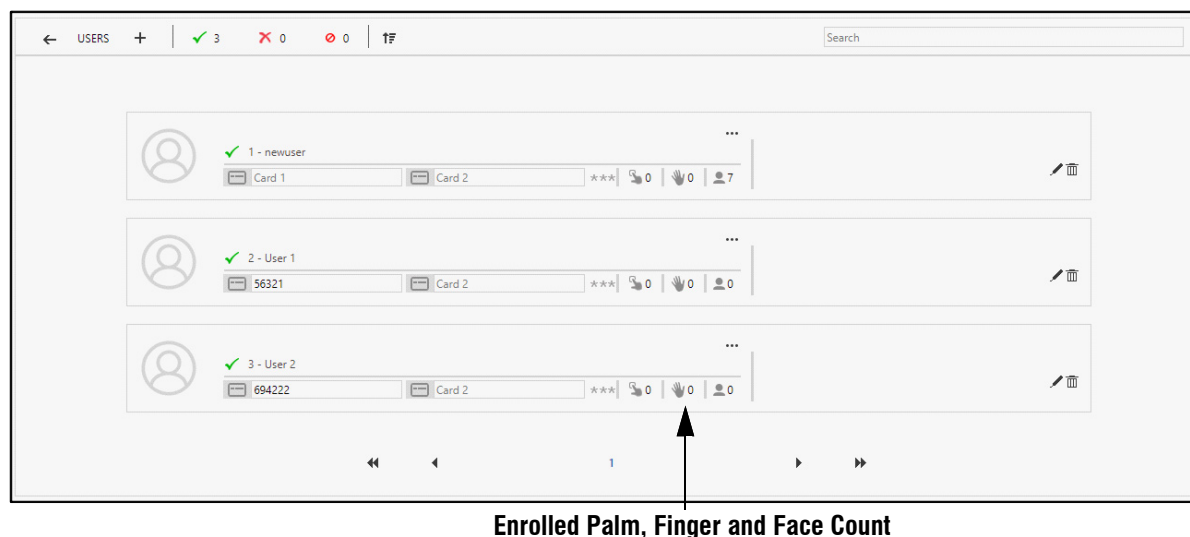
The Users Dashboard enables you to view the basic information of a user as well as add, edit and delete a user.

The details displayed on the dashboard are — Total Number of Users, Active Users , Inactive Users  and Blocked Users .



To add a new User, click **Add User**  on the Dashboard. For more details, refer to [“Adding Users”](#).

To view the list of users and their basic details, click **Users**. The details of the existing users appear in a list.



The details displayed are — State of the User, User ID, User Name, Access Card Number, PIN, Enrolled Credentials and assigned Access Rules.



The count of face images in **Face Credentials** will be updated whenever:

- face images are deleted from Users > User Configuration > Face Images (Updated At).
- face images are updated/deleted from Users > User Configuration > Face Recognition.
- face images are updated from Enrollment > User.
- face images are updated from Panel Configuration > Advanced Profile > Enrollment.

## Adding Users

You can also add a new user from this page. To do so,

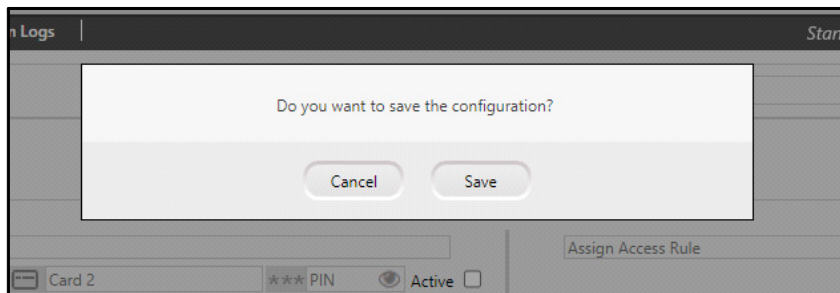
Click **Add User** .

Now, configure the basic details of the user — User ID, User Name, Access Card number, PIN number, Assign Access Rule. Now select the Active check box to enable the user.

## Assign Access Rule

Click on **Assign Access Rule** text box and a drop-down with a list of Access Rules appears (this appears only if the Access Rules are pre-configured). Select the check boxes for the desired Access Rules.

If the Access Rules are not pre-configured, you need to create Access Rules first. Click **Add Access Rule** . The following pop-up appears.

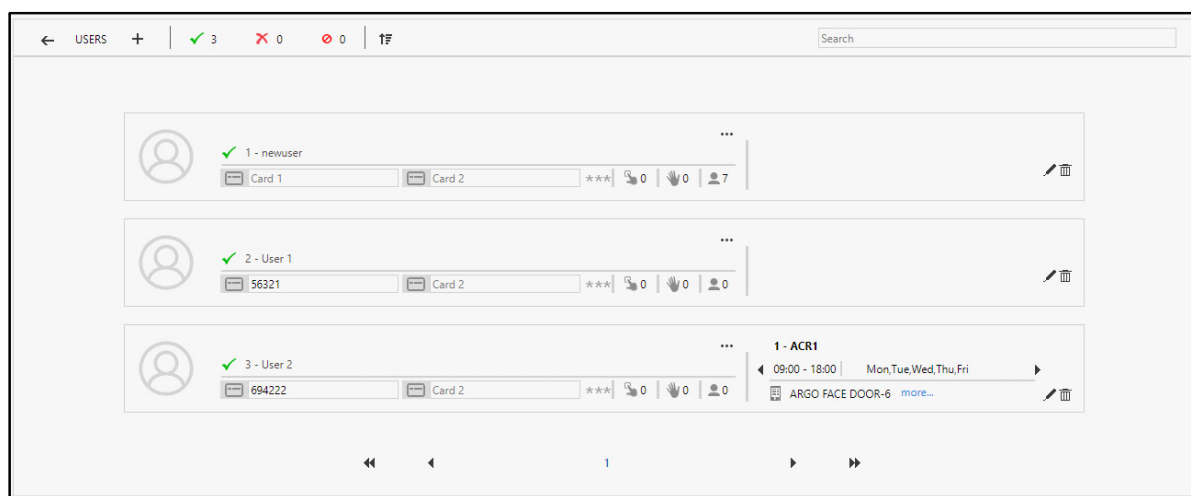


Click **Save** to save the configurations. The **Access Rules** page appears.



Now configure the Access Rule as per your requirement. For details, refer to [“Access Rules Dashboard”](#). After configuring the Access Rule, assign this Rule to the desired user.

Click **OK** to save the configured details of the user or click **Cancel** to discard the changes.



Once you have saved the configurations, you can edit or delete the user.

Click **Edit** to edit the user details.

Click **Delete** to delete the desired user.

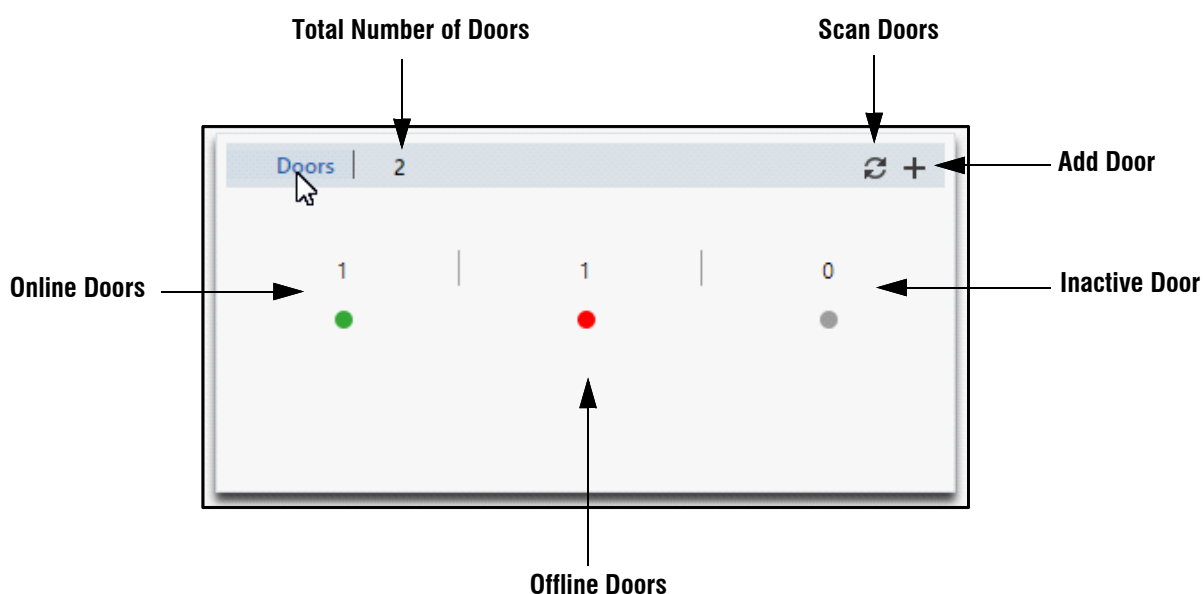
For detailed configuration of a user, refer to [“User Configuration”](#).

## Doors Dashboard

Using the Doors Dashboard, you can add a new Door easily and quickly by configuring few basic door details.

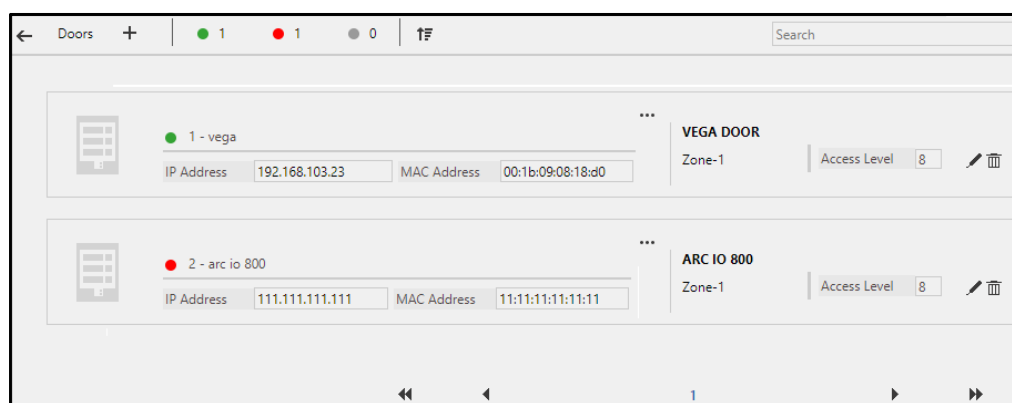
The Doors Dashboard enables you to view the basic details of the door as well as add, edit and delete a door.

The details displayed on the dashboard are— Total Number of Doors, Online Doors ●, Inactive Doors ● and Offline Doors ●.



To add a new Door, click **Add Door** + on the Dashboard. For more details, refer to [“Adding Doors”](#).

To view the list of doors and their basic details, click **Doors**. The details of the existing doors appear in a list.

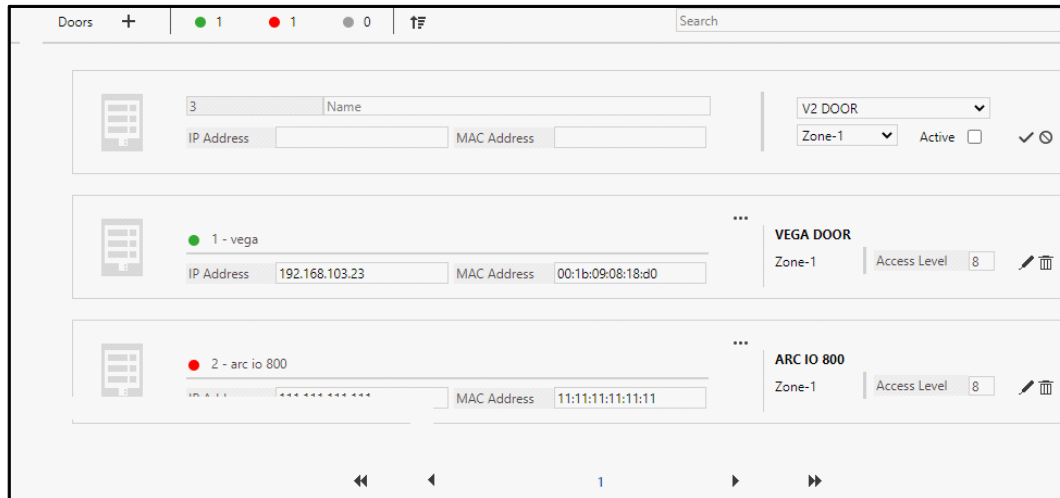


The details displayed are — State of the Door, Door ID, Door Name, IP Address, MAC Address, Door Type, Zone and Access Level.

## Adding Doors

You can also add a new door from this page. To do so,

Click **Add Door**  .



Now configure the basic details of a door — Door Name, IP Address, MAC Address, Door Type and Zone. Now select the Active check box to enable the door.

Click **OK**  to save the configured details of the door or click **Cancel**  to discard the changes.

Once you have saved the configurations, you can edit or delete the door.

Click **Edit**  to edit the door details.

Click **Delete**  to delete the desired door.

## Scan Doors

Click **Scan Doors**  on the Door Dashboard to scan the available doors which are connected to the same network as the PANEL200. The available doors appear in a list.

| Door                           | Type         | IP Address      | MAC Address       | Assign Zone |   |
|--------------------------------|--------------|-----------------|-------------------|-------------|---|
| ARC DC 200-00:1b:09:07:9a:74   | ARC DC 200   | 192.168.103.234 | 00:1b:09:07:9a:74 | Zone-1      | ✓ |
| VEGA DOOR-00:1b:09:05:96:1a    | VEGA DOOR    | 192.168.103.233 | 00:1b:09:05:96:1a | Zone-1      | ✓ |
| VEGA DOOR-00:1b:09:08:63:a5    | VEGA DOOR    | 192.168.103.14  | 00:1b:09:08:63:a5 | Zone-1      | ✓ |
| ARC DC 200-00:1b:09:07:65:25   | ARC DC 200   | 192.168.103.9   | 00:1b:09:07:65:25 | Zone-1      | ✓ |
| ARGO DOOR-00:1b:09:08:1c:99    | ARGO DOOR    | 192.168.103.122 | 00:1b:09:08:1c:99 | Zone-1      | ✓ |
| VEGA DOOR-00:1b:09:08:19:09    | VEGA DOOR    | 192.168.103.206 | 00:1b:09:08:19:09 | Zone-1      | ✓ |
| PATH V2 DOOR-00:1b:09:07:a6:7a | PATH V2 DOOR | 192.168.103.11  | 00:1b:09:07:a6:7a | Zone-1      | ✓ |
| ARGO DOOR-00:1b:09:07:87:55    | ARGO DOOR    | 192.168.103.238 | 00:1b:09:07:87:55 | Zone-1      | ✓ |
| ARC DC 200-00:1b:09:07:9a:6e   | ARC DC 200   | 192.168.103.70  | 00:1b:09:07:9a:6e | Zone-1      | ✓ |
| ARC DC 200-00:1b:09:07:ca:93   | ARC DC 200   | 192.168.103.124 | 00:1b:09:07:ca:93 | Zone-1      | ✓ |
| ARGO DOOR-00:1b:09:06:10:0a    | ARGO DOOR    | 192.168.103.208 | 00:1b:09:06:10:0a | Zone-1      | ✓ |

Click **Select** ✓ to select the desired door/s to add them to the PANEL200. You can add only five doors at a time.

If the number of available doors in the list are less than or equal to five, click **Select All** to add all the doors to the PANEL200.



The error message— “Maximum 5 doors are allowed to select” will appear if you select more than five doors to be added at a time.

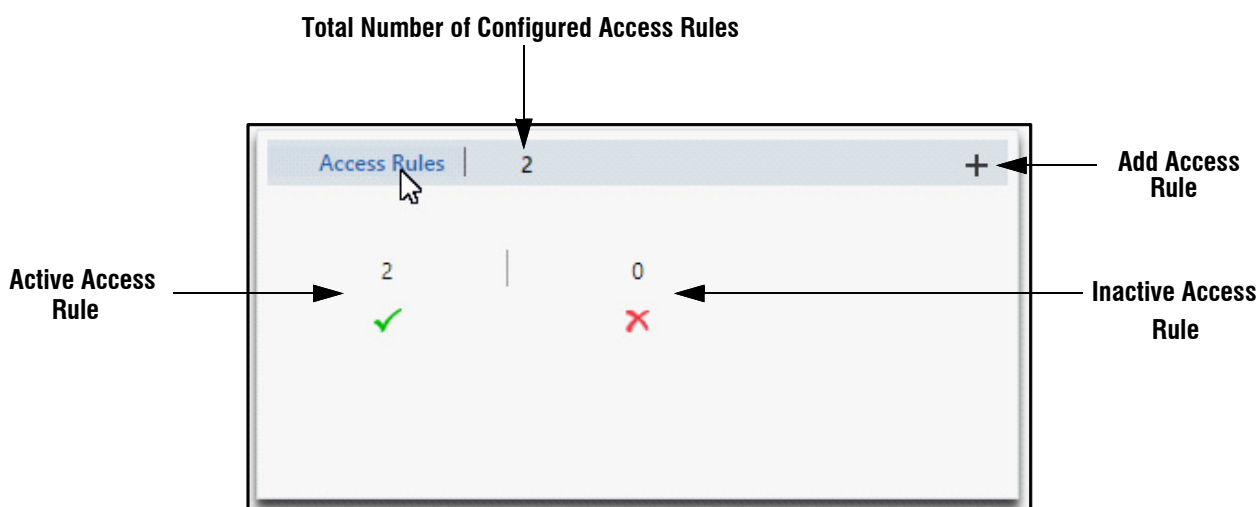
Click **Done** to save the settings.

For detailed configuration of a door, refer to “Door Configuration”.

## Access Rules Dashboard

The Access Rule Dashboard enables you to view the Access Rules as well as add, edit and delete an Access Rule.

This details displayed on the dashboard are — Total number of Configured Access Rules, Active Rules ✓ and Inactive rules ✗.



To add a new Door, click **Add Access Rule**  on the Dashboard. For more details, refer to [“Adding Access Rules”](#).

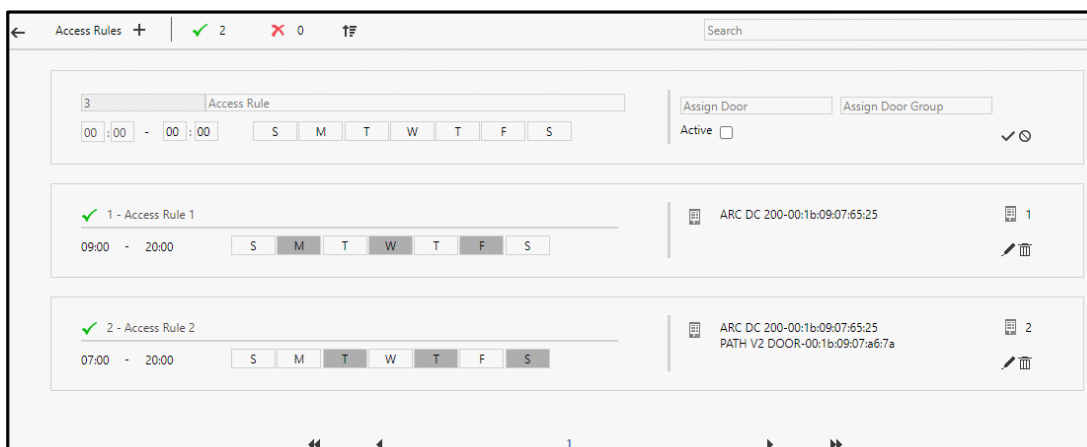
To view the list of Access Rules, click **Access Rules**. It displays the details of the existing Rules.



## Adding Access Rules

You can also add a new access rule from this page. To do so,

Click **Add Access Rule** .



Now, configure the basic details to create a new Access Rule — Access Rule ID, Applicable Access Rule Time and Days, Assign Door/Door Group. Now select the Active check box to enable the Access Rule.

Click **OK**  to save the configured details of the Access Rule or click **Cancel**  to discard the changes.

Once you have saved the configurations, you can edit or delete the Access Rules.

Click **Edit**  to edit the Access Rule details.

Click **Delete**  to delete the desired Access Rule.

For detailed configuration of an Access Rule, refer to [“Access Rule”](#).



---

Panel Configuration allows you to:

- configure the basic profile parameters. For details, refer to [“Basic Profile”](#).
- configure the advanced profile parameters. For details, refer to [“Advanced Profile”](#).
- configure the access profile parameters. For details, refer to [“Access Features”](#).
- configure the special function parameters. For details, refer to [“Special Functions”](#).
- configure the input output parameters. For details, refer to [“Input Output”](#).
- configure the zone configuration parameters. For details, refer to [“Zone Configuration”](#).
- configure the man trap door group parameters. For details, refer to [“Man Trap Door Group”](#).
- configure the network setting parameters. For details, refer to [“Network Settings”](#),
- configure the date and time parameters. For details, refer to [“Date and Time”](#).

### **Third Party - Server Mode**

Along with the above Panel Configurations you can also configure the following:

- configure the server settings parameters. For details, refer to [“Server Settings”](#).

### **COSEC-Server Mode**

You can configure the following:

- configure the basic profile parameters. You can configure the following only — [“Panel Mode”](#) in [“Basic Profile”](#).
- configure the network setting parameters. You can configure the following only — [“LAN Settings”](#), [“Advanced LAN Settings”](#), [“Wi-Fi Network Settings”](#), [“Wi-Fi Access Point Settings”](#), [“Mobile Broadband”](#) in [“Network Settings”](#).
- configure the date and time parameters. For details, refer to [“Date and Time”](#).
- configure the server settings parameters. For details, refer to [“Server Settings”](#)
- configure the CCC settings parameters. For details, refer to [“CCC Settings”](#).

# Basic Profile

The Basic Profile allows you to:

- configure the general settings. For details, refer to [“General”](#).
- configure the access settings. For details, refer to [“Access Settings”](#).
- configure the multi-language settings. For details, refer to [“Multi-Language”](#).
- configure the display settings. For details, refer to [“Display”](#).
- change the panel mode and configure encryption settings. For details, refer to [“Panel Mode”](#).

## General

To configure the General parameters,

Click **Panel Configuration > Basic Profile > General**. The **General** page appears.

The screenshot shows the 'Basic Profile' configuration window with the 'General' tab selected. The settings are as follows:

| Parameter                                            | Value                    |
|------------------------------------------------------|--------------------------|
| Panel Name                                           | Panel200                 |
| SD Card Status                                       | Normal                   |
| Template Per Finger                                  | Single Template/Finger   |
| Max. No. of Fingers Per User                         | Two                      |
| Max. No. of Palms Per User                           | Ten                      |
| Max. No. of Faces Per User                           | Ten                      |
| Run PVR Door in Guide Mode                           | <input type="checkbox"/> |
| Auto Clear Alarm                                     | <input type="checkbox"/> |
| Alarm Clear Timer                                    | 10 sec(10-65535)         |
| Override IO Linking and Time Triggered during Disarm | <input type="checkbox"/> |
| Face Validation Device                               | S                        |

Buttons: Save, Cancel

Configure the following parameters:

- **Panel Name:** Configure a suitable name for the PANEL200.
- **SD Card Status:** This displays whether the SD Card is connected or not.

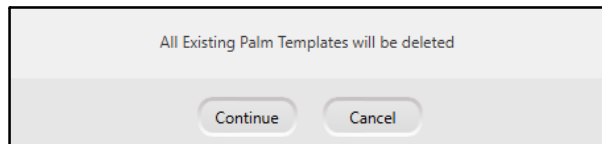


*Do not remove the SD Card for proper functioning of the PANEL200.*

- **Template Per Finger:** Select the number of templates to be saved per finger credential enrolled for the user from the drop-down list.
- **Max. No. of Fingers Per User:** Select the maximum number of fingers per user to be allowed for enrollment from the drop-down list.
- **Max. No. of Palms Per User:** Select the maximum number of palms per user to be allowed for enrollment from the drop-down list.

- **Max. No. of Faces Per User:** Select the maximum number of faces per user to be allowed for enrollment from the drop-down list.
- **Run PVR Door in Guide Mode:** PVR (Palm Vein Reader) doors can be used with or without hand guides, depending on which, the enrollment and identification of palm credentials vary. Hence, PVR can run in two modes, the Guide Mode and the Non-Guide Mode (default mode). Palm templates are saved and identified by the door differently, depending on the mode selected.

Select the check box to enable. The following pop-up appears.



Click **Continue** to confirm or click **Cancel** to discard. If you click **Continue**, all the existing Palm templates will be deleted and all future palm enrollment and identification will be performed in the Guide Mode only.

- **Auto Clear Alarm:** Select the check box to clear the alarms automatically on expiry of the **Alarm Clear Timer**.
- **Alarm Clear Timer:** Configure the time in seconds after which the alarms on PANEL200 should be cleared automatically.
- **Override IO Linking and Time Triggered during Disarm:** Select the check box to enable overriding of IO Linking/Time Triggered configurations for a door when the Disarm Special Function is enabled.
- **Face Validation Device:** Click the **Select Door** picklist. The **Panel Doors** pop-up appears. Select the desired door. The face images uploaded manually will be validated using the selected door.

**OR**

You can also search for the desired door. To do so, enter the keyword in the Search box. Click **Search**

 . The doors will be filtered as per the keyword. Select the desired door.

The selected doors ID and Name appear.

The selected door will appear under [“Face Recognition”](#) in [“User Configuration”](#).

Click **Save** to save the settings or click **Cancel** to discard.

## Access Settings

To configure the Access Settings parameters,

Click **Panel Configuration > Basic Profile > Access Settings**. The **Access Settings** page appears.

**Basic Profile**

General | **Access Settings** | Multi-Language | Display | Panel Mode

Working Days ☒ Sun ☒ Mon ☒ Tue ☒ Wed  
☒ Thu ☒ Fri ☒ Sat ☒ Holiday

Working Hours(HH:MM) 00 : 00 To 23 : 59

Break Hours(HH:MM) 13 : 00 To 14 : 00

Allowed Early-IN(HH:MM) 00 : 10

Allowed Late-OUT(HH:MM) 00 : 10

Save Cancel

Configure the following parameters:

- **Working Days:** By default, all the check boxes are selected. Clear the check boxes of the days which you do not wish to include in Working Days. The access on doors will be allowed only for those days whose check boxes are enabled.
- **Working Hours (HH:MM):** Configure the time to be set as the working hours in HH:MM format.
- **Break Hours (HH:MM):** Configure the time to be set as break hours in HH:MM format.
- **Allowed Early-IN (HH:MM):** Configure the duration (HH:MM format) before the official entry time during which a user is permitted to enter the office. For example: If 10 minutes is allowed as Early-IN; then user can enter 10 minutes before the shift start time.
- **Allowed Late-OUT (HH:MM):** Configure the duration (HH:MM format) after the official exit time during which a user is permitted to leave the office. For example, if the Allowed Late-OUT is set as 00:10 (10 minutes) and the official shift end time is 06:00 PM, the user will be allowed to exit any time, upto 06:10 PM.

Click **Save** to save the settings or click **Cancel** to discard.

## Multi-Language

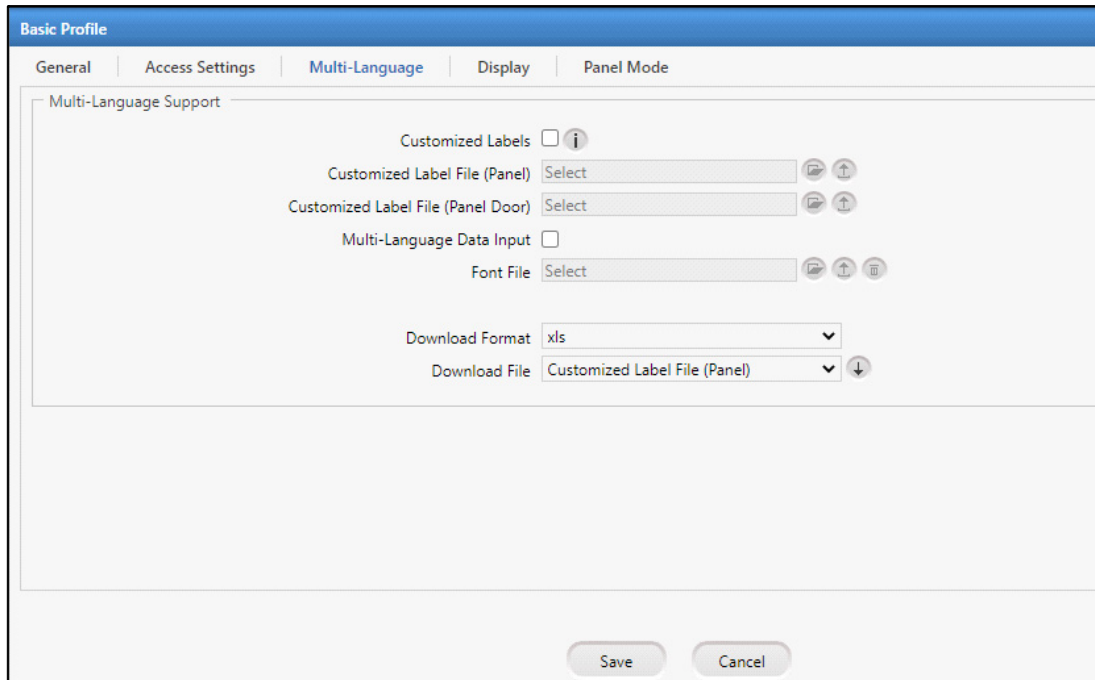
The Multi-Language page allows you to download the sample file and upload the translated file for both PANEL200 and its doors. When you upload the translated file for doors, all the doors connected to the PANEL200 will be updated with the uploaded language automatically. You can also enable multi-language input on PANEL200 and send Fonts to the connected doors for multi-language input.



*For Dot -matrix doors (PVR, Door V4, Door V3, Wireless Door), Multi-language is supported for English.*

To configure the Multi-Language parameters,

Click **Panel Configuration > Basic Profile > Multi-Language**. The **Multi-Language** page appears.



To enable Multi-Language, you need to first [“Download the Sample File”](#) and then [“Upload the Translated File”](#).

## Download the Sample File

- **Download Format:** Select the desired format in which you wish to download the sample file from the drop-down list.
- **Download File:** Select the desired sample file — Sample File (Panel), Sample File (Panel Door) — which you wish to download from the drop-down list. When you upload a translated file, you can also download the same — Customized Label File (Panel), Customized Label File (Panel Door) — later for your reference.

## Upload the Translated File

- **Customized Labels:** Select the check box to enable uploading the Customized Label File, that is, translated file.
- **Customized Label File (Panel):** Click **Browse**  and select the desired file to be uploaded. Click **Upload**  to upload the file.
- **Customized Label File (Panel Door):** Click **Browse**  and select the desired file to be uploaded. Click **Upload**  to upload the file.
- **Multi-language Data Input:** Select the check box if you wish to enable the multi-language data input in PANEL200.

- **Font File:** The Font File is used to send fonts to the connected doors when multi-language is to be used.

Click **Browse**  and select the desired file to be uploaded. Click **Upload**  to upload the file.

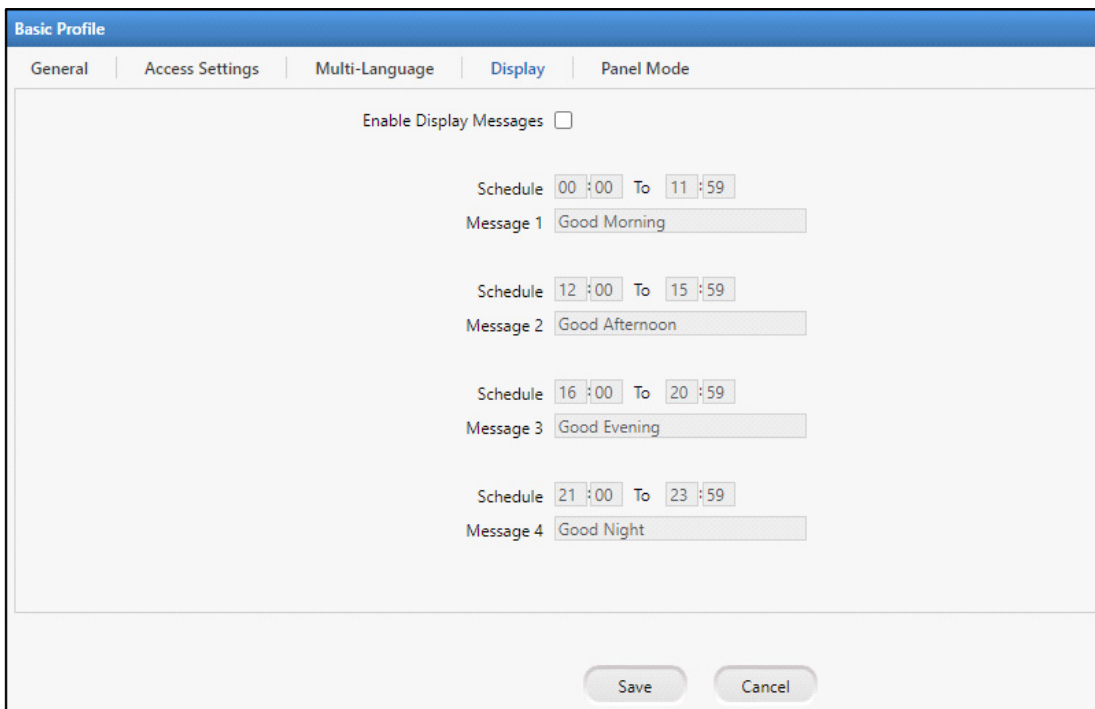
If you wish to delete the file, click **Delete** .

Click **Save** to save the settings or click **Cancel** to discard.

## Display

To configure the Display parameters,

Click **Panel Configuration > Basic Profile > Display**. The **Display** page appears.



**Basic Profile**

General | Access Settings | Multi-Language | **Display** | Panel Mode

Enable Display Messages ☐

Schedule 00 : 00 To 11 : 59  
Message 1 Good Morning

Schedule 12 : 00 To 15 : 59  
Message 2 Good Afternoon

Schedule 16 : 00 To 20 : 59  
Message 3 Good Evening

Schedule 21 : 00 To 23 : 59  
Message 4 Good Night

Save Cancel

Configure the following parameters:

- **Enable Display Messages:** Select the check box to display messages on the doors. You can configure 4 Display Messages.
- **Schedule:** Configure the time duration for which you wish each message should be displayed in HH:MM format.
- **Message 1- 4:** Configure the message to be displayed.

Click **Save** to save the settings or click **Cancel** to discard.

## Panel Mode

To configure the Panel Mode parameters,

Click **Panel Configuration > Basic Profile > Panel Mode**. The **Panel Mode** page appears.

The screenshot shows the 'Basic Profile' configuration window with the 'Panel Mode' tab selected. The 'Panel Mode' dropdown is set to 'Standalone Mode'. The 'Encryption' section contains the following settings: Authentication Type is 'Digest', Authentication Algorithm is 'MD5', Web Server Encryption is unchecked, HTTP Port is 80, HTTPS Port is 443, SSL Certificate is 'Certificate and Key File', Certificate File and Key File are both 'Choose a file', Allowed TLS Version is 'TLS 1.0 & Above', Panel Door Secured Communication is unchecked, and Request Retry Timer (min) is 2. There are 'Save' and 'Cancel' buttons at the bottom.

Configure the following parameters:

- **Panel Mode:** Select the desired mode — Server Mode, Standalone Mode, Third Party Mode. For details, refer to [“Standalone Mode”](#), [“COSEC-Server Mode”](#), [“Third Party-Server Mode”](#).



*The PANEL200 will reboot when the mode is changed and the configurations will have to be done again.*

## Encryption

- **Authentication Type:** Select the desired Authentication Type from the drop-down list options — Basic or Digest.



*It is advised to use Digest Authentication for enhanced security as Basic Authentication will increase network security risks.*

If **Authentication Type** is selected as **Basic**, the PANEL200 will serve HTTP/HTTPS APIs from any clients having Basic Authentication.

If **Authentication Type** is selected as **Digest**, the PANEL200 will serve HTTP/HTTPS APIs from any clients having Digest Authentication.

- **Authentication Algorithm:** If Authentication Type is selected as Digest, select the desired Authentication Algorithm from the drop-down list options — MD5 or SHA-256.
- **Encryption:** Select the desired Encryption mode by selecting the respective check box — **Web Server Encryption** and/ or **TCP Server Encryption** to establish secure HTTPS connection between client-server.

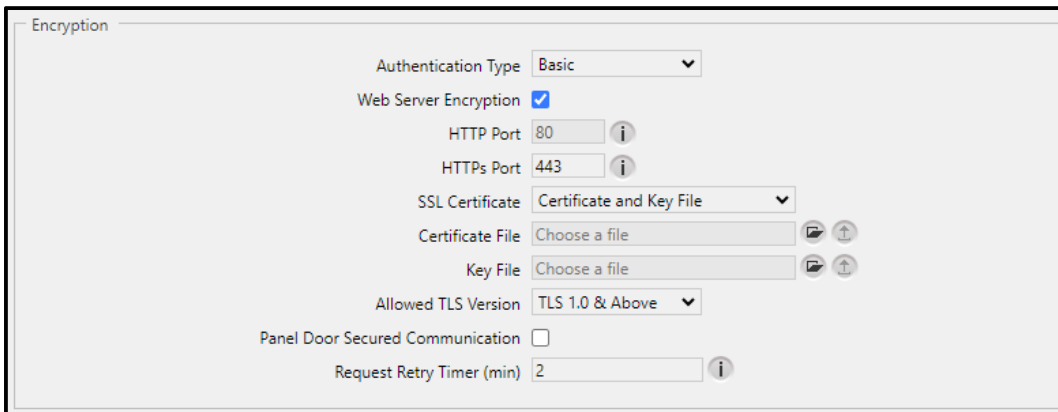


*TCP Server Encryption is applicable only for COSEC - Server Mode.*

- **Web Server Encryption:** Select the check box to establish secure HTTPS connection with Web Server to access PANEL webpages or API. This will secure the webpages of PANEL200.
- **TCP Server Encryption:** Applicable only for **COSEC - Server Mode**; select the check box to establish secure connection with COSEC Server, TCP Server and CCC Server.
- **HTTP Port:** Configure the HTTP Port. You can configure HTTP only when **Web Server Encryption** is disabled.
- **HTTPs Port:** Configure the HTTPs Port. You can configure when **Web Server Encryption** or **TCP Server Encryption** is enabled.

When **Web Server Encryption** or **TCP Server Encryption** check boxes are selected then only **SSL Certificate**, **Certificate File**, **Key File** and **Allowed TLS Version** will be configurable.

- **SSL Certificate:** Select the desired type of SSL Certificate from the drop-down list — Certificate and Key File or #PKCS12 Certificate File.
- If you select **Certificate and Key File** as **SSL Certificate** then only you can upload **Certificate File** and **Key file**.
  - Click **Browse**  to select the desired certificate. Click **Upload**  to upload the selected certificate. Supported Formats: .crt,.cer. Supported Format for Key File: .key.



The screenshot shows the 'Encryption' configuration window. It includes the following fields and controls:

- Authentication Type:** A dropdown menu set to 'Basic'.
- Web Server Encryption:** A checked checkbox.
- HTTP Port:** A text input field with the value '80' and an information icon.
- HTTPs Port:** A text input field with the value '443' and an information icon.
- SSL Certificate:** A dropdown menu set to 'Certificate and Key File'.
- Certificate File:** A text input field with the placeholder 'Choose a file' and a 'Browse' icon.
- Key File:** A text input field with the placeholder 'Choose a file' and a 'Browse' icon.
- Allowed TLS Version:** A dropdown menu set to 'TLS 1.0 & Above'.
- Panel Door Secured Communication:** An unchecked checkbox.
- Request Retry Timer (min):** A text input field with the value '2' and an information icon.

- If you select **#PKCS12 Certificate File** as **SSL Certificate** then you can upload **Certificate File** and enter the desired **Password**.
  - Click **Browse**  to select the desired certificate. Click **Upload**  to upload the selected certificate. Supported Formats: .p12, .pfx.



Encryption

Authentication Type Basic ▼

Web Server Encryption ☒

HTTP Port 80 ⓘ

HTTPs Port 443 ⓘ

SSL Certificate #PKCS12 Certificate File ▼

Certificate File Choose a file ⓘ

Password

Allowed TLS Version TLS 1.0 & Above ▼

Panel Door Secured Communication ☐

Request Retry Timer (min) 2 ⓘ

- **Allowed TLS Version:** Select the desired TLS Version from the drop-down list — TLS 1.0 & Above, TLS 1.1 & Above or TLS 1.2.
- **Panel Door Secured Communication:** Select the check box to establish secure communication between PANEL200 and all connected doors.
- **Request Retry Timer (min):** Configure the desired time period in minutes. This is the time after which the door should make a request to the PANEL200 for the face images.

Click **Save** to save the settings or click **Cancel** to discard.

# Advanced Profile

The Advanced Profile allows you to:

- configure the settings. For details, refer to [“Settings”](#).
- configure the alarms & timers settings. For details, refer to [“Alarms and Timers”](#).
- configure the enrollment settings. For details, refer to [“Enrollment”](#).
- configure the wiegand settings. For details, refer to [“Wiegand”](#).

## Settings

To configure the General parameters,

Click **Panel Configuration > Advanced Profile > Settings**. The **Settings** page appears.

**Advanced Profile**

Settings | Alarms and Timers | Enrollment | Wiegand

Generate Events ☒

Generate Exit Switch Events ☐

Generate Invalid User Events ☐

Degraded Access ☐

Degraded Wait Timer  sec(1-99)

Facility Code Check ☐

Facility Code  (1-65535)

Additional Security Code ☐

ASC Code  (1-65535)

Confirm ASC Code

Smart Identification ☐

Auto Acknowledge Alarm ☐

Alarm Auto Acknowledge Wait Timer  sec(10-65535)

Allow Door Access Through Mobile ☐

Mobile Entry Access Mode  ⓘ

Save Cancel

**Advanced Profile**

Settings | Alarms and Timers | Enrollment | Wiegand

Facility Code  (1-65535)

Additional Security Code ☐

ASC Code  (1-65535)

Confirm ASC Code

Smart Identification ☐

Auto Acknowledge Alarm ☐

Alarm Auto Acknowledge Wait Timer  sec(10-65535)

Allow Door Access Through Mobile ☐

Mobile Entry Access Mode  ⓘ

Mobile Exit Access Mode  ⓘ

API Security Key

PIN Change Code

Auto Add/Update Enrolled Face as Profile Photo ☒

Assign Doors to New Users

Assign Door

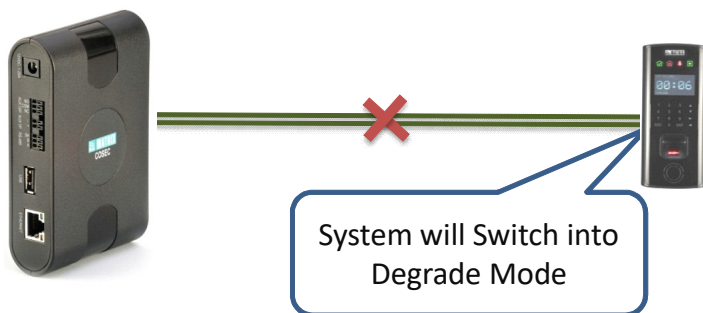
Configure the following parameters:

- **Generate Events:** The check box is selected by default, that is, all the events — User, Door, Alarm, System — are generated and stored in the Event Logs. Clear the check box if you do not wish to store the events.

If you clear the Generate Events check box the User Allowed, User Denied, Time Out etc events will still be displayed on the door display screen.

- **Generate Exit Switch Events:** Select the check box if you want the doors to generate events for the inputs from the Exit Switch. The Exit Switch events will be generated when the mode is either Exit or Both.
- **Generate Invalid User Events:** Select the check box if you want the doors to generate events for invalid user access.
- **Degraded Access:** Select the check box if you wish to allow valid user to access the facility even if the door is not communicating with the PANEL200.
- **Degraded Wait Timer (sec):** Configure duration in seconds, after the expiry (default:5seconds) of which the door switches to the Degraded Mode.

The PANEL200 continuously monitors the status of all configured doors through the pulses regularly transmitted from PANEL200 and ACK message received back from doors. Once the door detects PANEL200 as Offline, then the door will start the Degrade Wait Timer. If PANEL200 does not change its state to Online before expiry of this timer, then the door changes its mode to Degraded Mode.



To enable Degraded Mode for each Zone, refer to [“Zone Configuration”](#).

- **Facility Code Check:** Select the check box to enable the doors to check the Facility Code always for accessing via RFID Cards even if the doors are not in Degraded Mode.
- **Facility Code:** Facility Codes or Site Codes are encoded on cards, along with a card number, to ensure that cards belong to the facility where access is permitted. Facility Code is a unique 8 or 16 bits, of every HID Proximity card number specific to a site and is encoded into the card by the manufacturer.
  - User defined Facility Code (FC) can also be written onto the card at the time of enrollment while using Smart Cards and PANEL200 reads this code while allowing access on the door.
  - Configure a Facility Code (ranging from 1 to 65535) to be written onto the card. This Facility Code can be included in the [“Card Format”](#) which can then be assigned to the user. When user tries to access a facility, then FC will be verified to allow access to the door.

The top screenshot shows the 'Settings' tab with the following options:

- Generate Events ☒
- Generate Exit Switch Events ☐
- Generate Invalid User Events ☐
- Degraded Access ☐
- Degraded Wait Timer 5 sec (1-99)
- Facility Code Check ☐
- Facility Code 1 (1-65535)

The bottom screenshot shows the 'Card Format' tab with the following settings:

- ID 2
- Name Matrix Format
- Read Order Forward
- Truncate To 64 Bits (1-128)
- Configure 32 Bits (0-128)
- Sequence of Operation Reading Order then Bit Configuration
- Include FC in Card No. ☒

The 'Bit Configuration' section includes a table to define the card reading pattern:

| Bit           | 1                        | 2                        | 3                        | 4                        | 5                        | 6                        | 7                        | 8                        | 9                        | 10                       | 11                       | 12                       | 13                       | 14                       | 15                       | 16                       |
|---------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Even Parity   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Odd Parity    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Facility Code | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Card Number   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

- **Additional Security Code:** To take the security level a step higher, an Additional Security Code can also be added.
  - This Additional Security Code check is possible only with Smart Cards which will prevent duplicate cards and restrict unauthorized access to the facility.
  - Select the check box to enable this functionality at the Panel level and configure the **ASC code** (ranging from 1 to 65535). Re-enter the code to confirm.
  - This feature must also be enabled at the Zone level. For details, refer to [“Advance Configuration 3”](#) in [“Zone Configuration”](#). Now the user; who is assigned the zone enabled with ASC will be checked for ASC verification on the door.
- **Smart Identification:** Select the check box to enable Smart Card Identification of the user.
  - This enables user identification into another office by means of Smart Card, though S/he is not enrolled into that particular office's system. For example, Employee working in Mumbai branch of a office can be identified on the door of Delhi office using Smart Identification.
  - For this the Smart Identification feature must also be enabled from [“Advance Configuration 3”](#) in [“Zone Configuration”](#). Make sure you have enrolled the [“SI User”](#) with desired SI options.
- **Auto Acknowledge Alarm:** Select the check box to enable the auto-acknowledgment of all alarms. The Alarms can be enabled from [“Alarms and Timers”](#).
 

Set the duration in seconds for the **Alarm Auto Acknowledge Wait Timer (sec)**. Once the alarm is activated, this timer begins and on the expiry of this timer, the alarm buzzer will automatically stop.
- **Allow Door Access Through Mobile:** Select the check box to allow the access to the door using COSEC Mobile Applications — APTA, ACS.

- **Mobile Entry Access Mode:** Select the desired option — Mobile Only, Mobile then Biometrics, Mobile then Card and Mobile then PIN.

The option Mobile then PIN is applicable for ACS Application only.

- **Mobile Exit Access Mode:** Select the desired option — Mobile Only, Mobile then Biometrics, Mobile then Card and Mobile then PIN.

The option Mobile then PIN is applicable for ACS Application only.

- **API Security Key:** Configure the security key for the API.
- **PIN Change Code:** Configure the code for changing PIN of the user. This PIN is to be entered from the Wiegand input pin pad connected to the door. When entered, the doors mode changes to the pin change mode and you can enter the old and new password.
- **Auto Add/Update Enrolled Face as Profile Photo:** Select the check box to set the enrolled image of a user as the Profile Photo automatically on successful Face Enrollment.



*The PANEL200 will consider the enrolled face image located at index number 0 to set it as Profile Photo.*

- **Assign Doors to New User:** Select the desired option according to which you wish to assign doors to the new users from the drop-down list options — All Doors, Selected Doors, None.

If you select **All Doors**, then all the doors added to the PANEL will be assigned automatically to any newly created user. Any newly added doors will also be assigned to all the users.

If you select **None**, no doors will be assigned automatically to any newly created users. You need to manually assign the desired doors from User ["Profile"](#).

If you select **Selected Doors**, click the **Assign Door** picklist. The **Assign Door** pop-up appears. Click the **Door** or **Door Group** picklist and select the check boxes of the desired doors/door groups that you wish to assign to the newly created users. The selected doors/doors of the selected door groups appear in the grid.

If you wish to remove the doors, click **Delete**  of the respective door.

Click **Ok** to assign the doors. The number of selected doors appears against **Assign Door**.

If you do not select any doors/door groups in Door or Door Group picklist, then no doors will be assigned to the newly created users.



*You need to manually assign the desired doors to the users from User **“Profile”**:*

- *If you add any new door to the PANEL.*
- *If you add any door to the Door Group after the same is assigned to the user.*

Click **Save** to save the settings or click **Cancel** to discard.

## Alarms and Timers

To configure the Alarms and Timers parameters,

Click **Panel Configuration > Advanced Profile > Alarms and Timers**. The **Alarms and Timers** page appears.

### Alarms

Configure the following parameters:

All the alarms when triggered appear in the Alarm Report. For details, refer to **“Alarm”**.

Applicable Doors and their Alarms are listed below:

| Alarms          | Applicable Doors |      |      |            |            |            |     |              |            |            |      |              |       |  | ARGO<br>FACE210 |
|-----------------|------------------|------|------|------------|------------|------------|-----|--------------|------------|------------|------|--------------|-------|--|-----------------|
|                 | ARGO<br>FACE     | ARGO | VEGA | PATH<br>V2 | Door<br>V3 | Door<br>V4 | PVR | ARC<br>DC200 | Door<br>V1 | Door<br>V2 | Path | ARC<br>DC100 | IO800 |  |                 |
| Duress          | x                | √    | √    | √          | √          | √          | √   | √            | x          | x          | x    | x            | x     |  | x               |
| Dead Man        | √                | √    | √    | √          | √          | √          | √   | √            | x          | x          | x    | x            | x     |  | √               |
| Panic           | √                | √    | √    | √          | √          | √          | √   | √            | x          | x          | x    | x            | x     |  | √               |
| Door<br>Offline | √                | √    | √    | √          | √          | √          | √   | √            | x          | x          | x    | x            | x     |  | √               |
| Door Fault      | √                | √    | √    | √          | √          | √          | √   | √            | x          | x          | x    | x            | x     |  | √               |

|                                             |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---------------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Occupancy Violated                          | √ | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| Tail-Gating                                 | X | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| Man Trap Timer Violation                    | √ | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| Access Denied - Anti-Pass Back              | √ | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| Access Denied - Access Route Violated       | √ | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| Access Denied - Access Route Timer Violated | √ | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| Access Denied - Other Reasons               | √ | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| User Unidentified                           | √ | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| Multiple Unauthorized Attempts              | √ | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| Alarm Re-issue Wait Timer                   | √ | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| Man Trap Alarm Wait Timer                   | √ | √ | √ | √ | √ | √ | √ | √ | X | X | X | X | X | √ |
| Face Mask Compulsion                        | √ | X | X | X | X | X | X | X | X | X | X | X | X | √ |
| Door Lock Held open                         | X | X | X | X | X | X | X | √ | X | X | X | X | X | X |
| Door Lock Abnormal                          | X | X | X | X | X | X | X | √ | X | X | X | X | X | X |
| Door Lock Manual Open                       | X | X | X | X | X | X | X | √ | X | X | X | X | X | X |

Select the check boxes of the respective alarms to enable.



*The Alarms need to be enabled at the PANEL200 from Advance Profile as well as on the desired doors. For details, refer to “Alarms” in “Door Configuration”.*

*For the desired feature alarms, make sure the features are enabled from “Access Features” as well as “Zone Configuration”.*

- **Duress Alarm:** Duress Alarm can be generated when a facility/premise has been accessed by a valid user but under some threat or forced entry. In this situation, the user can give an alert to the security by entering the duress code along with user code. This duress will be reported to the security at remote location without any local alarm.



*Duress Alarm is not applicable for ARGO FACE and ARGO FACE210 Door.*

- **Dead Man Alarm:** Select the check box to enable. Dead Man Alarm is generated when the person working in restricted environment does not come out of the Dead Man Zone within a pre-defined Alert time.
- **Panic Alarm:** Select the check box to enable, if you wish to allow users to generate this alarm at the time of an emergency. Make sure this alarm is also enabled on the desired doors and the door is in normal condition (that is, armed).
- **Door Offline Alarm:** Select the check box to enable, if you wish to generate this alarm when the door does offline. Make sure this alarm is also enabled on the desired doors.
- **Door Fault Alarm:** Select the check box to enable, if you wish to generate this alarm when the door is accessed and held open for a long time. Make sure this alarm is also enabled on the desired doors.
- **Occupancy Violated Alarm:** Select the check box to enable. On violation of Occupancy Rule, this alarm will be generated and user is allowed to either enter or exit the zone.
- **Tail-Gating Alarm:** Select the check box to enable. When more than one person enters a secured area using a single person's access credentials then Tail-Gating Alarm will be activated.



*Tail-Gating Alarm is not applicable for PATH V2, ARGO Door and ARGO FACE.*

- **Man Trap Timer Violation:** Select the check box to enable. Whenever the timer, Man Trap Timer - Internal/ Man Trap Timer - External Reader (Sec) is configured for a particular door, let us consider it is configured for internal reader under Advanced Configuration of the desired door. In this case, the user is expected to punch on internal reader of any door present in the same zone/door group within the specified duration of the Man Trap Timer. If user fails to do so, Man Trap Timer Violation alarm will be activated.



*If Block User for Mantrap is enabled in “Access Features” in “Set3”, then user will be trapped within the premises whenever Man Trap Timer is violated.*

- **Access Denied-Anti-Pass Back Alarm:** Select the check box to enable. This Alarm can be enabled to restrict fraudulent use of card by enabling the Anti-Pass back feature for a zone. When the restriction is hard, the user needs to follow entry and exit sequence; else access will be denied and alarm will be generated.
- **Access Denied- Access Route Violated:** Select the check box to enable. This Alarm can be enabled to restrict the violation of Access Route configured for the user. When the restriction is hard, the user has to follow the Access Route; only then s/he will be allowed to access the doors in the route.
- **Access Denied-Access Route Timer Violated:** Select the check box to enable. Access Route has multiple levels and doors in each level. If you wish the user should access each level within a stipulated duration, then the Access Route Timer is configured. If the user does not access the desired doors in each level within the timer duration, that is the Access Route Timer is violated, then this alarm is generated.
- **Access Denied-Other Reasons:** Select the check box to enable. This alarm can be enabled to indicate the violations of other Access Control Policies (except Anti-Pass Back Violation and Access Route Violation) while accessing the door.
- **User Unidentified:** Select the check box to enable. This alarm will be generated when the credential of user accessing the door are not identified.
- **Multiple Unauthorized Attempts:** Select the check box to enable. This alarm will be generated when an unauthorized user is trying to access the door multiple times.



- **Alarm Re-issue Wait Timer (min):** Configure the duration in minutes for which an acknowledged alarm should wait before being re-issued.
- **Man Trap Alarm Wait Timer:** Select the check box to enable. This ensures that the user accesses sequential doors of a Man Trap (Zone/ Door group) within a specific time-frame.
- **Face Mask Compulsion:** Select the check box to enable. The alarm will be triggered when the users face mask is not identified.



*For Face Mask Compulsion Alarm to be triggered, make sure you have:*

- *enabled Face Mask Compulsion from Door Configuration > ARGO FACE/ARGO FACE210 Door > Face Identification Settings.*
- *set the Restriction Type as Hard from Door Configuration > ARGO FACE/ARGO FACE210 Door > Face Identification Settings.*
- *enabled the Face Mask Compulsion Alarm from Door Configuration > ARGO FACE/ARGO FACE210 Door > Alarms.*

## Timers

| Timers                   |                                 |             |
|--------------------------|---------------------------------|-------------|
| Inter-Digit Wait Timer   | <input type="text" value="3"/>  | sec (1-99)  |
| Multi-Input Wait Timer   | <input type="text" value="5"/>  | sec (3-99)  |
| Late-IN Early-OUT Timer  | <input type="text" value="60"/> | min (1-99)  |
| Door Abnormal Wait Timer | <input type="text" value="10"/> | sec (1-255) |
| Palm Enrollment Time Out | <input type="text" value="60"/> | sec (3-99)  |

- **Inter-Digit Wait Timer (sec):** Defines the time interval (in seconds) allowed between two consecutive digit entries on the door keypad. If the next digit is not entered within this duration, the system treats the user input as complete.
- **Multi-Input Wait Timer (sec):** Configure the duration (in seconds) for which you want the PANEL200 to wait for the second credential input from the user when multiple credentials are required to grant access.



*If you have Smart Cards assigned to users, then we recommend you to set the value of the Multi-Input Wait Timer (sec) greater than or equal to 10 seconds to make sure the relevant data is read from these cards to avoid access denial.*

- **Late-IN Early-OUT Timer (min):** Configure the duration (in minutes) for which the Late In and Early Out special functions remain active after being enabled. Once the defined duration elapses, the functions are automatically deactivated.
- **Door Abnormal Wait Timer (sec):** Configure the duration (in seconds) for which the PANEL200 should wait before triggering an alarm when an abnormal door status is detected. If the condition persists beyond the defined duration, the PANEL200 generates an alarm.
- **Palm Enrollment Time Out (sec):** Configure the duration in seconds for which a Palm enrollment command will be valid for credential input on a PVR door. Once this timer expires, a new enrollment command needs to be generated.

Click **Save** to save the settings or click **Cancel** to discard.

## Enrollment

To configure the Enrollment parameters,

Click **Panel Configuration > Advanced Profile > Enrollment**. The **Enrollment** page appears.

The screenshot shows the 'Enrollment' configuration page under the 'Advanced Profile' section. The page has tabs for 'Settings', 'Alarms and Timers', 'Enrollment' (selected), and 'Wiegand'. The configuration options are as follows:

- Enrollment Using Door:** ☒
- Enrollment Mode:** Read Only Card (dropdown)
- Enrollment Using:** User ID (dropdown)
- Template Using Finger:** Single Template/Finger (dropdown)
- Max Number Of Fingers:** Two (dropdown)
- Max Number Of Palms:** Ten (dropdown)
- Max Number Of Faces:** Thirty (dropdown)
- Number Of Fingers:** Two (dropdown)
- Number Of Palms:** Two (dropdown)
- Number Of Cards:** One (dropdown)
- Enable Self-Enrollment:** ☐
- Self-Enrollment Retry Count:** 5 (input field, range 0-255)
- Authorization on Enrollment:** ☐
- Save FP Image:** ☒ (with an information icon)

At the bottom, there are 'Save' and 'Cancel' buttons.

Configure the following parameters:

- **Enrollment Using Door:** Select the check box to enable enrollment of users from the door. The enrollment can be done by accessing the Menu from the door display screen.



*Users can also be enrolled from “User” under “Enrollment”.*

- **Enrollment Mode:** Select the desired option from the drop-down list:
  - If you select **Read Only Card**, **Smart Card** or **Biometric Then Card**, select the **Number of Cards** to be enrolled from the drop-down list.
  - If you select **Biometric**, select the **Number of Fingers** and **Number of Palms** to be enrolled from the drop-down list.
  - If you select **Duress Finger**, select the **Number of Fingers** to be enrolled from the drop-down list.
  - If you select **Face**, by default **Number Of Faces** to be enrolled from the door is set as 1. This can be modified from the respective door display screen only. The drop-down value on the door will be displayed as per the value set in *Panel Configuration > Basic Profile > General > Max. No. of Faces Per User*. For details, refer to “General”.
- **Enrollment Using:** Select the desired option — **User ID**, **Reference Number** — which must be entered at the door at the time of enrollment using Special Function.
- **Template Using Finger:** It displays the number of templates to be saved per fingerprint credential enrolled for the user. It displays the value as configured in “General”.
- **Max Number Of Fingers:** It displays the maximum number of fingers allowed to be enrolled for a user. It displays the value as configured in “General”.

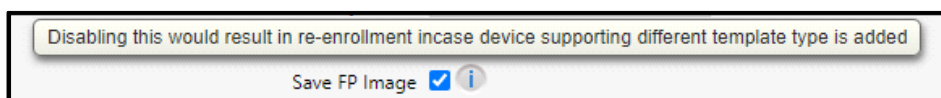
- **Max Number Of Palms:** It displays the maximum number of palms allowed to be enrolled for a user. It displays the value as configured in [“General”](#).
- **Max Number Of Faces:** It displays the maximum number of faces allowed to be enrolled for a user. It displays the value as configured in [“General”](#).
- **Number Of Fingers:** Select number of fingers allowed to be enrolled for a user from the given drop-down. The number displayed in the drop-down will be as configured in Max Number of Fingers.
- **Number Of Palms:** Select number of palms allowed to be enrolled for a user. The number displayed in the drop-down will be as configured in Max Number of Palms.
- **Number Of Cards:** Select the number of cards allowed to be enrolled for a user.
- **Enable Self-Enrollment:** Select the check box to enable self-enrollment. The Self-Enrollment feature enables the user to enroll himself/herself at a door using the pre-assigned access PIN, without the help of any operator or HR executive.

An alert message containing the access PIN is sent to the user once this feature is enabled. Make sure it is enabled for the desired users from [“Basic Access Control”](#) in [“User Configuration”](#). Self-Enrollment is beneficial for organizations with large number of employees.

- **Self-Enrollment Retry Count:** Configure the maximum number of retry counts you wish to allow for self-enrollment. The user will get locked if the retry counts exceed the set limit.
- **Authorization on Enrollment:** Select the check box to enable, that is, if you want that the enrolled must be authorized after their credentials have been enrolled. These users appear on the [“Authorization”](#) page. You can either Authorize or Reject such users. Once you authorize the desired users, they can access all the doors using their credential.

The VIP user will be allowed access even if not authorized and will be displayed on the Authorization page.

- **Save FP Image:** By default the check box is selected, that is fingerprint images will be saved in the PANEL200. Clear the check box if you do not wish to save the fingerprint images in the PANEL200.



Click **Save** to save the configuration or click **Cancel** to discard.

## Wiegand

To configure the Wiegand parameters,

Click **Panel Configuration > Advanced Profile > Wiegand**. The **Wiegand** page appears.

**Advanced Profile**

Settings | Alarms and Timers | Enrollment | **Wiegand**

Wiegand Interface: Input Mode ▼

Wait For Panel Signal: ☒

Wait For User Verification: ☒

Wait Timer: 2 sec

Send From: MSB Bit ▼

Wiegand Out Format: 26 Bit ▼

Save Cancel

Configure the following parameters:

- **Wiegand Interface:** Select the interface as Input Mode or Output Mode. The doors can be connected both as inputs (for example, to receive data from a Wiegand Reader) or outputs (for example, to support output to third party panel) via the Wiegand interface.
- **Wait for Panel Signal:** Select the check box to enable. If this option is enabled the door will wait for reply from the connected third party device before triggering any output, as per the defined Wait Timer (Sec).
- **Wait for User Verification:** Select the check box to enable. If this option is enabled, user verification will be requested on third party device before triggering any output.
- **Wait Timer:** Configure the duration for which the PANEL200 should wait for reply from the connected third party device before triggering any output.
- **Send From:** Select the desired format sending order for reader data — MSB Bit, LSB Bit.
- **Wiegand Output Format:** Select the desired option from the drop-down list — 26 Bit, Actual, 37 Bit, Custom.

If you select **Custom**, you need to configure the Wiegand Format. For each of the listed events, a custom Wiegand Output Format can be selected using the picklist. Also an access code can be assigned for each communication. This will depend on the number of output bits configured for Access Code in the selected Wiegand Output Format.

| Settings                                   | Alarms and Timers | Enrollment | Wiegand |
|--------------------------------------------|-------------------|------------|---------|
| Send From                                  |                   | MSB Bit    |         |
| Wiegand Out Format                         |                   | Custom     |         |
| Wiegand Format                             |                   |            |         |
| For Allowed Events                         |                   | ID         | Name    |
| Allowed Code                               |                   | 0          |         |
| For Identified Events                      |                   | ID         | Name    |
| Identified Code                            |                   | 0          |         |
| For Denied With Invalid Biometric Events   |                   | ID         | Name    |
| Invalid Biometric Code                     |                   | 0          |         |
| For Denied With Invalid Card Events        |                   | ID         | Name    |
| Invalid Card Code                          |                   | 0          |         |
| For Denied With Invalid PIN Events         |                   | ID         | Name    |
| Invalid PIN Code                           |                   | 0          |         |
| For Denied With Credential Time-Out Events |                   | ID         | Name    |
| Credential Time-Out Code                   |                   | 0          |         |

For details refer to [“Wiegand Format”](#).

Click **Save** to save the settings or click **Cancel** to discard.

# Access Features

---

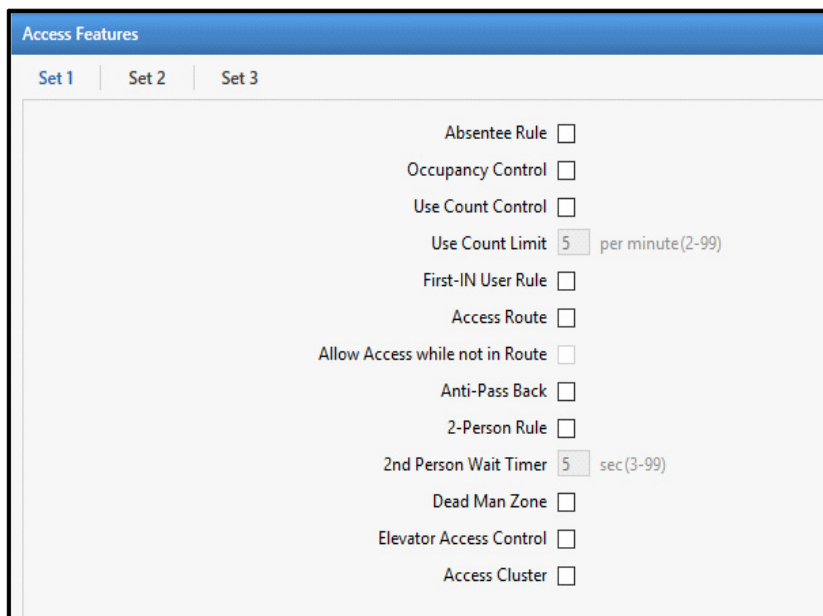
The Access Features allows you to:

- configure the Set 1 settings. For details, refer to [“Set1”](#).
- configure the Set 2 settings. For details, refer to [“Set2”](#).
- configure the Set 3 settings. For details, refer to [“Set3”](#).

## Set1

To configure the Set 1 parameters,

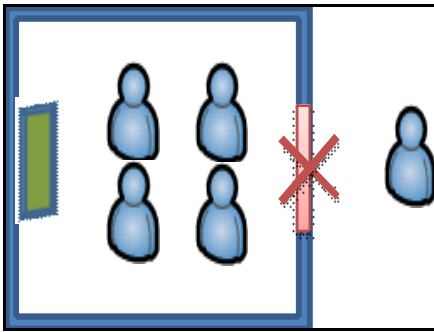
Click **Panel Configuration > Access Features > Set 1**. The **Set 1** page appears.



The screenshot shows the 'Access Features' configuration window with the 'Set 1' tab selected. The window contains a list of configuration options, each with a checkbox and, in some cases, a numeric input field and a unit. The options are: Absentee Rule (checkbox), Occupancy Control (checkbox), Use Count Control (checkbox), Use Count Limit (input field with '5' and 'per minute(2-99)'), First-IN User Rule (checkbox), Access Route (checkbox), Allow Access while not in Route (checkbox), Anti-Pass Back (checkbox), 2-Person Rule (checkbox), 2nd Person Wait Timer (input field with '5' and 'sec(3-99)'), Dead Man Zone (checkbox), Elevator Access Control (checkbox), and Access Cluster (checkbox).

Configure the following parameters:

- **Absentee Rule:** Select the check box to enable this rule at the Panel level. Using this rule, you can set the maximum number of days (1–365) for which a credential can remain unused. If the credential is not used within the defined period, the user will be automatically blocked after expiration. Make sure you have enabled Absentee Rule and configured Absent Days Count under [“Profile”](#) in [“User Configuration”](#).
- **Occupancy Control:** Select the check box to enable at the Panel level. This feature enables the PANEL200 to monitor and control the number of users permitted within a secured area or controlled zone. Occupancy Control functionality requires entry and exit readers installed in the controlled area. Make sure Occupancy Control is enabled in the desired zone. For details, refer to [“Advance Configuration 2”](#) in [“Zone Configuration”](#)



- **Use Count Control:** Select the check box to enable at the Panel level.
- **Use Count Limit:** Configure the maximum number of times an authorized user can use his/her credentials (per minute) in order to enter/exit a controlled area within a specified time period, after which the credential will be blocked.

**Example:** If the use count per minute is set as 5, then the valid user can access the door, that is punch on the door for entry/exit only 5 times in a minute. After one minute her/his credentials will be blocked and the credentials need to be restored.

- **First-IN User Rule:** Select the check box to enable at the Panel level.

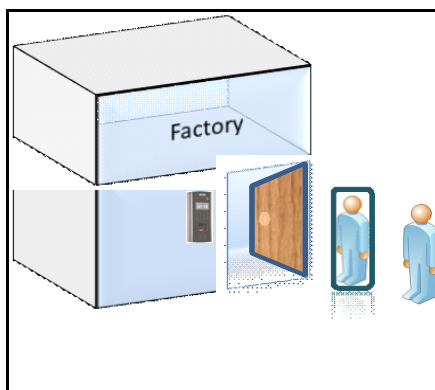
Make sure:

- you have enabled *First-IN User Rule* in the desired zone. For details, refer to [“Advance Configuration 2”](#) in [“Zone Configuration”](#).
- you have created the First IN User Group. For details, refer to [“First-IN User Rule”](#).

The First-IN user functionality enables the door to wait in locked mode till a valid First-IN user credential is detected whose working hours overlap the current doors time.

First-IN users are users defined in the PANEL200 whose credentials are used to unlock the access to a particular zone.

As soon as the zone is unlocked using a First-IN user credential, the Panel200 will allow access to others in the zone till the First-IN user's working hours or the expiry of the configured timer.



Once the period is over, the access to the designated zone will be deactivated. The PANEL200 now waits for another valid First-IN user credential with valid access time.

- **Access Route:** Select this check box to enable at the Panel level.

Make sure:

- The members doors of the Access Route are configured. For details, refer to [“Access Route”](#).
- Access Route is assigned to the desired users. For details, refer to [“Basic Access Control”](#) in [“User Configuration”](#).

The user has to follow the Access Route as per the configured levels and restrictions.

- **Allow Access while not in Route:** Select the check box to allow the access to the door which is not in Access Route but assigned to the user. For details, refer to [“User Configuration”](#).
- **Anti-Pass Back:** Select the check box to enable. The Anti-Pass Back or APB feature is used to ensure that users pass through an entry reader followed by an exit reader. It prevents a card holder from passing back his/her card to other person to gain entry into an access controlled area.

Exit reader must be installed for this feature to function smoothly.

Make sure Anti-Pass Back is enabled in the desired zone. For details, refer to [“Advance Configuration 1”](#) in [“Zone Configuration”](#).

- **2- Person Rule:** Select the check box to enable at the Panel level. This functionality requires 2 people to unlock the facility and access the secured premise. This is typically used in high security areas such as cash room, locker room, high end server room, research lab etc.

Make sure:

- it is enabled in the desired zone. For details, refer to [“Advance Configuration 1”](#) in [“Zone Configuration”](#).
- the Primary and Secondary groups are configured. For details, refer to [“2-Person Rule”](#).

- **2nd Person Wait Timer (sec):** Configure the duration in seconds after which the second person is allowed to punch.
- **Dead Man Zone:** Select the check box to enable at the Panel level. It ensures the physical safety of an employee who is working in the risky environment. The user is expected to come out of the zone at predefined intervals to reset the alarm.

Make sure, it is enabled in the desired zone. For details, refer to [“Advance Configuration 2”](#) in [“Zone Configuration”](#)

- **Elevator Access Control:** Select the check box to enable. Elevator Access Control is used for controlling the access to the floors of elevators for security purpose. Linking users with the Elevator Floor Group, that is, users can be assigned the desired Elevator Floor Group as per your requirement.

Make sure the Elevator Access Control is enabled for the desired users. For details, refer to [“Advanced Access Control 2”](#) in [“User Configuration”](#). If Elevator Access Control is not enabled, users will have access to the free floors only.

- **Access Cluster:** Select the check box to enable at the PANEL200 level. Depending on the Cluster assigned to the user, s/he will be allowed access/denied access to specific Zones/Group of doors. To create clusters, refer to [“Access Cluster”](#). To assign these clusters, refer to [“Basic Configuration”](#) in [“Door Configuration”](#).

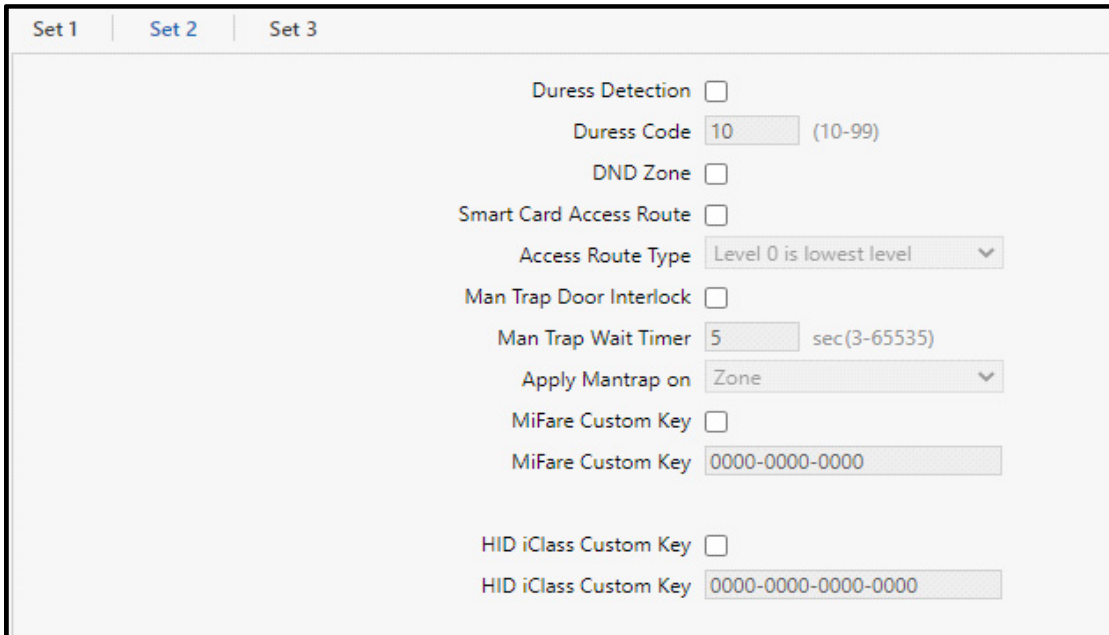
Click **Save** to save the changes or click **Cancel** to discard.



## Set2

To configure the Set 2 parameters,

Click **Panel Configuration > Access Features > Set 2**. The **Set 2** page appears.



The screenshot shows the 'Set 2' configuration page. At the top, there are tabs for 'Set 1', 'Set 2' (selected), and 'Set 3'. The configuration options are as follows:

- Duress Detection**: ☐
- Duress Code**:  (10-99)
- DND Zone**: ☐
- Smart Card Access Route**: ☐
- Access Route Type**:  (dropdown)
- Man Trap Door Interlock**: ☐
- Man Trap Wait Timer**:  sec(3-65535)
- Apply Mantrap on**:  (dropdown)
- MiFare Custom Key**: ☐
- MiFare Custom Key**:
- HID iClass Custom Key**: ☐
- HID iClass Custom Key**:

Configure the following parameters:

- **Duress Detection:** Select the check box to enable. This enables a user to notify the security when s/he is forced to access the door under constraint, threat or force.

A Duress Alarm event will be generated in PANEL200 when duress is detected.

- **Duress Code:** Configure a 2 digit Duress Code. The default code is 10. The user enters this 2 digit Duress Code after her/his allotted PIN code when s/he is forced to access the door.

The keys need to be pressed in the following order:

(User Pin Code) ->(Right Arrow Key) ->(2 digit Duress Code)-> Press "Enter"



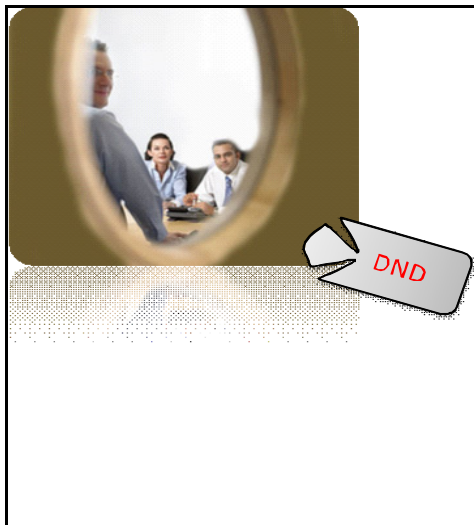
- *Only those users, who are assigned a PIN code, can access this feature.*
- *If the door is in Locked state then, user is not allowed, so no Duress will be detected.*
- **DND Zone:** Select the check box to enable. DND feature allows the user to declare that a particular zone is not to be accessed by other users for a specific period of time thereby ensuring that the users inside the zone are not disturbed by others.

The DND can be activated using a Special Card, that is, Special Function 21 on PANEL200 or it can be activated on the door using Active DND Special Function.

Make sure:

- the DND Zones Access Level is higher than Users Access Level. For example, if DND Zones Access Level is set as 5 and Users Access Level is set as 4; then user is not allowed to enter in DND Zone. However, VIP Users can access the DND Zone.

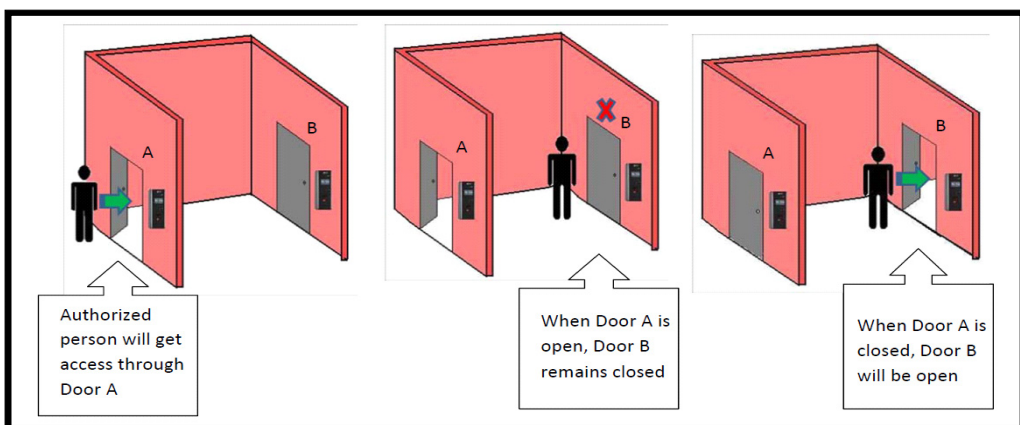
- DND Zone is enabled in the desired Zones. For details, refer to [“Advance Configuration 1”](#) in [“Zone Configuration”](#).



- **Smart Card Access Route:** Select the check box to enable. In this the user is allowed to access only specified doors with specified levels in the predefined route sequentially.
- **Access Route Type:** You can select the Access Route Type as incremental by selecting Level 0 as lowest level or decremental by selecting Level 0 as highest level.

Make sure:

- Access Route is configured. For details, refer to [“Smart Card Access Route”](#).
- The Smart Card Access Route is assigned to the desired users. For details, refer to [“Advanced Access Control”](#) in [“User Configuration”](#).
- **Man Trap Door Interlock:** Select the check box to enable at the Panel level. Mantrap Interlock provides safety, security and environmental control between two or more rooms by ensuring that opening any door causes all other doors to lock until the opened door returns to the closed position.



- **Man Trap Wait Timer (sec):** Configure the duration in seconds for which the door needs to wait for the other door in the same zone where the mantrap feature is enabled to close.
- **Apply Mantrap on:** Select the desired option — Zone, Door Group — on which the Mantrap rule is to be applied.

Make sure:

- Man Trap Door Group is created. For details, refer to [“Man Trap Door Group”](#).
- Man Trap is enabled for the desired Zone. For details, refer to [“Advance Configuration 2”](#) in [“Zone Configuration”](#)
- The Man Trap Door Group is assigned to the desired doors. For details, refer to [“Basic Configuration”](#) in [“Door Configuration”](#).

### Custom Key

You can either use the default Matrix Key for Smart Cards or customize the Smart Card Key. You can change the Smart Card Key as many times as you want or revert to the default Matrix Smart Card Key.

You can define custom keys for HID as well as for MiFare cards. To use a custom key, select the type of Smart Card you wish to use and enter the desired key in hexadecimal digits.

- **MiFare Custom Key:** Select the check box and configure the desired key in 12 hexadecimal digits.
- **HID iClass Custom Key:** Select the check box and configure the desired key in 12 hexadecimal digits.

Click **Save** to save the changes or click **Cancel** to discard.

## Set3

To configure the Set 2 parameters,

Click **Panel Configuration > Access Features > Set 3**. The **Set 3** page appears.

Configure the following parameters:

- **Block User For:** Select the desired access policy check boxes to block the users for violating them — Tail-Gating, Man Trap Timer Violation, Occupancy Violation, Anti-Pass Back Violation and Multiple Unauthorized Attempts.

For Multiple Unauthorized Attempts, configure the number of attempts you wish to allow in **Allowed Unauthorized Attempts**, after which the user will be blocked.

Click **Save** to save the settings or click **Cancel** to discard.

# Special Functions

---

Special Functions enable the users to perform certain pre-defined operations directly from the doors. These operations are related to various time and attendance marking functions, administrative tasks, zone-related access, global functions and door-control functionality as well as alarm management.

These functions can be accessed by using designated **Special Function Cards** by the users of the “**Functional Group**” assigned against the Special Function. By default, some of the Special Functions are accessible to All Functional Groups whereas you can assign desired Functional Group — Admin, Staff, Visitor — to the remaining Special Functions, as described in the table below.

There are five **Global Special Functions** which are used to carry out mass operations in cases of emergency or when all the doors need to be controlled at the same time. The Global Special Functions are applicable to all doors, irrespective of the zones.

Make sure all the users are assigned authentication credentials (user name and password) for accessing Special Functions.

For example, in factories where workers can avail short leave, a security guard uses the Special Card enrolled for **Short Leave-IN** on the Entry door to give access to the workers. This same card can be used for multiple workers. Each worker is assigned credentials for authentication using which they can access the door.

The following Special Functions are supported:

| Special Function    | Functional Group      | Description                                                                              |
|---------------------|-----------------------|------------------------------------------------------------------------------------------|
| Official Work- IN   | All                   | Late-IN is marked as official work hours.                                                |
| Official Work - OUT | All                   | Early-OUT is marked as official work hours.                                              |
| Short Leave - IN    | All                   | Late-IN is marked as short leave hours.                                                  |
| Short Leave - OUT   | All                   | Early-OUT is marked as short leave hours.                                                |
| Regular - IN        | All                   | Punch IN at start time of the shift is considered as beginning of Regular working hours. |
| Regular - OUT       | All                   | Punch OUT at end time of the shift is considered as completion of Regular working hours. |
| Break End           | All                   | Punch IN marked after break end is considered as end of break hours.                     |
| Break Start         | All                   | Punch OUT marked at the beginning of break time is considered as start of break hours.   |
| Over Time - IN      | All                   | Punch IN marked at the beginning of Over-Time is considered as start of Over-Time.       |
| Over Time - OUT     | All                   | Punch OUT marked at the completion of Over-Time is considered as end of Over-Time.       |
| Set Panic Alarm     | All                   | Used to generate Panic alarm during an emergency.                                        |
| Enroll User         | Admin, Staff, Visitor | Used to switch door mode into Enrollment mode so that users can be enrolled.             |
| Enroll Special Card | Admin, Staff, Visitor | Used to switch door mode into Enrollment mode so that special cards can be enrolled.     |

| Special Function       | Functional Group      | Description                                                                                                                                                |
|------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delete Credentials     | Admin, Staff, Visitor | Used to delete user credential data.                                                                                                                       |
| Late IN- Start         | Admin, Staff, Visitor | Punch IN marked after accessing Late IN - Start special function will be considered as Late IN.                                                            |
| Late IN - Stop         | Admin, Staff, Visitor | Punch IN marked after accessing Late IN - Stop special function will not be considered as Late IN.                                                         |
| Early OUT - Start      | Admin, Staff, Visitor | Punch OUT marked after accessing Early OUT - Start special function will be considered as Early OUT.                                                       |
| Early OUT - Stop       | Admin, Staff, Visitor | Punch OUT marked after accessing Early OUT - Stop special function will not be considered as Early OUT.                                                    |
| View User Profile      | Admin, Staff, Visitor | Displays User Profile details of the authenticated user.                                                                                                   |
| Activate DND           | Admin, Staff, Visitor | Activates DND for the zone assigned to the door.                                                                                                           |
| Deactivate DND         | Admin, Staff, Visitor | Deactivate DND for the zone assigned to the door.                                                                                                          |
| Activate Dead Man      | Admin, Staff, Visitor | Activates Dead Man for the zone assigned to the door.                                                                                                      |
| Deactivate Dead Man    | Admin, Staff, Visitor | Deactivates Dead Man for the zone assigned to the door.                                                                                                    |
| Door Lock              | Admin, Staff, Visitor | Locks the door.                                                                                                                                            |
| Door Unlock            | Admin, Staff, Visitor | Unlocks the door.                                                                                                                                          |
| Door Normal            | Admin, Staff, Visitor | Resets the door status to normal.                                                                                                                          |
| Zone Lock              | Admin, Staff, Visitor | Locks the all the doors in the zone assigned to the door.                                                                                                  |
| Zone Unlock            | Admin, Staff, Visitor | Unlock the all the doors in the zone assigned to the door.                                                                                                 |
| Zone Normal            | Admin, Staff, Visitor | Resets the door status to normal for all the doors in the zone assigned to the door.                                                                       |
| Mute Door Buzzer       | Admin, Staff, Visitor | Mutes the door's alarm.                                                                                                                                    |
| Mute Panel Buzzer      | Admin, Staff, Visitor | Mutes the PANEL's alarm.                                                                                                                                   |
| Clear Door Aux Output  | Admin, Staff, Visitor | Reset the door's Aux Output.                                                                                                                               |
| Clear Panel Aux Output | Admin, Staff, Visitor | Reset the PANEL's Aux Output.                                                                                                                              |
| Door Arm               | Admin, Staff, Visitor | To arm the door. When armed, all the configured I/O Links, Time Triggered functions, Alarms will function normally.                                        |
| Door Disarm            | Admin, Staff, Visitor | To disarm the door. When disarmed, all the configured I/O Links, Time Triggered functions, Alarms will stop.                                               |
| Zone Arm               | Admin, Staff, Visitor | To arm the zone. When armed, all the I/O Links, Time Triggered functions, Alarms of all the doors in the zone assigned to the door will function normally. |
| Zone Disarm            | Admin, Staff, Visitor | To disarm the zone. When disarmed, all the I/O Links, Time Triggered functions, Alarms of all the doors in the zone assigned to the door will stop.        |
| Clear Alarm            | Admin, Staff, Visitor | To clear the alarms of the PANEL.                                                                                                                          |
| Global Lock            | Admin, Staff, Visitor | To lock all the doors connected to the PANEL.                                                                                                              |
| Global Unlock          | Admin, Staff, Visitor | To unlock all the doors connected to the PANEL.                                                                                                            |

| Special Function | Functional Group      | Description                                                                                                                                     |
|------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Global Normal    | Admin, Staff, Visitor | To reset all the doors connected to the PANEL to their normal state.                                                                            |
| Global Arm       | Admin, Staff, Visitor | To arm all the doors connected to the PANEL. When armed, all the configured I/O Links, Time Triggered functions, Alarms will function normally. |
| Global Disarm    | Admin, Staff, Visitor | To disarm all the doors connected to the PANEL. When disarmed, all the configured I/O Links, Time Triggered functions, Alarms will stop.        |

The Special Function allows you to:

- configure the configuration parameters. For details, refer to [“Configuration”](#)
- configure the schedule for the special functions. For details, refer to [“Schedule”](#).

## Configuration

To configure the Configuration parameters,

Click **Panel Configuration > Special Function > Configuration**. The **Configuration** page appears.

| Sr. No. | Special Function    | Active                              | Functional Group | Card 1 | Card 2 | Card 3 | Card 4 |   |
|---------|---------------------|-------------------------------------|------------------|--------|--------|--------|--------|---|
| 1       | Official Work - IN  | <input checked="" type="checkbox"/> | All              |        |        |        |        | ↔ |
| 2       | Official Work - OUT | <input checked="" type="checkbox"/> | All              |        |        |        |        | ↔ |
| 3       | Short Leave - IN    | <input checked="" type="checkbox"/> | All              |        |        |        |        | ↔ |
| 4       | Short Leave - OUT   | <input checked="" type="checkbox"/> | All              |        |        |        |        | ↔ |
| 5       | Regular - IN        | <input checked="" type="checkbox"/> | All              |        |        |        |        | ↔ |
| 6       | Regular - OUT       | <input checked="" type="checkbox"/> | All              |        |        |        |        | ↔ |
| 7       | Break End           | <input checked="" type="checkbox"/> | All              |        |        |        |        | ↔ |
| 8       | Break Start         | <input checked="" type="checkbox"/> | All              |        |        |        |        | ↔ |
| 9       | Over Time - IN      | <input checked="" type="checkbox"/> | All              |        |        |        |        | ↔ |
| 10      | Over Time - OUT     | <input checked="" type="checkbox"/> | All              |        |        |        |        | ↔ |

Save Cancel

Configure the following parameters:

- **Active:** Select the check box of the desired Special Function to enable.
- **Functional Group:** Select the desired Functional Group to which you wish to assign the Special Function from the drop-down list options — All, Admin, Staff, Visitor. For details, refer to [“Functional Group”](#).



From Firmware Version V13R3 and later, the default Functional Group will be set as Admin for the Special Functions — Enroll User, Enroll Special Card, Delete Credentials.

If the Functional Group itself is deleted, then the Special Function assigned to it will not function. You need to manually re-assign the desired Functional Group.

- **Card 1/2/3/4:** Configure the Card Serial Number (CSN) or Facility Code Separated CSN to be assigned against the Special Function. You can configure 4 cards against each Special Function.

The sample CSN/Facility Code separated CSN Format are as follows:

- **Card Serial Number** = 1343933547.
- **Facility Code separated CSN** = 12,345789



The maximum character limit for Card Serial Number (CSN) is 20 digits. While the maximum character limit for Facility Code separated CSN is 21 digits.

- If you enroll a “**Special Card**” against a Special Function, the card number will be displayed against the Special Function.

Click **Save** to save the settings or click **Cancel** to discard.

To erase all the enrolled cards against a Special Function, click **Undo**  corresponding to the desired Special Function.

You can also create Schedules according to which you wish to allow users to access the Special Functions.

## Schedule

You can create schedules for specific Special Function according to which users will be able to access them on the assigned doors.

To configure the Schedule parameters,

Click **Panel Configuration > Special Function > Schedule**. The **Schedule** page appears.

Special Function

Configuration | Schedule

ID

Name

Start Time

End Time

Active Days ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

| ID               | Name | Start Time | End Time |  |
|------------------|------|------------|----------|--|
| No Record Found! |      |            |          |  |

Add

- Click **Add**.

Special Function

Configuration | Schedule

ID

Name

Start Time

End Time

Active Days ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

| ID               | Name | Start Time | End Time |  |
|------------------|------|------------|----------|--|
| No Record Found! |      |            |          |  |

Save Cancel

Configure the following parameters:

- **ID**: This is auto-generated and will be displayed once you click **Add**.



- **Name:** Select the desired Special Function from the drop-down list for which you wish to create the schedule.
- **Start Time:** Configure the start time from which the selected Special Function must start functioning.
- **End Time:** Configure the end time at which the selected Special Function must stop functioning.
- **Active Days:** Select the check boxes of the desired days on which the selected Special Function must function.
- Click **Save** to save the settings or click **Cancel** to discard.

The created schedule appears in the right pane. You can edit or delete the created schedules.

**Special Function**

Configuration | Schedule

ID: 1

Name: Official Work - IN

Start Time: 09:00

End Time: 10:00

Active Days: ☐ Sun ☒ Mon ☒ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

| ID | Name                | Start Time | End Time |  |
|----|---------------------|------------|----------|--|
| 1  | Official Work - IN  | 09:00      | 10:00    |  |
| 2  | Official Work - OUT | 05:00      | 07:00    |  |

Add Delete Save Cancel

To Edit,

- Click on the desired schedule in the right pane.
- Edit its parameters on the right as per your requirement.
- Click **Save** to save the settings.

To Delete,

- In the right pane, click **Delete** corresponding to the desired schedule.

# Input Output

---

The Input Output page enables you to define Input/Output (I/O) configuration for the PANEL200.

The Input/Output (I/O) configuration determines how the output or response is influenced by the input applied on it. The PANEL200 can be configured to trigger a specific response to any changes in door state or event occurrences at the door. This change in door state or occurrence of events can be considered as an input while the response or action that is generated by the PANEL200 on detection of this input, is defined as the output.

The Input Output allows you to:

- configure the configuration parameters. For details, refer to [“Configuration”](#).
- configure the input group parameters. For details, refer to [“Input Group”](#).
- configure the IO linking parameters. For details, refer to [“IO Linking”](#).
- configure the Time Trigger parameters. For details, refer to [“Time Triggered”](#).

## Configuration

To configure the Configuration parameters,

Click **Panel Configuration > Input Output > Configuration**. The **Configuration** page appears.

Configure the following parameters:

### Auxiliary Input

- **Enable:** Select the check box to enable.
- **Supervised:** Select the check box to enable the Auxiliary Input for four-state monitoring where the door is monitored for Normally Open, Normally Closed, Door Fault and Door Disconnection.
- **Sense Type:** The PANEL200 by default can sense two states of a door — Normally Open (NO) and Normally Closed (NC) depending on which the output is determined. Select the desired option — NC or NO.

For example, any deviation of the door from its normal state may lead to the trigger of a Door Abnormal Alarm.

- For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an Alarm is generated.

- **Enable:** Select the check box to enable.
- **Output Group No.:** Configure the Output Group Number to which the Auxiliary Output is to be assigned based on the “Output Group” defined in the PANEL200.

Click **Save** to apply the changes.

An Input Group is formed by grouping together multiple input ports (logical groups). This option allows you to assign user-friendly names to frequently used inputs and also configuring the input parameters. You can club any of the inputs (not constrained to particular door) and define them in a group.

This page displays a grid containing a list of configured input groups along with their details like input group type and the number of members in a particular group. Maximum 99 Input Groups can be added.

To configure the Input Group parameters,

Click **Panel Configuration > Input Output > Input Group**. The **Input Group** page appears.

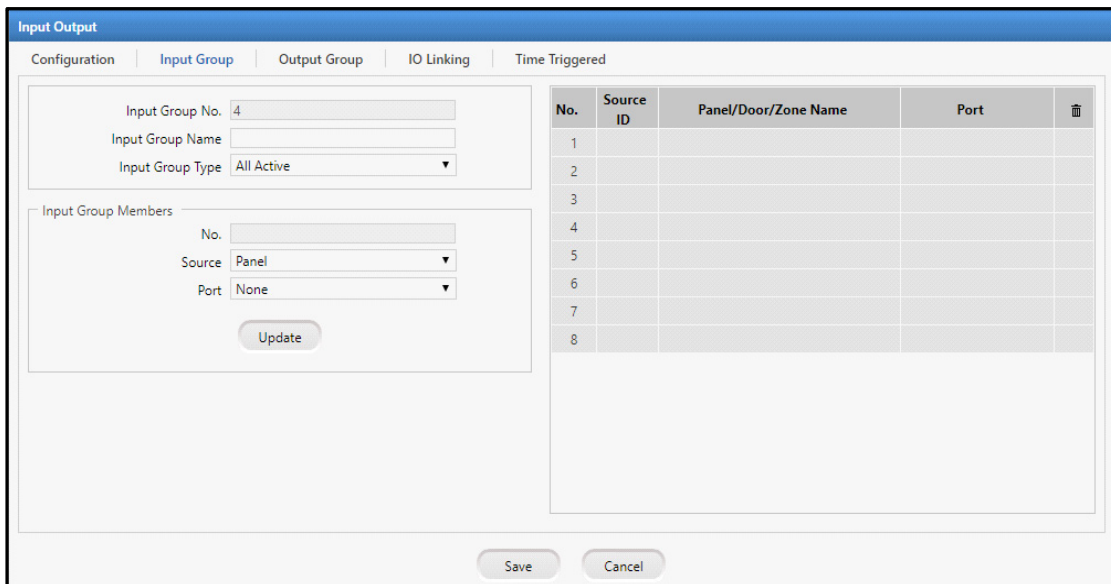
All the created Input Groups appear in the grid. By default, three groups — Aux Input Group, Door Force Open, Fire Alarm IN — are already created and are displayed here with their details — Input Group Name, Input Group Type, number of Members. You can click the same and edit them per your requirement or you can add a new Input Group.

You cannot delete the default Input Groups. However, other created groups can be deleted. To do so, click **Delete**  corresponding to the desired group.

## Adding an Input Group

To add a new group,

Click **Add**. You can add upto 99 groups. Each group can have upto 8 members.



| No. | Source ID | Panel/Door/Zone Name | Port |  |
|-----|-----------|----------------------|------|--|
| 1   |           |                      |      |  |
| 2   |           |                      |      |  |
| 3   |           |                      |      |  |
| 4   |           |                      |      |  |
| 5   |           |                      |      |  |
| 6   |           |                      |      |  |
| 7   |           |                      |      |  |
| 8   |           |                      |      |  |

Configure the following parameters:

- **Input Group No.:** The Input Group No. is auto generated by the PANEL200.
- **Input Group Name:** Configure a name you wish to assign to the group.
- **Input Group Type:** Select the desired option — All Active, Any One Active.

### Input Group Members

You can add maximum **8** members. Click the desired No. in the right pane and configure its parameters.

- **No.:** The selected No. is displayed.
- **Source:** Select the desired option — Panel, Door, Zone.

If you select **Panel**, configure the following:

- **Port:** Select the desired option from the drop-down list.

If you select **Door**, configure the following:

- **Port:** Select the desired option from the drop-down list.



*The **Port** options differ as per the selected **Source** option.*

- **Door:** Click **Select Door** picklist. The **Panel Doors** pop-up appears. Select the desired door.

**OR**

If required, you can also search for the desired door.

**Search By:** Select the desired option by which you wish to search for the door — Door ID, Door Name.

In the corresponding box enter the keyword. Click **Search** . The doors will be filtered as per the keyword. Click to select the desired door.

The selected doors name appear against the Door.

- **User:** This option is applicable only if any **User** option is selected as the Port option.

Select the desired option — All, Selected — from the drop-down list.

If you select **Selected**,

- **Users Selected:** Click the **Users Selected** picklist. The **User** pop-up appears. Select the check boxes of the desired users. Maximum 10 users can be selected. Click **Ok**.

**OR**

If required, you can also search for the desired user.

**Search By:** Select the desired option by which you wish to search for the user — User ID, User

Name. In the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Select the check boxes of the desired users. Maximum 10 users can be selected. Click **Ok**.

The number of selected users appears against Users Selected.

If you select **Zone**, configure the following:

- **Port:** Select the desired option from the drop-down list.



*The **Port** options differ as per the selected **Source** option.*

- **Zone:** Click **Select Zone** picklist. The **Zone** pop-up appears. Select the desired Zone.

**OR**

If required, you can also search for the desired door.

**Search By:** Select the desired option by which you wish to search for the door — Zone ID, Zone Name.

In the corresponding box enter the keyword. Click **Search** . The zones will be filtered as per the keyword. Click to select the desired zone.

The selected zones name appear against the Zone.

- Click **Update**. The configured member appears right pane. Similarly, you can add other members to the group.

You can edit or delete any member.

To edit, click on the desired member from the right pane. Edit the parameters as per your requirement. Click **Update**.

To delete, click **Delete**  corresponding to the desired member.

Click **Save** to save the settings. Similarly, you can add other groups.

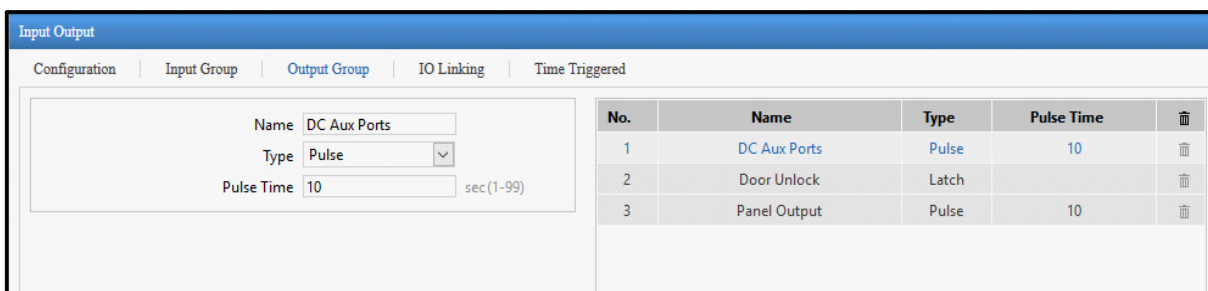
To view all the Input Groups, click the **Input Group** tab again. All the created Input Groups appear in the grid.

## Output Group

You can organize the output ports of PANEL/doors into groups before using them in Input/Output linking programs.

To configure the Input Group parameters,

Click **Panel Configuration > Input Output > Input Group**. The **Input Group** page appears.



| No. | Name         | Type  | Pulse Time |                                                                                       |
|-----|--------------|-------|------------|---------------------------------------------------------------------------------------|
| 1   | DC Aux Ports | Pulse | 10         |  |
| 2   | Door Unlock  | Latch |            |  |
| 3   | Panel Output | Pulse | 10         |  |

All the created Output Groups appear in the grid. By default, three groups — DC Aux Ports, Door Unlock, Panel Output — are already created and are displayed here with their details — Name, Type, Pulse Time. You can click the same and edit them per your requirement or you can add a new Output Group.

You cannot delete the default Output Groups. However, other created groups can be deleted. To do so, click **Delete**

 corresponding to the desired group.

## Adding an Output Group

To add a new group,

Click **Add**. You can add upto 99 groups.

| No. | Name         | Type  | Pulse Time |  |
|-----|--------------|-------|------------|--|
| 1   | DC Aux Ports | Pulse | 10         |  |
| 2   | DC Aux Ports | Pulse | 10         |  |
| 3   | Panel Output | Pulse | 10         |  |

Configure the following parameters:

- **Name:** Configure a name you wish to assign to the group.
- **Type:** Select the desired option — Pulse, Interlock, Latch, Toggle.

**Pulse:** If you select this option, you need to configure the **Pulse Time** in seconds. The output will remain active for the configured duration.

**Interlock:** If you select this option, the output follows the input. The output will be active till the input is active after which it returns to normal state.

**Latch:** If you select this option, the output will be active for an infinite period and needs to be reset manually. It means once the input is active, output will be active. It has to be reset manually. For example: During a fire alarm, door should be unlocked permanently so Latch output is used.

**Toggle:** If you select this option, the output group toggles its state whenever an input group is activated.

- **Pulse Time:** If you have selected Pulse option for Type, configure the Pulse Time. This is duration for which the output will remain active.

Click **Add**. The Output Group appears in the right pane.

You can edit or delete the group.

To edit, click the desired group from the right pane and edit it as per your requirement. Click **Update**.

To delete, click **Delete** corresponding to the desired group

## IO Linking

I/O Linking (Input/Output Linking) is a feature that allows you to define relationships between inputs and outputs. Inputs can come from PANEL/doors, while outputs can control actions like unlocking doors, triggering sirens, etc. By linking them, you can automatically respond to specific events — for example, unlocking emergency exits when a fire alarm is triggered, or activating a buzzer when a door is forced open. This ensures faster, automated responses without manual intervention.

To configure the IO Linking parameters,

Click **Panel Configuration > Input Output > IO Linking**. The **IO Linking** page appears.

| No. | Link Name       | Input Group     | Output Group |  |
|-----|-----------------|-----------------|--------------|--|
| 1   | Aux Linking     | Aux Input Group | DC Aux Ports |  |
| 2   | Force Open Link | Door Force Open | Panel Output |  |
| 3   | Fire-Unlock     | Fire Alarm In   | Door Unlock  |  |

All the created IO Links appear in the grid. By default, three IO Links — Aux Linking, Force Open Link, Fire-Unlock— are already created and are displayed here with their details — Link Name, Input Group, Output Group. You can click the same and edit them per your requirement or you can add a new Output Group.

You cannot delete the default IO Links. However, other created IO Links can be deleted. To do so, click **Delete**



corresponding to the desired IO Link.

## Adding an IO Link

To add a new IO Link,

Click **Add**. You can add upto 99 IO Links.

| No. | Link Name       | Input Group     | Output Group |  |
|-----|-----------------|-----------------|--------------|--|
| 1   | Aux Linking     | Aux Input Group | DC Aux Ports |  |
| 2   | Force Open Link | Door Force Open | Panel Output |  |
| 3   | Fire-Unlock     | Fire Alarm In   | Door Unlock  |  |

Configure the following parameters:



- **Link Name:** Configure a name you wish to assign to the IO Link.
- **Active:** Select the check box to enable the link.
- **Input Group Name:** Click the **Select Input Group** picklist. The **Input Group** pop-up appears. Select the desired group.

**OR**

If required, you can also search for the desired group.

**Search By:** Select the desired option by which you wish to search for the group — Input Group No., Input Group Name. In the corresponding box enter the keyword. Click **Search** . The groups will be filtered as per the keyword. Click to select the desired group.

The selected group name appear against the Input Group Name.

- **Output Group Name:** Click the **Select Output Group** picklist. The **Output Group** pop-up appears. Select the desired group.

**OR**

If required, you can also search for the desired group.

**Search By:** Select the desired option by which you wish to search for the group — Output Group No., Output Group Name. In the corresponding box enter the keyword. Click **Search** . The groups will be filtered as per the keyword. Click to select the desired group.

The selected group name appear against the Output Group Name.

- **Time Zone 1:** The Time Zones define the time slots in which the IO Links will be activated.

Click the **Select Time Zone** picklist. The **Time Zone** pop-up appears. Select the desired time zone.

**OR**

If required, you can also search for the desired time zone.

**Search By:** Select the desired option by which you wish to search for the time zone — Time Zone ID, Time Zone Name. In the corresponding box enter the keyword. Click **Search** . The time zones will be filtered as per the keyword. Click to select the desired time zone.

The selected time zone name appear against the Time Zone 1.

Similarly, configure **Time Zone 2** and **Time Zone 3**.

Click **Add**. The IO Link appears in the right pane.

You can edit or delete the IO Link.

To edit, click the desired IO Link from the right pane and edit it as per your requirement. Click **Update**.

To delete, click **Delete**  corresponding to the desired IO Link.

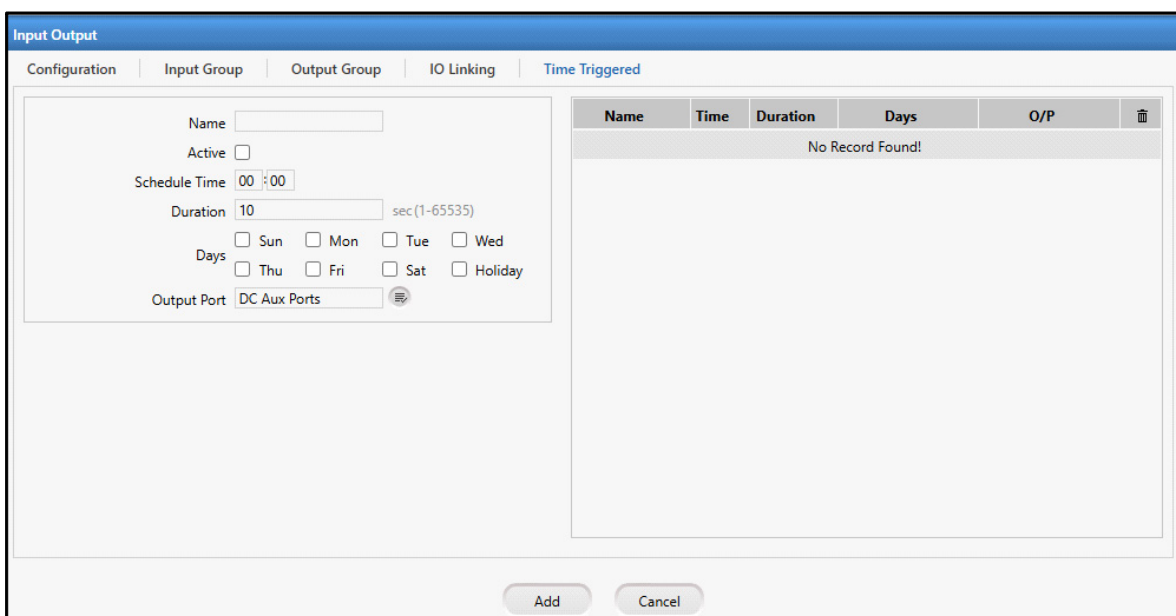
## Time Triggered

The Time Triggered feature allows certain Outputs or Output Group to be automatically activated or deactivated based on a predefined schedule. Instead of waiting for an input event (like a sensor), the PANEL200 performs the action at a specific time or within a set time range.

For example: Unlocking all office doors automatically at 9:00 AM and locking them again at 6:00PM, Activating sirens or lights during night hours for enhanced security, Triggering an announcement system every day at a scheduled time.

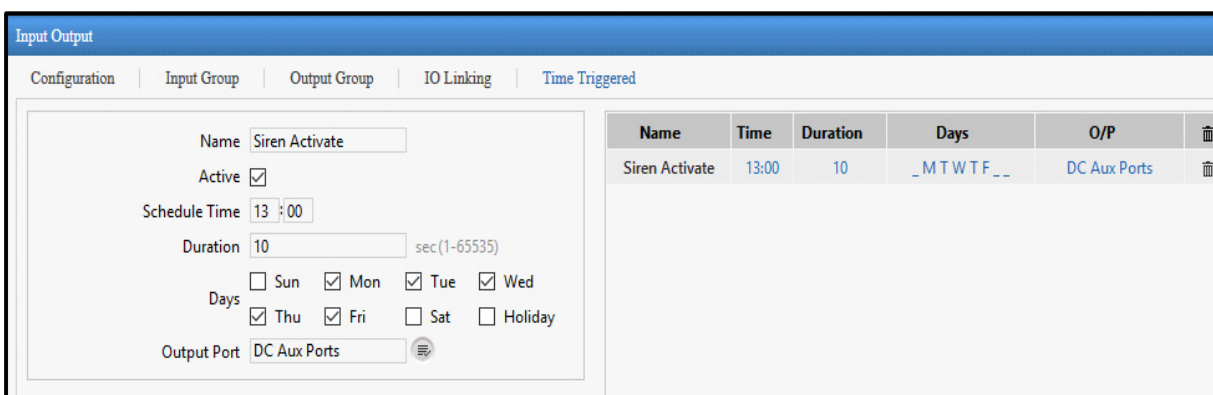
To configure the Time Triggered parameters,

Click **Panel Configuration > Input Output > Time Triggered**. The **Time Triggered** page appears.



| Name             | Time | Duration | Days | O/P |  |
|------------------|------|----------|------|-----|--|
| No Record Found! |      |          |      |     |  |

Click **Add**. You can add upto 99 Time Triggered schedules.



| Name           | Time  | Duration | Days     | O/P          |                                                                                       |
|----------------|-------|----------|----------|--------------|---------------------------------------------------------------------------------------|
| Siren Activate | 13:00 | 10       | _MTWTF__ | DC Aux Ports |  |

Configure the following parameters:

- **Name:** Configure a name that you wish to assign to the time triggered schedule.

- **Active:** Select the check box to enable the time triggered schedule.
- **Schedule Time:** Configure the time at which you wish to activate the time triggered schedule.
- **Duration:** Configure the duration (seconds) for which you want the time triggered schedule to remain active.
- **Days:** Select the check boxes of the desired days on which you want the time triggered schedule to be applied.
- **Output Port:** Click the **Select Output Group** picklist. The **Output Group** pop-up appears. Select the desired group.

**OR**

If required, you can also search for the desired group.

**Search By:** Select the desired option by which you wish to search for the group — Output Group No., Output Group Name. In the corresponding box enter the keyword. Click **Search** . The groups will be filtered as per the keyword. Click to select the desired group.

The selected group name appear against the Output Port.

Click **Add**. The Time Triggered schedule appears in the right pane with the details — Name, Time, Duration, Output Port.

You can edit or delete any created Time Triggered schedule.

To edit, click the desired Time Triggered schedule from the right pane and edit it as per your requirement. Click **Update**.

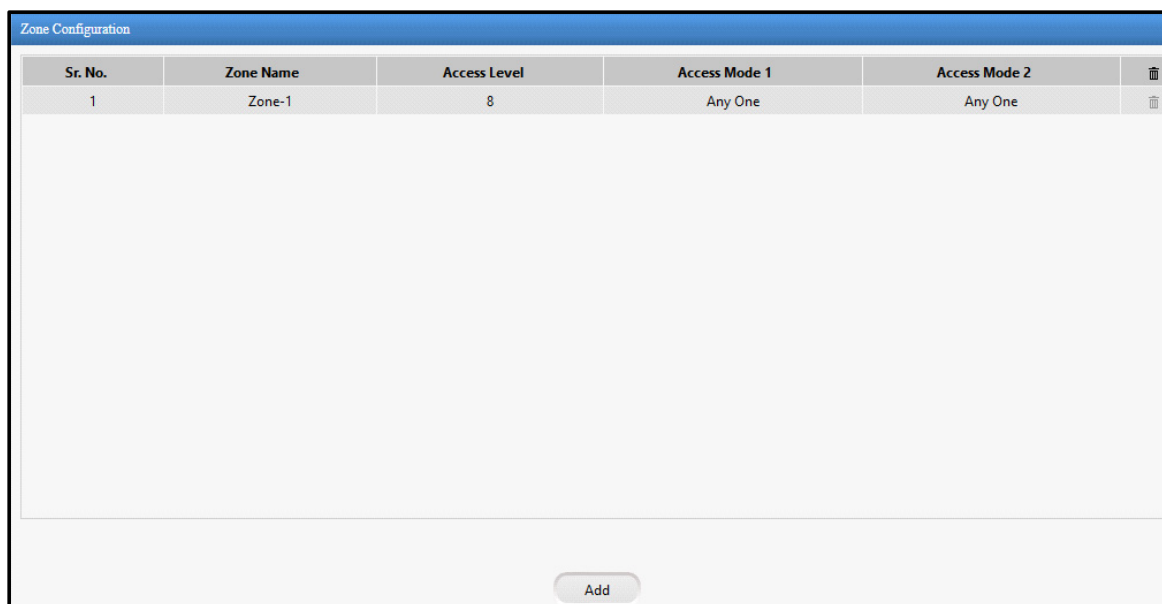
To delete, click **Delete**  corresponding to the desired IO Link.

# Zone Configuration

Access Zones are areas with well defined boundaries, which are defined to effectively implement an Access Security System with Access Policies. A site can have multiple Access Zones and each Zone can have multiple doors. You need to create the Zones first and then the same needs to be assigned to the desired doors.

To configure the Zone parameters,

Click **Panel Configuration > Zone Configuration**. The **Zone Configuration** page appears.



| Sr. No. | Zone Name | Access Level | Access Mode 1 | Access Mode 2 |                                                                                     |
|---------|-----------|--------------|---------------|---------------|-------------------------------------------------------------------------------------|
| 1       | Zone-1    | 8            | Any One       | Any One       |  |

[Add](#)

All the created Zones appear in the grid. By default Zone-1 is already created and it is displayed here, with its details — Zone Name, Access Level, Access Mode1, Access Mode2. You can click the same and edit it as per your requirement or you can add a new Zone.

You cannot delete the default Zone-1. However, other created zones can be deleted. To do so, click **Delete**  corresponding to the desired zone.

The Zone Configuration allows you to:

- configure the basic configuration parameters. For details, refer to [“Basic Configuration”](#).
- configure the advance configuration 1 parameters. For details, refer to [“Advance Configuration 1”](#).
- configure the advance configuration 2 parameters. For details, refer to [“Advance Configuration 2”](#).
- configure the advance configuration 3 parameters. For details, refer to [“Advance Configuration 3”](#).

To add a new Zone,

Click **Add**. You can add upto 99 Zones.

The screenshot shows a web interface titled "Zone Configuration". It contains a table with the following columns: "Sr. No.", "Zone Name", "Access Level", "Access Mode 1", "Access Mode 2", and a delete icon (trash can). The table has one data row with the following values: "1", "Zone-1", "8", "Any One", and "Any One". Below the table, there is a light blue button labeled "Add".

| Sr. No. | Zone Name | Access Level | Access Mode 1 | Access Mode 2 |  |
|---------|-----------|--------------|---------------|---------------|--|
| 1       | Zone-1    | 8            | Any One       | Any One       |  |

Add

## Basic Configuration

To configure the Basic Configuration parameters,

Click **Panel Configuration > Zone Configuration > Basic Configuration**. The **Basic Configuration** page appears.

The screenshot shows the "Basic Configuration" page within the "Zone Configuration" section. It features a tabbed interface with "Basic Configuration" selected. The form contains the following fields and controls:

- Zone ID: Text input field with value "1".
- Zone Name: Text input field with value "Zone-1".
- Access Level: Dropdown menu with value "Level 8".
- Access Control On Exit Mode: Checkbox, currently unchecked.
- Allow Exit When Locked: Checkbox, currently checked.
- Degraded Mode: Checkbox, currently checked.
- Degrade Mode Type: Dropdown menu with value "Advance".
- Door Mode Selection: Checkbox, currently unchecked.
- Access Mode: Section header for the following fields.
- Internal or Reader Group 1 Mode: Dropdown menu with value "Biometric+Card".
- External or Reader Group 2 Mode: Dropdown menu with value "Any One".

Configure the following parameters:

- **Zone ID:** The Zone ID is auto generated by the PANEL200.
- **Zone Name:** Configure a name you wish to assign to the zone.
- **Access Level:** Select the desired access level you wish to assign to the zone from the drop-down list.

- **Access Control on Exit Mode:** Select the check box to enable. The following access control policies will be checked for the user on exit:
  - User validity check
  - Blocked user check
  - Inactive (disabled) user check
  - Additional Security Code when credential type is card
  - Time based access check
  - Access Group enabled check
- **Allow Exit When Locked:** Select the check box to enable. The user will be allowed to exit even when the door is locked.
- **Degraded Mode:** Select the check box to allow a valid user to access the facility even if the door is not in communication with the PANEL. Make sure you have enabled Degraded Mode and configured the Degraded Wait Timer under “Settings” in “Advanced Profile”.
- **Degraded Mode Type:** If you have enabled Degraded Mode, you can select the Degraded Mode Type — Basic, Advanced.

If you select **Basic**, the user will be allowed/denied entry on the basis of limited checking of credential (that is finger and card) verification, and the Access Policies will not be checked if configured. During Exit, user will be allowed to exit only after the credentials are verified. No other checking/verification will be done during exit.

If you select **Advanced**, the user will be allowed/denied entry/exit on the basis of checking the credential (all credentials will be supported) as well as the user details will be verified and checked. However, Access Policies will not be checked, if configured.

- **Door Mode Selection:** Select the check box to enable. The user will be allowed to select the punch type, that is IN/OUT while punching on the door.

## Access Mode

**Internal or Reader Group1 Mode:** Select the desired access mode from the drop-down list.

**External or Reader Group2 Mode:** Select the desired access mode from the drop-down list.



*Biometric and BLE credentials are not supported in OSDP Readers. Hence, select the Access Mode accordingly.*

Click **Save** to save the settings or click **Cancel** to discard.

## Advance Configuration 1

To configure the Advance Configuration 1 parameters,

Click **Panel Configuration > Zone Configuration > Advance Configuration 1**. The **Advance Configuration 1** page appears.

Zone Configuration

Basic Configuration | **Advance Configuration 1** | Advance Configuration 2 | Advance Configuration 3

**2-Person Rule**

Enable ☒

Primary Group QA TL Group

Secondary Group QA Member Group

Mode Primary Must

**Anti-Pass Back**

On Entry ☒ Local

On Exit ☐

Restriction Type Soft

Forgiveness ☒

Reset After ☐ Day Change ☒ Timer Expiry

Timer 30 min (1-999)

**DND Zone**

Enable ☐

Configure the following parameters:

### 2-Person Rule

For this feature, valid credential of two people are required to access a secured area. It is typically used in high security areas or in areas where industrial safety is required.

**2-Person Rule**

Enable ☐

Primary Group

Secondary Group None

Mode Primary Must

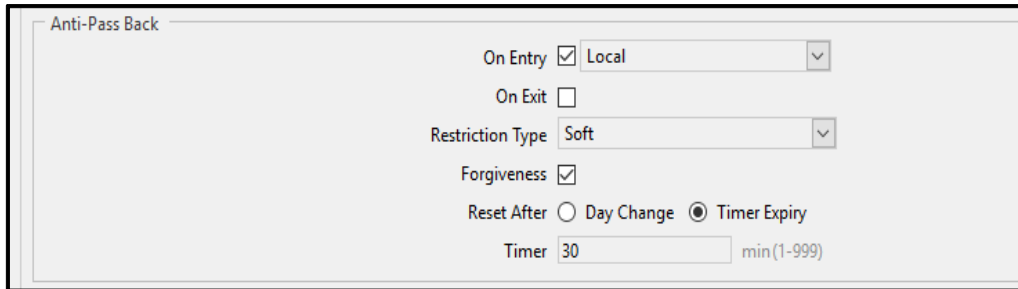
- **Enable:** Select the check box to enable.
- **Primary Group:** Select the desired Primary Group from the drop-down list. This is mandatory. A member from the Secondary Group always needs to be accompanied by a member from the Primary Group to be considered as valid users for accessing the door. However, any two members from the Primary Group are also considered as valid users for accessing the door. Make sure these groups are already configured. For details, refer to [“2-Person Rule”](#).
- **Secondary Group:** Select the desired Secondary Group from the drop-down list. A user from this group can be allowed access only if accompanied by a user from a Primary Group. If Secondary Group is selected as None then both members from Primary Group are required to access the door. Make sure these groups are already configured. For details, refer to [“2-Person Rule”](#).
- **Mode:** Select the desired mode — Primary Must, Primary and Secondary Must.
  - **Primary Must:** In this mode, the 2-Person Rule will grant access only when atleast 1 user belongs to the Primary Group, that is, the access is granted if both users are from Primary Group or 1 from

Primary and second from Secondary Group. The only situation when access will be denied is, when both the users are from the Secondary Group.

- **Primary and Secondary Must:** In this mode, the 2-Person Rule will grant access only in one condition, one user must belong to the Primary Group and the other must belong to the Secondary Group. In all other situations the access will be denied.

## Anti-Pass Back (APB)

The Anti-Pass Back or APB feature is used to ensure that users pass through an entry reader followed by an exit reader before their credential are accepted for the second time at another designated entry reader.



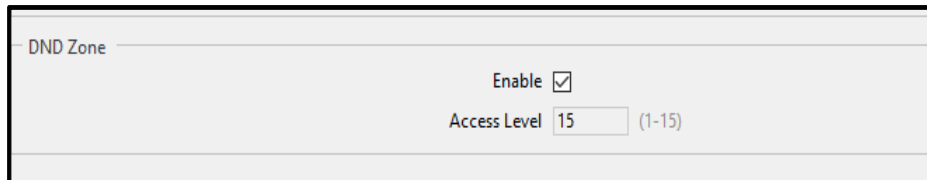
- **On Entry:** Select the check box to enable. The PANEL200 monitors the entry reader for APB violation. Select the desired option — Local or Global.
  - **Local:** If you select this option, the Anti-Pass Back feature will be applied at the Zone level.
  - **Global:** If you select this option, the Anti-Pass Back feature will be applied across all zones, that is, at the Panel level.
- **On Exit:** Select the check box to enable. The PANEL200 monitors the entry as well as the exit reader for APB violation.
- **Restriction Type:** Select the desired option — Hard, Soft — from the drop-down list.
  - **Hard APB:** The access to the user will be denied, if the previous exit is not registered. It does not allow a second entry using the same card without an exit.
  - **Soft APB:** The access to the user will be granted even if the previous exit is not registered. It allows a second entry of the same user without an exit. However, an event and a warning are generated that indicates the second entry.
- **Forgiveness:** Select this check box to enable. The PANEL200 will reset the APB status as per the selected option. Select the desired option:
  - **Reset After Day Change:** This will reset the APB status of all the users to Null at midnight. This enables a user, who left the building in the evening without exit punch, to use her/his card for entry the next morning.
  - **Reset After Timer Expiry:** This will reset the APB status of all the users after the expiry of the Forgiveness Timer.
    - **Forgiveness Timer (Mins):** Configure the duration in minutes after which Anti-Pass Back status should be reset for all the users.



If you have set Restriction Type as Hard, you can reset ABP using command from the Monitor. Click **Monitor**, for the PANEL, click **Select Command** under **Action**.

## DND Zone

DND Zone feature allows the you restrict user access to a particular zone for a specific time period thereby ensuring that the users inside the zone are not disturbed by others.



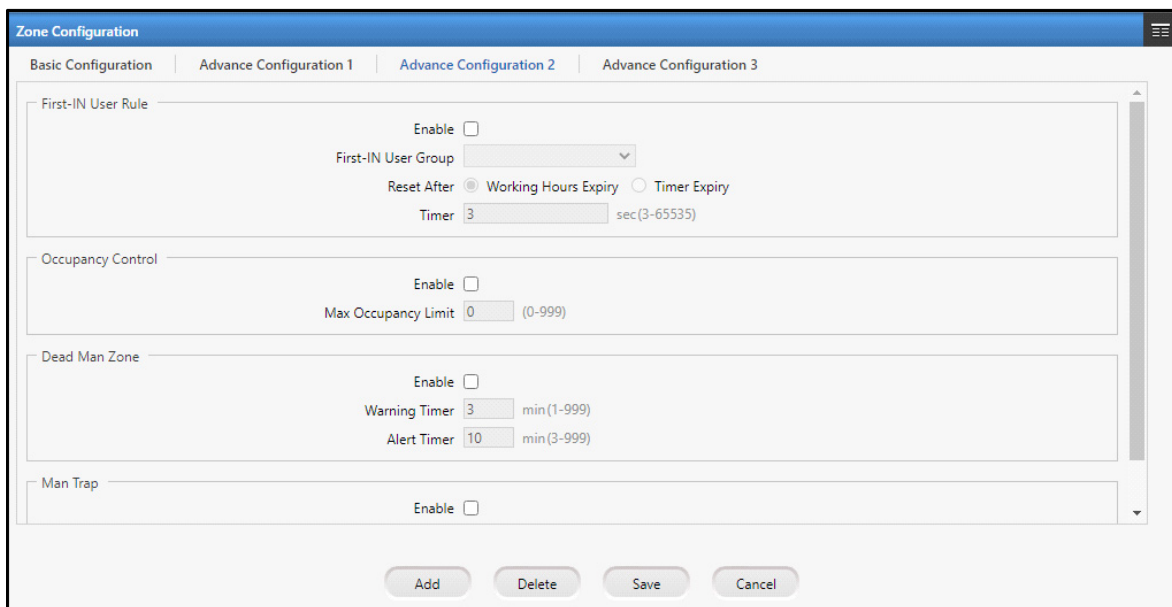
- **Enable:** Select the check box to enable. The DND can be enabled using a Special Card or through the door via the Menu on the display screen.
- **Access Level:** Configure the desired level. Make sure the DND Access Level is higher than the Zone Access Level so that the unwanted users are restricted to access the DND Zone.

Click **Save** to save the settings or click **Cancel** to discard.

## Advance Configuration 2

To configure the Advance Configuration 2 parameters,

Click **Panel Configuration > Zone Configuration > Advance Configuration 2**. The **Advance Configuration 2** page appears.

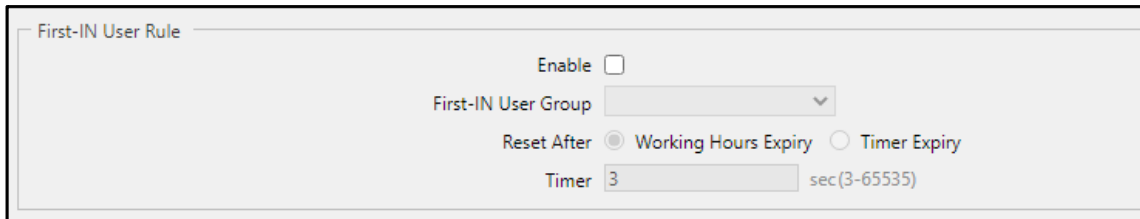


Configure the following parameters:

### First-IN User Rule

The First-IN user functionality enables the door to wait in locked mode till a valid First-IN user credential is detected whose effective working hours overlaps the current door time. As soon as the zone is unlocked using a First-IN user

credential, the PANEL200 allows access to that zone till the detected First-IN user's working hours or till the expiry of the timer. Once the time duration is over then PANEL200 deactivates the access to the designated zone and waits for another valid First-IN user's credentials.



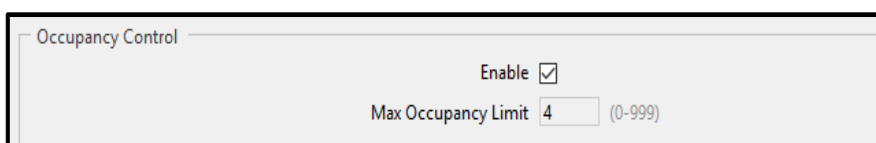
The screenshot shows a configuration window titled "First-IN User Rule". It contains the following fields and controls:

- Enable:** A checkbox that is currently unchecked.
- First-IN User Group:** A dropdown menu with a downward arrow.
- Reset After:** Two radio buttons. "Working Hours Expiry" is selected, and "Timer Expiry" is unselected.
- Timer:** A text input field containing the value "3", followed by the unit "sec(3-65535)".

- **Enable:** Select the check box to enable.
- **First-IN User Group:** Select the desired First-IN User Group from the drop-down list. Make sure the groups are already created. For details, refer to [“First-IN User Rule”](#).
- **Reset After:** Select the desired option — **Working Hours Expiry**, **Timer Expiry**.
  - **Working Hours Expiry:** If you select this option, then First-IN user's punch will remain valid till the working hours of First-IN user. After the expiry of the working hours, the First-IN user needs to punch again so that other users can access the premise.
  - **Timer Expiry:** If you select this option, then First-IN user's punch will remain valid till the expiry of the Timer.
    - **Timer:** Configure the duration in seconds. For this duration the First-IN user's punch will remain valid. After the expiry of the timer the First-IN user needs to punch again so that other users can access the premise.

## Occupancy Control

This functionality enables the monitoring and control of the number of users permitted within a secured area or controlled zone. It requires entry and exit readers in the controlled area.



The screenshot shows a configuration window titled "Occupancy Control". It contains the following fields and controls:

- Enable:** A checkbox that is checked.
- Max Occupancy Limit:** A text input field containing the value "4", followed by the range "(0-999)".

- **Enable:** Select the check box to enable.
- **Maximum Occupancy Limit:** Configure the maximum number of users allowed within the selected zone. For example, if maximum limit is set as 4, then when the 5th person tries to enter the zone, access to the zone will be denied.

## Dead Man Zone

It allows you to keep track of the safety and security of a user while performing a specific task, by making it mandatory for the user to present his/her card/finger/face on the door within a pre-defined time period.

Dead Man Zone

Enable ☒

Warning Timer  sec (1-999)

Alert Timer  min (3-999)

- **Enable:** Select the check box to enable.
- **Warning Timer (min):** Configure the duration in minutes. Within this duration the user inside the Dead Man Zone needs to present her/his card/finger/face to reset the timer and thus prevent the alarm.
- **Alert Timer (min):** Configure the maximum duration in minutes, for which the user is allowed to remain inside the Dead Man Zone.



**Warning Timer** specifies the minimum time within which user needs to come out and present his credentials.

**Alert Timer** specifies the maximum time for which user is allowed to remain in the dead man zone.

*In case, the presence of user is not marked at a predefined time an alarm is activated.*

*When the user enters into the zone, the Warning Timer and the Alert Timer will start. If the user comes out of the zone within the Alert time, then the alarm will reset else a warning alarm will be activated.*

## Man Trap

Mantrap provide safety, security and environmental control between two or more rooms by ensuring that opening any door causes all other doors to lock until the opened door returns to the closed position.

Man Trap

Enable ☒

Ignore Man Trap Timer ☐

- **Enable:** Select the check box to enable.
- **Ignore Man Trap Timer:** Select the check box, if you wish to ignore the Man Trap Wait Timer, that is, the Man Trap process will not use the Man Trap Wait Timer to open the next door, instead it will wait indefinitely for one door to close before the second door can open.

Click **Save** to save the settings or click **Cancel** to discard.

## Advance Configuration 3

To configure the Advance Configuration 3 parameters,

Click **Panel Configuration > Zone Configuration > Advance Configuration 3**. The **Advance Configuration 3** page appears.

Zone Configuration

Basic Configuration | Advance Configuration 1 | Advance Configuration 2 | Advance Configuration 3

Additional Security

Enable ☐

Smart Identification

Enable ☐

Access Mode Card

Add Delete Save Cancel

Configure the following parameters:

### Additional Security

The Additional Security Check (ASC) is possible only with Smart Cards, which will prevent usage of duplicate card and restrict unauthorized access to the facility. The user, who is assigned the zone enabled with ASC will be checked for ASC verification on the door.

Additional Security

Enable ☐

- **Enable:** Select the check box to enable.

### Smart Identification

This enables user identification in another office by means of Smart Card, though s/he is not enrolled in that particular office's system. For example, Employee working in Mumbai branch of a office can be identified on the door of the Delhi office using Smart Identification.

Smart Identification

Enable ☒

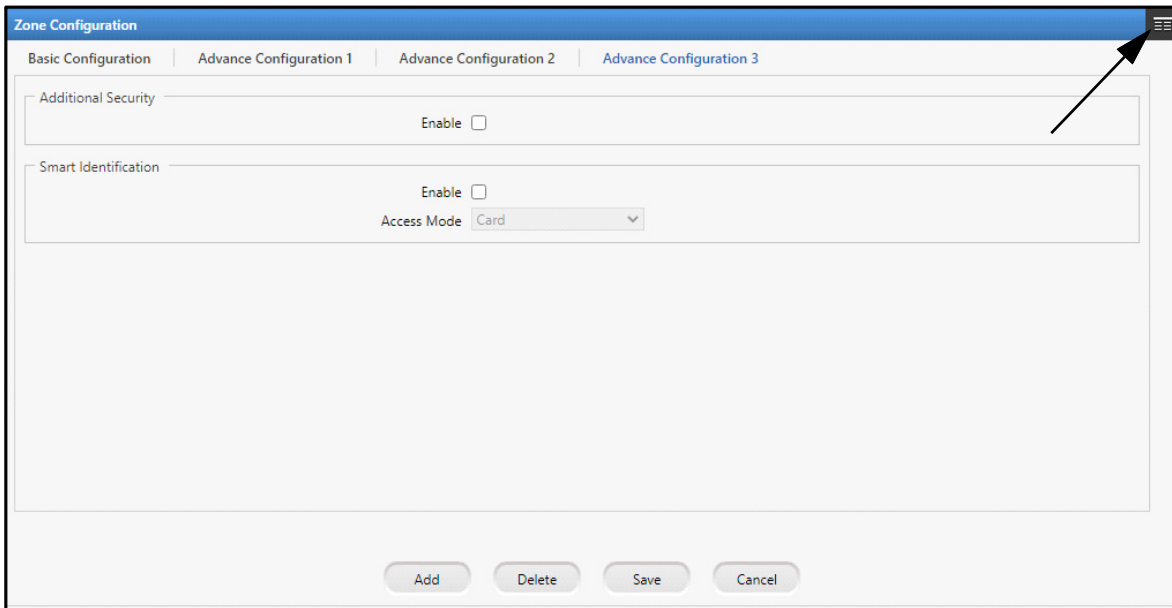
Access Mode Card

- Card
- Card+PIN
- Biometric+ Card
- Biometric+ Card+PIN

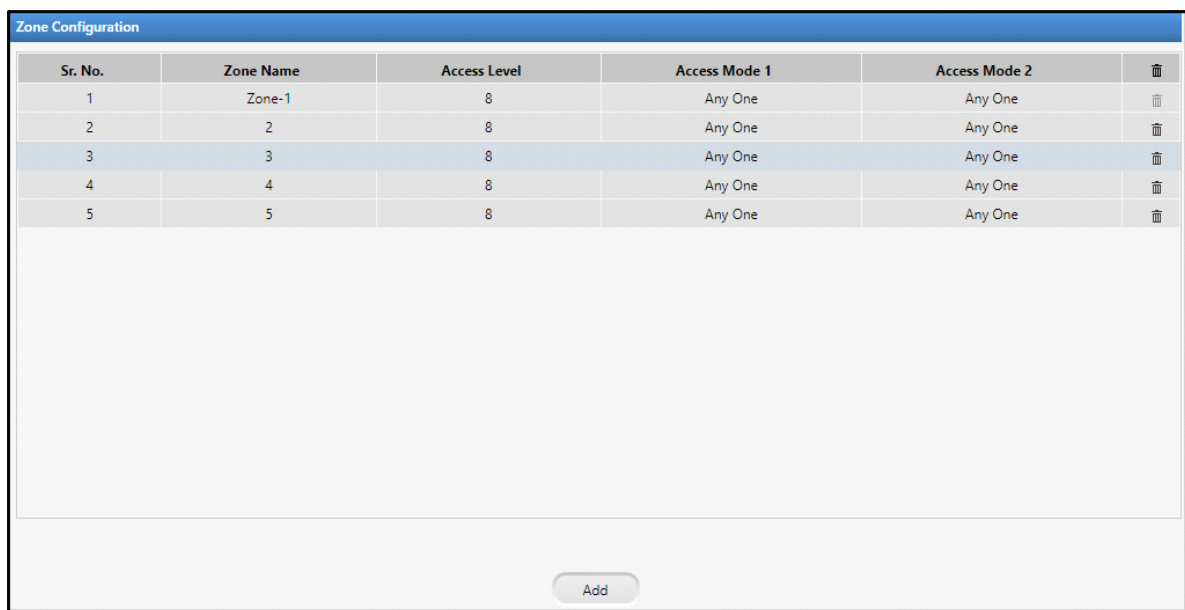
- **Enable:** Select the check box to enable.
- **Access Mode:** Select the desired access mode for Smart Card from the drop-down list. This enables identification of the user across multiple offices using the Smart Card, though the user is not enrolled in these office systems.

Click **Save** to save the settings or click **Cancel** to discard.

After you have completed all the configurations of the Zone, if you wish to view all the created Zones, click **View List** .



The Zone Configuration page appears with all the created Zones.



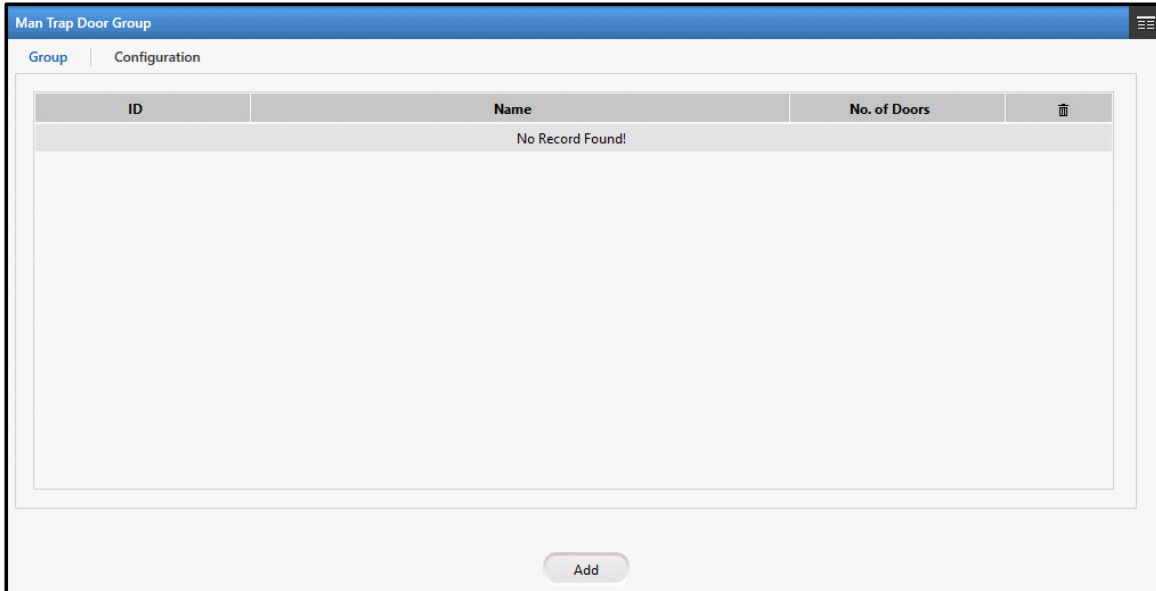
| Sr. No. | Zone Name | Access Level | Access Mode 1 | Access Mode 2 |                                                                                       |
|---------|-----------|--------------|---------------|---------------|---------------------------------------------------------------------------------------|
| 1       | Zone-1    | 8            | Any One       | Any One       |  |
| 2       | 2         | 8            | Any One       | Any One       |  |
| 3       | 3         | 8            | Any One       | Any One       |  |
| 4       | 4         | 8            | Any One       | Any One       |  |
| 5       | 5         | 8            | Any One       | Any One       |  |

# Man Trap Door Group

---

To configure the Man Trap Door Group parameters,

Click **Panel Configuration > Man Trap Door Group**. The **Man Trap Door Group** page appears.



All the created Man Trap Door Groups appear in the grid with their details — ID, Name and No. of Doors.

You can click the desired group and edit it as per your requirement or you can add new groups.

You can also delete any group. To do so, click **Delete**  corresponding to the desired group.

The Man Trap Door Group allows you to:

- configure the group parameters. For details, refer to [“Group”](#).
- configure the configuration parameters. For details, refer to [“Configuration”](#).

To add a Man Trap Door Group,

Click **Add**. You can create maximum **15** Man Trap Door Groups. Each group can have a maximum of **9** doors (except IO controllers).

## Group

| Door ID          | Door Name |  |
|------------------|-----------|--|
| No Record Found! |           |  |

Configure the following parameters:

- **Door Group ID:** The Door Group ID is auto-generated by the PANEL200.
- **Door Group Name:** Configure a name you wish to assign to the Man Trap Door Group.
- **Door:** Click the **Door** picklist. The **Panel Doors** pop-up appears. Select the door to be added to the group. You cannot add one door to multiple groups.

**OR**

You can also search for the desired door. To do so, enter the keyword in the Search box. Click **Search**

 . The doors will be filtered as per the keyword. Select the desired door.

The selected doors ID and Name appear.

- Click **Update** to add the selected door to the group.

Similarly, you can add another door to the group. These appear in the right pane.

| Door ID | Door Name |  |
|---------|-----------|--|
| 6       | VEGA      |  |
| 15      | ARGO      |  |

You can delete any added door. To do so, click **Delete**  corresponding to the desired door.

- Click **Save**.

## Configuration

To configure the Configuration parameters,

Click **Panel Configuration > Man Trap Door Group > Configuration**. The **Configuration** page appears.

Man Trap Door Group 1 Man Trap Group1

Enable Man Trap ☒

Enable Strict Man Trap ☒

Save

- **Man Trap Door Group:** Click the **Man Trap Door Group** picklist. The **Man Trap Door Group** pop-up appears. Select the desired door group on which you wish to enable Man Trap.

OR



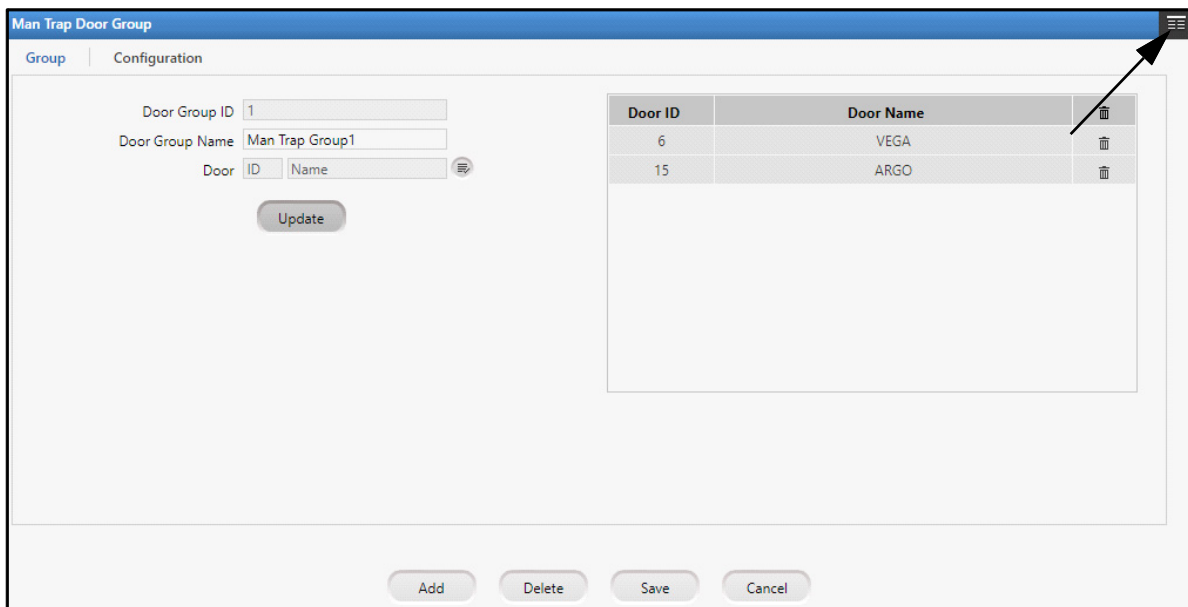
You can also search for the desired group. To do so, enter the keyword in the Search box. Click **Search**

 . The groups will be filtered as per the keyword. Select the desired door group on which you wish to enable Man Trap.

- **Enable Man Trap:** Select the check box to enable the Man Trap on the selected door group. When one door is opened then all other doors of the group will remain locked until the wait timer expires. If the user tries to access the other door after the expiry of the timer then user will be allowed to access the door. Make sure, you have configured the Man Trap parameters in “Set2” in “Access Features”.
- **Enable Strict Man Trap:** Select the check box to enable Strict Man Trap. In this case, the Man Trap process will not use the Wait Timer to open the next door. Instead it will indefinitely wait for one door to close before the second door can open.
- Click **Save** to save the settings.

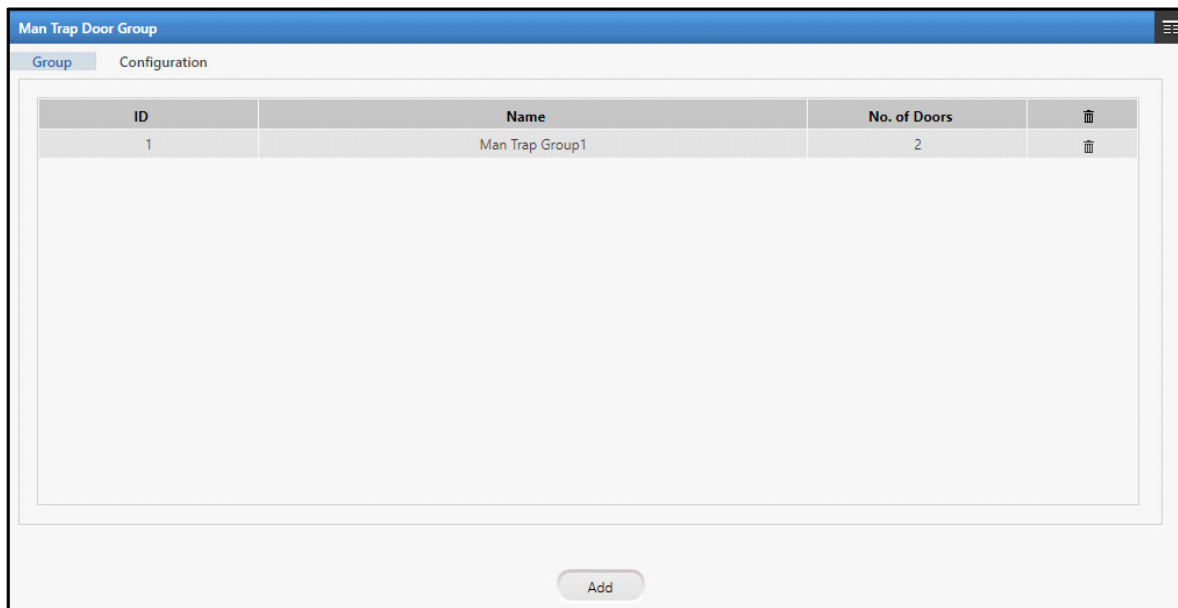
After you have completed all the configurations of the Man Trap Door Group and if you wish to view all the created

Man Trap Door Groups, click **View List**  .



| Door ID | Door Name |                                                                                       |
|---------|-----------|---------------------------------------------------------------------------------------|
| 6       | VEGA      |   |
| 15      | ARGO      |  |

The Man Trap Door Group page displays all the created Man Trap Door Groups.



You can delete any created Man Trap Door Group. To do so, click **Delete**  corresponding to the desired Man Trap Door Group.

# Network Settings

The Network Settings allows you to:

- configure the lan settings. For details, refer to “[LAN Settings](#)”.
- configure the advanced lan settings. For details, refer to “[Advanced LAN Settings](#)”.
- configure the Wi-Fi network settings. For details, refer to “[Wi-Fi Network Settings](#)”.
- configure the Wi-Fi access point settings. For details, refer to “[Wi-Fi Access Point Settings](#)”.
- configure the mobile broadband settings. For details, refer to “[Mobile Broadband](#)”.
- configure the DDNS settings. For details, refer to “[DDNS](#)”.
- configure the Matrix DNS settings. For details, refer to “[Matrix DNS](#)”.

## LAN Settings

To configure the LAN Settings parameters,

Click **Panel Configuration > Network Settings > LAN Settings**. The **LAN Settings** page appears.

The screenshot shows the 'Network Settings' interface with the 'LAN Settings' tab selected. The configuration fields are as follows:

| Parameter       | Value             |
|-----------------|-------------------|
| IP Assignment   | Static            |
| IP Address      | 192.168.103.228   |
| MAC Address     | 00:1b:09:08:7b:d5 |
| Subnet Mask     | 255.255.255.0     |
| Default Gateway | 192.168.103.228   |
| Preferred DNS   | 192.168.103.1     |
| Alternate DNS   |                   |

Below the configuration fields is a 'Test Network Connection' section with an 'Enter URL' input field and a 'Test' button.

Configure the following parameters:

- **IP Assignment:** Select the IP Assignment option from the drop-down list — Static, DHCP.

If you select the IP Assignment option as **DHCP**, the IP Address, Subnet Mask, Default Gateway, Preferred and Alternate DNS are automatically assigned by the DHCP Server.

If you select the IP Assignment option as **Static**, configure the following:

- **IP Address:** Configure the IP Address.
- **MAC Address:** It displays the MAC Address of PANEL200.
- **Subnet Mask:** Configure the Subnet Mask.
- **Default Gateway:** Configure the Default Gateway.
- **Preferred DNS:** Configure the Preferred DNS.
- **Alternate DNS:** Configure the Alternate DNS.

## Test Network Connection

- **Enter URL:** Configure the URL and click **Test** to test the network connection of PANEL200.

Click **Save** to save the configuration or click **Cancel** to discard.

## Advanced LAN Settings

To configure the Advanced LAN Settings parameters,

Click **Panel Configuration > Network Settings > Advanced LAN Settings**. The **Advanced LAN Settings** page appears.



*If you have upgraded the PANEL Firmware with 802.1X Settings enabled and later you downgrade the PANEL Firmware, the PANEL webpages will not be accessible from the Network Switch. To access the PANEL webpages, disable 802.1X Settings in the Network Switch.*

## Pre-Requisites

To configure 802.1X Settings, make sure the following Pre-requisites are met:

- A **RADIUS Server** is installed on a PC with Linux OS. This PC and the PANEL must be in the same network.
- PANEL is connected to a Network Switch with 802.1X Authentication support.
- Device Identity is configured in **RADIUS Server** for establishing authentication between PANEL and RADIUS Server.



*Make sure you have enabled 802.1X Settings in the PANEL prior to connecting the same to a Network Switch with 802.1X Authentication support.*

*Make sure **MAC Authentication Bypass (MAB)** is not enabled in your Network Switch.*

Configure the following parameters:

## 802.1X Settings

- **Enable:** Select the check box to enable.
- **Authentication Method:** It displays EAP-TLS and is un-editable.

- **Anonymous Identity:** If you wish that the PANEL should be displayed as an Anonymous Identity in the RADIUS Server, configure the same. In this the identity of PANEL200 will not be disclosed. This be used for display purpose only and not for communication.
- **Identity:** Configure the PANEL's Identity as configured in the RADIUS Server. When PANEL is connected to the Network Switch, it sends this identity to the RADIUS Server. The RADIUS Server matches this identity with the one it already has to validate the PANEL's Identity.

If there is a mismatch between the PANEL's Identify configured in RADIUS Server and the one configured here, then the PANEL's Identity will not be validated by the RADIUS Server. Hence, communication between PANEL and RADIUS Server will not be established.

- **Device Certificate:** Click **Browse**  and select the path from where you wish to upload the Device Certificate. The supported formats are —.pem, .crt, .cer, .pfx and .p12. The maximum file size can be 10 KB. Click **Upload**  to upload the certificate. The Device Certificate is used by RADIUS Server for validation. For details, refer to ["Authentication Process between PANEL and RADIUS Server"](#).

A Bundled Certificate can have Device Certificate, Private Key and CA Certificate or can have only Device Certificate and Private Key. If you have a Bundled Certificate, you need to upload it here.

If you wish to remove the Device Certificate, click **Delete** .

- **Private Key:** Click **Browse**  and select the path from where you wish to upload the Private Key. The supported format is .key. The maximum file size can be 10 KB. Click **Upload**  to upload the key. If you wish to remove the Private Key, click **Delete** .

- **Private Key Password:** Configure the Private Key Password.
- **Upload CA Certificate:** Click **Browse**  and select the path from where you wish to upload the CA Certificate. The supported formats are —.pem, .crt, .cer, .pfx and .p12. The maximum file size can be 10 KB. Click **Upload**  to upload the certificate. The CA Certificate is used by PANEL for validation. For details, refer to ["Authentication Process between PANEL and RADIUS Server"](#). If you wish to remove the CA Certificate, click **Delete** .

Click **Save** to save the configuration or click **Cancel** to discard. Once the identity of PANEL is validated by the RADIUS Server, the authentication process between PANEL and RADIUS Server begins.

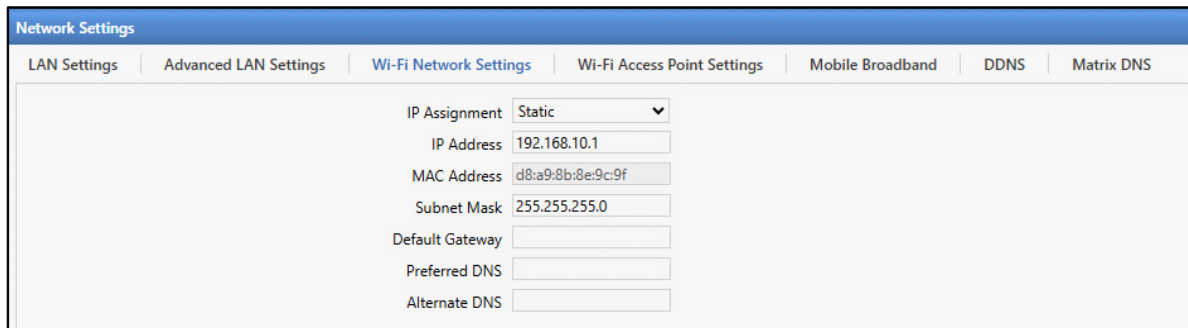
## Authentication Process between PANEL and RADIUS Server

- RADIUS Server sends its CA Certificate to PANEL.
- PANEL validates the RADIUS Server using its uploaded CA Certificate.
- If RADIUS Server's Certificate is valid, then PANEL sends its Device Certificate to RADIUS Server.
- RADIUS Server validates the PANEL's Device Certificate using its installed CA Certificate.
- If the PANEL's Device Certificate is valid, the RADIUS Server communicates to the Network Switch that the PANEL is Authorized.
- The Network Switch will communicate the same to the PANEL.
- Once both certificates are valid, a TLS communication is established. PANEL can now securely communicate over the network using TLS encryption.

## Wi-Fi Network Settings

To configure the Wi-Fi Network Settings parameters,

Click **Panel Configuration > Network Settings > Wi-Fi Network Settings**. The **Wi-Fi Network Settings** page appears.

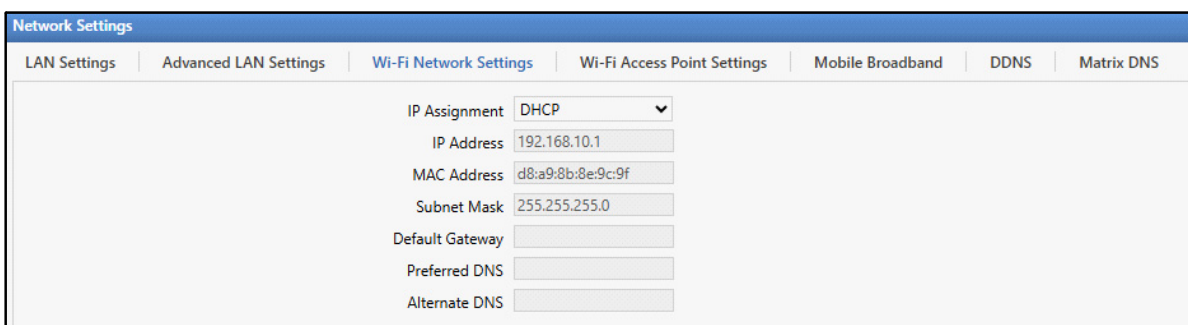


The screenshot shows the 'Network Settings' page with the 'Wi-Fi Network Settings' tab selected. The 'IP Assignment' dropdown is set to 'Static'. The following fields are visible:

| Field           | Value             |
|-----------------|-------------------|
| IP Assignment   | Static            |
| IP Address      | 192.168.10.1      |
| MAC Address     | d8:a9:8b:8e:9c:9f |
| Subnet Mask     | 255.255.255.0     |
| Default Gateway |                   |
| Preferred DNS   |                   |
| Alternate DNS   |                   |

Configure the following parameters:

- **IP Assignment:** You can select the IP Assignment mode as Static or DHCP.
- **Static:** If you select this option, configure the IP Address, Subnet mask, Default Gateway, Preferred DNS and Alternate DNS for Wi-Fi access.
- **DHCP:** If you select this option, the IP Address and Subnet Mask for Wi-Fi access will be assigned dynamically by the Wi-Fi Router. When PANEL200 is being connected through Wi-Fi, make sure the IP Assignment mode is set as DHCP. To search and select the desired networks, refer to [“Wi-Fi Access Point Settings”](#). After you select the desired Wi-Fi with which you wish to connect and the connection is established, all the DHCP network settings will be assigned to the PANEL200. Now, change the IP Addressing Mode to Static.



The screenshot shows the 'Network Settings' page with the 'Wi-Fi Network Settings' tab selected. The 'IP Assignment' dropdown is set to 'DHCP'. The following fields are visible:

| Field           | Value             |
|-----------------|-------------------|
| IP Assignment   | DHCP              |
| IP Address      | 192.168.10.1      |
| MAC Address     | d8:a9:8b:8e:9c:9f |
| Subnet Mask     | 255.255.255.0     |
| Default Gateway |                   |
| Preferred DNS   |                   |
| Alternate DNS   |                   |

Click **Save** to save the settings or click **Cancel** to discard.

## Wi-Fi Access Point Settings

The Wi-Fi Access Point supports wireless connection for communicate between the PANEL200 and the PANEL200 web page.

To configure the Wi-Fi Network Settings parameters,

Click **Panel Configuration > Network Settings > Wi-Fi Access Point Settings**. The **Wi-Fi Access Point Settings** page appears.

The screenshot shows the 'Wi-Fi Access Point Settings' page within the 'Network Settings' section. The page has a blue header with the title 'Network Settings' and a tabbed interface with the following tabs: LAN Settings, Advanced LAN Settings, Wi-Fi Network Settings, Wi-Fi Access Point Settings (selected), Mobile Broadband, DDNS, and Matrix DNS. The main content area is divided into two columns. The left column contains three sections: 1. 'Wi-Fi' with a checkbox, 'Connection Status' text, 'SSID (Network Name)' text input, and 'Security Type' dropdown menu (set to 'No Authentication'). 2. 'WPS Settings' with 'WPS Push Button' (checked) and 'WPS PIN From Device' (disabled). 3. 'Test Network Connection' with 'Enter URL' text input and a 'Test' button. The right column contains a 'Search Network' button with a magnifying glass icon. At the bottom of the page are 'Save' and 'Cancel' buttons.

Configure the following parameters:

- **Wi-Fi:** Select the check box. You can either insert the Wi-Fi dongle in your PANEL200 or search for the Wi-Fi networks available in your network.

Click **Search Network**  to search for the available Wi-Fi networks or can use "[WPS Settings](#)" to establish connection.

The screenshot shows the 'Network Settings' window with the 'Wi-Fi Network Settings' tab selected. On the left, there are configuration fields for Wi-Fi, including a checked 'Wi-Fi' checkbox, 'Connection Status' (Not Connected), 'SSID (Network Name)' (MYNET\_OFFICE), 'Security Type' (WPA2 Enterprise), 'Encryption Type' (EAP), 'Advance Authentication' (PEAP), 'Anonymous Identity', 'User Name' (admin), 'PEAP Version' (Auto), 'Inner Authentication' (Auto), and a 'Security Key' field. Below these are 'WPS Settings' with 'WPS Push Button' and 'WPS PIN From Device' options. On the right, a table lists available Wi-Fi networks. At the bottom are 'Save' and 'Cancel' buttons.

| No. | SSID         | Security Type | Status | Strength | Select                           |
|-----|--------------|---------------|--------|----------|----------------------------------|
| 1   | MYNET_OFFICE | Secure        |        | Moderate | <input checked="" type="radio"/> |
| 2   | DEFAULT_FR   | Secure        |        | Moderate | <input type="radio"/>            |
| 3   | MYNET_OFFICE | Secure        |        | Weak     | <input type="radio"/>            |
| 4   | MYNET_OFFICE | Secure        |        | Weak     | <input type="radio"/>            |
| 5   | NETGEAR78    | Secure        |        | Weak     | <input type="radio"/>            |
| 6   | DEFAULT_FR   | Secure        |        | Weak     | <input type="radio"/>            |
| 7   | <hidden>     | Secure        |        | Moderate | <input type="radio"/>            |
| 8   | MY-WIFI-TEST | Open          |        | Weak     | <input type="radio"/>            |
| 9   | MyNet_Guest  | Open          |        | Moderate | <input type="radio"/>            |
| 10  | MyNet_Guest  | Open          |        | Weak     | <input type="radio"/>            |
| 11  | MyNet_Guest  | Open          |        | Weak     | <input type="radio"/>            |

The list of Wi-Fi networks appear in the right pane.

Select the radio button of the desired Wi-Fi network with which you wish to establish connectivity.

- **Connection Status:** It displays the connectivity status of the PANEL200 with the Wi-Fi Network. The Wi-Fi Signal Strength  will display the real-time signal strength of the selected network.
- **SSID:** This will be fetched automatically when the connectivity is established with the selected network.
- **Security Type:** This will be fetched automatically when you select the desired network and it is a secure network.
- **Encryption Type:** This will be fetched automatically when you select the desired network and it is a secure network.
- **Security Key:** You need to configure the Security Key of the Wi-Fi device here for authentication.

When the connection with Wi-Fi is established, **Connection Status** will display Connected.

For example, if you are the mobile as hotspot, Security Type will display WPA-2 personal and you need to enter your hotspot password in Security Key.



**Network Settings**

LAN Settings | Advanced LAN Settings | **Wi-Fi Network Settings** | Wi-Fi Access Point Settings | Mobile Broadband | DDNS | Matrix DNS

Wi-Fi ☒

Connection Status: Connected

SSID (Network Name): OnePlus Nord CE 5G

Security Type: WPA - 2 personal

Encryption Type: PSK

Security Key: .....

WPS Settings

WPS Push Button ☒

WPS PIN From Device ☐

Test Network Connection

Enter URL:  Test

| No. | SSID                  | Security Type | Status | Strength | Select                |
|-----|-----------------------|---------------|--------|----------|-----------------------|
| 1   | OnePlus Nord CE 5G    | Secure        |        | Weak     | <input type="radio"/> |
| 2   | DEFAULT_FR            | Secure        |        | Strong   | <input type="radio"/> |
| 3   | MYPNET_OFFICE         | Secure        |        | Moderate | <input type="radio"/> |
| 4   | Galaxy S23 Ultra D560 | Secure        |        | Weak     | <input type="radio"/> |
| 5   | vivo 1609             | Secure        |        | Weak     | <input type="radio"/> |
| 6   | MYPNET_OFFICE         | Secure        |        | Weak     | <input type="radio"/> |
| 7   | DEFAULT_FR            | Secure        |        | Weak     | <input type="radio"/> |
| 8   | DEFAULT_FR            | Secure        |        | Weak     | <input type="radio"/> |
| 9   | MYPNET_OFFICE         | Secure        |        | Weak     | <input type="radio"/> |
| 10  | DEFAULT_FR            | Secure        |        | Weak     | <input type="radio"/> |

Search Network

Save Cancel

In some Routers no authentication may be required.

**Network Settings**

LAN Settings | Advanced LAN Settings | **Wi-Fi Network Settings** | Wi-Fi Access Point Settings | Mobile Broadband | DDNS | Matrix DNS

Wi-Fi ☒

Connection Status: Not Connected

SSID (Network Name): MYPNET\_OFFICE

Security Type: No Authentication

WPS Settings

WPS Push Button ☒

WPS PIN From Device ☐

Test Network Connection

Enter URL:  Test

| No. | SSID          | Security Type | Status | Strength | Select                           |
|-----|---------------|---------------|--------|----------|----------------------------------|
| 1   | MYPNET_OFFICE | Secure        |        | Moderate | <input checked="" type="radio"/> |
| 2   | DEFAULT_FR    | Secure        |        | Moderate | <input type="radio"/>            |
| 3   | MYPNET_OFFICE | Secure        |        | Weak     | <input type="radio"/>            |
| 4   | MYPNET_OFFICE | Secure        |        | Weak     | <input type="radio"/>            |
| 5   | NETGEAR78     | Secure        |        | Weak     | <input type="radio"/>            |
| 6   | DEFAULT_FR    | Secure        |        | Weak     | <input type="radio"/>            |
| 7   | <hidden>      | Secure        |        | Moderate | <input type="radio"/>            |
| 8   | MY-WIFI-TEST  | Open          |        | Weak     | <input type="radio"/>            |
| 9   | MyNet_Guest   | Open          |        | Moderate | <input type="radio"/>            |
| 10  | MyNet_Guest   | Open          |        | Weak     | <input type="radio"/>            |
| 11  | MyNet_Guest   | Open          |        | Weak     | <input type="radio"/>            |

Search Network

Save Cancel

## WPS Settings

WPS can be used if the Router is accessible. WPS Settings support 2 types of connections:

### WPS Push Button

This option can be used when the Router also has the WPS Push Button support. To use this option,

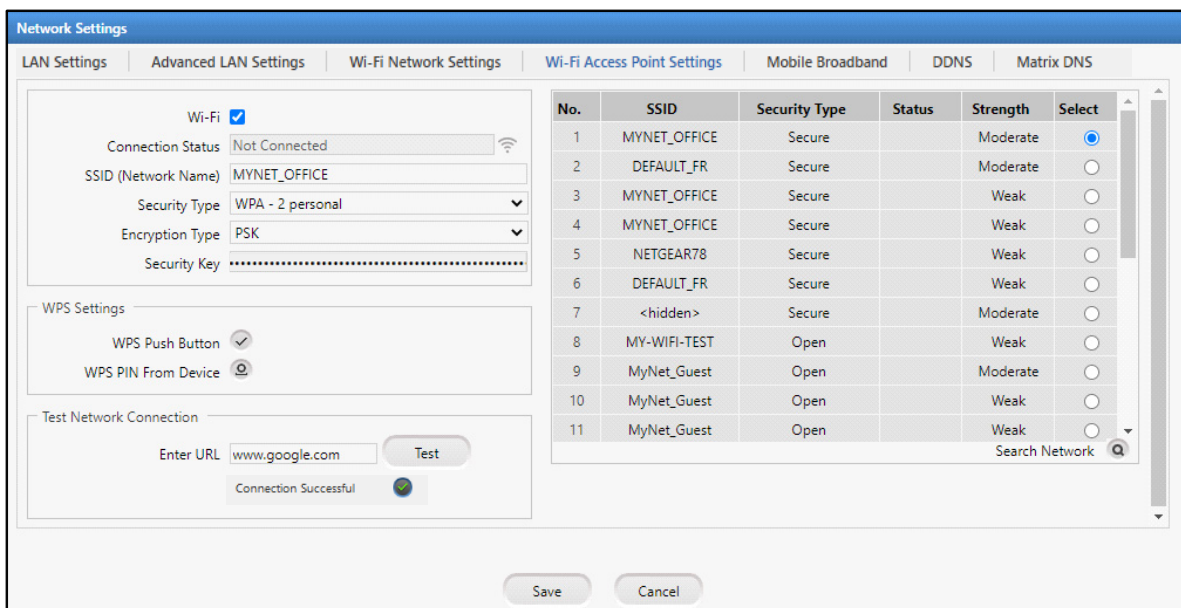
- Click **WPS Push Button** ☒. The PANEL200 will try to establish a connection with the Router for 2 minutes. Make sure you press the WPS Push Button on the Router within 2 minutes, only then the connectivity will be established with the PANEL200.

## WPS PIN from Device

- Click **WPS PIN from Device** . The PANEL200 will generate a random 9 digit PIN and displays it. Make sure this PIN is configured in the Registrar Configuration of the Router within 2 minutes, only then the connectivity will be established with the PANEL200.

The Wi-Fi Access Points parameters will be automatically updated according to the Wi-Fi network with which the connectivity is established.

## Test Network Connection



The screenshot shows the 'Network Settings' page with the following sections:

- Wi-Fi:** Checked. Connection Status: Not Connected. SSID (Network Name): MYNET\_OFFICE. Security Type: WPA - 2 personal. Encryption Type: PSK. Security Key: [Redacted].
- WPS Settings:** WPS Push Button: [Checked]. WPS PIN From Device: .
- Test Network Connection:** Enter URL: www.google.com. Test button. Connection Successful: [Green checkmark].
- Wi-Fi Access Point Settings Table:**

| No. | SSID         | Security Type | Status | Strength | Select                           |
|-----|--------------|---------------|--------|----------|----------------------------------|
| 1   | MYNET_OFFICE | Secure        |        | Moderate | <input checked="" type="radio"/> |
| 2   | DEFAULT_FR   | Secure        |        | Moderate | <input type="radio"/>            |
| 3   | MYNET_OFFICE | Secure        |        | Weak     | <input type="radio"/>            |
| 4   | MYNET_OFFICE | Secure        |        | Weak     | <input type="radio"/>            |
| 5   | NETGEAR78    | Secure        |        | Weak     | <input type="radio"/>            |
| 6   | DEFAULT_FR   | Secure        |        | Weak     | <input type="radio"/>            |
| 7   | <hidden>     | Secure        |        | Moderate | <input type="radio"/>            |
| 8   | MY-WIFI-TEST | Open          |        | Weak     | <input type="radio"/>            |
| 9   | MyNet_Guest  | Open          |        | Moderate | <input type="radio"/>            |
| 10  | MyNet_Guest  | Open          |        | Weak     | <input type="radio"/>            |
| 11  | MyNet_Guest  | Open          |        | Weak     | <input type="radio"/>            |

Search Network 

Save Cancel

- Enter URL:** After configuring the above parameters, you can test the network connectivity. Configure the desired the URL.
- Click **Test**.

Click **Save** to save the settings or click **Cancel** to discard.

## Mobile Broadband

The PANEL200 can be connected to the internet (wireless connectivity) using Mobile Broadband via USB dongle. Make sure the USB dongle is inserted into the USB port of the PANEL200.

To configure the Mobile Broadband parameters,

Click **Panel Configuration > Network Settings > Mobile Broadband**. The **Mobile Broadband** page appears.

The screenshot shows the 'Network Settings' window with the 'Mobile Broadband' tab selected. It contains a table of modem profiles and a section for connection details.

| Active                           | Profile Name | Dial Number | User Name | Password | Service | APN            | Preferred Port |
|----------------------------------|--------------|-------------|-----------|----------|---------|----------------|----------------|
| <input checked="" type="radio"/> | Airtel       | *99#        |           |          | GSM     | airtelgprs.com | None           |
| <input type="radio"/>            | Bsnl         | *99***1#    |           |          | GSM     | bsnlnet        | None           |
| <input type="radio"/>            | Vodafone     | *99#        |           |          | GSM     | www            | None           |
| <input type="radio"/>            | TATA Photon+ | #777        | internet  | .....    | CDMA    |                | None           |
| <input type="radio"/>            | Reliance     | #777        |           |          | CDMA    |                | None           |

Below the table is the 'Connection Details' section with the following fields:

- Connection Status: No Modem
- IP Address:
- Default Gateway:
- Preferred DNS:
- Alternate DNS:

At the bottom is the 'Test Network Connection' section with a text input for 'Enter URL' (containing 'www.google.com') and a 'Test' button.

You can configure multiple mobile broadband modem profiles. The dongle options are Airtel, BSNL, Vodafone, TATA Photon+ and Reliance. After connecting the broad band dongle, select the profile of the desired service provider.

Configure the following parameters:

- **Profile Name:** By default the name of the service provider is displayed. You can edit the same, if required.
- **Dial Number:** Configure the number that needs to be dialed to establish connectivity
- **User Name:** Configure the user name for authentication.
- **Password:** Configure the password for authentication.
- **Service:** Select the desired type of service — GSM, CDMA.
- **ANP:** If you select GSM as the Service, configure the APN (Access Point Name), that is, the URL to be used to access the respective service provider.
- **Preferred Port:** Click **Select Port** . The **Select a Port** pop-up appears. Select the desired COM Port using which the PANEL200 will communicate with the dongle.

## Connection Details

When the connection is established the following details of the selected Profile will be displayed — **Connection Status**, **IP Address**, **Default Gateway**, **Preferred DNS** and **Alternate DNS** Address.

## Test Network Connection

- **Enter URL:** After configuring the above parameters, you can test the network connectivity. Configure the desired the URL.

- Click **Test**.

Click **Save** to save the settings or click **Cancel** to discard.

## DDNS

Dynamic DNS (DDNS) is a service that maps internet domain names to IP Addresses. DDNS Service Provider provides the host name/domain name to the internet devices and also embed DDNS client in the internet device. By doing so, whenever a new IP Address is assigned to internet host, the DDNS client running on the internet host updates its new IP Address in the Dynamic DNS Server.

The DDNS enables you to register PANEL200 on DDNS Server by configuring its Host Name. DDNS Server will resolve the IP Address of configured Host Name and will map the same with the IP Address also. Whenever, the Public IP Address of PANEL200 changes it will be updated automatically in DDNS Server.

Once the IP Address is updated in the DDNS Server, you can access the PANEL200 using the host name/domain.



*This feature will work for LAN interface only.*

Before configuring DDNS settings, check the Internet connectivity from LAN Settings page by entering the URL: [www.google.com](http://www.google.com). Once the connection is successful, the PANEL200 is connected with Internet.

The screenshot displays the 'Network Settings' window with several tabs: LAN Settings, Advanced LAN Settings, Wi-Fi Network Settings, Wi-Fi Access Point Settings, Mobile Broadband, DDNS, and Matrix DNS. The 'LAN Settings' tab is active, showing fields for IP Assignment (Static), IP Address (192.168.103.228), MAC Address (00:1b:09:08:7b:d5), Subnet Mask (255.255.255.0), Default Gateway (192.168.103.228), Preferred DNS (192.168.103.1), and Alternate DNS. Below this, the 'Test Network Connection' section contains an 'Enter URL' field with 'www.google.com', a 'Test' button, and a status indicator showing 'Connection Successful' with a globe icon.

To configure the DDNS parameters,

Click **Panel Configuration > Network Settings > DDNS**. The **DDNS** page appears.

Network Settings

LAN Settings | Advanced LAN Settings | Wi-Fi Network Settings | Wi-Fi Access Point Settings | Mobile Broadband | **DDNS** | Matrix DNS

Enable ☐

DDNS Server: DynDNS

User Name:

Password:

Host Name:

Update Interval: 5 min(5-99)

Default Save Cancel

Configure the following parameters:

- **Enable:** Select the check box to enable the registration of Host Name on the DDNS Server.
- **DDNS Server:** DynDNS is displayed and it is un-editable.
- **User Name:** Configure the user name you created on DynDNS.org here.
- **Password:** Configure the password you created on DynDNS.org here.
- **Host Name:** Configure the host name you created on DynDNS.org here. For example: **cosecdevice.dyndns.org**. The PANEL200 can be accessed using this Host Name.

https://account.dyn.com/dns/

Dyn

Back to Dyn | Welcome devanand | My Services | My Cart | Log Out | Search Dyn | SUPPORT | ABOUT

My Account

My Services

DynDNS Pro/Hosts

Managed DNS Express

Domain names, DNS hosting, Dyn Email services

Health Check

Email Delivery Express

Renew Services

Auto Renew Settings

Sync Expirations

Tips on Getting Started

Account Settings

Billing

My Cart 0 Items

DNS Services

DYNDNS HOSTNAMES + Add New Hostname

| HOSTNAME                                  | SERVICE | DETAILS         | LAST UPDATED           |
|-------------------------------------------|---------|-----------------|------------------------|
| <a href="#">cosecdevice.dyndns.org</a>    | Host    | 180.211.118.106 | Jul. 11, 2018 5:43 PM  |
| <a href="#">ipvsqa.dyndns.org</a>         | Host    | 180.211.118.106 | Jul. 09, 2018 8:45 AM  |
| <a href="#">ipvsqatest.dyndns.org</a>     | Host    | 180.211.118.106 | Jun. 25, 2018 3:42 PM  |
| <a href="#">matrixipcamera.dyndns.org</a> | Host    | 186.65.12.123   | Mar. 06, 2018 12:26 PM |
| <a href="#">nrv6404xqa.dyndns.org</a>     | Host    | 180.211.118.106 | Jun. 25, 2018 11:33 AM |
| <a href="#">qatelecom.dyndns.org</a>      | Host    | 192.168.105.55  | Jun. 19, 2018 12:19 PM |

> Host Update Logs

> Bulk Update IP Address And Service Type

- **Update Interval:** Configure the duration in minutes after which PANEL200 will send its Public IP Address to the DDNS Server. The same will be updated, if it is found to be different than the one registered.

Click **Save** to save the settings or click **Cancel** to discard.

Network Settings

LAN Settings | Advanced LAN Settings | Wi-Fi Network Settings | Wi-Fi Access Point Settings | Mobile Broadband | **DDNS** | Matrix DNS

Enable ☒

DDNS Server: DynDNS

User Name: admin

Password: .....

Host Name: cosecdevice.dyndns.com

Update Interval: 5 min (5-99)

Now, you can log into the DDNS Server by entering URL **account.dyndns.com** and view the registration of Host Name. The PANEL200 is registered by the Host Name with its Public IP Address.

https://account.dyn.com/dns/dyndns/auxlanglog.html

Dyn

Back to Dyn | Welcome devanand | My Services | My Cart | Log Out

Search Dyn

SUPPORT | ABOUT

My Account

My Services

- DynDNS Pro/Hosts
- Managed DNS Express
- Domain names, DNS hosting, Dyn Email services
- Health Check
- Email Delivery Express
- Renew Services
- Auto Renew Settings
- Sync Expirations
- Tips on Getting Started

Account Settings

Billing

My Cart 0 items

Host Update Logs Viewer

Displayed are your 100 last updates within the last 5 days. Log entries may take 10-15 minutes to appear.

| Time                | Host                   | IP              | Params                                                                                             | Client                                  | Response              |
|---------------------|------------------------|-----------------|----------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------|
| 2018-07-11 16:02:20 | cosecdevice.dyndns.org | 111.93.228.226  | backmx=NO<br>mx=cosecdevice.dyndns.org<br>offline=NO<br>system=dyndns<br>wildcard=OFF<br>backmx=NO | inadyn/1.98.1<br>troglodite@vmlinux.org | good 111.93.228.226   |
| 2018-07-11 16:02:17 | cosecdevice.dyndns.org | 180.211.118.106 | mx=cosecdevice.dyndns.org<br>offline=NO<br>system=dyndns<br>wildcard=ON<br>backmx=NO               | inadyn/1.96<br>inarcis2002@hotmail.com  | nochg 180.211.118.106 |
| 2018-07-11 16:00:14 | cosecdevice.dyndns.org | 180.211.118.106 | mx=cosecdevice.dyndns.org<br>offline=NO<br>system=dyndns<br>wildcard=ON<br>backmx=NO               | inadyn/1.96<br>inarcis2002@hotmail.com  | good 180.211.118.106  |

You can access the PANEL200 by entering host name for example, cosecdevice.dyndns.org in the browser.

## Matrix DNS

The Matrix DNS enables you to register PANEL200 on Matrix DNS Server by configuring its Hostname. Matrix DNS Server will resolve the IP Address of the configured host name and will map the same also.



*This feature will work for LAN interface only.*

To configure the Matrix DNS parameters,

Click **Panel Configuration > Network Settings > Matrix DNS**. The **Matrix DNS** page appears.

Network Settings

LAN Settings | Advanced LAN Settings | Wi-Fi Network Settings | Wi-Fi Access Point Settings | Mobile Broadband | DDNS | **Matrix DNS**

Enable ☒

Host Name: Panel\_RnD

Forwarded Port: 80 (1-65535)

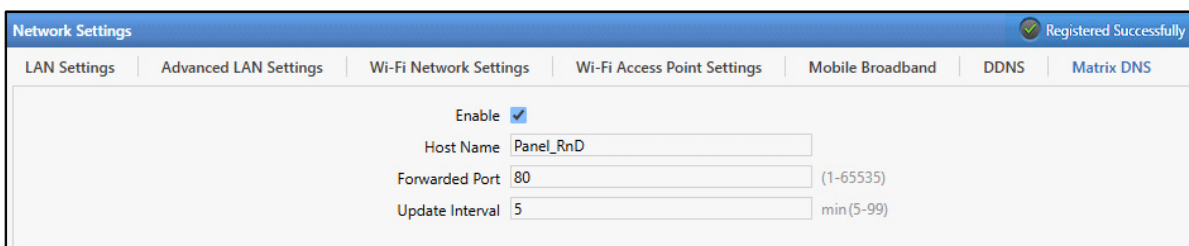
Update Interval: 5 min (5-99)

Configure the following parameters:

- **Enable:** Select the check box to enable the registration of host name on the Matrix DNS Server.
- **Host Name:** Configure the host name. You will be able to access the PANEL200 with this host name from the Matrix DNS Server.
- **Forwarded Port:** Configure the communication port on which PANEL200 will listen.
- **Update Interval:** Configure the duration in minutes after which PANEL200 send its Public IP to the Matrix DNS Server. The same will be updated, if it is found to be different than the one registered.

Click **Save** to save the settings or click **Cancel** to discard.

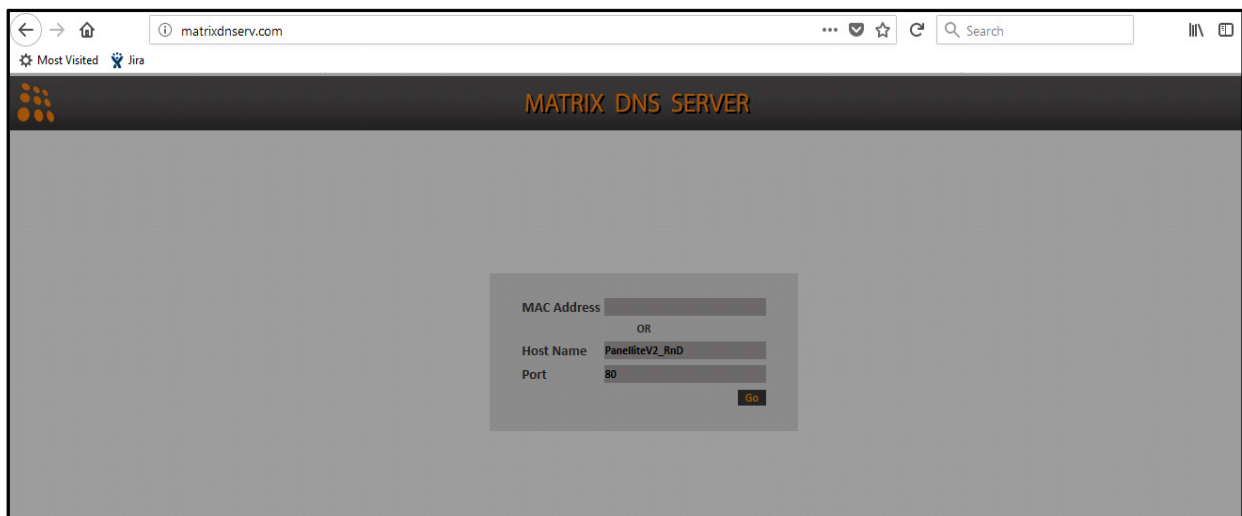
Once the Host Name is registered, the successful registration message will be displayed.



The screenshot shows the 'Network Settings' window with the 'Matrix DNS' tab selected. A green status bar at the top right indicates 'Registered Successfully'. The configuration fields are as follows:

| Field           | Value                               | Range/Unit |
|-----------------|-------------------------------------|------------|
| Enable          | <input checked="" type="checkbox"/> |            |
| Host Name       | Panel_RnD                           |            |
| Forwarded Port  | 80                                  | (1-65535)  |
| Update Interval | 5                                   | min(5-99)  |

Now, on Matrix DNS Server, that is, URL: [www.matrixdnserv.com](http://www.matrixdnserv.com), you can enter the registered Host Name.



The screenshot shows the Matrix DNS Server website. The header reads 'MATRIX DNS SERVER'. The main content area contains a registration form with the following fields:

| Field       | Value          |
|-------------|----------------|
| MAC Address |                |
| OR          |                |
| Host Name   | PaneliteV2_RnD |
| Port        | 80             |

A 'Go' button is located at the bottom right of the form.

Once the Host Name is entered, the MAC Address of the PANEL200 will appear automatically which confirms the registration of PANEL200 on the Matrix DNS Server.



**MATRIX DNS SERVER**

MAC Address

00-18-09-04-EB-3F

OR

Host Name

PanelliteV2\_RnD

Port

80

Go

Matrix DNS Server will resolve the IP Address for configured Host Name. So, now PANEL200 can be accessed using the Host Name.



# Date and Time

To configure the Date and Time parameters,

Click **Panel Configuration > Date and Time**. The **Date and Time** page appears.

The screenshot shows the 'Date and Time' configuration interface. At the top, a header bar displays the current date and time: '06, August 2025 16:21:23'. Below this, the configuration area includes a 'Time Zone' dropdown menu currently set to '(GMT+05:30) Chennai, Kolkata, New Delhi, Mumbai'. Next to it is a 'Time Format' dropdown set to '24 hours'. The 'Date' is shown as '06-08-2025' with a calendar icon for selection. The 'Time' is shown as '16:21:00' with up/down arrows and a close icon. A checkbox for 'Auto synchronize with NTP' is present, along with a text field for 'Preferred NTP Server' containing 'time.windows.com'. A section for 'Daylight Saving Time' contains checkboxes for 'Forward Clock' and 'Reverse Clock'. Each has a 'Month' dropdown (both set to 'January'), a 'Week' dropdown (both set to 'First'), a 'Day' dropdown (both set to 'Sunday'), and a 'Duration' field (both set to '00:00'). At the bottom, there are 'Save' and 'Cancel' buttons.

Configure the following parameters:

- **Time Zone:** Select the time zone as per your region from the drop-down list.
- **Time Format:** Select a desired time format from the drop-down list — 12 hour, 24 hour.
- **Date & Time:** By default, the current Date and Time will be set automatically. You can change the same if required. To set the date, click the calendar and select the desired date. You can set the time in HH:MM:SS format. Click the desired box and use the up/down arrows to set the time.
- Click **Set Date and Time**  to save the changes.

## Auto Synchronize with NTP

If you want the Date and Time to automatically synchronize with the Preferred NTP Server (predefined or user-defined NTP Server Address), configure the following:

- **Auto Synchronize With NTP:** Select the check box to enable.
- **Preferred NTP Server:** Configure the Preferred NTP Server of your choice. Here, you can configure any one of the pre-defined NTP Servers or any other Server of your choice. The PANEL200 will first try to fetch the Date and Time from this configured Server Address. If it does not get Date and Time in three tries; PANEL200 will check from the pre-defined NTP Servers. If you have entered one of the three pre-defined NTP Servers (ntp1.cs.wisc.edu, time.windows.com, time.nist.gov); then PANEL200 will first check that Server. If it receives the updates then, updated Date and Time will be reflected on door webpage and display screen. Valid Values: a-z A-Z 0-9 - . (dot).

If you keep the Preferred NTP Server blank, PANEL200 will check for Date and Time from the pre-defined NTP Server.

If you have manually entered the Date and Time, then these values will be reflected on the door webpage and display screen.

## Daylight Saving Time (DST)

Many countries observe the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn. The PANEL200 can be configured to be compatible with this procedure keeping the RTC of the PANEL200 updated with such changes.

Configure the following:

- **Daylight Saving Time:** Select the check box to enable.
- **Forward:** Select the desired month, week and day from the drop-down list and configure the desired time (HH:MM format) at which the clock is to be forwarded to increase the daylight time. For example, the clock is forwarded on the first Sunday of October at 6 am.
- **Reverse Clock:** Select the desired month, week and day from the drop-down list and configure the desired time (HH:MM format) at which the clock is to be reversed to normalize the time. For example, the clock is reversed on the first Sunday of January at 5 am
- **Duration:** Configure the time **Duration** (HH:MM format), by which the clock is to be forwarded or reversed. For example, the clock is forwarded and reversed by 1 hour. Now considering the day and time set in the above examples, the clock will be forwarded to 7 am and reversed to 4 am on the specified days.

Click **Save** to save the settings or click **Cancel** to discard.

# Server Settings

You need to configure these settings if you have selected the Panel Mode as

- COSEC-Server Mode. For details, refer to [“COSEC-Server Mode”](#).  
**OR**
- Third Party-Server Mode. For details, refer to [“Third Party-Server Mode”](#).

## COSEC-Server Mode

The PANEL200 can be connected with COSEC CENTRA or COSEC VYOM.

To configure the Server Settings parameters,

Click **Panel Configuration > Server Settings**. The **Server Settings** page appears.

- **Connectivity Status:** Displays the connectivity status of the PANEL200 with the COSEC CENTRA or COSEC VYOM. A **Green** dot is displayed if the connection is established, else a **Red** dot is displayed.
- **Server Connection:** Select the desired server from the drop-down list — COSEC CENTRA, COSEC VYOM — with which the PANEL200 is to be connected.

If you select COSEC CENTRA, refer to [“COSEC CENTRA”](#).

If you select COSEC VYOM, refer to [“COSEC VYOM”](#).



- *For **Device Based** license, make sure the PANEL200 is connected with COSEC CENTRA*
- *If you change the Server, all settings except Network Settings will be set to default.*

## COSEC CENTRA

If you have selected COSEC CENTRA as the Server Connection,

The screenshot shows the 'Server Settings' window with the following configuration:

- Connectivity Status:** Green dot, via Ethernet
- Server Connection:** COSEC CENTRA (dropdown)
- Configuration:** Basic (selected), Custom (radio button)
- URL:** 192.168.103.88, 11000
- License Server:**
  - Connectivity Status:** Red dot, Disconnected
  - License Dongle:** Red dot, USB Port Disabled
  - URL:** 192.168.50.100, 15025
- Web Server:**
  - Encryption (HTTPs):** ☐
  - Interface Selection:** Auto (selected), Manual (radio button)
  - Network Interface:** Ethernet (dropdown)
  - URL:** 192.168.103.88, 80
  - Test:** button
  - Directory Name:** cosec
  - Request Retry Timer (min):** 2

Buttons at the bottom: Default, Save, Cancel.

Configure the following parameters:

**Configuration:** Select the desired option — Basic, Custom.

- If you select **Basic**, configure the following:
  - **URL:** Configure the IP Address or Host Name of the Server where the Monitor Service is running. Configure the Port number through which the PANEL200 is to be connected. It is the TCP Listening Port. The default Port is 11000.

When the PANEL200 is added manually or auto added to the COSEC CENTRA Server and a connection between PANEL200 and Server is established, a Green dot will be displayed in the Connection Status.

For example, here PANEL200 is added to the COSEC CENTRA Server with IP Address 192.168.104.12 and Port is 11000.

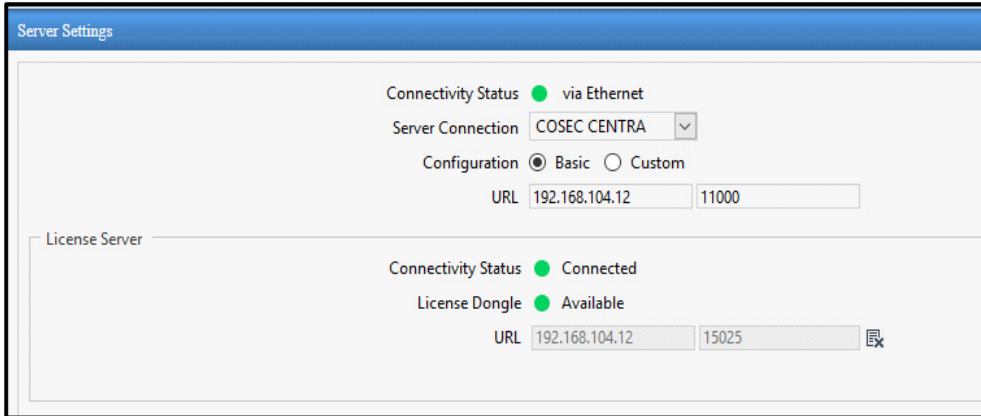
- If you select **Custom**, configure the following:
  - **Ethernet URL:** Configure the IP Address or Host Name of the Server. Configure the Port number through which the PANEL200 is to be connected.
  - **Wi-Fi URL:** Configure the IP Address or Host Name of the Server. Configure the Port number through which the PANEL200 is to be connected.
  - **Broadband URL:** Configure the IP Address or Host Name of the Server. Configure the Port number through which the PANEL200 is to be connected.

Your PANEL200 will get connected to the configured Server with the available interface.

## License Server

- **Connectivity Status:** It displays the connectivity status of the PANEL200 with the License Server.

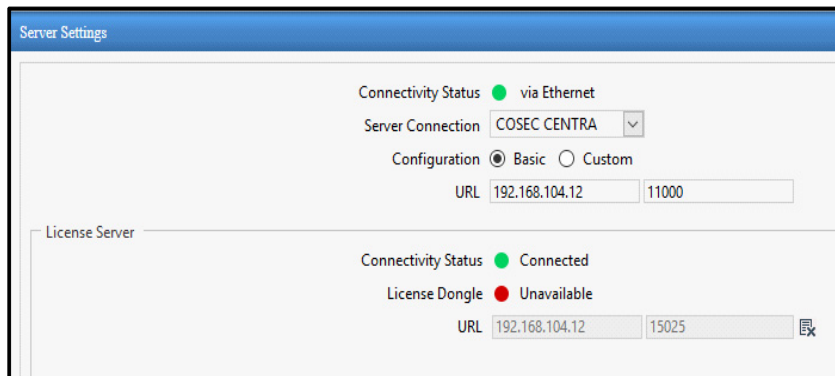
A **Green** dot is displayed when the connection is established with Status as Connected and if the connection is not established, a **Red** dot is displayed with Status as Disconnected.



- **License Dongle:** It displays the status of the dongle, that is, if it is connected or not connected with the PANEL200.

If connected a **Green** dot with Status as **Available** is displayed.

If the dongle is removed from the PANEL200, then a **Red** dot with Status as **Unavailable** is displayed.



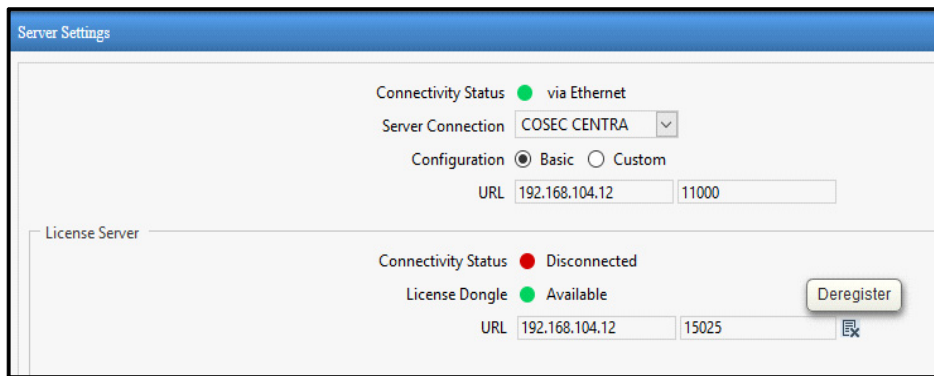
- **URL:** Configure the IP Address or Host Name of the License Server where the Master Service is running. Configure the Port number of the License Server.

If the communication is established with the License Server, the Connectivity Status displays a Green dot with Status as Connected.

If you wish to stop the communication with the current License Server, click **DeRegister**



The Connectivity Status will display a Red dot with Status as Disconnected.

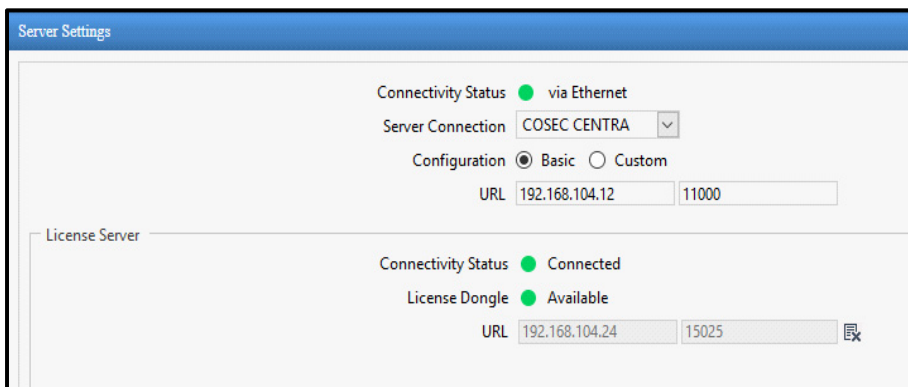


The screenshot shows the 'Server Settings' window. Under the 'License Server' section, the 'Connectivity Status' is indicated by a red dot and the text 'Disconnected'. The 'License Dongle' status is shown as a green dot and 'Available'. The 'URL' field is set to '192.168.104.12' and the 'Port' is '15025'. A 'Deregister' button is visible next to the URL field.

Now, you can configure the IP Address of desired License Server where the Master Service is running.



*Make sure the **License Verification Mode** is set as **Device Based** in the new License Server.*



The screenshot shows the 'Server Settings' window. Under the 'License Server' section, the 'Connectivity Status' is indicated by a green dot and the text 'Connected'. The 'License Dongle' status is shown as a green dot and 'Available'. The 'URL' field is set to '192.168.104.24' and the 'Port' is '15025'.

- Click **Save**.

Once PANEL200 is connected to the License Server, the Connectivity Status displays a Green dot with Status as Connected. Hence, the Master Service on the new License Server will fetch the License Key available in dongle through the PANEL200 and will send the same to other services.

## Web Server

- **Encryption (HTTPS):** Select the Web Server Encryption check box to establish secure HTTPS connection with Web Server to access PANEL200 web pages or API. This will secure the Web pages of PANEL200.
- **Interface Selection:** Select the Interface as **Auto** or **Manual**.
- **Network Interface:** If you have selected **Manual** as the Interface Selection option, select the desired **Network Interface** — **Ethernet, Wi-Fi, Mobile Broadband** — for the network connectivity. PANEL will communicate with the configured Server through the selected interface only.

If you have selected **Auto** as the Interface Selection option, PANEL will communicate will configured Server with available interface with predefined priorities.

- **URL:** Configure the URL (IP Address/ Domain Name) of COSEC CENTRA with which the PANEL200 is connected. If the Encryption (HTTPS) check box is enabled the **Port** configured is 443, else it is 80. You can change it if required.



*In case the Web Server URL is same as that of the Server Address/ Server URL, then the same should be configured in the URL.*

- Click **Test** to check the connectivity of the PANEL with the Server.
- **Directory Name:** Configure the name of the directory in the Server with which the connectivity/syncing needs to be done.
- **Request Retry Timer (min):** Configure the desired time period in minutes. This is the time after which the PANEL should make a request to the Server for connectivity.

Click **Save** to save the settings. You can also click **Default** to set all the parameters to their default values.

## COSEC VYOM

If you have selected COSEC VYOM as the Server Connection,

The screenshot shows the 'Server Settings' window. At the top, 'Connectivity Status' is 'via Ethernet' with a green dot. 'Server Connection' is set to 'COSEC VYOM'. Below it, 'URL' is 'device.matrixvyom.com' and '15025'. 'Tenant ID' is '2'. 'Redirected Server' is '191.168.11.133' and '11009'. A 'Web Server' section is below, with 'Encryption (HTTPS)' checked, 'Interface Selection' set to 'Auto', 'Network Interface' set to 'Ethernet', 'URL' is 'device.matrixvyom.com' and '443', 'Directory Name' is empty, and 'Request Retry Timer (min)' is '2'. A 'Test' button is next to the URL. At the bottom are 'Default', 'Save', and 'Cancel' buttons.

Configure the following parameters:

- **URL:** Configure the IP Address or Host Name of COSEC VYOM. Host Name can be maximum of 253 characters.
- **Port:** Configure the Listening Port of Master Service. The default Port is 15025.
- **Tenant ID:** Configure the Tenant ID with which the PANEL200 is to be connected.

This screenshot shows the 'Server Settings' window with 'Connectivity Status' as 'Ethernet: Connecting...' with a red dot. 'Server Connection' is 'COSEC VYOM'. 'URL' is '192.168.102.226' and '15025'. 'Tenant ID' is '1'. 'Redirected Server' is '192.168.102.226' and '15025'.

Once the PANEL200 gets connected with the Master Service, then Master Service will fetch the Tenant ID and its IP Address and Port where PANEL200 will be redirected. The PANEL200 will then be added to the Monitor Service of the Tenant.

While adding, if you have enabled **Auto add New Devices** in the COSEC Server, the PANEL200 will be added automatically or you will have to add PANEL200 manually.

Once the connectivity is established, the Connectivity Status displays a **Green** dot.

## Web Server

- **Encryption (HTTPS):** Select the Web Server Encryption check box to establish secure HTTPS connection with Web Server to access PANEL200 web pages or API. This will secure the Web pages of PANEL200.
- **Interface Selection:** Select the Interface as **Auto** or **Manual**.
- **Network Interface:** If you have selected **Manual** as the Interface Selection option, select the desired **Network Interface** — **Ethernet, Wi-Fi , Mobile Broadband** — for the network connectivity. PANEL will communicate with the configured Server through the selected interface only.

If you have selected **Auto** as the Interface Selection option, PANEL will communicate will configured Server with available interface with predefined priorities.

- **URL:** Configure the URL (IP Address/ Domain Name) of COSEC VYOM with which the PANEL200 is connected. If the Encryption (HTTPS) check box is enabled the **Port** configured is 443, else it is 80. You can change it if required.



*In case the Web Server URL is same as that of the Server Address/ Server URL, then the same should be configured in the URL.*

- Click **Test** to check the connectivity of the PANEL with the Server.
- **Directory Name:** Configure the name of the directory in the Server with which the connectivity/syncing needs to be done.



- **Request Retry Timer (min):** Configure the desired time period in minutes. This is the time after which the PANEL should make a request to the Server for connectivity.

Click **Save** to save the settings. You can also click **Default** to set all the parameters to their default values.

## Third Party-Server Mode

If you have selected Third Party Mode as the Server Connection,

Configure the following parameters:

- **Authentication Type:** Select the desired option — Basic, Digest — from the drop-down list.
- **Encryption (HTTPS):** Select the Encryption (HTTPS) check box to establish secure HTTPS connection with Web Server to access PANEL200 web pages or API. This will secure the Web pages of PANEL200.
- **Interface Selection:** Select the Interface as **Auto** or **Manual**.
- **Network Interface:** If you have selected **Manual** as the Interface Selection option, select the desired **Network Interface** — **Ethernet, Wi-Fi , Mobile Broadband** — for the network connectivity. PANEL will communicate with configured Server through selected interface only.

If you have selected **Auto** as the Interface Selection option, PANEL will communicate will configured Server with available interface with predefined priorities.

- **URL:** Configure the URL (IP Address/ Domain Name) of Third Party Server with which the PANEL200 is connected. If the Encryption (HTTPS) check box is enabled the **Port** configured is 443, else it is 80. You can change it if required.



*In case the URL is same as that of the Server Address/ Server URL, then the same should be configured in the URL.*

- **Directory Name:** Configure the name of the directory in the Third Party Server with which the connectivity/ syncing needs to be done.

- **User ID:** Configure the User ID that will be used for authentication while establishing connectivity with the Third Party Server.
- **Password:** Configure the Password that will be used for authentication while establishing connectivity with the Third Party Server.

Click **Save** to save the settings. You can also click **Default** to set all the parameters to their default values.

# CCC Settings

---



*CCC Settings are configurable only if you have selected the Panel Mode as COSEC-Server Mode.*

The CCC Settings enable the PANEL200 to communicate with third party application and send events using TCP notification. Using this functionality you will be able to send events from the PANEL200 to a Command and Control Centre (CCC) as well as receive commands from a CCC and implement those commands in the PANEL200.

To configure the **CCC Settings** parameters,

Click **Panel Configuration > CCC Settings**. The **CCC Settings** page appears.

Configure the following parameters:

- **TCP Notification:** Select the check box to enable.
- **IP Address:** Configure the IP Address of the computer on which the TCP Server Application is installed.
- **Port:** Configure the TCP Listening Port of the TCP Server Application.



*Make sure the TCP IP Address and Port configured are not the same as the configured URL and Port in Server Settings > Web Server. For details, refer to [“Web Server”](#).*

- **Interface Selection:** Select the desired interface — Auto, Manual.
- **Network Interface:** If you have selected **Manual** as the Interface Selection option, select the desired **Network Interface** — **Ethernet, Wi-Fi , Mobile Broadband** — for the network connectivity. PANEL will communicate with configured Server through selected interface only.

In have selected Auto as the Interface Selection option, the PANEL200 will communicate will configured Server with available interface with predefined priorities.

Click **Save** to save the settings. You can also click **Default** to set all the parameters to their default values.



---

The Devices allows you to:

- configure the door configuration parameters. For details, refer to [“Door Configuration”](#).
- configure the door groups. For details, refer to [“Door Group”](#).
- configure the video surveillance parameters. For details, refer to [“Video Surveillance”](#).

The status of all the doors added to the PANEL200, can be viewed from the Dashboard in a single glance. For details, refer to [“Doors Dashboard”](#) in [“Dashboard”](#). You can also add new doors from the Dashboard.

### **COSEC-Server Mode**

You can configure the following:

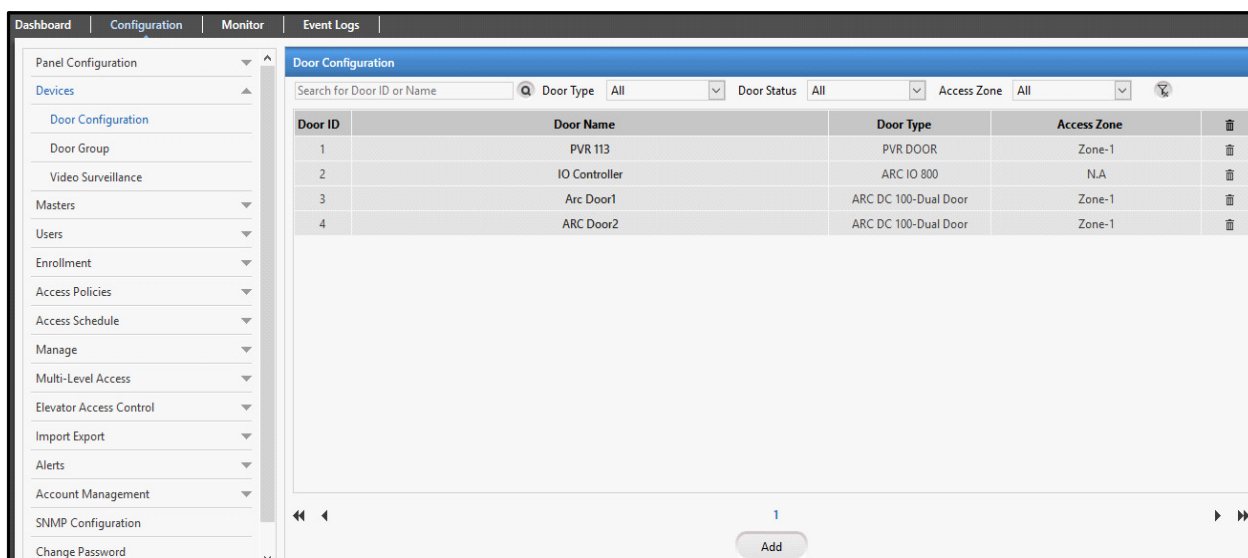
- On the Door Configuration page, you can set the filters — Door Type, Door Status, Access Zone — to view the records, however you cannot configure the [“Door Configuration”](#) parameters.
- configure the door groups. For details, refer to [“Door Group”](#).

# Door Configuration

You can add various type of doors to the PANEL200. PANEL200 can control upto 255 doors using Ethernet communication and upto 32 doors using RS-485 communication.

To configure the Door Configuration parameters,

Click **Devices > Door Configuration**. The **Door Configuration** page appears.



All the added doors appear in the grid with their details — Door ID, Door Name, Door Type and Access Zone. To add a new door, refer to [“Adding Doors”](#).

You can click the desired door and edit its configuration as per your requirement.

You can also delete any door. To do so, click **Delete**  corresponding to the desired door.

You can [“Search”](#) for the desired door or apply the desired [“Filters”](#) — Door Type, Door Status, Access Zone — as per which you wish to view the doors.

## Search

You can search for the desired doors using the Search bar. Enter the keyword according to which you wish to search. The search will be carried out in the Door ID and Door Name column only. Click **Search**  The doors will be filtered as per the entered keyword.

## Filters

You can apply any one or a combination of the filters as per your requirement:

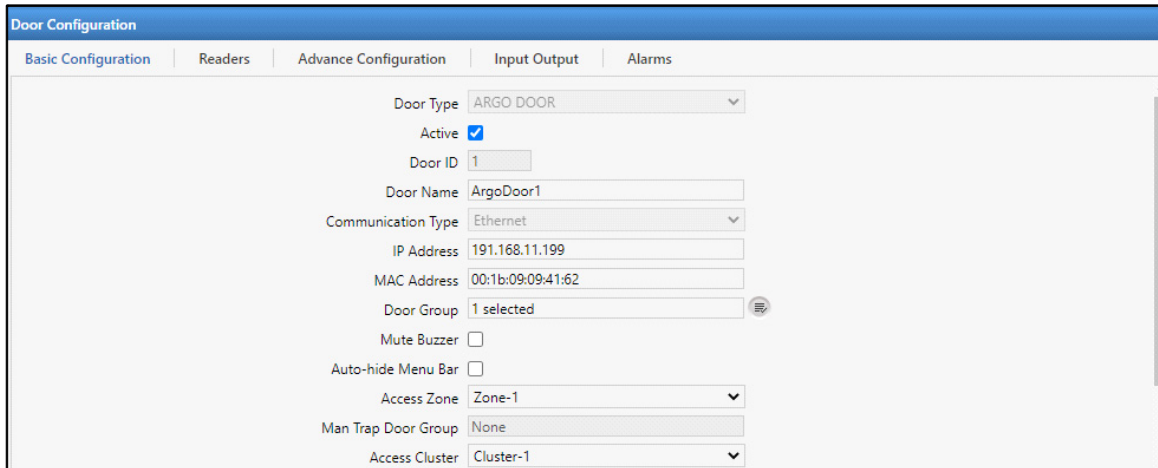
- **Door Type:** Select the desired type of door from the drop-down list
- **Door Status:** Select the desired Status from the drop-down list.
- **Access Zone:** Select the desired Access Zone from the drop-down list.

The doors will be displayed as per the set filters.

To clear the set filters, click **Clear Filter**  .

## Adding Doors

Click **Add**<sup>1</sup>.



The screenshot shows the 'Door Configuration' window with the 'Basic Configuration' tab selected. The window has a blue header and a light gray background. The configuration fields are as follows:

- Door Type: ARGO DOOR (dropdown)
- Active: ☒
- Door ID: 1 (text input)
- Door Name: ArgoDoor1 (text input)
- Communication Type: Ethernet (dropdown)
- IP Address: 191.168.11.199 (text input)
- MAC Address: 00:1b:09:09:41:62 (text input)
- Door Group: 1 selected (dropdown with a menu icon)
- Mute Buzzer: ☐
- Auto-hide Menu Bar: ☐
- Access Zone: Zone-1 (dropdown)
- Man Trap Door Group: None (dropdown)
- Access Cluster: Cluster-1 (dropdown)

The Door Configuration allows you to:

- configure the basic configuration parameters. For details, refer to [“Basic Configuration”](#).
- configure the reader parameters. For details, refer to [“Readers”](#).
- configure the advance configuration parameters. For details, refer to [“Advance Configuration”](#).
- configure the advance configuration 2 parameters. For details, refer to [“Advance Configuration 2”](#).
- configure the input output parameters. For details, refer to [“Input Output”](#).
- configure the special function parameters. For details, refer to [“Special Function”](#).
- configure the alarms. For details, refer to [“Alarms”](#).
- configure the face identification settings. For details, refer to [“Face Identification Settings”](#).



*There are different types of doors as well as each door type has variants. Hence, the features and functionalities supported will depend on the door and the variant you wish to add.*

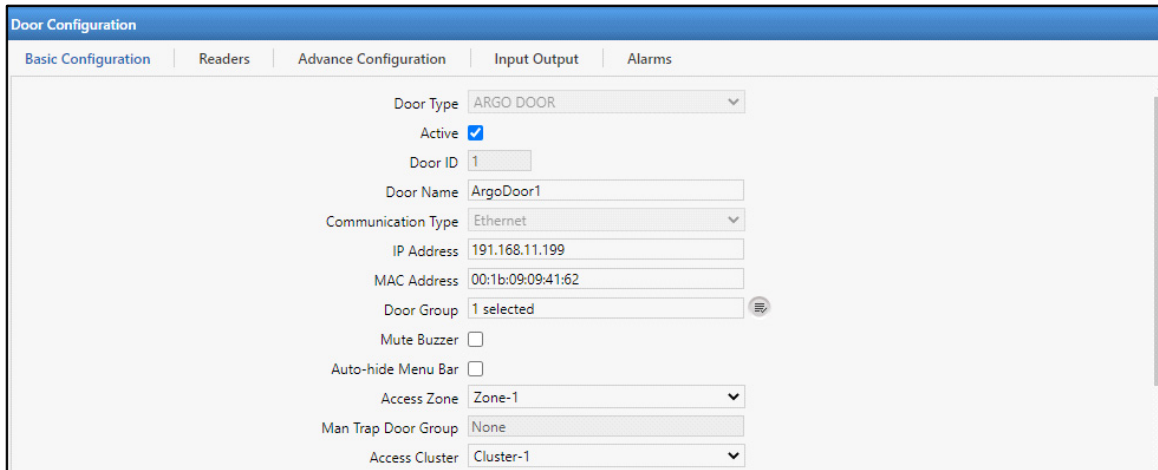
## Basic Configuration

To configure the Basic Configuration parameters,

Click **Devices > Door Configuration > Basic Configuration**. The **Basic Configuration** page appears.

---

1. You will be able to add, edit as well as delete ARGO FACE210. However, these devices are available for Beta evaluation only. Full support will be included in a future Server release aligned with the respective device launch.



Door Configuration

Basic Configuration | Readers | Advance Configuration | Input Output | Alarms

Door Type: ARGO DOOR

Active: ☒

Door ID: 1

Door Name: ArgoDoor1

Communication Type: Ethernet

IP Address: 191.168.11.199

MAC Address: 00:1b:09:09:41:62

Door Group: 1 selected

Mute Buzzer: ☐

Auto-hide Menu Bar: ☐

Access Zone: Zone-1

Man Trap Door Group: None

Access Cluster: Cluster-1

Configure the following parameters:

- **Door Type:** Select the type of door from the drop-down list.
- **Mode (Only for ARC DC100 and ARC DC200):** Select the desired mode — Single Door, Dual Door.
- **Active:** Select the check box to enable the door in the network.
- **Door ID:** The ID will be auto generated by the PANEL200.
- **Door Name:** Configure a user-friendly name for the door.
- **Communication Type:** Select the desired type of communication you wish the door to establish with PANEL200 — Ethernet, RS-485.
- **IP Address:** Configure the IP Address you wish to assign to the door. Once the door is connected with the PANEL200, the status of the door will be displayed as Online in the Monitor.
- **MAC Address:** Configure the MAC Address of the door.
- **Door Group:** Click the **Door Group** picklist. The **Door Group** pop-up appears. Select the check boxes of the desired Door Groups. Click **Ok**. The number of selected groups appear.

**OR**

You can also search for the desired door group. To do so, enter the keyword in the Search box. Click

**Search**  . The door groups will be filtered as per the keyword. Select the check boxes of the desired Door Groups. Click **Ok**. The number of selected groups appear.

If the mode of ARC DC100/ARC DC200 is selected as Dual Door with Dual Readers, then along with the above parameters configure Door Name, Mute Buzzer and Access Zone for Door 1 and Door 2 respectively.

If the mode of ARC DC100/ARC DC200 is selected as Dual Door with Single Readers, then along with the above parameters configure Door Name and Mute Buzzer for Door 1 and Door 2 separately. Access Zone is configured earlier.



- **Connect Doors with:** This parameter will appear when you add ARC DC100/ARC DC200 in Dual Door mode.
- Select the option as **Single Reader** for both the doors to communicate with only one reader (Reader 1).
- Select the option as **Dual Readers** for both the doors to communicate with individual readers, that is, Door 1 with Reader 1 and Door 2 with Reader 2.
- **Mute Buzzer:** Select the check box to mute the door buzzer.
- **Auto-hide Menu Bar:** Select the check box to hide the menu bar automatically on the door display screen.



*Auto-hide Menu Bar is applicable for VEGA, ARGO, ARGO FACE and ARGO FACE210 Door.*

- **Inverse Polarity for External Buzzer:** When external reader is connected to ARC controller via Wiegand Interface and external buzzer is connected with ARC, then enable the Inverse Polarity check box to get buzzer output when any event (for example, User Allowed) is generated.

This is applicable for ARC Dual Door Dual Reader, Dual Door Single Reader and ARC Single Door.

Door Configuration

Basic Configuration | Readers | Advance Configuration | Input Output

Door Type: ARC DC 100

Mode: Single Door

Active: ☒

Door ID: 2

Door Name: ARC as Single door

Communication Type: Ethernet

IP Address: 192.168.104.60

MAC Address: f7:65:77:43:32:42

Mute Buzzer: ☐

Inverse Polarity for External Buzzer: ☒

Access Zone: Zone-1

Door Group: None

Access Cluster: Cluster-1

- **Access Zone:** Select the desired Access Zone from the drop-down list you wish to assign to the door.
- **Man Trap Door Group:** It displays the Man Trap Door Group assigned to the door. To create/assign Man Trap Door Groups, refer to ["Man Trap Door Group"](#).
- **Access Cluster:** Select the desired Access Cluster from the drop-down list you wish to assign to the door.

## Allowed Acknowledgment

- **Display Duration:** Configure the duration for which the acknowledgment message should be displayed on the door display screen.
- **LED-Buzzer Duration:** Select the desired duration option — Long, Medium, Short, Shortest — for which the buzzer should be triggered from the drop-down list. Hover-over the  icon to view the details of LED-Buzzer duration in milliseconds for each option.

## Denied Acknowledgment

- **Display Duration:** Configure the duration for which the acknowledgment message should be displayed on the door display screen.
- **LED-Buzzer Duration:** Select the desired duration option — Long, Medium, Short, Shortest — for which the buzzer should be triggered from the drop-down list. Hover-over the  icon to view the details of LED-Buzzer duration in milliseconds for each option.



*Allowed/Denied Acknowledgment is applicable for PVR, VEGA, Door V3, Door V4, PATH V2, ARC DC200, ARGO, ARGO FACE and ARGO FACE210 Door.*

*The following is applicable to ARGO, VEGA, ARGO FACE, ARGO FACE210, PATH V2 and ARC DC200 only:*

- *The range (250ms-3000ms) for Allowed/Denied Acknowledgment Display Duration.*
- *The option **Shortest** for LED-Buzzer Duration.*

Click **Save** to save the settings or click **Cancel** to discard.

## Readers

To configure the Reader parameters,

Click **Devices > Door Configuration > Readers**. The **Readers** page appears.

For ARC DC100, refer to [“ARC DC100 - Reader Parameters”](#)

For ARC DC200, refer to [“ARC DC200 - Reader Parameters”](#)



*Reader parameters differ according to the selected Door Type.*

The screenshot shows the 'Door Configuration' window with tabs for Basic Configuration, Readers, Advance Configuration, Input Output, Alarms, and Face Identification Settings. The 'Readers' tab is active, showing two sections: 'Internal Readers' and 'External Reader'.

**Internal Readers:**

- Card Reader: MiFare -U Reader
- Mode: Entry
- Card Format: 1 Selected (with a menu icon)
- Default...
- Advertise Bluetooth: ☒
- Bluetooth Name: ARGO FA-IN
- Range:
  - ☐ Short (1-2m)
  - ☐ Medium (5-7m)
  - ☐ Long (>8m)
  - ☒ Custom
- Custom Bluetooth Range (dBm): Near (-40 dBm) [slider] Far (+10 dBm) -30 [info icon]

**External Reader:**

- External Reader: ATOM RD200
- Mode: Exit
- Exit Switch: ☒
- Card Format: 1 Selected (with a menu icon)
- Default...
- Configure Bluetooth From Panel: ☒
- Advertise Bluetooth: ☒
- Bluetooth Name: ARGO FACE- 1-OUT
- Range:
  - ☐ Short (1-2m)
  - ☒ Medium (5-7m)
  - ☐ Long (>8m)

Configure the following parameters:

## Internal Readers

Configure the following parameters:

- **Card Reader:** Select the desired reader from the drop-down list.
- **Finger Reader:** Select the desired reader from the drop-down list.
- **Mode:** Select the desired **Mode** — **Entry**, **Exit**.
- **Card Format:** By default, the Default Format is assigned. Click the **Select Card Format** picklist. The **Card Format** pop-up appears. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of selected formats and their names appear.

**OR**

You can also search for the desired card format. To do so, enter the keyword in the Search box. Click

**Search**  . The card formats will be filtered as per the keyword. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of selected formats and their names appear.

For Card Format details, refer to [“Card Format”](#).

- **Advertise Bluetooth:** Select the check box to enable the Bluetooth of the reader. Then, configure the following parameters:
- **Bluetooth Name:** By default, if the Door Name is configured then in **Bluetooth Name**, Door Name will be displayed here along with the Mode type. The prefix will be the Door Name and the suffix will be -IN or -OUT as per the set Mode. If required, you can configure the bluetooth name as per your requirement. The Bluetooth Name can be a maximum of 10 characters.
- **Range:** The PANEL200 supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired **Bluetooth Range** to control the boundary for marking the attendance.

Select the Bluetooth Range as — Short (1m-2m), Medium (5m-7m), Long (>8m) or Custom.

- If you select **Custom** option for Bluetooth Range, configure the **Custom Bluetooth Range** manually or set the range using the slider. Drag the slider towards the left to decrease the value or drag the slider to the right to increase the value. A lower value indicates a shorter range.



*Custom option for Bluetooth Range is applicable to ARGO, VEGA, ARGO FACE, ARGO FACE210, PATH V2 and ARC DC200 only.*

Click **Save** to save the settings or click **Cancel** to discard.

## External Reader

- **External Reader:** Select the type of External Reader from the drop-down list.
- **Mode:** Select the desired mode — **Entry, Exit**.
- **Exit Switch:** By default, it is select, that is, it is enabled. Clear the check box to disable.
- **Card Format:** By default, the Default Format is assigned. Click the **Select Card Format** picklist. The **Card Format** pop-up appears. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of selected formats and their names appear.

**OR**

You can also search for the desired card format. To do so, enter the keyword in the Search box. Click

**Search**  . The card formats will be filtered as per the keyword. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of selected formats and their names appear.

For Card Format details, refer to "[Card Format](#)".

- **Configure Bluetooth From Panel:** When you select **External Reader** as — CB U Reader, ATOM RD300, ATOM RD200 or ATOM RD100, select **Configure Bluetooth from Panel** check box to enable Bluetooth feature for the doors with which these external readers are connected.
- **Advertise Bluetooth:** Select the check box to enable Bluetooth of the reader. Then configure the following parameters.
- **Bluetooth Name:** By default, if the Door Name is configured then in **Bluetooth Name**, Door Name will be displayed here along with the Mode type. The prefix will be the Door Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the bluetooth name as per your requirement.

If **External Reader Type** is ATOM RD100 or CB U Reader, the Bluetooth Name can be a maximum of 20 characters.

- **Range:** The PANEL200 supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired **Bluetooth Range** to control the boundary for marking the attendance.

Select the desired **Bluetooth Range** as — **Short (1m - 2m)**, **Medium (5m - 7m)** or **Long (> 8m)**.

- **Re-detection Delay:** When **External Reader** is selected as **UHF Reader** from the drop-down list then only **Re-detection Delay** parameter will be applicable. Configure the duration for which a card will not be read or/and detected again after it is used for access once. Valid Value is 0- 60 minutes.

Click **Save** to save the settings or click **Cancel** to discard.

## ARC DC100 - Reader Parameters

For **Single Door ARC DC100** configure the following parameters for **Reader1 Group** and **Reader2 Group**.

- **RS-485 Reader:** Select the desired RS-485 Reader from the drop-down list.
- **Wiegand Reader:** Select the desired Wiegand Reader from the drop-down list.
- **Short-Range Reader:** Select this option to identify the user from a short distance.
- **Long-Range Reader:** Select this option to identify the user from a long distance.
- **PIN-W Reader:** Select this option to support PIN pad device and accept the PIN from pin pad for identifying the user.
- **Card+PIN-W Reader:** Select this option to identify the user with Card and the PIN from pin pad. If card format is 4 or 8 bit then first entered input is considered as PIN input. If card format is greater than 8 bit then first entered input is considered as CARD input.



*If Card format is of 26 bit, make sure card is displayed first. When card is verified, then PIN must be entered to verify the user.*

- **Mode:** Select the desired mode — Entry, Exit — for Reader1 Group.
- **Exit Switch (Only for Reader2 Group):** Select the check box to enable Exit Switch feature for Reader2 Group so that the door can be opened without checking any access policy.
- **Card Format:** By default, the Default Format is assigned. Click the **Select Card Format** picklist. The **Card Format** pop-up appears. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of selected formats and their names appear.

**OR**

You can also search for the desired card format. To do so, enter the keyword in the Search box. Click

**Search**  . The card formats will be filtered as per the keyword. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of selected formats and their names appear.

For Card Format details, refer to [“Card Format”](#).

For **ARC DC100 - Dual Door Dual Reader** configure the following parameters for **Door 1** and **Door 2**.

- **RS-485 Reader:** Select the desired RS-485 Reader from the drop-down list.
- **Wiegand Reader:** Select the Wiegand Reader from the drop-down list.
- **Short-Range Reader:** Select this option to identify the user from a short distance.
- **Long-Range Reader:** Select this option to identify the user from a long distance.
- **PIN-W Reader:** Select this option to support PIN pad device and accept the PIN from pin pad for identifying the user.
- **Card+PIN-W Reader:** Select this option to identify the user with Card and the PIN from pin pad. If card format is 4 or 8 bit then first entered input is considered as PIN input.

If card format is greater than 8 bit then first entered input is considered as CARD input.



*If Card format is of 26 bit, then make sure card is displayed first. When card is verified, then PIN must be entered to verify the user.*

- **Mode:** Select the desired mode — Entry, Exit — for doors.
- **Exit Switch:** Select the check box to enable Exit Switch, so that the door can be opened without checking any access policy.
- **Card Format:** By default, the Default Format is assigned. Click the **Select Card Format** picklist. The **Card Format** pop-up appears. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of select formats and their names appear.

**OR**

You can also search for the desired card format. To do so, enter the keyword in the Search box. Click

**Search**  . The card formats will be filtered as per the keyword. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of select formats and their names appear.

For Card Format details, refer to [“Card Format”](#).

For ARC DC100 - Dual Door Single Reader configure the parameters as described for Dual Door, Dual Reader. For Door2, Exit switch can be configured as it is not connected with any reader.



*The following Access Policies will not work with ARC DC100 - Dual Door Single Reader:*

- *Duress Detection, Mantrap, Anti Pass Back (APB), Dead Man, Occupancy Control, Use Count, Door lock, Door unlock, Smart Card based Access Route, Multi credential Access Mode.*

*Readers configurations are not applicable for ARC IO800.*

Click **Save** to save the settings or click **Cancel** to discard.

## ARC DC200 - Reader Parameters

### Single Door Dual Reader

For **Single Door ARC DC200** configure the following parameters for **Reader1 Group** and **Reader2 Group**.

The screenshot shows the 'Door Configuration' window with the 'Readers' tab selected. The 'Reader1 Group' section is expanded, showing the following settings:

- Advertise Bluetooth:** ☒
- Bluetooth Name:** ARC DC 200
- Range:** ☐ Short (1-2m), ☐ Medium (5-7m), ☐ Long (>8m), ☒ Custom
- Custom Bluetooth Range (dBm):** A slider between 'Near (-40 dBm)' and 'Far (+10 dBm)' is set to -30.
- RS-485 Interface Protocol:** Matrix Proprietary
- Matrix Reader Type:** ATOM RD100
- Wiegand Reader:** Short - Range Reader
- Mode:** Entry
- Card Format:** 1 Selected
- Default...**
- Configure Bluetooth From Panel:** ☒
- Advertise Bluetooth:** ☒
- Bluetooth Name:** ARC DC 200-00:1b:-IN
- Range:** ☐ Short (1-2m), ☒ Medium (5-7m), ☐ Long (>8m)

The screenshot shows the 'Door Configuration' window with the 'Readers' tab selected. The 'Reader2 Group' section is expanded, showing the following settings:

- RS-485 Interface Protocol:** Matrix Proprietary
- Matrix Reader Type:** ATOM RD300
- Wiegand Reader:** Short - Range Reader
- Mode:** Exit
- Exit Switch:** ☒
- Card Format:** 1 Selected
- Default...**
- Configure Bluetooth From Panel:** ☒
- Advertise Bluetooth:** ☒
- Bluetooth Name:** ARC DC 200-00:1b-OUT
- Range:** ☐ Short (1-2m), ☒ Medium (5-7m), ☐ Long (>8m)

- **Advertise Bluetooth:** Select the check box to enable Bluetooth of ARC DC200 and it will be visible to other devices for communication. Then configure the following parameters.
- **Bluetooth Name:** By default, if the Door Name is configured then it will be displayed here. If required, you can configure the bluetooth name as per your requirement. The **Bluetooth Name** can be a maximum of 10 characters.
- **Bluetooth Range:** The PANEL200 supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the **Bluetooth Range** as — **Short (1m - 2m)**, **Medium (5m - 7m)**, **Long (> 8m)** or **Custom**.

- **Custom Bluetooth Range (dBm):** If you select **Custom** option for Bluetooth Range, configure the Bluetooth Range manually or set the range using the slider. Drag the slider towards the left to decrease the value or drag the slider to the right to increase the value.

### Reader 1/ Reader 2 Group

- **RS-485 Interface Protocol:** Select the desired option — Matrix Proprietary, OSDP.

If you select RS-485 Interface Protocol as Matrix Proprietary, you can configure the parameters for Matrix Reader Type as well as Wiegand Reader. For details, refer to [“Matrix Reader Type and Wiegand Reader”](#).

If you select RS-485 Interface Protocol as OSDP, you need to configure the OSDP Parameters. OSDP Protocol is supported for 3rd Party Readers only. For details refer to [“OSDP Parameters”](#).

### Matrix Reader Type and Wiegand Reader

- **Matrix Reader Type:** Select the desired type of reader to be connected on RS-485 interface.



*While connecting Matrix ATOM Reader with Matrix COSEC ARC DC200, we recommend you to use RS-485 interface, as security concerns may arise if connecting via Wiegand interface.*

- **Wiegand Reader:** Select the desired Wiegand Reader from the drop-down list.
- **Short-Range Reader:** Select this option to identify the user from a short distance.
- **Long-Range Reader:** Select this option to identify the user from a long distance.
- **Re-detection Delay:** When **Wiegand Reader** is selected as **Long-Range Reader**, then only **Re-detection Delay** parameter is applicable. Configure the duration for which a card will not be read or/and detected again after it is used for access once. Valid Value is 0- 60 minutes.
- **PIN-W Reader:** Select this option to support PIN pad device and accept the PIN from pin pad for identifying the user.
- **Card+PIN-W Reader:** Select this option to identify the user with Card and the PIN from pin pad. If card format is 4 or 8 bit then first entered input is considered as PIN input. If card format is greater than 8 bit then first entered input is considered as CARD input.
- **CB-W Reader:** Select this option to identify the user with Card/Bluetooth over Wiegand Interface.



*If Card format is of 26 bit, make sure card is displayed first. When card is verified, then PIN must be entered to verify the user.*

- **Mode:** Select the desired mode — **Entry** or **Exit**.
- **Exit Switch (Only for Reader2 Group):** Select the check box to enable Exit Switch feature for Reader2 Group so that the door can be opened without checking any access policy.
- **Card Format:** By default, the Default Format is assigned. Click the **Select Card Format** picklist. The **Card Format** pop-up appears. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of selected formats and their names appear.



OR

You can also search for the desired card format. To do so, enter the keyword in the Search box. Click

**Search**  . The card formats will be filtered as per the keyword. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of selected formats and their names appear.

For Card Format details, refer to [“Card Format”](#).

- **Configure Bluetooth from Panel:** When you select **Matrix Reader Type** as — CB U Reader or ATOM RD100/200/300, select **Configure Bluetooth from Panel** check box to enable Bluetooth feature for aforementioned external readers.

Once you enable **Configure Bluetooth from Panel**, configure the following Bluetooth parameters:

- **Advertise Bluetooth:** Select the check box to enable Bluetooth of the reader. Then configure the following parameters.
- **Bluetooth Name:** By default, if the Door Name is configured then in **Bluetooth Name**, Door Name will be displayed here along with the Mode type. The prefix will be the Door Name and the suffix will be -IN or -OUT as per the set Mode.

If required, you can configure the name of bluetooth as per your requirement. The **Bluetooth Name** can be a maximum of 20 characters.

- **Bluetooth Range:** The Panel200 supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the **Bluetooth Range** as — **Short (1m-2m)**, **Medium (5m-7m)** or **Long (>8m)**.

## ARC DC200 - Dual Door Single Reader

**Door Configuration**

Basic Configuration | **Readers** | Advance Configuration | Input Output | Alarms

Advertise Bluetooth ☒

Bluetooth Name

Range ☐ Short (1-2m)  
☐ Medium (5-7m)  
☐ Long (>8m)  
☒ Custom

Custom Bluetooth Range (dBm) Near (-40 dBm)  Far (+10 dBm)  ⓘ

Door 1

RS-485 Interface Protocol

Matrix Reader Type

Wiegand Reader

Mode

Exit Switch ☒

Card Format  ⓘ

Default...

Configure Bluetooth From Panel ☒

Advertise Bluetooth ☒

Bluetooth Name

Range ☐ Short (1-2m)  
☒ Medium (5-7m)  
☐ Long (>8m)

Door 2

Exit Switch ☒

## ARC DC200 - Dual Door Dual Reader

**Door Configuration**

Basic Configuration | **Readers** | Advance Configuration | Input Output | Alarms

Advertise Bluetooth ☒

Bluetooth Name

Range ☐ Short (1-2m)  
☐ Medium (5-7m)  
☐ Long (>8m)  
☒ Custom

Custom Bluetooth Range (dBm) Near (-40 dBm)  Far (+10 dBm)  ⓘ

Door 1

RS-485 Interface Protocol

Matrix Reader Type

Wiegand Reader

Mode

Exit Switch ☒

Card Format  ⓘ

Default...

Configure Bluetooth From Panel ☒

Advertise Bluetooth ☒

Bluetooth Name

Range ☐ Short (1-2m)  
☒ Medium (5-7m)  
☐ Long (>8m)

The screenshot shows the configuration interface for 'Door 2'. It includes several dropdown menus and checkboxes. The 'RS-485 Interface Protocol' is set to 'Matrix Proprietary'. The 'Matrix Reader Type' is 'ATOM RD100'. The 'Wiegand Reader' is 'Short - Range Reader'. The 'Mode' is 'Exit'. The 'Exit Switch' is checked. The 'Card Format' is '1 Selected'. The 'Configure Bluetooth From Panel' and 'Advertise Bluetooth' checkboxes are both checked. The 'Bluetooth Name' is 'ARC DC 200 DD DR-OUT'. The 'Bluetooth Range' is set to 'Medium (5-7m)' with radio buttons for 'Short (1-2m)', 'Medium (5-7m)', and 'Long (>8m)'.

- **Advertise Bluetooth:** Select the check box to enable Bluetooth of ARC DC200 and it will be visible to other devices for communication. Then configure the following parameters.
- **Bluetooth Name:** By default, if the Door Name is configured then it will be displayed here. If required, you can configure the bluetooth name as per your requirement.
- **Bluetooth Range:** The PANEL200 supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance.

Select the **Bluetooth Range** as — **Short (1m - 2m)**, **Medium (5m - 7m)**, **Long (> 8m)** or **Custom**.

- **Custom Bluetooth Range (dBm):** If you select **Custom** option for Bluetooth Range, configure the Bluetooth range manually or set the range using the slider. Drag the slider towards the left to decrease the value or drag the slider to the right to increase the value.

## Door 1/ Door 2

- **RS-485 Interface Protocol:** Select the desired option — Matrix Proprietary, OSDP.

If you select RS-485 Interface Protocol as Matrix Proprietary, you can configure the parameters for Matrix Reader Type as well as Wiegand Reader. For details, refer to [“Matrix Reader Type and Wiegand Reader”](#).

If you select RS-485 Interface Protocol as OSDP, you need to configure the OSDP Parameters. OSDP Protocol is supported for 3rd Party Readers only. For details refer to [“OSDP Parameters”](#).

## Matrix Reader Type and Wiegand Reader

- **Matrix Reader Type:** Select the desired type of reader to be connected on RS-485 interface.



*While connecting Matrix ATOM Reader with Matrix COSEC ARC DC200, we recommend you to use RS-485 interface, as security concerns may arise if connecting via Wiegand interface.*

- **Wiegand Reader:** Select the desired Wiegand Reader from the drop-down list.
  - **Short-Range Reader:** Select this option to identify the user from a short distance.
  - **Long-Range Reader:** Select this option to identify the user from a long distance.

- **Re-detection Delay:** When **Wiegand Reader** is selected as **Long-Range Reader**, then only **Re-detection Delay** parameter will be applicable. Configure the duration for which a card will not be read or/and detected again after it is used for access once. Valid Value is 0- 60 minutes.
- **PIN-W Reader:** Select this option to support PIN pad device and accept the PIN from pin pad for identifying the user.
- **Card+PIN-W Reader:** Select this option to identify the user with Card and the PIN from pin pad. If card format is 4 or 8 bit then first entered input is considered as PIN input. If card format is greater than 8 bit then first entered input is considered as CARD input.
- **CB-W Reader:** Select this option to identify the user with Card/Bluetooth over Wiegand Interface.



*If Card format is of 26 bit, make sure card is displayed first. When card is verified, then PIN must be entered to verify the user.*

- **Mode:** Select the desired mode — **Entry** or **Exit**.
- **Exit Switch:** Select the check box to enable Exit Switch so that the door can be opened without checking any access policy.



*For ARC DC200 - Dual Door Single Reader, in Door2 only Exit Switch can be connected and the remaining parameters are not applicable.*

- **Card Format:** By default, the Default Format is assigned. Click the **Select Card Format** picklist. The **Card Format** pop-up appears. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**.The number of select formats and their names appear.

**OR**

You can also search for the desired card format. To do so, enter the keyword in the Search box. Click

**Search**  . The card formats will be filtered as per the keyword. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**.The number of select formats and their names appear.

For Card Format details, refer to "[Card Format](#)".

- **Configure Bluetooth from Panel:** When you select **Matrix Reader Type** as — CB U Reader or ATOM RD100/200/300, select **Configure Bluetooth from Panel** check box to enable Bluetooth feature for aforementioned external readers.

Once you enable **Configure Bluetooth from Panel**, configure the following Bluetooth parameters:

- **Advertise Bluetooth:** Select this check box to enable Bluetooth of the reader. Then configure the following parameters.
- **Bluetooth Name:** By default, if the Door Name is configured then it will be displayed here.

If required, you can configure the name of bluetooth as per your requirement. The **Bluetooth Name** can be a maximum of 20 characters.

- **Bluetooth Range:** The PANEL200 supports different ranges of bluetooth using which the users can mark their attendance. You can set the desired range to control the boundary for marking the attendance. Select the bluetooth range as — Short (1m-2m), Medium (5m-7m) or Long (>8m).

Click **Save** to save the settings or click **Cancel** to discard.

### OSDP Parameters

If you select **RS-485 Interface Protocol** as **OSDP**, you need to configure the following parameters. OSDP Protocol is supported for Third Party Readers only.



*Only Card and PIN credential will be supported for User, if OSDP Reader is configured and connected.*

- **Mode:** Select the desired mode — **Entry** or **Exit**.
- **Exit Switch:** Select the check box to enable Exit Switch so that the door can be opened without checking any access policy.



*For ARC DC200 - Dual Door Single Reader, in Door1 — Mode, Exit Switch and Card Format are applicable and in Door2 only Exit Switch is applicable.*

*For ARC DC200 - Dual Door Dual Reader, in Door 1/2 — Mode, Exit Switch and Card Format are applicable.*

*For ARC DC200 - Single Door Dual Reader, in Reader 1 Group — Mode and Card Format are applicable and in Reader 2 Group — Mode, Exit Switch and Card Format are applicable.*

- **Card Format:** By default, the Default Format is assigned. Click the **Select Card Format** picklist. The **Card Format** pop-up appears. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of selected formats and their names appear.

**OR**

You can also search for the desired card format. To do so, enter the keyword in the Search box. Click

**Search** . The card formats will be filtered as per the keyword. Select the check boxes of the desired formats. You can select upto 5 formats. Click **Ok**. The number of selected formats and their names appear.

For Card Format details, refer to [“Card Format”](#).



*If you are using Cards with parity bits included, then make sure you configure the Card Format accordingly. For details, refer to [“Card Format”](#). Make sure you select this Card Format for the OSDP Readers to ensure proper functioning of the Cards.*

## OSDP Settings

- **OSDP Address:** Configure the unique identifier assigned to the 3rd Party Reader (Peripheral Device - PD). This allows the door (Control Panel - CP) to communicate and manage individual readers in the same network.
- **Baud Rate:** Select the Baud Rate of the 3rd Party Reader from the drop-down list. This is the rate at which data will be transmitted/received between the door and 3rd Party Reader.
- **Enable OSDP Secure Channel:** If you wish that the door and the 3rd Party Reader should utilize the Secure Channel Protocol (SCP) for communication using encryption and authentication mechanism select the **Enable OSDP Secure Channel** check box and configure the Encryption Key.
- **Encryption Key:** Configure the value which will be used as the key. This is a cryptographic value used in encryption algorithms to convert and transmit data in encrypted form or vice versa. Encryption Keys are used within Secure Channel Protocol (SCP) to encrypt or decrypt the transmitted data between door and 3rd Party Readers.

Click **Save** to save the settings or click **Cancel** to discard.

For list of Commands and Responses supported in OSDP, refer to, "[Supported OSDP Commands and Responses](#)"

## Advance Configuration

To configure the Advance Configuration parameters,

Click **Devices > Door Configuration > Advance Configuration**. The **Advance Configuration** page appears.

Door Configuration

Basic Configuration | Readers | **Advance Configuration** | Input Output | Alarms

Auto Re-lock ☐

Auto Re-lock Timer  sec(1-65535)

Pulse Timer  sec(0.1-65535.0)

Auto IP Assignment ☒

Door Interlock ☐

Door

Man Trap Timer - Internal Reader  sec(0-999)

Man Trap Timer - External Reader  sec(0-999)

Duplicate Access Time Interval  sec(0-9999)

Add Delete Save Cancel



*Advance Configuration is not applicable for ARC IO800.*

- **Auto Re-lock:** Select the check box to allow the door to re-lock immediately when the door status changes to close after normal open irrespective of the Pulse Time. However, it is supported only if a door sense is installed and enabled.
- **Auto Re-lock Timer:** Configure the duration in seconds for the Auto Re-lock operation.

- **Reader Group 1 - Tamper / Reader Group 2 - Tamper:** This is applicable when ARC DC200 is configured as Single Door Dual Reader. You can configure separate options for each Reader. Select the desired Tamper option — NO, NC — as per your requirement.
- **Door Group - Tamper:** This is applicable when ARC DC200 is configured as Dual Door Single/Dual Reader. You can configure separate options for each Door. Select the desired tamper option — NO, NC — as per your requirement.
- **Alarm:** Select the check box to set all door-based alarms as active.
- **Tamper Alarm:** Select the check box to activate the Tamper Alarm.



*Alarm is applicable to Door V1, Door V2, Path V1, ARC DC100, ARC DC100 - Dual Door.  
Tamper Alarm is applicable to Door V1, Door V2, Path V1, ARC DC100.*

- **Pulse Timer (sec):** Configure the duration in seconds for which a door will remain in an open state on receiving a valid credential.



*The range (0.1 to 65535.0) seconds for **Pulse Timer** is applicable to ARGO, VEGA, ARGO FACE, ARGO FACE210, PATH V2 and ARC DC200 only.*

- **Auto IP Assignment:** There is option where the door can be assigned its IP from door webpage. Select the check box to enable this option.
- **Network Protocol:** Select the desired Network Protocol option — ICMP or UDP.
- **Tail-Gating:** Tail-gating refers to an access violation which occurs when more than one person tries to enter a secured area using a single person's access credentials.

If the check box is selected, the Occupancy Count of a Zone will be increased/decreased after considering the punch as well as the input from the Auxiliary Input Port.

- **Reset Wait Timer:** To reset the Tail-Gating Count, configure the Reset Wait Timer. Select the desired option — **Door Lock** or **Pulse Timer**.
- **Door Interlock:** Select the check box to enable Door Interlock for the selected door (for example PVR Door). This means if the PVR door is open then other doors will remain close.
- **Door:** Click the **Door** picklist. The **Door** pop-up appears. Select the check boxes of the desired doors to be assigned for the Interlock to the selected door (PVR door). Click **Ok**. The number of selected doors is displayed.

## OR

You can also search for the desired door. To do so, enter the keyword in the Search box. Click **Search**



. The doors will be filtered as per the keyword. Select the check boxes of the desired doors to be assigned for the Interlock to the selected door (PVR door). Click **Ok**. The number of selected doors is displayed.

For Example: If Door V3 and Vega doors are selected for Interlock with PVR door, then if PVR opens, V3 and Vega door will remain close.



*For Degraded mode, Door Interlock feature will not work.*

The **Man Trap Timers — Internal and External Readers** when set, allows you to fix the maximum time within which the user needs to cross the security area.

- **Man Trap Timer — Internal Reader (Sec):** Configure the desired duration in seconds. This is an alarm wait timer on the door to ensure that the user enters the next sequential door of a Man Trap within a specific time-frame.
- **Man Trap Timer — External Reader (Sec):** This is an alarm wait timer on the door to ensure that the user exits the door to enter the next sequential door of a Man Trap within a specific time-frame.

Whenever this timer is configured for a particular door say for internal reader, user is expected to punch on internal reader of other door present in the same zone/door group within the specified Man Trap Timer.

If user fails to do so, Man Trap Violation Alarm will be triggered, if configured.

Unless and until the same user punches on any internal reader in the same zone/group, no user will be allowed to punch on any internal reader in the same zone/group.

- **Duplicate Access Time Interval:** Configure the maximum duration in seconds for which the door should consider a subsequent user punch (after the first successful allowed punch) received as a duplicate punch.



**Duplicate Access Time Interval** is applicable to ARGO, VEGA, ARGO FACE and ARGO FACE210 only.

*The Duplicate Access Time Interval is not applicable:*

- if Duress Finger is detected by the door.
- when PANEL200 is in Degraded mode.
- to Smart Identification users.

Click **Save** to save the settings or click **Cancel** to discard.

## Advance Configuration 2



**Advance Configuration 2** is applicable only for COSEC- Server Mode.

To view the Advance Configuration 2 parameters,

Click **Devices > Door Configuration > Advance Configuration2**. The **Advance Configuration2** page appears

In COSEC- Server Mode, Temporary User Configuration is displayed as configured in the COSEC Server.



- **Temporary Addition of Unknown User:** It displays — Disabled, As Temporary User or As Temporary Worker— as configured in the Server.
- **Add Name via Device:** The check box will appear selected, if enabled in the Server.
- **Confirm before adding Temporary User:** The check box will appear selected, if enabled in the Server.

## Input Output

To configure the Input Output parameters,

Click **Devices > Door Configuration > Input Output**. The **Input Output** page appears.



*The parameters differ according to the Door Type.*

## Door

### Door Sense

- **Enable Door Sense:** Select the check box to enable the door for two-state monitoring.
- **Supervised:** Select the check box to enable the door for four-state monitoring where the door is also monitored for door fault and door disconnection.
- **Door Sense Type:** Select the desired option from the drop-down list — **NC, NO** (Default: NC).

### Door Relay

- **Output Group No. (Unlock):** Click the **Select Output Group** picklist. The **Output Group** pop-up appears. Select the desired group.

#### OR

If required, you can also search for the desired group.

**Search By:** Select the desired option by which you wish to search for the group — Output Group No., Name. In the corresponding box enter the keyword. Click **Search**  . The groups will be filtered as per the keyword. Select the desired group.

- **Output Group No. (Lock):** Click the **Select Output Group** picklist. The **Output Group** pop-up appears. Select the desired group.

#### OR

If required, you can also search for the desired group.

**Search By:** Select the desired option by which you wish to search for the group — Output Group No., Name. In the corresponding box enter the keyword. Click **Search**  . The groups will be filtered as per the keyword. Select the desired group.



*Door Relay is applicable for all doors except ARC IO800.*

*For ARC DC100 - Dual Door configure the above Door Sense and Door Relay parameters for both Door 1 and Door 2 respectively.*

*For ARC DC200/100 - Dual Door, only **Output Group No.** under Door Relay is applicable. The parameters **Output Group No. (Unlock)** and **Output Group No. (Lock)** are not applicable.*

## Lock



*Lock parameters are applicable to ARC DC100/200 only.*

- **Lock Sense:** Select the to enable the lock for two-state monitoring.
- **Lock Sense Type:** Select the desired option — **NC, NO** (Default: NO).

## Auxiliary Input

- **Aux Input Port (Applicable only for ARC IO800):** Select the desired auxiliary input port from the drop-down list.
- **Enable Auxiliary Input:** Select the check box to enable Auxiliary Input (for example, Smoke Detectors) depending on normal door state monitoring.
- **Supervised:** Select the check box to enable Auxiliary Input (for example, Smoke Detectors) depending on supervised door state monitoring.
- **Aux Input Sense Type:** Select the desired option — **NC**, **NO** (Default: NC).
- **Debounce Time (sec):** Configure the duration in seconds. It the minimum duration for which an input interface should remain in a given state before the PANEL200 reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

## Auxiliary Input 2 (Applicable only for ARC DC200 - Single Door)

- **Enable Auxiliary Input:** Select the check box to enable Auxiliary Input (for example, Smoke Detectors) depending on normal door state monitoring.
- **Aux Input Sense Type:** Select the desired option — **NC**, **NO** (Default: NC).
- **Debounce Time (sec):** Configure the duration in seconds. It the minimum duration for which an input interface should remain in a given state before the system reports it. For example, if a Normal door state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated.

## Auxiliary Output

- **Aux Output Port (Applicable only for ARC IO800):** Select the desired auxiliary output port from the drop-down list.
- **Enable Auxiliary Output:** Select the check box to enable Auxiliary Output (for example, Fire Alarm) for the selected door.
- **Output Group No.:** Click the **Select Output Group** picklist. The **Output Group** pop-up appears. Select the desired group.

### OR

If required, you can also search for the desired group.

**Search By:** Select the desired option by which you wish to search for the group — Output Group No., Name. In the corresponding box enter the keyword. Click **Search**  . The groups will be filtered as per the keyword. Select the desired group.

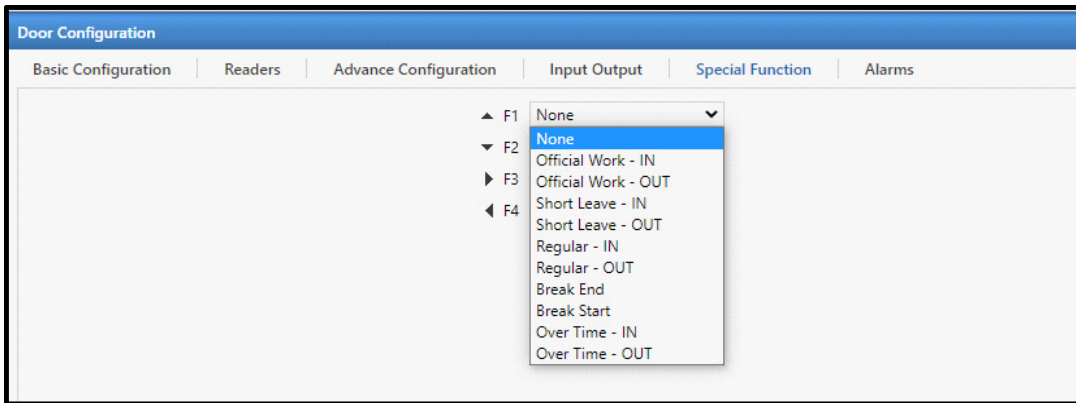
- **Elevator ID (Applicable only for ARC IO800):** Configure the Elevator ID to which the Auxiliary Output Port of the ARC IO800 is linked.
- **Floor No. (Applicable only for ARC IO800):** Configure the floor number to which the Auxiliary Output Port of the ARC IO800 is linked.

Click **Save** to save the settings or click **Cancel** to discard.

## Special Function

To configure the Special Function parameters,

Click **Devices > Door Configuration > Special Function**. The **Special Function** page appears



*Special function is applicable for Door V3, Door V4 and PVR Door. For other doors, refer to “[Special Card](#)” and “[Special Functions](#)”.*

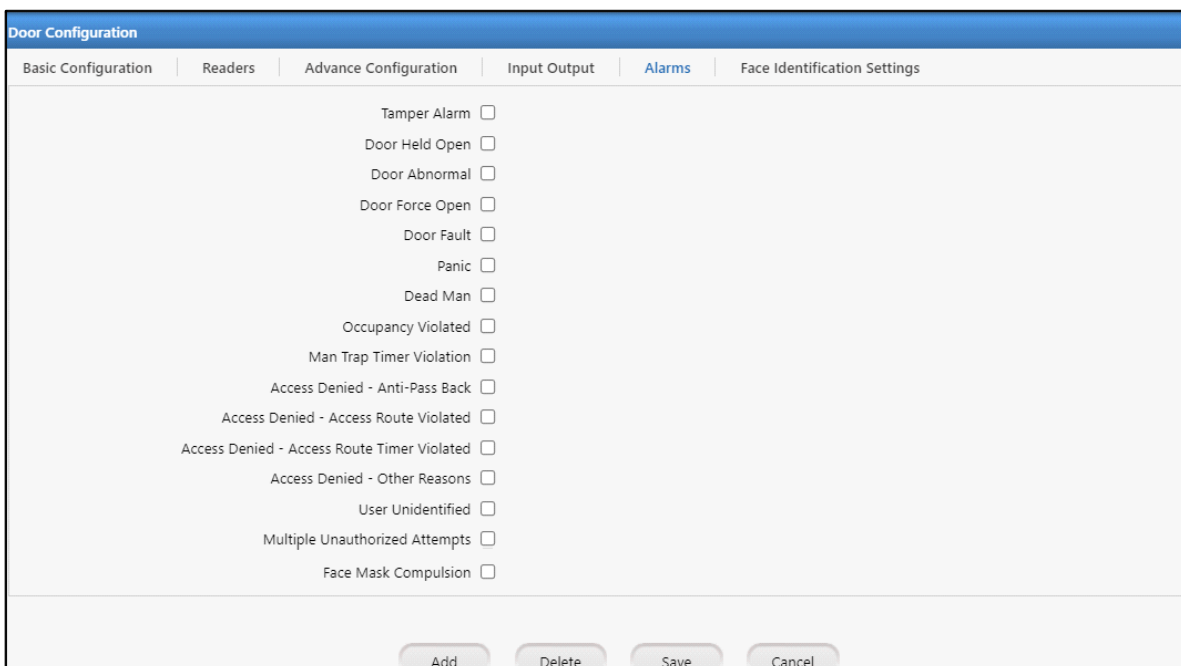
You can map upto 4 Special Functions to the arrow keys on the door keypad. For each arrow key, select the desired Special Function from the drop-down list, you wish to assign.

Click **Save** to save the settings or click **Cancel** to discard.

## Alarms

To configure the Alarm parameters,

Click **Devices > Door Configuration > Alarms**. The **Alarms** page appears.





*Alarms differ according to the Door Type.*

Alarms are required for the PANEL200 to indicate unauthorized access, emergency, tampering or occurrence of some fault etc. Alarms should be monitored, acknowledged and cleared in real time by the person who manages the Access Control System.

All the alarms related to door can be enabled or disabled. Select the check boxes of the alarms, you wish to enable and clear the check boxes of the alarms you wish to disable.

Click **Save** to save the settings or click **Cancel** to discard.

## Face Identification Settings

To configure the Face Identification Settings,

Click **Devices > Door Configuration > Face Identification Settings**. The **Face Identification Settings** page appears



*Face Identification Settings are applicable for ARGO FACE and ARGO FACE210 Door only.*

**Door Configuration**

Basic Configuration | Readers | Advance Configuration | Input Output | Alarms | **Face Identification Settings**

**Face Recognition**

Enable FR ☒

Server Type Local

Capturing Mode Free Scan

Enable Free Scan TimeOut ☐

Free Scan TimeOut 30 seconds (5 - 999)

Identification TimeOut 4 seconds (1 - 99)

Face Matching Score 94.00 (0.0-100.0)

Threshold for Face Detection 50.00 % (0-100)

**Face Enrollment**

Conflict Check ☒

Conflict Matching Threshold (Face) 93.00 % (1.0-99.99)

Add Delete Save Cancel

## Face Recognition

- **Enable FR:** Select the check box to enable the configuration of Face Recognition.
- **Server Type:** This is un-editable and displays Local.
- **Capturing Mode:** Select the desired option from the drop-down list — Tap and Go, Free Scan, Smart.
  - **Tap and Go:** If you select this option, you need to tap on the door display screen once. The motion recording screen appears and the door will capture and identify the user's face.
  - **Free Scan:** If you select this option, the door will display the motion recording screen till the expiry of the Free Scan TimeOut if enabled.

- **Enable Free Scan TimeOut:** Select the check box to enable the Free Scan TimeOut.
- **Free Scan TimeOut:** Configure the duration in seconds. In Free Scan method, multiple users can mark their attendance easily during peak entry hours. For example, if the Free Scan TimeOut is set as 30sec and if the user is identified in 10sec then the Free Scan TimeOut timer is reloaded again reloads after 10sec. Hence, door always remains in the scanning mode.
- **Identification TimeOut:** Configure the duration in seconds after which the face identification will time out.
- **Face Matching Score:** Configure the value in percentage for Face Matching Score. This will be considered while face identification of the user. If the Face Matching Score is set as low (for example, 20), then false matching may occur. If the Face Matching Score is set as high (for example, 70), then more accurate matching of template will be done.
- **Threshold for Face Detection:** Configure the threshold value (in percentage) that determines the confidence level required for the algorithm to recognize a face in a frame. When the system detects a face with a confidence score higher than the specified threshold, the image will be validated and forwarded for further processing.



*If the PANEL200's External Memory Storage exceeds 98%, then PANEL200 will stop face sync with associated doors. Hence, Face Recognition will not function.*

*If the door template count reaches 2 lakhs, even though the door has memory space the Face Recognition for new users will not function.*

*If the door template count is less than 2 lakhs but the doors memory is full, then Face Recognition will function.*

## Face Enrollment

- **Conflict Check:** Select the check box to enable the Conflict Check.
- **Conflict Matching Threshold (Face):** Configure the value in percentage for Conflict Matching Threshold. This will be considered while comparing the detected face with the face templates already present in the database. If a conflict is found, that is, if the PANEL200 detects a face template in the database similar to the new face, then a conflict error will be displayed.

Make sure a higher value is set for this parameter, as it will result in less equivalent matches with the face templates available in the database.

### Example: Face Enrollment of Suresh

- **Conflict Check** check box is selected.
- **Conflict Matching Threshold (Face)** is set as 93%.

Now during the face enrollment of Suresh, the PANEL200 will check in its database if his face matches with the faces of other users available in the database.

- **Case 1:** If Suresh's face matches 92% with Ram, then the PANEL200 will allow to enroll Suresh's face.
- **Case 2:** If Suresh's face matches 94% with Shyam, then the PANEL200 will display the conflict error while enrolling Suresh's face.

**Door Configuration**

Basic Configuration | Readers | Advance Configuration | Input Output | Alarms | **Face Identification Settings**

**Face Enrollment**

Conflict Check ☒

Conflict Matching Threshold (Face) 93.00 % (1.0-99.99)

**Face Antispoofing**

Face Anti-Spoofing ☒

Face Anti-Spoofing Threshold 90.00 % (1.0-99.99)

**Face Mask Compulsion**

Enable ☐ ⓘ

Approach to Camera Wait-Timer (Sec) 3.0

Mask Detection Time Out (Sec) 4

Restriction Type Soft

Face Mask Coverage 98.00 %

Visible Face 99.00 %

Add Delete Save Cancel

## Face Antispoofing

- **Face Anti-Spoofing:** Select the check box to enable Face Anti-Spoofing.
- **Face Anti-Spoofing Threshold:** Configure the threshold value (in percentage) for Face Anti-Spoofing. This parameter is used to verify the liveness of a user's face and determine whether the person is genuine or a spoof attempt (e.g., photo, video, or mask).

A higher threshold ensures stricter validation of liveness, reducing the chances of spoofing attacks being accepted, while a lower threshold may increase convenience but can compromise security.



*For FR Mode as Local, the default value of Face Anti-Spoofing Threshold will be 90.*

*If you upgrade the PANEL200 to V01R18 and later, the value of Face Anti-Spoofing Threshold will be set as 90 by default.*

## Face Mask Compulsion

- **Enable:** Select the check box to enable Face Mask Compulsion.
- **Approach to Camera Wait-Timer (Sec):** Configure the duration in seconds within which the user should approach the camera for face mask detection.
- **Mask Detection Time Out (Sec):** Configure the duration in seconds after which the mask identification timer will expire.
- **Restriction Type:** Select the desired type of restriction from the drop-down list — Soft or Hard.

If the restriction type is set as **Soft** and if a user is identified without mask, an event will be generated and the user will be allowed access.

If the restriction type is set as **Hard** and if a user is identified without mask, an event will be generated but the user will be denied access.



*If the Restriction Type is set as Soft and a user is detected without mask, the user will be allowed access and **User Allowed- Face Mask Not Detected** alert will be triggered, if configured. In “[Alert Message Configuration](#)”, select Event Type as **Access Control** and Event as **User Allowed- Face Mask Not Detected**.*

*If the Restriction Type is set as Hard and a user is detected without mask, the user will not be allowed access and **User Denied- Face Mask Not Detected** alert will be triggered, if configured. In “[Alert Message Configuration](#)”, select Event Type as **Access Control** and Event as **User Denied- Face Mask Not Detected**.*

- **Face Mask Coverage:** Configure the minimum percentage required for considering face as covered with the mask valid for Face Mask Compulsion at the time of user identification. Set higher percentage values for accurate face mask detection.
- **Visible Face:** Configure the maximum percentage required for the face to be visible during user enrollment/ identification. Set higher percentage value to identify or enroll face without mask accurately.

Click **Save** to save the settings or click **Cancel** to discard.



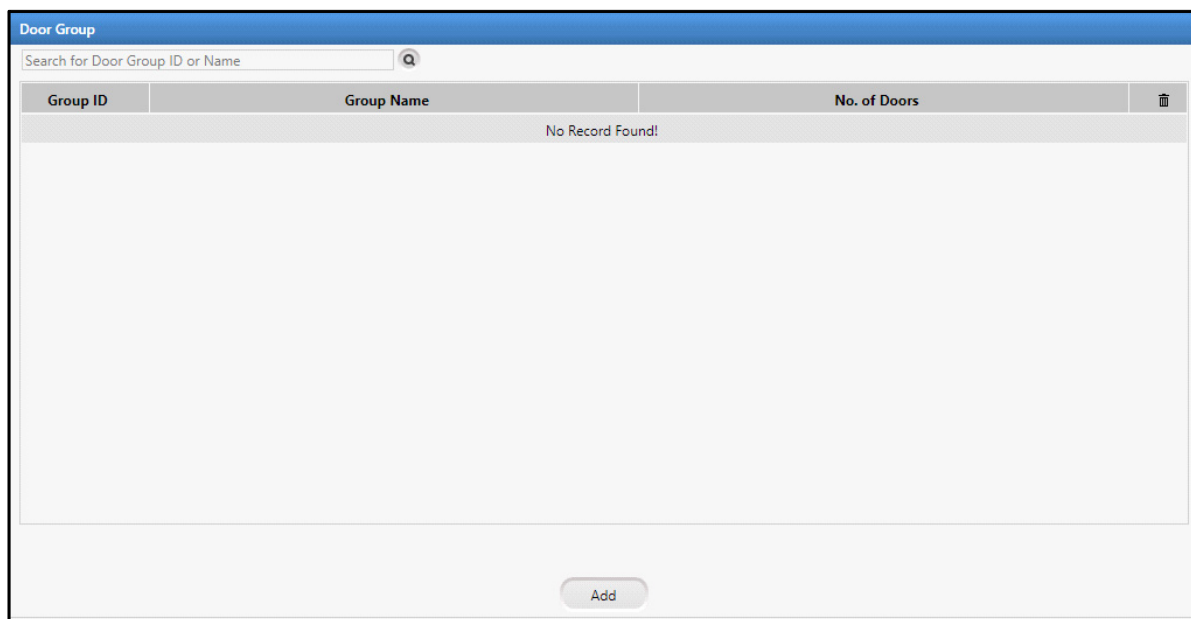
# Door Group

---

You can configure the Door Group with multiple doors. A single door can be added to multiple Door Groups. These groups are assigned to the users, to allow selective access.

To configure the Door Group parameters,

Click **Devices > Door Group**. The **Door Group** page appears.



All the added groups appear in the grid with their details — Group ID, Group Name, No. of Doors. To add a new Door Group, refer to [“Adding Door Groups”](#).

You can click the desired Door Group and edit its configuration as per your requirement.

You can also delete any Door Group. To do so, click **Delete**  corresponding to the desired Door Group.

You can search for the desired door groups using the **Search** bar. Enter the keyword according to which you wish to search. The search will be carried out in the Group ID and Group Name column only. Click **Search** . The Door Groups will be filtered as per the entered keyword.

## Adding Door Groups

Click **Add**. You can configure a maximum of **99** Door Groups and each Door Group can have upto **255** doors.

| Door ID          | Door Name |  |
|------------------|-----------|--|
| No Record Found! |           |  |

Configure the following parameters:

- **Door Group ID:** The Door Group ID is auto-generated by the PANEL200.
- **Door Group Name:** Configure a name you wish to assign to the Door Group.
- **Door:** Click the **Select Door** picklist. The **Door** pop-up appears. Select the check boxes of the desired doors you wish to add to the group. You cannot add one door to multiple groups.

### OR

You can search for the desired doors using the Search bar. Enter the keyword according to which you wish to search. The search will be carried out in the Door ID and Door Name column only. Click **Search** . The doors will be filtered as per the entered keyword. Select the check boxes of the desired doors you wish to add to the group. You cannot add one door to multiple groups.

- The doors added to the group appear in the right pane.

Door Group ID

1

Door Group Name

Door Group 1

Door

| Door ID | Door Name      |  |
|---------|----------------|--|
| 5       | ARC IO800 Door |  |
| 6       | VEGA           |  |
| 15      | ARGO           |  |

1

Add

Delete

Save

Cancel

You can delete any added door. To do so, click **Delete**  corresponding to the desired door.

- Click **Save**.

After you have completed all the configurations of the Door Group and if you wish to view all the created Door Groups, click **View List** .

Door Group ID

1

Door Group Name

Door Group 1

Door

| Door ID | Door Name      |  |
|---------|----------------|--|
| 5       | ARC IO800 Door |  |
| 6       | VEGA           |  |
| 15      | ARGO           |  |

1

Add

Delete

Save

Cancel

The Door Group page displays all the created Door Groups.

Door Group



| Group ID | Group Name   | No. of Doors |                                                                                     |
|----------|--------------|--------------|-------------------------------------------------------------------------------------|
| 1        | Door Group 1 | 3            |  |

1

Add

You can delete any created Door Group. To do so, click **Delete**  corresponding to the desired Door Group.

# Video Surveillance

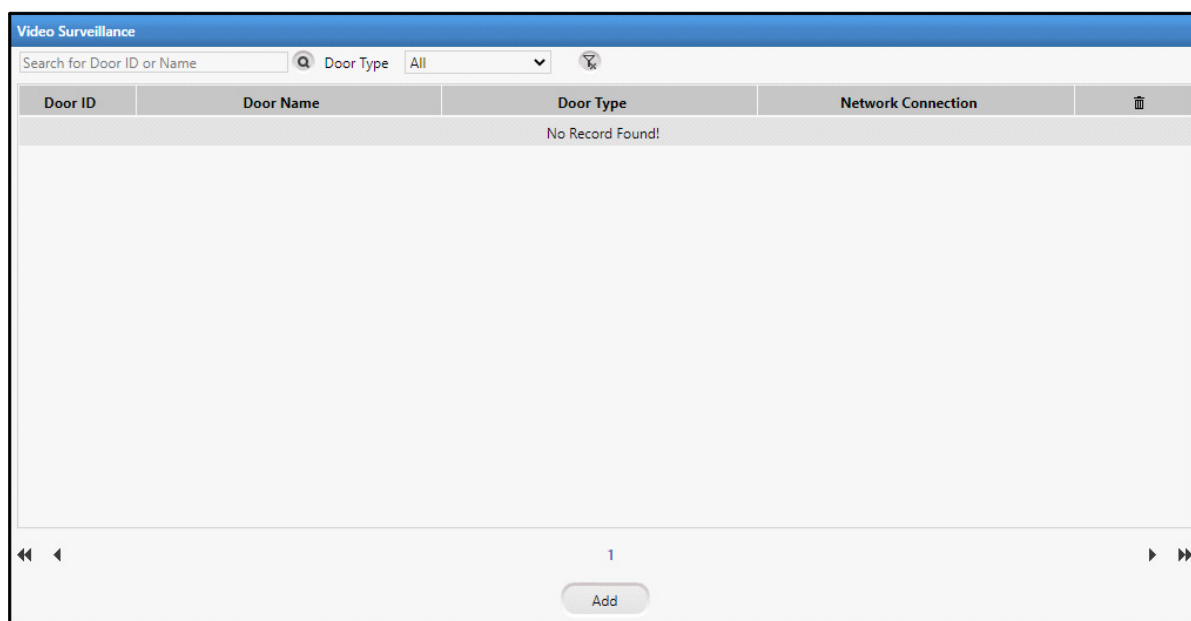
You can integrate PANEL200 with Matrix Network Video Recorder (NVR) and Hybrid Video Recorder (HVR)<sup>2</sup> to get images and videos triggered by the user events at the door.

For ARGO FACE/ARGO FACE210 Door, you can configure the Built-In Camera to get images triggered by the user events.



To configure the Video Surveillance parameters,

Click **Devices > Video Surveillance**. The **Video Surveillance** page appears.



All the Video Surveillance Integrations (that is, desired doors integrated with the SATATYA NVR/HVR) appear in the grid with their details — Door ID, Door Name, Door Type and Network Connection. To add a new Door Integration, refer to [“New Video Surveillance Integration”](#).

You can click the desired Video Surveillance Integration and edit its configuration as per your requirement.

---

2. *We have discontinued HVR.*

You can also delete any Video Surveillance Integration. To do so, click **Delete**  corresponding to the desired Video Surveillance Integration.

You can [“Search”](#) for the desired Video Surveillance Integrations or apply the [“Filter”](#) — Door Type — as per which you wish to view the Integrations.

## Search

You can search for the desired Integrations using the **Search** bar. Enter the keyword according to which you wish to search. The search will be carried out in the Door ID and Door Name column only. Click **Search**  The Integrations will be filtered as per the entered keyword.

## Filter

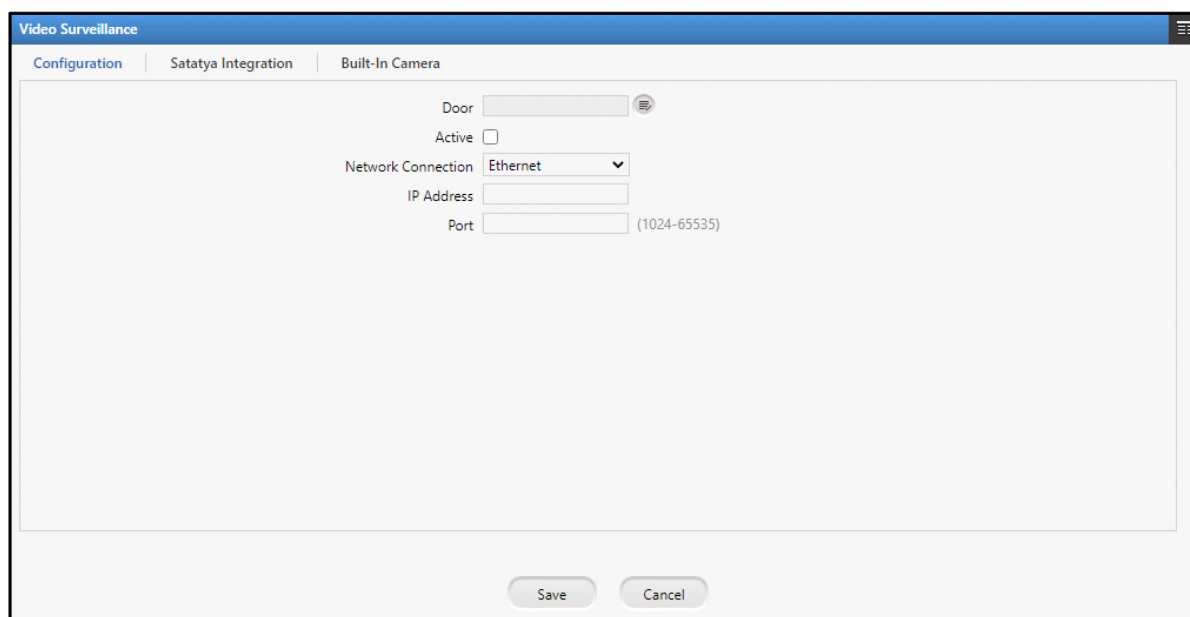
You can also filter the Integrations by applying the Door Type filter. To do so, in **Door Type**, select the desired door from the drop-down list. The Integrations will be displayed as per the set filter.

To clear the set filter, click **Clear Filter**  .

## New Video Surveillance Integration

To add a new Video Surveillance Integration,

Click **Add**. You can add upto 255 integrations. For each door only one integration can be added.



The screenshot shows a web application window titled "Video Surveillance". It has three tabs: "Configuration" (selected), "Satatya Integration", and "Built-In Camera". The "Configuration" tab contains the following fields:

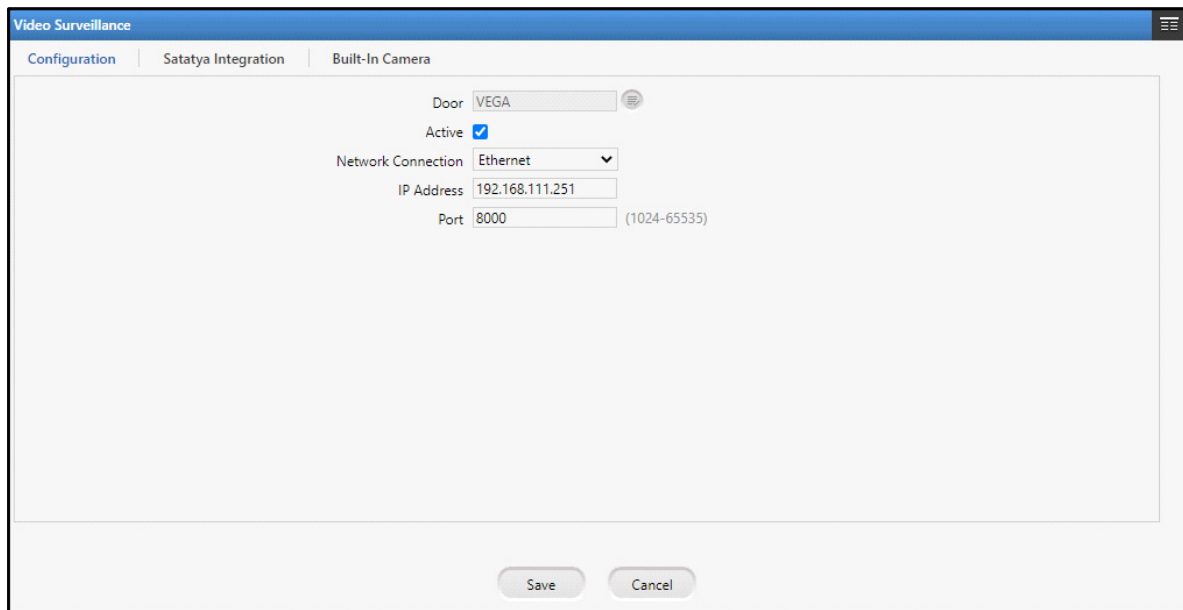
- Door: A text input field with a dropdown arrow icon.
- Active: A checkbox.
- Network Connection: A dropdown menu with "Ethernet" selected.
- IP Address: A text input field.
- Port: A text input field with the value "(1024-65535)" displayed next to it.

At the bottom of the window, there are two buttons: "Save" and "Cancel".

The Video Surveillance allows you to:

- configure the configuration parameters. For details, refer to [“Configuration”](#).
- configure the Satatya Integration parameters. For details, refer to [“Satatya Integration”](#).
- configure the Built-In camera parameters. For details, refer to [“Built-In Camera”](#).

## Configuration



The screenshot shows a web-based configuration interface for a video surveillance system. The title bar is 'Video Surveillance'. There are three tabs: 'Configuration' (selected), 'Satatya Integration', and 'Built-In Camera'. The 'Configuration' tab is active, showing a form with the following fields: 'Door' with a dropdown menu showing 'VEGA', 'Active' with a checked checkbox, 'Network Connection' with a dropdown menu showing 'Ethernet', 'IP Address' with a text field containing '192.168.111.251', and 'Port' with a text field containing '8000'. To the right of the port field is a range indicator '(1024-65535)'. At the bottom of the form are 'Save' and 'Cancel' buttons.

Configure the following parameters:

- **Door:** Click the **Select Door** picklist. The **Panel Doors** pop-up appears. Select the door you wish to integrate with the Network Video Recorder.

**OR**

You can search for the desired doors using the Search bar. Enter the keyword according to which you wish to search. The search will be carried out in the Door ID and Door Name column only. Click **Search** . The doors will be filtered as per the entered keyword. Select the door you wish to integrate with the Network Video Recorder.



*Once you save the selected door with these configurations, you will not be able to change the selected door. However, you will be able to edit the other parameters.*

- **Active:** Select the check box to enable.
- **Network Connection:** Select the desired network connection option — Ethernet, Broadband, Wireless — using which you wish to establish connectivity.
- **IP Address:** Configure the IP Address of SATATYA NVR/ HVR which you wish to use for surveillance.
- **Port Number:** Configure the Port number of NVR/HVR on which the door will connect with the Network Video Recorder. The default port is 8000.

Click **Save** to save the settings or click **Cancel** to discard.

## Satatya Integration



*Satatya Integration is not applicable for ARGO FACE and ARGO FACE210 Door.*

To configure the Satatya Integration parameters,

Click **Devices > Satatya Integration**. The **Satatya Integration** page appears.

Configure the following parameters to create a schedule:

- **ID:** The ID is auto-generated by the PANEL200. This is the first serial number in the grid below.
- **Name:** Configure a name you wish to assign to the event- action schedule.
- **Active:** Select the check box to enable the schedule.
- **Schedule:** Configure the time duration of the schedule. That is, the start and end time in HH:MM format of the schedule.
- **Days:** Select the check boxes for the desired days of the week on which you wish run the schedule.  
  
**For example:** A schedule from 09:00 to 18:00 can be configured for working days (Monday to Friday) to monitor the exit of the employees from the working area.
- **Event:** Select the desired event from the drop-down list for which the corresponding action is to be configured.
- **Mode:** Select the desired mode from the drop-down list — Entry, Exit or Both.
- **Action:** Select the desired action to be taken by the SATATYA device from the drop-down list. The options are — Recording, Image Upload, Video Pop-up, PTZ Preset, Mail Image.
  - If you select **Recording**, configure the duration (in minutes) of recording in **Duration** as well as select the check boxes of the desired **Camera** channels.



- If you select **Upload Image**, select the check boxes of the desired **Camera** channels. Images will be uploaded as per the FTP settings.
- If you select **Video Pop-up**, configure the duration (in seconds) for which the video pop-up must appear in **Duration** as well as select the check boxes of the desired **Camera** channels. The video pop up will be generated on the Local Client of SATATYA device for the selected cameras.
- If you select **PTZ Preset**, configure the desired **PTZ Position Number** as defined in the SATATYA device as well as select the check boxes of the desired **Camera** channels.
- If you select **Mail Image**, configure the desired Email Address in **Email ID** as well as select the check boxes of the desired **Camera** channels.
- Click **Add** to complete the process of linking the event with the action.

The integrated event and action appears in the grid as per the configurations done.

For example: For Access Allowed event on door, the video pop-up of Camera 12 will appear for 10 seconds.

| Sr. No. | Name           | Event          | Action       | Start Time | End Time | Active |    |
|---------|----------------|----------------|--------------|------------|----------|--------|---------------------------------------------------------------------------------------|
| 1       | Access Allowed | Access Allowed | Video Pop-Up | 09:00      | 18:00    | Active |   |
| 2       |                |                |              |            |          |        |  |
| 3       |                |                |              |            |          |        |  |

Similarly, you can configure other events and actions as per your requirement. You can configure upto three event-action schedules.

To configure another event-action schedule, click on the Sr.No.2 row and follow the same steps as mentioned above.

| Sr. No. | Name           | Event          | Action       | Start Time | End Time | Active |  |
|---------|----------------|----------------|--------------|------------|----------|--------|---------------------------------------------------------------------------------------|
| 1       | Access Allowed | Access Allowed | Video Pop-Up | 09:00      | 18:00    | Active |  |
| 2       | Access Denied  | Access Allowed | Upload Image | 09:00      | 18:00    | Active |  |
| 3       |                |                |              |            |          |        |  |

You can update a schedule, if required. Select the desired schedule from the grid and make the desired changes as per your requirement. Click **Update** to save the schedule.

You can also delete a schedule, if required. To do so, click **Delete**  corresponding to the desired schedule.

## Built-In Camera



**Built-In Camera** is applicable for ARGO FACE and ARGO FACE210 Door only.

You can create schedules for capturing snapshots for User Allowed/Denied events.

To configure the Built-In Camera parameters,

Click **Devices > Video Surveillance > Built-In Camera**. The **Built-In Camera** page appears.

| Sr. No. | Name | Event | Start Time | End Time | Active |  |
|---------|------|-------|------------|----------|--------|--|
| 1       | test | Both  | 09:00      | 23:00    | Active |  |
| 2       |      |       |            |          |        |  |
| 3       |      |       |            |          |        |  |

Configure the following parameters to create schedule,

- **ID:** This is auto-generated and is the first serial number of the grid.
  - **Name:** Configure a name you wish to assign to the event- action schedule.
  - **Active:** Select the check box to enable the schedule.
  - **Schedule:** Configure the time duration of the schedule. That is, the start and end time in HH:MM format of the schedule. This is duration for which the door will capture snapshots for the selected event.
  - **Days:** Select the check boxes for the desired days of the week on which you wish to run the schedule.
- For example:** A schedule from 08:00 to 10:00 can be configured for working days (Monday to Friday) to monitor the entry of employees at the main gate.
- **Event:** Select the event from the drop-down list for which the door should capture snapshots.
  - Click **Add** to add the schedule for the selected event. The configured schedule will appear in the grid on the first serial number. Maximum 99 schedules can be created for one ARGO FACE/ARGO FACE210 Door.

**Video Surveillance**

Configuration | Satatya Integration | Built-In Camera

ID:

Name:

Active: ☒

Schedule:  to

Days: ☐ Sun ☒ Mon ☒ Tue ☒ Wed  
☒ Thu ☒ Fri ☐ Sat ☐ Holiday

Event:

| Sr. No. | Name           | Event          | Start Time | End Time | Active |  |
|---------|----------------|----------------|------------|----------|--------|--|
| 1       | Access Allowed | Access Allowed | 09:00      | 18:00    | Active |  |
| 2       |                |                |            |          |        |  |
| 3       |                |                |            |          |        |  |

1 2 3 4 5 6 7 8 9 10

To add another schedule, click the desired serial number from the grid and follow the same steps as mentioned above.

**Video Surveillance**

Configuration | Satatya Integration | Built-In Camera

ID:

Name:

Active: ☒

Schedule:  to

Days: ☒ Sun ☒ Mon ☒ Tue ☒ Wed  
☒ Thu ☒ Fri ☒ Sat ☒ Holiday

Event:

| Sr. No. | Name           | Event          | Start Time | End Time | Active |  |
|---------|----------------|----------------|------------|----------|--------|--|
| 1       | Access Allowed | Access Allowed | 09:00      | 18:00    | Active |  |
| 2       | Access Denied  | Access Denied  | 00:00      | 23:59    | Active |  |
| 3       |                |                |            |          |        |  |

1 2 3 4 5 6 7 8 9 10

You can update a schedule, if required. To do so,

- Select the desired schedule and edit it as required.
- Click **Update** to update the schedule.

If you wish to delete a schedule, click **Delete** corresponding to the desired schedule.

All the captured snapshots for the configured events will be displayed in the Event Logs. For details, refer to [“Event Logs”](#). The count of captured snapshots will be displayed on the Storage Details page. For details, refer to [“Storage Details”](#). The maximum count of captured snapshots can be 2000.



*Make sure SD Card is present in the PANEL200 for storing the snapshots.*



On exceeding 80% of the threshold snapshot count, the **Captured Snapshot Count Full** alert will be triggered if configured. In [“Alert Message Configuration”](#), select Event Type as **System** and Event as **Captured Snapshot Count Full**.

On reaching 100% of the threshold snapshot count,

- the **Captured Snapshot Count Full** alert will be triggered if configured in [“Alert Message Configuration”](#). Select Event Type as **System** and Event as **Captured Snapshot Count Full**.
- when the next snapshot is received, the first snapshot will be overwritten and so on.

Capture Snapshot functionality is not supported in Degraded mode.

When the PANEL200 event storage limit is reached and the next snapshot is received on reaching the threshold snapshot count, the first snapshot will be overwritten and so on.

---

The Master allows you to:

- configure different card formats. For details, refer to [“Card Format”](#).
- configure card personalization. For details, refer to [“Card Personalization”](#).
- configure the wiegand formats. For details, refer to [“Wiegand Format”](#).

# Card Format

---

All cards store a sequence of numbers which can be read by card reader devices, when a card is presented. This unique card number sequence is then verified against the enrolled user in the access control system to allow access to the card-holder. Hence, the pattern or structure of this card number must be compatible with the corresponding card reader format to support identification. This programmable data pattern of a the card is known as Card Format.

Different card manufacturers across the industry provide some standard as well as proprietary card formats. However, organizations may require a flexible format to match their site requirements. PANEL200 provides the option, wherein you can write your own card format which are compatible with your access control system.

You can assign maximum 5 card formats to Internal as well as External Readers.

You can create upto 9 Card Formats. Custom Formats allow enhance security by:

- Setting formats of up to 128 bits.
- Providing the option to add Facility Code to the Card Serial Number.
- Adding Parity bits for added accuracy of sent data.

## CARD FORMAT

You can select maximum 5 card formats for Internal as well as External Readers.

How it works:

- When you present the card on a reader then received bits will be compared with the configured card reader's configurable bits.
- The card format will be applied to the card whose configurable bits matches with the received bits.
- If a card is detected for which received bits do not match with any of the configured bits then default format for that card will be used.
- If there are two or more card formats assigned in a device whose configurable bits are same then card formats based on Format ID will be applied.

**Case1:** If there are five formats configured for a reader. Formats 3 and 5 have same number of configurable bits equal to 26 bits. Now, a 26 bit card is presented on the reader. Then, only format 3 will be applied on the card.

**Case 2:** If a card format is configured as follows:

Truncate to bits = 24

Read Order = Reverse Bit Wise

Configurable Bits = 26

Sequence of Operation = Bit Configuration then Reading Order

Bit Configuration:

Bit 1: Odd Parity

Bit 2-9: FC

Bit 10-25: CSN

Bit 26: Even Parity

Now, if a 26 bit card is presented on the reader then as configurable bits are also 26 this format should be applied. However, after truncation the bits length must be 24. So, last 2 bits (MSB) should be discarded/ ignored in bit configuration. After that bit reversal will be done.

**Case 3:** If a card format is configured as follows:

Truncate to bits = 24

Read Order = Reverse Bit Wise

Configurable Bits = 26

Sequence of Operation = Reading Order then Bit Configuration

Bit Configuration:

Bit 1: Odd Parity

Bit 2-9: FC

Bit 10-25: CSN

Bit 26: Even Parity

Now, if a 26 bit card is presented on the reader then as configurable bits are also 26 this format should be applied. Now truncated Bits = 24. First 26 bits will be reversed and then bit configuration will be applied for first 24 bits only. Last 2 bits after reversal will be discarded.

To configure the Card Formats,

Click **Masters > Card Format**. The **Card Format** page appears.

| ID | Name           |  |
|----|----------------|--|
| 1  | Default Format |  |
| 2  |                |  |
| 3  |                |  |
| 4  |                |  |
| 5  |                |  |
| 6  |                |  |
| 7  |                |  |
| 8  |                |  |
| 9  |                |  |

You can configure upto 9 Card Formats. Configure the following parameters:

- **ID:** At ID 1, the Default Format is configured. Click on the desired ID in the right pane for which you wish to configure the Card Format.
- **Name:** Configure a name you wish to assign to the Card Format.
- **Configure (Bits):** Configure the number of bits that need be configured in the card structure. If the number of bits received at the card reader is greater than the number of configured bits, then Default Card Format will be applicable for the reader. As soon as you configure the number of bits, the **Bit Configuration** grid appears.

| ID | Name           |
|----|----------------|
| 1  | Default Format |
| 2  | Card Format 1  |
| 3  |                |
| 4  |                |
| 5  |                |
| 6  |                |
| 7  |                |
| 8  |                |
| 9  |                |

- **Truncate To (Bits):** Configure the maximum number of bits that will be allowed for the card format.
- **Read Order:** The Read Order parameter indicates the sequence in which the card serial number must be read by the card reader. Select the desired option from the drop-down list:
  - **Forward:** If you select this option, the bits will be processed in the order of their arrival.
  - **Reverse bitwise:** If you select this option, all incoming bits will be received and then reversed before processing them further.
  - **Reverse bytewise:** If you select this option, each incoming byte will be reversed separately and then used for further processing.
- **Sequence of Operation:** Select the desired option from the drop-down list. On the basis of the option selected, the sequence of operation will be decided, that is, which operation (Read Order or Bit Configuration) needs to be performed first and then followed by the other.
- **Include FC in Card No.:** Select the check box, to ensure that the Card Number or Card ID includes Facility Code as well.

## Bit Configuration

- In **Bit Configuration**, all configurable bits of the card data will appear numerically in a serial order, from left to right, as boxes as per the number of bits entered in **Configure**.

For example, if you set Configurable bits as 32, then a grid from 1 to 32 will be created. Here, each box represents a bit.



Card Format

ID: 2

Name: Card Format 1

Configure: 32 Bits (0-128)

Truncate To: 64 Bits (1-128)

Read Order: Forward

Sequence of Operation: Reading Order then Bit Configuration

Include FC in Card No. ☒

Bit Configuration

Select a color and click on Bits to define Card Reading Pattern

Even Parity ☐

Odd Parity ☒

Facility Code ☐

Card Number ☐

| ID | Name           |  |
|----|----------------|--|
| 1  | Default Format |  |
| 2  | Card Format 1  |  |
| 3  |                |  |
| 4  |                |  |
| 5  |                |  |
| 6  |                |  |
| 7  |                |  |
| 8  |                |  |
| 9  |                |  |

Save Cancel

You can add **Parity** and **Facility Code** to the Card Number. For this, in the **Color Selection** area, click to select the color box which represents the bit type to be added to the card number. Then click on the number in the grid where the selected bit type is to be placed.

For example, if you select Odd Parity (dark blue color) and select 10 and 11 from 32 configurable bits. Then these 2 bits will be set with Odd parity and rest with card number.

Card Format

ID: 2

Name: Card Format 1

Configure: 32 Bits (0-128)

Truncate To: 64 Bits (1-128)

Read Order: Forward

Sequence of Operation: Reading Order then Bit Configuration

Include FC in Card No. ☒

Bit Configuration

Select a color and click on Bits to define Card Reading Pattern

Even Parity ☐

Odd Parity ☒

Facility Code ☐

Card Number ☐

Color Select Area

| ID | Name           |  |
|----|----------------|--|
| 1  | Default Format |  |
| 2  | Card Format 1  |  |
| 3  |                |  |
| 4  |                |  |
| 5  |                |  |
| 6  |                |  |
| 7  |                |  |
| 8  |                |  |
| 9  |                |  |

Save Cancel

- Click **Save** to save the settings. The Card Format appears in the right pane.

Similarly, you can add other Card Formats.

You can edit or delete any Card Formats, except the Default Card Format.

To edit, click the desired Card Format from the right pane and edit its parameters as per your requirement. Click **Update**.

To delete, click **Delete**  corresponding to the desired Card Format.

Once the Card Formats are configured these appear as the Card Format options in “[Internal Readers](#)” and “[External Reader](#)”. You can select the desired option as per your requirement.

# Card Personalization

You can configure the memory mapping of Smart Cards as per your requirement. You can configure your own card format by adding user-defined fields as well as modifying length, type and location of predefined fields on the available memory sectors in specific HID iClass and MiFare cards. A maximum of 99 fields can be configured for each personalized format out of which 24 fields are predefined.

Card Personalization allows you to:

- add or modify fields such as name, ID, department, shift, fingerprint templates etc. to be written on the Smart Card. For details, refer to [“Fields”](#).
- configure a field profile based on card type and card mode. For details, refer to [“Configuration”](#).

To configure the Card Personalization parameters,

Click **Masters > Card Personalization > Fields**. The **Fields** page appears.

Card Personalization

Fields | Configuration

Field Name: 30 Chars

Field Type: text

Max Field Length (Bytes):

Add Cancel

| Index | Field Name               | Field Type | Length (Bytes) |  |
|-------|--------------------------|------------|----------------|--|
| 1     | Facility Code            | Numeric    | 2              |  |
| 2     | Additional security code | Numeric    | 2              |  |
| 3     | User ID                  | Numeric    | 4              |  |
| 4     | Value                    | Numeric    | 4              |  |
| 5     | User Name                | text       | 15             |  |
| 6     | Designation              | text       | 15             |  |

1 2 3 4

Save Cancel

## Fields

Configure the following parameters:

The Index 1 to 50 are reserved for predefined fields. By default, predefined fields are available from Index 1 to 24. These predefined fields can be modified. To do so, select the desired field from the grid. You can edit the Field Type and Max Field Length (Bytes). The predefined fields cannot be deleted.

You can also add other fields as per your requirement. These will be added from Index 51 onwards, till 99.

- **Field Name:** Configure a name you wish to assign to the field.
- **Field Type:** Select the desired option — Text, Date, Numeric — from the drop-down list.

The screenshot shows the 'Card Personalization' window with the 'Configuration' tab selected. It contains configuration options for a field: Field Name (Date of Birth), Field Type (Date), Date Type (ASCII), Date Format (ddmmyy), Separator (None), and Max Field Length (Bytes) (6). Below these are 'Add' and 'Cancel' buttons. A table lists predefined fields with their indices, names, types, and lengths. At the bottom are 'Save' and 'Cancel' buttons.

| Index | Field Name              | Field Type | Length (Bytes) |  |
|-------|-------------------------|------------|----------------|--|
| 19    | Door Mode               | Numeric    | 1              |  |
| 20    | User Finger template 1  | Raw        | 384            |  |
| 21    | User Finger template 2  | Raw        | 384            |  |
| 22    | Card id                 | Numeric    | 16             |  |
| 23    | Smart Access Route ID   | Numeric    | 1              |  |
| 24    | Smart Access User Level | Numeric    | 1              |  |

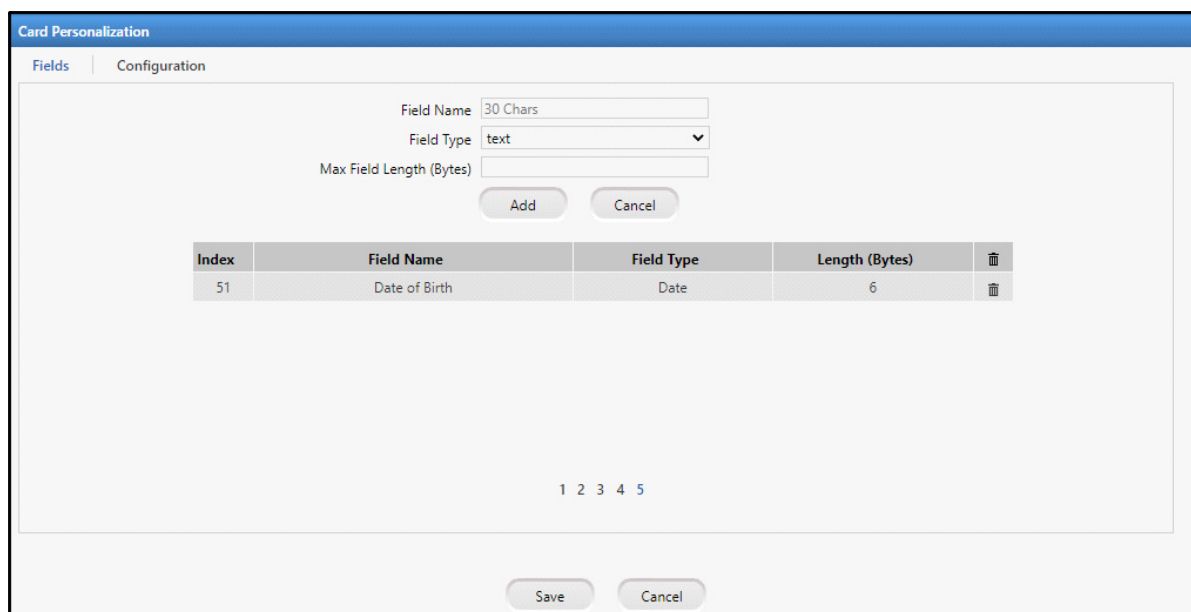
- **Max Field Length (Bytes):** If you select **Text** or **Numeric** as the Field Type, configure the maximum length you wish to allow for the field in bytes.

If you select **Date** as the Field Type, configure the following:

- **Date Type:** Select the desired option — **HEX**, **BCD**, **ASCII** — from the drop-down list.
- **Date Format:** Select the desired format from the drop-down list.
- **Separator:** This will appear only if you have selected the Date Type as **ASCII**. Configure the desired option from the drop-down list.
- **Max Field Length (Bytes):** This will be displayed automatically according to the selected Field Type and is un-editable.
- Click **Add**. The new field will be added in the grid at Index 51. These new fields can be edited or deleted.

To edit, select the desired field from the grid. Edit it as per your requirement and click **Update**.

To delete, click **Delete**  corresponding the desired field in the grid.



The 'Card Personalization' window has two tabs: 'Fields' and 'Configuration'. The 'Fields' tab is active, showing a form with the following fields:

- Field Name: 30 Chars
- Field Type: text (dropdown)
- Max Field Length (Bytes):

Below the form are 'Add' and 'Cancel' buttons. A table below shows the current configuration:

| Index | Field Name    | Field Type | Length (Bytes) |                                                                                     |
|-------|---------------|------------|----------------|-------------------------------------------------------------------------------------|
| 51    | Date of Birth | Date       | 6              |  |

At the bottom of the table are page numbers: 1 2 3 4 5. At the bottom of the window are 'Save' and 'Cancel' buttons.



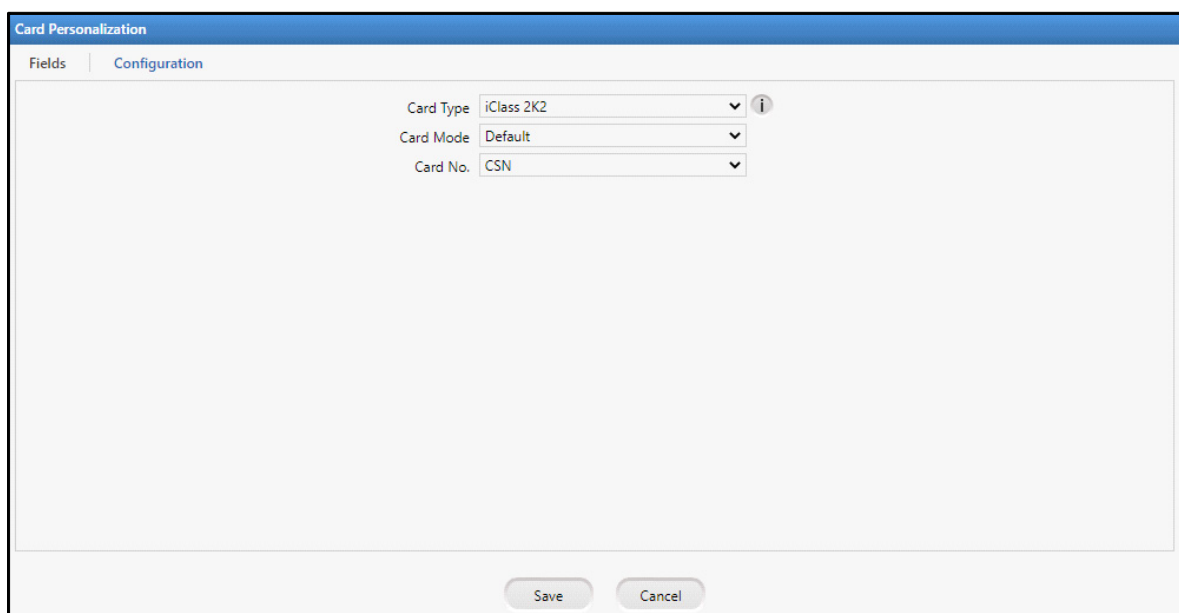
*If any predefined field types are changed from text to numeric, then make sure only numeric values are configured in such fields. If any mismatch occurs, then while writing or reading information from card, conversion process will not take place and the field will remain Blank.*

## Configuration

You can assign the configured Fields to Card Types according to your requirement.

To configure the Configuration parameters,

Click **Masters > Card Personalization > Configuration**. The **Configuration** page appears.



The 'Card Personalization' window has two tabs: 'Fields' and 'Configuration'. The 'Configuration' tab is active, showing the following fields:

- Card Type: iClass 2K2 (dropdown)
- Card Mode: Default (dropdown)
- Card No.: CSN (dropdown)

At the bottom of the window are 'Save' and 'Cancel' buttons.

Configure the following parameters:

- **Card Type:** Select the desired iClass or Mifare option from the drop-down list. Hover-over Info  to view the details of the selected option. The following details are displayed — Total No. of Pages, Total writeable Memory, Total Memory.
- **Card Mode:** If you select the Card Type as any iClass option, then you can configure the Card Mode. Select the desired option — Default, Custom — from the drop-down list.
  - **Default:** Select the Card Mode as **Default** to use the Default Card Format where location of each field is fixed as per Card Type you select.
    - **Card No.:** If Card Mode is selected as **Default**, select the desired Card Number option to be used — CSN, UID (Universal Identifier number). In this case the original CSN or UID will be used.



*UID is applicable to iClass Cards only.*

- **Custom Mode:** Select the Card Mode as **Custom**, if you wish to configure all the predefined fields locations as per your requirement. For details, refer to [“Field Profile”](#).
- **Card No.:** If Card Mode is selected as **Custom**, select the desired Card Number option — CSN, UID, Custom — to be used.

You can use the original **CSN or UID** or you can select **Custom** to use the card number defined at the time of enrollment. While location of CSN is fixed, it is mandatory to define a [“Field Profile”](#) for Custom Card Nos.



*UID is applicable to iClass Cards only.*

- **Read CSN:** Select the check box, the CSN number will be read if the PANEL200 is unable to read the Custom Number.

## Field Profile

If Custom is selected as the Card Mode, for each selected field the location on the card memory can be defined. Maximum 99 new fields can be added.

You can Search for the desired fields. To do so,

- **Field:** Click the **Field** picklist. The **Fields** pop-up appears. Click to select the desired field.

**OR**

If required, you can also search for the desired field.

**Search By:** Select the desired option by which you wish to search for the field — Index, Name, Type. In the corresponding box enter the keyword. Click **Search** . The fields will be filtered as per the keyword. Click to select the desired field.

- **Length:** This is displayed automatically as per the selected Field.
- **Page:** Select the desired page. This differs according to the selected Card Type.

- **Block:** Select the desired block. This differs according to the selected Card Type.
- **Bytes:** Configure the number of bytes to be used. This differs according to the selected Card Type.
- Click **Add**. The configured field appears in the grid.

Card Personalization

Fields | Configuration

Card Type: iClass 16K2  
 Card Mode: Custom  
 Card No.: CSN  
 Read CSN: ☐

Field Profile

Field: Index | Name  
 Length (Bytes):  
 Page: 0  
 Block: 19  
 Byte: 0

Add Cancel

| Field     | Start Position (Page-Block-Byte) | End Position (Page-Block-Byte) | Length (Bytes) |  |
|-----------|----------------------------------|--------------------------------|----------------|--|
| User ID   | 0-19-0                           | 0-19-3                         | 4              |  |
| User Name | 0-20-0                           | 0-21-6                         | 15             |  |

Save Cancel

You can edit or delete the fields from the grid.

To edit, click on the desired field and edit the details as per your requirement. Click **Update**.

To delete, click **Delete** corresponding to the desired Field.

Click **Save** to save the settings or click **Cancel** to discard.

# Wiegand Format

Wiegand Readers can send outputs in standard formats, actual information as well as in custom data format. For custom data formats the structure can be defined. You can create and save multiple profiles for different Wiegand Output Formats. Based on the output required, Wiegand Output Format must be selected for allowed and denied events in “Wiegand” in “Advanced Profile”.

To configure the Configuration parameters,

Click **Masters > Wiegand Format**. The **Wiegand Format** page appears

| ID | Name |  |
|----|------|--|
| 1  |      |  |
| 2  |      |  |
| 3  |      |  |
| 4  |      |  |
| 5  |      |  |
| 6  |      |  |

You can configure upto 6 different formats. For each format configure the following parameters:

- **ID:** Select the ID from the right pane for which you wish to configure the parameters.
- **Name:** Configure a name you wish to assign to the format.
- **Output Bits:** Configure the total number of bits that you wish to configure. As soon as you configure the number, the bits appear under Color Selection for Output Bits.

## Color Selection for Output Bits

- You can define the following — Parity, Facility Code, Access Code, Blank — in the Wiegand Format.

Access Code provides an indication to the Third Party Panel whether the user has been allowed or denied by the door.

- For this, under Color Selection For Output Bits, click to select the color which represents the bit type to be added to the Wiegand Format. Then, click on the number in the grid where the selected bit type is to be placed.



- For example, If you select Odd Parity (blue color) and select 1,2 and 3 from 32 configurable bits. Then these 3 bits will be set with Odd parity.

**Wiegand Format**

ID: 1  
Name: Format 1  
Output Bits: 32

Color Selection For Output Bits

Even Parity ☐  
Odd Parity ☒  
Facility Code ☐  
Card No. ☐  
Access Code ☐  
Blank ☐

Facility Code: Read From Card No. (selected)  
☐ Read from device instead of Card No.  
☐ Replace with Card No.

Save Cancel

| ID | Name |  |
|----|------|--|
| 1  |      |  |
| 2  |      |  |
| 3  |      |  |
| 4  |      |  |
| 5  |      |  |
| 6  |      |  |

Similarly, you can configure the bits as per your requirement.

## Facility Code

If **Facility Code** is marked under Color Selection for Output Bits, you must specify the source from where it must be read. Select the desired option — Read From Card No., Read From Card Memory, Read FC from device config.

**Wiegand Format**

ID: 1  
Name: Format 1  
Output Bits: 32

Color Selection For Output Bits

Even Parity ☐  
Odd Parity ☒  
Facility Code ☐  
Card No. ☐  
Access Code ☐  
Blank ☐

Facility Code: Read From Card No. (selected)  
☐ Read from device instead of Card No.  
☐ Replace with Card No.

Save Cancel

| ID | Name |  |
|----|------|--|
| 1  |      |  |
| 2  |      |  |
| 3  |      |  |
| 4  |      |  |
| 5  |      |  |
| 6  |      |  |

- Read from Device instead of Card No.:** Select the check box when you want to send the Facility Code stored in the door.

This option is used when card is not selected as the Access Mode options in [“Basic Configuration”](#) and when FC is set as Read From Card No.

- **Replace with Card No.:** Select the check box, if you want the Card No. to be sent when the FC is not obtained.
- Click **Save** to save the settings. The Wiegand Format appears in the right pane.

| ID | Name     |  |
|----|----------|--|
| 1  | Format 1 |  |
| 2  |          |  |
| 3  |          |  |
| 4  |          |  |
| 5  |          |  |
| 6  |          |  |

You can edit or delete the formats.

To edit, click the desired format from the right pane. Make the changes as per your requirement and click **Save**.



*If a Wiegand Format is edited and saved, it is automatically sent to all the doors to which this format is assigned.*

To delete, click **Delete**  corresponding to the desired Format.

---

The Users allows you to:

- configure the user configuration parameters. For details, refer to [“User Configuration”](#)
- configure the access groups. For details, refer to [“Access Group”](#).
- configure the functional groups. For details, refer to [“Functional Group”](#).
- view the list of blocked users. For details, refer to [“Blocked User”](#).

The status of all the users added to the PANEL200, can be viewed from the Dashboard in a single glance. For details, refer to [“Users Dashboard”](#) in [“Dashboard”](#). You can also add new users from the Dashboard.

### **COSEC-Server Mode**

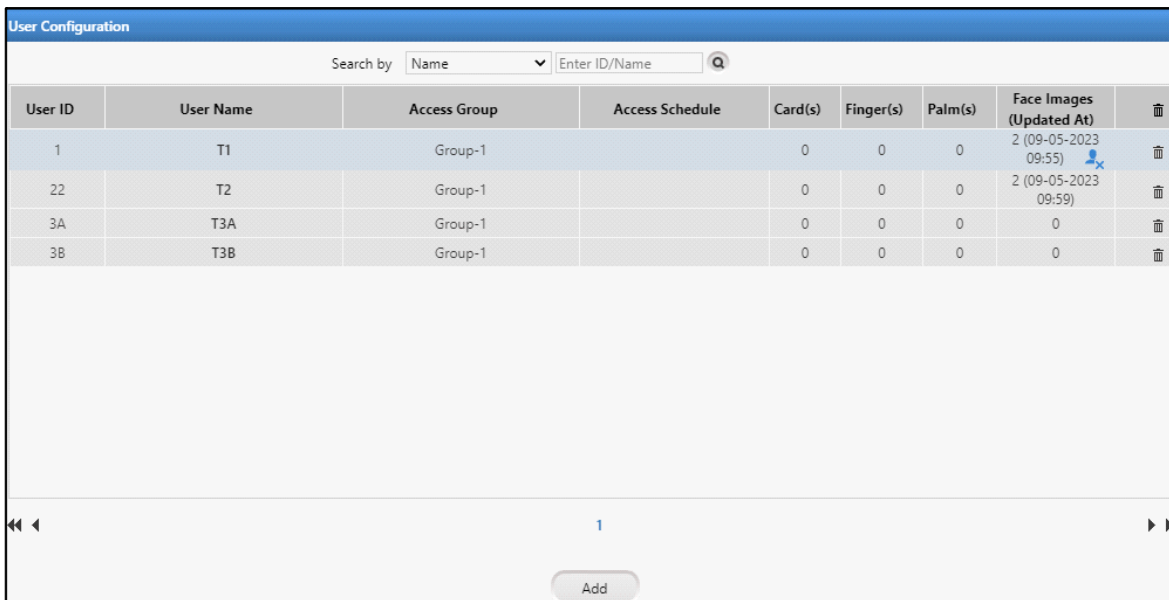
You can configure the following:

- you cannot configure the [“User Configuration”](#) parameters, however you can use the search functionality.
- view the list of blocked users. For details, refer to [“Blocked User”](#).

# User Configuration

To configure the User Configuration parameters,

Click **Users > User Configuration**. The **User Configuration** page appears.



| User ID | User Name | Access Group | Access Schedule | Card(s) | Finger(s) | Palm(s) | Face Images (Updated At) |                                                                                     |
|---------|-----------|--------------|-----------------|---------|-----------|---------|--------------------------|-------------------------------------------------------------------------------------|
| 1       | T1        | Group-1      |                 | 0       | 0         | 0       | 2 (09-05-2023 09:55)     |  |
| 22      | T2        | Group-1      |                 | 0       | 0         | 0       | 2 (09-05-2023 09:59)     |  |
| 3A      | T3A       | Group-1      |                 | 0       | 0         | 0       | 0                        |  |
| 3B      | T3B       | Group-1      |                 | 0       | 0         | 0       | 0                        |  |

1

Add

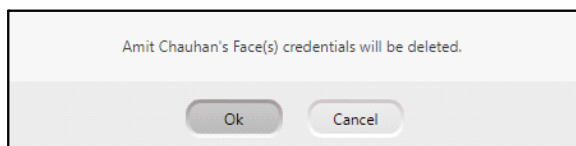
All the added users appear in the grid with their details — User ID, User Name, Access Group, Access Schedule, enrolled Cards, enrolled Fingers, enrolled Palms, enrolled Face images of the user. To add a new user, refer to [“Adding Users”](#).

You can click the desired user and edit its configuration as per your requirement.

You can also delete any user. To do so, click **Delete**  corresponding to the desired user.

If you wish to delete all the images of the user, you can do so,

- Hover-over the **Face Images (Updated At)** entry of the desired user.
- Click **Delete Images** , to delete all the face images of the user. The following pop-up appears.



- Click **Ok** to delete the images. The images will be deleted from the PANEL as well as the doors which are assigned to the user.

Similarly, you can also delete Card, Finger and Palm credentials of the user.



*Face Images (Updated At) is also applicable for COSEC - Server Mode, when Via Panel is selected as the option for Face Sync In Panel Door in the Server.*

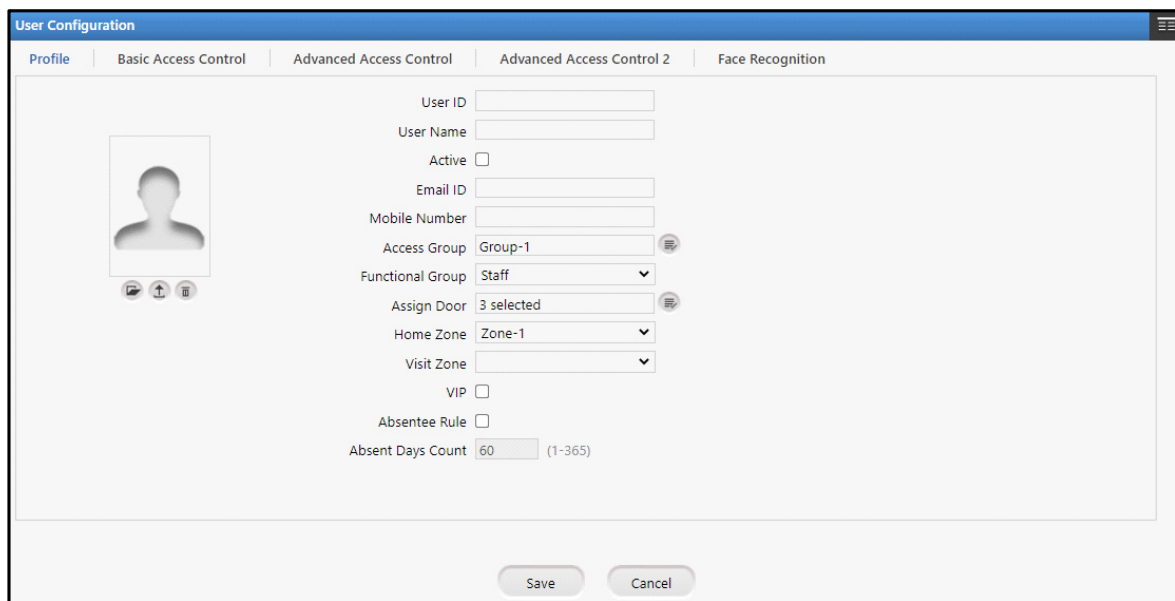
If required you can also search for the desired users. To do so,

- **Search By:** Select the desired option by which you wish to search for the desired user — Name, AlphanumId. In the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword.

## Adding Users

PANEL200 supports a maximum of 25000 users.

To add a user, Click **Add**.



The image shows a screenshot of the 'User Configuration' window in the PANEL200 system. The window has a blue header bar with the title 'User Configuration' and a hamburger menu icon on the right. Below the header is a tabbed interface with five tabs: 'Profile' (selected), 'Basic Access Control', 'Advanced Access Control', 'Advanced Access Control 2', and 'Face Recognition'. The 'Profile' tab is active, displaying a form for user configuration. On the left side of the form is a placeholder for a user profile picture with three small icons below it: a camera, an up arrow, and a trash can. The form fields include: 'User ID' (text input), 'User Name' (text input), 'Active' (checkbox), 'Email ID' (text input), 'Mobile Number' (text input), 'Access Group' (dropdown menu showing 'Group-1'), 'Functional Group' (dropdown menu showing 'Staff'), 'Assign Door' (dropdown menu showing '3 selected'), 'Home Zone' (dropdown menu showing 'Zone-1'), 'Visit Zone' (dropdown menu), 'VIP' (checkbox), 'Absentee Rule' (checkbox), and 'Absent Days Count' (text input showing '60' with a range '(1-365)' to its right). At the bottom of the window are two buttons: 'Save' and 'Cancel'.

The User Configuration allows you to:

- configure the profile parameters. For details, refer to [“Profile”](#).
- configure the basic configuration parameters. For details, refer to [“Basic Access Control”](#).
- configure the advance configuration parameters. For details, refer to [“Advanced Access Control”](#).
- configure the advance configuration 2 parameters. For details, refer to [“Advanced Access Control 2”](#).
- configure the face recognition parameters. For details, refer to [“Face Recognition”](#).

## Profile

To configure the Profile parameters,

Click **Users > User Configuration > Profile**. The **Profile** page appears.

Configure the following parameters:

- **User ID:** Configure a unique ID. It can be an alphanumeric value. It can be a maximum of upto 15 characters.
- **User Name:** Configure a name that identifies the user. It can be a maximum of upto 45 characters.
- **Reference ID:** This is auto-generated by the PANEL200.
- **Active:** Select the check box to enable. The user will be active.
- **Email ID:** Configure the Email ID of the user.
- **Mobile Number:** Configure the Mobile Number of the user.



*The Alerts — SMS and Email are sent on the Mobile Number and Email ID configured here.*

- **Access Group:** By default, Group-1 will be assigned, you can change the same. To do so, click the **Select Access Group** picklist. The **Access Group** pop-up appears. Select the desired group.

**OR**

If required, you can also search for the desired group.

**Search By:** Select the desired option by which you wish to search for the group — ID, Name. In the corresponding box enter the keyword. Click **Search** . The groups will be filtered as per the keyword. Select the desired group.

The selected group appears against Access Group.

- **Functional Group:** Select the desired option — Admin, Staff, Visitor — from the drop-down list.
- **Assign Door:** By default, all the doors are assigned to the users. The doors assigned are as per the configuration done in **Assign Doors to New Users**. For details, refer to [“Settings”](#).

However, you can assign or revoke doors as per your requirement manually also.

To do so,

- Click the **Assign Door** picklist. The **Assign Door** pop-up appears. Click the **Door** or **Door Group** picklist and select the check boxes of the desired doors/door groups that you wish to assign to the user. The selected doors/doors of the selected door groups appear in the grid.

**OR**

You can also search for the desired door/door group. To do so, enter the keyword in the Search box.

Click **Search** . The doors/door groups will be filtered as per the keyword. Select the check boxes of the desired doors/door groups that you wish to assign to the user. The selected doors/doors of the selected door groups appear in the grid.

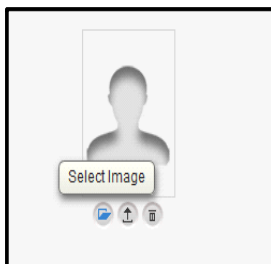
- If you wish to remove the doors, click **Delete**  corresponding to the desired door.
- Click **Ok** to assign the doors.
- **Home Zone:** Select the home zone to be assigned for the user from the drop-down list.
- **Visit Zone:** Select the visit zone to be assigned for the user from the drop-down list.
- **VIP:** Select the check box, if unrestricted access is to be given to the user.
- **Absentee Rule:** Select the check box to enable the Absentee Rule at user level. This rule allows you to configure maximum number of days for which user will be allowed to remain absent, thereafter the user will be denied access.

Make sure Absentee Rule is also enabled in [“Set1”](#) in [“Access Features”](#).

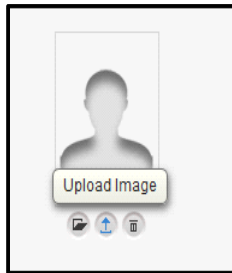
- **Absent Days Count:** If you have enabled the **Absentee Rule**, configure the maximum number of days (1 to 365) for which user will be allowed to remain absent.

You can upload the image of the user. To do so,

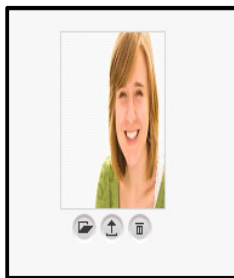
- Click **Select Image**  and select the image from the desired location.



- Click **Upload Image**  to upload the image.



- Click **Save**



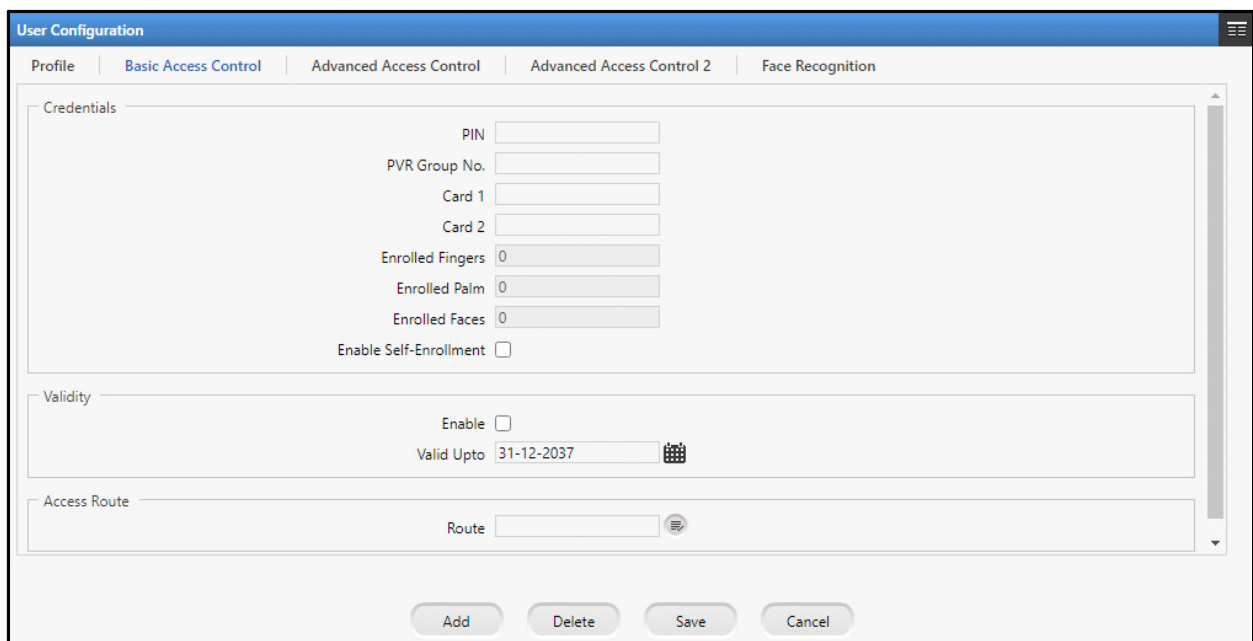
- Click **Remove**  to delete the image.

Click **Save** to save the settings or click **Cancel** to discard.

## Basic Access Control

To configure the Basic Access Control parameters,

Click **Users > User Configuration > Basic Access Control**. The **Basic Access Control** page appears.



Configure the following parameters:



## Credentials

- **PIN:** Configure a PIN (numeric, 1 to 15 digits) for the user.
- **PVR Group No.:** Configure the PVR Group Number that you wish to assign to the user, if applicable. It is a number allotted to a group of users assigned on a door. This enables the door to match a palm credential against only those users who are part of the same Biometric Group thus reducing processing time.
- **Card 1/Card 2:** Configure a Card Serial Number (CSN) or a Facility Code separated CSN which is to be assigned to the user.

Format:

- **Card Serial Number** = 1343933547.
- **Facility Code separated CSN** = 12,345789



The maximum character limit for Card Serial Number (CSN) is 20 digits. While the maximum character limit for Facility Code separated CSN is 21 digits.

If there is any discrepancy while entering the Card Number (CSN), the PANEL200 will display an error.

The Access Card Number will be used to allow/deny access to users. PANEL200 supports upto two cards per user. So if required, configure the **Card 2** number also.

Once you save the configurations, hover-over the Facility Code separated CSN value of any Card, the PANEL200 will display an encoded (converted) value of Facility Code separated CSN.

- **Enrolled Fingers/Palm/Faces:** This displays the number of finger/palm/face templates enrolled against the selected user.



*The count of face images in **Enrolled Faces** will be updated whenever:*

- *face images are deleted from Users > User Configuration > Face Images (Updated At).*
- *face images are updated/deleted from Users > User Configuration > Face Recognition.*
- *face images are updated from Enrollment > User.*
- *face images are updated from Panel Configuration > Advanced Profile > Enrollment.*

- **Enable Self-Enrollment:** Select the check box to enable self-enrollment for the user. The Self-Enrollment feature enables the user to enroll himself/herself at a door using a pre-assigned access PIN, without the help of any operator or HR executive.

Make sure you have enabled Self-Enrollment in [“Enrollment”](#) in [“Advanced Profile”](#).

## Validity

- **Enable:** Select the check box to enable. The user's credential will be activated for a predefined period.
- **Valid Upto:** Click the calendar and select the end date on which the validity of the user credential will expire.

## Access Route

- **Route:** Click the **Select Route** picklist. The **Route** pop-up appears. Select the desired route. The user will be assigned this predefined Access Route, based on which user has to access the configured doors of the route.

### OR

If required, you can also search for the desired group.

**Search By:** Select the desired option by which you wish to search for the route — ID, Name. In the corresponding box enter the keyword. Click **Search** . The routes will be filtered as per the keyword. Click to select the desired route.

The selected route appears against the Route. For details, refer to [“Access Route”](#).

Click **Save** to save the settings or click **Cancel** to discard.

## Advanced Access Control

To configure the Advanced Access Control parameters,

Click **Users > User Configuration > Advanced Access Control**. The **Advanced Access Control** page appears.

User Configuration

Profile | Basic Access Control | **Advanced Access Control** | Advanced Access Control 2 | Face Recognition

Basic

Restrict Access ☐

Bypass Finger ☐

Bypass Palm ☐

Shift Based Access

Enable ☐

Shift Schedule 1

Start Shift GS

Holiday Schedule

Smart Card Access Route

Max Route Level 75

Smart Card Access Route

Mobile Based Access

Enable ☐

Add Delete Save Cancel

User Configuration

Profile | Basic Access Control | **Advanced Access Control** | Advanced Access Control 2 | Face Recognition

Bypass Palm ☐

Shift Based Access

Enable ☐

Shift Schedule 1

Start Shift GS

Holiday Schedule

Smart Card Access Route

Max Route Level 75

Smart Card Access Route

Mobile Based Access

Enable ☐

IMEI Max 40 Chars

Enroll IMEI i

Add Delete Save Cancel

### Basic

- **Restrict Access:** Select the check box to restrict access for the user, that is, punches on the doors will be considered for attendance only and will not open the door for access.
- **Bypass Finger/Palm:** Select the check box, if Finger/Palm identification issues are being faced by the user. You can bypass the Finger/Palm check for the user. The user can punch in or out using the assigned PIN or card and the same will be considered for attendance calculation.

## Shift Based Access

- **Enable:** Select the check box to enable shift based user access, that is, as per the shift working hours of the user. If the Shift Based Access option is not enabled, then the default “[Access Settings](#)” will be applied.
- **Shift Schedule:** Select a shift schedule from the drop-down list to be assigned to the user.
- **Start Shift:** If there are multiple shifts in the Shift Schedule assigned to the user, the starting shift needs to be selected from the drop-down list.
- **Holiday Schedule:** Select the Holiday Schedule to be assigned to the user from the drop-down list.



*Make sure you have configured the desired “[Shifts and Schedules](#)” and “[Holiday Schedule](#)”.*

## Smart Card Access Route

- **Max Route Level:** Select the route level upto which the user is to be allowed access from the drop-down list.
- **Smart Card Access Route:** Click the **Select Smart Routes** picklist. The **Smart Card Access Route** pop-up appears. Select the desired route to be assigned to the user.

**OR**

If required, you can also search for the desired route.

**Search By:** Select the desired option by which you wish to search for the route — ID, Name. In the corresponding box enter the keyword. Click **Search**  . The groups will be filtered as per the keyword. Select the desired route.

The selected route appears against Smart Card Access Route.

## Mobile Based Access

- **Enable:** Select the check box to allow the user to access the doors through the Mobile.
- **IMEI:** Configure the IMEI (International Mobile Equipment Identity) number of the Mobile.

Click **Enroll IMEI** to enroll a user to access doors through Mobile. The enrollment for the selected user will be activated for 60 seconds.

Click **Save** to save the settings or click **Cancel** to discard.

## Advanced Access Control 2

To configure the Advanced Access Control 2 parameters,

Click **Users > User Configuration > Advanced Access Control 2**. The **Advanced Access Control 2** page appears.

The screenshot shows the 'User Configuration' window with the 'Advanced Access Control 2' tab selected. The page contains four main sections, each with a collapse icon on the left:

- Elevator Access Control:** Includes a checkbox for 'Elevator Access Control' and a table for 'Elevator Floor Group' with columns 'ID' and 'Name'.
- Smart Elevator Access Control:** Includes a checkbox for 'Smart Elevator Access Control' and a table for 'Smart Elevator Floor Group' with columns 'ID' and 'Name'.
- Access Cluster:** Includes a checkbox for 'Access Cluster Check'.
- Access Rule:** Includes a text field for 'Access Rule' and a picklist icon.

At the bottom of the window are four buttons: 'Add', 'Delete', 'Save', and 'Cancel'.

### Elevator Access Control

- **Elevator Access Control:** Select the check box, to allow elevator access to the user.
- **Elevator Floor Group:** It displays the Elevator Floor Group assigned to the user from Users Linking tab of Elevator Floor Group page. For details, refer to [“Users Linking”](#) in [“Elevator Floor Group”](#).

### Smart Elevator Access Control

- **Smart Elevator Access Control:** Select the check box to allow smart elevator access to the user.
- **Smart Elevator Floor Group:** It displays the Smart Elevator Floor Group assigned to the user from Users Linking tab of Smart Elevator Floor Group page. For details, refer to [“Users Linking”](#) in [“Smart Elevator Floor Group”](#).

### Access Cluster

- **Access Cluster Check:** Select the check box to allow access cluster checking for the user.

For details, refer to [“Access Cluster”](#).

### Access Rule

- **Access Rule:** Click the **Select Access Rule** picklist. The **Access Rules** pop-up appears. Select the check boxes of the desired access rules to be assigned to the user. Click **Ok**.

OR

You can also search for the desired rule. To do so, enter the keyword in the Search box. Click **Search**

 . The rules will be filtered as per the keyword. Select the check boxes of the desired access rule to be assigned to the user. Click **Ok**.

The access of the doors will be provided to the user as per the selected rule/s. The number of selected rules appears against Access Rule.



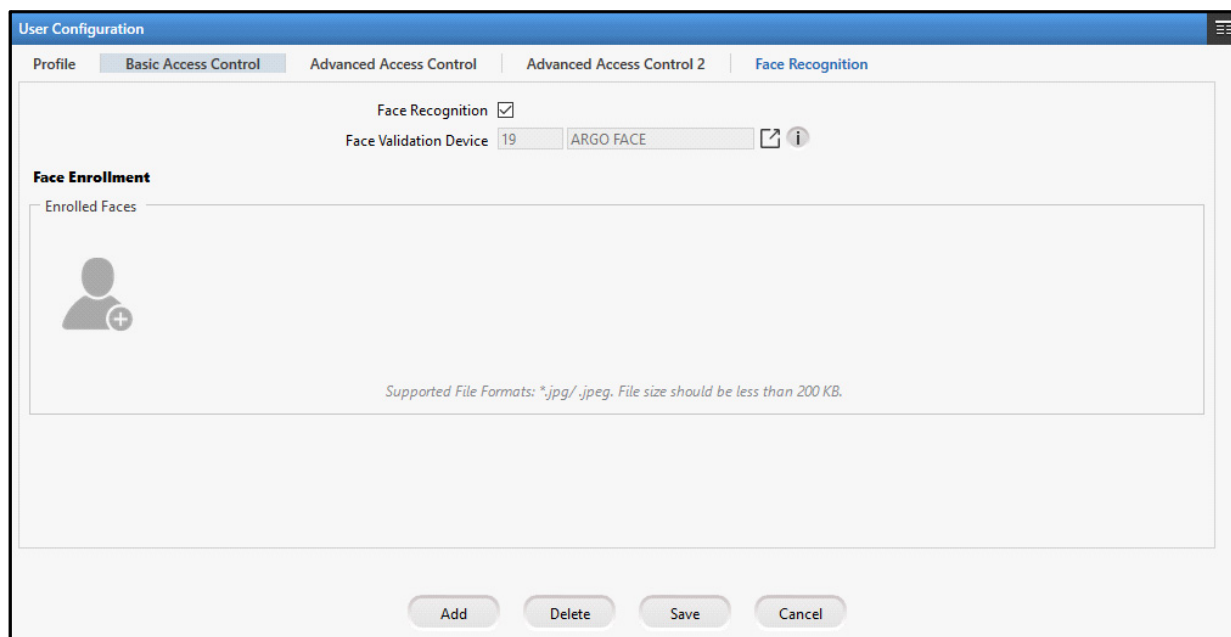
*Maximum 99 Access Rules can be assigned to a user.*

For details, refer to [“Access Rule”](#).

## Face Recognition

To configure the Face Recognition parameters,

Click **Users > User Configuration > Face Recognition**. The **Face Recognition** page appears.



- **Face Recognition:** Select the check box to enable Face Recognition.



*If you clear this check box, the face images will be deleted from the doors but will be available with the PANEL200.*

- **Face Validation Device:** The door selected as the **Face Validation Device** in [“General”](#) appears here. The face images uploaded from this page will be validated by the door selected for face validation.

Click  if you wish to change the **Face Validation Device**. You will be re-directed to select the door from Panel Configuration > Basic Profile > General. For details, refer to [“General”](#).



*Any user other than Admin can change the **Face Validation Device** only if **Panel Configuration Access Rights** are granted. For details, refer to [“Users”](#) in [“Account Management”](#).*

## Face Enrollment



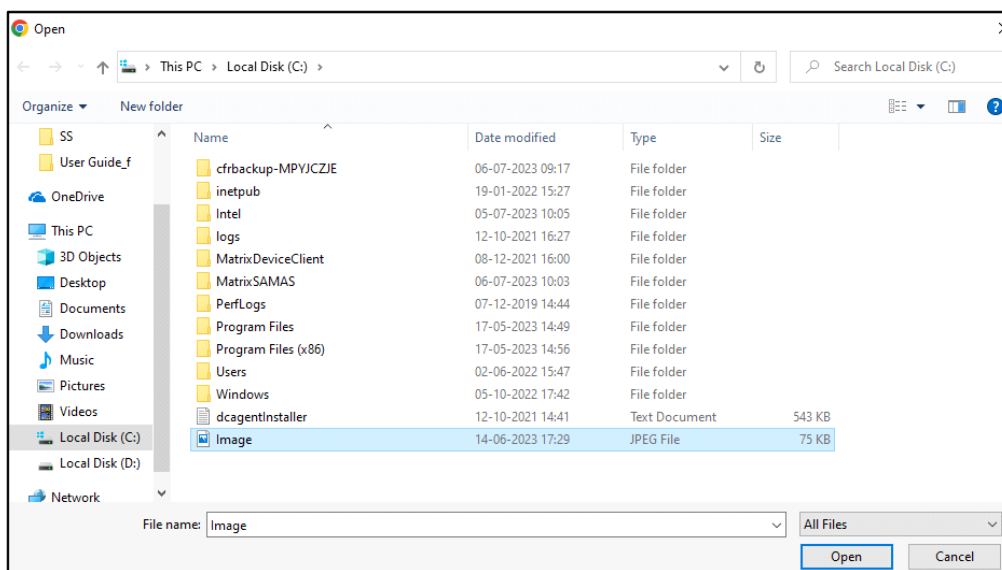
*The complete face images will not be visible due to security reasons in this document.*

*Make sure the **Face Validation Device** is assigned. For details, refer to [“General”](#).*

*When faces are enrolled from **Face Recognition- Face Enrollment**, then these requests will not be displayed in Enrollment > Authorization ([“Authorization”](#)) for approval even if the **Authorization on Enrollment** is enabled from Panel Configuration > Advanced Profile > Enrollment. For details, refer to [“Enrollment”](#).*

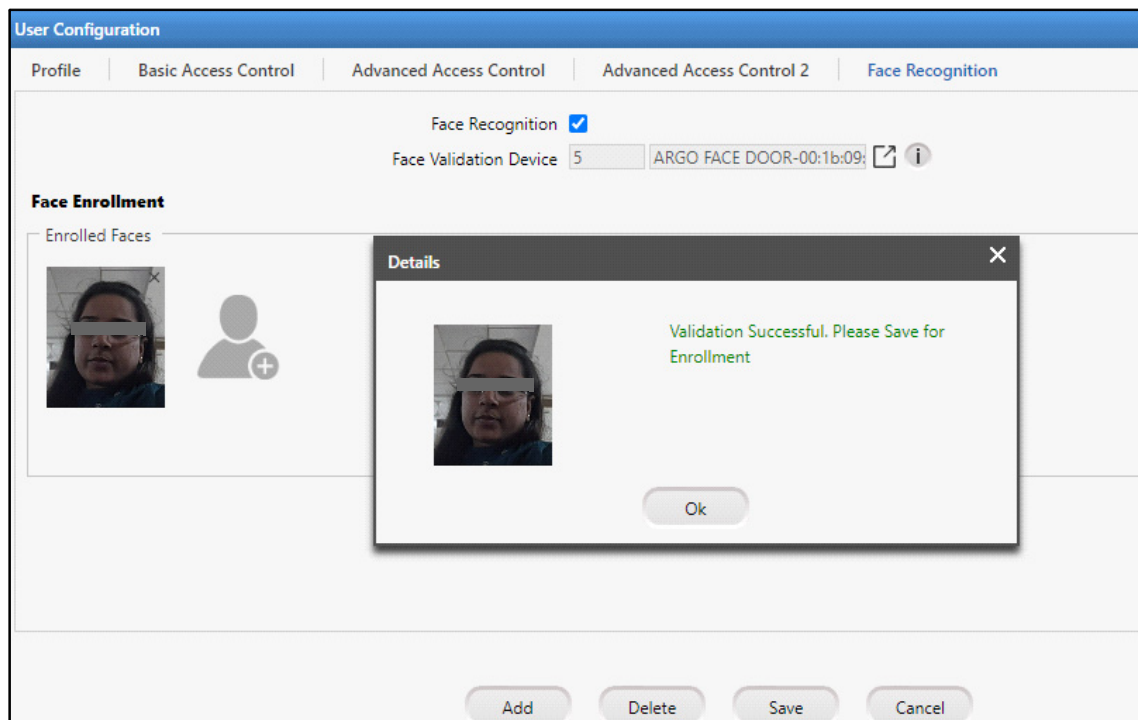
All the enrolled faces of the user will be displayed here. You can also upload images from this page if required. To do so,

- Click **Upload Face Image**  and select the image from the desired location.



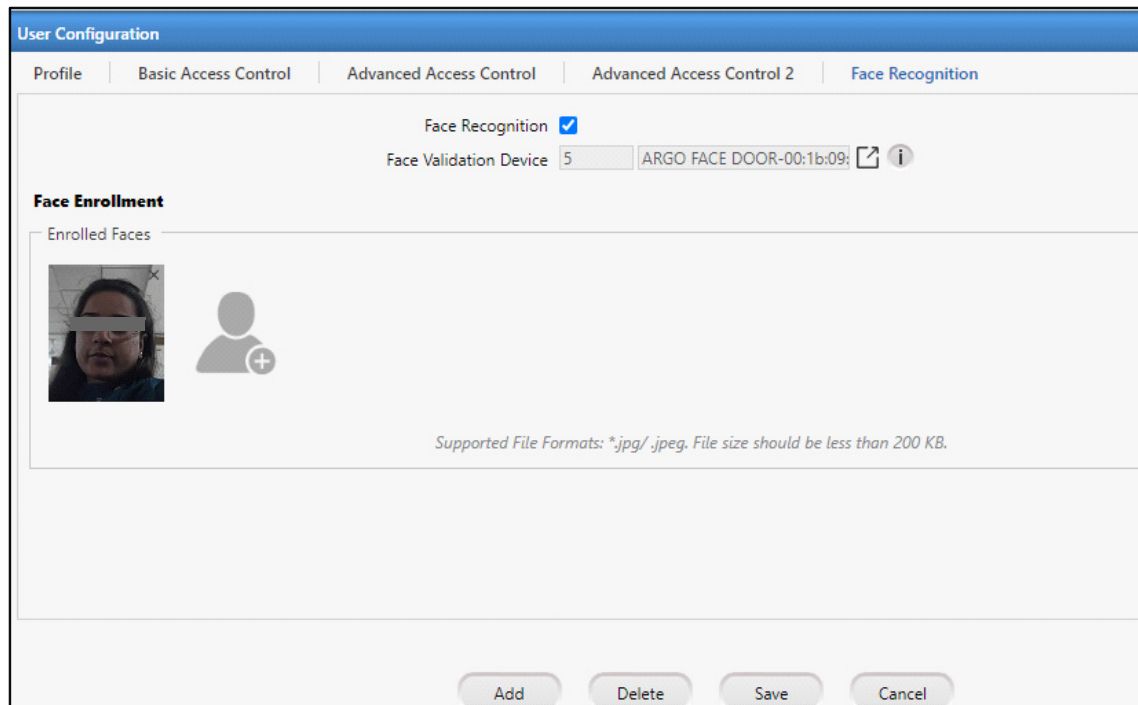
The image will be uploaded and then validated by the configured Face Validation Device. The image preview appears under Face Enrollment.

Once the image validation is done and the image is uploaded successfully, the **Details** pop-up appears.



- Click **Ok** to close the pop-up. Click **Save** to enroll the image.

The enrolled image now appears under Face Enrollment once uploaded successfully.



To delete the images,

- Click **Mark For Removal**  on the top right corner of the desired image.



- The **Mark For Removal**  turns red once the image is selected. Click **Save** to delete the images. The images will be deleted from the PANEL as well as the associated door.

If you do not wish to remove another image, click **Mark For Removal**  again.

If you wish, you can perform dual actions simultaneously on a single **Save** click. To do so,

- select an image for removal, by clicking **Mark For Removal** .
- select an image for uploading, by clicking **Upload Face Image**  and select an image to upload.

Then click **Save**. Both actions will be executed.

The count of face images will be updated in **Face Images (Updated At)** displayed in the User List, whenever any image is uploaded or deleted.



*The door selected as the Face Validation device will sync the available face images with all the other Face Recognition doors (ARGO FACE/ARGO FACE210 doors) connected with the PANEL.*

*While uploading the images manually, if the selected images of the user do not match with the face data available with the Face Validation Device, a conflict error will be displayed and the images will not be uploaded.*

To configure the Access Group parameters,

All the created Access Groups appear in the grid. By default, Group-1 is already created and it is displayed here. You can click the same and edit it as per your requirement or you can add a new Access Group.



To add a new Access Group,

Click **Add**. You can create maximum **99** Access Groups.

| Member | ID | Time Schedule | Access Level |
|--------|----|---------------|--------------|
| 1      | 1  | Time Zone 1   | 8            |
| 2      | 1  | Time Zone 1   | 8            |
| 3      | 1  | Time Zone 1   | 8            |
| 4      | 1  | Time Zone 1   | 8            |
| 5      | 1  | Time Zone 1   | 8            |
| 6      | 1  | Time Zone 1   | 8            |
| 7      | 1  | Time Zone 1   | 8            |
| 8      | 1  | Time Zone 1   | 8            |

Configure the following parameters:

- **Group ID:** The Group ID is auto-generated by the PANEL200.
- **Group Name:** Configure a name you wish to assign to the group.
- **Active:** Select the check box to enable the Access Group.

### User Access Level

- **Working Hours:** Select the desired access level you wish to assign to the user from the drop-down list.
- **Break Hours:** Select the desired access level you wish to assign to the user from the drop-down list.
- **Non-Working Hours:** Select the desired access level you wish to assign to the user from the drop-down list.

The Access Level assigned to the user is compared with the Access Level of the Zone assigned to the user. Only if User Access Level is greater than or equal to the Access Level of the Zone, the user is allowed access.



*Make sure you have assigned the appropriate Access Levels to the Zones. For details, refer to [“Basic Configuration”](#) in [“Zone Configuration”](#).*

For example,

If shift is defined from 9am to 6pm and Access Level for Work Hours is set at **9**, Access Level for Break Hours is set at **8**, Access Level for Non-Working Hours is set at **8**, Access Level for the Zone1 is set at **9** (Not Home zone)

- Case1: Then if employee punches between 9 to 6, he will be allowed access.
- Case2: If employee punches before 9am, he will be denied access as access level for Non-working hours (8) is less than the access level of Door in Zone1(9).

- **Case3:** If employee punches during break hours, he will be denied access as access level for Break hours (8) is less than the access level of Door in Zone1(9).

## Schedule Based Access Level Override

The right pane displays 8 predefined members. These members cannot be deleted, they can only be updated from Schedule Based Access Level Override.

There are certain specific areas for which access needs to be provided even during the Break Hours, such as the Canteen. In such cases you can define a specific Time Zone for this, such as Lunch Time. To provide such access you need to configure Schedule Based Access Level Override.

**Access Group**

Group ID: 2  
Group Name: HO Group  
Active: ☒

User Access Level  
Work Hours: 8  
Break Hours: 8  
Non-Working Hours: 8

Schedule Based Access Level Override  
Time Zone: Lunch Time  
Access Level: 9  
Active: ☒  
Update Cancel

| Member | ID | Time Schedule | Access Level |
|--------|----|---------------|--------------|
| 1      | 1  | Time Zone 1   | 8            |
| 2      | 1  | Time Zone 1   | 8            |
| 3      | 1  | Time Zone 1   | 8            |
| 4      | 1  | Time Zone 1   | 8            |
| 5      | 1  | Time Zone 1   | 8            |
| 6      | 1  | Time Zone 1   | 8            |
| 7      | 1  | Time Zone 1   | 8            |
| 8      | 1  | Time Zone 1   | 8            |

Save Cancel

Select the desired Member number from the right pane and configure the following parameters:

- **Time Zone:** Click the **Select Time Zone** picklist. The **Time Zone** pop-up appears. Select the desired time zone.

**OR**

If required, you can also search for the desired time zone.

**Search By:** Select the desired option by which you wish to search for the time zone — ID, Time Zone

Name. In the corresponding box enter the keyword. Click **Search**  . The time zones will be filtered as per the keyword. Select the desired time zone.

The selected time zone appears against Time Zone. To configure a Time Zone, refer to [“Time Zone”](#).

- **Access Level:** Select the desired access level you wish to assign to the Time Zone from the drop-down list. Time Zone based Access Levels allow the user to configure additional time slots for certain groups to have access to various zones during different time periods of the day.
- **Active:** Select the check box to enable.

- Click **Update** and **Save** to apply the changes.

| Member | ID | Time Schedule | Access Level |
|--------|----|---------------|--------------|
| 1      | 4  | Lunch Time    | 9            |
| 2      | 1  | Time Zone 1   | 8            |
| 3      | 1  | Time Zone 1   | 8            |
| 4      | 1  | Time Zone 1   | 8            |
| 5      | 1  | Time Zone 1   | 8            |
| 6      | 1  | Time Zone 1   | 8            |
| 7      | 1  | Time Zone 1   | 8            |
| 8      | 1  | Time Zone 1   | 8            |

The Time schedule for Lunch Time zone is enabled for the HO Group as shown above.

The User Access Levels as well as Scheduled Based Access Level Override can be configured but only one option will be applicable at a time.

For example: If Access level of Break is 8, then employee will not be allowed to access in break hours. But the Lunch Time Zone has access level 9, so the employee will be allowed to access the lunch area.

Click **Save** to save the settings or click **Cancel** to discard.

After you have created the Access Group, you can assign it to the users. For details, refer to ["Profile"](#) in ["User Configuration"](#).

After you have completed all the configurations of the Access Group and if you wish to view all the created Access

Groups, click **View List** .

The Access Group page displays all the created Access Groups.

| Access Group |            |                   |             |                   |
|--------------|------------|-------------------|-------------|-------------------|
| Group ID     | Group Name | User Access Level |             |                   |
|              |            | Working Hours     | Break Hours | Non-Working Hours |
| 1            | Group-1    | 8                 | 8           | 8                 |
| 2            | HO Group   | 8                 | 8           | 8                 |

# Functional Group

To configure the Functional Group parameters,

Click **Users > User Configuration > Functional Group**. The **Functional Group** page appears.

| Group ID | Group Name |  |
|----------|------------|--|
| 1        | Staff      |  |
| 2        | Visitor    |  |
| 3        | Admin      |  |

By default, 3 Functional Groups are created — Admin, Staff, Visitor. You cannot delete the same but can edit the same.

To edit, click on the desired group from the right pane. You can edit the name as per your requirement. Click **Save**.

You can add a new Functional Group. To do so,

- Click **Add**.

| Group ID | Group Name |  |
|----------|------------|--|
| 1        | Staff      |  |
| 2        | Visitor    |  |
| 3        | Admin      |  |

Configure the following parameters:

- **Group ID:** The Group ID is auto generated by the PANEL200.
- **Group Name:** Configure user-friendly name you wish to assign to the Functional Group.
- Click **Save** to apply the changes.

| Group ID | Group Name |  |
|----------|------------|--|
| 1        | Staff      |  |
| 2        | Visitor    |  |
| 3        | Admin      |  |
| 4        | Factory    |  |

The new Functional Group appears in the right pane.

You can edit or delete the new Functional Groups.

To edit, click the desired Functional Group from the right pane and edit it. Click **Save**.

To delete, click **Delete**  corresponding to the desired Functional Group in the right pane.

After you have created the Functional Group, you can assign it to the users. For details, refer to [“Profile”](#) in [“User Configuration”](#).



# Blocked User

PANEL200 allows blocking of users for certain access policies — Tail-Gating, Man Trap Timer Violation, Occupancy Violation, Anti-Pass Back Violation, Multiple Unauthorized Attempts as well as due to the Absentee rule, Use Count Control rule. For more details, refer to [“Access Features”](#).

Blocking a user only deactivates the credential and does not result in the deletion of user information from the PANEL200.

To view the Blocked Users,

Click **Users > User Configuration > Blocked User**. The **Blocked User** page appears.

| Blocked User |      |            |          |               |                          |
|--------------|------|------------|----------|---------------|--------------------------|
| User         |      | Date       | Time     | Reason        | Select                   |
| ID           | Name |            |          |               |                          |
| 4            | karm | 13-08-2025 | 00:00:00 | Absentee Rule | <input type="checkbox"/> |

Restore

The blocked users are displayed with the details — User ID, User Name, Date and Time on which they were blocked and the Reason for blocking.

You can restore the blocked users. To do so,

- Click the check boxes of the desired users.
- Click **Restore**. The selected users will be unblocked.



*Make sure the Alert Service is running to generate Block User Events.*

*The Alert (Blocked User) can be configured from Alert Message Configuration which will send SMS or Email to Admin or Reporting In-charge notifying that the user is blocked. For details, refer to [“Alert Message Configuration”](#)*



---

Once the users have been added to the PANEL200, you can start the enrollment process and assign credentials to the users. Enrollment can be defined as a process wherein the Panel200 accepts and stores the user credentials against a particular user.

The enrollment process can be initiated either from the PANEL200 or from the door by using special cards or Menu.

The Enrollment allows you to:

- configure the user credential enrollment parameters. For details, refer to [“User”](#).
- configure the special card enrollment parameters. For details, refer to [“Special Card”](#).
- configure the SI user enrollment parameters. For details, refer to [“SI User”](#).
- authorize or reject the enrolled users credentials. For details, refer to [“Authorization”](#).

### **COSEC-Server Mode**

You can configure the following:

- configure the user credential enrollment parameters. For details, refer to [“User”](#).
- configure the special card enrollment parameters. For details, refer to [“Special Card”](#).

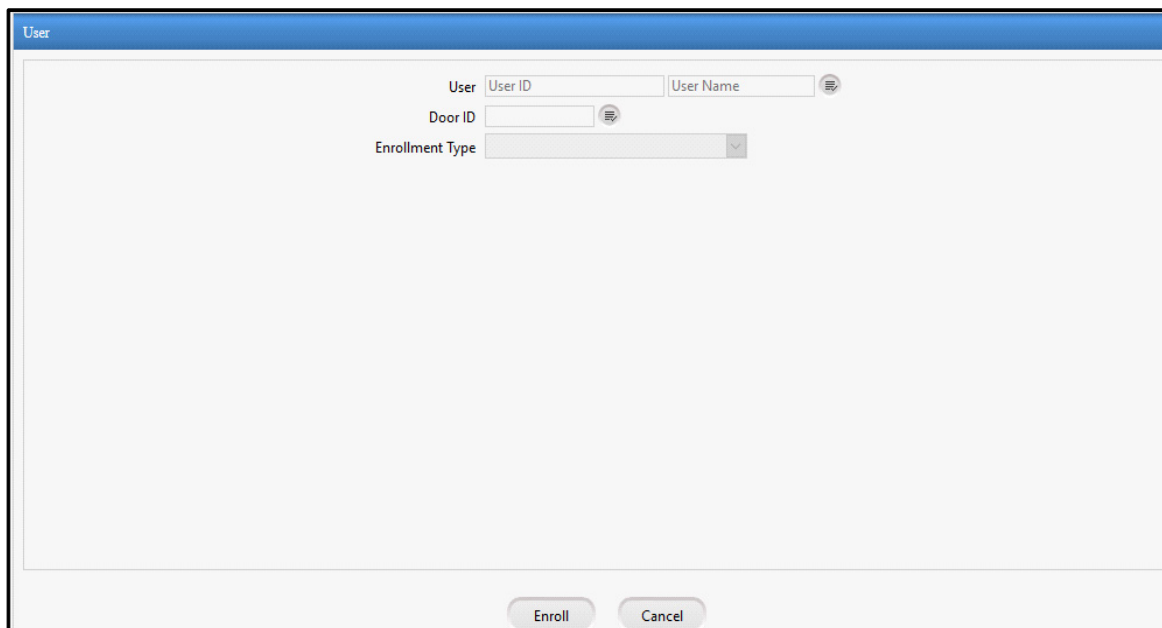
# User

---

Once users have been added to the PANEL200, the enrollment process can be initiated. Enrollment can be defined as a process wherein the PANEL200 accepts and stores the user credentials against a particular user. It supports enrollment of user cards, finger templates, palm templates, face templates and special cards.

To configure the User credential enrollment parameters,

Click **Enrollment > User**. The **User** page appears.

The screenshot shows a web interface titled "User" in a blue header bar. Below the header, there are four input fields: "User ID", "User Name", "Door ID", and "Enrollment Type". Each of the first three fields has a small circular icon with three horizontal lines to its right, indicating a picklist. The "Enrollment Type" field is a dropdown menu. At the bottom of the form, there are two buttons: "Enroll" and "Cancel".

Configure the following parameters:

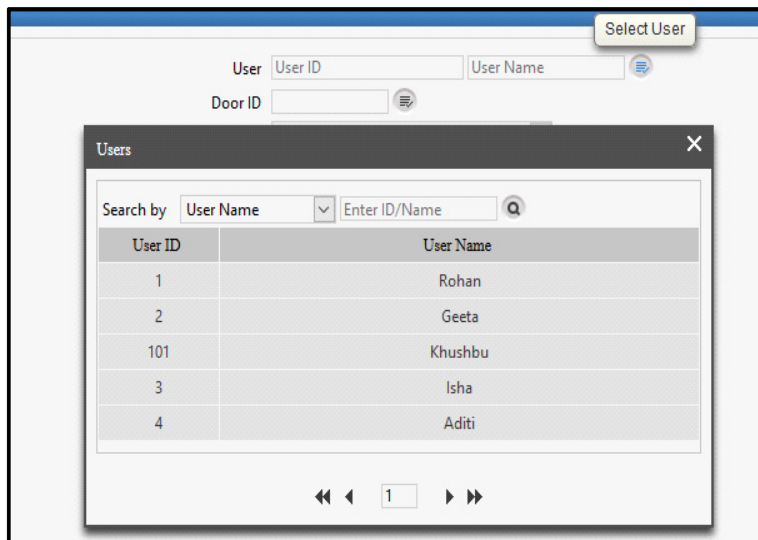
- **User:** Click **Select User** picklist. The **Users** pop-up appears. Select the desired user.

**OR**

If required, you can also search for the desired user.

**Search By:** Select the desired option by which you wish to search for the user — User ID, User Name. In the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Click to select the desired user.

The selected user's ID and Name appear against the User.



- **Door ID:** Click the **Select Door** picklist. The **Panel Doors** pop-up appears. Select the desired door.

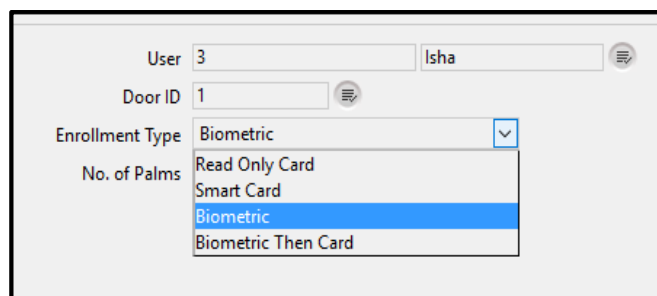
**OR**

If required, you can also search for the desired door.

**Search By:** You can also search for the desired door. To do so, enter the keyword in the Search box. Click

**Search**  . The doors will be filtered as per the keyword. Select the desired door.

The selected doors ID appears against the Door ID. On this door the enrollment will be performed for the selected user.



*Enrollment can also be done using the door. For details, refer to [“Enrollment”](#).*

- **Enrollment Type:** Select the desired **Enrollment Type** from the drop-down list. The Enrollment Types for a user that can be performed on a door depends on the door type. The following options are available:
  - Read Only Card
  - Smart Card
  - Biometric
  - Biometric Then Card
  - Mobile Device
  - Duress Finger
  - Face



*If ARC DC200 (Single Door Dual Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Reader Group 1/2 and Reader Group 1/2 is selected in Enrollment > User > Enrollment Using, then only Read Only Card option will be functional as Enrollment Type.*

*If ARC DC200 (Single Door Dual Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Reader Group 1/2 and Device is selected in Enrollment > User > Enrollment Using, then only Mobile Device option will be functional as Enrollment Type.*

*If ARC DC200 (Dual Door Single Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Door 1 and Reader Group 1 is selected in Enrollment > User > Enrollment Using, then only Read Only Card option will be functional as Enrollment Type.*

*If ARC DC200 (Dual Door Single Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Door 1 and Device is selected in Enrollment > User > Enrollment Using, then only Mobile Device option will be functional as Enrollment Type.*

*If ARC DC200 (Dual Door Dual Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Door 1 and Reader Group 1 is selected in Enrollment > User > Enrollment Using, then only Read Only Card option will be functional as Enrollment Type.*

*If ARC DC200 (Dual Door Dual Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Door 2 and Reader Group 1 is selected in Enrollment > User > Enrollment Using, then only Read Only Card option will be functional as Enrollment Type.*

*If ARC DC200 (Dual Door Dual Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Door 1/2 and Device is selected in Enrollment > User > Enrollment Using, then only Mobile Device option will be functional as Enrollment Type.*

- If you have selected **Read Only Cards**,
  - **No. of Cards:** Select the number of cards to be enrolled from the drop-down list.
- If you have selected **Smart Card**,
  - **No. of Cards:** Select the number of cards to be enrolled from the drop-down list.
  - **Smart Card Options:** Select the check boxes of the desired details to be written on the Smart Card
    - User ID
    - User Name
    - Facility Code (FC)
    - Additional Security Code (ASC)
    - Finger Template: Select the number of templates to be written on to the card from the drop-down list.
  - **Smart Card with Personalized Details:** Select the check boxes of the desired details and configure the detail in the corresponding box to be written on the Smart Card:
    - Designation
    - Branch

- Department
  - Blood Group
  - Emergency Contact
  - Medical History
- If you have selected **Biometric**,
  - **No. of Fingers/Palms:** Select the number of finger/palm to be enrolled from the drop-down list.
- If you have selected **Biometric then Card**,
  - **No. of Cards:** Select the number of cards to be enrolled from the drop-down list.
  - **No. of Fingers/Palms:** Select the number of finger/palm to be enrolled from the drop-down list.
  - **Smart Card Options:** Select the check boxes of the desired details to be written on the Smart Card
    - User ID
    - User Name
    - Facility Code (FC)
    - Additional Security Code (ASC)
  - **Smart Card with Personalized Details:** Select the check boxes of the desired details and configure the detail in the corresponding box to be written on the Smart Card:
    - Designation
    - Branch
    - Department
    - Blood Group
    - Emergency Contact
    - Medical History
- If you have selected **Mobile Device**,
  - **Access Card Selection:** Select the desired **Access Card** to be enrolled from the drop-down list.
  - **Facility Code:** Select the check box to include the Facility Code in the Access Card Number.
- If you have selected **Duress Finger**,
  - **No. of Fingers:** Select the number of fingers to be enrolled from the drop-down list.
- If you have selected **Face**,
  - **No. of Faces:** Select the number of faces to be enrolled from the drop-down list.

Click **Enroll** to initiate enrollment or **Cancel** to discard the changes on the selected door.

After the enrollment is successful, the number of credentials enrolled for a user are displayed in User Configuration:

| User Configuration                                                                   |           |              |                 |         |           |         |                             |   |
|--------------------------------------------------------------------------------------|-----------|--------------|-----------------|---------|-----------|---------|-----------------------------|---|
| Search by <span>Name</span> <span>▼</span> <span>Enter ID/Name</span> <span>🔍</span> |           |              |                 |         |           |         |                             |   |
| User ID                                                                              | User Name | Access Group | Access Schedule | Card(s) | Finger(s) | Palm(s) | Face Images<br>(Updated At) | 🗑 |
| 111                                                                                  | 1111      | Group-1      |                 | 0       | 2         | 0       | 10 (13-06-2023<br>10:17)    | 🗑 |
| 222                                                                                  | 222       | Group-1      |                 | 0       | 0         | 0       | 0                           | 🗑 |
| 9                                                                                    | 999       | Group-1      |                 | 0       | 0         | 0       | 12 (13-06-2023<br>10:28)    | 🗑 |



# Special Card

---

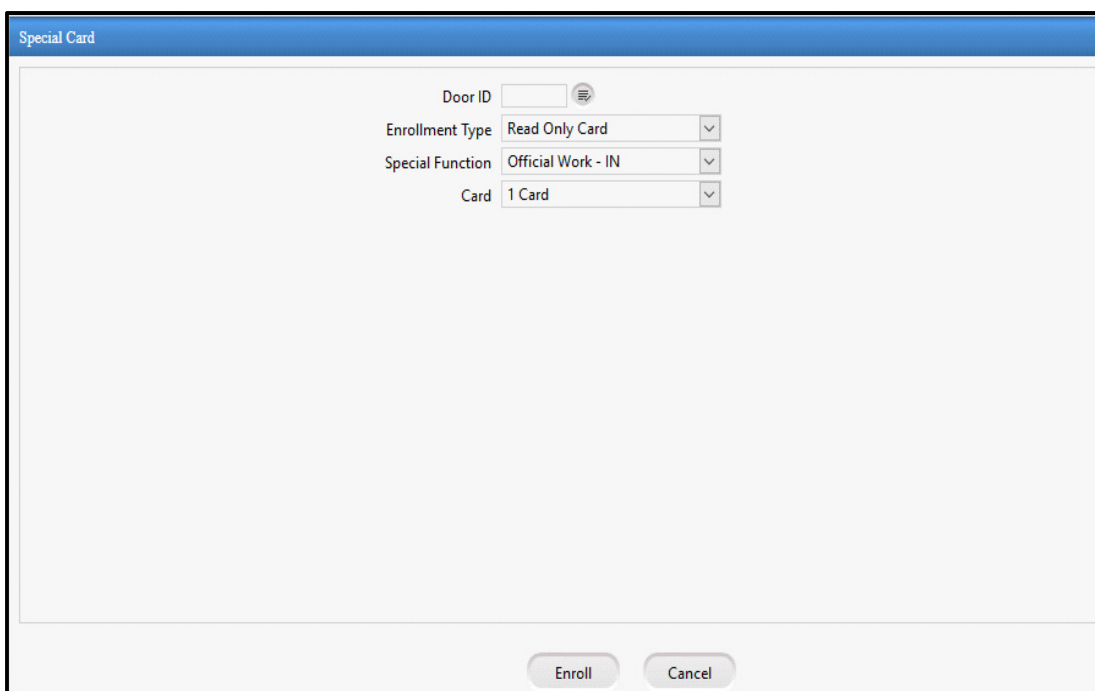
A Special Card is a RFID card that can be encoded for a Special Function and the card-holder can execute the Special Function at the door just by displaying this Special Card.

A Special Card is useful when the user has to perform routine tasks, where repeated manual entry of codes can become tedious. It is also required when a door does not have keypad or LCD display for manual entry of special codes.

For example, in factories where workers can avail Short Leave, a security guard uses the Special Card enrolled for **Short Leave-IN** on the Entry door to give access to the workers. This same card can be used for multiple workers. Each worker is assigned credentials for authentication using which they can access the door.

To configure the Special Card enrollment parameters,

Click **Enrollment > Special Card**. The **Special Card** page appears.

The screenshot shows a web-based form titled "Special Card" in a blue header bar. The form contains four rows of configuration options: "Door ID" with a text input field and a picklist icon; "Enrollment Type" with a dropdown menu showing "Read Only Card"; "Special Function" with a dropdown menu showing "Official Work - IN"; and "Card" with a dropdown menu showing "1 Card". At the bottom of the form are two buttons: "Enroll" and "Cancel".

Configure the following:

- **Door ID:** Click the **Select Door** picklist. The **Panel Doors** pop-up appears. Select the desired door.

**OR**

You can also search for the desired door. To do so, enter the keyword in the Search box. Click **Search**



. The doors will be filtered as per the keyword. Select the desired door.

The selected door's ID appears against the Door ID. On this door the enrollment will be performed for the Special Card.

- **Enrollment Type:** Select the desired option from the drop-down list — Read Only Card, Smart Card.



If ARC DC200 (Single Door Dual Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Reader Group 1/2 and Reader Group1/2 is selected in Enrollment > User > Enrollment Using, then only Read Only Card option will be functional as Enrollment Type.

If ARC DC200 (Dual Door Single Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Door 1 and Reader Group1 is selected in Enrollment > User > Enrollment Using, then only Read Only Card option will be functional as Enrollment Type.



If ARC DC200 (Dual Door Dual Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Door 1 and Reader Group1 is selected in Enrollment > User > Enrollment Using, then only Read Only Card option will be functional as Enrollment Type.

If ARC DC200 (Dual Door Dual Reader) is selected as the Door, OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers > Door 2 and Reader Group1 is selected in Enrollment > User > Enrollment Using, then only Read Only Card option will be functional as Enrollment Type.

- **Special Function:** Select the desired option from the drop-down list for which the Special Card is to be enrolled. For more details, refer to ["Special Functions"](#).
- **Card:** Select the desired card number on which the Special Function is to be enrolled from the drop-down list. Maximum four cards can be enrolled for a single Special Function.
- Click **Enroll** to initiate enrollment on the selected door. You will be prompted by the selected door to display the Special Card for enrollment.

After the card has been enrolled the Card Number is displayed against the selected Special Function on the Special Function page. For more details, refer to ["Special Functions"](#).

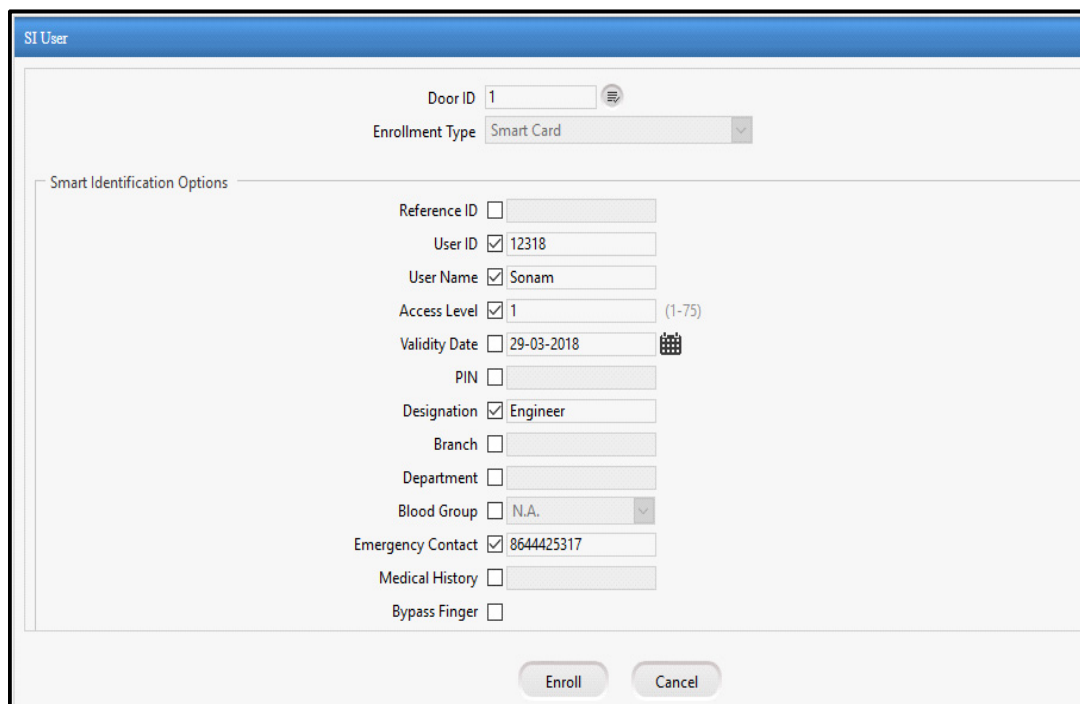
| Special Function |                     |                                     |                  |                  |        |        |        |
|------------------|---------------------|-------------------------------------|------------------|------------------|--------|--------|--------|
| Configuration    |                     |                                     |                  | Schedule         |        |        |        |
| Sr. No.          | Special Function    | Active                              | Functional Group | Card 1           | Card 2 | Card 3 | Card 4 |
| 1                | Official Work - IN  | <input checked="" type="checkbox"/> | All              |                  |        |        |        |
| 2                | Official Work - OUT | <input checked="" type="checkbox"/> | All              |                  |        |        |        |
| 3                | Short Leave - IN    | <input checked="" type="checkbox"/> | All              | 1252629933542272 |        |        |        |
| 4                | Short Leave - OUT   | <input checked="" type="checkbox"/> | All              |                  |        |        |        |
| 5                | Regular - IN        | <input checked="" type="checkbox"/> | All              |                  |        |        |        |
| 6                | Regular - OUT       | <input checked="" type="checkbox"/> | All              |                  |        |        |        |
| 7                | Break End           | <input checked="" type="checkbox"/> | All              |                  |        |        |        |
| 8                | Break Start         | <input checked="" type="checkbox"/> | All              |                  |        |        |        |
| 9                | Over Time - IN      | <input checked="" type="checkbox"/> | All              |                  |        |        |        |
| 10               | Over Time - OUT     | <input checked="" type="checkbox"/> | All              |                  |        |        |        |

# SI User

You can enroll certain users as Smart Identification Users, so that these users are allowed access to other branch offices by means of Smart Card, even though they are not enrolled in the systems of the branch offices.

To configure the Special Identification User enrollment parameters,

Click **Enrollment > SI User**. The **SI User** page appears.



The screenshot shows the 'SI User' enrollment form. At the top, there is a 'Door ID' field with a value of '1' and a picklist icon. Below it is the 'Enrollment Type' dropdown menu, which is set to 'Smart Card'. The main section is titled 'Smart Identification Options' and contains several fields: 'Reference ID' (checkbox), 'User ID' (checkbox with value '12318'), 'User Name' (checkbox with value 'Sonam'), 'Access Level' (checkbox with value '1' and a range '(1-75)'), 'Validity Date' (checkbox with value '29-03-2018' and a calendar icon), 'PIN' (checkbox), 'Designation' (checkbox with value 'Engineer'), 'Branch' (checkbox), 'Department' (checkbox), 'Blood Group' (checkbox with value 'N.A.' and a dropdown arrow), 'Emergency Contact' (checkbox with value '8644425317'), 'Medical History' (checkbox), and 'Bypass Finger' (checkbox). At the bottom right, there are 'Enroll' and 'Cancel' buttons.

Configure the following parameters:

- **Door ID:** Click the **Select Door** picklist. The **Panel Doors** pop-up appears. Select the desired door.

**OR**

You can also search for the desired door. To do so, enter the keyword in the Search box. Click **Search**

 . The doors will be filtered as per the keyword. Select the desired door.

The selected doors ID appears against the Door ID. On this door the enrollment will be performed for the SI User.



*If ARC DC200 is selected as the Door and if OSDP is selected as the RS-485 Interface Protocol option in Devices > Door Configuration > Readers, then the Enrollment functionality will not work.*

- **Enrollment Type:** By default, Smart Card is displayed and it is un-editable.

## Smart Identification Options



*The Smart Identification Options differ according to the Door Type.*

Select the check boxes of the desired options and configure the details against each option. This information will be written onto the Smart Card for the SI User during enrollment:

- **Reference ID:** If you wish to use the Reference ID for Smart Identification, select the check box and configure the desired ID (maximum 8 digits).
- **User ID:** If you wish to use User ID for Smart Identification, select the check box and configure the desired ID (maximum 15 characters).
- **User Name:** If you wish to use the User Name for Smart Identification, select the check box and configure the user name (maximum 15 characters).
- **Access Level:** If you wish to use the Access Level for Smart Identification, select the check box and configure the desired level you wish to assign (valid:1 to 75).
- **Validity Date:** If you wish to use the Validity Date for Smart Identification, select the check box and click the calendar to select the desired date till which the user should be considered as a valid user.
- **PIN:** If you wish to use the PIN for Smart Identification, select the check box and configure the desired PIN number for the user (maximum 6 digits).
- **Finger Template:** If you wish to use the Finger Template for Smart Identification, select the check box and select the number of templates to be considered for enrollment from the drop-down list.
- **Designation:** If you wish to use the Designation for Smart Identification, select the check box and configure the designation.
- **Branch:** If you wish to use the Branch for Smart Identification, select the check box and configure the branch name.
- **Department:** If you wish to use the Department for Smart Identification, select the check box and configure the department name.
- **Blood Group:** If you wish to use the Blood Group for Smart Identification, select the check box and select the blood group from the drop-down list.
- **Emergency Contact:** If you wish to use the emergency number for Smart Identification, select the check box and configure the contact number.
- **Medical History:** If you wish to use the medical history for Smart Identification, select the check box and configure the medical history.
- **Bypass Finger:** Select the check box, if you wish to that the finger must be bypassed.
- **VIP:** Select the check box, if you want VIP to be written onto the Smart Card.
- **ASC:** Select the check box, if you want the ASC defined in the PANEL200 to be written onto the Smart Card.

- **Facility Code:** Select the check box, if you want the Facility Code defined in the PANEL200 to be written onto the Smart Card.
- **Smart Access Route ID and Smart Access User Level:** Select the check box and configure the Smart Access Route ID and Smart Access User Level. Users will be allowed access to only specified doors with specified levels in predefined route using the Smart Card.

Click **Enroll** to enroll the user or click **Cancel** to discard the changes.

# Authorization

---

When enrollment of new user is done, then the enrolled credentials require authorization for accessing the doors.

The Authorization requests will appear here only if **Authorization on Enrollment** check box is enabled from “Enrollment” under “Advanced Profile”.



*When faces are enrolled from **Face Recognition- Face Enrollment** (“Face Enrollment”), then only these requests will not be displayed here for approval even if the **Authorization on Enrollment** is enabled from “Enrollment” under “Advanced Profile”.*

To view the Authorization requests,

Click **Enrollment > Authorization**. The **Authorization** page appears.

| User ID          | User Name | Status | Authorize <input type="checkbox"/> | Reject <input type="checkbox"/> |
|------------------|-----------|--------|------------------------------------|---------------------------------|
| No Record Found! |           |        |                                    |                                 |

The **Status** column displays the status of the applications — Pending, Authorized, Rejected.

The screenshot shows a window titled "Authorization". At the top, there is a "Search User" text box with a magnifying glass icon, a "User Status" dropdown menu set to "All", and a "Clear Filter" icon. Below this is a table with the following columns: "User ID", "User Name", "Status", "Authorize", and "Reject". The table contains one row with the data: User ID: 3, User Name: Isha, Status: Pending, Authorize: ☐, and Reject: ☐. At the bottom of the window, there are "Save" and "Cancel" buttons.

| User ID | User Name | Status  | Authorize <input type="checkbox"/> | Reject <input type="checkbox"/> |
|---------|-----------|---------|------------------------------------|---------------------------------|
| 3       | Isha      | Pending | <input type="checkbox"/>           | <input type="checkbox"/>        |

You can approve or reject the desired application. To do so, select the corresponding check box under **Authorize/Reject** as per your requirement.

**OR**

You can also search for the desired application. To do so, enter the keyword in the Search box. Click **Search** . The applications will be filtered as per the keyword. Now, select the corresponding check box under **Authorize/Reject** as per your requirement.

**OR**

You can filter the applications on the basis of the User Status. Select the desired option — All, Pending, Rejected. The application will appear according to the set filter. Now, select the corresponding check box under **Authorize/Reject** as per your requirement.

To clear the set filters, click **Clear Filter** .

Authorization

Search User

User Status

All

| User ID | User Name | Status  | Authorize <input checked="" type="checkbox"/> | Reject <input type="checkbox"/> |
|---------|-----------|---------|-----------------------------------------------|---------------------------------|
| 3       | Isha      | Pending | <input checked="" type="checkbox"/>           | <input type="checkbox"/>        |

Save

Cancel

For example, select the check box under **Authorize** and click **Save**.

The authorized user can use the credentials to access the doors.



---

Access Control Policies can be configured to detect and report intrusions at various places such as access to warehouse, cash rooms in Banks, Research and Development Departments in Corporate as well as other places where unauthorized access needs to be monitored.

Access Control Policies allows you to grant, record, deny, detect and report access to facilities, services, information and other assets that need to be protected from unauthorized access.

All the events related to the Access Policies set by you appear in the Access Policy Reports. For details, refer to [“Access Policies”](#) in [“Reports”](#).

The Access Policies and allows you to:

- configure the 2-person rule parameters. For details, refer to [“2-Person Rule”](#).
- configure the access route parameters. For details, refer to [“Access Route”](#).
- configure the first-in user parameters. For details, refer to [“First-IN User Rule”](#).
- configure the smart card access route parameters. For details, refer to [“Smart Card Access Route”](#).
- configure the time zone parameters. For details, refer to [“Time Zone”](#).
- configure the occupancy control parameters. For details, refer to [“Occupancy Control”](#).
- configure the access rule parameters. For details, refer to [“Access Rule”](#).

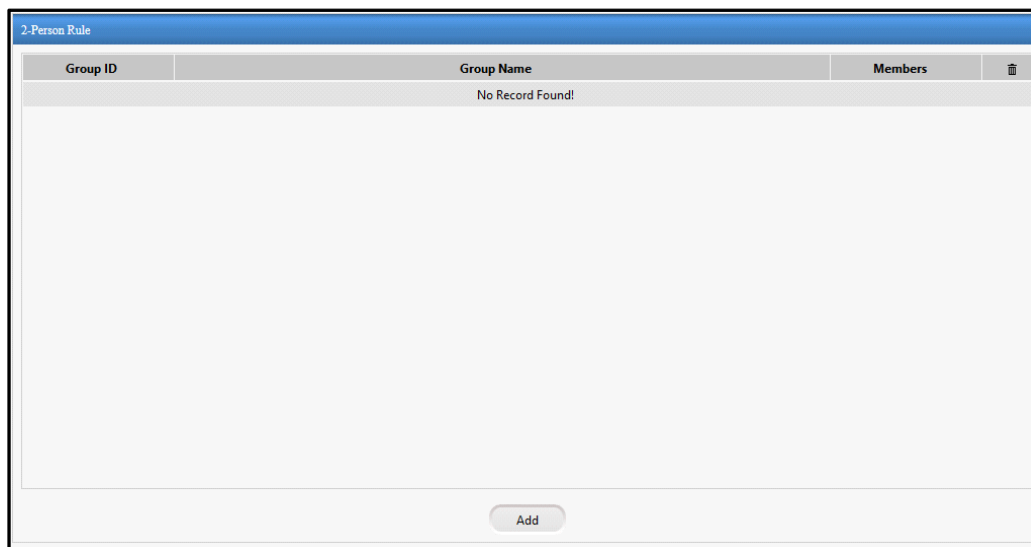
## 2-Person Rule

---

2-Person Rule is when you want to allow access to a zone only when valid credentials of two users are presented on the door. This is a control mechanism, wherein higher level of security can be provided especially for critical areas like Cash Rooms, R&D Labs, Sensitive Documents Storage Rooms etc.

To configure the 2-Person Rule,

Click **Access Policies > 2-Person Rule**. The **2-Person Rule** page appears.



All the created **2-Person Rules** appear in the grid with their details — Group ID, Group Name, Number of Members in the rule.

You can click the desired rule and edit it as per your requirement or you can add new rule.

You can also delete any rule. To do so, click **Delete**  corresponding to the desired rule.

## Adding 2-Person Rule

To add a 2-Person Rule,

Click **Add**. You can create maximum **16** 2-Person Rules. Each rule can have 20 members.

| Member ID | User ID | User Name |  |
|-----------|---------|-----------|--|
| 1         |         |           |  |
| 2         |         |           |  |
| 3         |         |           |  |
| 4         |         |           |  |
| 5         |         |           |  |
| 6         |         |           |  |
| 7         |         |           |  |
| 8         |         |           |  |
| 9         |         |           |  |
| 10        |         |           |  |
| 11        |         |           |  |
| 12        |         |           |  |
| 13        |         |           |  |
| 14        |         |           |  |

Configure the following parameters:

- **Group ID:** The Group ID is auto-generated by the PANEL200.
- **Group Name:** Configure a name you wish to assign to the rule.

### Group Members

- **User:** Click **Select User** picklist. The **Users** pop-up appears. Select the desired user.

**OR**

If required, you can also search for the desired user.

**Search By:** Select the desired option by which you wish to search for the user — User ID, User Name. In

the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Click to select the desired user.

The selected user's ID and Name appear against the User.

Users

Search by

User Name

Enter ID/Name

Q

| User ID | User Name |
|---------|-----------|
| U1      | Smita     |
| Smita   | Smita     |
| 2959    | Jaldeep   |

4

Click **Update** to save the member in the grid. Similarly, you can add other members.

2-Person Rule

Group ID

1

Group Name

2PersonRule1

Group Members

User ID

Update

Cancel

| Member ID | User ID | User Name |  |
|-----------|---------|-----------|--|
| 1         | Smita   | Smita     |  |
| 2         | Ak2     | Ak2       |  |
| 3         |         |           |  |
| 4         |         |           |  |
| 5         |         |           |  |
| 6         |         |           |  |
| 7         |         |           |  |
| 8         |         |           |  |
| 9         |         |           |  |
| 10        |         |           |  |
| 11        |         |           |  |
| 12        |         |           |  |
| 13        |         |           |  |
| 14        |         |           |  |

1

2

Add

Delete

Save

Cancel

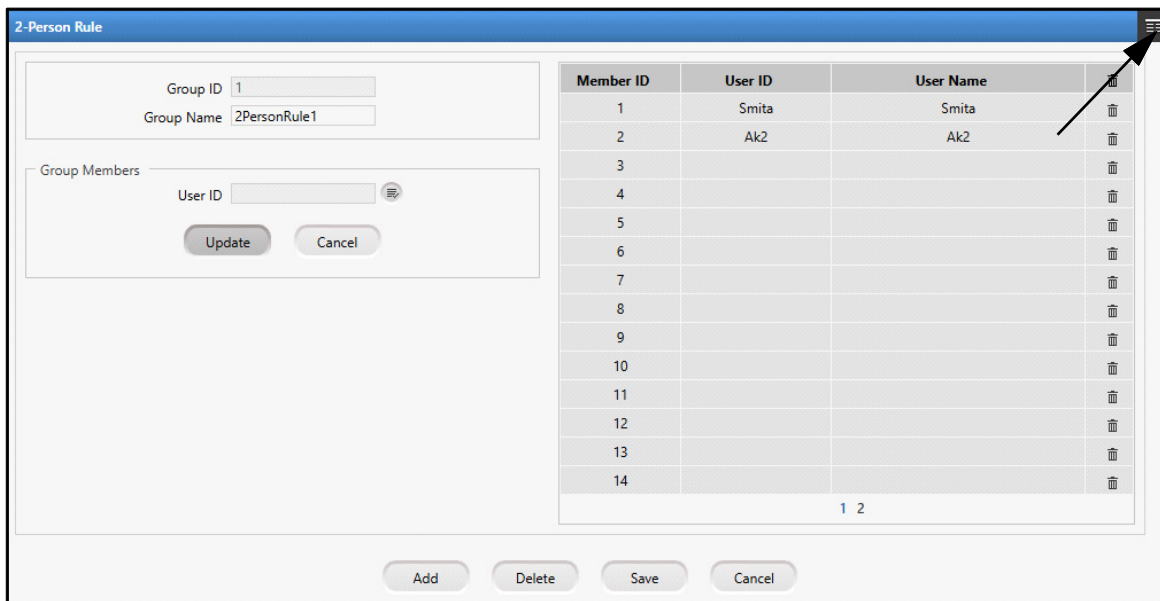
You can also delete any member if required. To do so, click **Delete**  corresponding to the desired member.



*If the first person is an authorized user and the 2nd person is a VIP then, PANEL200 considers the VIP as an authorized 2nd person to validate the 2 -Person Rule.*

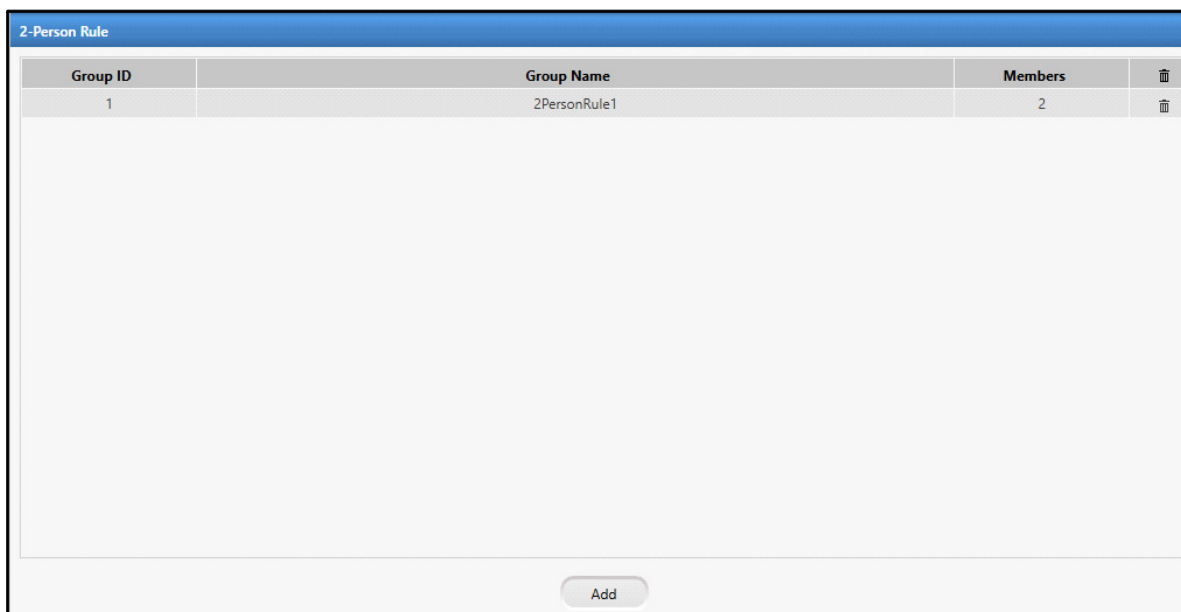
Click **Save** to save the settings or click **Cancel** to discard.

After you have completed all the configurations and if you wish to view all the created 2-Person Rules, click **View List** .



| Member ID | User ID | User Name |  |
|-----------|---------|-----------|--|
| 1         | Smita   | Smita     |  |
| 2         | Ak2     | Ak2       |  |
| 3         |         |           |  |
| 4         |         |           |  |
| 5         |         |           |  |
| 6         |         |           |  |
| 7         |         |           |  |
| 8         |         |           |  |
| 9         |         |           |  |
| 10        |         |           |  |
| 11        |         |           |  |
| 12        |         |           |  |
| 13        |         |           |  |
| 14        |         |           |  |

The 2-Person Rule page displays all the created 2-Person Rules.



| Group ID | Group Name   | Members |  |
|----------|--------------|---------|--|
| 1        | 2PersonRule1 | 2       |  |

After you create the rules, you must:

- select the 2-Person Rule check box to enable at the Panel level. For details, refer to “Set1” in “[Access Features](#)”
- enable it in the desired zone. For details, refer to “[Advance Configuration 1](#)” in “[Zone Configuration](#)”.
- assign this zone to the desired doors. Now this rule will be applicable for those doors who are assigned the zone which is enabled for the rule. For details, refer to “[Basic Configuration](#)” in “[Door Configuration](#)”.
- assign the doors to the users. For details, refer to “[Profile](#)” in “[User Configuration](#)”.

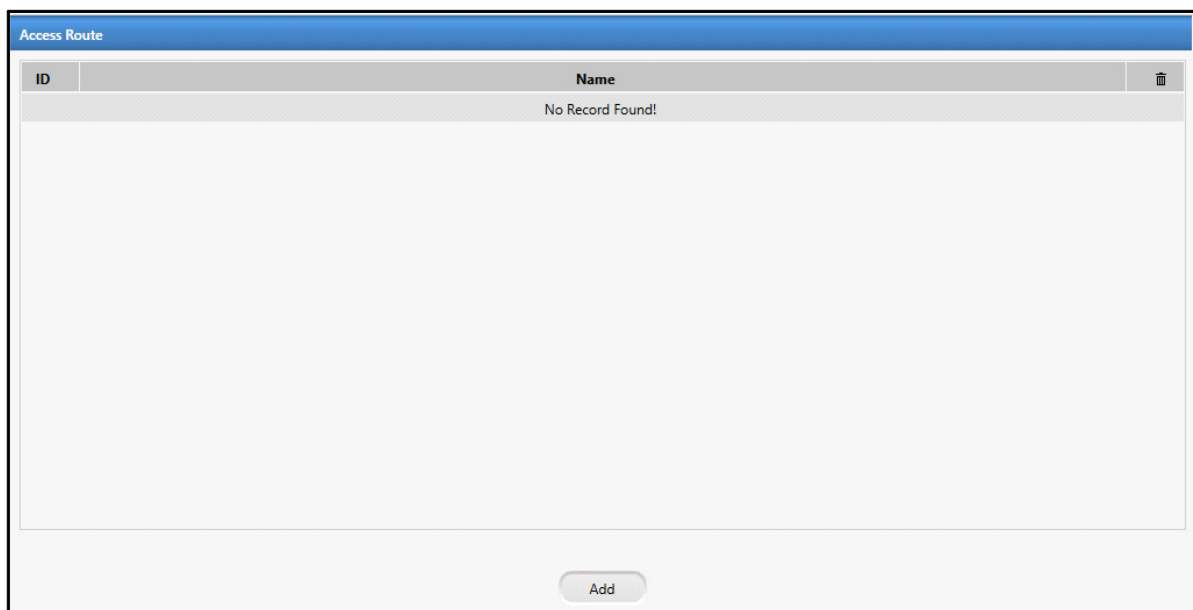
# Access Route

---

The Access Route functionality enables you to define an access policy which allows the user to access only specified doors with specific levels in predefined route, in a sequential or non-sequential manner.

To configure the Access Route,

Click **Access Policies > Access Route**. The **Access Route** page appears.



All the created **Access Routes** appear in the grid with their details — ID, Name.

You can click the desired Access Route and edit it as per your requirement or you can add new Access Route.

You can also delete any Access Route. To do so, click **Delete**  corresponding to the desired Access Route.

## Adding Access Route

To add an Access Route,

Click **Add**. You can create maximum **255** Access Routes. Each Access Route can have 255 members.

| Member ID | Door ID | Door Name | Level |  |
|-----------|---------|-----------|-------|--|
| 1         |         |           |       |  |
| 2         |         |           |       |  |
| 3         |         |           |       |  |
| 4         |         |           |       |  |
| 5         |         |           |       |  |
| 6         |         |           |       |  |
| 7         |         |           |       |  |
| 8         |         |           |       |  |
| 9         |         |           |       |  |
| 10        |         |           |       |  |
| 11        |         |           |       |  |
| 12        |         |           |       |  |
| 13        |         |           |       |  |
| 14        |         |           |       |  |

Configure the following parameters:

- **ID:** The ID is auto-generated by the PANEL200.
- **Name:** Configure a name you wish to assign to the Access Route.
- **Active:** Select the check box to enable the Access Route.

| Member ID | Door ID | Door Name | Level |  |
|-----------|---------|-----------|-------|--|
| 1         |         |           |       |  |
| 2         |         |           |       |  |
| 3         |         |           |       |  |
| 4         |         |           |       |  |
| 5         |         |           |       |  |
| 6         |         |           |       |  |
| 7         |         |           |       |  |
| 8         |         |           |       |  |
| 9         |         |           |       |  |
| 10        |         |           |       |  |
| 11        |         |           |       |  |
| 12        |         |           |       |  |

- **Sequenced Route:** Select the check box to enable a sequential route. The PANEL200 checks the route based on the levels defined. For example, the user has to present his/her credential on Level 1 door and then go on to Level 2, Level 3 and so on. In this case the order has to be maintained for both, IN as well as the OUT punches. Therefore it is necessary to have exit readers installed on all doors of the access route.

If it is disabled then the doors will not have any sequence in the route.

- **Restrictions:** Select the desired Restriction type from the drop-down list.

- **Hard:** If you select this option, access will be allowed only if the Access Route is followed.
  - **Soft:** If you select this option, access will be allowed on any door with an Access Route Violation message.
- **Reset on Lowest Level:** Select the check box to enable the PANEL200 to reset the current level status to allow access on the lowest level.  
  
This option is useful when the user is not following the proper order while exiting the premises. If enabled then the user will be allowed access on the lowest level irrespective of his/her state but this will be applicable only on the entry side.
  - **Check on Last Exit Level:** If you have enabled Sequenced Route, select the check box if you wish the Panel200 to check the last exit level.
  - **Last Exit Level Restriction:** Select the desired restriction type from the drop-down list.
    - **Hard:** If you select this option, exit will be allowed only if the Access Route is followed.
    - **Soft:** If you select this option, exit will be allowed with an Access Route Violation message.

## Configured Route

If you have **not** enabled Sequenced Route, you need to configure a route for accessing the doors.

- **Door:** Click the **Select Door** picklist. The **Panel Doors** pop-up appears. Select the desired door.

**OR**

You can also search for the desired door. To do so, enter the keyword in the Search box. Click **Search**



. The doors will be filtered as per the keyword. Select the desired door.

The selected doors name appears.

- **Level:** Select the Level you wish to assign to the selected door from the drop-down list.

Multiple doors can be assigned the same level. However, a single door cannot be assigned to the multiple levels.

If you have enabled Sequenced Route, then you need to configure parameters for **Entry** as well as **Exit** for each door.



## Entry

The screenshot shows a configuration window with two main sections: 'Entry' and 'Exit'. The 'Entry' section is currently selected and active, indicated by a minus sign on its header. It contains the following settings: 'Enabled' is checked with a checkbox; 'Route Timer' is a text input field containing '600' with a unit dropdown set to 'sec (1-65535)'; 'Level Restriction' is a dropdown menu currently showing 'Soft'; and 'Perform Action' is a dropdown menu currently showing 'On User Punch'. The 'Exit' section is below it and is inactive, with its header also having a minus sign. Its settings are identical but the 'Enabled' checkbox is unchecked. At the bottom of the window are two buttons: 'Update' and 'Cancel'.

This option allows user to configure the route timer between two levels (say *between door 2 & door 3*) during entry and perform an action for any violation as per the selected restriction. An alarm will also be triggered for the violation of Access Route. This alarm can be cleared/acknowledged by the Admin group users.

- **Enabled:** Select the check box to apply the Access Route Timer between two levels.
- **Route Timer:** Configure the duration in seconds between two access levels.
- **Level Restriction:** Select the desired restriction type from the drop-down list.
  - **Hard:** If you select this option, the entry to the next level will not be allowed.
  - **Soft:** If you select this option, the entry to the next level will be allowed, with a violation message.
- **Perform Action:** Select desired option — On User Punch, On Timer Elapsed — on the occurrence of which an action (Alarm Triggered) needs to taken when there is an Access Route violation.

## Exit

Similarly, you can configure the parameters for Exit.

If you have enabled Sequenced Route or not, Click **Update** to add the selected door to the route.

Similarly, you can add another door to the route. These appear in the right pane.

The 'Access Route' window displays configuration for 'RnD Route1'. On the left, settings include ID 1, Name 'RnD Route1', Active checked, Sequenced Route unchecked, Restrictions set to 'Soft', and Reset On Lowest Level checked. Below this is a 'Configured Route' section with a Door field and a Level dropdown set to 1, with 'Update' and 'Cancel' buttons. On the right is a table with columns: Member ID, Door ID, Door Name, Level, and a delete icon. The table contains one row: Member ID 1, Door ID 2, Door Name VEGA, Level 1. At the bottom are 'Save' and 'Cancel' buttons.

| Member ID | Door ID | Door Name | Level |  |
|-----------|---------|-----------|-------|--|
| 1         | 2       | VEGA      | 1     |  |
| 2         |         |           |       |  |
| 3         |         |           |       |  |
| 4         |         |           |       |  |
| 5         |         |           |       |  |
| 6         |         |           |       |  |
| 7         |         |           |       |  |
| 8         |         |           |       |  |
| 9         |         |           |       |  |
| 10        |         |           |       |  |
| 11        |         |           |       |  |
| 12        |         |           |       |  |
| 13        |         |           |       |  |
| 14        |         |           |       |  |

You can delete any added door from the route. To do so, click **Delete**  corresponding to the desired door.

Click **Save** to save the settings or click **Cancel** to discard.

After you have completed all the configurations of the Access Route and if you wish to view all the created Access Routes, click **View List** .

This image is identical to the previous one, but includes an arrow pointing to the 'View List' icon (three horizontal lines) located in the top right corner of the window's header bar.

The Access Route page displays all the created Access Routes.

Access Route

| ID | Name       |  |
|----|------------|--|
| 1  | RnD Route1 |  |

Add

You can delete any created Access Route. To do so, click **Delete**  corresponding to the desired Access Route.

After you configured the Access Route, you must:

- select the Access Route check box to enable at the Panel level. For details, refer to “Set1” in “Access Features”
- assign the route to the users. For details, refer to “Basic Access Control” in “User Configuration”.

You can reset the Access Route using Command if you have set Hard restriction. For details refer to [“Monitor”](#).



- *Whenever Panel Route Access is Reset from the Details in Monitor; user's access level will be set to unknown and whenever user punches on any door; that door's access level will be considered as user's access level.*
- *After that Access Route will work as before.*

# First-IN User Rule

---

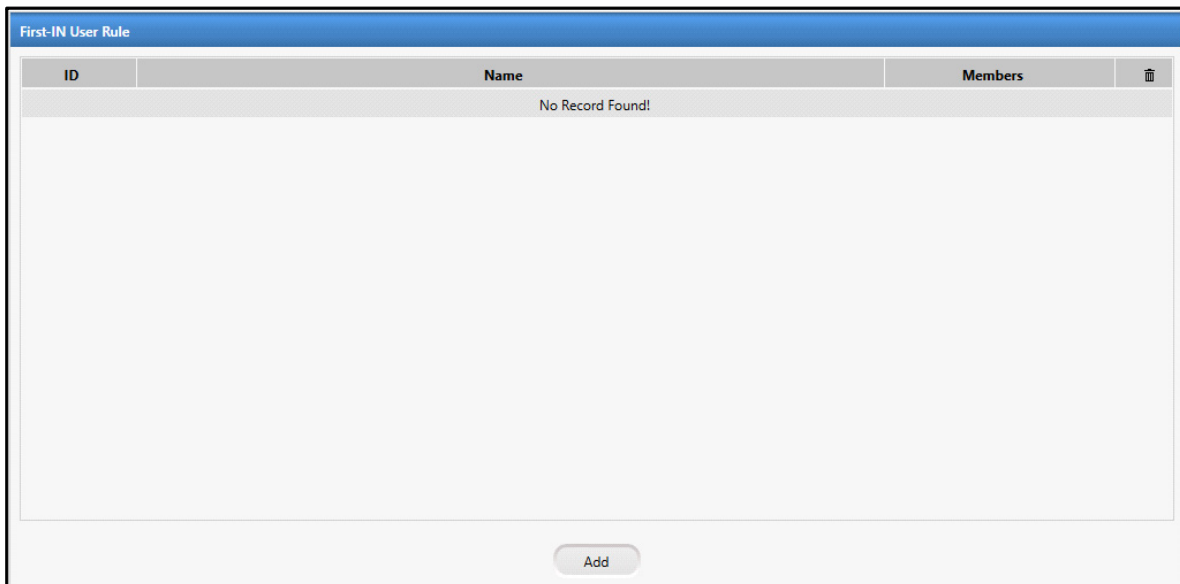
First-IN User Rule ensures the access to the zone is granted only when the valid credentials of the user (First-IN User) are presented on the door. As soon as the zone is unlocked using the First-IN user credential, the Panel200 will allow access to others in the zone till the First-IN user's working hours or the expiry of the configured timer.

Once the period is over, the access to the designated zone will be deactivated. The PANEL200 now waits for another valid First-IN user credential.

VIP user can access the First-IN User zone even when the zone is not activated by a First-IN user. However, the VIP user cannot activate the zone to allow access to other users.

To configure the First-IN User Rule,

Click **Access Policies > First-IN User Rule**. The **First-IN User Rule** page appears.



All the created **First-IN User Rules** appear in the grid with their details — ID, Name, Number of Members in the rule.

You can click the desired rule and edit it as per your requirement or you can add a new rule.

You can also delete any rule. To do so, click **Delete**  corresponding to the desired rule.

## Adding First-IN User Rule

To add a First-IN User Rule,

Click **Add**. You can create maximum **99** First-IN Rules. Each rule can have 999 members.

| Member No | User ID | User Name |  |
|-----------|---------|-----------|--|
| 1         |         |           |  |
| 2         |         |           |  |
| 3         |         |           |  |
| 4         |         |           |  |
| 5         |         |           |  |
| 6         |         |           |  |
| 7         |         |           |  |
| 8         |         |           |  |
| 9         |         |           |  |
| 10        |         |           |  |
| 11        |         |           |  |
| 12        |         |           |  |
| 13        |         |           |  |
| 14        |         |           |  |

Configure the following parameters:

- **ID:** The ID is auto-generated by the PANEL200.
- **Name:** Configure a name you wish to assign to the rule.

### Group Members

- **User:** Click **Select User** picklist. The **Users** pop-up appears. Select the check boxes of the desired users which you wish to add as members to the rule. Click **Ok**.

**OR**

If required, you can also search for the desired user.

**Search By:** Select the desired option by which you wish to search for the user — User ID, User Name. In the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Select the check boxes of the desired users which you wish to add as members to the rule. Click **Ok**.

Users

Search by

User Name

Enter ID/Name

Q

| User ID | User Name |
|---------|-----------|
| U1      | Smita     |
| Smita   | Smita     |
| 2959    | Jaldeep   |

4

The selected users added as members appear in the right pane.

First-IN User Rule

ID 1

Name HR Group

Group Members

Users

| Member No | User ID | User Name |  |
|-----------|---------|-----------|--|
| 1         | Smita   | Smita     |  |
| 2         | 2959    | Jaldeep   |  |
| 3         |         |           |  |
| 4         |         |           |  |
| 5         |         |           |  |
| 6         |         |           |  |
| 7         |         |           |  |
| 8         |         |           |  |
| 9         |         |           |  |
| 10        |         |           |  |
| 11        |         |           |  |
| 12        |         |           |  |
| 13        |         |           |  |
| 14        |         |           |  |

1 2 3 4 5 6 7 8 9 10

Save

Cancel

You can also delete any member if required. To do so, click **Delete**  corresponding to the desired member.

Click **Save** to save the settings or click **Cancel** to discard.

After you have completed all the configurations, if you wish to view all the created First-IN Rules, click **View List**



First-IN User Rule

ID 1

Name HR Group

Group Members

Users

| Member No | User ID | User Name |  |
|-----------|---------|-----------|--|
| 1         | Smita   | Smita     |  |
| 2         | 2959    | Jaldeep   |  |
| 3         |         |           |  |
| 4         |         |           |  |
| 5         |         |           |  |
| 6         |         |           |  |
| 7         |         |           |  |
| 8         |         |           |  |
| 9         |         |           |  |
| 10        |         |           |  |
| 11        |         |           |  |
| 12        |         |           |  |
| 13        |         |           |  |
| 14        |         |           |  |

Save

Cancel

The First-IN Rule page displays all the created First-IN Rules.

| ID | Name     | Members |  |
|----|----------|---------|--|
| 1  | HR Group | 2       |  |

Add

After you create the rules, you must:

- select the First-IN Rule check box to enable at the Panel level. For details, refer to [“Set1”](#) in [“Access Features”](#)
- enable it in the desired zone. For details, refer to [“Advance Configuration 2”](#) in [“Zone Configuration”](#).
- assign this zone to the desired doors. Now this rule will be applicable for those doors who are assigned the zone which is enabled for the rule. For details, refer to [“Basic Configuration”](#) in [“Door Configuration”](#).
- assign the doors to the users. For details, refer to [“Profile”](#) in [“User Configuration”](#).

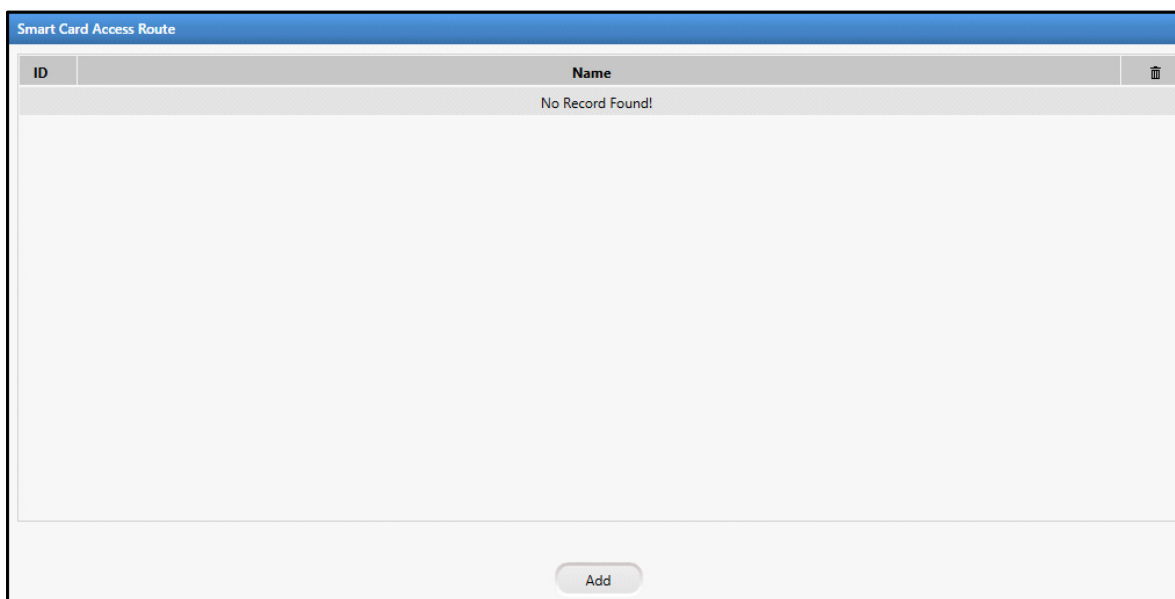
# Smart Card Access Route

---

The Smart Card Access Route allows users to access only specified doors with specified levels in the predefined route sequentially.

To configure the Smart Card Access Route,

Click **Access Policies > Smart Card Access Route**. The Smart Card Access Route page appears.



All the created Smart Card Access Routes appear in the grid with their details — ID, Name.

You can click the desired route and edit it as per your requirement or you can add a new route.

You can also delete any route. To do so, click **Delete**  corresponding to the desired route.



## Adding Smart Card Access Route

To add a Smart Card Access Route,

Click **Add**. You can create maximum **99** Smart Access Card Routes. Each route can have 255 members.

| ID               | Name | Level |  |
|------------------|------|-------|--|
| No Record Found! |      |       |  |

Configure the following parameters:

- **ID:** The ID is auto-generated by the PANEL200.
- **Name:** Configure a name you wish to assign to the Smart Card Access Route.
- **Active:** Select the check box to enable the Smart Card Access Route.
- **Sequenced Route:** Select the check box to enable the sequenced route.
- **Restrictions:** Select the Restriction type from the drop-down list.
  - **Hard:** If you select this option, access will be allowed only if the access route is followed.
  - **Soft:** If you select this option, access will be allowed on any door within the access route with an Access Route Violation message.
- **Reset on Start Level:** Select the check box to enable the PANEL200 to reset the current level status to allow access on the lowest level.

This option is useful when the user is not following the proper order while exiting the premises. If this is enabled then the user will be allowed access on the lowest level irrespective of his/her state but this will be applicable only on the entry side.

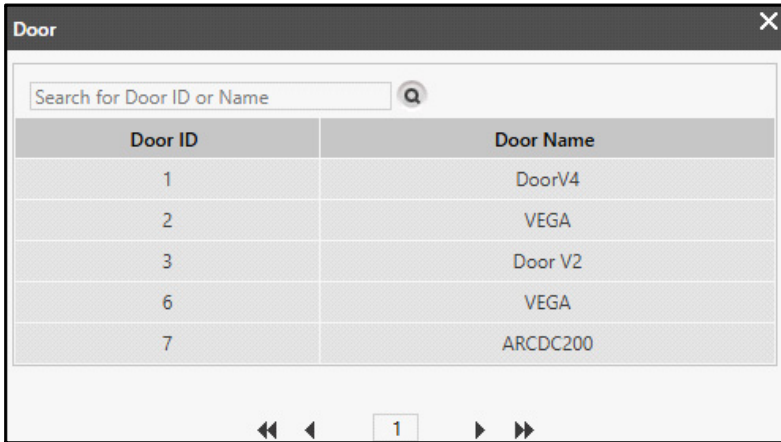
### Configured Route

- **Door:** Click the **Select Door** picklist. The **Door** pop-up appears. Select the desired door.

**OR**

You can also search for the desired door. To do so, enter the keyword in the Search box. Click **Search**

 . The doors will be filtered as per the keyword. Select the desired door.



The 'Door' window displays a search bar and a table of doors. The search bar contains the text 'Search for Door ID or Name' and a magnifying glass icon. The table has two columns: 'Door ID' and 'Door Name'. The rows are as follows:

| Door ID | Door Name |
|---------|-----------|
| 1       | DoorV4    |
| 2       | VEGA      |
| 3       | Door V2   |
| 6       | VEGA      |
| 7       | ARCDC200  |

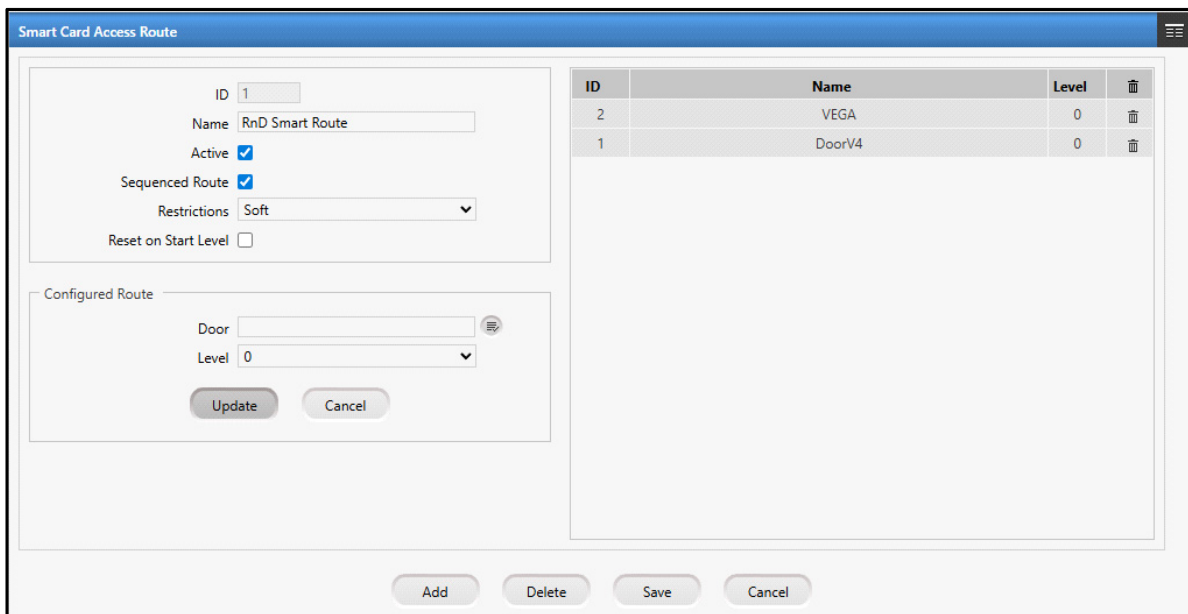
At the bottom of the window, there are navigation arrows and a page indicator showing '1'.

The selected doors name appears.

- **Level:** Select the Level you wish to assign to the selected door from the drop-down list.

Multiple doors can be assigned the same level. However, a single door cannot be assigned to the multiple levels.

Click **Update** to add the selected door to the route. Similarly, you can add other doors. These appear in the right pane.



The 'Smart Card Access Route' window is divided into two main sections. The left section contains configuration options for a route:

- ID: 1
- Name: RnD Smart Route
- Active: ☒
- Sequenced Route: ☒
- Restrictions: Soft (dropdown)
- Reset on Start Level: ☐

The right section is titled 'Configured Route' and contains a table with the following data:

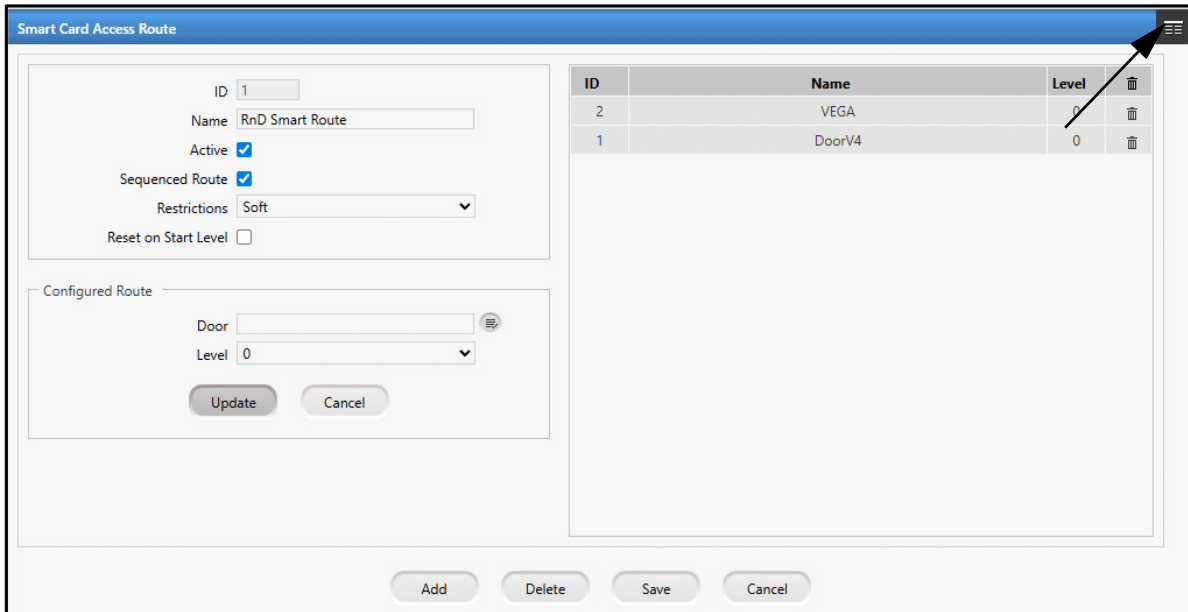
| ID | Name   | Level |                                                                                       |
|----|--------|-------|---------------------------------------------------------------------------------------|
| 2  | VEGA   | 0     |  |
| 1  | DoorV4 | 0     |  |

At the bottom of the 'Configured Route' section, there are 'Update' and 'Cancel' buttons. At the very bottom of the window, there are 'Add', 'Delete', 'Save', and 'Cancel' buttons.

You can delete any added door from the route. To do so, click **Delete**  corresponding to the desired door.

Click **Save** to save the settings or click **Cancel** to discard.

After you have completed all the configurations of the Smart Card Access Route and if you wish to view all the created Smart Access Card Routes, click **View List**  .

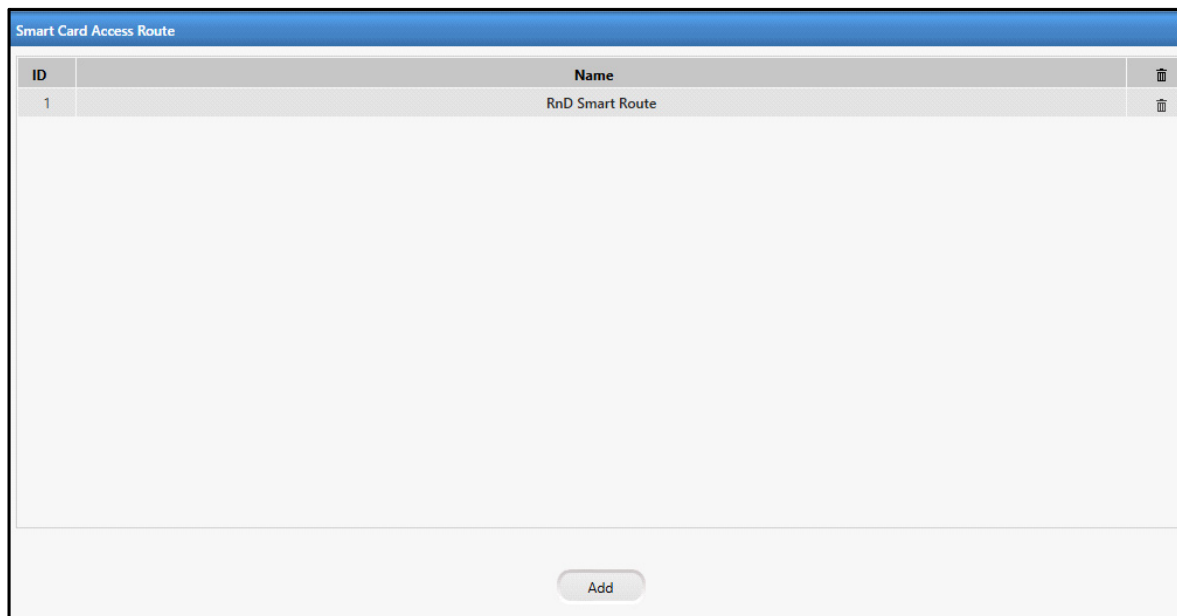


The screenshot shows the 'Smart Card Access Route' configuration window. On the left, there are configuration options for a selected route (ID 1, Name 'RnD Smart Route'). The 'Active' checkbox is checked, 'Sequenced Route' is checked, 'Restrictions' is set to 'Soft', and 'Reset on Start Level' is unchecked. Below these is a 'Configured Route' section with 'Door' and 'Level' (0) fields, and 'Update' and 'Cancel' buttons. On the right, a table lists the created routes:

| ID | Name   | Level |                                                                                     |
|----|--------|-------|-------------------------------------------------------------------------------------|
| 2  | VEGA   | 0     |  |
| 1  | DoorV4 | 0     |  |

At the bottom of the window are 'Add', 'Delete', 'Save', and 'Cancel' buttons. An arrow points to the 'View List' icon in the top right corner.

The Smart Card Access Route page displays all the created Smart Card Access Routes.



The screenshot shows the 'Smart Card Access Route' list view window. It displays a table with the following data:

| ID | Name            |                                                                                       |
|----|-----------------|---------------------------------------------------------------------------------------|
| 1  | RnD Smart Route |  |

At the bottom of the window is an 'Add' button.

You can delete any created Smart Card Access Route. To do so, click **Delete**  corresponding to the desired Smart Card Access Route.

After configuring the Smart Card Access Route, you must:

- select the Smart Card Access Route check box to enable at the Panel level. For details, refer to [“Set2” in “Access Features”](#)
- assign it to the desired users. For details, refer to [“Advanced Access Control” in “User Configuration”](#).

# Time Zone

---

Time Zone allows the PANEL200 to grant access to the users to certain Access Zone during a specified time period. This time period can be set as per your requirement, either as 24-hours or limited hours/minutes.

Each Time Zone represents a particular period of time. Time Zones may have overlapping time periods. The maximum time period which can be assigned to a time zone is 23:59 hours.

To configure the Time Zone,

Click **Access Policies > Time Zone**. The **Time Zone** page appears.

| ID | Name        |  |
|----|-------------|--|
| 1  | Time Zone 1 |  |

The Time Zone allows you to:

- configure the configuration parameters. For details, refer to [“Configuration”](#).
- configure the group parameters. For details, refer to [“Group”](#).

By default **Time Zone 1** is already created and is displayed in the right pane. You can edit the same, however you cannot delete it.

To edit, click **Time Zone 1** from the right pane, edit the parameters as per your requirement and click **Save**.

You can also add new Time Zones. To do so,

Click **Add**.

## Configuration

The screenshot shows the 'Time Zone' configuration window. It has two tabs: 'Configuration' and 'Group'. The 'Configuration' tab is active and contains the following fields:

- ID: 2
- Name: (empty)
- Active: ☐
- Start Time: 00:00
- End Time: 00:00
- Active Days: ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Holiday

The 'Group' tab is also visible and contains a table with the following data:

| ID | Name        |  |
|----|-------------|--|
| 1  | Time Zone 1 |  |

At the bottom of the window are 'Save' and 'Cancel' buttons.

Configure the following parameters:

- **ID:** The ID is auto-generated by the PANEL200.
- **Name:** Configure a name you wish to assign to the Time Zone.
- **Active:** Select the check box to enable the Time Zone.
- **Start Time:** Configure the Start Time (in hh:mm) of the Time Zone.
- **End Time:** Configure the End Time (in hh:mm) of the Time Zone.
- **Active Days:** Select the check box of the respective days for which the Time Zone will be applicable.
- **Holiday:** Select the check box if you want the Time Zone to be applicable on a Holiday.

Time Zone

Configuration

Group

ID 2

Name Lunch Time

Active ☒

Start Time 13 :00

End Time 15 :00

Active Days

☐ Sun
☒ Mon
☒ Tue
☒ Wed
☒ Thu
☒ Fri
☐ Sat
☐ Holiday

| ID | Name        |  |
|----|-------------|--|
| 1  | Time Zone 1 |  |

Save

Cancel

- Click **Save** to save the settings. The Time Zone appears in the right pane.

Time Zone

Saved Successfully

Configuration

Group

ID 2

Name Lunch Time

Active ☒

Start Time 13 :00

End Time 15 :00

Active Days

☐ Sun
☒ Mon
☒ Tue
☒ Wed
☒ Thu
☒ Fri
☐ Sat
☐ Holiday

| ID | Name        |  |
|----|-------------|--|
| 1  | Time Zone 1 |  |
| 2  | Lunch Time  |  |

Add

Delete

Save

Cancel

You can delete any added Time Zone. To do so, click **Delete**  corresponding to the desired Time Zone.

## Group

You can combine multiple time zones in a single group. To do so,

Click **Add**.

The screenshot shows a web application window titled "Time Zone". It has two tabs: "Configuration" and "Group". The "Group" tab is active. On the left, there is a form with three input fields: "ID", "Name", and "Time Zone" (which is a picklist). Below the form is a table with columns "ID" and "Name", and a "No Record Found!" message. On the right, there is a larger table with columns "ID", "Name", and a trash icon. It also shows a "No Record Found!" message. At the bottom center, there is an "Add" button.

Configure the following parameters,

- **ID:** The ID is auto-generated by the PANEL200.
- **Name:** Configure a name you wish to assign to the group.
- **Time Zone:** Click the **Time Zone** picklist. The **Time Zones** pop-up appears. Select the check boxes of the desired time zones. Click **Ok**.

### OR

If required, you can also search for the desired time zone

**Search By:** Select the desired option by which you wish to search for the time zone — ID, Time Zone

Name. In the corresponding box enter the keyword. Click **Search** . The time zones will be filtered as per the keyword. Select the check boxes of the desired time zones. Click **Ok**.

**Time Zones** [X]

Search by ID [v] Enter ID/Name [Q]

| ID | Time Zone Name |                          |
|----|----------------|--------------------------|
| 1  | Time Zone 1    | <input type="checkbox"/> |
| 2  | Lunch Time     | <input type="checkbox"/> |
| 3  | Maintenance    | <input type="checkbox"/> |

« « 1 » »

Ok

The selected Time Zone appears in the grid.

**Time Zone**

Configuration Group

ID 1

Name HO Zone Group

Time Zone [icon]

| ID | Name        |  |
|----|-------------|--|
| 2  | Lunch Time  |  |
| 3  | Maintenance |  |

| ID               | Name |  |
|------------------|------|--|
| No Record Found! |      |  |

Save Cancel

You can delete any added time zone. To do so, click **Delete** corresponding to the desired time zone.



- Click **Save** to save the settings. The Time Zone Group appears in the right pane.

The screenshot shows the 'Time Zone' configuration window with the 'Group' tab selected. The left pane contains input fields for 'ID' (1), 'Name' (HO Zone Group), and 'Time Zone' (with a dropdown icon). Below these is a table of existing groups:

| ID | Name        |  |
|----|-------------|--|
| 2  | Lunch Time  |  |
| 3  | Maintenance |  |

The right pane shows a table with the newly added group:

| ID | Name          |  |
|----|---------------|--|
| 1  | HO Zone Group |  |

At the bottom of the window are buttons for 'Add', 'Delete', 'Save', and 'Cancel'.

Similarly, you can add other groups. You can edit or delete the Time Zone Groups.

To edit, click the desired Time Zone Group from the right pane and edit the parameters as per your requirement.

To delete, click **Delete** corresponding to the desired Time Zone Group in the right pane.

After configuring the Time Zone, you can assign the desired time zone under [“Schedule Based Access Level Override”](#) in [“Access Group”](#).

# Access Cluster

The Access Cluster are groups of doors for which access can be allowed or denied depending on your requirement. For example, in chemical industries, if a user accesses a chemical prone area then s/he is restricted from going into areas which can harm him/her or the surroundings. So if the user is accessing one cluster (say chemical area); then s/he can be restricted from entering into another cluster (public area).

To configure the Access Cluster,

Click **Access Policies > Access Cluster**. The **Access Cluster** page appears.

| ID | Name      | Status   |
|----|-----------|----------|
| 1  | Cluster-1 | Inactive |

By default Cluster-1 is created and is disabled. You can use this cluster if required or create a new cluster.

To use Cluster-1, click the same from the right pane. Edit the parameters as per your requirement and click **Save**.

You cannot delete Cluster-1. However you can disable the same.

## Adding Access Cluster

To add an Access Cluster,

Click **Add**. You can add a maximum of **75** Clusters.

The 'Access Cluster' dialog box contains the following configuration fields on the left:

- ID: 2
- Name: (empty text box)
- Active: ☐
- Cluster Mode: Allow All Clusters (dropdown menu)
- Restriction Duration: 00 : 00

On the right, there is a table with the following data:

| ID | Name      | Status   |
|----|-----------|----------|
| 1  | Cluster-1 | Inactive |

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Configure the following parameters:

- **Name:** Configure a name you wish to assign to the cluster. For example, Cluster A
- **Active:** Select the check box to enable the cluster.
- **Cluster Mode:** Select the desired option:
  - **Allow All Clusters:** If you select this option, users accessing Cluster A will be allowed to access all other clusters.
  - **Allow Selected:** If you select this option, users accessing Cluster A will be allowed to access only selected clusters. If you select this option, you must configure **Allowed Cluster**.
  - **Allowed Cluster:** Click the **Allowed Cluster** picklist. The **Access Cluster** pop-up appears. Select the check boxes of the desired clusters you wish to allow access to. Click **Ok**.

OR

You can also search for the desired cluster. To do so, enter the keyword in the Search box. Click

**Search**  . The clusters will be filtered as per the keyword. Select the check boxes of the desired clusters you wish to allow access to. Click **Ok**.

The selected cluster appears in the grid. You can also delete any clusters you added. To do so, click

**Delete**  corresponding to the desired cluster.

- **Deny All Clusters:** If you select this option, users accessing Cluster A will be denied access to all other clusters till the restricted duration.
- **Restricted Duration:** Configure the duration in HH:MM format. Only after the expiry of this duration, the users will be allowed to access another cluster.

- Click **Save** to save the settings. The cluster appears in the right pane.

The 'Access Cluster' window displays configuration settings for a cluster on the left and a list of clusters on the right.

**Left Panel Configuration:**

- ID: 2
- Name: Cluster A
- Active: ☒
- Cluster Mode: Allow All Clusters (dropdown)
- Restriction Duration: 00 : 00

**Right Panel Table:**

| ID | Name      | Status   |
|----|-----------|----------|
| 1  | Cluster-1 | Inactive |
| 2  | Cluster A | Active   |

**Buttons:** Add, Delete, Save, Cancel

You can edit or delete any cluster.

To edit, click the desired Cluster from the right pane, edit the parameters as per your requirement and click **Save**.

You can delete any added cluster. To do so, click **Delete**  corresponding to the desired cluster.



*First time, that is, after PANEL200 is rebooted when user accesses the door of any cluster, user should be allowed. (Provided other access policies are verified).*

Let us understand this with the help of an example,

There are 3 clusters configured in PANEL200.

- For first cluster, mode selected is **Allow All Clusters** and Restricted Duration configured is 2 hours and 30 minutes.
- For second cluster, mode selected is **Allow Selected** and 1 allowed cluster is configured wherein allowed cluster no. configured is 3 and Restricted Duration is 40 minutes. (Here restricted duration is only for Denied Clusters)
- For third cluster, mode selected is **Deny All Clusters** and Restricted Duration configured is 1 hour.

The 'Access Cluster' window displays configuration settings for Cluster-1 on the left and a list of clusters on the right.

**Left Panel Configuration:**

- ID: 1
- Name: Cluster-1
- Active: ☒
- Cluster Mode: Allow All Clusters (dropdown)
- Restriction Duration: 02 : 30

**Right Panel Table:**

| ID | Name      | Status |
|----|-----------|--------|
| 1  | Cluster-1 | Active |

**Access Cluster**

ID

Name

Active ☒

Cluster Mode

Restriction Duration  :

Allowed Cluster

| ID | Name      |                                  |
|----|-----------|----------------------------------|
| 3  | Cluster-3 | <input type="button" value="⋮"/> |

| ID | Name      | Status |
|----|-----------|--------|
| 1  | Cluster-1 | Active |
| 2  | Cluster-2 | Active |
| 3  | Cluster-3 | Active |

**Access Cluster** Saved Success

ID

Name

Active ☒

Cluster Mode

Restriction Duration  :

| ID | Name      |                                  |
|----|-----------|----------------------------------|
| 3  | Cluster-3 | <input type="button" value="⋮"/> |

| ID | Name      | Status |
|----|-----------|--------|
| 1  | Cluster-1 | Active |
| 2  | Cluster-2 | Active |
| 3  | Cluster-3 | Active |

Case1: For first time user is accessing a door of Cluster 1.

- Now if user accesses any cluster 1, 2 or 3 s/he will be allowed.

Case 2: For first time user is accessing a door that belongs to cluster 2 at 2 o'clock.

- Now if user accesses cluster 2 s/he will be allowed.
- If user accesses cluster 3 s/he will be allowed as allowed cluster is cluster3.
- After accessing cluster 3, if user accesses cluster 1 or 2 before 1 hr, that is, at 3:00 on same day s/he will not be allowed.

Case 3: For first time user is accessing a door of cluster 3 at 2 o'clock.

- If user accesses cluster 3 s/he should be allowed. Note that the last accessed time should be updated even if door from same cluster is accessed, that is, after accessing door of cluster 3 any other door of cluster 3 is accessed.
- If user accesses cluster 1 or 2 before 1 hr, that is, before 3 o'clock s/he will not be allowed. But if user accesses cluster 2 at around 4:00 s/he will be allowed as restricted hour configured for cluster 3 to deny is 1 hr.

After you have created the Access Clusters, you must:

- select the Access Cluster check box to enable at the Panel level. For details, refer to "Set1" in "Access Features"
- assign these clusters to the desired doors. For details, refer to "Basic Configuration" in "Door Configuration".
- enabled the Access Cluster check box for the desired users. For details, refer to "Advanced Access Control 2" in "User Configuration".

# Occupancy Control

---

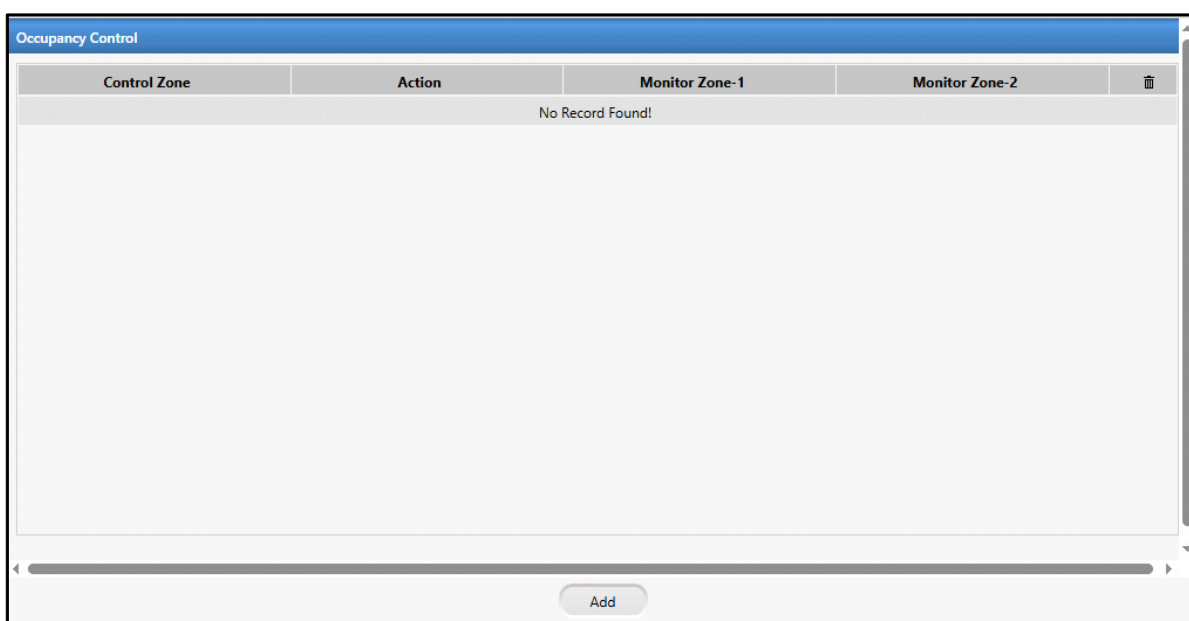
Occupancy Control enables the PANEL200 to monitor and control the number of users permitted within a secured area or controlled zone. This is useful for bank vaults, research organizations where enhanced security is required.

Occupancy Control can be used in two ways:

- can be applied on each zone separately
- occupancy of one zone (**Monitor zone**) can be monitored to control access into another zone (**Control zone**).

To configure the Occupancy Control,

Click **Access Policies > Occupancy Control**. The **Occupancy Control** page appears.



All the created Occupancy Control rules appear in the grid with their details — Control Zone, Action, Monitor Zone-1, Monitor Zone-2.

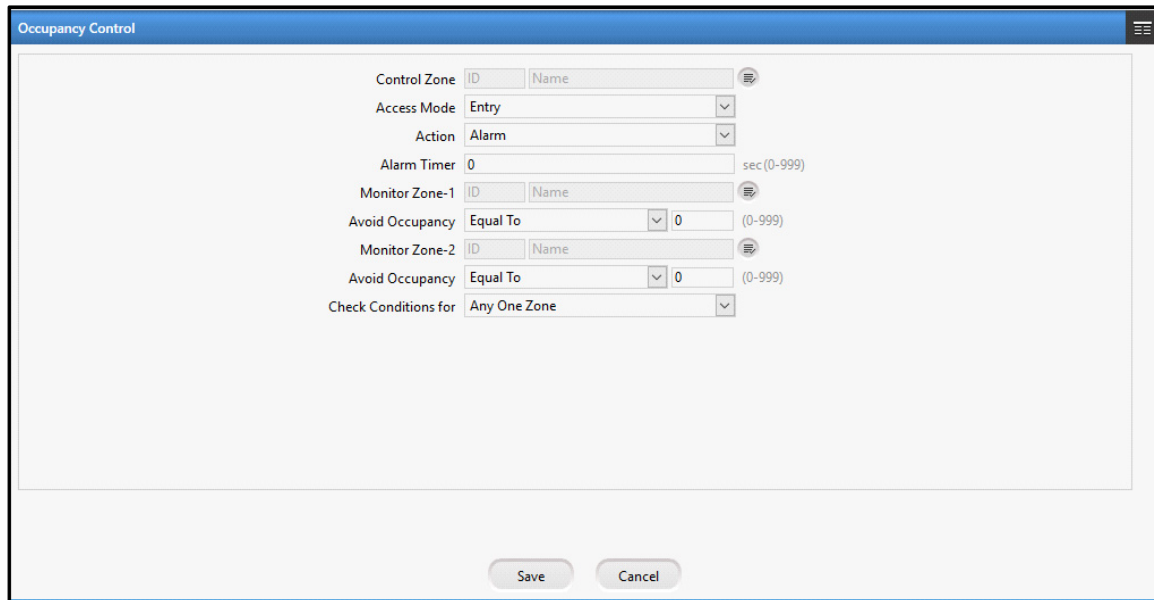
You can click the desired rule and edit it as per your requirement or you can add new rule.

You can also delete any rule. To do so, click **Delete**  corresponding to the desired rule.

## Adding Occupancy Control Rule

To add an Occupancy Control Rule,

Click **Add**. You can create maximum **99** Occupancy Control rules.



The 'Occupancy Control' window contains the following fields:

- Control Zone:** ID and Name picklists.
- Access Mode:** Entry (dropdown).
- Action:** Alarm (dropdown).
- Alarm Timer:** 0 (text) sec (0-999) (range).
- Monitor Zone-1:** ID and Name picklists.
- Avoid Occupancy:** Equal To (dropdown) 0 (text) (0-999) (range).
- Monitor Zone-2:** ID and Name picklists.
- Avoid Occupancy:** Equal To (dropdown) 0 (text) (0-999) (range).
- Check Conditions for:** Any One Zone (dropdown).

Buttons: Save, Cancel.

Configure the following parameters:

- **Control Zone:** Control Zone is the zone where the user access can be controlled based on the selected Action and the condition of the Monitor Zone.

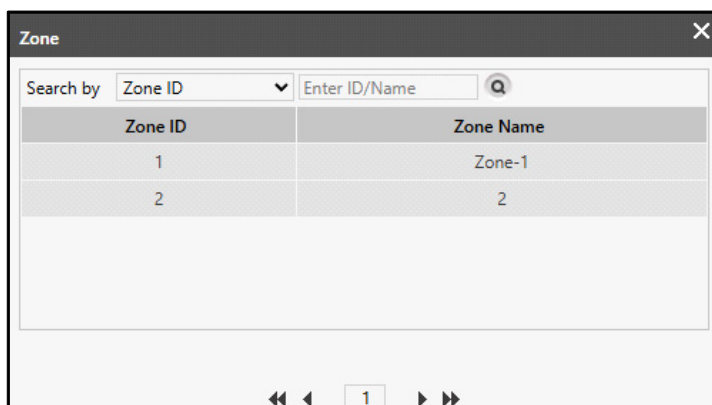
Click the **Control Zone** picklist. The **Zone** pop-up appears. Click to select the desired zone.

**OR**

If required, you can also search for the desired zone.

**Search By:** Select the desired option by which you wish to search for the user — Zone ID, Zone Name. In

the corresponding box enter the keyword. Click **Search** . The zones will be filtered as per the keyword. Click to select the desired zone.



The 'Zone' pop-up window shows a search interface with a table of zones.

| Zone ID | Zone Name |
|---------|-----------|
| 1       | Zone-1    |
| 2       | 2         |

Navigation: << < 1 > >>

The selected Zone's ID and Name appear.

- **Access Mode:** Select the desired option — Entry, Exit, Both — based on which Occupancy rule will be checked.
- **Action:** Select the desired action — Alarm, Restrict — from the drop-down list which is to be executed when there is a violation.

If you select **Restrict**, the user will not be allowed to enter or exit the zone on violation of the rule.

If you select **Alarm**, an alarm will be triggered on violation of the Occupancy Control rule after the expiry of the Alarm Timer. You must configure the **Alarm Timer**.

- **Alarm Timer:** Configure the duration in seconds. The door will declare a violation only after the expiry of this timer and then the user will be allowed to either enter or exit the zone.

**Monitor Zone-1:** Click the **Control Zone** picklist. The **Zone** pop-up appears. Click to select the desired zone.

**OR**

If required, you can also search for the desired zone.

**Search By:** Select the desired option by which you wish to search for the user — Zone ID, Zone Name. In the corresponding box enter the keyword. Click **Search** . The zones will be filtered as per the keyword. Click to select the desired zone.

The selected Zone's ID and Name appear.

- **Avoid Occupancy:** Select the desired user occupancy condition to be avoided for Monitor Zone-1 — **Equal To, Greater Than, Less Than** — and then configure the number of users in the corresponding box.

**Monitor Zone-2:** Click the **Control Zone** picklist. The **Zone** pop-up appears. Click to select the desired zone.

**OR**

If required, you can also search for the desired zone.

**Search By:** Select the desired option by which you wish to search for the user — Zone ID, Zone Name. In the corresponding box enter the keyword. Click **Search** . The zones will be filtered as per the keyword. Click to select the desired zone.

The selected Zone's ID and Name appear.

- **Avoid Occupancy:** Select the desired user occupancy condition to be avoided for Monitor Zone-2 — **Equal To, Greater Than, Less Than** — and then configure the number of users in the corresponding box.
- **Check Conditions For:** Select the desired option — Any One Zone, Both Zones. As per the selected option, the PANEL200 will check for the fulfillment of the Avoid Occupancy condition for the respective zone.



- Click **Save** to save the settings or click **Cancel** to discard.

After you have completed all the configuration of the Occupancy Control Rule, if you wish to view all the created Occupancy Control Rules, click View List .

The Occupancy Control page appears with all the created Occupancy Control Rules.

Let us understand this with the help of examples:

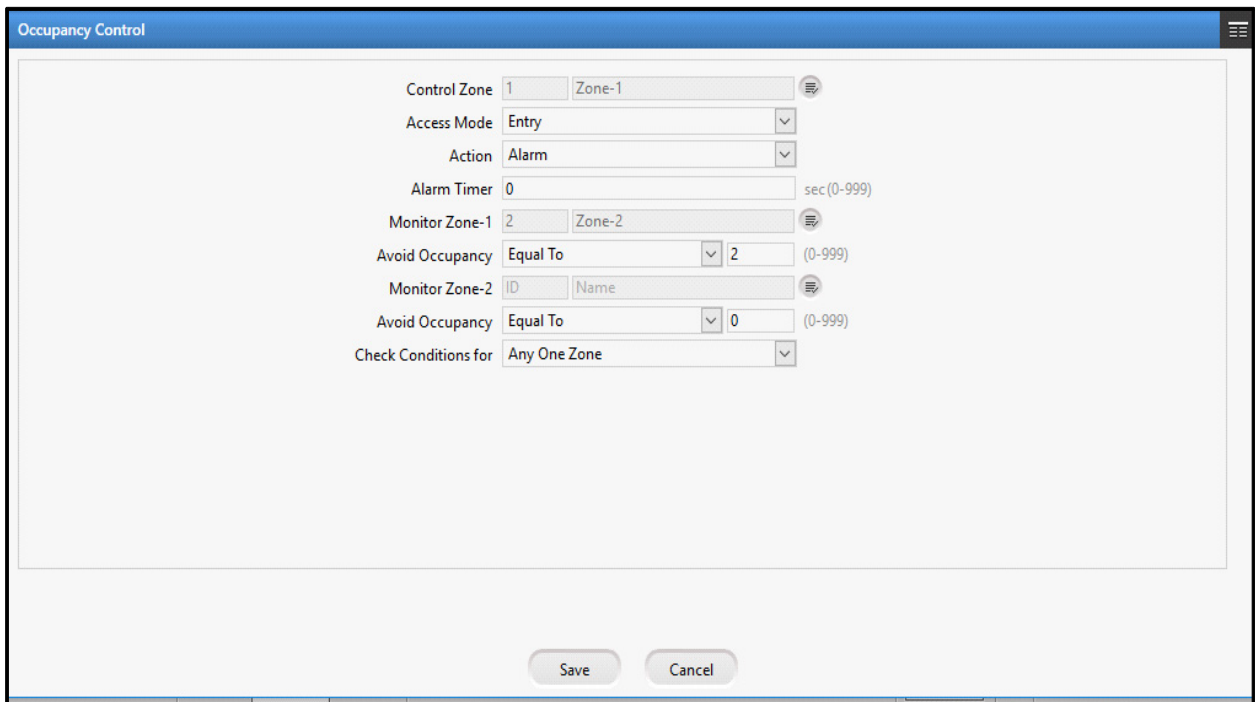
**Example 1:** Configuration are as follows:

There are two zones,

- Zone 1 - Control Zone - Door V3
- Zone 2 - Monitor Zone - PVR door

Initially occupancy of both the zones is empty.

- **Access Mode** of both zones is Entry.
- **Action** configured is Alarm and Alarm Timer is set as 0 seconds.
- **Avoid Occupancy** condition configured is equal to 2



When the second user enters in the Monitor Zone, s/he will be allowed access but occupancy condition is violated. Hence, the Occupancy Violated Alarm will be triggered when a user tries to access the Control Zone as well as the user will be allowed access.

**Example 2:** Configuration are as follows:

There are two zones,

- Zone 1 - Control Zone - Door V3

- Zone 2 - Monitor Zone - PVR door

Initially occupancy of both the zones is empty.

- **Access Mode** of both zones is Exit.
- **Action** configured is Restrict.
- **Avoid Occupancy** condition configured is greater than 1

When the second user enters in the Monitor Zone, s/he will be allowed access but occupancy condition is violated. Hence, when the user tries to access (exit) the Control Zone, access will be restricted due to violation of occupancy condition in the Monitor Zone.

**Example 3:** Configuration are as follows:

There are two zones,

- Zone 1 - Control Zone - Door V3
- Zone 2 - Monitor Zone - PVR door

Occupancy of both the zones is 4. User1 to User4 in Monitor Zone and User 5 to User 8 in Control Zone. User4 and User8 are VIP users.

**Access Mode** of both zones is Exit. Make sure **Access Control on Exit Mode** check box is selected for both the zones. For details, refer to ["Basic Configuration"](#) in ["Zone Configuration"](#).

**Action** configured is Restrict.

**Avoid Occupancy** condition configured is less than 3

Exit of User1 from Monitor Zone is allowed. Exit of User2 (normal user) or User4 (VIP user) from Monitor Zone will be allowed but it violates the occupancy condition.

Now when User5 tries to exit from the Control Zone then access will be denied to him/her. But at the same time if User8 (VIP user) tries to exit from the Control Zone then access will be allowed to him/her.

**Example 4:** Configuration are as follows:

There are two zones,

- Zone 1 - Control Zone - Door V3
- Zone 2 - Monitor Zone - PVR door

Initially occupancy of both the zones is empty.

**Access Mode** of both zones is Entry. (Configure Mode from Door Configuration > Reader. For details, refer to [“Door Configuration”](#))

**Access Mode** is selected as Entry for the Control Zone.

**Action** configured is Restrict. This will restrict the access of the user to the Control Zone if occupancy is violated in the Monitor Zone.

**Avoid Occupancy** condition configured is equal to 2 in Monitor Zone-1

- When User1 punches on PVR (Zone2), s/he is allowed access.
- When User2 punches on PVR (Zone2), s/he will also be allowed access.
- But when User3 punches on Door V3 in Control Zone (Zone1), s/he will be restricted access due to violation of occupancy = 2 in Monitor Zone (Zone2).



*If there are entry punches in a zone, the zone will be occupied. There must be exit punch from the reader or from door in Exit mode to decrease the occupancy from the zone.*

**Example 5:** The configurations are as follows:

- Consider the above Example 4 with change in Action as Alarm.
- **Action** configured is Alarm and Alarm Timer is set as 2 seconds. Alarm will be triggered after 2 seconds of user access in Control Zone when the occupancy is violated in the Monitor Zone.

When User1 and User2 punches on PVR door, they will be allowed access.

But when User3 punches on Door V3 then s/he will be allowed access, but after 2 seconds Alarm will be generated.

**Example 6:** The configurations are as follows:

There are 3 zones:

- Zone 1 - Control Zone - Door V3
- Zone 2 - Monitor Zone1 - PVR Door
- Zone-3 - Monitor Zone 2 - Door V3-115

Initially occupancy of all the zones is empty. Mode of all zones is Entry. (Configure Mode from Door Configuration > Reader. For details, refer to [“Door Configuration”](#))

**Access Mode** configured is Entry. This is the Access Mode of the Control Zone (Zone-1) for which the Action (Alarm/ Restrict) is to be taken.

**Action** configured is Alarm and the Alarm Timer is set as 2 seconds. This will trigger an Alarm after 2 seconds of user access in Control Zone when the occupancy is violated in the Monitor Zone.

**Avoid Occupancy** condition configured for Monitor Zone1 is equal to 2 and for Monitor Zone2 is greater than 1.

If **Check Conditions For** option is selected as:

- If **Any One Zone** is selected, then occupancy avoidance condition will be checked for any one zone. If occupancy is violated in either of the Monitor Zones then Alarm will be triggered after the duration of Alarm Timer when the user punches in Control Zone.
- If **Both Zones** is selected, then occupancy violation condition will be checked for both the zones and alarm will be triggered in Control Zone if occupancy is violated in both the Monitor Zones.

If Check Conditions For is configured as Any One Zone, then when User1 punches on Door V3-115 (Zone-3), s/he is allowed access. When User2 punches on Door V3-115 (Zone-3), s/he will be also be allowed access. But this is violating occupancy condition > 1

Now when User3 punches on Door V3 (Zone-1) then s/he will be allowed access but after 2 seconds Alarm will be triggered.

Similarly if Action is configured as Restrict; then User3 will be denied on Door V3.

If Check Conditions For is configured as Both Zones, then occupancy in PVR door will also be monitored.

# Access Rule

The Access Rule allows you to create conditional rules for a particular time duration to access the doors.

You can assign these rules to users as per your requirement.

The number of configured Access Rules are displayed under the Access Rules section on the Dashboard. For details, refer to [“Access Rules Dashboard”](#) in [“Dashboard”](#).

To configure the Access Rule,

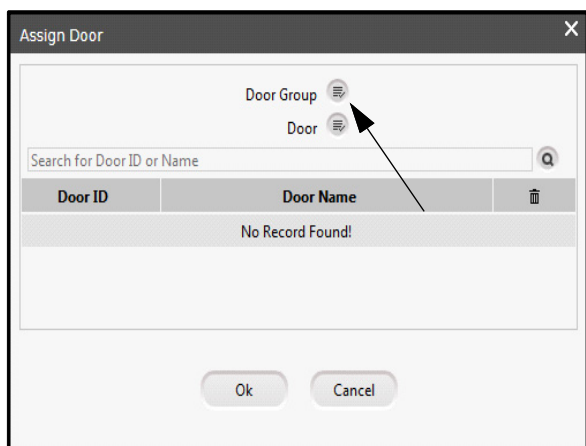
Click **Access Policies > Access Rule**. The **Access Rule** page appears.

The screenshot shows the 'Access Rule' configuration interface. It includes input fields for ID, Name, Active status, Start Time, End Time, and Active Days. There is also an 'Assign Door' button. Below these fields are two empty tables with headers 'ID' and 'Door Name' and 'ID' and 'Name'. At the bottom are 'Save' and 'Cancel' buttons.

To add a rule, click **Add**. You can create a maximum of **999** rules.

Configure the following parameters:

- **Group ID:** The ID is auto-generated by the PANEL200.
- **Group Name:** Configure a name you wish to assign to the rule.
- **Active:** Select the check box to enable the rule.
- **Start Time:** Configure the time in HH:MM format at which you wish to enable the rule.
- **End Time:** Configure the time in HH:MM format at which you wish to disable the rule.
- **Active Days:** Select the check boxes of the desired days on which you wish to apply the rule.
- **Assign Door:** Click the **Assign Door** picklist. The **Assign Door** pop-up appears. Click the **Door** or **Door Group** picklist and select the check boxes of the desired doors/door groups that you wish to assign to the user. The selected doors/doors of the selected door groups appear in the grid.



**OR**

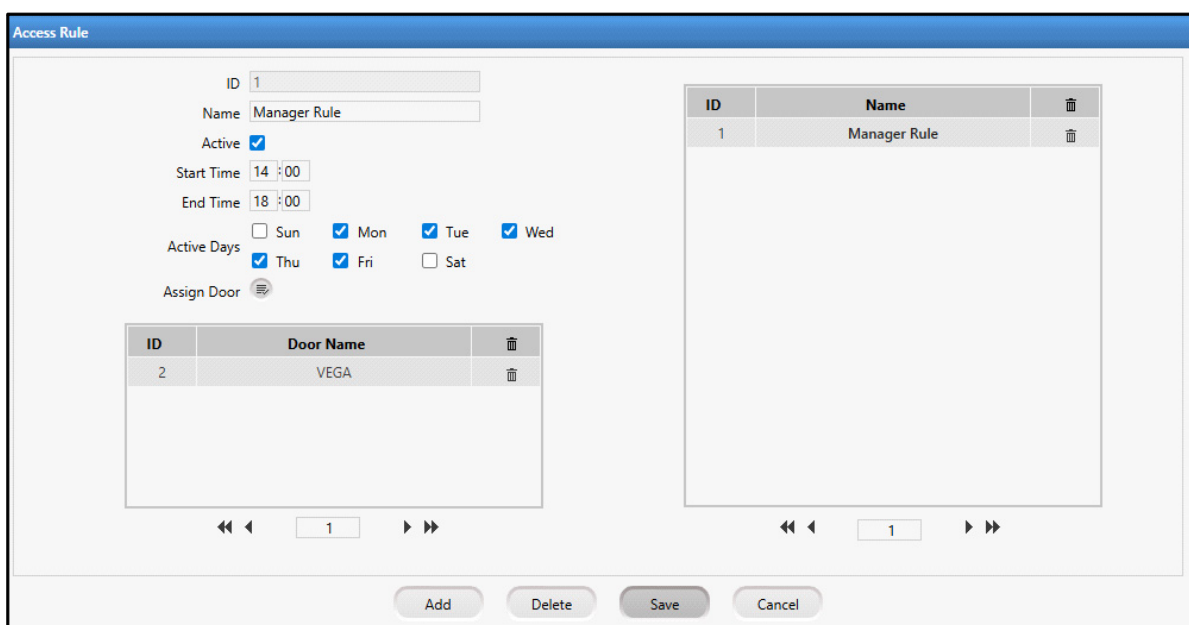
You can also search for the desired door/door group. To do so, enter the keyword in the Search box. Click

**Search** . The doors/door groups will be filtered as per the keyword. select the check boxes of the desired doors/door groups that you wish to assign to the user. The selected doors/doors of the selected door groups appear in the grid.

If you wish to remove the doors, click **Delete**  of the respective door.

Click **Ok** to assign the doors. The assigned doors will be displayed in the grid.

- Click **Save** to save the settings. The Access Rules appears in the right pane.



You can edit or delete any rule.

To edit, click the desired rule from the right pane and edit the parameters as per you requirement. Click **Save**.

To delete a rule, click **Delete**  corresponding to the desired rule.

---

Access Schedule allows you to:

- create Shifts and Schedules. For details, refer to [“Shifts and Schedules”](#).
- create Holiday Schedules. For details, refer to [“Holiday Schedule”](#).

To configure the Shifts and Schedules,

Click **Access Schedule > Shifts and Schedules**. The **Shifts and Schedules** page appears.



You can also delete any Shift. To do so, click **Delete**  corresponding to the desired Shift.

- configure the Shifts. For details, refer to “Shifts”.
- configure the Schedules. For details, refer to “Schedules”.

Click **Add**. You can create maximum **1402** Shifts.

To configure the Shift,

252 Matrix COSEC PANEL200 System Manual



Configure the following parameters:

- **Shift Code:** Configure a code which you wish to assign to the Shift.
- **Name:** Configure a name you wish to assign to the Shift.
- **Shift Type:** Select the desired Shift Type from the drop-down list options — Normal, Field Break, Rest Day.
  - **Normal:** This is a normal shift with usually one week off within a week.
  - **Field Break:** This is a shift where a long break is given after long continuous working hours. For example: a break of around 20 days is given after a working period of 2 months.
  - **Rest Day:** This is a like a normal shift with one week off given for rest after certain working hours, for example 10 to 12 working days.

If you have selected **Shift Type** as **Normal**, configure the following:

### Working Hour Details

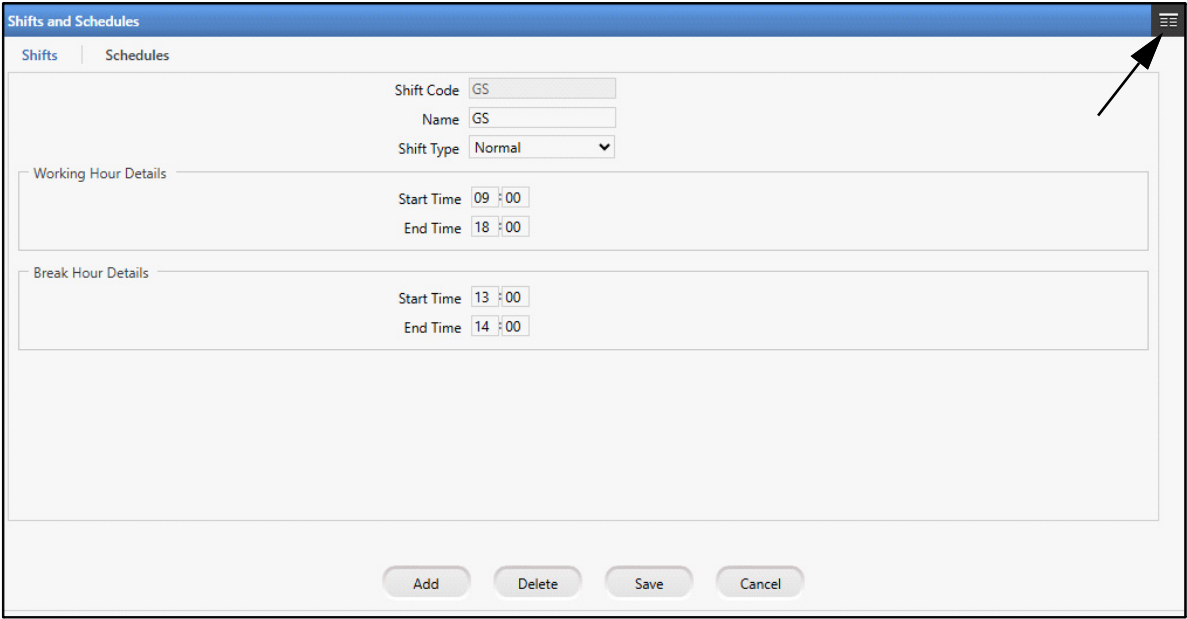
- **Start Time:** Configure the Start Time of the Working Hours in HH:MM format.
- **End Time:** Configure the End Time of the Working Hours in HH:MM format.

### Break Hour Details

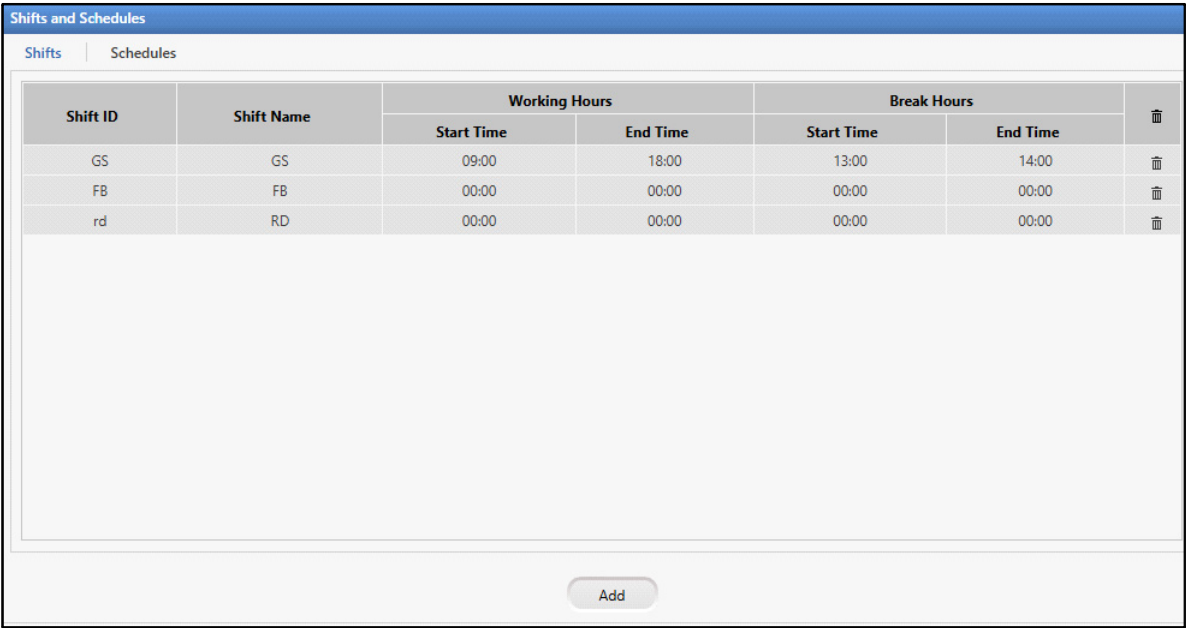
- **Start Time:** Configure the Start Time of the Break Hours in HH:MM format.
- **End Time:** Configure the End Time of the Break Hours in HH:MM format.

Click **Save** to save the settings. Similarly, you can add other Shifts. Now, you can add the Shifts to a Schedule.

After you have completed all the configurations of the Shift and if you wish to view all the created Shifts, click **View List** .



The Shifts page displays all the created Shifts.



| Shift ID | Shift Name | Working Hours |          | Break Hours |          |  |
|----------|------------|---------------|----------|-------------|----------|---------------------------------------------------------------------------------------|
|          |            | Start Time    | End Time | Start Time  | End Time |                                                                                       |
| GS       | GS         | 09:00         | 18:00    | 13:00       | 14:00    |  |
| FB       | FB         | 00:00         | 00:00    | 00:00       | 00:00    |  |
| rd       | RD         | 00:00         | 00:00    | 00:00       | 00:00    |  |

## Schedules

To configure the Schedules,

Click **Access Schedule > Shifts and Schedules > Schedules**. The **Schedules** page appears.

**Shifts and Schedules**

Shifts | Schedules

| Schedule ID | Schedule Name |  |
|-------------|---------------|--|
| 1           | Schedule1     |  |

1

Add

All the created Schedules appear in the grid with their details — Schedule ID and Schedule Name.

You can click the desired Schedule and edit it as per your requirement or you can add new Schedules.

You can also delete any Schedule. To do so, click **Delete** corresponding to the desired Schedule.

To add a Schedule,

Click **Add**. You can create maximum **999** schedules with **32** shifts in each.

**Shifts and Schedules**

Shifts | Schedules

Schedule ID: 2  
Name:   
Schedule Start Date: 01-01-2009

Off Day Configuration  
Off Day 1: Sunday  
Off Day 2: None  
Off Day2 On Weeks: ☐ W1 ☐ W2 ☐ W3 ☐ W4 ☐ W5 ☐ Last

Week Off Rotation  
Enable: ☐ Rotation Count: 7 (7-99)

Shift Based Access Rules  
Allow Multiple Shift: ☐ Deny On Field Break: ☒  
Deny On Week Off: ☒ Deny On Rest Day: ☒  
Deny On Holiday: ☒

| Enable                   | Shifts   | Configured Shifts | Repeat Days |
|--------------------------|----------|-------------------|-------------|
| <input type="checkbox"/> | Shift 1  |                   | 7           |
| <input type="checkbox"/> | Shift 2  |                   | 7           |
| <input type="checkbox"/> | Shift 3  |                   | 7           |
| <input type="checkbox"/> | Shift 4  |                   | 7           |
| <input type="checkbox"/> | Shift 5  |                   | 7           |
| <input type="checkbox"/> | Shift 6  |                   | 7           |
| <input type="checkbox"/> | Shift 7  |                   | 7           |
| <input type="checkbox"/> | Shift 8  |                   | 7           |
| <input type="checkbox"/> | Shift 9  |                   | 7           |
| <input type="checkbox"/> | Shift 10 |                   | 7           |
| <input type="checkbox"/> | Shift 11 |                   | 7           |
| <input type="checkbox"/> | Shift 12 |                   | 7           |
| <input type="checkbox"/> | Shift 13 |                   | 7           |
| <input type="checkbox"/> | Shift 14 |                   | 7           |

Save Cancel

Configure the following parameters:

- **Schedule ID:** The Schedule ID is auto-generated by the PANEL200.
- **Name:** Configure a name you wish to assign to the Schedule.

- **Schedule Start Date:** Select the desired date from which the schedule should start from the calendar.

## Off Day Configuration

- **Off Day 1:** Select the desired Day of the Week on which you wish to assign the Off Day 1 from the drop-down list.
- **Off Day 2:** Select the desired Day of the Week on which you wish to assign the Off Day 2 from the drop-down list. Select **None**, if you do not wish to assign Off Day 2.
- **Off Day2 On Weeks:** Select the check boxes of the desired Weeks of the Month in which you wish to assign the Off Day 2. The selected Day for Off Day 2 will be applicable for the selected Weeks of the Month.

For Example, you have done the following Off Day Configuration:

**Off Day 1:** Sunday

**Off Day 2:** Saturday

**Off Day2 On Weeks:** W2 and W4.

Then, Sunday will be considered as an Off Day for all the weeks, whereas Saturday will be considered as an Off Day for second and fourth week of the month only.

## Week Off Rotation

- **Enable:** Select the check box to enable Week Off Rotation.
- **Rotation Count:** Configure the number of days after which the selected Week Offs should be rotated. Minimum Rotation Count is 7.

For Example, you have done the following Off Day and Week Off Rotation configurations:

**Off Day 1:** Sunday

**Off Day 2:** None

**Week Off Rotation:** Enabled

**Rotation Count:** 15

Then, the Week Off, that is, Sunday will be rotated to Monday after a count of 15 days. Similarly, after another 15 days, the Week Off will rotate further to Tuesday and so on.

If both Off Day 1 and Off Day 2 are configured, they will rotate as explained above.

## Shift Based Access Rules

- **Allow Multiple Shift:** Select the check box if you wish to allow a user to work in multiple Shifts in the Schedule.
- **Deny on Field Break:** Select the check box if you wish to deny access to the user on Field Break day.
- **Deny on Week Off:** Select the check box if you wish to deny access to the user on Week Off day.
- **Deny on Rest Day:** Select the check box if you wish to deny access to the user on Rest Day.
- **Deny on Holiday:** Select the check box if you wish to deny access to the user on Holiday.

Once the Schedule configurations are done, you need to assign Shifts to the Schedule. In the right pane, configure the following:

- **Enable:** Select the check box to enable the Shift.
- **Configured Shifts:** Click the **Select Shifts** picklist. The **Shifts** pop-up appears. Select the desired Shift you wish to add to the Schedule.

**OR**

If required, you can also search for the desired shift.

**Search By:** Select the desired option by which you wish to search for the group — Shift Name, Shift ID. In the corresponding box enter the keyword. Click **Search** . The shifts will be filtered as per the keyword. Select the desired shift.

- **Repeat Days:** Configure the number of days for which the selected Shift should repeat.

Similarly, add other desired Shifts in the Schedule. Once all the Shifts are added, click **Save** to save the settings. Now you can assign the Shift Schedule to the desired user. For details, refer to [“Shift Based Access”](#) under [“User Configuration”](#).



*By default, the 1st Shift and Schedule will be assigned to all the users and will be displayed on User Configuration page.*

*You must enable it for the desired user from User Configuration> Advance Access Control > Shift Based Access.*

After you have completed all the configurations of the Schedule and if you wish to view all the created Schedules, click **View List** .

| Enable                   | Shifts   | Configured Shifts | Repeat Days |
|--------------------------|----------|-------------------|-------------|
| <input type="checkbox"/> | Shift 1  |                   | 7           |
| <input type="checkbox"/> | Shift 2  |                   | 7           |
| <input type="checkbox"/> | Shift 3  |                   | 7           |
| <input type="checkbox"/> | Shift 4  |                   | 7           |
| <input type="checkbox"/> | Shift 5  |                   | 7           |
| <input type="checkbox"/> | Shift 6  |                   | 7           |
| <input type="checkbox"/> | Shift 7  |                   | 7           |
| <input type="checkbox"/> | Shift 8  |                   | 7           |
| <input type="checkbox"/> | Shift 9  |                   | 7           |
| <input type="checkbox"/> | Shift 10 |                   | 7           |
| <input type="checkbox"/> | Shift 11 |                   | 7           |
| <input type="checkbox"/> | Shift 12 |                   | 7           |
| <input type="checkbox"/> | Shift 13 |                   | 7           |
| <input type="checkbox"/> | Shift 14 |                   | 7           |

The Schedules page displays all the created Schedules.

Shifts and Schedules

Shifts

Schedules

| Schedule ID | Schedule Name |  |
|-------------|---------------|--|
| 1           | Schedule1     |  |
| 2           | Schedule2     |  |

1

Add

# Holiday Schedule

To configure the Holiday Schedule,

Click **Access Schedule > Holiday Schedule**. The **Holiday Schedule** page appears.

Holiday Schedule

| Holiday Schedule No. | Name              |  |
|----------------------|-------------------|--|
| 1                    | Holiday Schedule1 |  |

Add

All the created Holiday Schedules appear in the grid with their details — Holiday Schedule No. and Name.

You can click the desired Holiday Schedule and edit it as per your requirement or you can add new schedules.

You can also delete any Holiday Schedule. To do so, click **Delete**  corresponding to the desired schedule.

To add a Holiday Schedule,

Click **Add**. You can create maximum 4 schedules with 32 holidays in each.

Holiday Schedule

Holiday Schedule No.2

Holiday Schedule NameHoliday Schedule2

Configured Holidays

Holiday No.

Holiday Name

From DateFrom Date

To DateTo Date

Update

| No. | Holiday Name | From Date | To Date |  |
|-----|--------------|-----------|---------|--|
| 1   |              |           |         |  |
| 2   |              |           |         |  |
| 3   |              |           |         |  |
| 4   |              |           |         |  |
| 5   |              |           |         |  |
| 6   |              |           |         |  |
| 7   |              |           |         |  |
| 8   |              |           |         |  |
| 9   |              |           |         |  |
| 10  |              |           |         |  |
| 11  |              |           |         |  |
| 12  |              |           |         |  |
| 13  |              |           |         |  |
| 14  |              |           |         |  |

123

Add

Delete

Save

Cancel

Configure the following parameters:

- **Holiday Schedule No.:** The Holiday Schedule No. is auto-generated by the PANEL200.
- **Holiday Schedule Name:** Configure a name you wish to assign to the Holiday Schedule.

## Configured Holidays

You can add maximum **32** Holidays to a schedule. Click the desired Holiday No. in the right pane and configure its parameters:

- **Holiday No.:** The selected Holiday No. is displayed.
- **Holiday Name:** Configure a name you wish to assign to the Holiday.
- **From Date:** Select the date from which the Holiday starts from the calendar.
- **To Date:** Select the date till which the Holiday lasts from the calendar.

Click **Update**. The configured Holiday is updated in the right pane. Similarly, you can add other desired Holidays to the schedule.

| No. | Holiday Name     | From Date  | To Date    |  |
|-----|------------------|------------|------------|--|
| 1   | Independence Day | 15-08-2025 | 15-08-2025 |  |
| 2   |                  |            |            |  |
| 3   |                  |            |            |  |
| 4   |                  |            |            |  |
| 5   |                  |            |            |  |
| 6   |                  |            |            |  |
| 7   |                  |            |            |  |
| 8   |                  |            |            |  |
| 9   |                  |            |            |  |
| 10  |                  |            |            |  |
| 11  |                  |            |            |  |
| 12  |                  |            |            |  |
| 13  |                  |            |            |  |
| 14  |                  |            |            |  |

You can delete any added Holiday. To do so, click **Delete** corresponding to the desired Holiday.

Once all the desired Holidays are added, click **Save** to save the settings. Now you can assign the Holiday Schedule to the desired user. For details, refer to [“Shift Based Access”](#) under [“User Configuration”](#).

After you have completed all the configurations of the Holiday Schedule, if you wish to view all the created Holiday Schedules, click **View List** .







---

Manage allows you to:

- configure System Maintenance settings. For details, refer to [“System Maintenance”](#).

## System Maintenance

The System Maintenance allows you to:

- configure the Firmware Upgrade settings. For details, refer to [“Firmware Upgrade”](#).
- configure the Backup and Restore. For details, refer to [“Backup and Restore”](#).
- configure the System settings. For details, refer to [“System”](#).

### COSEC-Server Mode

You can configure the following:

- configure the Firmware Upgrade settings. For details, refer to [“Firmware Upgrade”](#).
- configure the Backup and Restore. For details, refer to [“Backup and Restore”](#).
- configure the System settings. For details, refer to [“System”](#).

## Firmware Upgrade

To configure the Firmware Upgrade,

Click **Manage > System Maintenance > Firmware Upgrade**. The **Firmware Upgrade** page appears.

Configure the following parameters:

## Manual Firmware Upgrade

- **Upgrade For:** Select the door for which you wish to upgrade the firmware from the drop-down list.

The PANEL200's Firmware Version is compatible only with certain Firmware Version of the doors. The compatible Firmware Version of the door is displayed as you select the door from the drop-down list. To know the PANEL200's Firmware Version, refer to ["About Device"](#).

For example, the current Firmware Version of your PANEL200 is 20. The Firmware Version of Vega door supported by this version is 16. Now, if your Vega door has Firmware Version 15, you can upgrade the same manually.

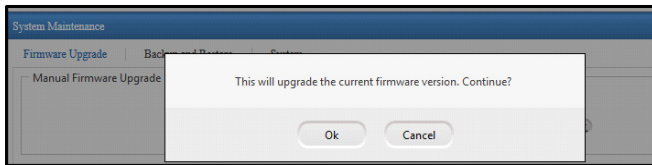
To upgrade the Firmware Version of PANEL200 or doors, you need to contact the Technical Support Team for the desired Firmware files.

If you need to upgrade the PANEL200's Firmware Version itself, you need to contact the Technical Support Team for the desired Firmware file for PANEL200. Since the PANEL200 is being upgraded, you can also ask for the compatible Firmware Version files of the desired doors as well.

- **Upgrade To:** Click **Browse File**  to browse the file and select the firmware. Click **Upgrade**  to upgrade the Firmware.

For example, the PANEL200's Firmware is to be upgraded.

The following pop-up appears.



Click **OK** to upgrade the firmware. The PANEL200 will be upgraded with the new Firmware and will reboot.

## Auto Firmware Upgrade

Auto Upgrade feature allows you to upgrade the Firmware of doors located at different places as well as the PANEL200 automatically through FTP Server. If there are any mismatches in the present Firmware Version of a door/PANEL200 and the Firmware Version present on the FTP, the door/PANEL200 can be upgraded with the latest Firmware by logging through the FTP Server.

If Auto Upgrade is enabled, PANEL200 will check the latest version of Firmware (of PANEL200 as well as doors) available on FTP at 00:00 AM every day. It will check whether there is mismatch in the current version stored in PANEL200/door and available firmware on the FTP Server.

Configure the following:

- **Interface Selection:** Select the Interface as Auto or Manual.
- **Network Interface:** If you have selected **Interface Selection** as **Manual**, select the desired Network Interface for the network connectivity from the drop-down list. PANEL200 will communicate with configured FTP Server through selected interface only.
- If you have selected **Interface Selection** as **Auto**, PANEL200 will communicate will configured FTP Server with available interface with predefined priorities.
- **FTP Server URL:** Configure the URL as the combined path with FTP Server Address and Port from where you wish to upgrade the Firmware. For example, URL: ftp://192.168.107.15.
- **User Name:** Configure the User Name required to access the FTP Server.

- **Password:** Configure the Password required to access the FTP Server.
- **Auto Upgrade:** Select the check box to automatically upgrade the Firmware of PANEL200.

Click **Save**  to save the settings. Now, click **Check Version** . The following details are displayed.

- **Last Upgrade on:** It will display the last Date and Time when the PANEL200's Firmware was updated.
- **Status:** It displays the connectivity status of PANEL200 with FTP Server.
- **Current Version in Panel:** It will display the current Firmware Version of PANEL200.
- **Latest Version on FTP:** It will display the latest Firmware Version available on the FTP Server.

Once you have saved the settings, the PANEL200's Firmware Version will upgrade automatically at 00:00:AM. You can also upgrade the Firmware immediately or set the configurations to default.

Click **Force Upgrade**  to upgrade the PANEL200's Firmware immediately. Using **Force Upgrade** you can upgrade the firmware of the PANEL200 as well as door with the firmware available on the FTP Server.

Click **Default**  to set the Auto Firmware settings to default.

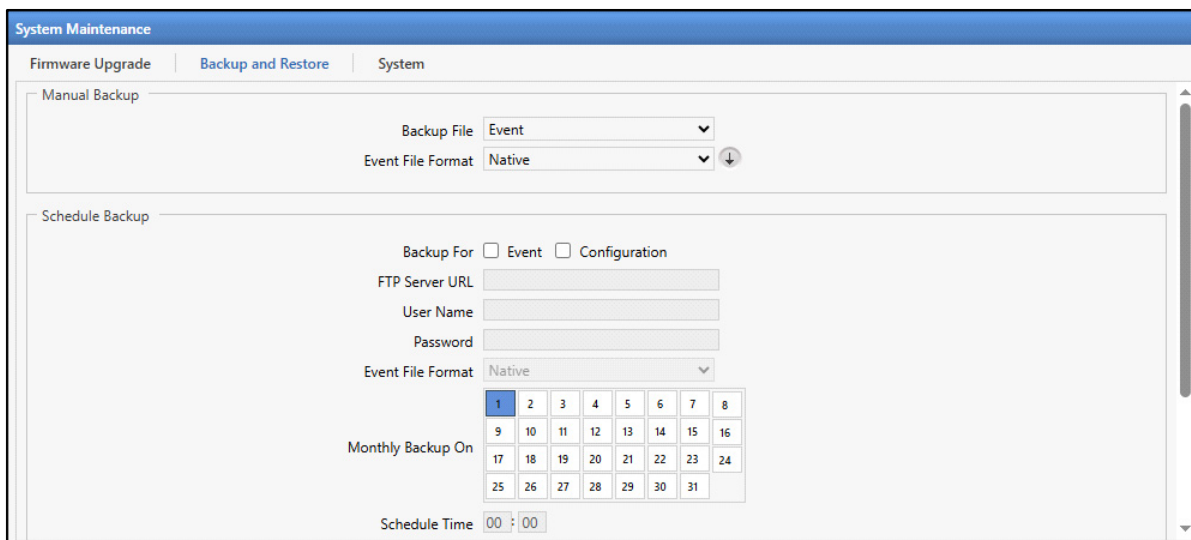
## Backup and Restore



*Make sure the SD Card is inserted in PANEL200 for performing Backup.*

To configure Backup and Restore,

Click **Manage > System Maintenance > Backup and Restore**. The **Backup and Restore** page appears.



**System Maintenance**

Firmware Upgrade | **Backup and Restore** | System

Manual Backup

Backup File: Event

Event File Format: Native

Schedule Backup

Backup For: ☐ Event ☐ Configuration

FTP Server URL:

User Name:

Password:

Event File Format: Native

Monthly Backup On:

|    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|
| 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  |
| 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |    |

Schedule Time: 00 : 00

Configure the following parameters:

## Manual Backup

- **Backup File:** Select the desired option for which you wish to take backup from the drop-down list options — Event, Configuration.



*The Configuration backup includes configuration of PANEL200, Finger Templates and Palm Templates. However, Face Templates will not be included in the Backup file.*

- **Event File Format:** If you have selected **Backup File** as **Event**, select the desired format in which you wish to download the backup file from the drop-down list — Native, xls, csv.

If you select **Backup File** as **Configuration**, by default, the file format will be displayed as **Native**.

Click **Backup**  to download the backup file. The file will be stored in the Downloads folder of your PC.

## Schedule Backup

Configure the following parameters:

- **Backup For:** Select the check box for which you wish to schedule the backup.
- **FTP Server URL:** Configure the URL of the FTP Server where you wish to store the backup files.
- **User Name:** Configure the User Name required to access the FTP Server.
- **Password:** Configure the Password required to access the FTP Server.
- **Event File Format:** If you have selected the **Backup For** as **Event**, select the desired format in which you wish to download the backup file from the drop-down list — Native, xls, csv.
- **Monthly Backup On:** Select the desired dates of the month on which you wish to schedule the backup.
- **Schedule Time:** Configure the time in HH:MM format when you wish to schedule the backup.

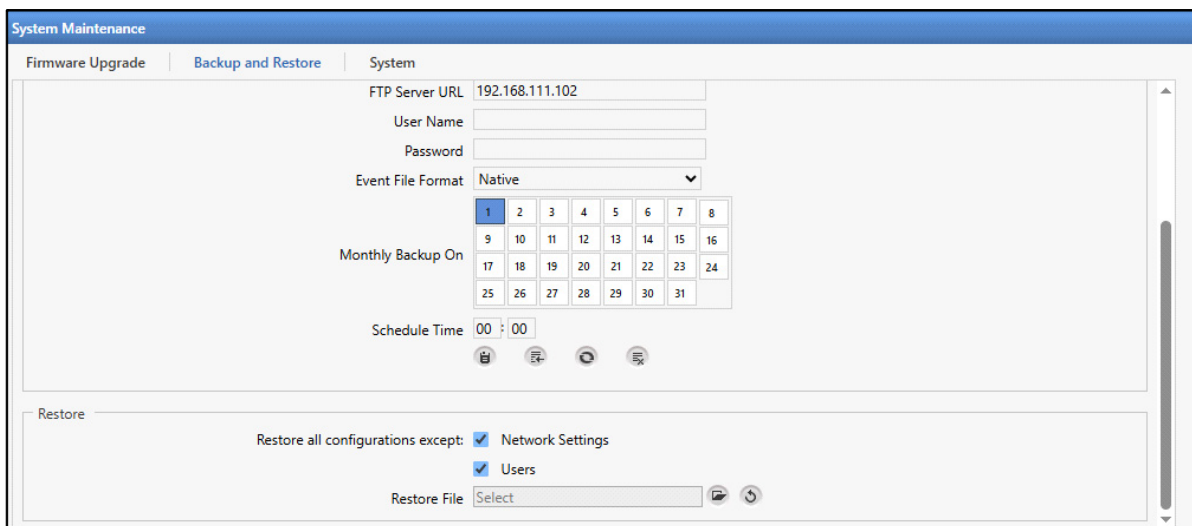
Click **Save**  to save the settings or click **Cancel**  to discard. Now, click **Test Connection**  to test the connection of PANEL200 with the configured FTP Server.

To set the configuration to default, click **Default**  .



*If the size of the Configuration backup file is greater than 250 MB, then the backup process might fail.*

## Restore



System Maintenance

Backup and Restore

FTP Server URL: 192.168.111.102

User Name:

Password:

Event File Format: Native

Monthly Backup On: 

|    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|
| 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  |
| 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |    |

Schedule Time: 00:00

Restore

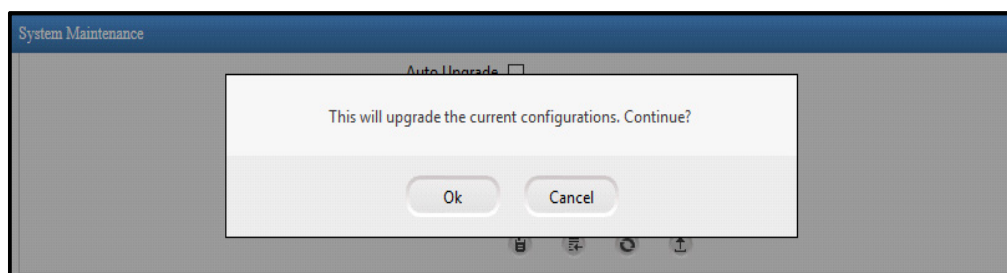
Restore all configurations except: ☒ Network Settings ☒ Users

Restore File: Select

Configure the following parameters:

- **Restore All configurations except:** Select the check boxes — Network Settings, Users — if you do not wish to restore the configurations for the same.
- **Restore File:** Click **Browse File**  and select the desired Configuration file. You can restore configurations by selecting a Native file only.

Click **Restore**  .The following pop-up appears.



Click **Ok**. The PANEL200 will reboot and the configuration will be restored.





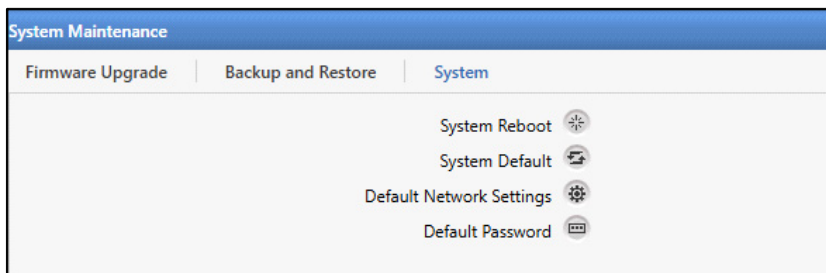
If the size of the Configuration backup file is greater than 250 MB, then the restore process might fail.

If backup of PANEL200 that supports Face Recognition feature is restored in older versions (PANEL200 that does not support this feature), the configuration will not be restored. However, if backup of older versions is restored in PANEL200 that supports Face Recognition feature, all the configuration will be restored and all new parameters will be set to the default values.

## System

To configure System settings,

Click **Manage > System Maintenance > System**. The **System** page appears.



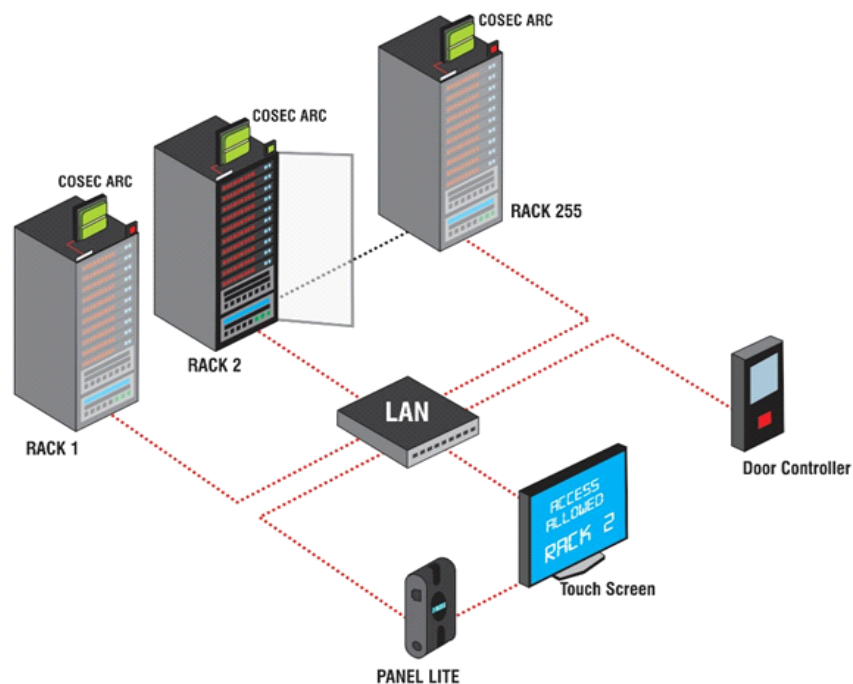
Configure the following parameters:

- **System Reboot:** Click to reboot the PANEL200.
- **System Default:** Click to set the PANEL200 settings to default.
- **Default Network Settings:** Click to set the Network Settings to default.
- **Default Password:** Click to set the Password to default.



Multi-Level Access enables the user to access multiple doors using single biometric/face/card credentials. Users can access only those doors which are assigned to their Access Routes. Thus, using Multi-Level Access, users can be granted access to specific doors using their enrolled credentials and unauthorized users can be denied access easily.

The Multi-Level Access page enables you to configure Multi-Level Access and club doors within groups denoted as Racks. Once Multi-Level Access configurations are done, you can access MLAT Access Control and MLAT Monitor. For details, refer to, [“Accessing MLAT Access Control and MLAT Monitor”](#).



The Multi-Level Access allows you to:

- configure the Multi-Level Access settings. For details, refer to [“Configuration”](#).
- configure the Assignment settings. For details, refer to [“Assignment”](#).

## COSEC-Server Mode

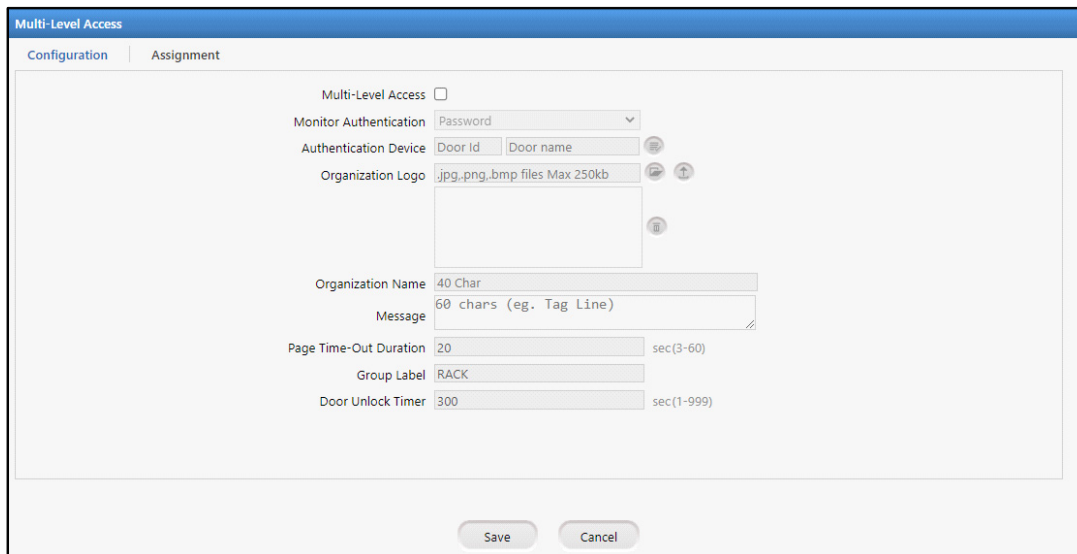
You can configure the following:

- configure the Multi-Level Access settings. For details, refer to “[Configuration](#)”.
- configure the Assignment settings. For details, refer to “[Assignment](#)”.

## Configuration

To configure Multi-Level Access settings,

Click **Multi-Level Access > Multi-Level Access > Configuration**. The **Configuration** page appears.



Configure the following parameters:

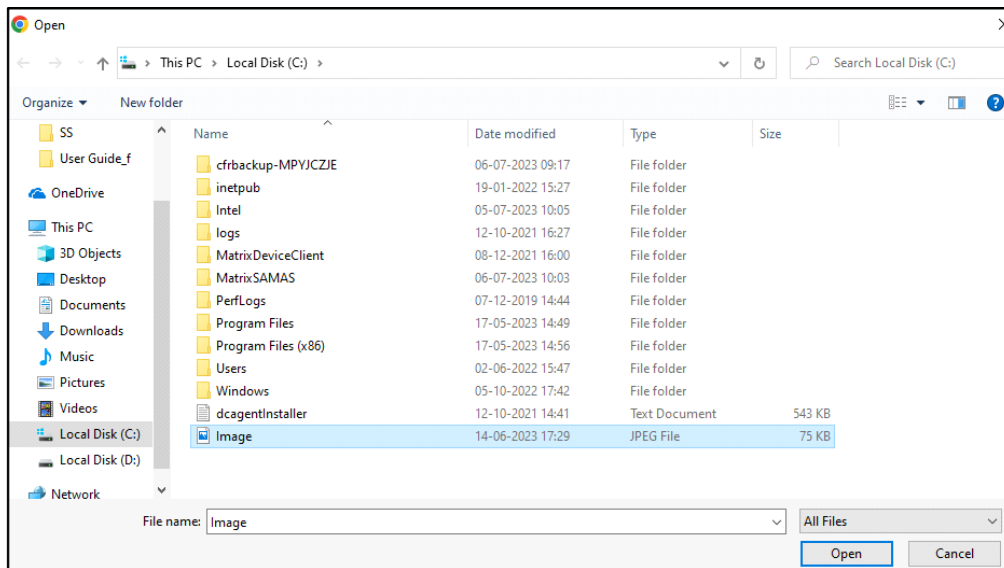
- **Multi-Level Access:** Select the check box to enable the Multi-Level Access configuration.
- **Monitor Authentication:** Select the desired option for authenticating users for accessing MLAT Monitor from the drop-down list — **User Credential** or **Password**.
  - **User Credential:** Select this option to grant MLAT Monitor access using credentials. The users need to show their credential on configured authenticating door to login.
  - **Password:** Select this option to grant MLAT Monitor access using password. The users need to enter their username and password on the authorization page of MLAT Monitor to login.
- **Authentication Device:** Click the **Select Door** picklist. The **Door** pop-up appears. Select the desired door through which you wish the user authentication must be done.

**OR**

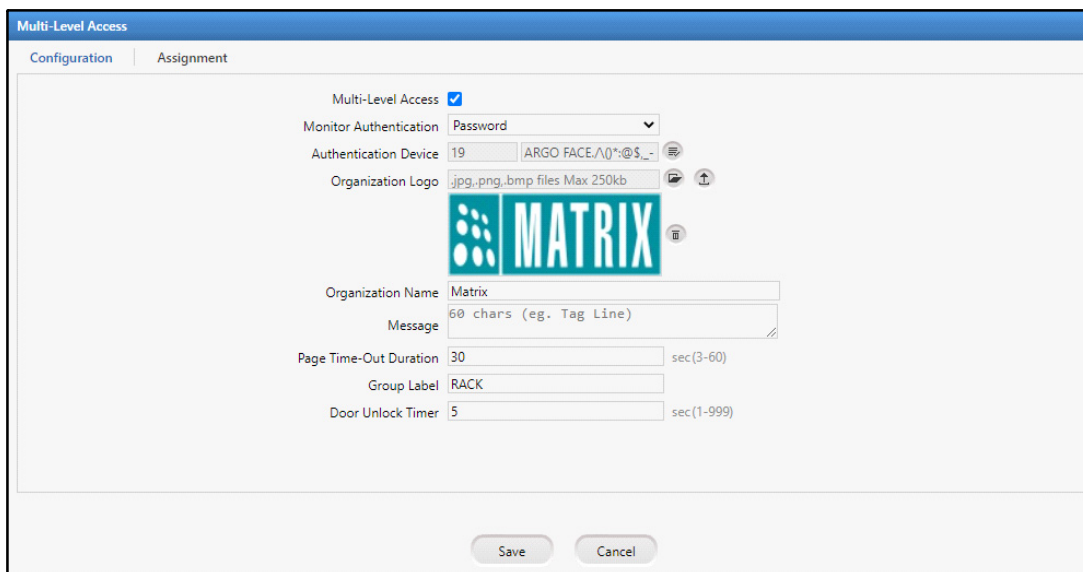
You can also search for the desired door. To do so, enter the keyword in the Search box. Click **Search**

 . The doors will be filtered as per the keyword. Select the desired door through which you wish the user authentication must be done.

- **Organization Logo:** Upload the desired Logo which you wish to display on the MLAT Access Control and MLAT Monitor page. The maximum file size is 250 KB.
- Click **Browse**  . The **Open** pop-up appears.



- Select the desired image to upload as the Logo and click **Open**.
- Click **Upload**  to upload the image.



- The image preview appears in the box once the image is uploaded.

If you wish to delete the image, click **Delete** .

- **Organization Name:** Configure the name of the organization.
- **Message:** Configure the desired message.

- **Page Time-Out Duration:** Configure the time in seconds after which the MLAT Access Control page will close if idle.
- **Group Label:** Configure the desired name for the group of doors.
- **Door Unlock Timer:** Configure the time in seconds after which the door gets locked automatically.

Click **Save** to save the settings or click **Cancel** to discard.

## Assignment

Once the Multi-Level Access configuration is done, you can assign racks to the doors to sort them in a logical manner. For example, all the doors on first floor can be assigned Rack 1 and so on.

To assign racks,

Click **Multi-Level Access > Multi-Level Access > Assignment**. The **Assignment** page appears.

| Door ID | Door Name                     | RACK Assignment (1 to 255) |
|---------|-------------------------------|----------------------------|
| 1       | ARGO./\Q*!~+:@\$ API - 199    | 0                          |
| 2       | ARGOFACE ./\@~*+()-108        | 0                          |
| 3       | VEGA !@\$*0_-+V.; API - 194   | 0                          |
| 4       | ARC !@\$*0_-+V.; SDDR 249     | 0                          |
| 5       | Door !@\$*0_-+V.; V4 - 190    | 0                          |
| 6       | Door !@\$*0_-+V.; PVR - 192   | 0                          |
| 7       | ARC !@\$*0_-+V.; DDDR 180 - 1 | 0                          |
| 8       | ARC !@\$*0_-+V.; DDDR 180 - 2 | 0                          |
| 9       | ARC DDDR 181 - 1              | 0                          |
| 10      | ARC DDDR 181 - 2              | 0                          |

- All the doors appear in a list. Configure the desired rack number in RACK Assignment against each door. The maximum Rack Assignments supported are 255.

Multi-Level Access

Configuration | Assignment

Search for Door ID or Name

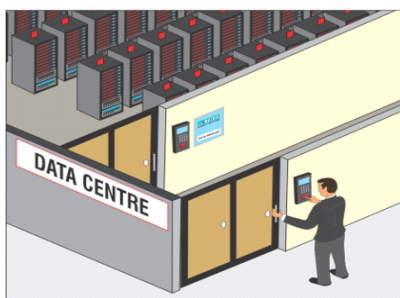
| Door ID | Door Name                     | RACK Assignment (1 to 255) |
|---------|-------------------------------|----------------------------|
| 1       | ARGO./\0"!_-+:@\$ API - 199   | 1                          |
| 2       | ARGOFACE ./\@_*+()-108        | 1                          |
| 3       | VEGA !@\$*()_-+V.; API - 194  | 1                          |
| 4       | ARC !@\$*()_-+V.; SDDR 249    | 2                          |
| 5       | Door !@\$*()_-+V.; V4 - 190   | 2                          |
| 6       | Door !@\$*()_-+V.; PVR - 192  | 2                          |
| 7       | ARC !@\$*()_-+V.;DDDR 180 - 1 | 3                          |
| 8       | ARC !@\$*()_-+V.;DDDR 180 - 2 | 3                          |
| 9       | ARC DDSR 181 - 1              | 3                          |
| 10      | ARC DDSR 181 - 2              | 4                          |

1 2

Save Cancel

Click **Save** to save the settings or click **Cancel** to discard.

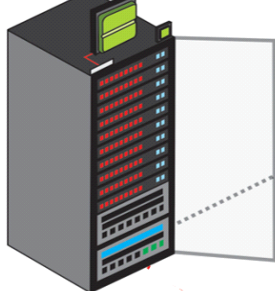
Data Centre Authentication



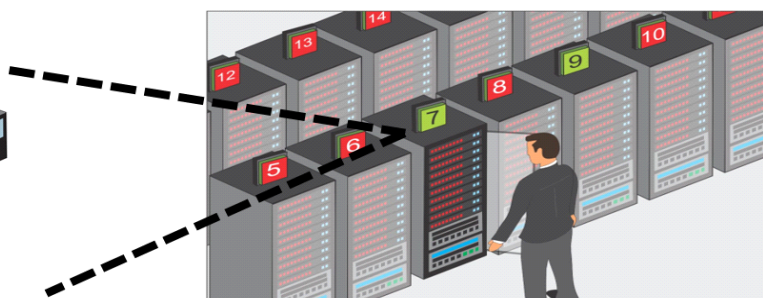
Data Centre Access Allowed



COSEC ARC



Rack Access Allowed



## Accessing MLAT Access Control and MLAT Monitor

Once you have configured Multi-Level Access, you can access MLAT Access Control and MLAT Monitor.

### MLAT Access Control

To access MLAT Access Control, enter PANEL200 IP/mlat.html, for example 192.168.103.26/mlat.html in your web browser. You can lock or unlock doors from this page.

## MLAT Monitor

To access MLAT Monitor, enter PANEL200 IP/mlatmonitor.html, for example 192.168.103.26/mlatmonitor.html in your web browser. You can monitor the status of all the doors from this page.

## Pre-requisites to access MLAT Access Control and MLAT Monitor

To access MLAT Access Control and MLAT Monitor, you need to:

- Assign the desired users to the configured Authentication Device and assign the necessary rights to the desired users. Refer to [“Profile”](#) and [“Access Rights”](#) respectively. Make sure the user credentials enrolled are as per the option selected in **Internal or Reader Group 1 Mode** under Access Mode. For details, refer to [“User”](#). You can also enroll the user credentials from the door. If you wish to do so, refer to [“Enrollment”](#).
- Create an Access Zone and set the Access Mode for **Internal or Reader Group 1 Mode**, refer to [“Basic Configuration”](#). The set credentials will be used by the authenticating door to allow access on both— MLAT Control and MLAT Monitor (if **Monitor Authentication** is configured as User Credential). Thus, make sure the set credentials are enrolled for the desired users on the authenticating door.
- Make sure you assign the same Access Zone to the users and the authenticating door. Refer to [“Profile”](#) and [“Basic Configuration”](#) respectively.
- Create and assign the desired Access Routes to the users. Refer to [“Access Route”](#) for creating access routes and refer to [“Basic Access Control”](#) to assign the access routes to the users.



*If the Access Policies are assigned to the users, then the same will be applicable while accessing MLAT Access Control and MLAT Monitor. For details, refer to [“Access Policies”](#).*

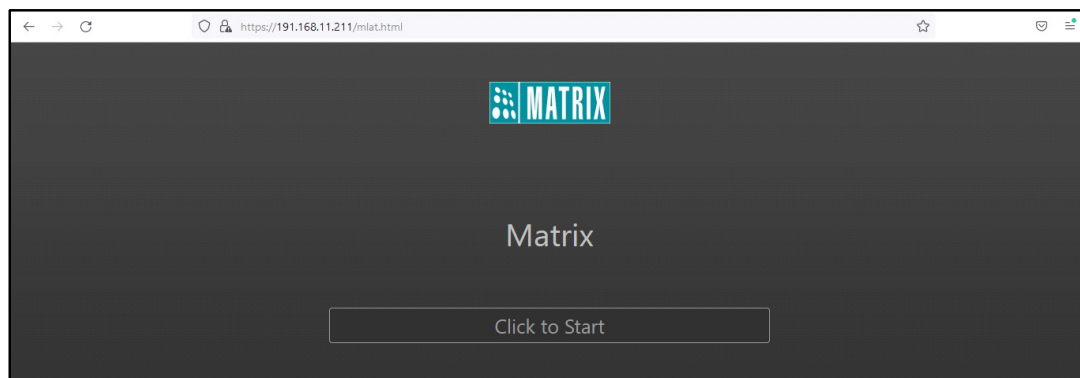
*If the Access Policies are applied on the assigned Zone, then the same will be applicable while accessing MLAT Access Control and MLAT Monitor. For details, refer to [“Zone Configuration”](#).*

*Make sure the PC from which you wish to access the MLAT Access Control/Monitor is close to the authenticating door.*

## Accessing MLAT Access Control

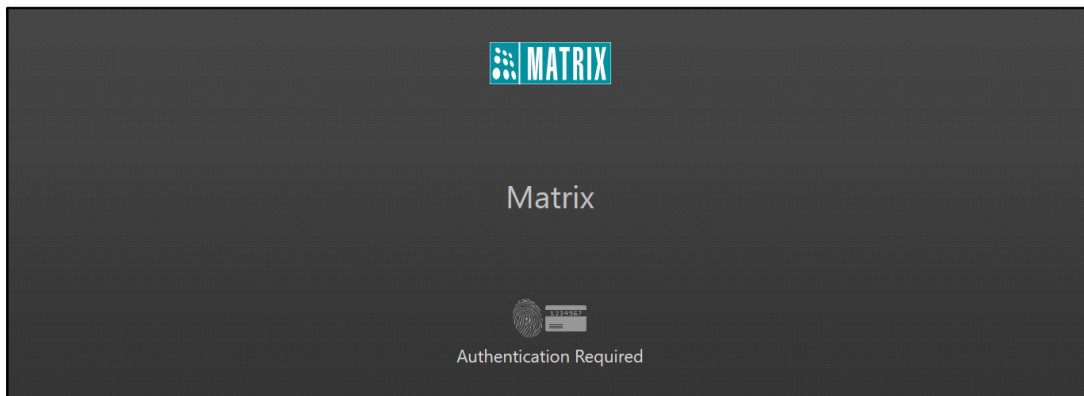
To access MLAT Access Control,

- Enter the PANEL200 IP/mlat.html, for example 192.168.103.26/mlat.html in your web browser. The MLAT Access Control page appears.



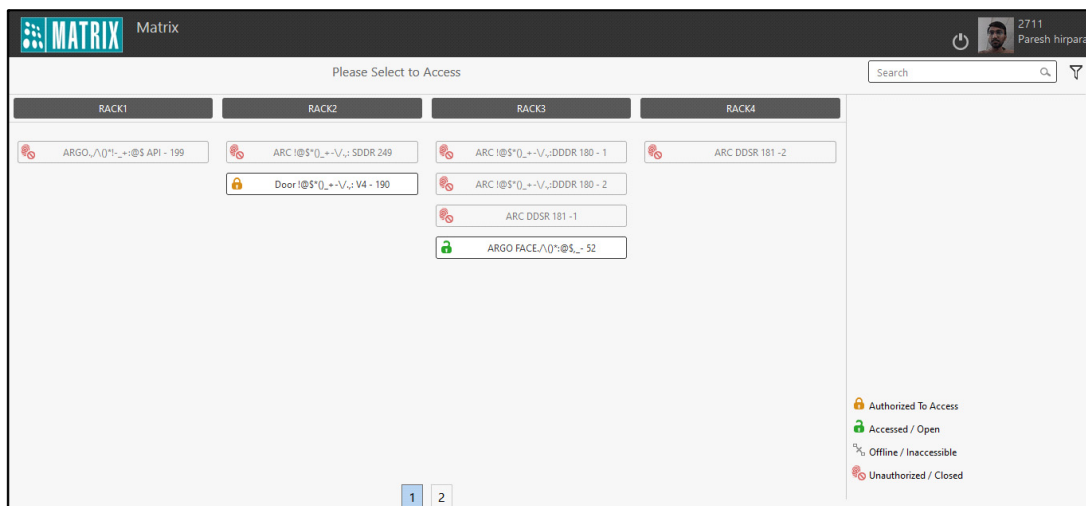


- Click on **Click to Start**. Now you need to show/enter your credentials on the configured authenticating door to login.



*The authenticating door's display screen is not accessible while accessing the MLAT Access Control page.*

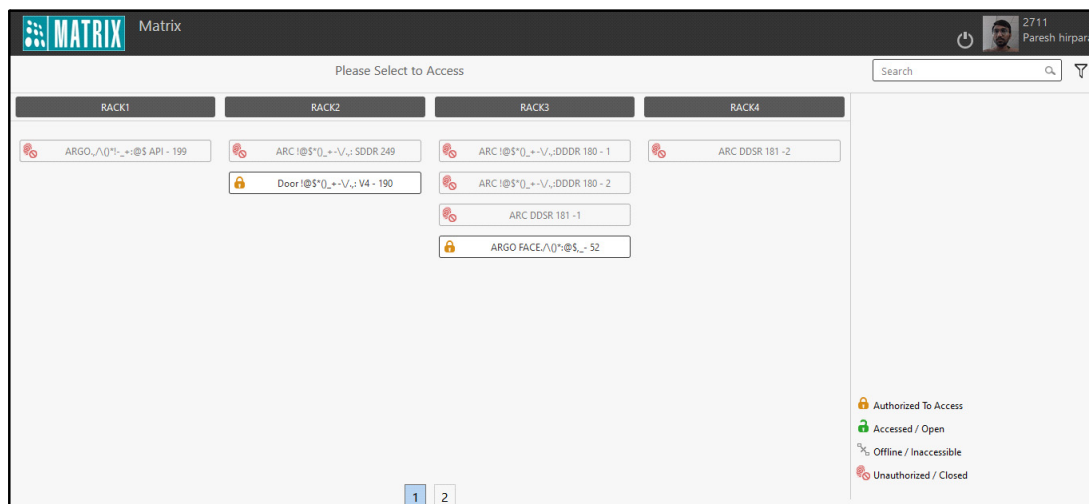
- All the doors assigned to various racks appear here along with their status. All the doors that are not assigned to your Access Route appear disabled.



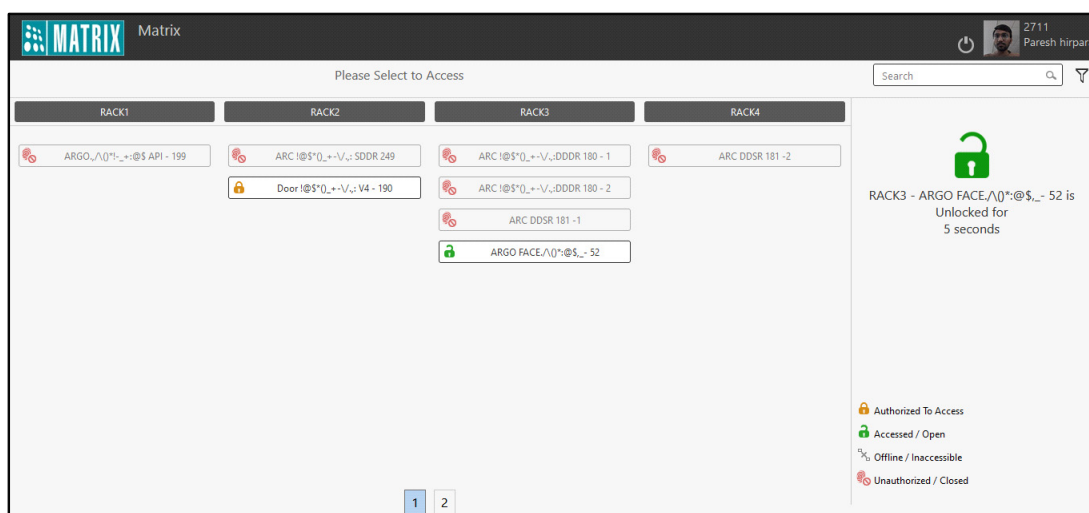
The icons for different door status are described on the bottom-right side of the page.

You can lock or unlock a door from this page. To do so,

- Click on the desired door to unlock it.



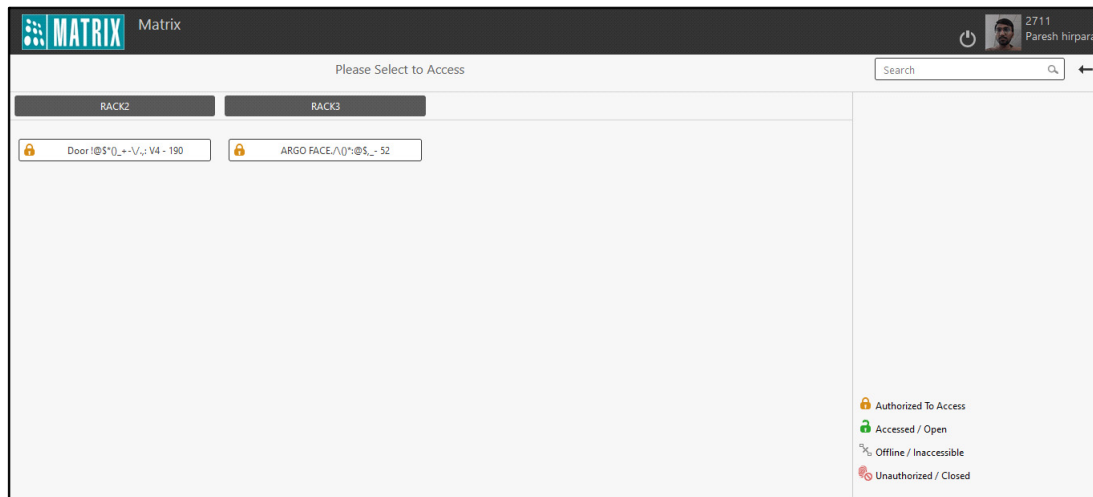
- The door status changes to **Open**. The details of this door appear on the right hand side of the page.



- The door remains unlocked for the time as configured in **Door Unlock Timer**. Once the timer expires, the door status changes to **Closed**.
- Similarly, you can lock a door as explained above.

You can access the following options — Search and Filter.

- Search:** You can search for the desired door using this option.
- Filter:** Click **Filter**  to view the doors assigned to your Access Route.

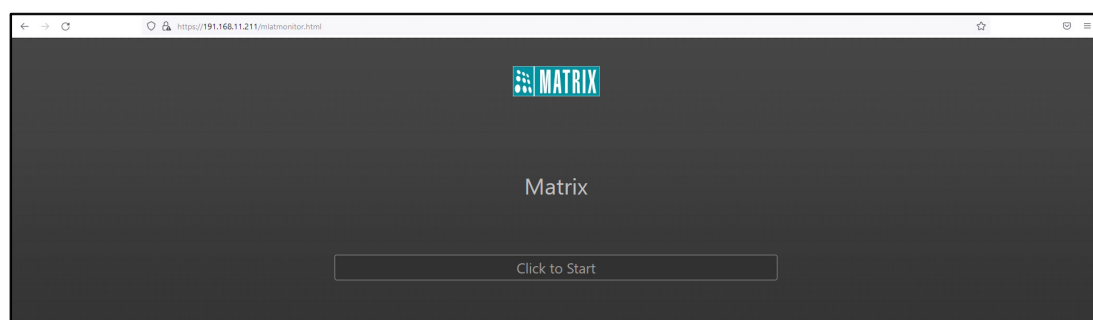


- Click **Filter**  again to view all the doors.

## Accessing MLAT Monitor

To access MLAT Monitor,

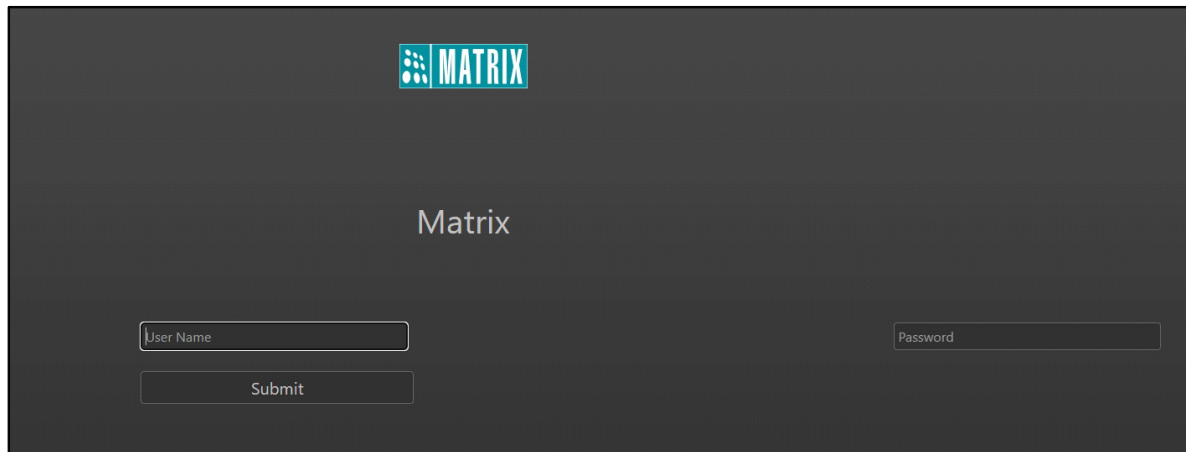
- Enter PANEL200 IP/mlatmonitor.html, for example 192.168.103.26/mlatmonitor.html in your web browser. The MLAT Monitor page appears.



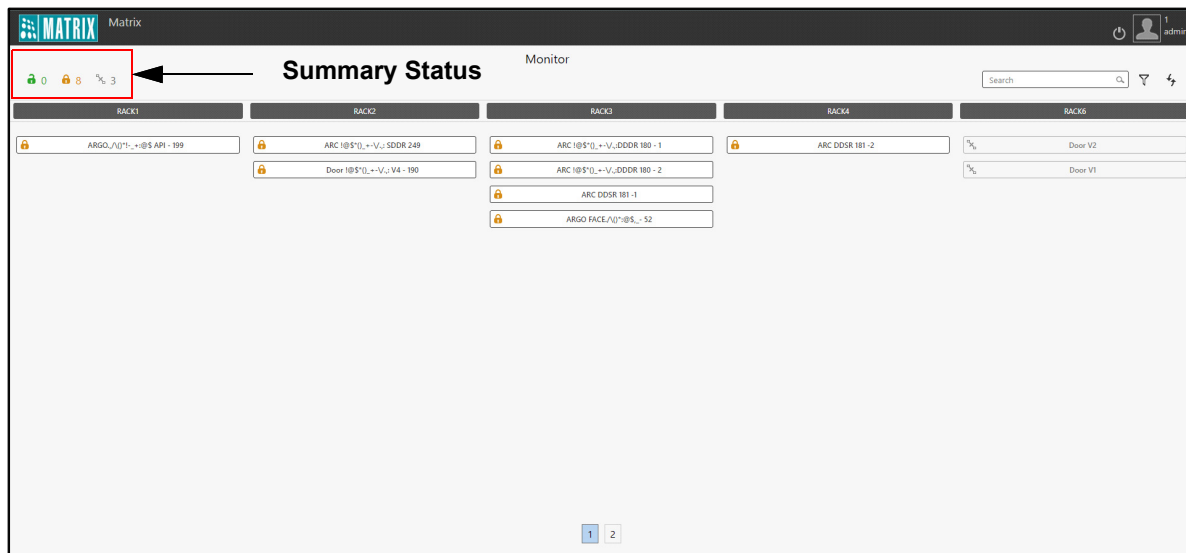
- Click on **Click to Start**.

If the **Monitor Authentication** is configured as **User Credential**, show/enter the credentials on the configured authenticating door to login.

If the **Monitor Authentication** is configured as **Password**, enter the username and password used to access the PANEL200 webpage. Click **Submit**.



- All the doors assigned to various racks appear here along with their status. The Summary Status of all the doors appears on the top-left corner of the page.

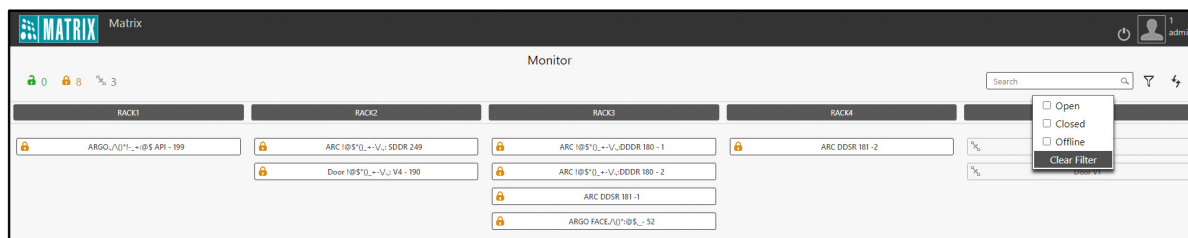


The following icons appear for different door status.

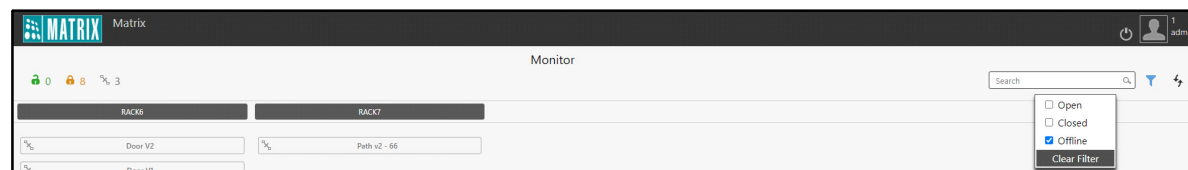
- **Open:**
- **Closed:**
- **Offline:**

You can access the following options — Search, Filter Status and Refresh.

- **Search:** You can search for the desired door using this option.
- **Filter Status:** Click **Filter Status** . The following pop-up appears.



- Select the check boxes for the Status Type— Open, Closed and Offline as per which you wish to filter the doors. Click **Clear Filter** to clear the filter.



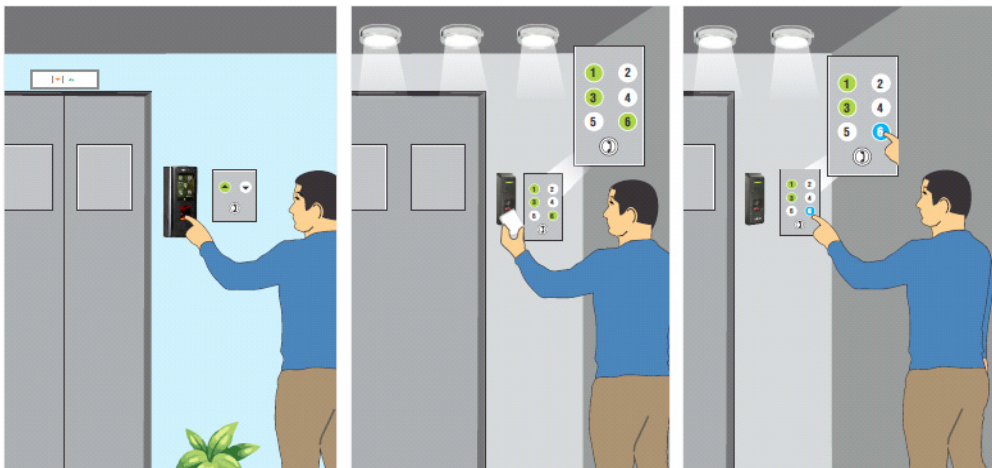
- The doors with the selected status appear as per the assigned racks.
- **Refresh:** Click **Refresh**  to refresh the door status for all the doors.





*This feature is applicable to PVR Door, Door V3, Door V4, Wireless, Vega, ARC IO800, ARGO Door, ARGO FACE Door, ARGO FACE210 Door, ARC DC100 and ARC DC200 only.*

Elevator can be considered as doorways in many organizations, buildings and restricted areas. A person accessing the elevator can gain access to any floor he/she wishes. Hence, to increase the security and restrict access for different floors in a building, Elevator Access Control (EAC) feature must be used.



### **EAC Configuration and Working**

Let us understand this with the help of an example:

Configure Elevator1 with 4 floors and Elevator 2 with 4 floors. Now configure an Elevator group say RnD Elevators which includes Elevator1 with floor1 and 2 and Elevator2 with floor 3 and 4. This means using Elevator1 you can access floors1 and 2 and with elevator2 you can access floors 3 and 4.

Now users must be authorized to access the elevators by linking them to the Elevator group. So link the RnD Elevator group from Users Linking tab by selecting the users from the picklist. Say user Dinesh is linked to RnD Elevators.

When the user Dinesh comes in the Elevator1, then he has to punch on the authenticating door, say Door V3. Once he is allowed the access to Door V3, the floors of Elevator1 (floor1 and 2)for which he is allowed access will get enabled. The floor1 and floor2 are enabled through the output port of IO controller. Hence he can press the desired floor button.

The IO Controller has 8 output ports which can be linked to 8 floors of an elevator.



*If an Output Port is already active with EAC Link and IO LINK is activated having same output port, then priority will be given to IO LINK and the desired port will be activated as per IO Link. The EAC Link will be deactivated.*

The Elevator Access Control allows you to:

- configure the Elevators. For details, refer to [“Elevator Configuration”](#).
- configure the Elevator Floor Groups. For details, refer to [“Elevator Floor Group”](#).



# Elevator Configuration



*This feature is applicable to PVR Door, Door V3, Door V4, Wireless, Vega, ARC IO800, ARGO Door, ARGO FACE Door, ARGO FACE210 Door, ARC DC100 and ARC DC200 only.*

To configure the Elevators,

Click **Elevator Access Control > Elevator Configuration**. The **Elevator Configuration** page appears.

| Elevator Configuration |               |         |                      |        |  |
|------------------------|---------------|---------|----------------------|--------|--|
| Elevator ID            | Elevator Name | Door ID | Door Name            | Floors |  |
| 1                      | Elevator 1    | 3       | SpecialCard_ArgoFace | 4      |  |
| 2                      | Elevator 2    | 9       | 2                    | 4      |  |
| <div>Add</div>         |               |         |                      |        |  |

All the created Elevators appear in the grid with their details — Elevator ID, Elevator Name, Door ID, Door Name and Floors.

You can click the desired Elevator and edit it as per your requirement or you can add new Elevators.

You can also delete any Elevator. To do so, click **Delete** corresponding to the desired Elevator.

To add an Elevator,

Click **Add**. You can create maximum **64** Elevators.

Configure the following parameters:

- **Elevator ID:** The Elevator ID is auto-generated by the PANEL200.
- **Elevator Name:** Configure a name you wish to assign to the Elevator.
- **Number of Floors:** Configure the number of floors that can be accessed using Elevator. You can add maximum **99** floors for an Elevator.
- **Authentication Device:** Click the **Authentication Device** picklist. The **Panel Doors** pop-up appears. Select the desired device which you wish to assign as the Authentication Device.

OR

You can also search for the desired door. To do so, enter the keyword in the Search box. Click **Search**

 . The doors will be filtered as per the keyword. Select the desired device which you wish to assign as the Authentication Device.

The user will be allowed to access the floors only after successful authentication. The Authentication Device must be placed inside the Elevator, so it is recommended to select individual Authentication Device for each Elevator.

- **Access Duration For Floors:** Configure the time duration in seconds for which the selected floors will be accessible to the user post authentication. The user must press the desired floor number within the configured Access Duration time after successful authentication to access the floor. If the Access Duration time expires, the user will not be able to access the floors and needs to authenticate again.

Click **Update**. The rows in the grid are updated to match the number of configured floors.

Now configure the floor settings:

- **Floor Name:** Configure a name you wish to assign to the Floor.

- **Free Access Floor:** Select the check box if the floor should be accessible by all users without any authentication.
- **IO Controller:** Click the **IO Controller** picklist. The **Panel Doors** pop-up appears. Select the desired IO Controller with which you wish to link the floor.

OR

You can also search for the desired IO Controller. To do so, enter the keyword in the Search box. Click

**Search** . The IO Controllers will be filtered as per the keyword. Select the desired IO Controller with which you wish to link the floor.

- **Output Port:** Click the **Output Port** picklist. The **Port** pop-up appears. Select the desired Output Port number of the selected IO Controller with which you wish to link the floor.



*Make sure that the same IO Controller **Port** should not be assigned to different floors of the Elevator.*

Click **Save**.

You can clear any floor settings from the grid. To do so, click **Clear**  corresponding to the desired floor.

You can also search for the desired floors using the search bar. Click **Search by** and select the desired option — Name, ID — through which you wish to search the floors from the drop-down list. Now, enter the keyword as per the selected option under **Search by** to search for the floors. The floors will be filtered as per the entered keyword.

After you have completed all the configurations of the Elevator and if you wish to view all the created Elevators, click **View List** .



# Elevator Floor Group

---

To configure the Elevator Floor Groups,

Click **Elevator Access Control > Elevator Floor Group**. The **Elevator Floor Group** page appears.

| Group ID         | Group Name | Elevators | Floors |  |
|------------------|------------|-----------|--------|--|
| No Record Found! |            |           |        |  |

Add

All the created Elevator Floor Groups appear in the grid with their details — Group ID, Group Name, Elevators and Floors.

You can click the desired group and edit it as per your requirement or you can add new groups.

You can also delete any group. To do so, click **Delete**  corresponding to the desired group.

You can search for the desired Elevator Floor Group. To do so,

- Click **Search by** and select the desired option through which you wish to search the Elevator Floor Group from the drop-down list. Now, enter the keyword as per the selected option under **Search by** to search for the Elevator Floor Groups. The Elevator Floor Groups will be filtered as per the entered keyword.

The Elevator Floor Group allows you to:

- configure the Configuration parameters. For details, refer to [“Configuration”](#).
- configure the User Linking settings. For details, refer to [“Users Linking”](#).

To add an Elevator Floor Group,

Click **Add**. You can create maximum **999** Elevator Floor Groups.

## Configuration

To configure the Elevator Floor Group,

Click **Elevator Access Control > Elevator Floor Group > Configuration**. The **Configuration** page appears.

| Sr. No.          | Elevator Name | Floor Name | Time Zone Group Name |  |
|------------------|---------------|------------|----------------------|--|
| No Record Found! |               |            |                      |  |

Configure the following parameters:

- **Group ID:** The Group ID is auto-generated by the PANEL200.
- **Group Name:** Configure a name you wish to assign to the Elevator Floor Group.

### Group Members

- **Elevator:** Click the **Select Elevator** picklist. The Elevator pop-up appears. All the elevators configured from [“Elevator Configuration”](#) appear in the list. Select the desired elevator.

**OR**

You can also search for the desired elevator. To do so, enter the keyword in the Search box. Click **Search**



. The elevators will be filtered as per the keyword. Select the desired elevator.

- **Floor:** Click the **Select Floor** picklist. The **Floor** pop-up appears. Select the desired floor of the selected Elevator.

**OR**

You can also search for the desired floor. To do so, enter the keyword in the Search box. Click **Search**



. The floors will be filtered as per the keyword. Select the desired floor.

- **Time Zone Group:** Click the **Select Time Zone Group** picklist. The **Time Zone Group** pop-up appears. All the Time Zone Groups configured from “Group” under “Time Zone” appear in the list. Select the desired Time Zone Group.

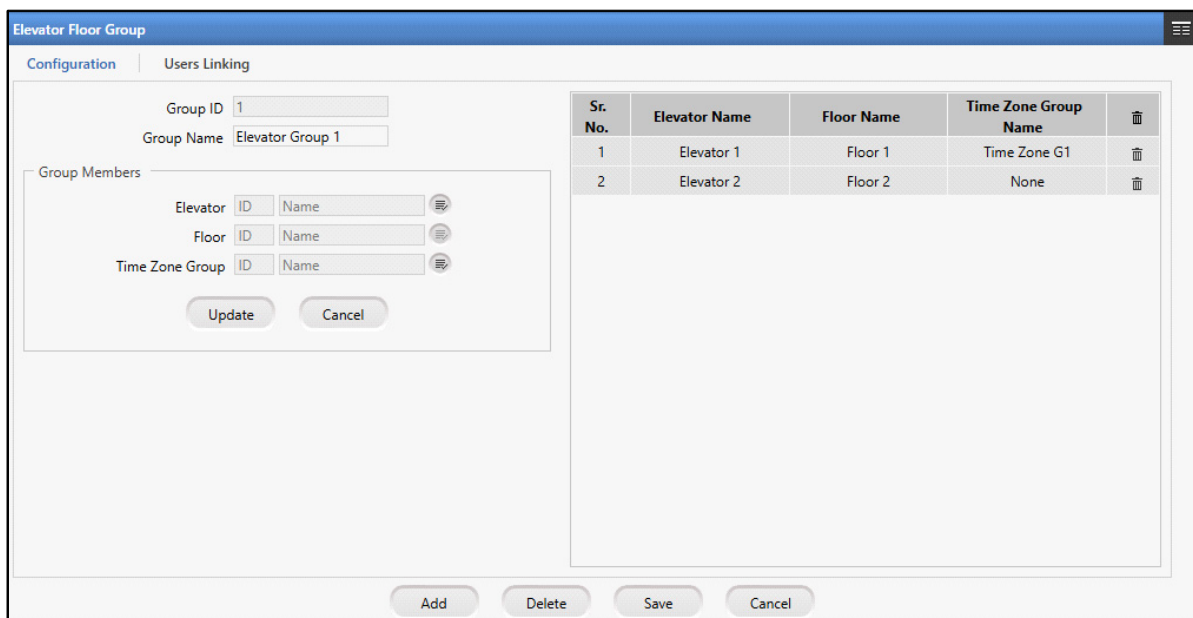
**OR**

You can also search for the desired time zone group. To do so, enter the keyword in the Search box. Click

**Search**  . The time zone groups will be filtered as per the keyword. Select the desired time zone group.

The selected floors will be accessible during the Time Zones under the selected Time Zone Group only. If no Time Zone Group is selected then the selected floors of the Elevator will be accessible throughout the day.

- Click **Update**. The configured Elevator appears in the grid in the right pane. Similarly, you can add other Elevators to the group.



| Sr. No. | Elevator Name | Floor Name | Time Zone Group Name |                                                                                      |
|---------|---------------|------------|----------------------|--------------------------------------------------------------------------------------|
| 1       | Elevator 1    | Floor 1    | Time Zone G1         |   |
| 2       | Elevator 2    | Floor 2    | None                 |  |

You can delete any added Elevator. To do so, click **Delete**  corresponding to the desired Elevator.

- Once all the desired Elevators are added, click **Save** to save the settings. Now, you need to link the desired users with the Elevator Floor Group. For details, refer to “Users Linking”.

After you have completed all the configurations of the Elevator Floor Group and if you wish to view all the created Elevator Floor Groups, click **View List**  .

Elevator Floor Group

Configuration

Users Linking

Group ID

1

Group Name

Elevator Group 1

Group Members

Elevator

ID

Name

Floor

ID

Name

Time Zone Group

ID

Name

Update

Cancel

| Sr. No. | Elevator Name | Floor Name | Time Zone Group Name |  |
|---------|---------------|------------|----------------------|--|
| 1       | Elevator 1    | Floor 1    | Time Zone G1         |  |
| 2       | Elevator 2    | Floor 2    | None                 |  |

Add

Delete

Save

Cancel

The Elevator Floor Group page displays all the created Elevator Floor Groups.

Elevator Floor Group

Configuration

Users Linking

Search by

Name

▼

Enter ID/Name

| Group ID | Group Name       | Elevators | Floors |  |
|----------|------------------|-----------|--------|--|
| 1        | Elevator Group 1 | 1         | 1      |  |
| 2        | Elevator Group 2 | 1         | 1      |  |

Add

## Users Linking

To configure the User Linking,

Click **Elevator Access Control > Elevator Floor Group > Users Linking**. The **Users Linking** page appears.



| Elevator Floor Group                                                                                                      |                  |       |
|---------------------------------------------------------------------------------------------------------------------------|------------------|-------|
| <div>Configuration   Users Linking</div> <div>Search by <span>Name</span> <span>Enter ID/Name</span> <span>Q</span></div> |                  |       |
| Group ID                                                                                                                  | Group Name       | Users |
| 1                                                                                                                         | Elevator Group 1 | 0     |
| 2                                                                                                                         | Elevator Group 2 | 0     |

All the created Elevator Floor Groups appear in the grid with their details — Group ID, Group Name and Users.

Click on the desired Elevator Floor Group with which you wish to link users.

| Elevator Floor Group                                                                                                                                                                                                                                                                                                                          |         |                                                                                                                                                                                          |      |         |                  |           |  |                            |  |  |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------|------------------|-----------|--|----------------------------|--|--|--|
| Configuration                                                                                                                                                                                                                                                                                                                                 |         | Users Linking                                                                                                                                                                            |      |         |                  |           |  |                            |  |  |  |
| <div> <div>Group ID <input type="text" value="1"/></div> <div>Group Name <input type="text" value="Elevator Group 1"/></div> </div>                                                                                                                                                                                                           |         | <table border="1"> <thead> <tr> <th>Sr. No.</th> <th>User ID</th> <th>User Name</th> <th></th> </tr> </thead> <tbody> <tr> <td colspan="4">No Record Found!</td> </tr> </tbody> </table> |      | Sr. No. | User ID          | User Name |  | No Record Found!           |  |  |  |
| Sr. No.                                                                                                                                                                                                                                                                                                                                       | User ID | User Name                                                                                                                                                                                |      |         |                  |           |  |                            |  |  |  |
| No Record Found!                                                                                                                                                                                                                                                                                                                              |         |                                                                                                                                                                                          |      |         |                  |           |  |                            |  |  |  |
| <div>Group Members</div> <div> <div>Access Group <input type="checkbox"/></div> <div>Users <input type="checkbox"/></div> </div> <table border="1"> <thead> <tr> <th>ID</th> <th>Name</th> <th></th> </tr> </thead> <tbody> <tr> <td colspan="3">No Record Found!</td> </tr> </tbody> </table> <div> <div>Save</div> <div>Cancel</div> </div> |         | ID                                                                                                                                                                                       | Name |         | No Record Found! |           |  | <div>Clear All Users</div> |  |  |  |
| ID                                                                                                                                                                                                                                                                                                                                            | Name    |                                                                                                                                                                                          |      |         |                  |           |  |                            |  |  |  |
| No Record Found!                                                                                                                                                                                                                                                                                                                              |         |                                                                                                                                                                                          |      |         |                  |           |  |                            |  |  |  |

Configure the following parameters:

- **Group ID:** It displays the Group ID of the selected Elevator Floor Group.
- **Group Name:** It displays the Group Name of the selected Elevator Floor Group.

## Group Members

You can select users individually or based on Access Groups.

**Access Group:** Click the **Access Group** picklist. The **Access Group** pop-up appears. All the configured Access Groups appear in the list. Select the check boxes of the desired Access Groups. Select the header row check box to select all the Access Groups on that page. Click **Ok**. The selected Access Groups appear in the grid.

**OR**

If required, you can also search for the desired group.

**Search By:** Select the desired option by which you wish to search for the group — ID, Name. In the corresponding box enter the keyword. Click **Search** . The groups will be filtered as per the keyword. Select the desired group. Select the check boxes of the desired Access Groups. Select the header row check box to select all the Access Groups on that page. Click **Ok**. The selected Access Groups appear in the grid.

If you wish to remove the Access Groups, click **Delete**  of the respective Access Groups.

**Users:** Click the **User** picklist. The **Users** pop-up appears. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**. The selected users appear in the grid.

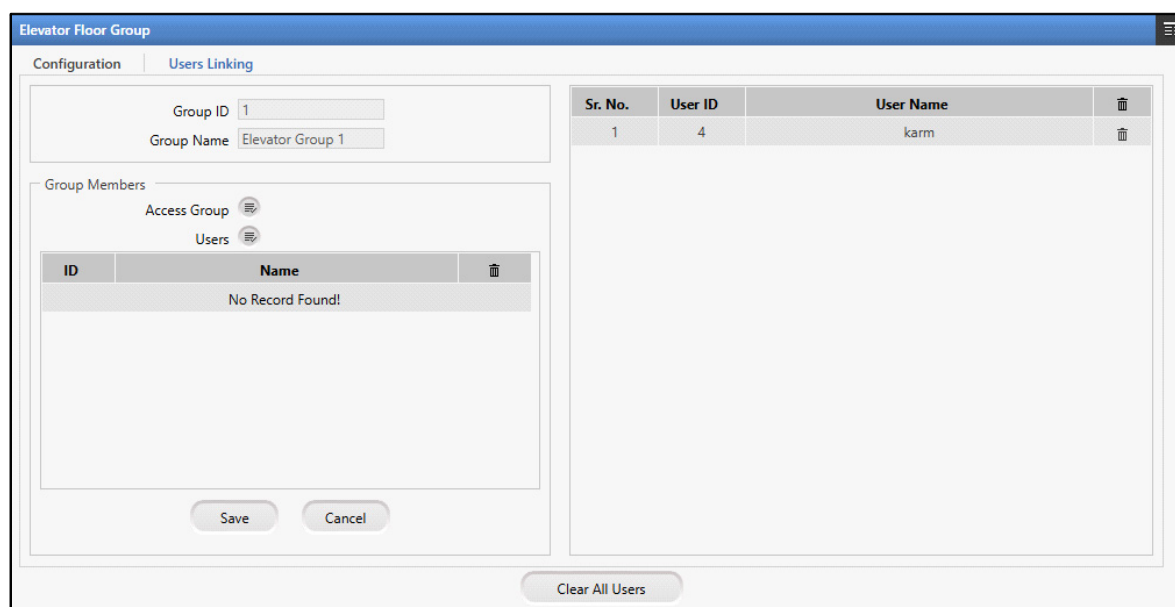
**OR**

If required, you can also search for the desired user.

**Search By:** Select the desired option by which you wish to search for the user — User ID, Name. In the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**. The selected users appear in the grid.

If you wish to remove the users, click **Delete**  of the respective user.

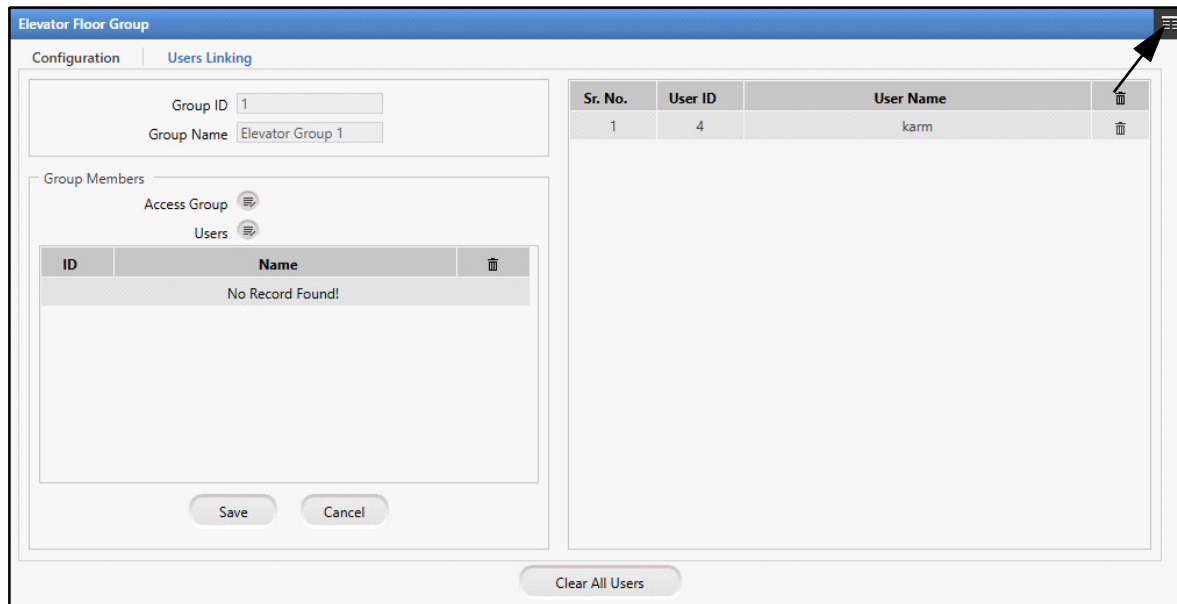
Click **Save** to save the settings. The selected users or users under the selected Access Groups appear in the grid in the right pane.



| Sr. No. | User ID | User Name |                                                                                       |
|---------|---------|-----------|---------------------------------------------------------------------------------------|
| 1       | 4       | karm      |  |

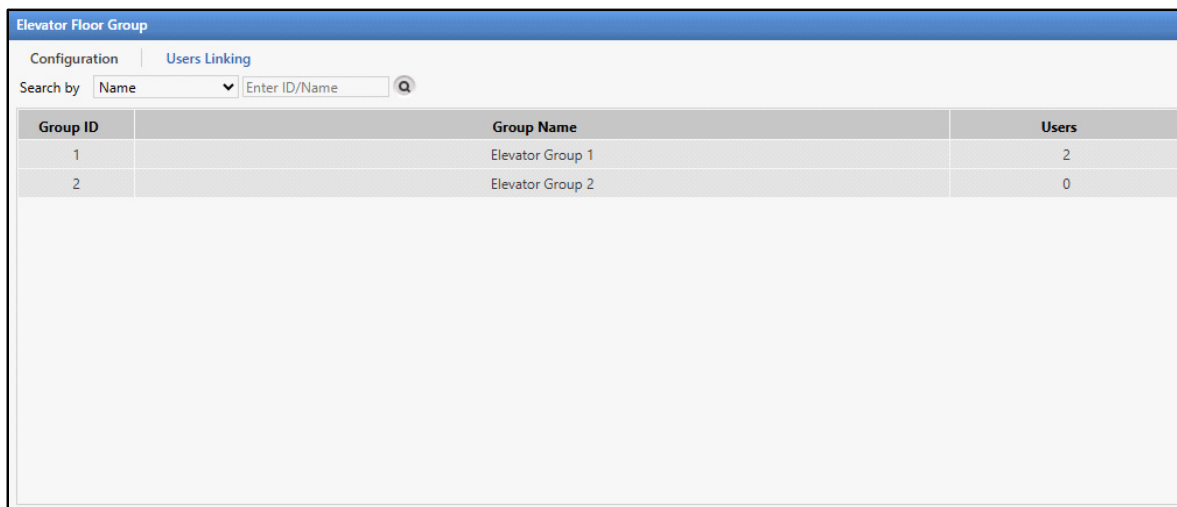
You can delete any added user. To do so, click **Delete**  corresponding to the desired user. If you wish to delete all the selected users, click **Clear All Users**.

After you have completed all the configurations of the Users Linking and if you wish to view all the linked users, click **View List** .



| Sr. No. | User ID | User Name |                                                                                     |
|---------|---------|-----------|-------------------------------------------------------------------------------------|
| 1       | 4       | karm      |  |

The Elevator Floor Group page displays the number of linked users with each Floor Group.



| Group ID | Group Name       | Users |
|----------|------------------|-------|
| 1        | Elevator Group 1 | 2     |
| 2        | Elevator Group 2 | 0     |

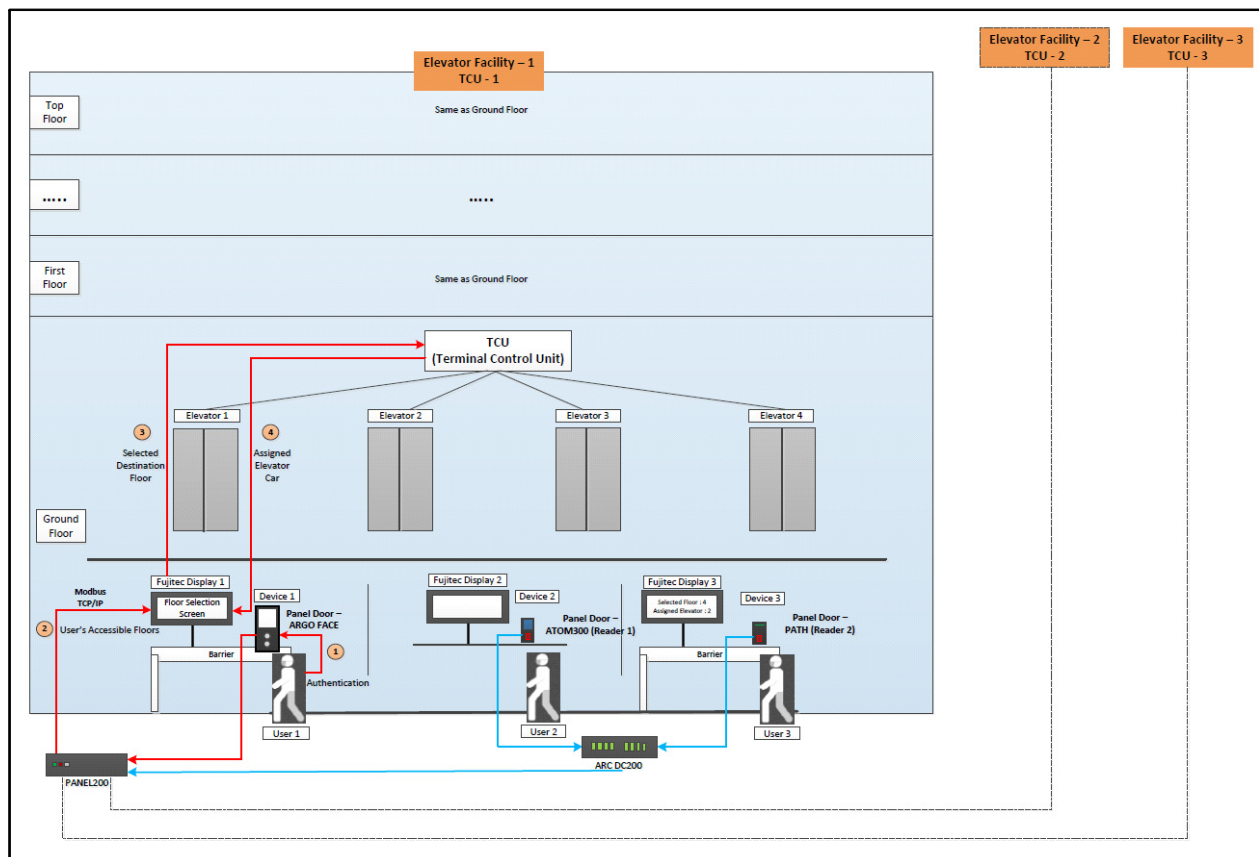


There are multiple Elevators within one premise (facility) or across multiple premises. In such cases the incoming traffic needs to be handled efficiently.



Let us understand this with the help of an example.

## Installation Setup at Premise (Facility) 1



Similarly, you have a setup at Premise2 and 3 also.

- Premise1 has 5 Floors and has 3 Elevators.
- Premise2 has 6 Floors and 3 Elevators.
- Premise3 has 6 Floors and has 3 Elevators.
- Doors [ARGO FACE and ARC DC200 - Dual Door Dual Readers, Door 1 is connected with ATOM300 and Door 2 is connected with PATH Reader] have been installed on each Floor for each Elevator along with Terminal Display Units.



*If you connect ARC DC200 - Single Door Dual Reader, then one Reader can be used for entry which is connected with Terminal Display Unit. While the other Reader can be used for exit.*

- Each Terminal Display Unit has a Door associated with it. This duo is assigned a Terminal ID for identification and communication.
- There is a Destination Control System that communicates with the various Terminal Control Units.
- Each premise has a Terminal Control Unit which controls and communicates with the various Terminal Display Units and doors connected within the premise via the Terminal ID assigned to it.

The configuration is done in such a way that users are assigned certain Doors as well as Floors of the Elevators that they can access within the Premises.

At Premise2 and 3, you can connect doors belonging to the same PANEL200 and configure them as mentioned above. Similarly, you can also connect doors belonging to different PANEL200s in the same Facility.

## How it works?

- When the user's valid credentials are received from the door, this information is passed by the door to the connected Panel200.
- If the connected door is ARC DC200, then the user's valid credentials are received by the connected Reader and this information is passed on to the ARC DC200 door. The ARC DC200 door then passes on this information to the connected Panel200.
- The Panel200 passes the information regarding the floors and doors that can be accessed by the user to the Terminal Control Unit.
- The Terminal Control Unit maintains a list of all the users and their corresponding doors and floors. This unit then passes this information to the Terminal Display Unit.
- The user's relevant floors are displayed on the respective Terminal Display Unit connected with the door. At the same time, the message to select the relevant floor on the Terminal Display Unit appears on the door's display screen.
- The user can now select the desired floor. This information is passed by the Terminal Display Unit to the Terminal Control Unit.
- The Terminal Control Unit derives the free Elevator access available as per the user selection and passes this information to the Terminal Display Unit.
- The Terminal Display Unit then displays the free Elevator number that the user needs to access.
- As per the information displayed, the user can move further towards the desired Elevator.

Hence, the frequent incoming traffic is handled efficiently within less time.



At the entry, along with the door if you have installed a barrier which users need to cross before they can reach the assigned Elevator, then configure the **Pulse Timer (sec)** considering your scenario. For details, refer [“Advance Configuration”](#) under [“Door Configuration”](#).

For doors, the information will always be passed to the TCU. However, if readers are connected, the information will be passed to the TCU only if the Reader Mode is set as **Entry**.

In case of ARC DC200 - Single Door Dual Reader, if readers are connected, the information will be passed to the TCU only if the Reader Mode is set as **Entry**.

In case of ARC DC200 - Dual Door Dual Reader, if readers are connected, the information will be passed to the TCU irrespective of the set Reader Mode.

## Configuration Details

Let us understand the configurations required for the functioning of this feature:

- You have configured the Elevator Facility Configuration. For details refer to [“Elevator Facility”](#).
- You have configured the Smart Elevator Floor Group. For details refer to [“Smart Elevator Floor Group”](#).
- Make sure the desired devices configured in the [“Elevator Facility”](#) are assigned to users. For details refer to [“Profile”](#) in [“User Configuration”](#).
- Enable Smart Elevator Access Control and assigned the desired Smart Elevator Floor Group to users. For details refer to [“Smart Elevator Access Control”](#) in [“Advanced Access Control 2”](#) under [“User Configuration”](#).



If Smart Elevator Access is enabled for the users and door is a part of the Elevator Facility Configuration, then the Access Policies will function as follows:

- **VIP Access:** VIP users will be able to access floors as per the Accessible Floors assigned to them.
- **2-Person Rule:** After both the users are validated, the floors accessible by both the users will be as per the Accessible Floors assigned to the first user.

The Smart Elevator Access Control allows you to:

- configure the Elevator Facility. For details, refer to [Elevator Configuration](#).
- configure the Smart Elevator Floor Groups. For details, refer to [Smart Elevator Floor Group](#).

# Elevator Facility

To configure the Elevator Facility,

Click **Smart Elevator Access Control > Elevator Facility**. The **Elevator Facility** page appears.

| Elevator Facility    |                        |       |        |                                                                                     |
|----------------------|------------------------|-------|--------|-------------------------------------------------------------------------------------|
| Elevator Facility ID | Elevator Facility Name | Doors | Floors |                                                                                     |
| 1                    | Facility 1             | 13    | 6      |  |
| 2                    | Facility 2             | 1     | 2      |  |
| <div>Add</div>       |                        |       |        |                                                                                     |

All the created Elevator Facilities appear in the grid with their details — Elevator Facility ID, Elevator Facility Name, Number of Doors and Number of Floors.

You can click the desired Elevator Facility and edit it as per your requirement or you can add new Elevator Facilities.

You can also delete any Elevator Facility. To do so, click **Delete**  corresponding to the desired Elevator Facility.

To add an Elevator Facility,

Click **Add**. You can create maximum **32** Elevator Facilities.



Configure the following parameters:

- **Elevator Facility ID:** The Elevator Facility ID is auto-generated by the Panel200.
- **Elevator Facility Name:** Configure a name you wish to assign to the Elevator Facility.
- **Elevator Brand:** It is un-editable and displays **Fujitec**.
- **Elevator Terminal IP Address:** Configure the IP Address of the Terminal Control Unit installed to manage the various Terminal Display Units and Doors communication.
- **Elevator Terminal Port Number:** Configure the Port of the Terminal Control Unit on which it will communicate with the various Terminal Display Units and Doors.
- **Assign Door:** Click the **Assign Door** picklist. The **Door** pop-up appears. Select the check boxes of the desired doors. Select the header row check box to select all the doors on that page. Click **Ok**. Maximum 127 doors can be assigned to a single Elevator Facility.

**OR**

You can search for the desired doors using the Search bar. Enter the keyword according to which you wish to search. Click **Search**  The doors will be filtered as per the entered keyword. Select the check boxes of the desired doors. Select the header row check box to select all the doors on that page. Click **Ok**. Maximum 127 doors can be assigned to a single Elevator Facility.

The selected doors appear in the grid under Configure Doors. Each Door appears in a separate row. Now you need to ["Configure Doors"](#) and assign them in ["Floor Configuration"](#).



*Doors once selected, appear in the grid and the same are removed from the Assign Door picklist.*

*Same Doors cannot be assigned to multiple Premises.*

## Configure Doors

Click the **Configure Doors** collapsible panel.



*The parameters — Consider Device Display for Floor Selection, Access Duration — will be applicable in future releases.*

The screenshot shows the 'Elevator Facility' configuration window. At the top, there are fields for 'Elevator Facility ID' (3), 'Elevator Facility Name' (Facility 4), 'Elevator Brand' (Fujitec), 'Elevator Terminal IP Address' (192.168.103.142), and 'Elevator Terminal Port Address' (2211). Below these is an 'Assign Door' button. The 'Configure Doors' section is expanded, showing a search bar with 'Name' selected and a search icon. Below the search bar is a table with the following data:

| Door ID | Door Name            | Consider Device Display for Floor Selection | Access Duration(sec) | Terminal ID | Network Interface |  |
|---------|----------------------|---------------------------------------------|----------------------|-------------|-------------------|--|
| 59      | COSEC_DEVICE_PATH_V2 | <input type="checkbox"/>                    | 10                   | 1 - 127     | Ethernet          |  |
| 62      | COSEC_DEVICE_ARC_V2  | <input type="checkbox"/>                    | 10                   | 1 - 127     | Ethernet          |  |
| 68      | COSEC_DEVICE_PATH_V2 | <input type="checkbox"/>                    | 10                   | 1 - 127     | Ethernet          |  |
| 76      | COSEC_DEVICE_ARC_V2  | <input type="checkbox"/>                    | 10                   | 1 - 127     | Ethernet          |  |

At the bottom of the window are 'Save' and 'Cancel' buttons.

Configure the following parameters:

- **Terminal ID:** Click the corresponding **Terminal ID** text box and configure the Terminal ID you wish to assign to the door.
- **Network Interface:** For each door, select the desired network interface over which the door is connected from the drop-down list options — Ethernet, Wireless, Mobile Broadband.

Click **Save**.

You can edit the Terminal /Network Interface if required.

To delete, click the corresponding **Delete** . The door is deleted from the grid.

You can also search for the desired doors using the search bar. Click **Search by** and select the desired option — Name, ID — through which you wish to search the doors. Now, enter the keyword as per the selected option under **Search by** to search for the doors. The doors will be filtered as per the entered keyword.

## Floor Configuration

Click the **Floor Configuration** collapsible panel.



*The parameter Free Access Floor will be applicable in future releases.*

Configure the following parameters:

- Click **Add** and configure the following. You can add upto 255 Floors in a single Premise.

- **Floor No.:** Configure the Floor Number.

- **Floor Name:** Configure a name you wish to assign to the Floor.

- **Device:** Click the **Device** picklist. The **Door** pop-up appears. Select the check boxes of the desired doors. Select the header row check box to select all the doors on that page. Click **Ok**.

**OR**

You can search for the desired doors using the Search bar. Enter the keyword according to which you wish to search. Click **Search** The doors will be filtered as per the entered keyword. Select the check boxes of the desired doors. Select the header row check box to select all the doors on that page. Click **Ok**.



*Same Doors cannot be assigned to multiple Floors.*

- Click **OK** to save the configuration. It displays the number of selected doors.

Elevator Facility ID

Elevator Facility Name

Elevator Brand

Elevator Terminal IP Address

Elevator Terminal Port Address

Assign Door 

Configure Doors 

Floor Configuration 

Search by  Enter No./Name 

| Floor No.                      | Floor Name                              | Free Access Floor               | Devices           |                                                                                                                                                                         |
|--------------------------------|-----------------------------------------|---------------------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="text" value="1"/> | <input type="text" value="FirstFloor"/> | <input type="text" value="No"/> | <a href="#">1</a> |   |

Click on the numeric value under Device to view the selected doors. The **Door** pop-up appears. The selected doors are displayed here.

To edit the entry, click **Edit** .

To delete, click the corresponding **Delete** . The entire entry is deleted.

Click **Save**.

You can also search for the desired floors using the search bar. Click **Search by** and select the desired option — Name, No.— through which you wish to search the floors. Now, enter the keyword as per the selected option under **Search by** to search for the floors. The floors will be filtered as per the entered keyword.

After you have completed all the configurations of the Elevator Facility and if you wish to view all the created Elevator Facilities, click **View List** .

Elevator Facility

Elevator Facility ID

Elevator Facility Name

Elevator Brand

Elevator Terminal IP Address

Elevator Terminal Port Address

Assign Door 

Configure Doors 

Floor Configuration 



Add Delete Save Cancel

The Elevator Facility page displays all the created Elevator Facilities.

Elevator Facility

| Elevator Facility ID | Elevator Facility Name | Doors | Floors |  |
|----------------------|------------------------|-------|--------|--|
| 1                    | Facility 1             | 0     | 2      |  |
| 2                    | Facility 4             | 1     | 5      |  |
| 3                    | Facility 2             | 5     | 2      |  |
| 4                    | Facility 3             | 126   | 255    |  |
| 5                    | Facility 6             | 0     | 2      |  |
| 6                    | Facility 7             | 0     | 2      |  |
| 7                    | Facility 8             | 0     | 2      |  |
| 8                    | Facility 9             | 0     | 2      |  |
| 9                    | Facility 10            | 4     | 4      |  |
| 10                   | Facility 12            | 10    | 2      |  |

Add

# Smart Elevator Floor Group

To configure the Smart Elevator Floor Groups,

Click **Smart Elevator Access Control > Smart Elevator Floor Group**. The **Smart Elevator Floor Group** page appears.

| Group ID | Group Name    | Elevator Facilities | Accessible Floors |  |
|----------|---------------|---------------------|-------------------|--|
| 1        | Floor Group 3 | 32                  | 283               |  |
| 2        | Floor Group 2 | 1                   | 2                 |  |
| 3        | Floor Group 1 | 2                   | 9                 |  |

All the created Smart Elevator Floor Groups appear in the grid with their details — Group ID, Group Name, Number of Elevator Facilities and Number of Accessible Floors.

You can click the desired group and edit it as per your requirement or you can add new groups.

You can also delete any group. To do so, click **Delete** corresponding to the desired group.

You can search for the desired Smart Elevator Floor Group. To do so,

- Click **Search by** and select the desired option — Name, ID — through which you wish to search the Smart Elevator Floor Group. Now, enter the keyword as per the selected option under **Search by** to search for the Smart Elevator Floor Groups. The Smart Elevator Floor Groups will be filtered as per the entered keyword.

The Smart Elevator Floor Group allows you to:

- configure the Configuration parameters. For details, refer to [“Configuration”](#).
- configure the User Linking settings. For details, refer to [“Users Linking”](#).

To add a Smart Elevator Floor Group,

Click **Add**. You can create maximum **999** Smart Elevator Floor Groups.

## Configuration

To configure the Smart Elevator Floor Group,

Click **Smart Elevator Access Control > Smart Elevator Floor Group > Configuration**. The **Configuration** page appears.



*Elevator Facilities once selected are removed from the Elevator Facility picklist. An Elevator Facility can be assigned to a single Smart Elevator Floor Group only.*

*The parameter — Accessible from Assigned Floor Only will be applicable in future releases.*

Configure the following parameters:

- **Group ID:** The Group ID is auto-generated by the Panel200.
- **Group Name:** Configure a name you wish to assign to the Smart Elevator Floor Group.

### Group Members

- **Elevator Facility:** Click the **Select Elevator Facility** picklist. The **Elevator Facility** pop-up appears. Select the desired Elevator Facility. All the Elevator Facilities configured from “**Elevator Facility**” appear in the list.  
**OR**  
You can search for the desired Elevator Facility using the Search bar. Enter the keyword according to which you wish to search. Click **Search**  The Elevator Facilities will be filtered as per the entered keyword. Select the desired Elevator Facility.
- **Accessible Floor:** Click the **Select Floor** picklist. The **Accessible Floor** pop-up appears. Select the check boxes of the desired floors of the selected Elevator Facility. Click **Ok**.  
**OR**

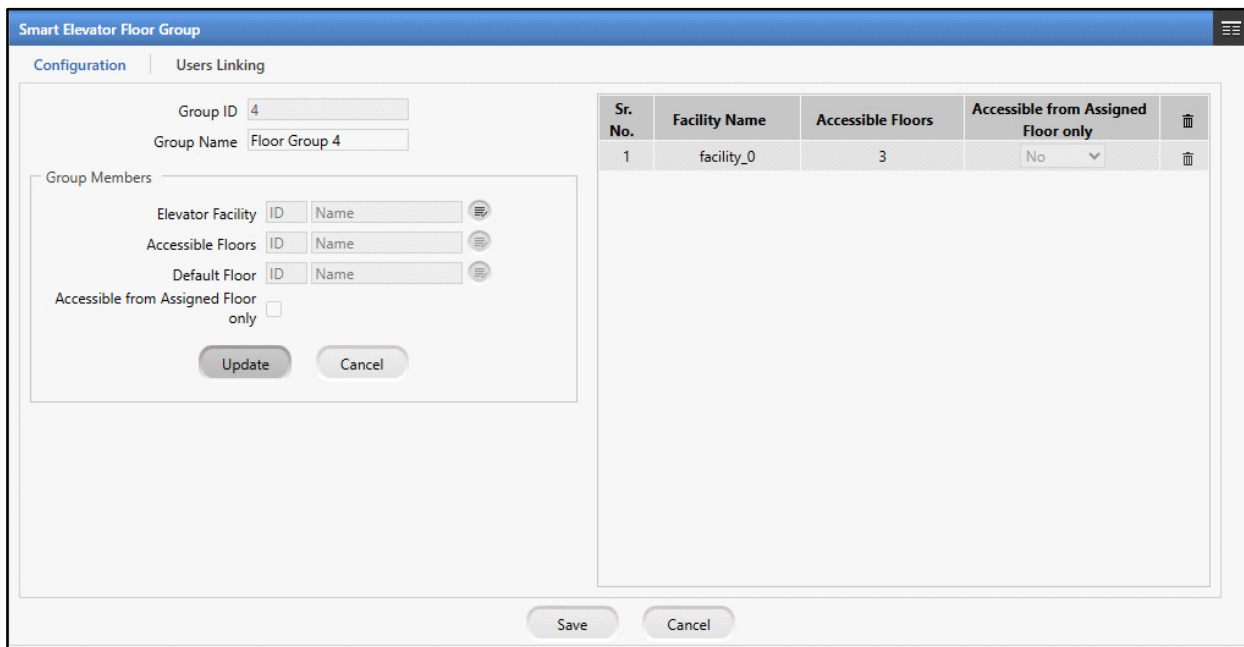
You can search for the desired floors using the Search bar. Enter the keyword according to which you wish to search. Click **Search**  The floors will be filtered as per the entered keyword. Select the check boxes of the desired floors. Select the header row check box to select all the floors on that page. Click **Ok**.

- **Default Floor:** Click the **Select Floor** picklist. The **Default Floor** pop-up appears. Select the desired floor of the selected Elevator Facility to be set as Default Floor. If the user does not select any floor on the actual Floor Selection Display Screen, then this floor will be allotted by default.

**OR**

You can search for the desired floor using the Search bar. Enter the keyword according to which you wish to search. Click **Search**  The floors will be filtered as per the entered keyword. Select the desired floor of the selected Elevator Facility to be set as Default Floor.

- Click **Update**. The configured Facility appears in the grid in the right pane. Similarly, you can add other Facilities to the group as members.



The screenshot shows the 'Smart Elevator Floor Group' configuration window. It has two tabs: 'Configuration' and 'Users Linking'. The 'Configuration' tab is active. It contains fields for 'Group ID' (value: 4) and 'Group Name' (value: Floor Group 4). Below these is a 'Group Members' section with three rows for 'Elevator Facility', 'Accessible Floors', and 'Default Floor'. Each row has 'ID' and 'Name' input fields and a menu icon. There is also a checkbox for 'Accessible from Assigned Floor only' which is currently unchecked. 'Update' and 'Cancel' buttons are at the bottom of the 'Group Members' section. To the right is a table with the following data:

| Sr. No. | Facility Name | Accessible Floors | Accessible from Assigned Floor only |                                                                                     |
|---------|---------------|-------------------|-------------------------------------|-------------------------------------------------------------------------------------|
| 1       | facility_0    | 3                 | No                                  |  |

'Save' and 'Cancel' buttons are at the bottom of the window.

You can delete any added Facility. To do so, click **Delete**  corresponding to the desired Facility.

- Once all the desired Facilities are added, click **Save** to save the settings. Now, you need to link the desired users with the Smart Elevator Floor Group. For details, refer to [“Users Linking”](#).

After you have completed all the configurations of the Smart Elevator Floor Groups and if you wish to view all the created Smart Elevator Floor Groups, click **View List** .



Smart Elevator Floor Group

Configuration

Users Linking

Group ID

4

Group Name

Floor Group 4

Group Members

Elevator Facility

ID

Name

Accessible Floors

ID

Name

Default Floor

ID

Name

Accessible from Assigned Floor only

☐

Update

Cancel

| Sr. No. | Facility Name | Accessible Floors | Accessible from Assigned Floor only |  |
|---------|---------------|-------------------|-------------------------------------|--|
| 1       | facility_0    | 3                 | No                                  |  |

Save

Cancel

The Smart Elevator Floor Group page displays all the created Smart Elevator Floor Groups.

Smart Elevator Floor Group

Configuration

Users Linking

Search by

Name

Enter ID/Name

| Group ID | Group Name    | Elevator Facilities | Accessible Floors |  |
|----------|---------------|---------------------|-------------------|--|
| 1        | Floor Group 3 | 32                  | 283               |  |
| 2        | Floor Group 2 | 1                   | 2                 |  |
| 3        | Floor Group 1 | 2                   | 9                 |  |
| 4        | Floor Group 4 | 1                   | 3                 |  |

Add

## Users Linking

To configure the User Linking,

Click **Smart Elevator Access Control > Smart Elevator Floor Group > Users Linking**. The **Users Linking** page appears.

Matrix COSEC Panel200 System Manual

309

Smart Elevator Floor Group

Configuration

Users Linking

Search by

Name

▼

Enter ID/Name

Q

| Group ID | Group Name    | Users |
|----------|---------------|-------|
| 1        | Floor Group 3 | 3     |
| 2        | Floor Group 2 | 0     |
| 3        | Floor Group 1 | 0     |
| 4        | Floor Group 4 | 0     |

All the created User Links appear in the grid with their details — Group ID, Group Name and Number of Users.

Click on the desired User Link in which you wish to assign users.

Elevator Floor Group

Configuration

Users Linking

Group ID

4

Group Name

Floor Group 4

Group Members

Access Group

Users

| ID               | Name |  |
|------------------|------|--|
| No Record Found! |      |  |

Save

Cancel

| Sr. No.          | User ID | User Name |  |
|------------------|---------|-----------|--|
| No Record Found! |         |           |  |

Clear All Users

Configure the following parameters:

- **Group ID:** It displays the Group ID of the selected Smart Elevator Floor Group.
- **Group Name:** It displays the Group Name of the selected Smart Elevator Floor Group.

## Group Members

You can select users individually or based on Access Groups.

- **Access Group:** Click the **Access Group** picklist. The **Access Group** pop-up appears. All the configured Access Groups appear in the list. Select the check boxes of the desired Access Groups. Select the header row check box to select all the Access Groups on that page. Click **Ok**.

### OR

You can also search for the desired Access Groups using the search bar. Click **Search by** and select the desired option — Name, ID — through which you wish to search the Access Groups. Now, enter the keyword as per the selected option under **Search by** to search for the Access Groups. The Access Groups will be filtered as per the entered keyword. Select the check boxes of the desired Access Groups. Select the header row check box to select all the Access Groups on that page. Click **Ok**.

The selected Access Groups appear in the grid.

If you wish to remove the Access Groups, click **Delete**  of the respective Access Groups.

- **Users:** Click the **User** picklist. The **Users** pop-up appears. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

### OR

You can also search for the desired users using the search bar. Click **Search by** and select the desired option — Name, ID — through which you wish to search the users. Now, enter the keyword as per the selected option under **Search by** to search for the users. The users will be filtered as per the entered keyword. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

The selected users appear in the grid.

If you wish to remove the users, click **Delete**  of the respective user.

Click **Save** to save the settings. The selected users appear in the grid in the right pane.

Elevator Floor Group

Configuration

Users Linking

Group ID 4

Group Name Floor Group 4

Group Members

Access Group

Users

| ID               | Name |  |
|------------------|------|--|
| No Record Found! |      |  |

Save

Cancel

| Sr. No. | User ID | User Name |  |
|---------|---------|-----------|--|
| 1       | 3       | user3     |  |
| 2       | 4       | user4     |  |

Clear All Users

You can delete any added user. To do so, click **Delete**  corresponding to the desired user. If you wish to delete all the selected users, click **Clear All Users**.

After you have completed all the configurations of the Users Linking and if you wish to view all the linked users, click **View List**  .

Elevator Floor Group

Configuration

Users Linking

Group ID 4

Group Name Floor Group 4

Group Members

Access Group

Users

| ID               | Name |  |
|------------------|------|--|
| No Record Found! |      |  |

Save

Cancel

| Sr. No. | User ID | User Name |  |
|---------|---------|-----------|--|
| 1       | 3       | user3     |  |
| 2       | 4       | user4     |  |

Clear All Users

The Smart Elevator Floor Group page displays all the created Smart Elevator Floor Groups.

Smart Elevator Floor Group

Configuration

Users Linking

Search by 

Name

Enter ID/Name

| Group ID | Group Name    | Elevator Facilities | Accessible Floors |  |
|----------|---------------|---------------------|-------------------|--|
| 1        | Floor Group 3 | 32                  | 283               |  |
| 2        | Floor Group 2 | 1                   | 2                 |  |
| 3        | Floor Group 1 | 2                   | 9                 |  |
| 4        | Floor Group 4 | 1                   | 3                 |  |

Add



---

Import Export allows you to:

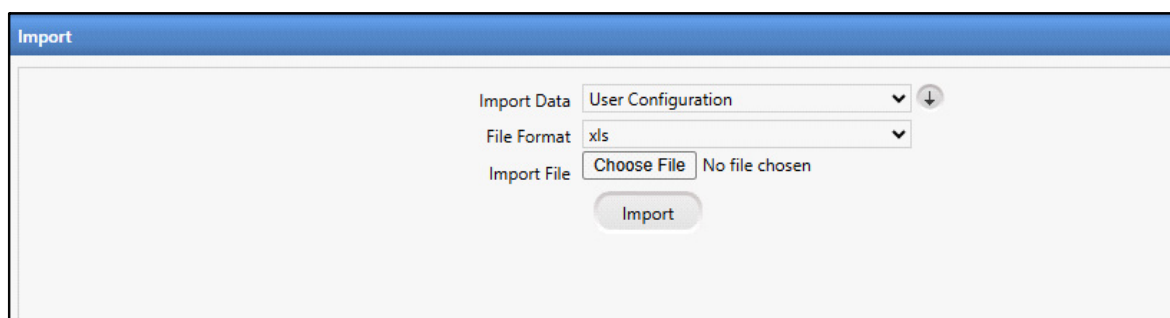
- import data into PANEL200. For details, refer to [“Import”](#).
- export data from PANEL200. For details, refer to [“Export”](#).
- configure and generate Reports. For details, refer to [“Reports”](#).

# Import

The Import feature allows you to import data in PANEL200. This saves the hassle of configuration which can be simplified by importing the desired configuration data using the Import functionality.

To import the data,

Click **Import Export > Import**. The **Import** page appears.



Configure the following parameters:

- **Import Data:** Select the desired type of data you wish to import through the import file from the drop-down list.

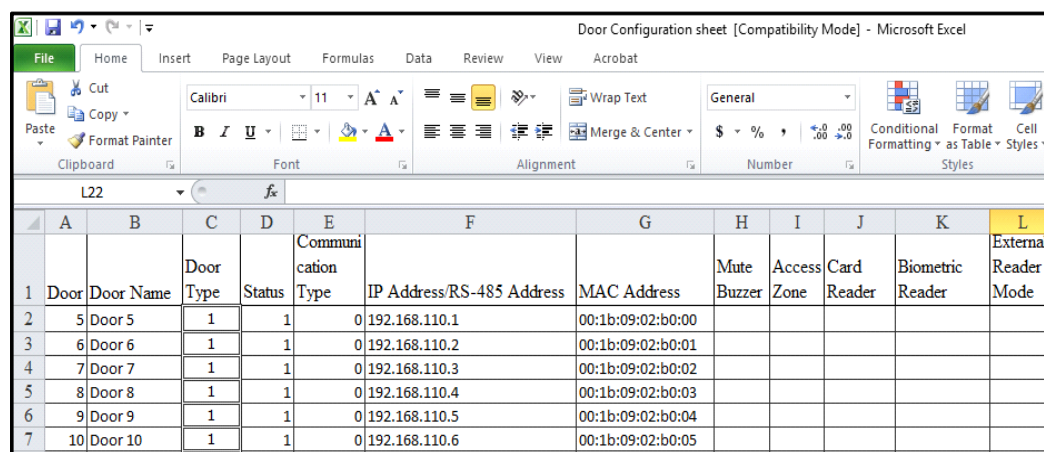
Click **Download Sample Import File** . Enter the data in this downloaded file according to the defined range and guidelines laid down in the **HELP** tab of the file.

Once the data is entered, you need to import this file into PANEL200.

- **File Format:** Select the desired File Format in which you wish to import the file from the drop-down list options.
- **Import File:** Click **Choose File** and select the desired file to be imported.

Click **Import** to import the selected file. When the file is imported successfully, **Import Success** message appears.

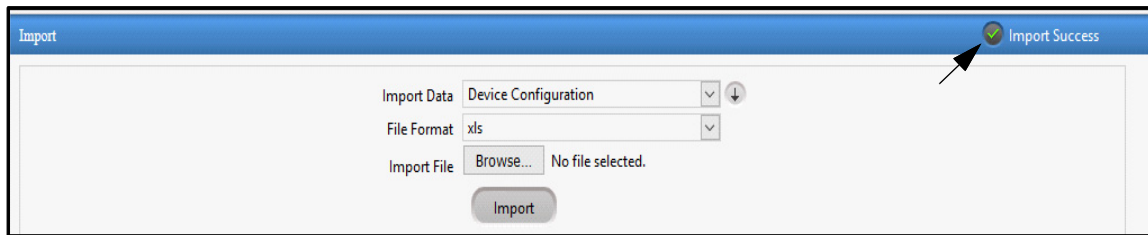
For example, let us consider importing Device Configuration. The excel file imported here has following device configurations:



|   | A    | B         | C         | D      | E                  | F                         | G                 | H           | I           | J           | K                | L                    |
|---|------|-----------|-----------|--------|--------------------|---------------------------|-------------------|-------------|-------------|-------------|------------------|----------------------|
|   | Door | Door Name | Door Type | Status | Communication Type | IP Address/RS-485 Address | MAC Address       | Mute Buzzer | Access Zone | Card Reader | Biometric Reader | External Reader Mode |
| 1 | 5    | Door 5    | 1         | 1      | 0                  | 192.168.110.1             | 00:1b:09:02:b0:00 |             |             |             |                  |                      |
| 2 | 6    | Door 6    | 1         | 1      | 0                  | 192.168.110.2             | 00:1b:09:02:b0:01 |             |             |             |                  |                      |
| 3 | 7    | Door 7    | 1         | 1      | 0                  | 192.168.110.3             | 00:1b:09:02:b0:02 |             |             |             |                  |                      |
| 4 | 8    | Door 8    | 1         | 1      | 0                  | 192.168.110.4             | 00:1b:09:02:b0:03 |             |             |             |                  |                      |
| 5 | 9    | Door 9    | 1         | 1      | 0                  | 192.168.110.5             | 00:1b:09:02:b0:04 |             |             |             |                  |                      |
| 6 | 10   | Door 10   | 1         | 1      | 0                  | 192.168.110.6             | 00:1b:09:02:b0:05 |             |             |             |                  |                      |



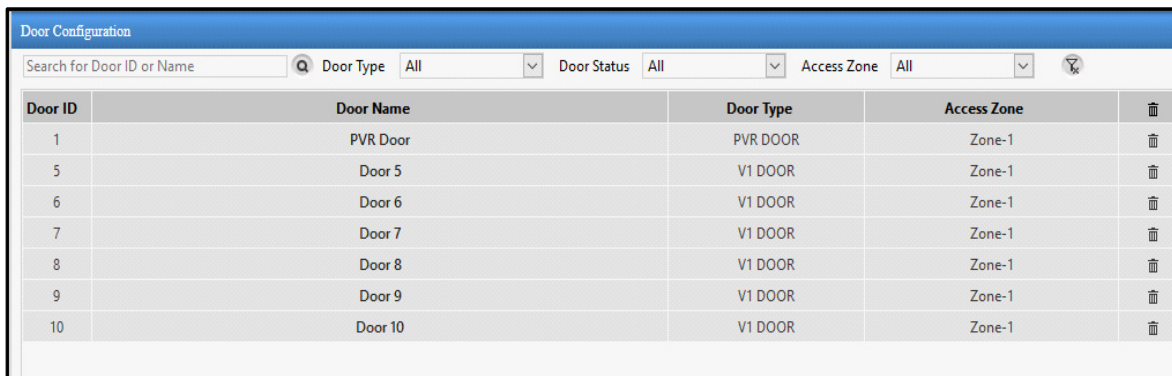
- Click **Import** to import the data from the selected file into the PANEL200. When the data is imported successfully, the message **Import Success** appears.



The screenshot shows the 'Import' dialog box. At the top right, a green circular icon with a checkmark and the text 'Import Success' is visible, with an arrow pointing to it. The main area of the dialog contains the following fields:

- Import Data:** A dropdown menu set to 'Device Configuration'.
- File Format:** A dropdown menu set to 'xls'.
- Import File:** A 'Browse...' button and the text 'No file selected.'
- Import:** A button at the bottom center.

- The imported data will be displayed on the Device Configuration page.



The screenshot shows the 'Door Configuration' page. At the top, there is a search bar and three filter dropdowns: 'Door Type' (set to 'All'), 'Door Status' (set to 'All'), and 'Access Zone' (set to 'All'). Below these is a table with the following data:

| Door ID | Door Name | Door Type | Access Zone |  |
|---------|-----------|-----------|-------------|--|
| 1       | PVR Door  | PVR DOOR  | Zone-1      |  |
| 5       | Door 5    | V1 DOOR   | Zone-1      |  |
| 6       | Door 6    | V1 DOOR   | Zone-1      |  |
| 7       | Door 7    | V1 DOOR   | Zone-1      |  |
| 8       | Door 8    | V1 DOOR   | Zone-1      |  |
| 9       | Door 9    | V1 DOOR   | Zone-1      |  |
| 10      | Door 10   | V1 DOOR   | Zone-1      |  |

# Export

---

Export allows you to:

- export data from PANEL200. For details, refer to [“Export”](#).
- configure Custom Templates. For details, refer to [“Templates”](#).

## Export

The Export feature allows you to export data from PANEL200. This feature is useful if you wish to export particular type of data from PANEL200 and the upload the same elsewhere.

To export the data,

Click **Import Export > Export**. The **Export** page appears.

| Template Type  | Template           | File Format | User Filter |
|----------------|--------------------|-------------|-------------|
| System Defined | User Configuration | xls         | Randomly    |

| User ID | Name |  |
|---------|------|--|
|---------|------|--|

Export

Configure the following parameters:

- **Template Type:** Select the desired Template Type according to the data type which you wish to export from the drop-down list options — Custom, System Defined.

If you select **Template Type** as **System Defined**, the data will be exported as per the system defined default template.

If you select **Template Type** as **Custom**, the data will be exported as per the configured [“Templates”](#).

- **Template:** Select the desired System Defined/Custom Template from the drop-down list. All the configured Custom Templates appear in the list if you select the **Template Type** as **Custom**.
- **File Format:** Select the desired File Format from the drop-down list.
- **Text File Separator:** If you have selected the **File Format** as **text/csv**, select the desired separator for the file.

- **User Filter:** If you have selected any User Configuration Template (System Defined or Custom), select the desired User Filter from the drop-down list options — Randomly, Access Group, All.
- If you select **All**, then all the users will be selected for export.
- If you select **Randomly**, click the **Select User/Group** picklist. The **Users** pop-up appears. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

**OR**

If required, you can also search for the desired user.

**Search By:** Select the desired option by which you wish to search for the user — User ID, Name. In the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

The selected users appear in the grid in the right pane. If you wish to remove the users, click **Delete**

 of the respective user.

- If you select **Access Group**, click the **Select User/Group** picklist. The **Access Group** pop-up appears. Select the check boxes of the desired groups. Select the header row check box to select all the groups on that page. Click **Ok**.

**OR**

If required, you can also search for the desired group.

**Search By:** Select the desired option by which you wish to search for the user — ID, Name. In the corresponding box enter the keyword. Click **Search** . The groups will be filtered as per the keyword. Select the check boxes of the desired groups. Select the header row check box to select all the groups on that page. Click **Ok**

The selected groups appear in the grid in the right pane. If you wish to remove the users, click **Delete**

 of the respective group.

Click **Export** to export the data.

## Templates

To create a Custom Template,

Click **Import Export > Export > Templates**. The **Templates** page appears.

Export

Export | Templates

Custom Template Name

Template Type User Configuration ▼

Add Field

| Sr. No. | Field Type | Field Name |  |
|---------|------------|------------|--|
|         |            |            |  |

Add

To add a new Template, click **Add**. Configure the following parameters:

- **Custom Template Name:** Configure a suitable name for the Custom Template.
- **Template Type:** Select the desired Template Type whose fields you wish to add to the Custom Template from the drop-down list.

Click **Add Field**. The **Export Field Configuration** pop-up appears.

Export Field Configuration

Fields User ID ▼

Display Name

Save Cancel

- **Fields:** Select the desired field to be added to the Custom Template. The fields will differ according to the selected Template Type. In a Custom Template, you can add the fields from a single Template Type only.
- **Display Name:** Configure a suitable Display Name for the selected field.

Click **Save**. The field will be added in the grid. Similarly, add the other desired fields.

Export

ExportTemplates

Custom Template Name

User Template

Template Type

User Configuration

Add Field

| Sr. No. | Field Type | Field Name |  |
|---------|------------|------------|--|
| 1       | User ID    | User ID    |  |

Save

Cancel

If you wish to remove the field, click  of the respective field.

Click **Save** to save the Custom Template or click **Cancel** to discard. All the configured Custom Templates appear in the **Template** drop-down list when you select **Template Type** as **Custom** under “[Export](#)”.

# Reports

---

Reports allows you to:

- generate the Alarm Report. For details, refer to [“Alarm”](#).
- generate the Device Report. For details, refer to [“Device”](#).
- generate the Access Policies Report. For details, refer to [“Access Policies”](#).
- generate the User Report. For details, refer to [“User”](#).
- generate the Elevator Access Control Report. For details, refer to [“Elevator Access Control”](#).
- generate the Event Report. For details, refer to [“Event”](#).



*The Reports will be generated in .xls format only.*

## Alarm

All the triggered alarms appear in the Alarm Report, if configured. For details, refer to [“Alarms”](#).

To generate the Alarm Report,

Click **Import Export > Report > Alarm**. The **Alarm** page appears.

The screenshot shows the 'Reports' interface with the 'Alarm' tab selected. It features a navigation bar with tabs for Alarm, Device, Access Policies, User, Elevator Access Control, and Event. Below the tabs, there is a 'Select Date' section with 'From Date' and 'To Date' input fields, each accompanied by a calendar icon. A 'Generate Report' button is positioned at the bottom center of the form.

Configure the following parameters:

- **Select Date:** Select the desired To and From date for which you wish to generate the report from the calendar.

Click **Generate Report**. The Alarm Report for the configured duration will be downloaded.

## Device

All the configured door details appear in the Device Report. For details, refer to [“Door Configuration”](#).

To generate the Device Report,

Click **Import Export > Report > Device**. The **Device** page appears.

The screenshot shows the 'Reports' interface with the 'Device' tab selected. It features a navigation bar with tabs for Alarm, Device, Access Policies, User, Elevator Access Control, and Event. Below the tabs, there is a 'Select Type' dropdown menu currently set to 'All'. A 'Generate Report' button is positioned at the bottom center of the form.

Configure the following parameters:

- **Select Type:** Select the desired Door Type for which you wish to generate the report. If you select **All**, the report will be generated for all the Door Types.

Click **Generate Report**. The Device Report for the selected Door Types will be downloaded.

## Access Policies

All the configured access policy details appear in the Access Policies Report. For details, refer to [“Access Policies”](#).

To generate the Access Policies Report,

Click **Import Export > Report > Access Policies**. The **Access Policies** page appears.

The screenshot shows a web application interface for generating reports. At the top, there is a 'Reports' header with tabs for 'Alarm', 'Device', 'Access Policies' (which is selected), 'User', 'Elevator Access Control', and 'Event'. Below this, there are two sub-tabs: 'Report' (selected) and 'Report Template'. The main area contains several configuration options: 'Select Date' with 'From Date' and 'To Date' fields and calendar icons; 'Type' set to 'Custom'; 'Event' set to 'Denied'; 'Rule' set to 'All'; 'Report Generation' set to 'Door Wise'; and 'Door' set to 'All'. Each dropdown menu has a downward arrow. At the bottom right, there is a 'Generate Report' button.

Access Policies allows you to:

- generate the Access Policies Report. For details, refer to [“Report”](#).
- configure custom Report Templates. For details, refer to [“Report Template”](#).

## Report

To generate the Access Policies Report,

Click **Import Export > Report > Access Policies > Report**. The **Report** page appears.

Configure the following parameters:

- **Select Date:** Select the desired To and From date for which you wish to generate the report from the calendar.
- **Type:** Select the desired Type according to which you wish to generate the report from the drop-down list options — Custom, Template Based.

If you select **Custom**, the report will be generated as per the default template.

If you select **Template Based**, the report will be generated as per the configured ["Report Template"](#).

- **Template:** If you select **Type** as **Template Based**, select the desired template you wish to use to generate the report from the drop-down list. All the templates created from ["Report Template"](#) appear in the list.
- **Event:** Select the desired Event for which you wish to generate the report from the drop-down list.
- **Rule:** Select the desired Access Policy according to which you wish to generate the report from the drop-down list.
- **Report Generation:** Select the desired option according to which you wish to generate the report from the drop-down list options — Door Wise, User Wise.
- **Door/User:** If you have selected **Report Generation** as **Door Wise/User Wise**, select the desired option— All or Randomly.

If you have selected **Door/User** as **Randomly**, click the **Door/Users** picklist. The Door/Users pop-up appears. Select the check boxes of the desired doors/users. Select the header row check box to select all the doors/users on that page. Click **Ok**.

**OR**



If required, you can also search for the desired users in the respective pop-up. **Search By:** Select the desired option by which you wish to search for the group — ID, Name. In the corresponding box enter the keyword. Click **Search**  . The groups will be filtered as per the keyword. Select the desired group.

If required, you can also search for the desired door in the respective pop-up. To do so, enter the keyword in the Search box. Click **Search**  . The doors will be filtered as per the keyword. Select the desired door.

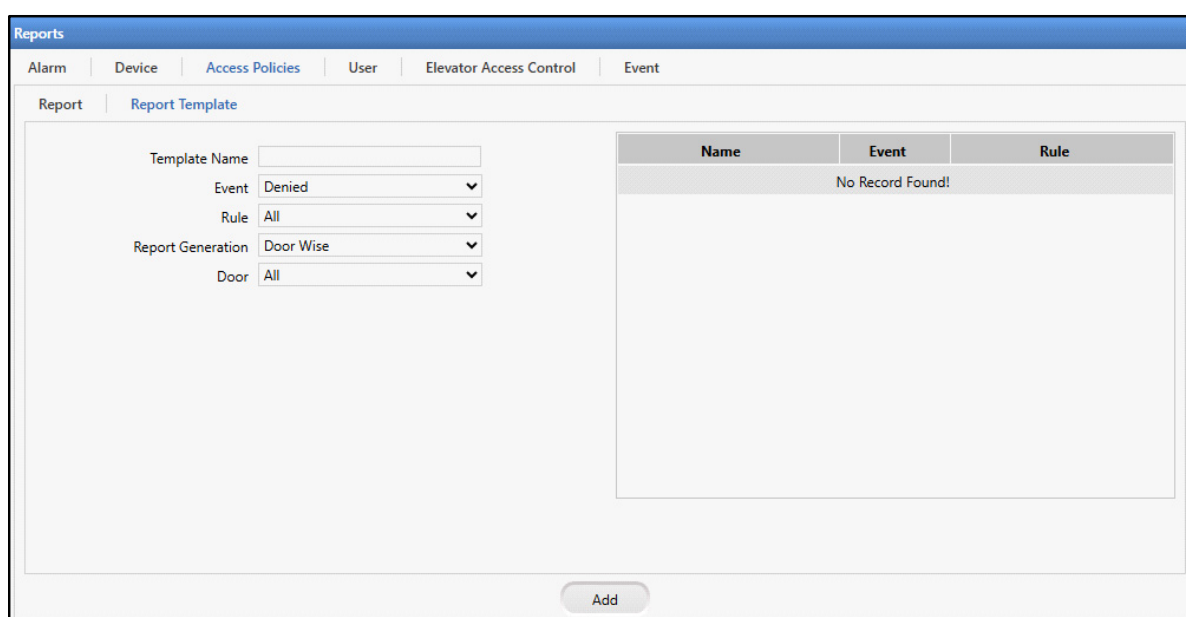
The selected doors/users appear in the grid in the right pane. If you wish to remove the doors/users, click **Delete**  of the respective door/user.

Click **Generate Report**. The Access Policies Report for the set filters will be downloaded.

## Report Template

To create a Custom Template,

Click **Import Export > Report > Access Policies > Report Template**. The **Report Template** page appears.



| Name             | Event | Rule |
|------------------|-------|------|
| No Record Found! |       |      |

To add a new Template, click **Add**. Configure the following parameters:

- **Template Name:** Configure a suitable name for the Template.
- **Event:** Select the desired Event according to which you wish to add Rules in the template from the drop-down list.
- **Rule:** Select the desired Rule which you wish to add in the template from the drop-down list. If you select **All**, then the report will be generated for all the Rules.
- **Report Generation:** Select the desired option according to which you wish to generate the report from the drop-down list options — Door Wise, User Wise.

- **Door/User:** If you have selected **Report Generation** as **Door Wise/User Wise**, select the desired option— All or Randomly.

If you have selected **Door/User** as **Randomly**, click the **Door/Users** picklist. Select the check boxes of the desired doors/users. Select the header row check box to select all the doors/users on that page. Click **Ok**. The selected doors/users appear in the grid.

**OR**

If required, you can also search for the desired user in the respective pop-up.

**Search By:** Select the desired option by which you wish to search for the user — User ID, Name. In the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

If required, you can also search for the desired door in the respective pop-up. To do so, enter the keyword in the Search box. Click **Search** . The doors will be filtered as per the keyword. Select the desired door.

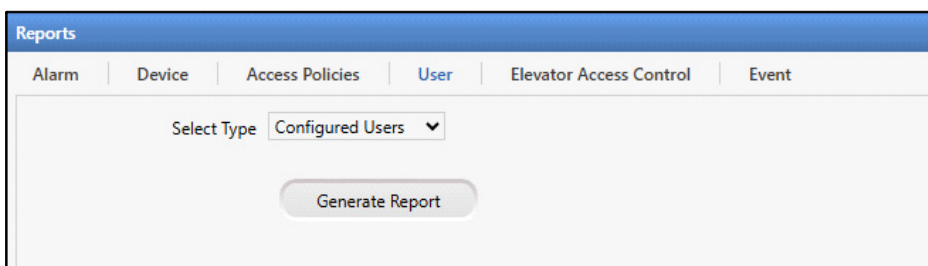
The selected doors/users appear in the grid. If you wish to remove the doors/users, click **Delete**  of the respective door/user.

Click **Save** to save the settings. The template will appear in the grid in the right pane. All the configured Templates appear in the **Template** drop-down list when you select **Type** as **Template Based** under “**Report**”.

## User

To generate the User Report,

Click **Import Export > Report > User**. The **User** page appears.



Configure the following parameters:

- **Select Type:** Select the desired User Type from the drop-down list.
- **Select Date:** If you have selected **Select Type** as **Blocked User/Who Is In**, select the desired To and From date for which you wish to generate the report from the calendar.
- **Door:** If you have selected **Select Type** as **Door Wise User**, select the desired doors for which you wish to generate the report from the drop-down list options — All, Randomly.

If you select **Randomly**, click the **Door** picklist. The **Door** pop-up appears. Select the check boxes of the desired doors. Select the header row check box to select all the doors on that page. Click **Ok**.

**OR**

If required, you can also search for the desired door. To do so, enter the keyword in the Search box. Click

**Search** . The doors will be filtered as per the keyword. Select the check boxes of the desired doors. Select the header row check box to select all the doors on that page. Click **Ok**.

The selected doors appear in the grid in the right pane. If you wish to remove the doors, click **Delete**  of the respective door.

- **User:** If you have selected **Select Type** as **User Wise Door/FP Enrollment Quality**, select the desired users for which you wish to generate the report from the drop-down list options — All, Randomly.

If you select **Randomly**, click the **User** picklist. The **Users** pop-up appears. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

**OR**

If required, you can also search for the desired user.

**Search By:** Select the desired option by which you wish to search for the user — User ID, Name. In the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

The selected users appear in the grid in the right pane. If you wish to remove the users, click **Delete**  of the respective user.

- **Zone:** If you have selected **Select Type** as **Who Is In**, select the desired zones for which you wish to generate the report from the drop-down list options — All, Randomly.

If you select **Randomly**, click the **Zone** picklist. The **Zone** pop-up appears. Select the check boxes of the desired zones. Select the header row check box to select all the zones on that page. Click **Ok**.

**OR**

If required, you can also search for the desired zone. To do so, enter the keyword in the Search box. Click

**Search** . The zones will be filtered as per the keyword. Select the check boxes of the desired zones. Select the header row check box to select all the zones on that page. Click **Ok**.

The selected zones appear in the grid in the right pane. If you wish to remove the zones, click **Delete**  of the respective zone.

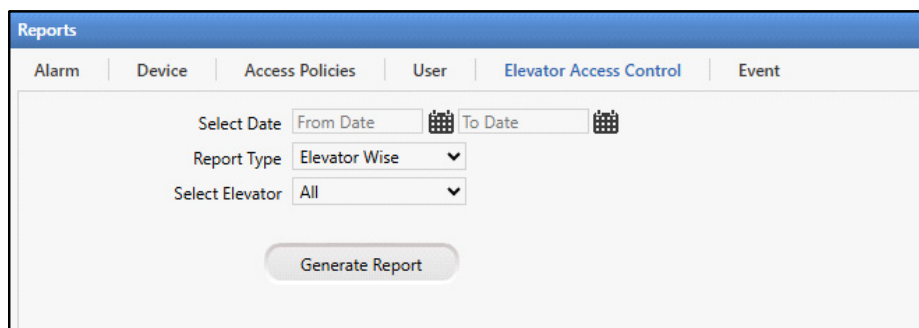
- **Enrollment Quality:** Configure the desired FP Enrollment Quality according to which you wish to generate the report.

Click **Generate Report**. The User Report for the set filters will be downloaded.

## Elevator Access Control

To generate the Elevator Access Control Report,

Click **Import Export > Report > Elevator Access Control**. The **Elevator Access Control** page appears.

The screenshot shows a web application interface for generating reports. At the top, there is a blue header bar with the word "Reports" on the left and a series of tabs: "Alarm", "Device", "Access Policies", "User", "Elevator Access Control" (which is highlighted in blue), and "Event". Below the tabs, there is a form area. It contains three rows of controls: "Select Date" with "From Date" and "To Date" text boxes and calendar icons; "Report Type" with a dropdown menu showing "Elevator Wise"; and "Select Elevator" with a dropdown menu showing "All". At the bottom of the form is a rounded button labeled "Generate Report".

Configure the following parameters:

- **Select Date:** Select the desired To and From date for which you wish to generate the report from the calendar.
- **Report Type:** Select the desired Report Type according to which you wish to generate the report from the drop-down list options — Elevator Wise, User Wise.
- **Select User:** If you have selected **Report Type** as **User Wise**, select the desired option— All or Randomly.

If you have selected **Select User** as **Randomly**, click the **User** picklist. The **Users** pop-up appears. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

**OR**

If required, you can also search for the desired user.

**Search By:** Select the desired option by which you wish to search for the user — User ID, User Name. In

the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

The selected users appear in the grid. If you wish to remove the users, click **Delete**  of the respective user.

- **Select Elevator:** If you have selected **Report Type** as **Elevator Wise**, select the desired option— All or Randomly.

If you have selected **Select Elevator** as **Randomly**, click the **Elevator** picklist. The Elevator pop-up appears. Select the desired elevator.

**OR**

You can also search for the desired elevator. To do so, enter the keyword in the Search box. Click **Search**

 . The elevators will be filtered as per the keyword. Select the desired elevator.

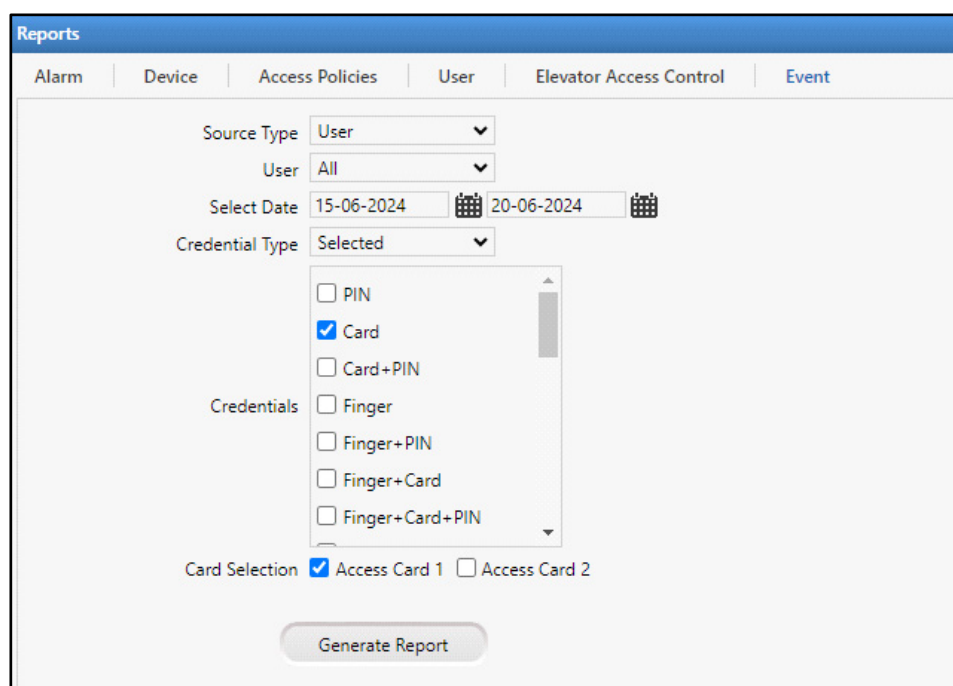
The selected elevator appear in the grid. If you wish to remove the elevators, click **Delete**  of the respective elevators.

Click **Generate Report**. The Elevator Access Control Report for the set filters will be downloaded.

## Event

To generate the Event Report,

Click **Import Export > Report > Event**. The **Event** page appears.



Configure the following parameters:

- **Source Type:** Select the desired Source Type from the drop-down list options — Door, User.
- **Door/User:** If you have selected **Source Type** as **Door/User**, select the desired option— All or Randomly.

If you have selected **Door/User** as **Randomly**, click the **Door/User** picklist. Select the check boxes of the desired doors/users. Select the header row check box to select all the doors/users on that page. Click **Ok**. The selected doors/users appear in the grid in the right pane.

**OR**

If required, you can also search for the desired user in the respective pop-up.

**Search By:** Select the desired option by which you wish to search for the user — User ID, Name. In the corresponding box enter the keyword. Click **Search**  . The users will be filtered as per the keyword.

Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

If required, you can also search for the desired door in the respective pop-up. To do so, enter the keyword in the Search box. Click **Search** . The doors will be filtered as per the keyword. Select the desired door.

The selected doors/users appear in the grid. If you wish to remove the doors/users, click **Delete**  of the respective door/user.

- **Select Date:** Select the desired To and From date for which you wish to generate the report from the calendar.
- **Credential Type:** If you have selected the **Source Type** as **User**, select the Credential Type for which you wish to generate report — All or Selected.
- **Credentials:** If you have selected **Credential Type** as **Selected**, select the check boxes for the desired Credentials for which you wish to generate report.
- **Card Selection:** If you have selected **Credentials** as **Card** or any combination of it, select the check box for the desired Card for which you wish to generate report — Access Card 1 or Access Card 2.

Click **Generate Report**. The Event Report for the set filters will be downloaded.

---

Alerts allows you to:

- configure the Alert Messages. For details, refer to [“Alert Message Configuration”](#).
- configure the Alert Servers. For details, refer to [“Alert Server Configuration”](#).

# Alert Message Configuration

The Alert Message Configuration allows you to configure Email and SMS alert messages for various events — Access Control, System, Alarm.

Make sure you have configured the Email ID and Mobile Number of the users to whom you wish to send Alerts under “Profile” in “User Configuration”.

To configure the Alert Messages,

Click **Alerts > Alert Message Configuration**. The **Alert Message Configuration** page appears.

| Alert Message Configuration                         |            |                |            |
|-----------------------------------------------------|------------|----------------|------------|
| Event                                               | Alert      | Alert Schedule | Recipients |
| User Allowed                                        | SMS, Email | Time Zone 1    | 1          |
| User Allowed - with Duress                          | SMS, Email | Time Zone 1    | 1          |
| User Allowed - Anti-Pass Back - Soft                | SMS, Email | Time Zone 1    | 1          |
| User Allowed - Smart Card Based Route Access - Soft | SMS, Email | Time Zone 1    | 1          |
| User Allowed - Panel Route Access - Soft            | SMS, Email | Time Zone 1    | 1          |
| User Denied - User Invalid                          | SMS, Email | Time Zone 1    | 0          |
| User Denied - Occupancy Control                     | SMS, Email | Time Zone 1    | 1          |
| User Denied - 2-Person Rule                         | SMS, Email | Time Zone 1    | 1          |
| User Denied - Time Out                              | SMS, Email | Time Zone 1    | 1          |
| User Denied - Anti-Pass Back                        | SMS, Email | Time Zone 1    | 1          |
| User Denied - Disabled User                         | SMS, Email | Time Zone 1    | 1          |
| User Denied - Blocked User                          | SMS, Email | Time Zone 1    | 1          |
| User Denied - First-IN User                         | SMS, Email | Time Zone 1    | 1          |
| User Denied - DND Enabled                           | SMS, Email | Time Zone 1    | 1          |

All the Events with the default Alerts (SMS, Email), Alert Schedule and Recipients appear in a list. You can edit the Alert configurations of the Events as per your requirement.

To edit the Event Alert configurations, click the desired Event from the list.

Alert Message Configuration

Event TypeAccess Control

EventUser Allowed

Active

AlertsSMSEmail

Alert ScheduleTime Zone

Time Zone1Time Zone 1

Message Preview

Recipients

SMS

Message<User Name> (ID: <User ID>): <Entry/ Exit> Allowed at <Door Name> on <Date - Time>

Default Message

(48/130)

Email

SubjectUser Allowed Access

Dear User,

Email<User Name> (ID: <User ID>): <Entry/ Exit> Allowed at <Door Name> on <Date - Time>

From System

Default Email

(195/300)

Default

Save

Cancel



Configure the following parameters:

- **Event Type:** It displays the Event Type as per the selected Event.



*When **Authorization on Enrollment** is enabled from “[Enrollment](#)” under “[Advanced Profile](#)”, then the Alert for **System Event- Authorization on Enrollment** will get enabled automatically for the Admin and HRD recipients.*

- **Event:** It displays the selected Event.



*If required, you can change the Event Type and then select the desired Event from the respective drop-down list. The parameters to be configured will differ as per the selected Event Type and Event.*

- **Active:** Select the check box to activate the Alert.
- **Alerts:** Select the check boxes of the Alerts — SMS, Email — that you wish to send.
- **Alert Schedule:** Select the desired option from the drop-down list according to which you wish to set the Alert Schedule — Time Zone, Time Zone Group.

If you select **Alert Schedule** as **Time Zone**, select the desired Time Zone.

- **Time Zone:** Click the **Time Zone** picklist. The **Time Zones** pop-up appears. Select the desired time zone.

**OR**

You can also search for the desired time zone. To do so, enter the keyword in the Search box. Click

**Search**  . The time zones will be filtered as per the keyword. Select the desired time zone.

If you select **Alert Schedule** as **Time Zone Group**, select the desired Time Zone Group.

- **Time Zone Group:** Click the **Select Time Zone Group** picklist. The **Time Zone Group** pop-up appears. All the Time Zone Groups configured from “[Group](#)” under “[Time Zone](#)” appear in the list. Select the desired Time Zone Group.

**OR**

You can also search for the desired time zone groups. To do so, enter the keyword in the Search box. Click

**Search**  . The time zone groups will be filtered as per the keyword. Select the desired time zone group.

The Alert will be sent according to the selected Time Zone/Time Zone Group.



*When client is situated in a time zone other than Alert Service's time zone, Alert Service will function as per the Tenant's time zone while processing Scheduled Tasks.*

Once the Alert configurations are done, you can edit the Alert Message content from “[Message Preview](#)” and select the “[Recipients](#)”.

## Message Preview

**SMS:** The default SMS content is displayed in the Message box. You can edit the text as per your requirement. We recommend you not to edit the tags. Click **Default Message** to revert the message content to default.

**Email:** The default Email content is displayed in the Subject and Email box. You can edit the text as per your requirement. We recommend you not to edit the tags. Click **Default Email** to revert the message content to default.

Click **Save** to save the settings or click **Cancel** to discard.

## Recipients

- **Send To:** Select the desired Recipients to whom you wish to send the Alerts — Individual, Selected Recipients, Both (Individual and Selected Recipients).
- **Individual:** The configured Alert will be sent to the user for whom event is generated. For example: If Access Allowed Event for the user James is generated; then the Alert message will be sent to James only.
- **Selected Recipients/Both (Individual and Selected Recipients):** Select the desired Recipients to whom you wish to send the Alert. Maximum 10 Recipients can be selected.
- **Recipient:** Click the **Select Recipients** picklist. The **User Selection** pop-up appears. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

OR

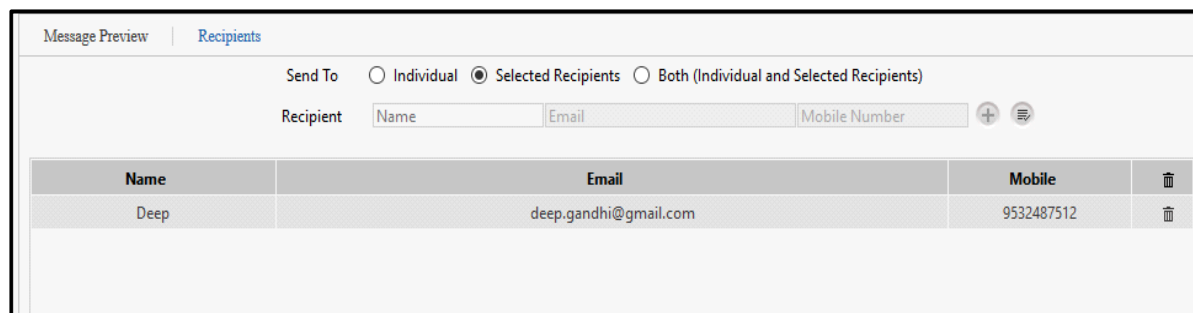
If required, you can also search for the desired user.

**Search By:** Select the desired option by which you wish to search for the user — Users, System Users. In the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Select the check boxes of the desired users. Select the header row check box to select all the users on that page. Click **Ok**.

The selected Recipients appear in the grid below.

Alternatively, you can also enter the Recipient's name or keyword in the search bar to search the desired Recipient. The list of matching users appears as you enter the text. Select the desired Recipient. The

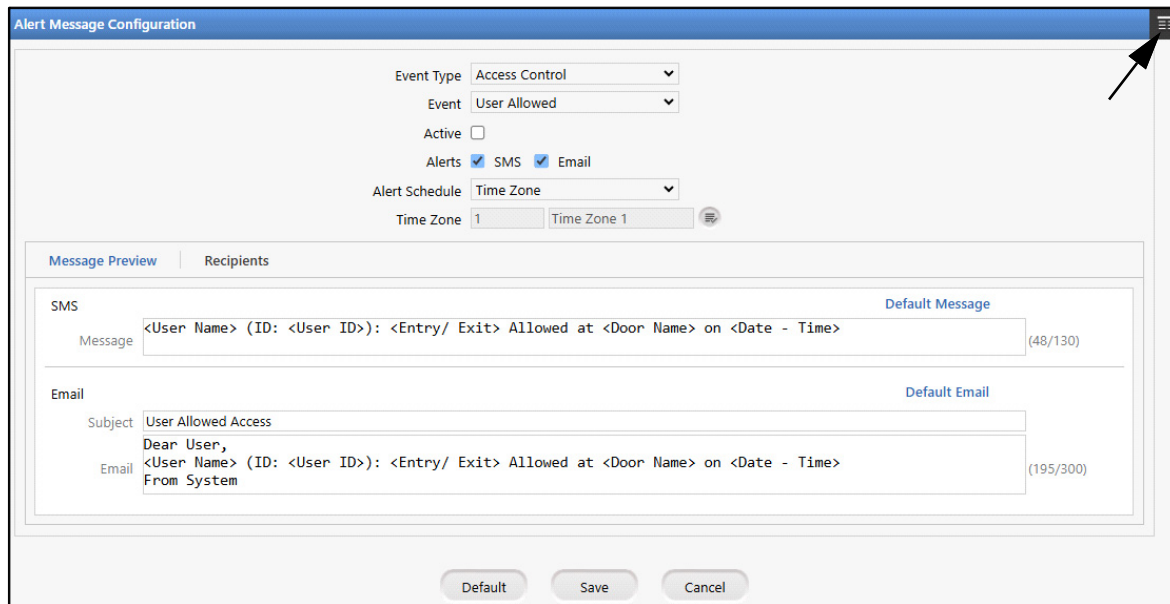
Email and Mobile Number appear in the respective fields, if configured. Click **Add Recipient** . The Recipient will appear in the grid below.



| Name | Email                 | Mobile     |                          |
|------|-----------------------|------------|--------------------------|
| Deep | deep.gandhi@gmail.com | 9532487512 | <input type="checkbox"/> |

Click **Save** to save the settings or click **Cancel** to discard.

After you have completed all the configurations of the Alert Message and if you wish to view the details of each Event's Alert Messages, click **View List** .



**Alert Message Configuration**

Event Type: Access Control  
 Event: User Allowed  
 Active: ☐  
 Alerts: ☒ SMS ☒ Email  
 Alert Schedule: Time Zone  
 Time Zone: 1 Time Zone 1

**Message Preview** | **Recipients**

**SMS** Default Message  
 Message: <User Name> (ID: <User ID>): <Entry/ Exit> Allowed at <Door Name> on <Date - Time> (48/130)

**Email** Default Email  
 Subject: User Allowed Access  
 Email: Dear User,  
 <User Name> (ID: <User ID>): <Entry/ Exit> Allowed at <Door Name> on <Date - Time> (195/300)  
 From System

Default Save Cancel

The Alert Message Configuration page displays all the Events with their Alerts, Alert Schedule and Recipients.

| Event                                               | Alert      | Alert Schedule | Recipients |
|-----------------------------------------------------|------------|----------------|------------|
| User Allowed                                        | SMS, Email | Time Zone 1    | 4          |
| User Allowed - with Duress                          | SMS, Email | Time Zone 1    | 1          |
| User Allowed - Anti-Pass Back - Soft                | SMS, Email | Time Zone 1    | 1          |
| User Allowed - Smart Card Based Route Access - Soft | SMS, Email | Time Zone 1    | 1          |
| User Allowed - Panel Route Access - Soft            | SMS, Email | Time Zone 1    | 1          |
| User Denied - User Invalid                          | SMS, Email | Time Zone 1    | 0          |
| User Denied - Occupancy Control                     | SMS, Email | Time Zone 1    | 1          |
| User Denied - 2-Person Rule                         | SMS, Email | Time Zone 1    | 1          |
| User Denied - Time Out                              | SMS, Email | Time Zone 1    | 1          |
| User Denied - Anti-Pass Back                        | SMS, Email | Time Zone 1    | 1          |
| User Denied - Disabled User                         | SMS, Email | Time Zone 1    | 1          |
| User Denied - Blocked User                          | SMS, Email | Time Zone 1    | 1          |
| User Denied - First-IN User                         | SMS, Email | Time Zone 1    | 1          |
| User Denied - DND Enabled                           | SMS, Email | Time Zone 1    | 1          |

1 2 3 4

# Alert Server Configuration

The Alert Server Configuration allows you to configure Email and SMS alerts for Access Control events, System events and Alarm events.

The Alert Server Configuration allows you to:

- configure the Email Settings. For details, refer to [“Email”](#).
- configure the SMS Settings. For details, refer to [“SMS”](#).

## Email

To configure the Email Settings,

Click **Alerts > Alert Server Configuration > Email**. The **Email** page appears.

Alert Server Configuration

Test Successful

Email | SMS

Enable ☒

Encryption (SSL) ☒

Server Address

Port  (1-65535)

User Name

Password

Sender's Email ID

Test Connection

Email ID  >

Default Save Cancel

Configure the following parameters:

- **Enable:** Select the check box to configure the Email settings.
- **Encryption (SSL):** Select the check box to enable encryption. In encrypted mode, the communication between PANEL200 and SMTP Server will be secured.
- **Server Address:** Configure the IP Address or Name of the configured SMTP Server.
- **Port:** Configure the TCP Port for the SMTP service as set in the SMTP Server. The default port is 25.
- **User Name:** Configure the username as set in the Email account.
- **Password:** Configure the password as set in the Email account.
- **Sender's Email ID:** Configure the Email ID of the sender.

## Test Connection

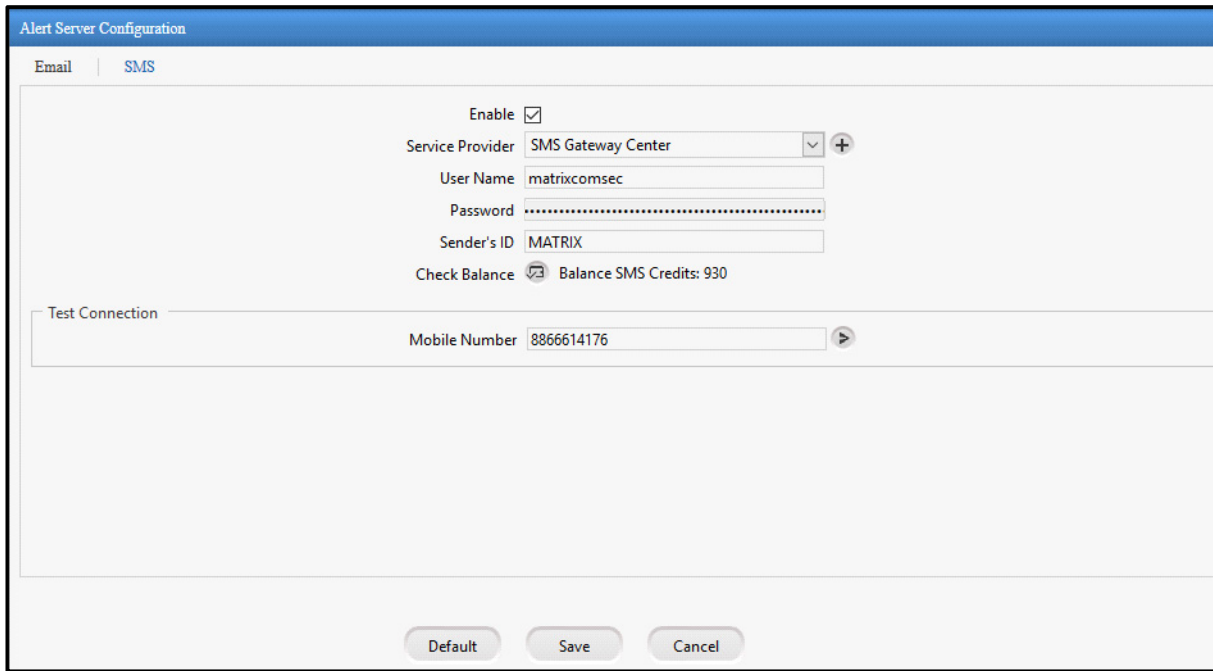
- **Email ID:** Configure the Email ID of the receiver to check the connectivity. Click **Send Message**  to send the test mail.

Click **Save** to save the settings or click **Cancel** to discard.

## SMS

To configure the SMS Settings,

Click **Alerts > Alert Server Configuration > SMS**. The **SMS** page appears.



Configure the following parameters:

- **Enable:** Select the check box to configure SMS settings.
- **Service Provider:** Select the desired Service Provider from the drop-down list. You can also configure 5 additional "[Custom Service Providers](#)". The configured Custom Service Providers appear in this list.  
Click **Edit** , if you wish to edit the parameters of the created Custom Service Provider.  
Click **Delete** , if you wish to delete the created Custom Service Provider.
- **User Name:** Configure the Username as provided to you by your SMS Service Provider.
- **Password:** Configure the Password as provided to you by your SMS Service Provider.
- **Sender's ID:** Configure the registered Sender ID.
- **Check Balance:** Click **Check Balance** to fetch the available SMS balance.

## Test Connection

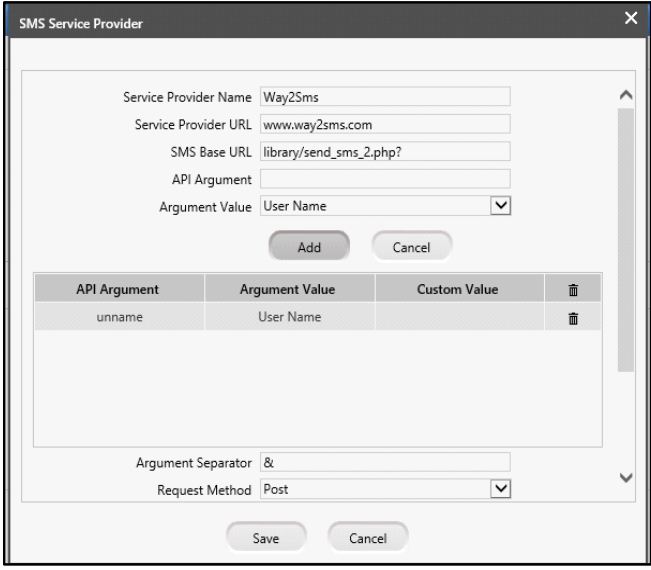
- **Mobile Number:** Configure the Mobile Number to which you wish to send the Test Message. Click **Send Message**  to send the test SMS.

Click **Save** to save the settings or click **Cancel** to discard.

## Custom Service Providers

You can configure upto 5 custom Service Providers.

Click **Add** . The **SMS Service Provider** pop-up appears.



The image shows a screenshot of the 'SMS Service Provider' configuration window. It contains several input fields for configuration: Service Provider Name (Way2Sms), Service Provider URL (www.way2sms.com), SMS Base URL (library/send\_sms\_2.php?), API Argument (empty), and Argument Value (User Name). Below these fields are 'Add' and 'Cancel' buttons. A table with 4 columns (API Argument, Argument Value, Custom Value, and a delete icon) is present, with one row showing 'uname' and 'User Name'. At the bottom, there are fields for 'Argument Separator' (&) and 'Request Method' (Post), along with 'Save' and 'Cancel' buttons.

| API Argument | Argument Value | Custom Value |  |
|--------------|----------------|--------------|--|
| uname        | User Name      |              |  |

Configure the following parameters:

- **Service Provider Name:** Configure the name of the Service Provider.
- **Service Provider URL:** Configure the Service Provider's Website used for registration.
- **SMS Base URL:** Configure the Base URL of the Service Provider. This is the URL to which arguments such as user name, password etc. are to be appended.
- **API Argument:** Configure the argument required to be mentioned while constructing the URL. You can add upto 10 API Arguments.
- **Argument Value:** Select a value to be mapped against the defined API Argument from the drop-down list. Select **Custom** to define a custom static value.
- **Custom Value:** Configure a custom value against the defined API Argument.

Click **Add** to add the new argument and value. The new argument and value appears in the grid below. Click **Delete** to delete the argument.

- **Argument Separator:** Define a character that can be used as a valid separator between arguments used to construct the API URL.
- **Request Method:** Select the method by which the request should be sent from the drop-down list.

If the **Request Method** is selected as **Post**, you can send long messages without any limitation.

If the **Request Method** is selected as **Web**, you can send short messages only.

- **Request Preview:** It displays the preview of URL, that is, Service Provider URL + SMS Base URL + SMS Arguments separated by argument separator in sequence.
- **Check Balance:** Select the check box to check the balance and configure the corresponding API.

Click **Save** to save the settings. The configured Service Provider appears in the **Service Provider** drop-down list under **"SMS"**.





---

Account Management allows you to:

- create Users and assign Access Rights to them. For details, refer to [“Users”](#).
- configure the Password Policy. For details, refer to [“Password Policy”](#).

# Users

To configure the Users,

Click **Account Management > Users**. The **Users** page appears.

| User | User Name | User Type |
|------|-----------|-----------|
| 1    | admin     | Admin     |
| 2    | hrd       | Hrd       |
| 3    | operator  | Operator  |
| 4    |           |           |
| 5    |           |           |
| 6    |           |           |
| 7    |           |           |
| 8    |           |           |
| 9    |           |           |
| 10   |           |           |

The Admin, HRD and Operator user accounts are created by default. You cannot edit these users. You can create upto 7 user accounts.

To create a new user account, click on the User Number from the right grid. Configure the following parameters:

- **Enable:** Select the check box to enable the user account.
- **User Name:** Configure a suitable user name.
- **User Type:** Select the User Type to be assigned to this user. The **"Access Rights"** of a user vary as per the selected User Type.
- **Password:** Configure the password for the user account according to the **"Password Policy"**.
- **Confirm Password:** Re-enter the password to confirm.
- **Email ID:** Configure the Email ID of the user.
- **Mobile Number:** Configure the Mobile Number of the user.

## Access Rights

The Access Rights for various features vary as per the selected User Type of the user. For example, if the User Type is selected as Admin, then by default, the Access Rights for all the features are granted.

Select or clear the check boxes of the desired features whose Access Rights you wish to grant or deny to the user.

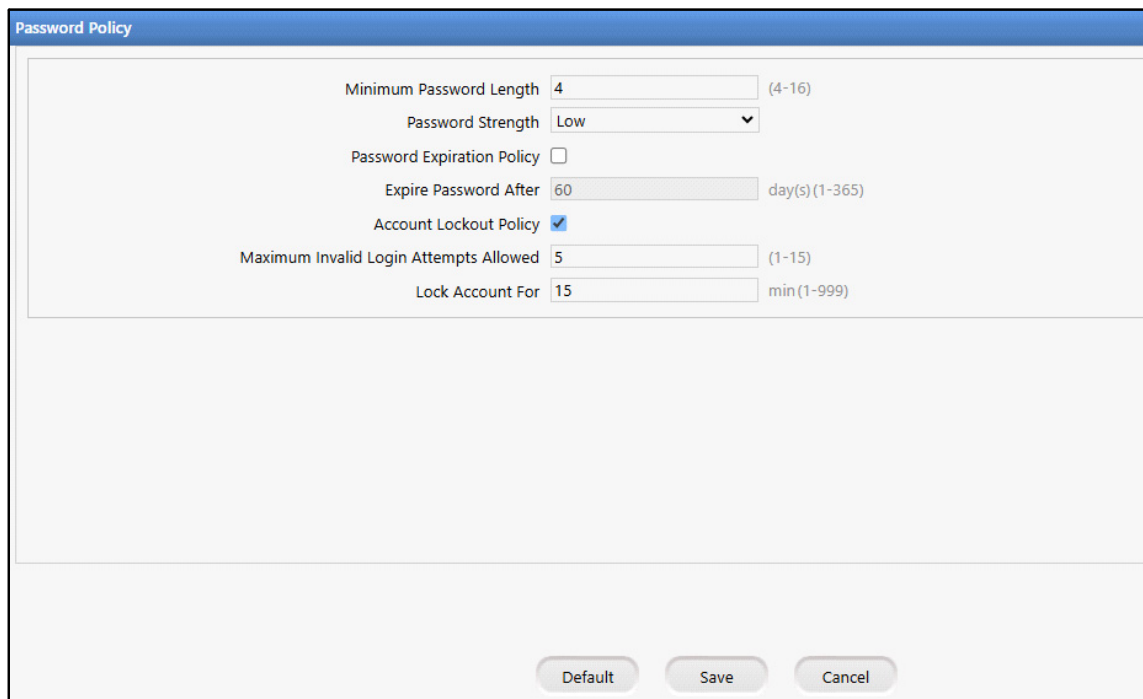
| Access Rights                                           |                                                        |
|---------------------------------------------------------|--------------------------------------------------------|
| Panel Configuration <input checked="" type="checkbox"/> | Access Policies <input checked="" type="checkbox"/>    |
| Devices <input checked="" type="checkbox"/>             | Access Schedule <input checked="" type="checkbox"/>    |
| Users <input type="checkbox"/>                          | Manage <input checked="" type="checkbox"/>             |
| Enrollment <input type="checkbox"/>                     | Enrollment Authorization <input type="checkbox"/>      |
| Account Management <input type="checkbox"/>             | Import Export <input checked="" type="checkbox"/>      |
| Masters <input type="checkbox"/>                        | Monitor <input type="checkbox"/>                       |
| Multi-Level Access <input type="checkbox"/>             | Change Password <input type="checkbox"/>               |
| Alerts <input type="checkbox"/>                         | Elevator Access Control <input type="checkbox"/>       |
| SNMP Configuration <input type="checkbox"/>             | Smart Elevator Access Control <input type="checkbox"/> |

Click **Save** to save the settings or click **Cancel** to discard.

# Password Policy

To configure the Password Policy,

Click **Account Management > Password Policy**. The **Password Policy** page appears.



Configure the following parameters:

- **Minimum Password Length:** Configure the minimum length of password as per your requirement.
- **Password Strength:** Select the desired Password Strength from the drop-down list. The Password Strength should be selected according to the Minimum Password Length.

The allowed characters for configuring Password vary as per the selected Password Strength. These are as below:

| Password Strength | Allowed Characters                                                                              |
|-------------------|-------------------------------------------------------------------------------------------------|
| Low               | No Restriction                                                                                  |
| Medium            | 1 Upper Case (A-Z), 1 Lower Case (a-z), 1 Number (0-9)                                          |
| High              | 1 Upper Case (A-Z), 1 Lower Case (a-z), 1 Number (0-9), 1 Special Character: _ . comma: @ ! + / |

- **Password Expiration Policy:** Select the check box if you wish that the password should be expired after the configured number of days.
- **Expire Password After:** Configure the number of days after which the password should expire.
- **Account Lockout Policy:** Select the check box if you wish that an account should be locked after certain failed login attempts.

- **Maximum Invalid Login Attempts Allowed:** Configure the number of maximum failed login attempts to be allowed to the user after which the account will be locked.
- **Lock Account For:** Configure the time period in minutes for which a user account remains locked after invalid login attempts. On expiry of this time, the user's account login will be restored.

Click **Save** to save the settings or click **Cancel** to discard.



---

The SNMP Configuration allows you to:

- configure the SNMP Settings. For details, refer to [“SNMP Settings”](#).
- configure the Notification Settings. For details, refer to [“Notification Settings”](#).

### **COSEC-Server Mode**

You can configure the following:

- configure the SNMP Settings. For details, refer to [“SNMP Settings”](#).
- configure the Notification Settings. For details, refer to [“Notification Settings”](#).

## **Simple Network Management Protocol (SNMP)**

Simple Network Management Protocol (SNMP) is an application-layer protocol used for exchanging management information between network devices. Using SNMP, you can manage and monitor network elements, audit network usage, detect network faults or inappropriate network access.

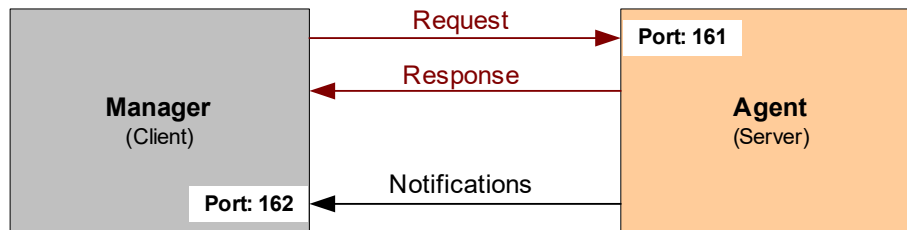
The SNMP architecture consists of:

1. Management Node (Agent)- PANEL200.
  2. Management Host (Manager)- Browser which monitors PANEL200.
  3. Management Information Base (MIB)- Information which is exchanged between Agent and Manager.
- **SNMP Agent** is a program that is bundled within the managed device. SNMP agent allows a managed device to collect the Management Information Base from the device and make it available to the SNMP Manager on request. It receives SNMP requests and generates SNMP responses or notifications (traps/informs). Also, an Agent can send Trap messages to the manager without any GetRequest command. In Trap messages there is no need of acknowledgement. The SNMP Agents are SNMP Servers. Here it is PANEL200.
  - **SNMP Manager**, usually the Network Management Station, communicates with multiple SNMP Agents implemented in the network. It generates SNMP requests and receives SNMP responses and notifications (traps/informs). When specific event occurs; a TRAP or Informed message will be sent to manager from Agent. The message can be Information, Warning or Error. The SNMP Manager is an SNMP Client. Here, it is the PC in which the SNMP Manager is installed and the Browser which monitors PANEL200.
  - **Management Information Base** is the commonly shared database between the Agent and the Manager. This information is known as managed objects. These managed objects are defined in MIB (Management Information Base) module. Any sort of status or information that can be accessed by the Manager is

defined in a MIB.

SNMP uses UDP (User Datagram Protocol) as the transport protocol for passing information between Managers and Agents. By default, the Agent listens on UDP port 161 for requests from Manager and the Manager listens on UDP port 162 for notification from Agent.

This SNMP Configuration page is used for configuring PANEL200 as an SNMP agent and to create Management Information Base (MIB) for SNMP.





# SNMP Configuration

SNMP Configuration allows you to configure PANEL200 as an SNMP agent and to create Management Information Base (MIB) for SNMP Manager.

The SNMP Configuration allows you to:

- configure the SNMP Settings. For details, refer to “[SNMP Settings](#)”.
- configure the Notification Settings. For details, refer to “[Notification Settings](#)”.

## MIB Files

MIB file manages all the information which is exchanged between Agent and Manager. Any sort of Status or Information that can be accessed by the manager is defined in the MIB. If the Manager needs to access any status or information about the client, the Manager must download and install the MIB files on the local disk.

To download these files,

- Click **Download MIB**.
- You will get a prompt with the option to open the file or save the file to a location. Save the file on the local disk.



You can **download MIB** file even if the *Enable* check box is unchecked.

## SNMP Settings

To configure the SNMP Settings,

Click **SNMP Configuration > SNMP Settings**. The **SNMP Settings** page appears.

SNMP Configuration

SNMP Settings | Notification Settings

Enable ☒

SNMP Listening Port  (1-65535)

SNMP Version

System Name

System Contact

System Location

Allow Access to SNMP Manager from

Community Name

Download MIB

Default Save Cancel

Configure the following parameters:

- **Enable:** Select the check box to enable SNMP settings.
- **SNMP Listening Port:** Configure the SNMP Listening Port.
- **SNMP Version:** Select the desired SNMP version as supported by your SNMP Manager from the drop-down list options — SNMPv1, SNMPv2c, SNMPv3.

SNMPv1: Trap message only (no need of acknowledgement).

SNMPv2c: Trap and Information (acknowledgement required) message both.

SNMPv3: Privacy enabled.

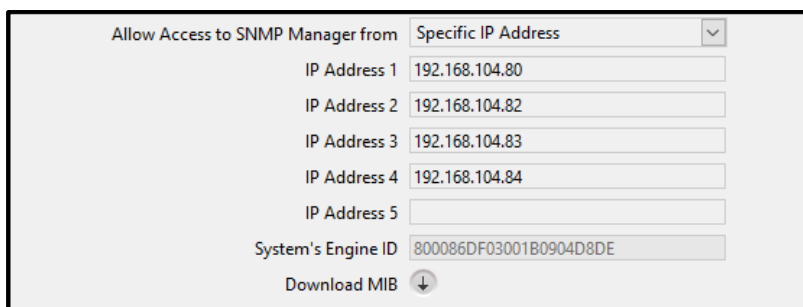
If you select **SNMPv3**, you need to configure the [“Security Settings”](#).

- **System Name:** Configure the System Name which is used to discover the PANEL200 in the network. Maximum 40 characters are allowed.
- **System Contact:** Configure the System Contact of a person which is used to contact in case of a notification. Maximum 40 characters are allowed.
- **System Location:** Configure the System Location where the PANEL200 is physically placed. Maximum 40 characters are allowed.
- **Allow Access to SNMP Manager from:** Select the desired option through which the SNMP Manager should access the PANEL200 from the drop-down list options — Any IP Address, Specific IP Address.

If you select **Allow Access to SNMP Manager from** as **Any IP Address**, then SNMP Manager can access the PANEL200 from any IP Address.

If you select **Allow Access to SNMP Manager from** as **Specific IP Address**, then SNMP Manager can access the PANEL200 from the configured **IP Address 1-5** only.

- **IP Address 1-5:** Configure the IP Addresses using which the SNMP Manager can access the PANEL200.



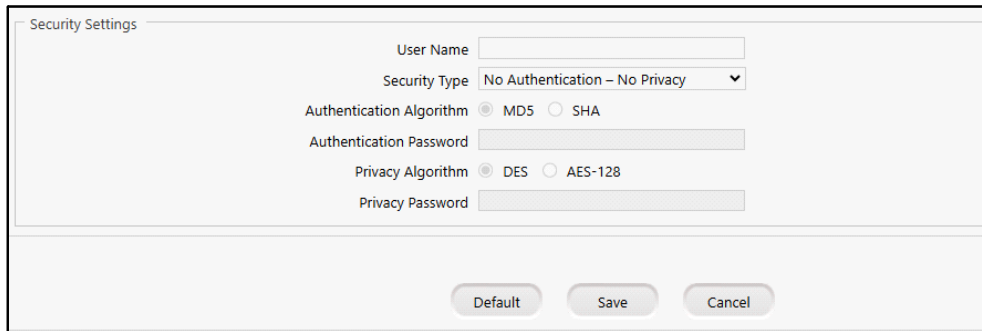
This is applicable for **GetRequest**, **GetNextRequest**, **GetBulkRequest** only.

- **System's Engine ID:** If you have selected **SNMP Version** as **SNMPv3**, the System's Engine ID is displayed. System's Engine ID is a unique identification of the PANEL200. It is a hexadecimal field with length of 22 characters consisting of Enterprise Number and PANEL200's MAC Address.
- **Community Name:** If you have selected **SNMP Version** as **SNMPv1/SNMPv2c**, configure the Community Name. The Community Name identifies the SNMP community in which the sender and

recipient of the message are located. It enables communication between PANEL200 and the SNMP Manager. Maximum 40 characters are allowed.

- **Download MIB:** Click **Download MIB** to download the MIB file. The MIB file manages all the information which is exchanged between SNMP Agent and SNMP Manager. Any sort of Status or Information that can be accessed by the manager is defined in the MIB.

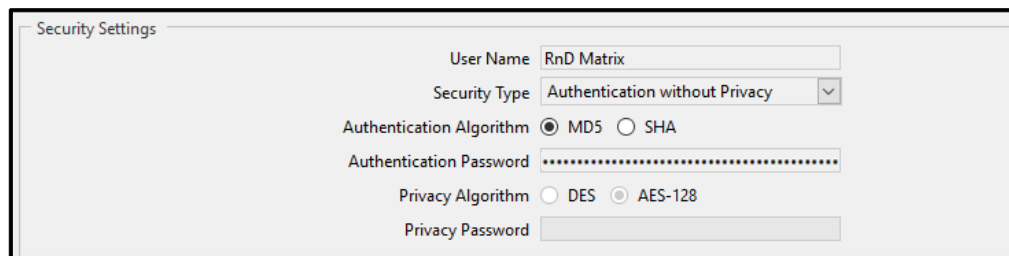
## Security Settings



The Security Settings dialog box contains the following fields and controls:

- User Name:** An empty text input field.
- Security Type:** A dropdown menu with the selected option "No Authentication – No Privacy".
- Authentication Algorithm:** Two radio buttons, "MD5" (selected) and "SHA".
- Authentication Password:** An empty text input field.
- Privacy Algorithm:** Two radio buttons, "DES" (selected) and "AES-128".
- Privacy Password:** An empty text input field.
- Buttons:** "Default", "Save", and "Cancel" buttons at the bottom.

- **User Name:** Configure the User Name which is used for Authentication and Privacy in SNMPv3. Maximum 40 characters are allowed.
- **Security Type:** Select the desired option from the drop-down list — No Authentication-No Privacy, Authentication without Privacy, Authentication with Privacy.
  - Select **No Authentication-No Privacy** when Authentication and Privacy are not required.
  - Select **Authentication without Privacy** when only Authentication is required. Incoming SNMP Messages will be authenticated in this case.
  - Select **Authentication with Privacy** when both Authentication and Privacy are required. Incoming SNMP Messages will be authenticated and encrypted-decrypted in this case.
- **Authentication Algorithm:** If you select **Security Type** as **Authentication without Privacy/ Authentication with Privacy**, select the desired Authentication Algorithm.
  - **MD5:** It is a message-digest algorithm which uses 128 bits and it is selected by default.
  - **SHA:** It is a Secure Hash Algorithm. It is a message-digest algorithm which uses 160 bits.



The Security Settings dialog box shows the following configured values:

- User Name:** "RnD Matrix"
- Security Type:** "Authentication without Privacy" (selected in dropdown)
- Authentication Algorithm:** "MD5" (selected radio button)
- Authentication Password:** A masked password field (dots)
- Privacy Algorithm:** "AES-128" (selected radio button)
- Privacy Password:** An empty text input field.

- **Authentication Password:** Configure the password used for Authentication with selected Authentication Algorithm.
- **Privacy Algorithm:** If you select **Security Type** as **Authentication with Privacy**, select the desired Privacy Algorithm.

- **DES:** It is an encryption-decryption method which uses 56 bits and it is selected by default.
- **AES-128:** It is an encryption-decryption method which uses 128 bits.
- **Privacy Password:** Configure the password used for Privacy with selected Privacy Algorithm.

Click **Save** to save the settings or click **Cancel** to discard.

## Notification Settings

To configure the SNMP Settings,

Click **SNMP Configuration > SNMP Settings**. The **SNMP Settings** page appears.

|               | Information                         | Warning                             | Alarm                               |
|---------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Door Events   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     |
| Alarm Events  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| System Events | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     |
| User Events   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     |

Configure the following parameters:

- **Enable Notification:** Select the check box to enable the Notifications. If this check box is enabled then PANEL200 will generate Notification message (Trap/Inform) as per the selected **SNMP Version** and **"Notification Filters"** when any error condition occurs.

For SNMPv1: Trap message is generated.

For SNMPv2c: Trap or Inform message is generated as selected in **Notification Type**.

For SNMPv3: Trap or Inform message is generated as selected in **Notification Type**.

- **Notification Type:** If you have selected **SNMP Version** as **SNMPv2c/SNMPv3**, select the desired Notification Type from the drop-down list.

If you want the PANEL200 to send notification message without acknowledgement, select **Trap**.

If you want the PANEL200 to send notification message with acknowledgement, select **Inform**.

- **Destination IP Address:** Configure the IP Address of the SNMP Manager where the Notifications should be received.

- **Destination Port:** Configure the port of the SNMP Manager where the Notifications should be received.
- **Retry Attempts:** If you have selected **Notification Type** as **Inform**, select the desired value of Retry Attempts from the drop-down list. Retry Attempts is the number of times the PANEL200 will retransmit the request if no acknowledge/response is received from Manager.
- **Retry Interval:** If you have selected **Notification Type** as **Inform**, configure the Retry Interval in seconds. Retry Interval specifies the time between retransmission of the request sent to the Manager if the response for the initial request from the Manager is not received by the system (Agent).

## Notification Filters

PANEL200 can send Trap/Inform Notifications to the SNMP Manager according to the set filters. Select the check boxes of the desired Events for which you wish to send Information, Warning or Alarm Notifications.

| Notification Filters |                                     |                                     |                                     |
|----------------------|-------------------------------------|-------------------------------------|-------------------------------------|
|                      | Information                         | Warning                             | Alarm                               |
| Door Events          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     |
| Alarm Events         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| System Events        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     |
| User Events          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     |

Click **Save** to save the settings or click **Cancel** to discard.



To change the password of PANEL200 and its doors,



*In COSEC-Server Mode you can configure the Change Password parameters.*

Click **Change Password**. The **Change Password** page appears.

The screenshot shows a web page titled "Change Password". It contains two main sections. The first section has three input fields labeled "Current Password", "New Password", and "Confirm New Password", followed by a "Save" button. The second section is titled "HRD Password" and contains a "Default HRD Password" button with a user icon. Below this is a section titled "Panel Door - Admin Password" with "New Password" and "Confirm New Password" input fields, followed by another "Save" button.



*Make sure the Password is configured as per the ["Password Policy"](#).*

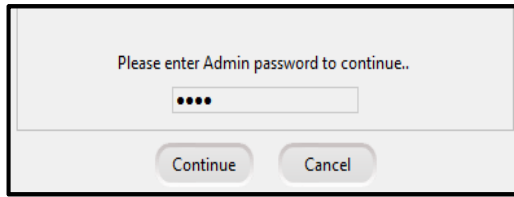
Configure the following parameters:

- **Current Password:** Configure the current password of PANEL200.
- **New Password:** Configure the new password. Allowed Characters: **A-Z a-z 0-9-\_.comma:!/+/**.
- **Confirm New Password:** Re-enter the new password to confirm.

Click **Save** to save the settings.

### HRD Password

Click **Default HRD Password** to set the HRD user login password to default. The following pop-up appears.

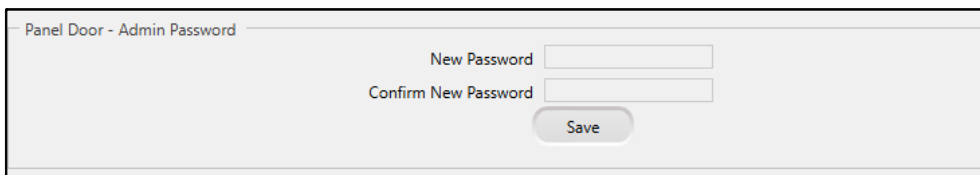
A dialog box with a light gray background and a black border. At the top, it says "Please enter Admin password to continue..". Below this is a text input field containing four black dots. At the bottom, there are two buttons: "Continue" on the left and "Cancel" on the right.

Enter the Admin login password.

Click **Continue** to confirm or click **Cancel** to discard.

## Panel Door-Admin Password

You can also change the password of the Admin user of the connected doors.

A configuration window titled "Panel Door - Admin Password". It has a light gray background and a black border. Inside, there are two text input fields. The first is labeled "New Password" and the second is labeled "Confirm New Password". Below these fields is a "Save" button.

- **New Password:** Configure the new password.
- **Confirm New Password:** Re-enter the new password to confirm.

Click **Save** to save the settings.



The Storage Details displays the status of internal storage of the PANEL200 and external storage.

To view the Storage Details,

Click **Storage Details**. The **Storage Details** page appears.

| Storage Details               |                |                 |
|-------------------------------|----------------|-----------------|
| Storage Type                  | Used Space(MB) | Total Space(MB) |
| Internal Storage              | 73864          | 222488          |
| External Storage(Memory Card) | 103168         | 15549952        |

The details displayed are — Storage Type, Free Space and Total Space.



On encountering 90% or above storage usage for External Storage, the **Device Storage** alert will be triggered, if configured. In [“Alert Message Configuration”](#), select Event Type as **System** and Event as **Device Storage**.

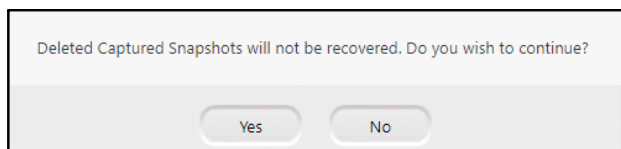
### Captured Snapshot Details

The count of captured snapshots for user events if configured appears here.

| Storage Details               |                |                         |
|-------------------------------|----------------|-------------------------|
| Storage Type                  | Used Space(MB) | Total Space(MB)         |
| Internal Storage              | 61             | 217                     |
| External Storage(Memory Card) | 3191           | 15176                   |
| Captured Snapshots Details    |                |                         |
| Captured Snapshots Count      | 3              | <button>Delete</button> |

You can delete the snapshots, if required.

- Click **Delete** to delete the captured snapshots. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

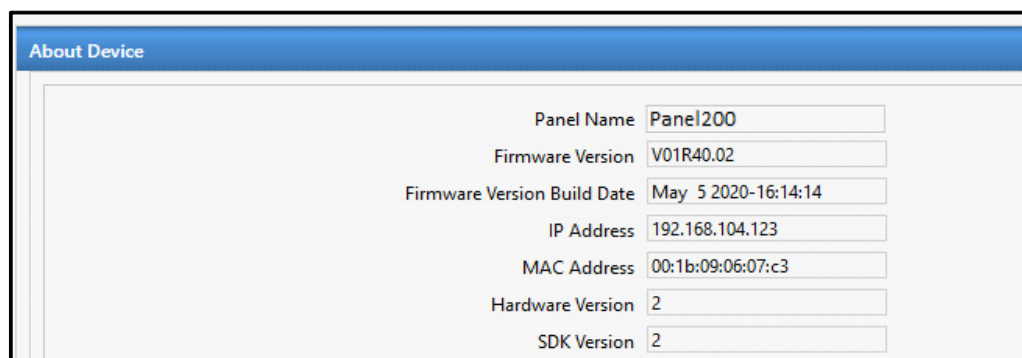


*All the captured snapshots will be deleted automatically when:*

- *the PANEL200 mode is changed.*
- *the PANEL200 is set to system/factory default.*

To view the PANEL200 details,

Click **About Device**. The **About Device** page appears.



The screenshot shows a web interface titled "About Device" in a blue header. Below the header, the following details are displayed in a light gray box:

|                             |                     |
|-----------------------------|---------------------|
| Panel Name                  | Panel200            |
| Firmware Version            | V01R40.02           |
| Firmware Version Build Date | May 5 2020-16:14:14 |
| IP Address                  | 192.168.104.123     |
| MAC Address                 | 00:1b:09:06:07:c3   |
| Hardware Version            | 2                   |
| SDK Version                 | 2                   |

The details displayed are — Panel Name, Firmware Version, Firmware Version Build Date, IP Address, MAC Address, Hardware Version and SDK Version.



---

Monitor and Event Logs allows you to:

- view the door status, IO links, Alarms, Live Events and Time Trigger functions. For details, refer to [“Monitor”](#).
- view the Event Logs. For details, refer to [“Event Logs”](#).

# Monitor

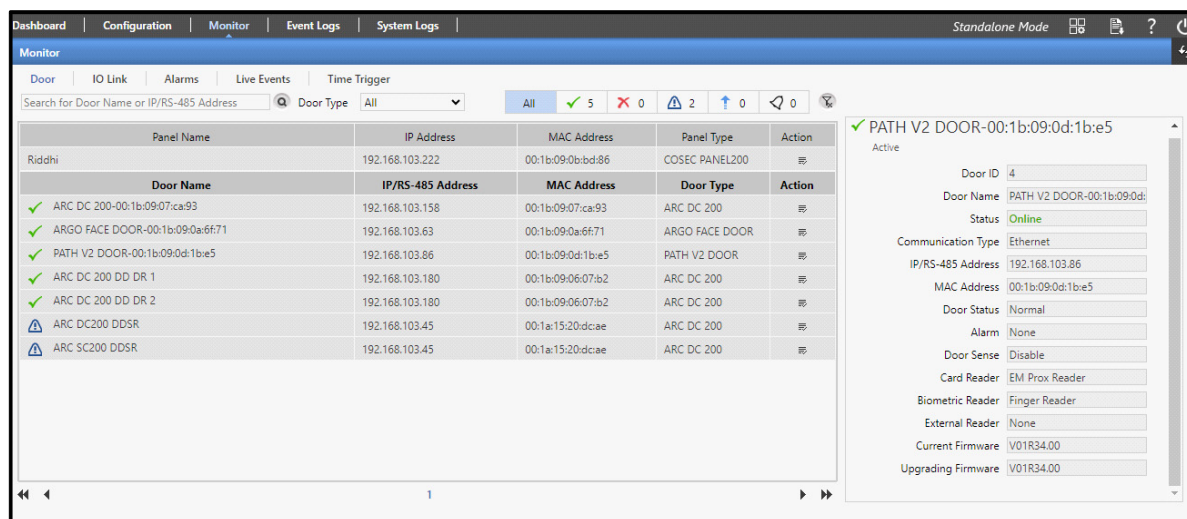
Monitor allows you to:

- view the door status and details. For details, refer to “[Door](#)”.
- view the IO Links. For details, refer to “[IO Link](#)”.
- view the Alarms. For details, refer to “[Alarms](#)”.
- view the Live Events. For details, refer to “[Live Events](#)”.
- view the Time Trigger functions. For details, refer to “[Time Trigger](#)”.

## Door

To view the door status and details,

Click **Monitor > Door**. The **Door** page appears.



By default, the details of PANEL200 and all the connected doors displayed are — Panel Name/Door Name, IP Address/IP/RS-485 Address, MAC Address, Panel Type/Door Type and Action.

You can search for the desired door whose status you wish to view. To do so,

- Enter the desired keyword according to which you wish to search the door. The doors will be filtered as per the entered keyword.

**OR**

- Alternatively, you can also select the desired door type from the **Door Type** drop-down list. The doors will be filtered as per the selected Door Type.

**OR**

- The doors can also be filtered on the basis of their **Status**. Click on the desired Status option — All, Online Devices  , Offline Devices  , Devices in Degrade State  , Upgrading Device  , Alarms on

Device  . Against each door Status, the numeric value displays the number of doors of respective status type.

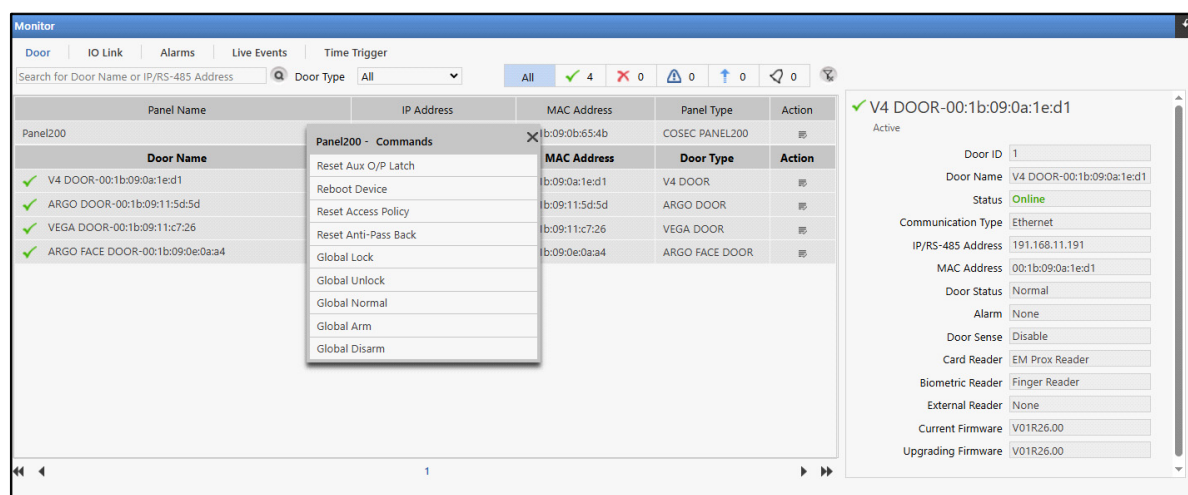
As per the selected filter, the doors appear in the grid. Hover-over the door whose details you wish to view from the grid. The details of the door are displayed in the right pane.

Click **Clear Filter**  to clear the filters.

You can also send commands to the PANEL200 and its connected doors. Different doors have different sets of commands.

For PANEL200,

- **Action:** Click **Select Command** under Action for the PANEL200. The list of commands appears. Select the desired command to be executed by the PANEL200 — Reset Aux O/P Latch, Reboot Device, Reset Access Policy, Reset Anti-Pass Back, Global Lock, Global Unlock, Global Normal, Global Arm, Global Disarm.



The screenshot shows the 'Monitor' interface with a 'Door' tab selected. A table lists connected devices, including a PANEL200 and several doors. A context menu is open over the PANEL200, showing a list of commands: Reset Aux O/P Latch, Reboot Device, Reset Access Policy, Reset Anti-Pass Back, Global Lock, Global Unlock, Global Normal, Global Arm, and Global Disarm. On the right, the details for 'V4 DOOR-00:1b:09:0a:1e:d1' are displayed, showing its status as 'Online' and various configuration parameters like IP/RS-485 Address, MAC Address, and Door Status.

| Panel Name                        | IP Address | MAC Address        | Panel Type       | Action        |
|-----------------------------------|------------|--------------------|------------------|---------------|
| PANEL200                          |            |                    |                  |               |
| <b>Door Name</b>                  |            | <b>MAC Address</b> | <b>Door Type</b> | <b>Action</b> |
| ✓ V4 DOOR-00:1b:09:0a:1e:d1       |            | b:09:0a:1e:d1      | V4 DOOR          |               |
| ✓ ARGO DOOR-00:1b:09:11:5d:5d     |            | b:09:11:5d:5d      | ARGO DOOR        |               |
| ✓ VEGA DOOR-00:1b:09:11:c7:26     |            | b:09:11:c7:26      | VEGA DOOR        |               |
| ✓ ARGO FACE DOOR-00:1b:09:0e:0aa4 |            | b:09:0e:0aa4       | ARGO FACE DOOR   |               |

For Door,

- **Action:** Click **Select Command** under Action for the desired door. The list of commands appears. Select the desired command to be executed by the door.

The screenshot shows the 'Monitor' interface with tabs for Door, IO Link, Alarms, Live Events, and Time Trigger. The 'Door' tab is active, displaying a list of doors. A context menu is open for the door 'ARGO FACE DOOR-00:1b:09:0a:6f:71', showing various commands like 'Normalize Door', 'Lock Door', 'Unlock Door', etc. The detailed view on the right shows the door is 'Active' and provides details like Door ID, Door Name, Status (Online), Communication Type (Ethernet), IP/RS-485 Address, MAC Address, Door Status (Normal), Alarm (None), Door Sense (Disable), Card Reader (EM Prox Reader), External Reader (None), Current Firmware (V01R20.00), and Upgrading Firmware (V01R20.00).

## IO Link

To view the IO Links,

Click **Monitor > IO Links**. The **IO Link** page appears.

Monitor

Door

IO Link

Alarms

Live Events

Time Trigger

| Link No. | Link Name    | Output Type | Reset IO Link                                                                         |
|----------|--------------|-------------|---------------------------------------------------------------------------------------|
| 1        | User Allowed | Latch       |  |

All the active IO Links appear on this page. The details displayed are — Link No., Link Name, Output Type, Reset IO Link.

Click **Reset IO Link** against the desired IO Link to reset the link. Only those IO Links which have Output Type as **Latch** can be reset.

## Alarms

To view the Alarms,



*Make sure the desired alarms are configured in “Advanced Profile” and “Door Configuration”.*

Click **Monitor > Alarms**. The **Alarms** page appears.



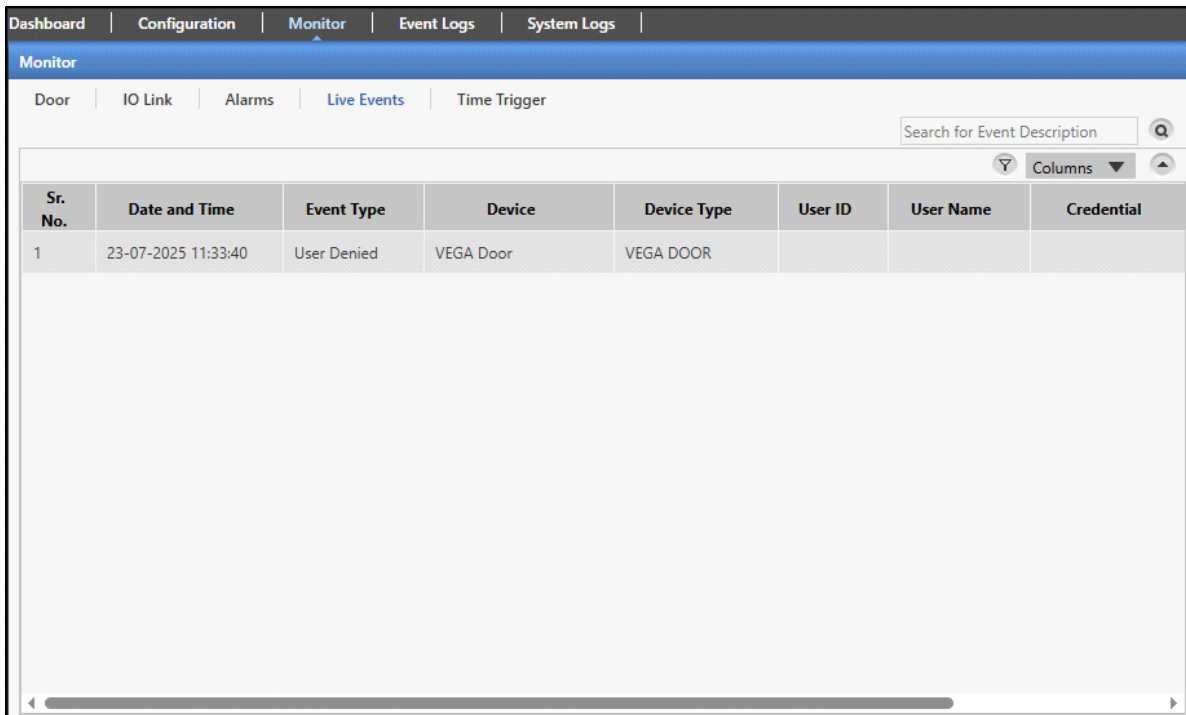


## Live Events

Live Events page enables you to view the live occurrence of events of various doors. These events are automatically updated as they occur.

To view the Live Events,

Click **Monitor > Live Events**. The **Live Events** page appears.



| Sr. No. | Date and Time       | Event Type  | Device    | Device Type | User ID | User Name | Credential |
|---------|---------------------|-------------|-----------|-------------|---------|-----------|------------|
| 1       | 23-07-2025 11:33:40 | User Denied | VEGA Door | VEGA DOOR   |         |           |            |

All the Live Events appear in the grid. By default, the details displayed are — Sr. No., Date and Time, Event Type, Device, Device Type, User ID, User Name and Description. You need to select the **Credential** and **Entry/Exit** columns from “[Select Columns](#)” to view the details of these columns.

### Select Columns

You can select the columns which should be displayed or hidden in the Live Event grid as per your requirement. Click **Columns** drop-down list. By default, the **Credential** and **Entry/Exit** check boxes are cleared, that is these columns are hidden. Select or clear the check boxes of the columns which should be displayed or hidden from the Live Event grid respectively.

Monitor

Door | IO Link | Alarms | Live Events | Time Trigger

Search for Event Description

Columns

| Sr. No. | Date and Time       | Event Type   | Device    | Device Type | User ID | User Name | Credential | Entry/Exit | Description |
|---------|---------------------|--------------|-----------|-------------|---------|-----------|------------|------------|-------------|
| 3       | 23-07-2025 14:11:56 | Door         | VEGA Door | VEGA DOOR   | u1      | u1        |            |            |             |
| 2       | 23-07-2025 14:11:54 | Door         | VEGA Door | VEGA DOOR   |         |           |            |            |             |
| 1       | 23-07-2025 14:11:51 | User Allowed | VEGA Door | VEGA DOOR   | u1      | u1        |            |            |             |

Column Settings

☒ Date and Time

☒ Event Type

☒ Device

☒ Device Type

☒ User ID

☒ User Name

☐ Credential

☐ Entry/Exit

☒ Description

Filter Events

You can filter these events according to — Event Type, Device, Device Type, User ID, User Name, Credential.

To do so,

- Click **Filter**  in the header row.

Dashboard

Configuration

Monitor

Event Logs

System Logs

Monitor

Door

IO Link

Alarms

Live Events

Time Trigger

Search for Event Description

Columns

| Sr. No. | Date and Time       | Event Type  | Device    | Device Type | User ID | User Name | Credential |
|---------|---------------------|-------------|-----------|-------------|---------|-----------|------------|
| 1       | 23-07-2025 11:33:40 | User Denied | VEGA Door | VEGA DOOR   |         |           |            |

Individual filters appear on the header rows of the respective columns.

| Monitor                      |               |            |             |              |         |           |            |
|------------------------------|---------------|------------|-------------|--------------|---------|-----------|------------|
| Door                         | IO Link       | Alarms     | Live Events | Time Trigger |         |           |            |
| Search for Event Description |               |            |             |              |         |           | Q          |
|                              |               |            |             |              |         |           | Columns    |
| Sr. No.                      | Date and Time | Event Type | Device      | Device Type  | User ID | User Name | Credential |

- Click on **Filter** of the desired column to filter the Live Events. The **Filter**  icon toggles to **Clear Filter**  icon.
- If you click **Filter** of the **Event Type**, **Device Type** and/or **Credential**, then select the check boxes of the desired options according to which you wish to filter the Live Events.
- If you click **Filter** of the **User ID**, **User Name** and/or **Device**, the **Users/Devices** pop-up appears. Select the check boxes of the desired users/doors. If you wish to select all the users/doors, select the header row check box.

The Live Events will appear according to the set filters.

Once the Live Events Logs are fetched in the grid, you can perform the following functions — “[Search](#)” and “[Clear Filter](#)”.

## Search

You can search for the desired Live Events using the Search bar. Enter the keyword (upto 30 characters) according to which you wish to search. The search will be carried out in the Description column only. Click **Search**  The Live Events will be filtered as per the entered keyword.



*Make sure the check box for **Description** column under “[Clear Filter](#)” is selected to use the search functionality.*

## Clear Filter

Click **Clear Filter**  to clear all the set filters.

## Time Trigger

To view the Time Trigger Functions,

Click **Monitor > Time Trigger**. The **Time Trigger** page appears.

| Monitor |         |            |             |              |
|---------|---------|------------|-------------|--------------|
| Door    | IO Link | Alarms     | Live Events | Time Trigger |
| Name    |         | Start Time | End Time    | Output Port  |
| test4   |         | 10:43:00   | 04:55:15    | Door Unlock  |
|         |         |            |             | Reset        |

All the active Time Trigger functions appear on this page. The details displayed are — Name, Start Time, End Time, Output Port, Reset.

Click **Reset**  against the desired Time Trigger function to reset it.

# Event Logs

Event Log allows you to view the details of occurrence of events, such as User Allowed, User Denied, Door events, Alarm events, System events etc., along with the date and time of their occurrence.

To view the Event Logs,

Click **Event Logs**. The **Logs** page appears.

The screenshot shows the 'Event Logs' page in a software interface. On the left, there are filter sections: 'Search by' with a 'Date and Time' range (From: 25-07-2025 00:00, To: 25-07-2025 23:59), 'Event Type' with checkboxes for User Allowed, User Denied, System, Alarm, and Door, and 'Event Filter' with dropdowns for Device Type, Device, User, and Credential. A 'Clear Filter' button is below. At the bottom left is a 'Backup' section with 'Save Log On PC' and a file format dropdown set to 'xls'. On the right, a table titled 'Logs' displays event data. The table has columns: Date and Time, Event Type, Device, Device Type, User ID, User Name, and Description. Two rows of data are visible. A 'Columns' dropdown is in the top right of the table area. Navigation arrows and a page number '1' are at the bottom of the table.

| Date and Time       | Event Type | Device   | Device Type    | User ID | User Name | Description                |
|---------------------|------------|----------|----------------|---------|-----------|----------------------------|
| 25-07-2025 10:11:25 | System     | Panel200 | COSEC PANEL200 |         |           | Master Controller Power ON |
| 25-07-2025 10:11:25 | Door       |          |                |         |           | Door status unlocked       |

You can set the following filters in **Search by** to view the Event Logs — “Date and Time”, “Event Type” and “Event Filter”.

Configure the following parameters:

## Date and Time

- **From:** Select the date from which you wish to view the Event Logs from the calendar and specify the time.
- **To:** Select the date till which you wish to view the Event Logs from the calendar and specify the time.

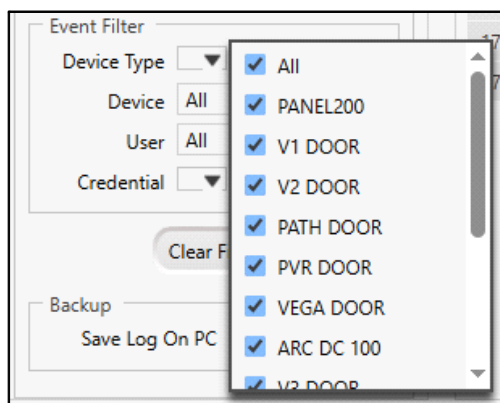
Click **Apply**.

## Event Type

Select the check boxes for the desired Event Type — User Allowed, User Denied, Door, Alarm, System — for which you wish to view the Event Logs.

## Event Filter

- **Device Type:** Click the drop-down list and select the check boxes of the desired doors for which you wish to view the events.



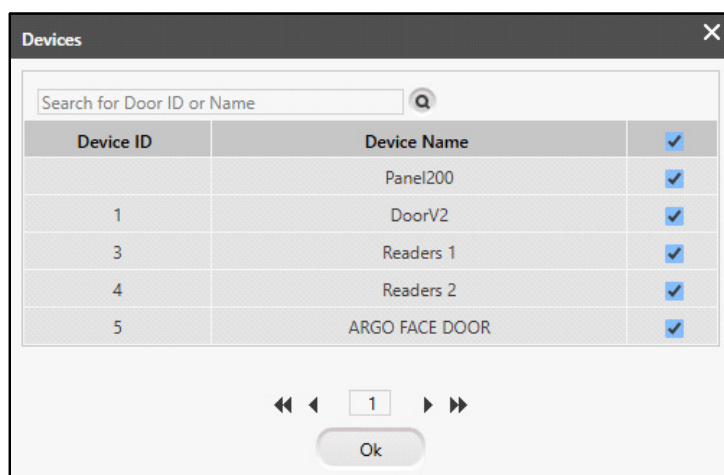
- **Device:** Select the desired option from the drop-down list — All, Randomly — on the basis of which you wish to view the events.

If you select **Randomly**, click the picklist. The **Devices** pop-up appears. Select the check boxes of the desired doors. If you wish to select all the doors, select the header row check box. Click **Ok**.

**OR**

You can also search for the desired door. To do so, enter the keyword in the Search box. Click **Search**

 . The doors will be filtered as per the keyword. Select the check boxes of the desired doors. If you wish to select all the doors, select the header row check box. Click **Ok**.



- **User:** Select the desired option from the drop-down list — All, Randomly — on the basis of which you wish to view the events.

If you select **Randomly**, click the picklist. The **Users** pop-up appears. Select the check boxes of the desired users. If you wish to select all the users, select the header row check box. Click **Ok**.

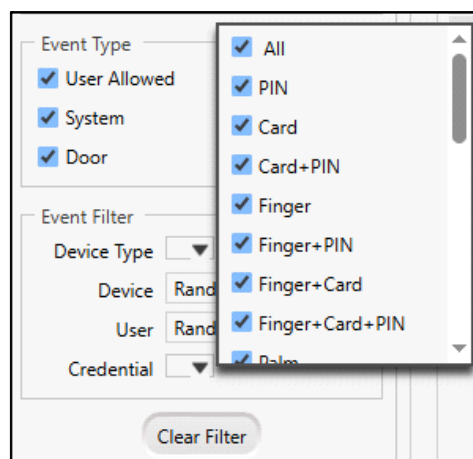
**OR**

If required, you can also search for the desired user.

**Search By:** Select the desired option by which you wish to search for the user — User ID, User Name. In the corresponding box enter the keyword. Click **Search** . The users will be filtered as per the keyword. Select the check boxes of the desired users. If you wish to select all the users, select the header row check box. Click **Ok**.



- **Credential:** Click the drop-down list and select the check boxes of the desired Credentials for which you wish to view the events.



The Event Logs will appear as per the set filters.



Search for Event Description

Search by  
Date and Time  
From 01-07-2025 00:00  
To 25-07-2025 23:59  
Apply

Event Type  
☒ User Allowed ☒ User Denied  
☒ System ☒ Alarm  
☒ Door

Event Filter  
Device Type  
Device Randomly  
User Randomly  
Credential  
Clear Filter

Backup  
Save Log On PC xls

Logs

| Date and Time       | Event Type | Device         | Device Type    | User ID | User Name | Credential | Entry/Exit | Description       |
|---------------------|------------|----------------|----------------|---------|-----------|------------|------------|-------------------|
| 16-07-2025 15:02:31 | System     | Panel200       | COSEC PANEL200 |         |           |            |            | Master Controller |
| 16-07-2025 15:02:46 | Door       | ARGO FACE Door | ARGO FACE DOOR |         |           |            |            | Door controller   |
| 01-07-2025 09:32:50 | System     | Panel200       | COSEC PANEL200 |         |           |            |            | Master Controller |
| 01-07-2025 10:00:08 | System     | Panel200       | COSEC PANEL200 |         |           |            |            | Master Controller |
| 01-07-2025 10:24:13 | System     | Panel200       | COSEC PANEL200 |         |           |            |            | Master Controller |
| 01-07-2025 15:13:10 | Door       | ARGO FACE Door | ARGO FACE DOOR |         |           |            |            | Door controller   |
| 01-07-2025 15:14:56 | Door       | ARGO FACE Door | ARGO FACE DOOR |         |           |            |            | Door controller   |
| 01-07-2025 15:15:04 | Door       | ARGO FACE Door | ARGO FACE DOOR |         |           |            |            | Door controller   |
| 01-07-2025 17:04:33 | Door       | ARGO FACE Door | ARGO FACE DOOR |         |           |            |            | Door controller   |
| 01-07-2025 17:04:40 | Door       | ARGO FACE Door | ARGO FACE DOOR |         |           |            |            | Door controller   |
| 01-07-2025 17:26:48 | Door       | ARGO FACE Door | ARGO FACE DOOR |         |           |            |            | Door controller   |
| 01-07-2025 18:00:37 | Door       | ARGO FACE Door | ARGO FACE DOOR |         |           |            |            | Door controller   |
| 02-07-2025 09:39:46 | System     | Panel200       | COSEC PANEL200 |         |           |            |            | Master Controller |
| 02-07-2025 09:40:06 | Door       | ARGO FACE Door | ARGO FACE DOOR |         |           |            |            | Door controller   |
| 02-07-2025 09:40:10 | Door       | ARGO FACE Door | ARGO FACE DOOR |         |           |            |            | Door controller   |

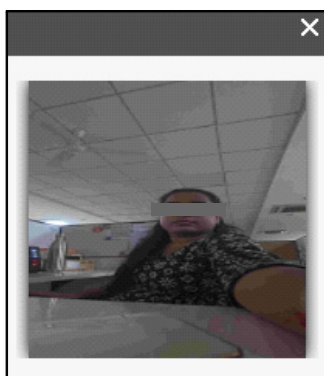
1 2 3 4 5 6 7 8 9 10

The details displayed are — Date and Time, Event Type, Device, Device Type, User ID, User Name, Credential, Entry/Exit, Description and Snapshot Image .



*The Snapshot Image Icon will appear enabled only for Captured Snapshot.*

Click **Snapshot Image**  to view the captured snapshots on user events. A pop-up with the captured snapshot appears.



These snapshots are captured on user events as configured. For more details, refer to [“Built-In Camera”](#).



*The complete face images will not be visible due to security reasons in this document.*

*On exceeding 98% of the External Memory (refer [“Storage Details”](#)), PANEL will not save the captured snapshots and on clicking **Snapshot Image** icon, a blank pop-up will be displayed.*

*On clicking **Snapshot Image** icon for events for which snapshot has been deleted or not saved, a blank pop-up will be displayed.*

Once the Event Logs are fetched in the grid, you can perform the following functions — [“Search”](#), [“Select Columns”](#) and [“Clear Filter”](#).

You can also take the [“Backup”](#) of the Event Logs.

## Search

You can search for the desired Event Logs using the Search bar. Enter the keyword (upto 30 characters) according to which you wish to search. The search will be carried out in the Description column only. Click **Search** . The Event Logs will be filtered as per the entered keyword.



Make sure the check box for **Description** column under “**Select Columns**” is selected to use the search functionality.

## Select Columns

You can select the columns which should be displayed or hidden in the Event Log grid as per your requirement. Click **Columns** drop-down list. By default, the **Credential** and **Entry/Exit** check boxes are cleared, that is these columns are hidden. Select or clear the check boxes of the columns which should be displayed or hidden from the Event Log grid respectively.

| Logs                |            |          |                |         |           |                               | Columns ▾                                         |
|---------------------|------------|----------|----------------|---------|-----------|-------------------------------|---------------------------------------------------|
| Date and Time       | Event Type | Device   | Device Type    | User ID | User Name | Description                   | Column Settings                                   |
| 16-07-2025 15:02:31 | System     | Panel200 | COSEC PANEL200 |         |           | Master Controller             | <input checked="" type="checkbox"/> Date and Time |
| 16-07-2025 15:02:31 | Door       |          |                |         |           | Door status unlo              | <input checked="" type="checkbox"/> Event Type    |
| 16-07-2025 15:02:46 | Door       | DoorV2   | V2 DOOR        |         |           | Door controller C             | <input checked="" type="checkbox"/> Device        |
| 01-07-2025 09:32:50 | System     | Panel200 | COSEC PANEL200 |         |           | Master Controller             | <input checked="" type="checkbox"/> Device Type   |
| 01-07-2025 09:32:50 | Door       |          |                |         |           | Door status unlo              | <input checked="" type="checkbox"/> User ID       |
| 01-07-2025 09:47:05 | Door       |          |                |         |           | Door controller C             | <input checked="" type="checkbox"/> User Name     |
| 01-07-2025 10:00:08 | System     | Panel200 | COSEC PANEL200 |         |           | Master Controller             | <input type="checkbox"/> Credential               |
| 01-07-2025 10:00:08 | Door       |          |                |         |           | Door status unlo              | <input type="checkbox"/> Entry/Exit               |
| 01-07-2025 10:00:15 | System     | Panel200 | COSEC PANEL200 |         |           | Update of Firmw               | <input checked="" type="checkbox"/> Description   |
| 01-07-2025 10:24:13 | System     | Panel200 | COSEC PANEL200 |         |           | Master Controller Power ON    |                                                   |
| 01-07-2025 10:24:13 | Door       |          |                |         |           | Door status unlocked          |                                                   |
| 01-07-2025 10:24:20 | System     | Panel200 | COSEC PANEL200 |         |           | Update of Firmware Successful |                                                   |
| 01-07-2025 10:34:44 | Door       |          |                |         |           | Door controller ON Line       |                                                   |
| 01-07-2025 10:34:44 | Door       |          |                |         |           | Door controller ON Line       |                                                   |
| 01-07-2025 10:34:44 | Door       |          |                |         |           | Door controller ON Line       |                                                   |

## Clear Filter

Click **Clear Filter** to clear all the applied filters.

## Backup

- **Save Log On PC:** Select desired format in which the backup of the Event Log is to be taken from the drop-down list options — xls, csv or text. Click **Save**  to save the file at the desired location.

---

## *Appendix*

---

### Supported OSDP Commands and Responses

#### Terminologies Used

| Abbreviations | Description                                                        |
|---------------|--------------------------------------------------------------------|
| PD            | Peripheral Devices                                                 |
| CP            | Control Panel                                                      |
| ACU           | Access Control Unit                                                |
| APDU          | Application Protocol Data Unit                                     |
| SCS           | Secure Channel Session                                             |
| SPE           | Secure PIN Entry                                                   |
| AES           | Advanced Encryption Standard                                       |
| CBC           | Cypher Block Chaining                                              |
| cUID          | Client's Unique Identifier                                         |
| ICV           | Initial Chaining Vector                                            |
| MK            | Master Key                                                         |
| PGM           | Portable Grey Map                                                  |
| SCBK          | Secure Channel Base Key                                            |
| MAC           | Message Authentication Code                                        |
| S-ENC         | Session Key for ensuring data confidentiality (message encryption) |
| S-MAC1        | Session Key for Message Authentication, key 1                      |
| S-MAC2        | Session Key for Message Authentication, key 2                      |
| C-MAC         | Command MAC (for packets from ACU to PD)                           |
| R-MAC         | Reply MAC (for packets from PD to ACU)                             |

Given below is the list of supported “[Commands](#)” and “[Responses](#)”.

## Commands

- [“Poll \(osdp\\_POLL\)”](#)
- [“ID Report Request \(osdp\\_ID\)”](#)
- [“Peripheral Device Capabilities Request \(osdp\\_CAP\)”](#)
- [“Local Status Report Request \(osdp\\_LSTAT\)”](#)
- [“Reader LED Control Command \(osdp\\_LED\)”](#)
- [“Reader Buzzer Control Command \(osdp\\_BUZ\)”](#)
- [“Communication Configuration Command \(osdp\\_COMSET\)”](#)
- [“Encryption Key Set Command \(osdp\\_KEYSET\)”](#)
- [“Challenge and Secure Session Initialization Request \(osdp\\_CHLNG\)”](#)
- [“Server’s Random Number and Server Cryptogram \(osdp\\_SCRIPT\)”](#)

### Poll (osdp\_POLL)

This command serves as a general inquiry. The PD may return any reply that is marked as a possible "poll response". Normally, the PD will return any unreported input data or status change information as a poll response.

| Packet Format Field | Code    | Name      |
|---------------------|---------|-----------|
| CMND                | 0x60    | osdp_POLL |
| DATA                | Omitted |           |

### ID Report Request (osdp\_ID)

This command requests the return of the PD ID Report. The id request code parameter may request the extended form of the PD ID block.

| Packet Format Field | Code | Name                      |
|---------------------|------|---------------------------|
| CMND                | 0x61 | osdp_ID                   |
| DATA                | 0x00 | Send Standard PD ID Block |

For response refer to [“Device Identification Report \(osdp\\_PDID\)”](#).

### Peripheral Device Capabilities Request (osdp\_CAP)

This command requests the PD to return a list of its functional capabilities, such as the type and number of input points, outputs points, reader ports, etc.

| Packet Format Field | Code | Name                |
|---------------------|------|---------------------|
| CMND                | 0x62 | osdp_CAP            |
| DATA                | 0x00 | Send Standard Reply |

For response refer to [“Device Capabilities Report \(osdp\\_PDCAP\)”](#)

## Local Status Report Request (osdp\_LSTAT)

This command instructs the PD to reply with a local status report.

| Packet Format Field | Code    | Name       |
|---------------------|---------|------------|
| CMND                | 0x64    | osdp_LSTAT |
| DATA                | Omitted |            |

For response refer to [“Local Status Report \(osdp\\_LSTATR\)”](#).

## Reader LED Control Command (osdp\_LED)

This command controls the LEDs associated with one or more readers.

Once the temporary command's timer expires the LED will revert to the last permanent state set. The permanent command is volatile (does not transcend power cycles).

The LED will flash, alternating between the color specified for ON and color specified for OFF at the rate specified by the corresponding timers. Setting both color codes to the same value will produce a steady (non-flashing) output.

The 16-bit timer applies to the temporary LED commands only.

The LED Control Command message packet may contain multiple 14-byte records. The PD should use the total message length to determine the number of records present. The number of records should not exceed the number of LEDs as reported in [“Function Code 4 – Reader LED Control”](#); however the upper limit should not exceed the receive buffer size of the PD as reported in [“Function Code 10 – Receive BufferSize”](#).

Records containing an invalid Reader/LED number will result in a 0x09 error reply.

If the ACU sets a Temporary Setting and tries to establish another Temporary Setting, then a new Temporary Command should override a currently active temporary command.

The ON Time OFF Time values cannot both be set to zero.

| Packet Format Field | Code | Name     | Meaning |
|---------------------|------|----------|---------|
| CMND                | 0x69 | osdp_LED |         |

| Packet Format Field                        | Code                                                                     | Name          | Meaning                                                                                      |
|--------------------------------------------|--------------------------------------------------------------------------|---------------|----------------------------------------------------------------------------------------------|
| DATA<br>14 bytes repeated 1 or more times. | 0x00 = First Reader<br>0x01 = Second Reader<br>etc.                      | Reader Number |                                                                                              |
|                                            | 0x00 = first LED<br>0x01 = second LED<br>etc.                            | LED Number    |                                                                                              |
|                                            | Temporary Settings                                                       |               |                                                                                              |
|                                            | Refer to "Temporary Control Code Values"                                 | Control Code  | The mode to enter temporarily                                                                |
|                                            | 0x00 – 0xFF                                                              | ON time       | An 8 bit ON duration of the flash, in units of 100 ms<br><br>A zero value means no duration  |
|                                            | 0x00 – 0xFF                                                              | OFF time      | An 8 bit OFF duration of the flash, in units of 100 ms<br><br>A zero value means no duration |
|                                            | Refer to "Color Values"                                                  | ON color      | The color to set during the ON time                                                          |
| DATA<br>14 bytes repeated 1 or more times. | Refer to "Color Values"                                                  | OFF color     | The color to set during the OFF time                                                         |
|                                            | Refer to details mentioned under "Reader LED Control Command (osdp_LED)" | Timer (LSB)   | A 16 bit timer value, in units of 100 ms<br>A zero value means "forever"                     |
|                                            |                                                                          | Timer (MSB)   |                                                                                              |
|                                            | Permanent Settings                                                       |               |                                                                                              |
|                                            | Refer to "Permanent Control Code Values"                                 | Control Code  | The mode to return to after the timer expires,                                               |
|                                            | 0x00 – 0xFF                                                              | ON time       | An 8 bit ON duration of the flash, in units of 100 ms<br><br>A zero value means no duration  |
|                                            | 0x00 – 0xFF                                                              | OFF time      | An 8 bit OFF duration of the flash, in units of 100 ms<br><br>A zero value means no duration |
|                                            | Refer to "Color Values"                                                  | ON color      | The color to set during the ON time.                                                         |
|                                            | Refer to "Color Values"                                                  | OFF color     | The color to set during the OFF time                                                         |

## Temporary Control Code Values

| Temporary Control Code Value | Meaning                                                                                                              |
|------------------------------|----------------------------------------------------------------------------------------------------------------------|
| 0x00                         | NOP – do not alter this LED's temporary settings. The remaining values of the temporary settings record are ignored. |
| 0x01                         | Cancel any temporary operation and display this LED's permanent state immediately                                    |
| 0x02                         | Set the temporary state as given and start timer immediately.                                                        |

## Permanent Control Code Values

| Permanent Control Code Value | Meaning                                                                                                              |
|------------------------------|----------------------------------------------------------------------------------------------------------------------|
| 0x00                         | NOP – do not alter this LED's permanent settings. The remaining values of the temporary settings record are ignored. |
| 0x01                         | Set the permanent state as given.                                                                                    |

## Color Values

| Color Value                                                                                                                                                                                                                                                | Meaning           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| 0                                                                                                                                                                                                                                                          | Black (off/unlit) |
| 1                                                                                                                                                                                                                                                          | Red               |
| 2                                                                                                                                                                                                                                                          | Green             |
| 3                                                                                                                                                                                                                                                          | Amber             |
| 4                                                                                                                                                                                                                                                          | Blue              |
| 5                                                                                                                                                                                                                                                          | Magenta           |
| 6                                                                                                                                                                                                                                                          | Cyan              |
| 7                                                                                                                                                                                                                                                          | White             |
| The reply can be any of the following: <ul style="list-style-type: none"><li>osdp_ACK as described in <a href="#">“Positive Acknowledgment (osdp_ACK)”</a></li><li>osdp_NAK as described in <a href="#">“Negative Acknowledgment (osdp_NAK)”</a></li></ul> |                   |

Examples:

To cause the first LED on the first Reader to flash red (100 ms) / black (200 ms) for 3 seconds, then resume its current display mode:

0, 0, 2, 1, 2, 1, 0, 30, 0, 0, 0, 0, 0, 0

To set the reader's second LED to display a steady green output

0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 2, 2

## Reader Buzzer Control Command (osdp\_BUZ)

This command defines commands to a single, monotone audible annunciator (beeper or buzzer) that may be associated with a reader.

The permanent command is volatile (does not transcend power cycles).

A record that contains an invalid Reader Number will result in a 0x09 error reply.

| Packet Format Field                       | Code                                                                                                                             | Name          | Meaning                                                                                                   |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------|-----------------------------------------------------------------------------------------------------------|
| CMND                                      | 0x6A                                                                                                                             | osdp_BUZ      |                                                                                                           |
| DATA<br>5 bytes repeated 1 or more times. | 0x00 = First Reader<br>0x01 = Second Reader<br>etc.                                                                              | Reader Number |                                                                                                           |
|                                           | 0x00 = no tone (off) – use of this value is deprecated. 0x01 = off<br>0x02 = default tone<br>0x03-0xFF = Reserved for future use | Tone Code     | Requested Tone State                                                                                      |
|                                           | 0x00 – 0xFF                                                                                                                      | On Time       | The ON duration of the sound, in units of 100 ms. Must be nonzero unless the tone code is 0x01 (off.)     |
|                                           | 0x00 – 0xFF                                                                                                                      | OFF Time      | The OFF duration of the sound, in units of 100 ms                                                         |
|                                           | 0x00 – 0xFF                                                                                                                      | Count         | The number of times to repeat the ON/OFF cycle. 0 = tone continues until another tone command is received |

## Communication Configuration Command (osdp\_COMSET)

This command sets the PD's communication parameters. The settings will take effect AFTER the PD has completed its response to this command. It is recommended that communication parameters set by this command (address, baud rate) are non-volatile.

If the PD is unable to comply, it will return the values that it will use after the completion of this reply.

| Packet Format Field | Code        | Name          | Meaning                                                                                                                    |
|---------------------|-------------|---------------|----------------------------------------------------------------------------------------------------------------------------|
| CMND                | 0x6E        | osdp_COMSET   |                                                                                                                            |
| DATA 5 bytes        | 0x00 – 0x7E | Address       | Unit ID to which this PD will respond after the change takes effect.                                                       |
|                     | 0x00 – 0xFF | Baud Rate LSB | The baud rate is expressed as a 32-bit integer holding the actual value of the baud rate to use, such as 9600, 38400, etc. |
|                     | 0x00 – 0xFF | Baud Rate     |                                                                                                                            |
|                     | 0x00 – 0xFF | Baud Rate     |                                                                                                                            |
|                     | 0x00 – 0xFF | Baud Rate MSB |                                                                                                                            |



For response, refer to “[Communication Configuration Report \(osdp\\_COM\)](#)”.

## Encryption Key Set Command (osdp\_KEYSET)

This command transfers an encryption key from the ACU to a PD.

| Byte                      | Name     | Meaning                                | Value                          |
|---------------------------|----------|----------------------------------------|--------------------------------|
| 0                         | Key_Type | Encryption method to use with this key | 0x01 – Secure Channel Base Key |
| 10                        | Length   | Number of bytes of key data            | (Key Length in bits + 7) / 8   |
| 2- (2+Length)             | Data     | Key data                               | Any                            |
| Reply: osdp_ACK, osdp_NAK |          |                                        |                                |

### Note:

The following notes apply to Key\_Type = 0x01:

The Length indicates the number of bytes containing key data in the array Data[]. It is computed as the integer value of the quantity of Key Length in bits plus 7 divided by 8. For example, the Length shall be 16, and the Data[] array shall contain the 128-bit Secure Channel base key (SCBK).

This command shall be sent by the ACU and accepted by the PD only while the connection is “secure”. The “secure” connection in this context shall mean that either:

- a) the current connection is encrypted, and the session keys are based on the current SCBK (or SCBK-D), or
- b) that the connection is inherently secure via physical security, such as ACU/PD are connected via simple short cable. The “inherently secure” connection shall be asserted to the ACU and to the PD by setting the devices into a special installation setup mode. The devices should exit the setup mode automatically after a successful completion of this osdp\_KEYSET command.

## Challenge and Secure Session Initialization Request (osdp\_CHLNG)

This command is the first in the Secure Channel Session Connection Sequence (SCS-CS). It delivers a random challenge to the PD and it requests the PD to initialize for the secure session. It's SCS connection sequence value is SCS\_11.

| Byte                                                    | Name          | Meaning                                    | Value |
|---------------------------------------------------------|---------------|--------------------------------------------|-------|
| 0 -7                                                    | Random Number | Random number generated by the ACU (RND.A) | Any   |
| Command structure: none<br>Reply: osdp_NAK, osdp_CCrypt |               |                                            |       |

## Server's Random Number and Server Cryptogram (osdp\_SCRYPT)

This command transfers a block of data used for encryption synchronization. It's SCS connection sequence value is SCS\_12.

| Byte                         | Name       | Meaning                         | Value                                                |
|------------------------------|------------|---------------------------------|------------------------------------------------------|
| 0 - 15                       | Cryptogram | 16-byte Server Cryptogram array | Any. Refer to the Server Cryptogram paragraph below. |
| Reply: osdp_NAK, osdp_RMAC_I |            |                                 |                                                      |

### Server Cryptogram

The Server Cryptogram is computed by encrypting the concatenated RND.B[8] and RND.A[8] using key S-ENC. RND.A[8] is generated by the ACU (server) and RND.B[8] is generated by the PD (client).

ServerCryptogram = ENC( RND.B[8] || RND.A[8], S-ENC )

## Responses

- "Positive Acknowledgment (osdp\_ACK)"
- "Negative Acknowledgment (osdp\_NAK)"
- "Device Identification Report (osdp\_PDID)"
- "Device Capabilities Report (osdp\_PDCAP)"
- "Local Status Report (osdp\_LSTATR)"
- "Card Data Report, Raw Bit Array (osdp\_RAW)"
- "Keypad Data Report (osdp\_KEYPAD)"
- "Communication Configuration Report (osdp\_COM)"
- "Client's ID and Client's Random Number (osdp\_CCRYPT)"

### Positive Acknowledgment (osdp\_ACK)

There is no reply structure associated with this reply. Sent in response to all valid commands that do not require a specific response or will not receive an immediate response.

| Packet Format Field | Code    | Name     | Meaning |
|---------------------|---------|----------|---------|
| CMND                | 0x40    | osdp_ACK |         |
| DATA                | Omitted |          |         |

### Negative Acknowledgment (osdp\_NAK)

The optional completion code array may be omitted if none of the command records were processed either because the command had only one record, or because none of the records were processed due to invalid record sizing.

Bytes 1-N are present only for error codes that define its use. The optional completion code array may be omitted if none of the command records were processed either because the command had only one record, or because none of the records were processed due to invalid record sizing.

| Packet Format Field | Code                                   | Name       | Meaning                                |
|---------------------|----------------------------------------|------------|----------------------------------------|
| CMND                | 0x41                                   | osdp_NAK   |                                        |
| DATA                | Refer to <a href="#">“Error Codes”</a> | Error Code | Refer to <a href="#">“Error Codes”</a> |
|                     | 0x00 – 0xFF                            | Data       | Error Code dependent, 1 – N            |

## Error Codes

| Error Code Value | Meaning                                                                                                                                                                                                                                                                                                                                             |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00             | No error                                                                                                                                                                                                                                                                                                                                            |
| 0x01             | Message check character(s) error (bad cksum/crc)                                                                                                                                                                                                                                                                                                    |
| 0x02             | Command length error                                                                                                                                                                                                                                                                                                                                |
| 0x03             | Unknown Command Code – Command not implemented by PD                                                                                                                                                                                                                                                                                                |
| 0x04             | Unexpected sequence number detected in the header                                                                                                                                                                                                                                                                                                   |
| 0x05             | This PD does not support the security block that was received                                                                                                                                                                                                                                                                                       |
| 0x06             | Encrypted communication is required to process this command                                                                                                                                                                                                                                                                                         |
| 0x07             | BIO_TYPE not supported                                                                                                                                                                                                                                                                                                                              |
| 0x08             | BIO_FORMAT not supported                                                                                                                                                                                                                                                                                                                            |
| 0x09             | Unable to process command record<br><br>0x09 indicates that one or more command records had invalid parameters and was not processed which can be followed by an optional array, where each byte represents the completion code of the corresponding command record. A zero value indicates no error, and the value 0xFF indicates a generic error. |

## Device Identification Report (osdp\_PDID)

Sent in response to an osdp\_ID command. Note also that the “cUID”, used in certain Secure Channel operations, is the first 8 bytes of the PDID response.

Reply Structure: 12-byte fixed record.

| Packet Format Field | Code | Name      | Meaning |
|---------------------|------|-----------|---------|
| CMND                | 0x45 | osdp_PDID |         |

| Packet Format Field | Code        | Name                | Meaning                                                                                                                                                                                                                                                                |
|---------------------|-------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DATA 12 Bytes       | 0x00 – 0xFF | Vendor Code 1st     | IEEE assigned OUI<br>The Vendor Code is a 24-bit identifier of the manufacturer. It is recommended that each manufacturer use its IEEE assigned Organizationally Unique Identifier, the same 24 bits it uses to form the MAC addresses of its Ethernet-based products. |
|                     | 0x00 – 0xFF | Vendor Code 2nd     |                                                                                                                                                                                                                                                                        |
|                     | 0x00 – 0xFF | Vendor Code 3rd     |                                                                                                                                                                                                                                                                        |
|                     | 0x00 – 0xFF | Model Number        | Manufacturer's model number<br>The Model field is assigned by and managed by the Vendor.                                                                                                                                                                               |
|                     | 0x00 – 0xFF | Version             | Manufacturer's version of this product<br>The Version Number field is assigned by and managed by the Vendor.                                                                                                                                                           |
|                     | 0x00 – 0xFF | Serial Number (LSB) | 4-byte serial number<br>The 32-bit Serial Number field is assigned and managed by the Vendor.                                                                                                                                                                          |
|                     | 0x00 – 0xFF | Serial Number       |                                                                                                                                                                                                                                                                        |
|                     | 0x00 – 0xFF | Serial Number       |                                                                                                                                                                                                                                                                        |
|                     | 0x00 – 0xFF | Serial Number (MSB) |                                                                                                                                                                                                                                                                        |
|                     | 0x00 – 0xFF | Firmware Major      | Firmware revision code<br>The Firmware Revision fields are assigned and managed by the Vendor.                                                                                                                                                                         |
|                     | 0x00 – 0xFF | Firmware Minor      |                                                                                                                                                                                                                                                                        |
|                     | 0x00 – 0xFF | Firmware Build      |                                                                                                                                                                                                                                                                        |

## Device Capabilities Report (osdp\_PDCAP)

Sent in response to an osdp\_CAP command. The Device Capabilities report message may contain multiple records of this form (3 bytes per record). Use the total message length to determine the number of records present.

The records may be in any order. If a function code is omitted from the list, The ACU may assume that the PD has no support for that function code. A list of Function Codes and their definition, and the corresponding compliance levels is incorporated as Annex B of this Document.

Reply Structure: 3-byte element, repeated one or more times.

| Packet Format Field | Code        | Name          | Meaning                                                                   |
|---------------------|-------------|---------------|---------------------------------------------------------------------------|
| CMND                | 0x46        | osdp_PDCAP    |                                                                           |
| DATA 3 Bytes        | 0x00 – 0xFF | Function Code | Repeated once per capability. Refer to <a href="#">“Function Codes”</a> . |
|                     | 0x00 – 0xFF | Compliance    |                                                                           |
|                     | 0x00 – 0xFF | Number of     |                                                                           |

## Function Codes

| Byte | Name          | Meaning                                 | Value                                                                     |
|------|---------------|-----------------------------------------|---------------------------------------------------------------------------|
| 0    | Function Code | Function/feature code                   | Refer to Function Codes mentioned below.                                  |
| 1    | Compliance    | Level of compliance with above function | Refer to the compliance levels mentioned in the respective Function Codes |
| 2    | Number of     | Number of objects of this type          | Refer to Number of Objects in the respective Function Code.               |

### Function Code 1 – Contact Status Monitoring

This function indicates the ability to monitor the status of a switch using a two-wire electrical connection between the PD and the switch. The on/off position of the switch indicates the state of an external device.

The PD may simply resolve all circuit states to an open/closed status, or it may implement supervision of the monitoring circuit. A supervised circuit is able to indicate circuit fault status in addition to open/closed status.

#### **Compliance Levels:**

01 – PD monitors and reports the state of the circuit without any supervision. The PD encodes the circuit status per its default interpretation of contact state to active/inactive status.

02 – Like 01, plus: The PD accepts configuration of the encoding of the open/closed circuit status to the reported active/inactive status. (User may configure each circuit as "normally closed" or "normally open".)

03 – Like 02, plus: PD supports supervised monitoring. The operating mode for each circuit is determined by configuration settings.

04 – Like 03, plus: the PD supports custom End-Of-Line settings within the Manufacturer's guidelines.

The End-Of-Line circuit parameters are defined by the manufacturer of the PD.

**Number Of:** The number of Inputs.

### Function Code 2 – Output Control

This function provides a switched output, typically in the form of a relay. The Output has two states: active or inactive. The ACU can directly set the Output's state, or, if the PD supports timed operations, the ACU can specify a time period for the activation of the Output.

#### **Compliance Levels:**

01 – The PD is able to activate and deactivate the Output per direct command from the ACU.

02 – Like 01, plus: The PD is able to accept configuration of the Output driver to set the inactive state of the Output. The typical state of an inactive Output is the state of the Output when no power is applied to the PD and the Output device (relay) is not energized. The inverted drive setting causes the PD to energize the Output during the inactive state and de-energize the Output during the active state.

This feature allows the support of "fail-safe/fail-secure" operating modes.

03 – Like 01, plus: The PD is able to accept timed commands to the Output. A timed command specifies the state of the Output for the specified duration.

04 – Like 02 and 03 – normal/inverted drive and timed operation.

**Number Of:** The number of Outputs.

### **Function Code 3 – Card Data Format**

This capability indicates the form of the card data is presented to the Control Panel.

#### ***Compliance Levels:***

01 – the PD sends card data to the ACU as array of bits, not exceeding 1024 bits.

02 – the PD sends card data to the ACU as array of BCD characters, not exceeding 256 characters.

03 – the PD can send card data to the ACU as array of bits, or as an array of BCD characters.

**Number Of:** N/A, set to 0.

### **Function Code 4 – Reader LED Control**

This capability indicates the presence of and type of LEDs.

#### ***Compliance Levels:***

01 – the PD support on/off control only

02 – the PD supports timed commands

03 – like 02, plus bi-color LEDs

04 – like 02, plus tri-color LEDs

**Number Of:** The number of LEDs per reader.

### **Function Code 5 – Reader Audible Output**

This capability indicates the presence of and type of an Audible Annunciator (buzzer or similar tone generator).

#### ***Compliance Levels:***

01 – the PD supports on/off control only

02 – the PD supports timed commands

**Number Of:** This field is ignored. Per 6.11 there is only one audible output per PD.

### **Function Code 6 – Reader Text Output**

This capability indicates that the PD supports a text display emulating character-based display terminals.

#### ***Compliance Levels:***

00 – The PD has no text display support

01 – The PD supports 1 row of 16 characters

02 – the PD supports 2 rows of 16 characters

03 – the PD supports 4 rows of 16 characters

04 – FF Reserved for future use

80 – FF Reserved for private use

**Number Of:** Number of textual displays per reader.

### **Function Code 7 – Time Keeping**

This capability indicates that the type of date and time awareness or time keeping ability of the PD. This function has been deprecated.

#### ***Compliance Levels:***

00 – The PD does not support time/date functionality  
0x01-0xff – reserved for future use

**Number Of:** N/A, set to 0.

### **Function Code 8 – Check Character Support**

All PDs shall be able to support the checksum mode. This capability indicates if the PD is capable of supporting CRC mode.

#### ***Compliance Levels:***

00 – The PD does not support CRC-16, only checksum mode.  
01 – The PD supports the 16-bit CRC-16 mode.

**Number Of:** N/A, set to 0.

### **Function Code 9 – Communication Security**

This capability indicates the extent to which the PD supports communication security as defined in Annex D.

#### ***Compliance Levels:***

This field is a bit map of the supported encryption algorithms:  
0x01 – (Bit-0) AES128 support  
(Bits 1-7) Must be zero

**Number of:** This field is encoded to represent the key exchange capabilities:  
0x01 – (Bit-0) default AES128 key  
(Bits 1-7) Must be zero

### **Function Code 10 – Receive BufferSize**

This capability indicates the maximum size single message the PD can receive.

#### ***Compliance Levels:***

This field is the LSB of the buffer size

**Number of:** This field is the MSB of the buffer size

### **Function Code 11 – Largest Combined Message Size**

This capability indicates the maximum size multi-part message which the PD can handle.

#### ***Compliance Levels:***

This field is the LSB of the combined buffer size

**Number of:** This field is the MSB of the combined buffer size

### **Function Code 12 – Smart Card Support**

This capability indicates what kind of smartcard support is available for communicating directly with a smart card.

#### ***Compliance Levels:***

Bit 0 (mask 0x01) – PD supports transparent reader mode

Bit 1 (mask 0x02) – PD supports extended packet mode.

Either one or both modes may be supported.

### **Function Code 13 – Readers**

This capability indicates the number of credential reader devices present. Compliance levels are bit fields to be assigned as needed.

#### ***Compliance Level:***

Must be zero

**Number of:** Indicates the number of attached downstream readers.

### **Function Code 14 – Biometrics**

This capability indicates the ability of the reader to handle biometric input

#### ***Compliance Levels:***

0 – No Biometric

1 – Fingerprint, Template 1

2 – Fingerprint, Template 2

3 – Iris, Template 1

### **Function Code 15 – Secure PIN Entry support**

This capability indicates if the reader is capable of supporting Secure PIN Entry (SPE) for smart cards. Secure PIN Entry is used with ISO 7816 (Smartcards). It is assumed the osdp\_KEYPAD message will be used if the keypad is to be read by the ACU.

#### ***Compliance Levels:***

0 = does not support SPE

1 = supports SPE

### **Function Code 16 – OSDP Version**

This capability indicates the version of OSDP this PD supports.

#### ***Compliance Levels:***

0 = unspecified (also used for pre-IEC 60839-11-5 implementations)

1 = IEC 60839-11-5

2 = SIA OSDP 2.2

3-0x7F = Reserved for future use

0x80-0xFF = reserved for private use



## Local Status Report (osdp\_LSTATR)

Sent in response to an osdp\_LSTAT command or as a "poll response"

The local status report applies to conditions directly monitored by the PD. Tamper status is detected by the PD by monitoring the enclosure tamper mechanism. Power monitor status can be derived from the status of the power supply. Normally this reply is sent in response to an osdp\_POLL command if either status has changed since the last POLL.

Reply Structure: 2 status bytes.

| Packet Format Field | Code                                  | Name          | Meaning                  |
|---------------------|---------------------------------------|---------------|--------------------------|
| CMND                | 0x48                                  | osdp_LSTATR   |                          |
| DATA 2 Bytes        | 0x00 – normal<br>0x01 – tamper        | Tamper Status | Status of tamper circuit |
|                     | 0x00 – normal<br>0x01 – power failure | Power Status  | Status of power          |

## Card Data Report, Raw Bit Array (osdp\_RAW)

Sent as a "poll response"

This reply is sent in response to an osdp\_POLL command after a card was read but the raw data was not decoded into a character array. Unreported card data is deleted in case of, or during, a communication loss.

Reply structure: 4-byte header, variable-length data.

| Packet Format Field | Code                                                             | Name            | Meaning                                                       |
|---------------------|------------------------------------------------------------------|-----------------|---------------------------------------------------------------|
| CMND                | 0x50                                                             | osdp_RAW        |                                                               |
| DATA                | 0x00 – 0xFF                                                      | Reader Number   | 0=First Reader 1=Second Reader                                |
|                     | 0x00 = not specified, raw bit array<br>0x01 = P/data/P (wiegand) | Format Code     | Format of included data                                       |
|                     | 0x00 – 0xFF                                                      | Bit Count (LSB) | 2-byte size (in bits) of the data at the end of the record    |
|                     | 0x00 – 0xFF                                                      | Bit Count (MSB) |                                                               |
|                     | 0x00 – 0xFF                                                      | Data            | 8 bits of card data per data byte MSB to LSB (left justified) |

## Keypad Data Report (osdp\_KEYPAD)

Sent as a "poll response"

This reply is sent in response to an osdp\_POLL if there is any data in the keypad buffer. It is applied when the keypad is in default operating mode. Unreported keypad data is deleted in case of, or during, a communication loss.

Reply Structure: 2-byte header, variable-length data.

| Packet Format Field                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Code        | Name          | Meaning                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|----------------------------------------------|
| CMND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 0x53        | osdp_KEYPAD   |                                              |
| DATA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 0x00 – 0xFF | Reader Number | 0=First Reader 1=Second Reader               |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 0x00 – 0xFF | Digit Count   | Number of keypad digits to follow.           |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 0x00 – 0xFF | Data          | Keypad data represented as ASCII characters. |
| <p>The key encoding uses the following data representation:</p> <ul style="list-style-type: none"> <li>• Digits 0 through 9 are reported as ASCII characters 0x30 through 0x39</li> <li>• The clear/delete/'*' key is reported as ASCII DELETE, 0x7F</li> <li>• The enter/'#' key is reported as ASCII return, 0x0D</li> </ul> <p>Special/function keys are reported as upper case ASCII:</p> <ul style="list-style-type: none"> <li>• A or F1 = 0x41, B or F2 = 0x42, C or F3 = 0x43, D or F4 = 0x44</li> <li>• F1 &amp; F2 = 0x45, F2 &amp; F3 = 0x46, F3 &amp; F4 = 0x47, F1 &amp; F4 = 0x48</li> </ul> |             |               |                                              |

## Communication Configuration Report (osdp\_COM)

Sent in response to an osdp\_COMSET command. This reply returns the communication parameters the PD will use after sending this reply.

Reply Structure: 5-byte record

| Packet Format Field | Code        | Name            | Meaning                           |
|---------------------|-------------|-----------------|-----------------------------------|
| CMND                | 0x54        | osdp_COM        |                                   |
| DATA 5 Bytes        | 0x00 – 0x7E | Address         | Unit ID for this PD to respond to |
|                     | 0x00 – 0xFF | Baud Rate (LSB) | 4 Byte Baud rate value            |
|                     | 0x00 – 0xFF | Baud Rate       |                                   |
|                     | 0x00 – 0xFF | Baud Rate       |                                   |
|                     | 0x00 – 0xFF | Baud Rate (MSB) |                                   |

## Client's ID and Client's Random Number (osdp\_CCrypt)

This reply sends a block of data used for encryption synchronization, sent in response to osdp\_CHLNG command. It's SCS connection sequence value is SCS\_13.

| Byte  | Name          | Meaning                               | Value |
|-------|---------------|---------------------------------------|-------|
| 0 - 7 | Client ID     | Client's Unique Identifier (cUID)     | Any   |
| 8 -15 | Random Number | PD's random number generated, (RND.B) | Any   |

| Byte    | Name       | Meaning                         | Value |
|---------|------------|---------------------------------|-------|
| 16 - 31 | Cryptogram | 16-byte Client Cryptogram array | Any   |

# Technical Specifications

|                                      |                                                                                                                            |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>GENERAL</b>                       |                                                                                                                            |
| Max. Door Controllers on Ethernet    | 255                                                                                                                        |
| Max. Door controller on RS-485 Users | 32<br>25,000                                                                                                               |
| Event Buffer                         | 500,000                                                                                                                    |
| <b>COMMUNICATION</b>                 |                                                                                                                            |
| Wi-Fi                                | Inbuilt Wi-Fi Module (IEEE 802.11 b/g/n)                                                                                   |
| Inbuilt Bluetooth                    | YES                                                                                                                        |
| Ethernet                             | YES (10/100 Mbps)                                                                                                          |
| RS-485                               | YES                                                                                                                        |
| USB                                  | One USB Port (for Data Transfer and 2G-3G-4G/ WiFi Dongle)                                                                 |
| SD Card                              | YES (8GB)                                                                                                                  |
| <b>INTERFACE</b>                     |                                                                                                                            |
| Aux-In                               | YES (4 states - short, open, activated & non-activated)                                                                    |
| Aux-Out                              | Form C and SPDT Relay                                                                                                      |
| <b>HARDWARE</b>                      |                                                                                                                            |
| CPU                                  | Cortex A8 800 MHz                                                                                                          |
| Flash Memory                         | 256 MB                                                                                                                     |
| RAM Memory                           | 256 MB (DDR3 SDRAM @ 800MHz)                                                                                               |
| Operating System                     | Linux based OS                                                                                                             |
| Communication Port                   | Ethernet & RS-485                                                                                                          |
| Tamper Detection                     | YES                                                                                                                        |
| RTC                                  | YES                                                                                                                        |
| <b>AUDIO-VISUAL</b>                  |                                                                                                                            |
| LED                                  | Tricolor LED (Power, Status & Alarm)                                                                                       |
| Buzzer                               | YES (12V)                                                                                                                  |
| <b>MECHANICAL</b>                    |                                                                                                                            |
| Mounting                             | Wall Mounting or Table Top                                                                                                 |
| Dimensions (L x H x D)               | 125.25mm X 81.5mm X 30.5mm (4.93" x 3.20" x 1.20")                                                                         |
| Input Power                          | External Power Adapter (12V DC @ 2A)                                                                                       |
| Weight                               | 0.140 Kgs (0.308 Lbs.)                                                                                                     |
| <b>COMPATIBILITY</b>                 |                                                                                                                            |
| System Integration                   | API For Software Integration                                                                                               |
| Architecture                         | Network Architecture - With COSEC CENTRA/VYOM<br>Standalone Architecture<br>Network Architecture - With Third Party Server |
| <b>ENVIRONMENTAL</b>                 |                                                                                                                            |
| Humidity                             | 5% to 95% RH Non-Condensing                                                                                                |
| Operating Temperature                | -10°C to +55°C (14°F to 131°F)                                                                                             |
| <b>CERTIFICATIONS</b>                |                                                                                                                            |
|                                      | FCC, CE, RoHS                                                                                                              |



*Due to continuous technology upgradations, product specifications are subject to change without notice.*

## **FCC Compliance**

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

# Disposal of Products/Components after End-Of-Life

---

Main components of Matrix products are given below:

- **Soldered Boards:** At the end-of-life of the product, the soldered boards must be disposed through e-waste recyclers. If there is any legal obligation for disposal, you must check with the local authorities to locate approved e-waste recyclers in your area. It is recommended not to dispose-off soldered boards along with other waste or municipal solid waste.
- **Batteries:** At the end-of-life of the product, batteries must be disposed through battery recyclers. If there is any legal obligation for disposal, you may check with local authorities to locate approved batteries recyclers in your area. It is recommended not to dispose off batteries along with other waste or municipal solid waste.
- **Metal Components:** At the end-of-life of the product, Metal Components like Aluminum or MS enclosures and copper cables may be retained for some other suitable use or it may be given away as scrap to metal industries.
- **Plastic Components:** At the end-of-life of the product, plastic components must be disposed through plastic recyclers. If there is any legal obligation for disposal, you may check with local authorities to locate approved plastic recyclers in your area.

After end-of-life of the Matrix products, if you are unable to dispose-off the products or unable to locate e-waste recyclers, you may return the products to Matrix Return Material Authorization (RMA) designation.

Make sure these are returned with:

- proper documentation and RMA number
- proper packing
- pre-payment of the freight and logistic costs.

Such products will be disposed-off by Matrix.

**"SAVE ENVIRONMENT SAVE EARTH"**



## **MATRIX COMSEC**

### **Head Office:**

394-GIDC, Makarpura, Vadodara - 390010, India.

Ph: (+91) 18002587747

E-mail: [Tech.Support@MatrixComSec.com](mailto:Tech.Support@MatrixComSec.com)

[www.MatrixComSec.com](http://www.MatrixComSec.com)