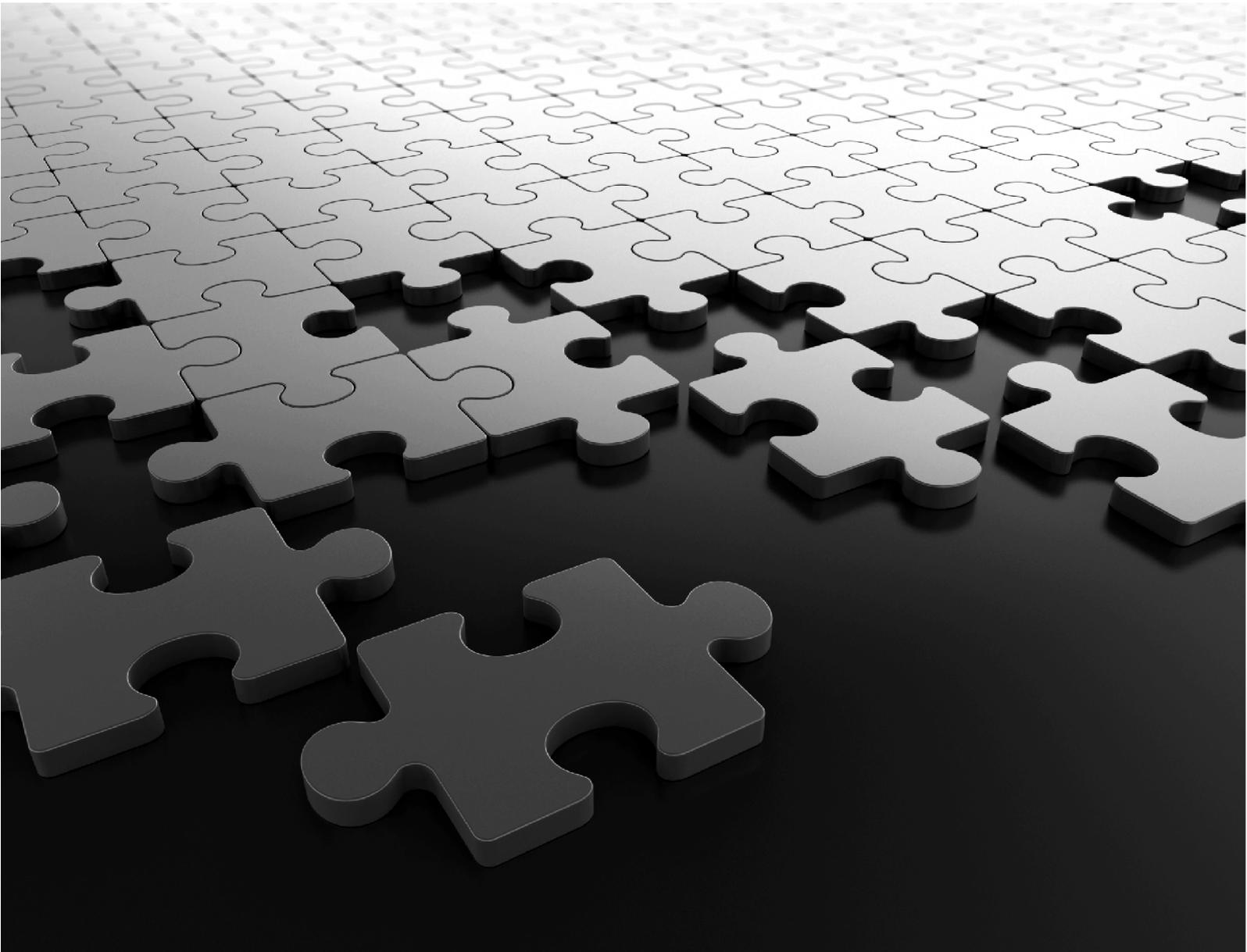


**COSEC Panel200
System Manual**





COSEC Panel200

Standalone Mode

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 33

Release date: November 15, 2024



Contents

Introduction	1
Quick Setup Wizard	5
Dashboard	10
Panel Configuration	13
<i>Basic Profile</i>	14
<i>Advanced Profile</i>	19
<i>Access Features</i>	28
<i>Special Functions</i>	34
<i>Input Output</i>	36
<i>Zone Configuration</i>	43
<i>Man Trap Door Group</i>	51
<i>Network Settings</i>	53
<i>Date and Time</i>	63
<i>Server Settings</i>	65
<i>CCC Settings</i>	69
Devices	70
<i>Door Configuration</i>	71
<i>Door Group</i>	80
<i>Video Surveillance</i>	82
Masters	85
<i>Card Format</i>	86
<i>Card Personalization</i>	90
<i>Wiegand Format</i>	93
Users	95
<i>User Configuration</i>	96
<i>Access Group</i>	102
<i>Functional Group</i>	106
<i>Blocked User</i>	108
Enrollment	110
<i>User</i>	111
<i>Special Card</i>	115
<i>SI User</i>	116
<i>Authorization</i>	118

Access Policies & Access Schedule.....	120
<i>2-Person Rule</i>	121
<i>Access Route</i>	124
<i>First-IN User Rule</i>	129
<i>Smart Card Access Route</i>	131
<i>Time Zone</i>	133
<i>Access Cluster</i>	136
<i>Occupancy Control</i>	138
<i>Access Rule</i>	143
<i>Shifts and Schedules</i>	146
<i>Holiday Schedule</i>	151
System Maintenance & About	153
<i>System Maintenance</i>	154
Multi-Level Access.....	162
Elevator Access Control	165
<i>Elevator Configuration</i>	167
<i>Elevator Floor Group</i>	170
Import, Export, Report.....	174
<i>Import</i>	175
<i>Export</i>	177
<i>Reports</i>	181
Alerts.....	187
<i>Alert Message Configuration</i>	188
<i>Alert Server Configuration</i>	191
Managing User Account and Password	195
<i>Users</i>	196
<i>Password Policy</i>	198
SNMP Configuration.....	199
<i>SNMP Configuration</i>	201
<i>Change Password</i>	206
<i>About Device</i>	208
Monitor & Event Log.....	209
<i>Monitor</i>	210
<i>Event Logs</i>	216

Welcome

Thank you for choosing the Matrix COSEC Multi-door Access Control System!

We are sure you will be able to make optimum use of this feature. 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 2 modes — Standalone Mode and Server Mode.

COSEC PANEL200 acts as a site controller and it can manage multiple controllers. It is a bridge between the controllers and the central COSEC server. It also has an Embedded Web Server. They synchronize all door controllers and implement advanced access control features.

To know more about COSEC PANEL200, please refer [“Know Your COSEC PANEL200”](#).

Intended Audience

This System Manual is written for:

1. **System Engineers**, who will install, maintain and support the COSEC system. System Engineers are persons who are responsible for configuring the COSEC system 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 COSEC system. No one, other than the System Engineer is permitted to make any alterations to the configuration of the COSEC system.

2. **System Administrators**, who are persons who will monitor and control the COSEC system 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.
3. **Users**, persons/organizations who will use the COSEC system. 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.
- **Configuration** - describes the Panel configuration along with other doors, users and access control policies.
- **Monitor** - describes details of door, Alarms, Live events of devices connected to Panel200.
- **Event Log**- gives the log of events based on different search criteria.

How to Read this System Manual

This document is organized in a manner to help you get familiar with the COSEC system, 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 COSEC application 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 terms **PANEL** refers to **COSEC PANEL200**, **PANEL DOOR** and **DIRECT DOOR** are used to refer the **COSEC DOOR** (including their variants) respectively. The term **device** is a general term referring collectively to any or all of the above controllers.



If you are accessing the COSEC Server GUI, Device Module > Device Configuration > Click Add Button, 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 Support for further details.



In general Vega Panel Lite (Panel LiteV2) is interchangeably referred as Panel200.

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

Getting Help

Our online help will provide you with immediate and context-related help. Click on the **Help** button, found in all the system windows. A help file will open up which enables the user to navigate to the relevant topic of interest. To get a more focused and context sensitive help click on the “?” symbol located on the upper right half of the web page.

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 with the COSEC system and other Matrix products, contact our Technical Support Help desk, Monday to Saturday 9:00 AM to 6:00 PM (GMT +5:30) except company holidays.

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

Know Your COSEC PANEL200

COSEC PANEL200 is an intelligent device used for access control application. It works on 2 different modes — [“Standalone Mode”](#) and [“Server Mode”](#).

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

When in Server Mode, COSEC PANEL200 manages multiple controllers and acts as a bridge between the controllers and the central COSEC server. They are responsible for synchronizing all door controllers and implementing advanced access control features.

Panel200 having support of SDK1 can be upgraded with SDK2. However, Panel 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”](#).

Features of COSEC PANEL200

- Ethernet, Wi-Fi, Bluetooth and RS-485
- USB Port for Wi-Fi, 3G/4G/LTE and Data Transfer
- Auxiliary Input and Output Ports
- Advance Access Control Features
- 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

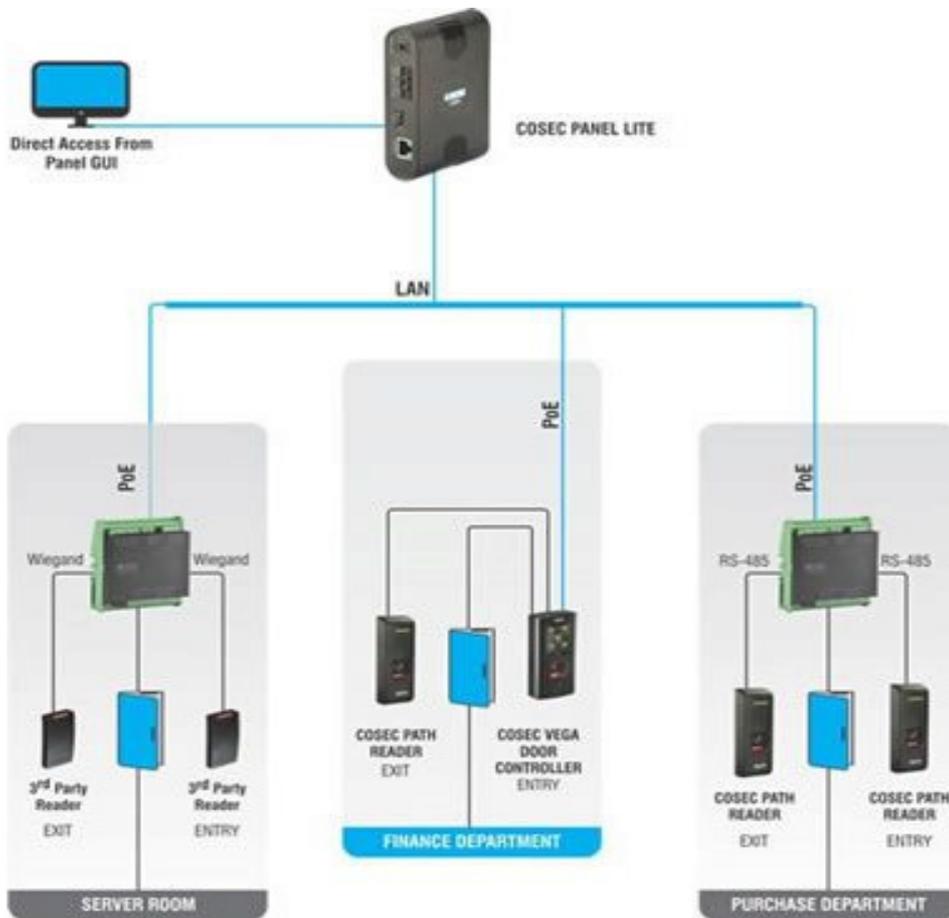
There are different applications of PANEL200. For details refer to [“Applications of PANEL200”](#)

Applications of PANEL200

USE	STANDALONE MODE	SERVER MODE
For	SMB, SME and SOHO	Enterprises and SME
Location	Single Location	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

Standalone Mode

In Standalone mode, COSEC PANEL 200 (site controller) works independently without requiring a server for access control application.

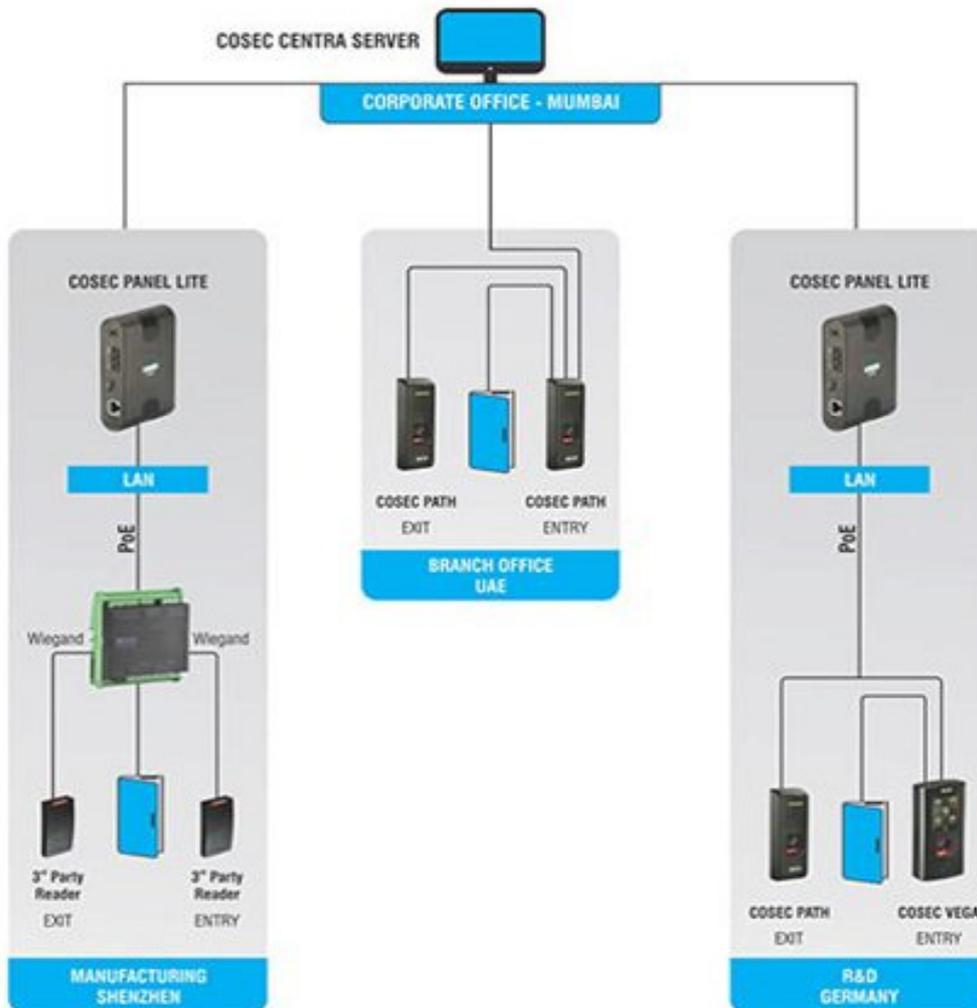


All Matrix COSEC biometric/face/card based door controllers are connected to the site controller for implementing advance access control features and restricting any unauthorized entry.

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

Server Mode

In Server Mode of operation, Panel acts as a bridge between COSEC and COSEC Door Controllers. COSEC biometric/face/card based door controllers are connected with COSEC PANEL200 using Ethernet or RS-485.



COSEC PANEL 200 is required in Server Architecture —

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

Features not supported in SDK1

- ARGO FACE 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 (Panel- 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 > Alarms and Timers > [“Alarms”](#)- Face Mask Compulsion, Duress and Tail-Gating for ARGO FACE Door.
 - Panel Configuration > Advanced Profile > [“Enrollment”](#)- Face as Enrollment Mode.
 - Panel Configuration > Advanced Profile > [“Enrollment”](#) - Max Number Of Faces.
 - Panel Configuration > Zone Configuration > [“Basic Configuration”](#) > Face/ Face + PIN/ Face + Card as Access Mode in- Internal or Reader Group1 Mode.
 - 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 Panel-Standalone mode.
 - Users > User Configuration > [“Basic Access Control”](#)- Enrolled Faces.
 - 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 and ARGO FACE Door.

- Devices > Door Configuration > [“Advance Configuration 2”](#) tab in Panel-Server Mode.
- Devices > Door Configuration > [“Face Identification Settings”](#) tab for Panel- Standalone Mode.
- Devices > Door Configuration > [“Face Identification Settings: Panel- Server Mode”](#) > Show Feedback for Unidentified Face and Generate Unidentified Face Event for Panel- Server Mode.
- Enrollment > [“User”](#)- Face as Enrollment Type and No. of Faces will not be supported.
- 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.
- 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 > [“Event Logs”](#)- Snapshot Image column 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.
 - Alerts > [“Alert Message Configuration”](#)- Event Type- Access Control, Event- User Allowed- Face Mask Not Detected will not be displayed.
 - Alerts > [“Alert Message Configuration”](#)- 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.



Quick Setup Wizard is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

Quick Setup Wizard is an easy and time saving installation process for Panel200, which enables the Admin to configure basic parameters — Date & Time, Network Parameters, Scan Devices and Status of the Devices— step by step very quickly.

This Wizard simplifies the basic setting up process of Panel200 in Standalone Mode.

After the Panel200 is powered on, login as an Administrator. For the Login details, refer "[Panel Configuration](#)"

When the Panel is logged in Standalone Mode for the first time, the **Setup Wizard** will start automatically and the welcome screen appears. For details, refer to "[Setup Wizard](#)".

When the Admin tries to access the Panel using its default IP for the first time, the Admin will be asked to set the password to access Panel as well as for Panel Doors.

MATRIX COSEC PANEL200

admin

...

...

Login

© 2010 Matrix ComSec Pvt. Ltd. All Rights Reserved.



After setting the password, click **Login** and the Setup Wizard will run.

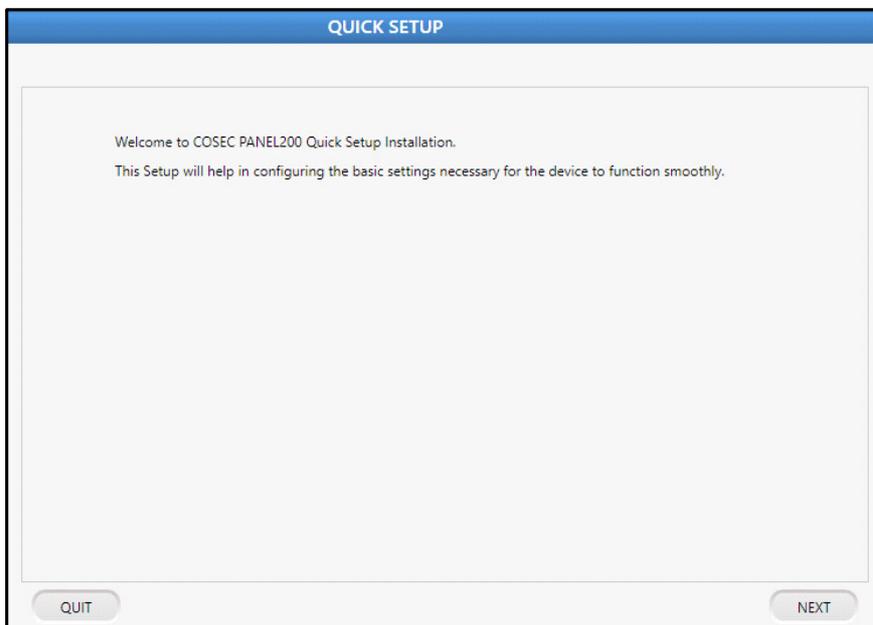
Setup Wizard

The Setup Wizard will guide the Admin step by step to configure the basic settings of the Panel.

When the Panel is logged in Standalone Mode for the first time, the **Setup Wizard** will start automatically.

An option to start Setup Wizard  is provided on **Dashboard** so that the Admin can access it again whenever required. For the configuration of Dashboard, refer "[Dashboard](#)".

The Quick Setup Wizard page appears as shown below:



Click **Next** to navigate through the Wizard and configure the following parameters:

Step 1: "[Date and Time](#)"

Step 2: "[Network](#)".

Step 3: "[Scan Devices](#)"

Step 4: "[Status](#)"

Click **Back** to navigate to the previous page.

You can quit the Setup Wizard from any page by clicking the **Quit** button.

Once you click **Quit**, the entered information in the respective page will not be saved and a popup will be displayed to confirm if the Admin wants to quit the wizard.

Click **Yes** to exit the Setup Wizard page, else to continue with the Wizard, click **No**.

Date and Time

This tab allows to configure the 'Date & Time' settings of the Panel200.

The screenshot shows the 'Date and Time' configuration page within the 'QUICK SETUP' wizard. The page is divided into four tabs: 1.Date and Time (selected), 2.Network, 3.Scan Devices, and 4.Status. The main content area displays the current date and time as '06, January 2020 14:15:43'. Below this, there are several configuration options: 'Time Zone' is set to '(GMT+05:30) Chennai, Kolkata, New Delhi, Mumbai'; 'Time Format' is set to '24 hours'; 'Date' is '06-01-2020' and 'Time' is '14 : 15 : 22'. There are checkboxes for 'Auto Synchronize With NTP' and 'Daylight Saving Time'. The 'Preferred NTP Server' field is empty with a 'Max 40 Chars' limit. The 'Daylight Saving Time' section includes dropdowns for 'Month' (January), 'Week' (First), and 'Day' (Sunday), along with 'Time' fields (00 : 00) and a 'Duration' field (00 : 00). At the bottom, there are 'QUIT', 'BACK', and 'NEXT' buttons.

The Date and Time page enables you to view and set date and time parameters for the Panel200 device.

- **Time Zone:** Select the time zone as per your region from the dropdown list.
- **Time Format:** Select a desired time format from the dropdown list — 12 hour or 24 hour.
- **Date & Time:** The current Date and Time will automatically be set. You can also set it as per your requirement

Auto Synchronize with NTP

If you require Date and time to be automatically synchronized with the Preferred NTP Server (predefined or user-defined NTP server address) selected by user, then you must enable **Auto Synchronize With NTP** checkbox.

Independent of the mode set from server as Auto or Manual, the Admin can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address. If it does not get Date and Time in three tries; device will check from 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 device will first check that server. If it receives the updates then, updated Date and Time will be reflected on device webpage and display screen. Valid Values: a-z A-Z 0-9 - . (dot).
 2. You can keep the Preferred NTP server blank. In this case device will check for Date and Time from the pre-defined NTP server.
 3. If you have manually entered Date and Time from webpage or Device Menu then the set values of Date and Time will be reflected on device webpage and display screen.

Daylight Saving Time (DST)

Select this checkbox to **enable** the DST feature.

Many countries follow the convention of adjusting clocks forward and backward. Clocks are set ahead during the spring and back to standard time in the autumn.

The COSEC Panel200 can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

For the **Forward Clock**, set a month, week, day and time at which the clock is to be set forward. Similarly, set the **Reverse Clock**. Also, set the **Duration** in hh:mm format by which the clock is to be set forward or backward.

Example: The above DST Setting implies that on 1st Sunday of November at 09:00 hours, the clock will be forwarded by 05:00 hours. And on last Monday of January at 09:00 hours, the clock will be reversed or set backward by 05:00 hours.

Click on the **Next** button to save the configuration and configure the **Network** settings.



You can manually set the Date and Time from **Configuration > Panel Configuration > Date and Time**. For more information, refer "[Date and Time](#)".

Network

This tab allows Admin to configure the Network settings for the Panel200.

The screenshot shows the 'QUICK SETUP' interface with the '2.Network' tab selected. The 'Network' section contains the following fields:

Panel Name	Panel Lite 1
IP Address	192.168.104.5
MAC Address	00:1b:09:04:65:d1
Subnet Mask	255.255.255.0
Default Gateway	192.168.104.1
Preferred DNS	192.168.111.5
Alternate DNS	

At the bottom of the screen, there are three buttons: 'QUIT', 'BACK', and 'NEXT'.

The basic details of the Panel200 —Panel Name, IP Address, MAC Address, Subnet Mask, Default Gateway, Preferred DNS and Alternate DNS are displayed.

The MAC Address field is a non-editable field.

You can edit the other parameters if required.

Click on the **Back** button to re-configure the parameters of Date and Time or **Next** to save the current configuration.



*You can manually configure the Network Settings from **Configuration> Panel Configuration> Network Settings**. For more information, refer [“Network Settings”](#).*

Scan Devices

The doors which are connected in the same network will be automatically scanned and displayed with their details — Door Type, Door Name, IP Address and MAC Address as shown below.

You can add any of these scanned devices by selecting **Add Device** checkbox of the respective devices.

QUICK SETUP

1.Date and Time 2.Network 3.Scan Devices 4.Status

Add Devices to Panel lite

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"/>

Navigation: << < 1 > >>

Buttons: QUIT, BACK, NEXT

You can edit the Name of the door if required.

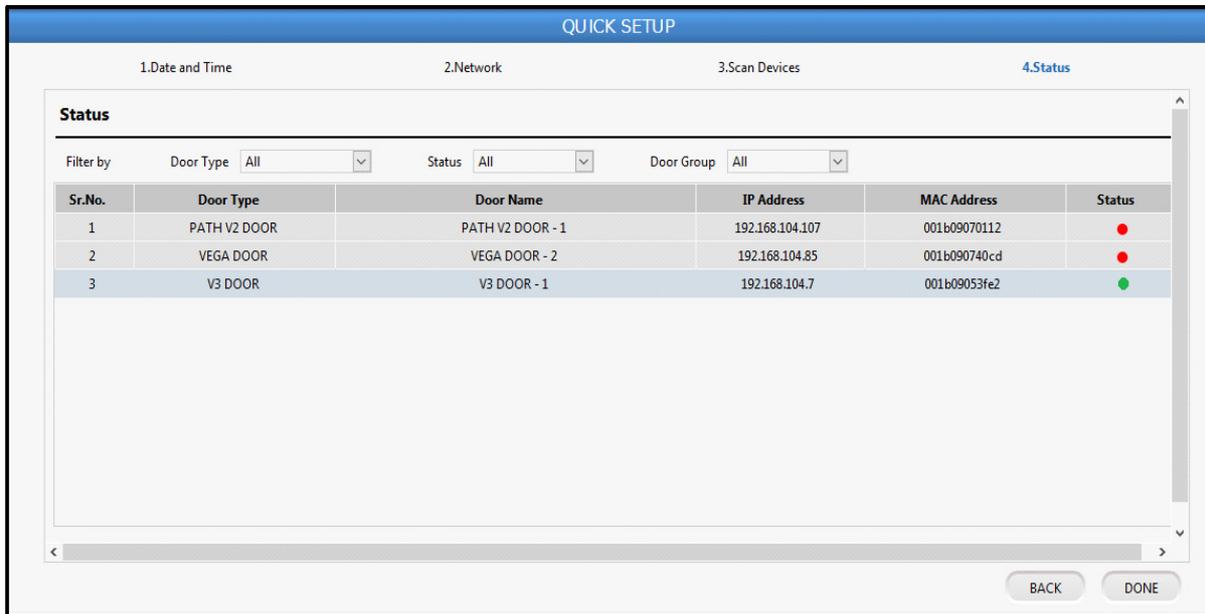
Click on the **Next** button to save and move ahead to the **Status** page.



- The list displays a maximum of 255 doors.
- The other Panel or devices which are already added to the Panel200 will not be displayed in the list.

Status

This tab displays the added Doors with their basic details and their status as shown below.



The screenshot shows the 'QUICK SETUP' interface with the '4.Status' tab selected. The interface includes a filter section with dropdown menus for 'Door Type', 'Status', and 'Door Group', all set to 'All'. Below the filters is a table with the following data:

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

At the bottom of the interface, there are 'BACK' and 'DONE' buttons.

In the status column, the devices which are online are denoted by 'Green' dots whereas the offline devices are denoted by the 'Red' colour dots.

Click **Done** to finish the setup wizard and **Back** button to re-configure the previous pages.

The above parameters can also be configured manually if you have already closed the Quick Setup Wizard. These are described further in this manual.

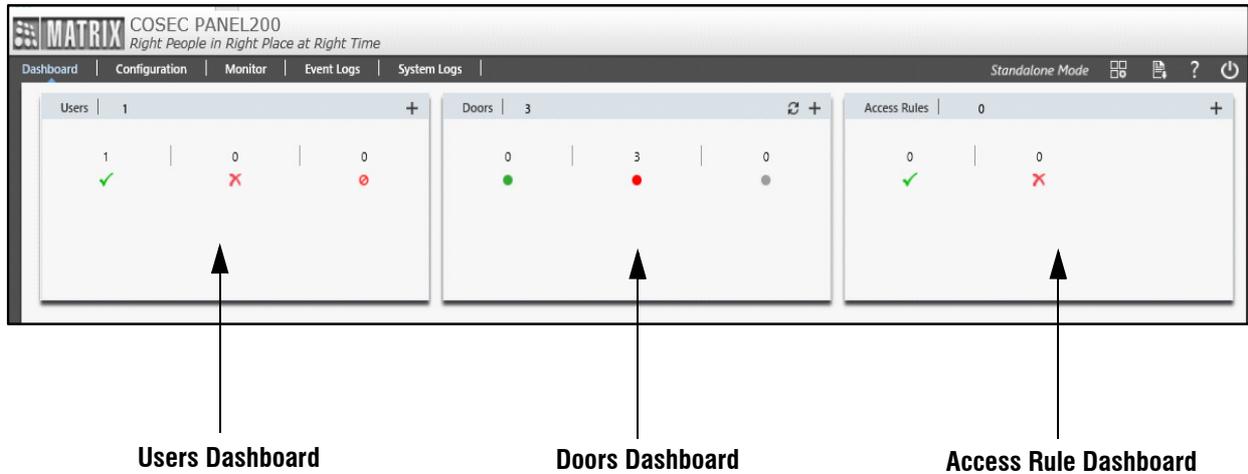
Dashboard enables you to Add/ Edit/ View— Users, Devices and Access Rules — easily and quickly by configuring their basic information.

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** as shown below.

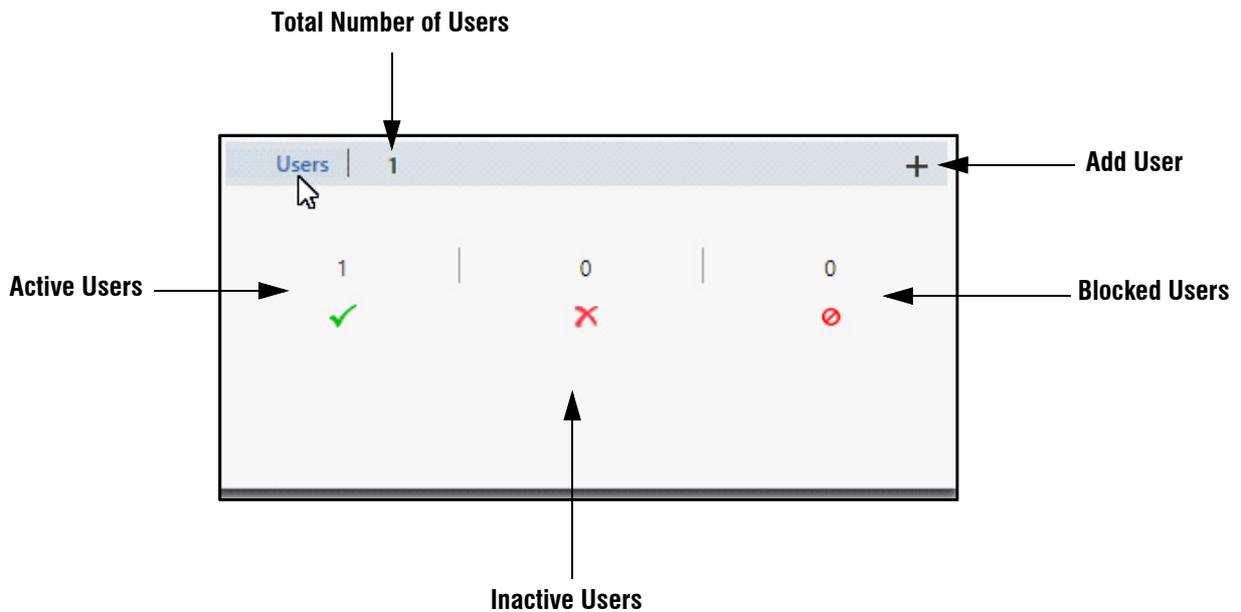


Users Dashboard

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

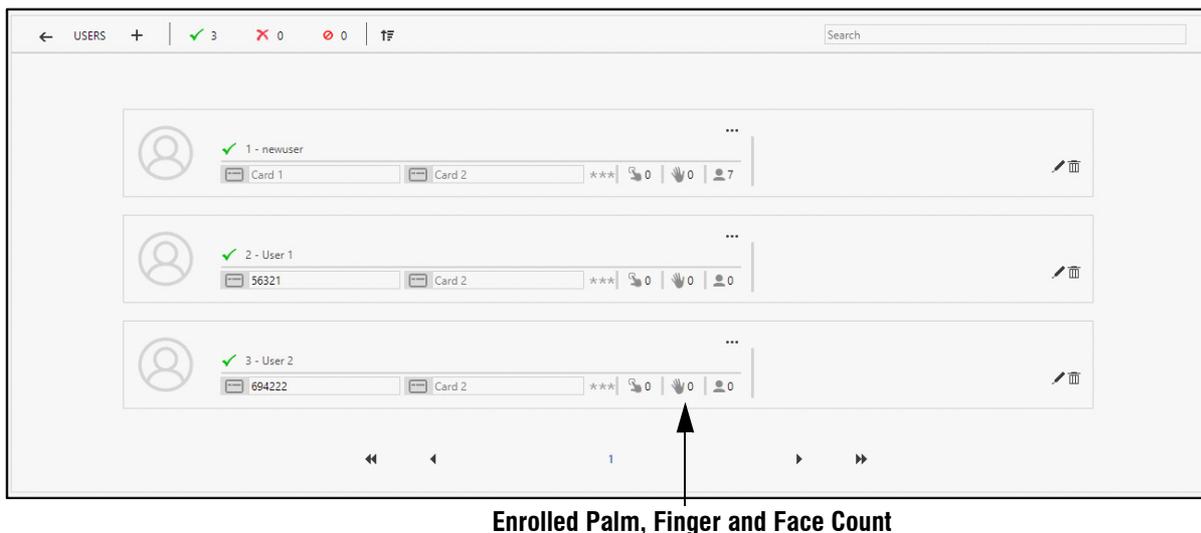
The Users Dashboard enables you to view the basic information of a user as well as add, edit and delete a user.

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:

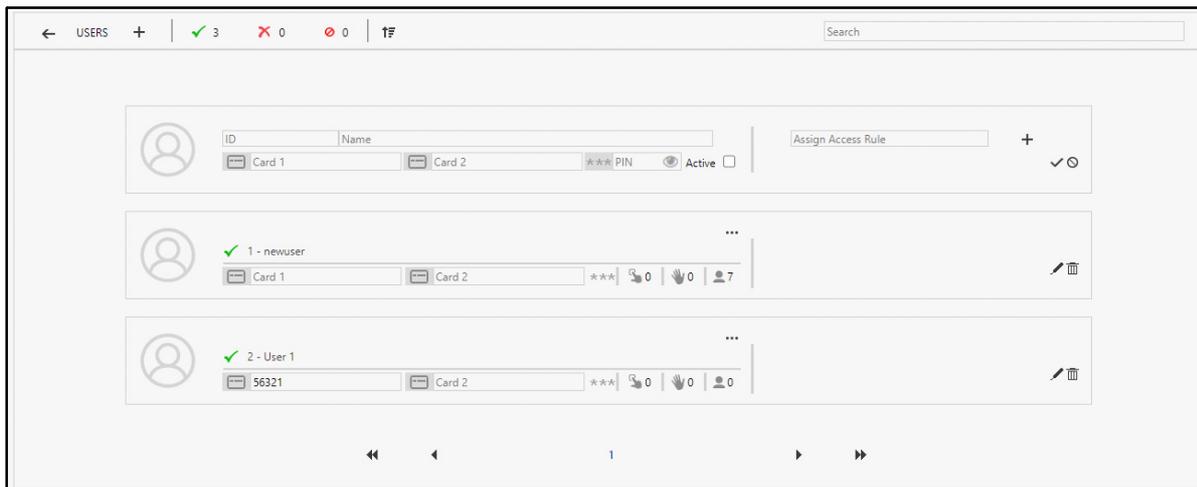
- face images are deleted from Users > User Configuration > Face Images (Updated At).
- face images are updated/deleted from Users > User Configuration > Face Recognition.
- face images are updated from Enrollment > User.
- face images are updated from Panel Configuration > Advanced Profile > Enrollment.

Face Credentials is applicable for Panel- Standalone Mode only.

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.

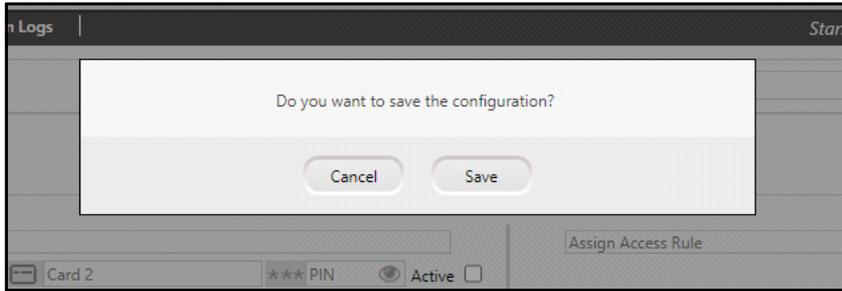
Assign Access Rule

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.

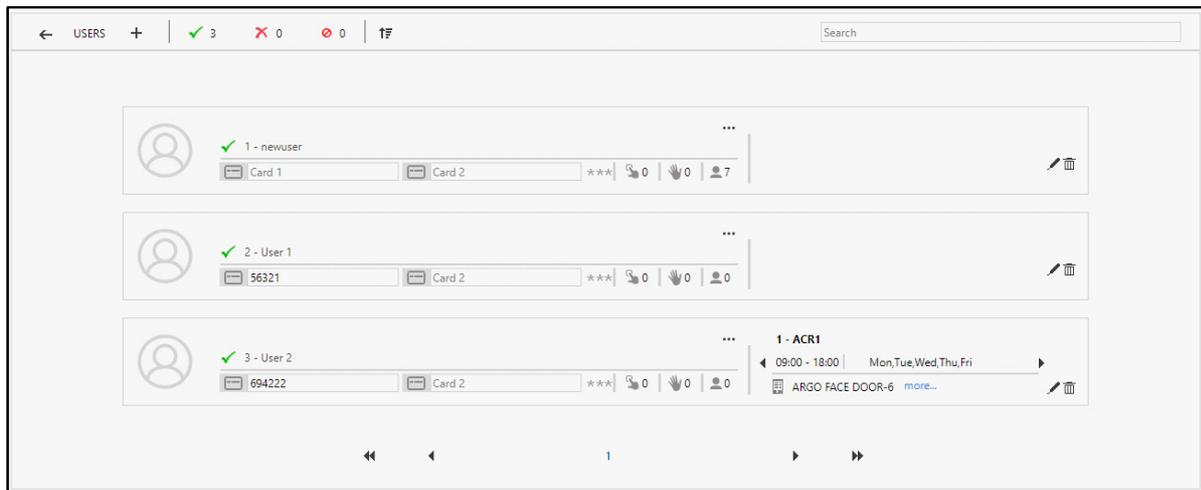


Click **Save** to save the configurations. The **Access Rules** page appears.



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.

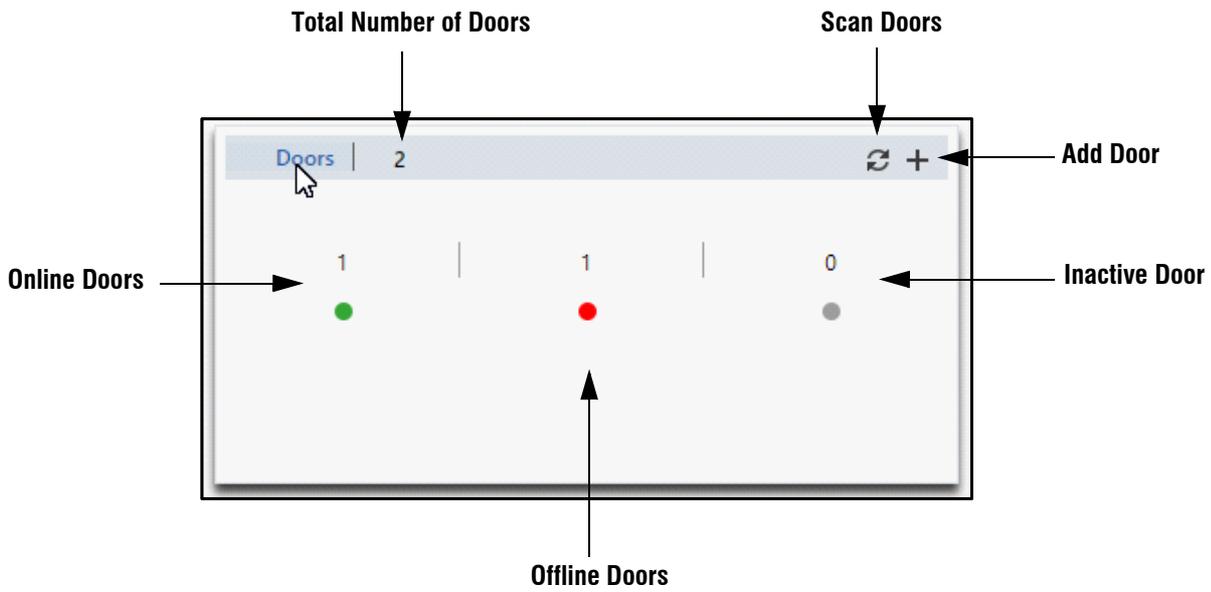
For detailed configuration of a user, refer to [“User Configuration”](#).

Doors Dashboard

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

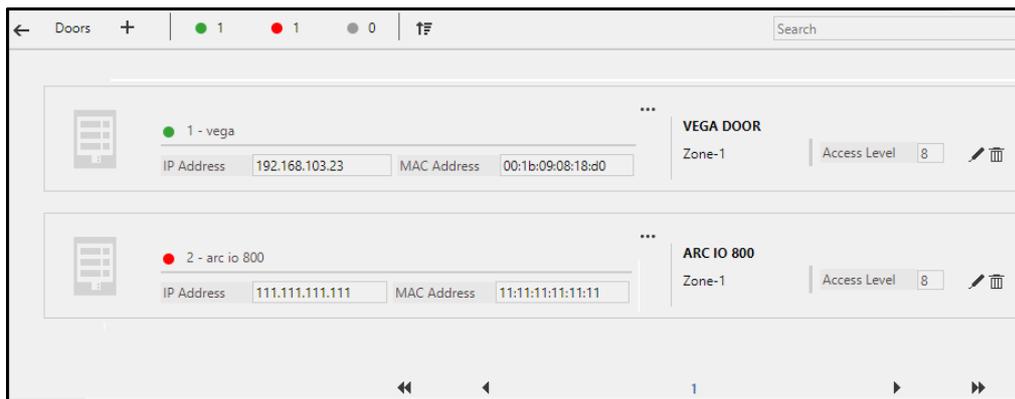
The Doors Dashboard enables you to view the basic details of the door as well as add, edit and delete a door.

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.

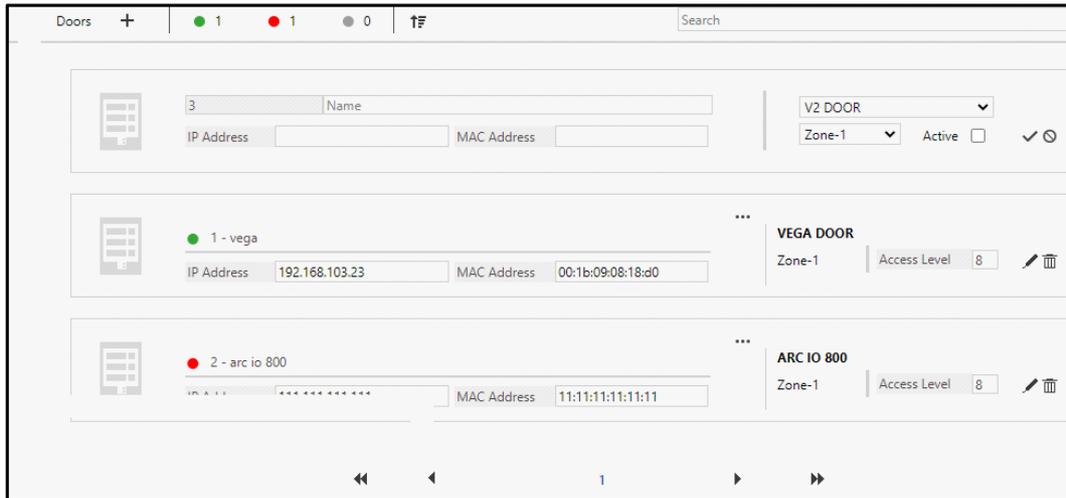


The details displayed are — State of the Door, Door ID, Door Name, IP Address, MAC Address, Door Type, Zone and Access Level.

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.

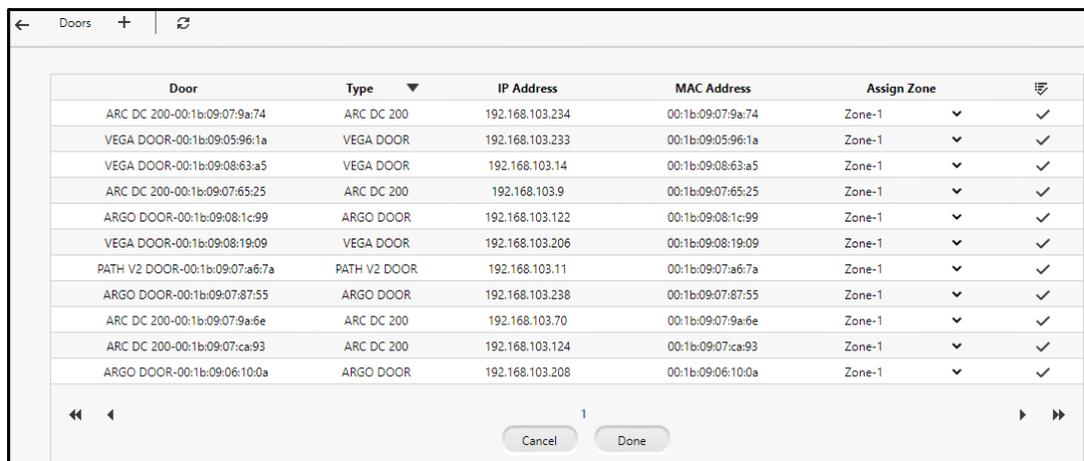
Once you have saved the configurations, you can edit or delete the door.

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. The available doors appear in a list.



Click **Select**  to select the desired door/s to add them to the Panel. 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 Panel.



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

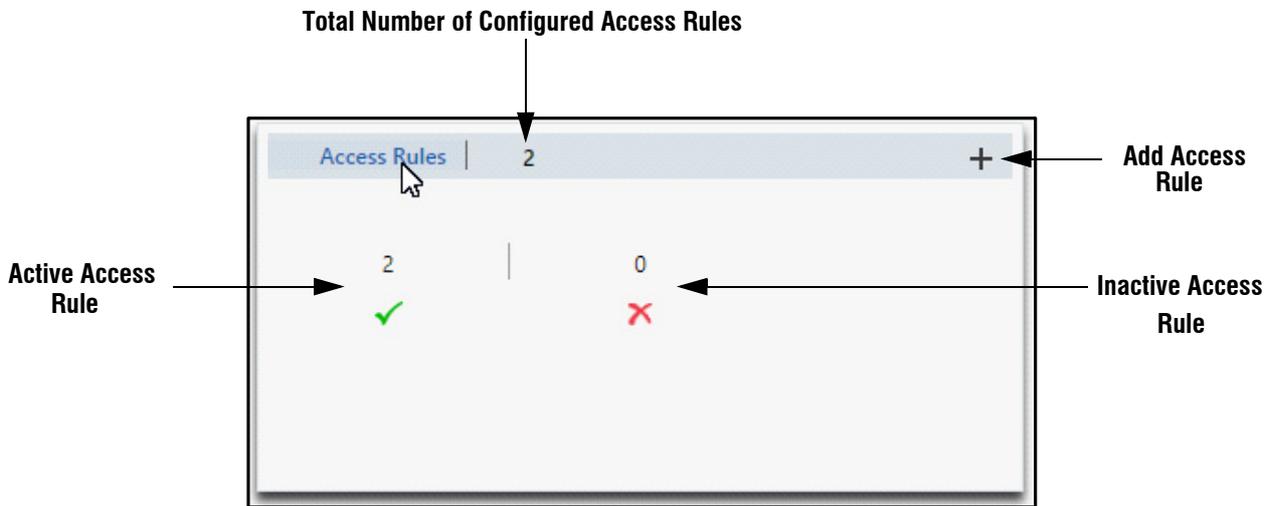
Click **Done** to save the settings.

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

Access Rules Dashboard

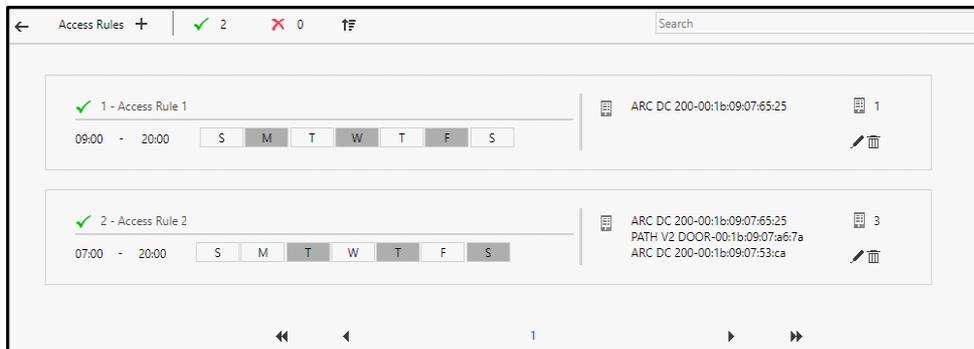
The Access Rule Dashboard enables you to view the Access Rules as well as add, edit and delete an Access Rule.

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”](#).

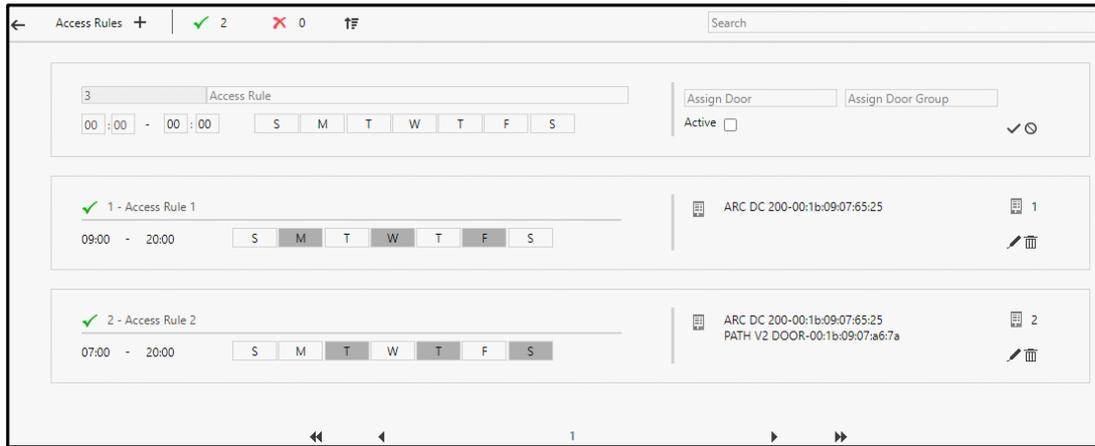
To view the list of Access Rules, click **Access Rules**. It displays the details of the existing Rules.



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”](#).



The terms **Panel**, **Panel lite** and **Panel200** are used alternately to refer to **Panel200** in this manual. The **Panel200** in Standalone Mode is called as **Standalone Panel Lite**.

The COSEC Panel200 is pre-configured with default **IP address: 192.168.50.1** and **Subnet Mask: 255.255.255.0**. You can login to the Webpage of Panel200 using default IP in the browser.

MATRIX COSEC PANEL200

User Name

Password

Remember Password

Login

© 2010 Matrix ComSec Pvt. Ltd. All Rights Reserved.

Then enter the login credentials for Panel200: Default Username: **Admin**; User defined Password.

Once Logged in, user will be redirected to the 'Quick Setup Wizard'. [See "Quick Setup Wizard" on page 11.](#)

Changing Network Configuration

To change the IP address of Panel200; Go to Configuration> Panel Configuration> Network Settings. [See "Network Settings" on page 75.](#)

Changing Panel Mode

To change the mode of Panel200; select *Configuration> Panel Configuration> Basic Profile> Panel Mode*. The default mode is Server Mode.

When you switch to Server Mode then, Server address is to be specified where the Panel200 is to be added.



The Panel200 will reboot when the mode is changed.

Basic Profile

The Basic Profile enables to define and configure basic parameters for the Panel200.



Certain fields may appear as read-only fields when device is in the Server Mode.

Under Basic Profile, you can configure the following:

- “General”
- “Access Settings”
- “Multi-Language”
- “Display”
- “Panel Mode”

General

The screenshot shows the 'Basic Profile' configuration window with the 'General' tab selected. The window has a blue header and a white body. The 'General' tab is highlighted in blue. Below the header, there are five tabs: 'General', 'Access Settings', 'Multi-Language', 'Display', and 'Panel Mode'. The 'General' tab contains the following settings:

- Panel Name: 249
- 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: 1 | 252

At the bottom of the window, there are two buttons: 'Save' and 'Cancel'.

Panel Name: Enter a unique 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 Panel200.

Template Per Finger: Select the no. of template copies to be saved per fingerprint credential enrolled for the user.

Max. No. of Fingers/Palms/Faces Per User: Select the maximum number of fingers/palms/faces per user allowed for the enrollment.

Run PVR Door in Guide Mode: PVR (Palm Vein Reader) Panel 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 device differently, depending on the mode selected.

Enable this option to remove all existing palm templates from the Panel200 and for all future palm enrollment and identification to be performed in the Guide mode only.

Auto Clear Alarm: Select this check-box to enable the feature. Specify the **timer duration** in seconds for alarms to be auto cleared.

Override IO Linking and Time Triggered during Disarm: Select this check-box to enable overriding of IO Linking/Time Triggered configurations for a device when the Disarm special function is enabled.

Face Validation Device: Click the picklist and select the desired device. The face images uploaded manually will be validated using the selected device. The selected device will appear on User Configuration > Face Recognition page. For details, refer to "[Face Recognition](#)".



Face Validation Device is applicable for Panel-Standalone Mode only.

Access Settings



Access Settings is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

Access Settings allows you to select the days and configure the duration of hours for which Panel200 can be accessed.

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

Working Days: While adding new devices, by default all the days including holidays for access are enabled. To change the default settings of working days, click on the relevant boxes(i.e. disable the box) which are not to be included in active working days.

Working Hours (HH:MM): While adding new devices, the default working hours is set as 00:00 to 23:59. The user can change the default working hours in HH:MM format.

Break Hours (HH:MM): The default break hours are set as 13:00 to 14:00. The user can change the default break hours in HH:MM format.

Allowed Early-IN (HH:MM): It specifies the number of hours before official entry time, during which the user is allowed to enter the office. Eg: If 10 minutes is allowed early-in; then user can enter 10 mins before the shift start time.

Allowed Late-OUT (HH:MM): It specifies the number of hours after official exit time, during which the user is allowed to exit from the office. Eg: If 10 minutes is allowed late-out; then user can go out 10 mins after the shift end.

Multi-Language



Multi-language is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

Multi-language feature can be configured from the webpage of Panel200. All the Panel Doors which are connected to the Panel200 will be updated with this multi-language file automatically.

This feature gives the provision to download a sample file which will contain all the default messages in English.

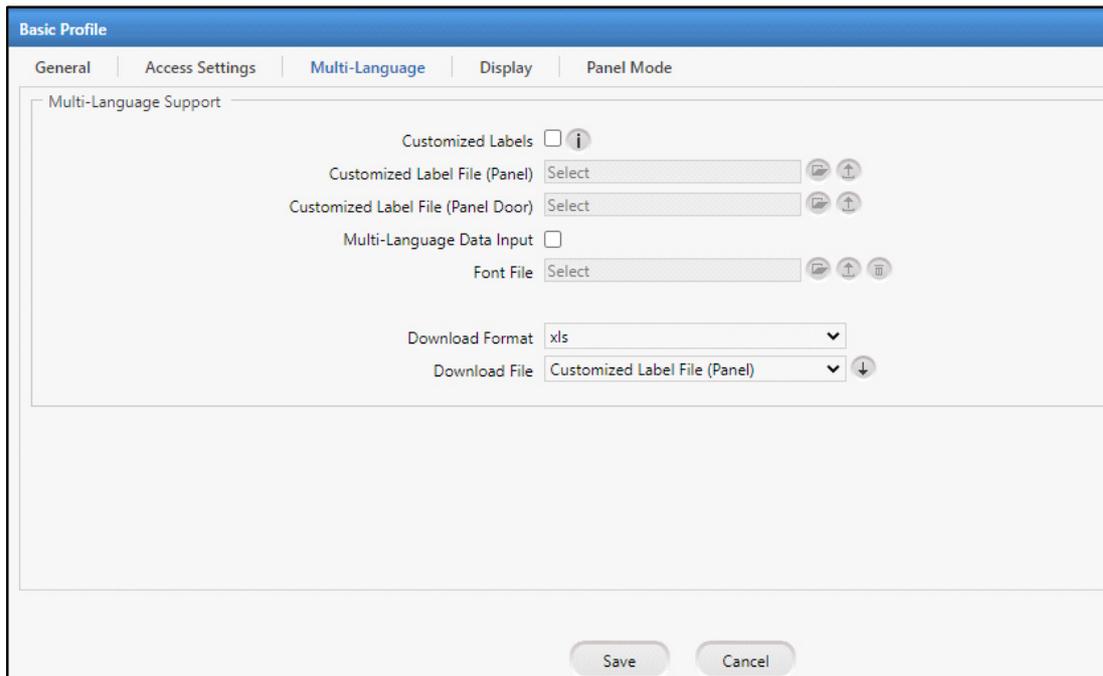
You can enter the custom messages in the desired languages for the variants of Panel door [Dot Matrix Devices & Vega separately] and upload the file. After successful uploading of file, Panel200 will sync the Labels to the respective Panel doors.



File can be uploaded in xls format only.

For Vega Controller-Multi-language is supported for: English, Spanish, Albanian, Thai, Vietnamese.

For Dot matrix devices- Multi-language is supported for: English.



Customized Labels: Select this check-box to view the Panel200's webpage in multi-language for all static strings and labels.

Customized Label File (Panel): Click Browse button to select the file and then click Upload button to upload the string file for Panel with multi-language strings. If there is no file uploaded then first download the sample file, enter the data and then upload it.

Customized Label File (Panel Door): Click Browse button to select the file and then click Upload button to upload the string file for Panel door with multi-language strings. This will provide multi-language for labels of Panel door display screen.

Multi-Language Data Input: Select this checkbox to view the panel's webpage in multi-language for all the data entered by the user. The extended ASCII keypad must be used to intake the multi-language data. The same will be stored in the device in Extended ASCII format.

Font File: Click Browse button to select the font file and then click Upload button to upload the font file of the required language. Click Delete button to remove the font file.

Download Format: Select the download format as xls or csv in which the sample file is to be downloaded.

Download File: You can download both original sample file as well as current file by selecting the file from the options.



The Help file and file which is imported will be in English only.

Display



Display is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

The screenshot shows a software configuration window titled "Basic Profile" with a blue header. Below the header are five tabs: "General", "Access Settings", "Multi-Language", "Display" (which is selected), and "Panel Mode". The main content area is white and contains the following settings:

- "Enable Display Messages" with an unchecked checkbox.
- Message 1: Schedule from 00:00 to 11:59, with the message text "Good Morning".
- Message 2: Schedule from 12:00 to 15:59, with the message text "Good Afternoon".
- Message 3: Schedule from 16:00 to 20:59, with the message text "Good Evening".
- Message 4: Schedule from 21:00 to 23:59, with the message text "Good Night".

At the bottom of the window, there are two buttons: "Save" and "Cancel".

Enable Display Messages: This feature allows the user to enable display messages on door controllers assigned to the Panel200. Upto 4 display messages can be configured for a door.

Schedule: For each message, the user needs to define the time period between which this message is to be displayed.

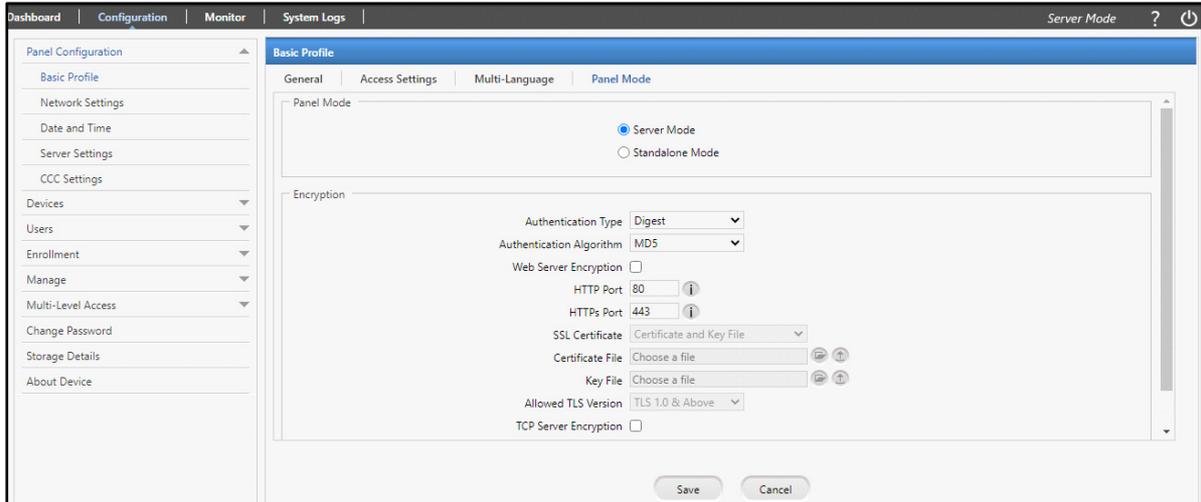
Message 1-4: Enter the message to be displayed in this field. Maximum 21 characters are allowed.

Panel Mode

Panel can be connected in COSEC Server when **Server Mode** is selected or it functions as Standalone Panel200 when **Standalone Mode** is selected.

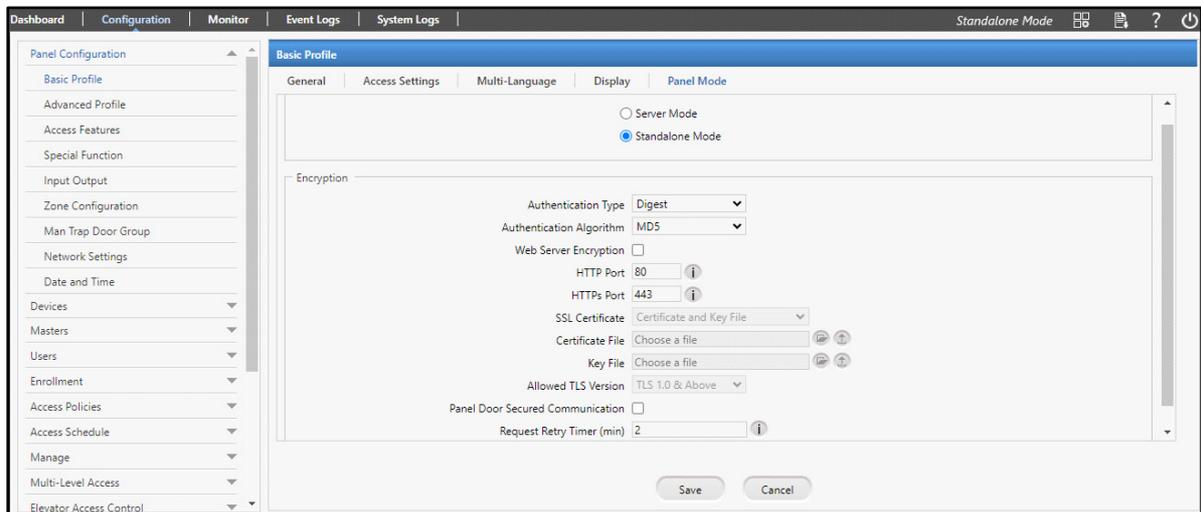
Panel Mode: Select the desired mode — **Server Mode** or **Standalone Mode**.

Panel in Server Mode.



The **Server Mode** should be enabled only if the Panel200 is to be configured using COSEC Server application.

Panel in Standalone Mode.



The Panel200 will reboot when the mode is changed and the configurations will have to be done again.

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 device will serve HTTP/HTTPs APIs from any clients having Basic Authentication.

If Authentication Type is selected as Digest, the device 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 checkbox — **Web Server Encryption** and/ or **TCP Server Encryption** to establish secure HTTPS connection between client-server.

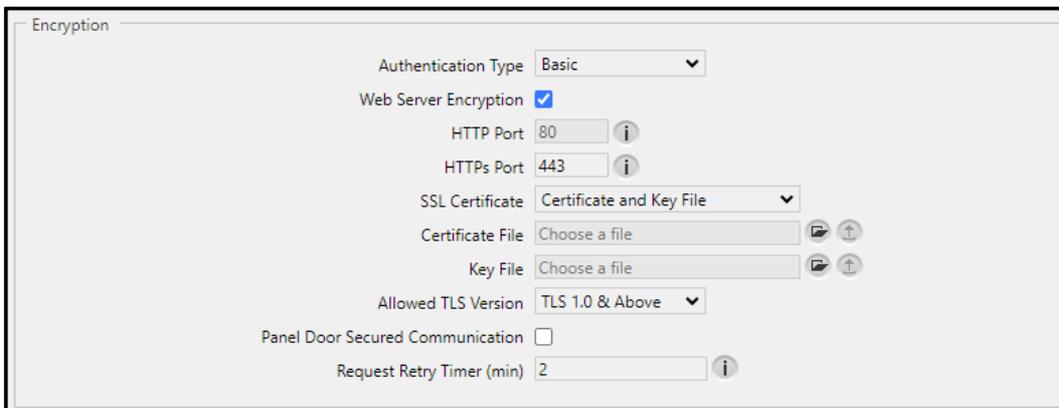


TCP Server Encryption is applicable only for Panel - Server Mode.

- **Web Server Encryption:** Select the Web Server Encryption checkbox to establish secure HTTPS connection with Web Server to access Panel web pages or API. This will secure the Web pages of Panel200.
- **TCP Server Encryption:** Applicable only for **Panel - Server Mode**; select the TCP Server Encryption checkbox to establish secure connection with COSEC Server, TCP Server and CCC Server.
- **HTTP Port:** Enter the desired value of HTTP Port. The default value of HTTP Port is 80. Configurable only when **TCP Server Encryption** is enabled.
- **HTTPs Port:** Enter the desired value of HTTPs Port for secure communication. The default value of HTTPs Port is 443. Configurable when **Web Server Encryption** or **Web Server Encryption** and **TCP Server Encryption** or **TCP Server Encryption** is enabled.

When **Web Server Encryption** or **Web Server Encryption** and **TCP Server Encryption** checkbox 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 dropdown 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  to select the desired certificate. Click  to upload the selected certificate.

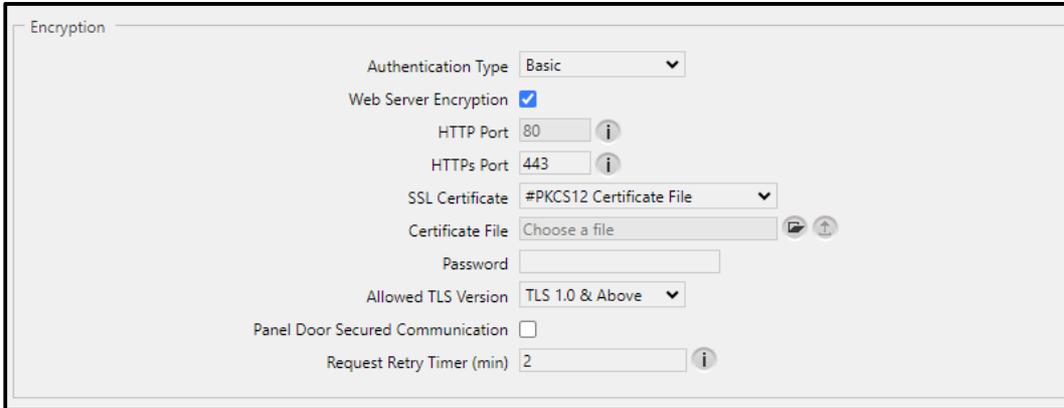


The screenshot shows the 'Encryption' configuration page. It includes the following fields and controls:

- Authentication Type: Basic (dropdown)
- Web Server Encryption:
- HTTP Port: 80 (input field with info icon)
- HTTPs Port: 443 (input field with info icon)
- SSL Certificate: Certificate and Key File (dropdown)
- Certificate File: Choose a file (input field with file selection and upload icons)
- Key File: Choose a file (input field with file selection and upload icons)
- Allowed TLS Version: TLS 1.0 & Above (dropdown)
- Panel Door Secured Communication:
- Request Retry Timer (min): 2 (input field with info icon)

- If you select **#PKCS12 Certificate File** as **SSL Certificate** then you can upload **Certificate File** and enter the desired **Password**.

- Click  to select the desired certificate. Click  to upload the selected certificate.



- **Allowed TLS Version:** Select the desired **TLS Version** from the dropdown list — **TLS 1.0 & Above**, **TLS 1.1 & Above** or **TLS 1.2**.
- **Panel Door Secured Communication:** Select this checkbox to establish secure communication between Panel and Panel doors.



Panel Door Secured Communication flag is only editable in Panel200 - Standalone Mode.

*If the **Panel Door Secured Communication** flag is enabled, then it is applicable to all the connected applicable Panel doors.*

- **Request Retry Timer (min):** Configure the desired time period in minutes. This is the time after which the Panel Door should make a request to the Panel for the face images.



Request Retry Timer (min) is applicable for Panel- Standalone Mode only.

Click **Save** to apply the changes. Click **Cancel** to abort the changes.



The Panel200 will reboot when the mode is changed.

Advanced Profile



Advance Profile is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

The Advanced Profile enables to define and configure advanced parameters for the Panel200.

Settings

Advanced Profile

Settings | Alarms and Timers | Enrollment | Wiegand

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)

Additional Security Code

ASC Code (1-65535)

Confirm ASC Code

Smart Identification

Auto Acknowledge Alarm

Alarm Auto Acknowledge Wait Timer 10 sec(10-65535)

Allow Door Access Through Mobile

Mobile Entry Access Mode Mobile ONLY ⓘ

Save Cancel

Advanced Profile

Settings | Alarms and Timers | Enrollment | Wiegand

Degraded Wait Timer 5 sec(1-99)

Facility Code Check

Facility Code 1 (1-65535)

Additional Security Code

ASC Code (1-65535)

Confirm ASC Code

Smart Identification

Auto Acknowledge Alarm

Alarm Auto Acknowledge Wait Timer 10 sec(10-65535)

Allow Door Access Through Mobile

Mobile Entry Access Mode Mobile ONLY ⓘ

Mobile Exit Access Mode Mobile ONLY ⓘ

API Security Key 2 chars

PIN Change Code 0-9 *

Auto Add/Update Enrolled Face as Profile Photo

Save Cancel

Generate Events: This checkbox is enabled by default. You can disable this check-box if events are not required to be generated and stored in Event logs. This will save the space in Panel200. The events can be user events, door events, alarm events and system events.

However; disabling Generate Events will still display User Allowed, User Denied, Time Out etc on door display.

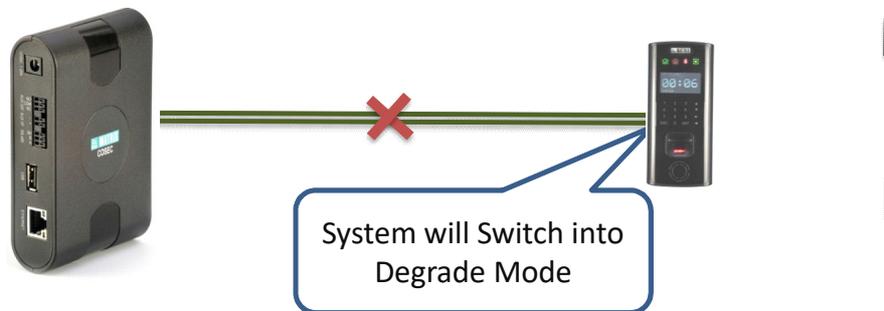
Generate Exit Switch Events: Select this checkbox to enable Panel Doors to generate events for the inputs from the Exit Switch. The exit switch events will be generated when the mode is either exit or both.

Generate Invalid User Events: Select this checkbox to enable the Panel Doors to generate events for invalid user access on door.

Degraded Access: Degraded mode allows a valid user to access the facility even if the Panel Door is not communicating with the Panel200. Select this checkbox to enable this feature at the panel level.

- **Degraded Wait Timer (sec):** Specify the time period in seconds, after the expiry of which the Door Controller switches from Network Fault to Degraded Mode. The default value is 5 sec.

The Master controller (here Panel200) continuously monitors the status of all configured Door Controllers through the pulses regularly transmitted from Master Controller and ACK message is received back from Door Controller. Once the Door Controller 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 Controller changes its mode to “Degraded Mode”.

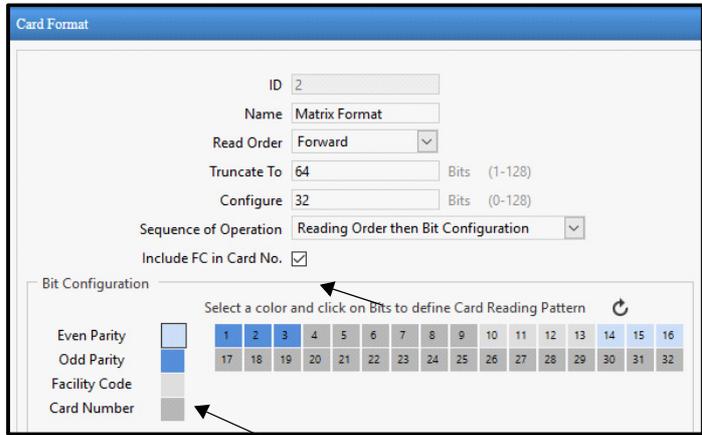
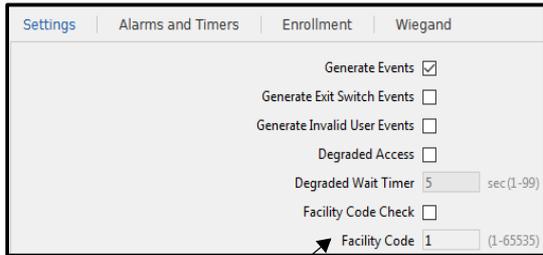


To enable Degraded Mode for each Zone you configure, refer to [“Zone Configuration”](#).

Facility Code Check: Select this checkbox to enable the Panel Doors to check the Facility Code always for the access via RFID Cards even if the Doors are not in degraded mode.

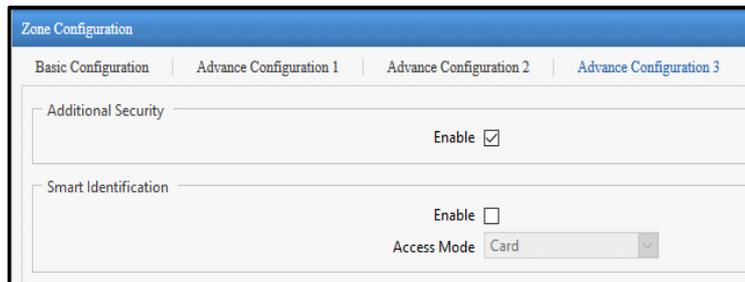
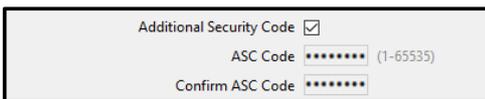
Facility Code: Facility or site codes are encoded on cards, along with a card number, to ensure that cards belong to the facility where access is permitted. Facility code is unique 8 or 16 bits of every HID Proximity card number specific to a site and is encoded into the card by the manufacturer.

- User defined Facility Code (FC) can also be written onto the card at the time of enrollment while using smart cards and system reads this code while allowing access to the Device.
- Enter a facility code (ranging from 1 to 65535) to be written onto the card. This Facility code can be included in the Card format (Masters> 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.



Additional Security Code: To take the security level a step higher, an Additional Security Code can be added.

- This Additional Security Check is possible only with Smart Cards which will prevent the duplicacy of card and restrict unauthorized access to the facility.
- Select the checkbox to enable this functionality at the Panel level and enter the **ASC code** (ranging from 1 to 65535). Re-enter the code to confirm.
- This feature must be enabled at the Zone level (Panel Configuration> Zone Configuration> Advance Configuration3). Now the user; who is assigned the zone enabled with ASC will be checked for ASC verification on the door.



Smart Identification: Select this checkbox 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. E.g. Employee working in Mumbai branch of a office can be identified on the door of Delhi's office using Smart Identification.
- For this the Smart Identification feature must be enabled from *Panel Configuration > Zone Configuration*. Then you must enroll the SI user with desired SI options from *Enrollment > SI User*.

Auto Acknowledge Alarm: Select this checkbox to enable the auto-acknowledgment of all alarms. The Alarms can be enabled from Alarms and Timers section.

- Set the time in seconds for the **Alarm Auto Acknowledge Wait Timer (sec)**. Once the alarm is activated, the wait timer will start and on expiry of the timer, the alarm buzzer will stop automatically.

Allow Door Access Through Mobile: Select this checkbox to allow the access to device using COSEC APTA.

- **Mobile Entry Access mode:** Select the entry access mode from the options of Mobile Only, Mobile then Biometrics, Mobile then Card and Mobile then PIN. When you hover your mouse over the info icon, an important message will be displayed.

- **Mobile Exit Access Mode:** Select the exit access mode from the options of Mobile Only, Mobile then Biometrics, Mobile then Card and Mobile then PIN. When you hover your mouse over the info icon, an important message will be displayed.
- **API Security Key:** Specify the security key for the API.
- **PIN Change Code:** Enter the code for changing pin of the user. This pin is to be entered from the wiegand input pin pad connected to the device. When entered, the device gets changed into pin change mode and asks for the old and new password.
- **Auto Add/Update Enrolled Face as Profile Photo:** Select this checkbox to set the enrolled image of a user as the Profile Photo automatically on successful Face Enrollment.

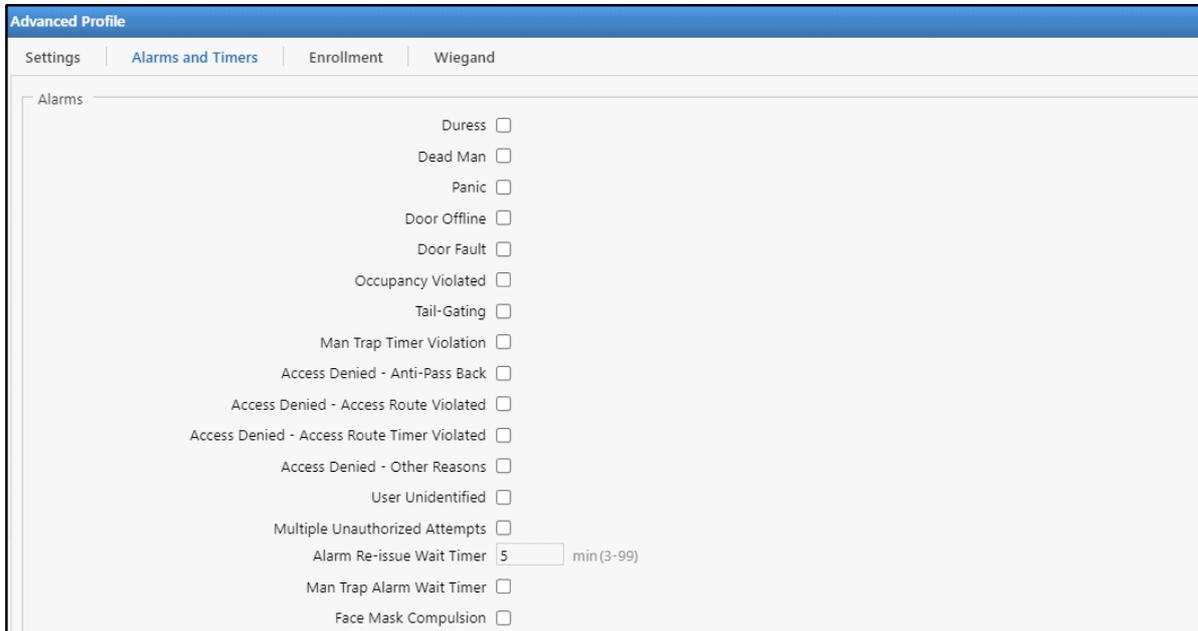


The Panel200 will consider the enrolled face image located at index number 0 to set it as Profile Photo.

Auto Add/Update Enrolled Face as Profile Photo is applicable for Panel- Standalone Mode only.

Alarms and Timers

Alarms



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 FACE	ARGO	VEGA	PATH V2	Door V3	Door V4	PVR	ARC DC200	Door V1	Door V2	Path	ARC DC100	IO800
Duress	X	√	√	√	√	√	√	√	X	X	X	X	X
Dead Man	√	√	√	√	√	√	√	√	X	X	X	X	X
Panic	√	√	√	√	√	√	√	√	X	X	X	X	X
Door 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
Door Lock Abnormal	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

Select the checkboxes of the respective alarms to activate.

1. Duress Alarm:

Duress Alarm can be generated when a facility/ premises has been accessed by a valid user but it is 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.



Enable the Duress Detection feature and set the Duress Code from Panel Configuration> Access Features> Set2



Duress Alarm is not applicable for ARGO FACE Door.

2. Dead Man Alarm:

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.



Enable the Dead Man Zone feature at PANEL level from Panel Configuration> Access Features> Set1 and at ZONE level from Zone Configuration.

3. Panic Alarm:

The user can enable the system to generate a Panic Alarm from the Door Controller by enabling the Panic Alarm check-box.

For this, make sure the Door Alarm is activated and the Door is in normal condition (that is, armed).

4. Door Offline Alarm:

The user can enable the system to generate a Door Offline Alarm by enabling the Door Offline check-box. For this, make sure the Door Offline Alarm is activated.

5. Door Fault Alarm:

The user can enable the system to generate a Door Fault Alarm by enabling the Door Fault check-box. For this, make sure the Door Alarm is activated. Hence, when the door is accessed and held open for a long time, then this alarm will be activated.

6. Occupancy Violated Alarm:

On violation of occupancy rule this alarm will be generated and user is allowed to either enter or exit the zone.

7. Tail-Gating Alarm:

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 Door.

8. Man Trap Timer Violation:

Whenever the timer "Man Trap Timer Internal/External Reader (Sec)" is configured for a particular door say for internal reader from Advanced configuration; user is expected to punch on internal reader of any door present in the same zone/door group within the specified Mantrap timer. If user fails to do so, Mantrap violation alarm will be activated.



If Block User for Mantrap is enabled in Panel Configuration >Access Features >Set 3 then user will be trapped within the premises whenever Mantrap Timer is violated.

9. Access Denied-Anti-Pass Back Alarm:

This Alarm can be enabled to alert the fraudulent use of card when Anti-Pass back feature is applied in a zone. When the restriction is hard, the user has to follow entry and exit sequence; else access will be denied and alarm will be generated.



Enable the Anti-Pass back feature at PANEL level from Panel Configuration> Access Features> Set1 and at ZONE level from Zone Configuration.

10. Access Denied- Access Route Violated:

This Alarm can be enabled to alert the violation of access route configured for the user. When the restriction is hard, the user has to follow the access route; only then he will be allowed to access the doors in the route.



Enable the Access Route feature at PANEL level from Panel Configuration> Access Features> Set1 and configure the Access Route feature from Access Policies > Access Route.

11. Access Denied-Access Route Timer Violated:

This alarm is activated when the Access Route Timer is violated.

12. Access Denied-Other Reasons:

This alarm can be enabled to alert the violations of other Access control policies (other than Anti-Pass Back violation & Access Route violation) while accessing the door.

13. User Unidentified:

This alarm can be enabled to alert the system when the credential of user accessing the door is not identified.

14. Multiple Unauthorized Attempts:

This alarm can be enabled to alert the system when an unauthorized user is trying to access the door multiple times.

15. Alarm Reissue Wait Timer (min):

Enter the time in minutes for which an acknowledged alarm should wait before being re-issued. The default value is 5 minutes.

16. Man Trap Alarm Wait Timer:

Select this checkbox to enable alarm wait timer on the Panel200 to ensure that the user accesses sequential doors of a man-trap (Zone/ Door group) within a specific time-frame.

17. Face Mask Compulsion:

Select this checkbox if you wish an alarm must be triggered to provide an alert when the face mask of a user is not identified.



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

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

Face Mask Compulsion is applicable for Panel- Standalone Mode only.

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): Enter the time period in seconds for which a door controller waits between two digits before considering the user input code as complete.

Multi-Input Wait Timer (sec): Enter the time period in seconds for which system needs to wait for the second credential input from the user when more than one credential is to be used 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): Enter the time period in minutes for which the Late In and Early Out special functions will remain in effect after being enabled.

Door Abnormal Wait Timer (sec): Enter the time period in seconds for which system needs to wait before generating an alarm for abnormal door status.

Palm Enrollment Time Out (sec): Enter the time period in seconds for which a Palm enrollment command will be valid for credential input on a PVR Panel Door. Once this timer runs out, a new enrollment command will have to be generated.

Enrollment

Advanced Profile

Settings | Alarms and Timers | Enrollment | Wiegand

Enrollment Using Door

Enrollment Mode Read Only Card

Enrollment Using User ID

Template Using Finger Single Template/Finger

Max Number Of Fingers Two

Max Number Of Palms Ten

Max Number Of Faces Thirty

Number Of Fingers Two

Number Of Palms Two

Number Of Cards One

Enable Self-Enrollment

Self-Enrollment Retry Count 5 (0-255)

Authorization on Enrollment

Save FP Image ⓘ

Save Cancel

1. **Enrollment Using Door:** Select this checkbox to enable a user to be enrolled on the door.



Enrollment can also be done using the Panel webpage. For details, refer to “User”.

2. **Enrollment Mode:** When the enrollment using door is enable; you can select a mode for user enrollment from the drop down list.
 - If **Read Only Card**, **Smart Card** or **Biometric Then Card** is selected, select the Number of Cards to be enrolled.
 - If **Biometric** is selected, select the Number of Fingers and Number of Palms to be enrolled.
 - If **Duress Finger** is selected, select the Number of Fingers to be enrolled.
 - If **Face** is selected, then **Number Of Faces** to be enrolled can be modified from the respective device display screen only. By default, **Number Of Faces** to be enrolled from the device is set as 1. However, the dropdown will display the value as set in *Panel Configuration > Basic Profile > General > Max. No. of Faces Per User*.



Face as Enrollment Mode is applicable for Panel- Standalone Mode only.

3. **Enrollment Using:** Select the option as alphanumeric **User ID** or **Reference Number** which the user must enter at the door at the time of enrollment using special function.
4. **Template Using Finger:** It displays the number of templates to be saved per fingerprint credential enrolled for the user. It is configured from *Panel Configuration > Basic Settings > General*.
5. **Max Number Of Fingers:** It displays the maximum number of fingers allowed to be enrolled for a user. It is configured from *Panel Configuration > Basic Settings > General*.
6. **Max Number Of Palms:** It displays the maximum number of palms allowed to be enrolled for a user. It is configured from *Panel Configuration > Basic Settings > General*.

- 7. Max Number Of Faces:** It displays the maximum number of faces allowed to be enrolled for a user. It is configured from *Panel Configuration > Basic Settings > General*.



Max Number Of Faces is applicable for Panel- Standalone Mode only.

- 8. 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 per the configured Max Number of Fingers.
- 9. Number Of Palms:** Select number of palms allowed to be enrolled for a user. The number displayed in the drop-down will be as per the configured Max Number of Palms.
- 10. Number Of Cards:** Select number of cards allowed to be enrolled for a user.
- 11. Enable Self-Enrollment:** Select this checkbox to activate self-enrollment. The Self-Enrollment feature enables the user to enroll himself/herself at a COSEC door controller 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. (*User Configuration > Basic Access Control*) Self-Enrollment is beneficial for organizations with large number of employees.
 - Self-Enrollment Retry Count:** Enter the maximum number of retry counts for self-enrollment. The user gets locked if the retry counts exceeds the limit.
- 12. Authorization on Enrollment:** Select this checkbox to allow authorization of users who have enrolled credentials. Once the user is authorized; he can access all the Panel doors using the credential.



The Enrollment of users can be authorized from *Enrollment > Authorization*

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

- 13. Save FP Image:** Select this checkbox to enable the finger print images to be saved in the Panel.



Wiegand

The screenshot shows the 'Advanced Profile' settings window with the 'Wiegand' tab selected. The settings are as follows:

- Wiegand Interface: Input Mode (dropdown)
- Wait For Panel Signal:
- Wait For User Verification:
- Wait Timer: 2 (text input) sec
- Send From: MSB Bit (dropdown)
- Wiegand Out Format: 26 Bit (dropdown)

At the bottom of the window are 'Save' and 'Cancel' buttons.

1. **Wiegand Interface:** Select the interface as Input Mode or Output Mode. The COSEC device can be connected both as input devices (e.g. to receive data from a Wiegand Reader) or output devices (e.g. to support output to third party panel) via the Wiegand interface.
2. **Wait for Panel Signal:** 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).
3. **Wait for User Verification:** If this option is enabled, user verification will be requested on third party device before triggering any output.
4. Select the **Wiegand Output Format** from the dropdown list and the format sending order for reader data as MSB or LSB Bit in the **Send From** field.

If **Custom** option is selected as Wiegand Output Format, the device will receive all different Wiegand output formats. For details refer [“Wiegand Format”](#).

These formats represent the format in which the output will be sent on Wiegand interface. You can assign different formats for each event or a single format for all the events. You can also select the output format by clicking on Select Wiegand-Out Format picklist.

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		

Click **Save** to apply the changes.

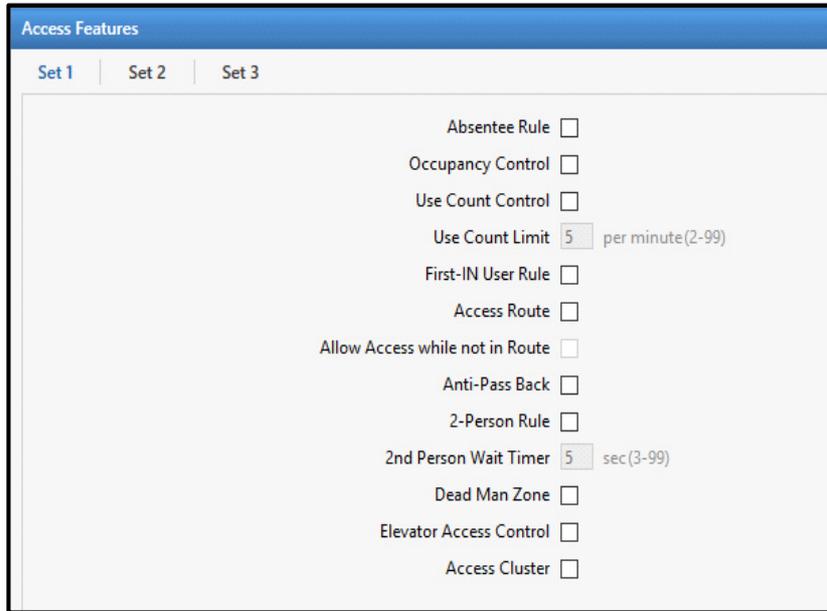
Access Features



Access Features is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

The Access Features page enables to configure the access control features for the device.

Set1



1. **Absentee Rule:** Select the check-box to enable this feature at Panel level. This rule sets the maximum number of days for non-usage of a credential (1 - 365 Days). On expiration (no credential usage - for the maximum number of days set) the User will be automatically blocked.

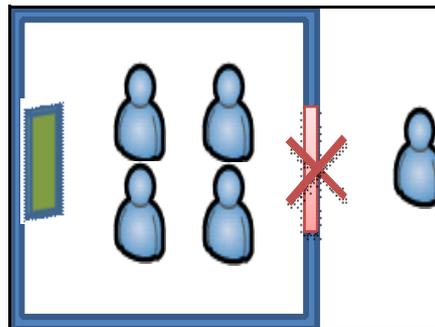


Absentee Rule must be enabled at user level from Users > User Configuration > Profile.

2. **Occupancy Control:** Select the check-box to enable this feature at Panel level. This feature enables the system to monitor and control the number of users permitted within a secured area or controlled zone. Occupancy control functionality requires entry and exit readers on the controlled area.



Occupancy Control must be enabled at Zone level from Panel Configuration > Zone configuration> Advance Configuration 2.



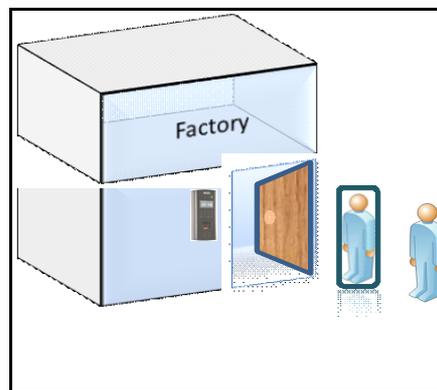
3. **Use Count Control:** Select the check-box to enable this feature at the Panel level.

4. **Use Count Limit** sets a maximum number of times an authorized user can use the Credentials in order to enter/exit a controlled area within a specified time period, after which the credential is blocked. Specify the maximum number of uses per minute in the Use Count Limit (per minute).

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

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

- The First-IN user functionality enables the system to wait in locked mode till a valid First-IN user credential is detected whose working hours overlap the current device time.
- First-IN users are users defined in the system 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 system will allow access to that zone till the detected First-IN user's working hours or the expiry of the configured timer.



Once the period is over then system deactivates the access to the designated zone. The system now waits for another valid first in user credential with valid access time to return the door to normal mode and allow access to users.



First-IN User Rule must be enabled and configured from Zone level from Panel Configuration > Zone configuration> Advance Configuration2.

You can create First IN User Group from Access Policies > First-IN User Rule.

6. **Access Route:** Select this check-box to enable the Access Route feature on Panel200. The members doors of the Access Route are configured and the Access route is assigned to the user from User Configuration > Basic Access Control. The user has to follow the access route as per configured levels and restrictions.



You can configure the Access Route from Access Policies > Access Route.

7. **Allow Access while not in Route:** Select this check-box to allow the access to the door which is not in Access Route but assigned to the user in door assignment from user configuration.
8. **Anti-Pass Back:** Select this check-box to enable the Anti-pass back feature.

- 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 available before the anti-pass back feature is configured.



You must activate the Anti-Pass Back feature at Zone level from Panel Configuration > Zone Configuration > Advance Configuration 1.

9. **2 Person-Rule:** Select the check-box to enable this feature 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.
10. **2nd Person Wait Timer (sec):** Set the wait time in seconds after which the second person is allowed to punch.



You must activate the 2 Person Rule at Zone level from Panel Configuration > Zone Configuration > Advance Configuration 1.

The Primary and Secondary groups for the 2 Person Rule are created from Access Policies > 2 Person Rule.

11. **Dead Man Zone:** Select the check-box to enable this feature 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.



You must activate the Dead Man Zone feature at Zone level from Panel Configuration > Zone Configuration > Advance Configuration 2.

Warning Timer specifies the minimum time within which user needs to come out and show 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.

Dead Man Zone can be activated by special function 23, Activate Dead-man.

12. **Elevator Access Control:** Select this check-box to activate the elevator access control functionality. It is used for controlling the access to the floors of elevators for security purpose.
 - Through user linking of Elevator Floor Group; user can be assigned to any Elevator Floor group. Make sure the EAC is enabled for the desired users. If EAC is not enabled, users will have access to the free floors only.
 - The user who is not enabled for EAC can access free access floors only.



You must activate the Elevator Access Control feature at User level from User Configuration > Advance Access Control 2

- Access Cluster:** Select the check-box to enable this feature 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.

Set2

The screenshot shows the 'Set 2' configuration page. At the top, there are three tabs: '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:

- Duress Detection:** Select this check-box to enable duress detection feature. This enables a user to provide an alert to the security when he is forced to access the door under constraint, threat or force.

A Duress Alarm event will be generated in Master controller (Panel200) when duress is detected. For direct doors; alarm event can be generated at remote location using IO linking.

- Duress Code:** Enter the 2 digit Duress Code. The default code is 10. The user can enter this 2 digit duress code after his allotted pin code when he is forced to access the door.

The keys have to be pressed in the following order:

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

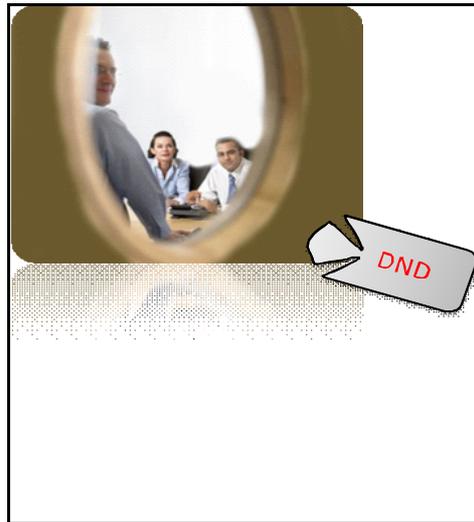


1. Only those users, who are assigned with PIN code, can access this feature.
2. If the door is in Lock state then, user is not allowed, so no duress will be detected.

- DND Zone:** Select the check-box to enable this feature. 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 i.e. Special function21 on Panel200 or it can be activated on the door using Active DND special function.
 - DND access Level must be higher than the zone access level. Eg:If DND Zone access level - 5 and User access level - 4; then user is not allowed to enter in DND zone.
 - VIP Users can access the DND Zone.



You must activate the DND Zone feature at Zone level from Panel Configuration > Zone Configuration > Advance Configuration 1.

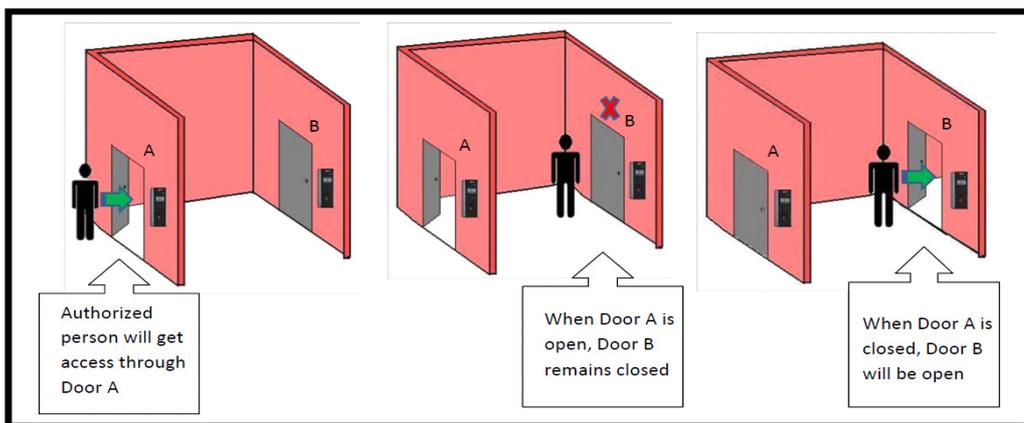


4. **Smart Card Access Route:** Select the check-box to enable the Smart Access Route. In this the user is allowed to access only specified doors with specified levels in predefined route, sequenced or un-sequenced.
5. **Access Route Type:** You can select the Access Route type as incremental by selecting Level 0 as lowest level and decremental by selecting Level 1 as highest level.



1. Access Route is configured from Access Policies > Access Route.
2. The Access Route must be assigned to the user from Users > User Configuration > Basic Access Control.

6. **Man Trap Door Interlock:** Select the check-box to enable the feature at the Panel level. Mantrap, interlock or airlock systems 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.



7. **Man Trap Wait Timer (sec):** Specify the time in seconds for which the door needs to wait for the other door in the same zone where the mantrap feature is enabled to get closed. By default, the value of the Man-trap timer is 5 seconds and valid range is from 3 sec to 99 sec.

8. **Apply Mantrap on:** Select the option as Zone or Door Group on which the Mantrap rule is to be applied.



When Man Trap is configured for Zone then you must activate the Man Trap feature at Zone level from Panel Configuration > Zone Configuration > Advance Configuration 2.

When Man Trap is configured for Door Group then you must activate the Man Trap feature at Door Group level from Panel Configuration > Door Group.

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 two custom keys—one for HID and one for MiFare cards. To use a custom key, select the type of Smart card to be used and enter the desired key in hexadecimal digits.

9. **MiFare Custom Key:** Select the MiFare Custom Key checkbox. For MiFare Cards, enter 12 hexadecimal digits as custom key.
10. **HID iClass Custom Key:** Check the box to enable HID iClass Card Key configuration. For HID Cards, enter a 16-hexadecimal-digit key.

Set3

Access Features

Set 1 | Set 2 | Set 3

Block User For

- Tail-Gating
- Man Trap Timer Violation
- Occupancy Violation
- Anti-Pass Back Violation
- Multiple Unauthorized Attempts
- Allowed Unauthorized Attempts (0-9)

Block User For: Enable the checkbox to block the users for violating the access policies like Tail-Gating, Man Trap Timer Violation, Occupancy Violation, Anti-Pass Back Violation and Multiple Unauthorized Attempts on standalone Panel200.

For Multiple Unauthorized Attempts, specify the **Allowed Unauthorized Attempts**.

Click **Save** to apply the changes.

Special Functions



Special Functions are configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

Special Functions are some functions that can be activated/ deactivated directly from the door controller itself. These functions allow user to use designated **special function card** to operate the special functions.

Example: In factories where workers avail shortleave; security guard can show the Special card enrolled for Shortleave IN on the Entry door and can give the access to the worker. This same card can be used for multiple workers.

It is used to activate Enrollment Mode, DND Zone, Dead-Man Timer, Lock door, unlock etc from any door controller without using the web access or COSEC.

It may also be required to mute an active alarm on door controller or Panel200.

There are four major groups of special functions and they are

- User
- Admin / HRD
- Zone Controls
- Alarms



Functional groups can be created from Users > Functional group.

Special Function							
13	Enroll User	<input checked="" type="checkbox"/>	Admin				↔
14	Enroll Special Card	<input checked="" type="checkbox"/>	Admin				↔
15	Delete Credentials	<input checked="" type="checkbox"/>	Admin				↔
16	Late IN - Start	<input checked="" type="checkbox"/>	Staff				↔
17	Late IN - Stop	<input checked="" type="checkbox"/>	Staff				↔
18	Early OUT - Start	<input checked="" type="checkbox"/>	Staff				↔
19	Early OUT - Stop	<input checked="" type="checkbox"/>	Staff				↔
20	View User Profile	<input checked="" type="checkbox"/>	Staff				↔
21	Activate DND	<input checked="" type="checkbox"/>	Staff				↔
22	Deactivate DND	<input checked="" type="checkbox"/>	Staff				↔
23	Activate Dead Man	<input checked="" type="checkbox"/>	Staff				↔
24	Deactivate Dead Man	<input checked="" type="checkbox"/>	Staff				↔

Select the **Active** check-box corresponding to a Special Function to activate it.

Select a **Functional Group** from the drop-down list which will be responsible for activating this function. For Firmware Version V13R3 or higher, the special functions **Enroll User**, **Enroll Special Card**, **Deleted Credentials** will have **Admin** as the default functional group.

User having functional group as “Admin” can enroll the credentials for other users. You can also change the functional group as required.

Eg: “Enroll User” special function can be enabled for the functional group HRD as shown below. However, some of the special functions can be activated by all the users by default.

Special Function				
13	Enroll User	<input checked="" type="checkbox"/>	Admin	<input type="text"/>
14	Enroll Special Card	<input checked="" type="checkbox"/>	Staff	<input type="text"/>
15	Delete Credentials	<input checked="" type="checkbox"/>	Visitor	<input type="text"/>
16	Late IN - Start	<input checked="" type="checkbox"/>	Admin	<input type="text"/>
			Factory	<input type="text"/>
			HRD	<input type="text"/>
			Staff	<input type="text"/>

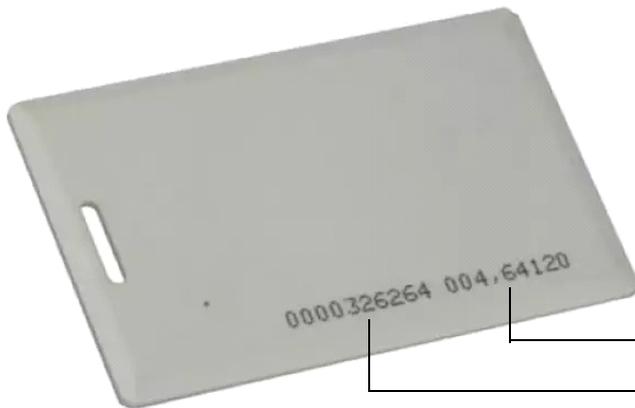


Functional groups can be created from Users > Functional group.

Enter 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**



Facility Code separated Card Serial Number

Card Serial Number

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.

You can configure 4 cards for one special function.

Special Function				
2	Official Work - OUT	<input checked="" type="checkbox"/>	All	<input type="text"/>
3	Short Leave - IN	<input checked="" type="checkbox"/>	All	23564
4	Short Leave - OUT	<input checked="" type="checkbox"/>	All	<input type="text"/>
5	Regular - IN	<input checked="" type="checkbox"/>	All	<input type="text"/>



You can enroll the card which is to be used for special function (say Short leave IN) from Enrollment > Special Card. Once the enrollment of card is done; the Card ID will appear in the Card field as shown above.

If the Card ID is already known before enrollment, then you can enter it here.

Use the **Undo** button to cancel the changes made for a special function.

Click **Save** to apply the changes.

Input Output



Input Output is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

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

The Input/Output (I/O) configuration of a system determines how the output or response of a system is influenced by the input applied on it. The system can be configured to trigger a specific response to any changes in door state or event occurrences at the door device.

This change of door state or occurrence of events may be considered as an input while the response or action that is generated by the system on detection of this input, is defined as the output.

Configuration

The screenshot shows the 'Input Output' configuration interface. It features a blue header with the title 'Input Output' and five tabs: 'Configuration', 'Input Group', 'Output Group', 'IO Linking', and 'Time Triggered'. The 'Configuration' tab is active. Below the tabs, there are two main sections. The first section, 'Auxiliary Input', contains four settings: 'Enable' (checked), 'Supervised' (checked), 'Sense Type' (set to 'NO' in a dropdown menu), and 'Debounce Time' (set to '5' with 'sec (0-99)' as a unit). The second section, 'Aux Output Port', contains two settings: 'Enable' (checked) and 'Output Group No.' (set to '1' with '(1-99)' as a unit).

Auxiliary Input

Enable: Enable this option for Auxiliary Input (e.g. Smoke Detectors) monitoring.

Supervised: Select this check-box, to enable the auxiliary input for four-state monitoring where the door is also monitored for *door fault* and *door disconnection*.

Sense Type: The system by can sense two states of a door - *Normally Open (NO)* and *Normally Closed (NC)* depending on which the output is determined. Specify the normal Sense Type as NC or NO.

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

Debounce Time (sec): It defines the minimum time for which an input interface must be maintained in a given state before the system reports it. Enter the Debounce time in seconds. The default value is 3 sec.

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.

Aux Output Port

Enable: Select this check-box to enable the Auxiliary Output port (e.g. Fire Alarm) for the panel.

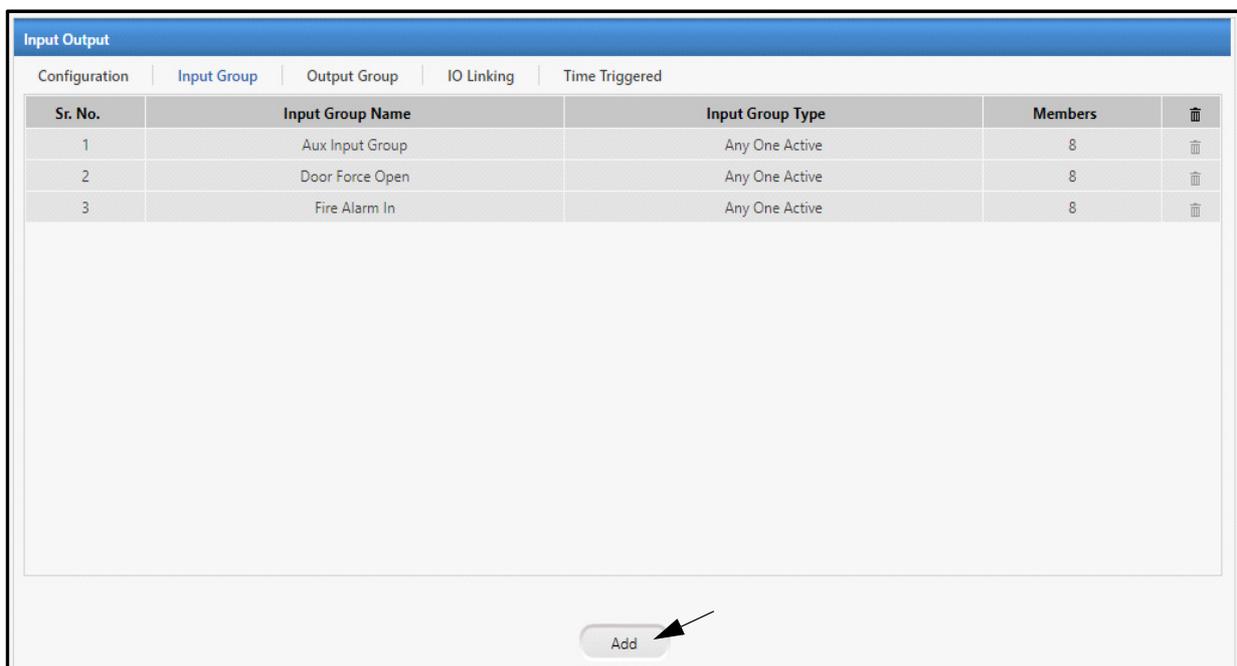
Output Group No.: Specify the Output Group Number to which the auxiliary output is to be assigned based on the output groups defined in the system.

Click **Save** to apply the changes.

Input Group

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 setting the input parameters. You can club any of the inputs (not constrained to particular Door Controllers) 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 Output Groups can be added.



The screenshot shows a web interface titled "Input Output" with a navigation menu containing "Configuration", "Input Group", "Output Group", "IO Linking", and "Time Triggered". Below the menu is a table with the following data:

Sr. No.	Input Group Name	Input Group Type	Members	
1	Aux Input Group	Any One Active	8	🗑️
2	Door Force Open	Any One Active	8	🗑️
3	Fire Alarm In	Any One Active	8	🗑️

At the bottom center of the interface is an "Add" button with an arrow pointing to it.

You can also delete a particular input group from this grid by clicking on Delete button.

Click on the **Add** button to create a new Input Group and also set the input parameters.

Specify the Input Group Name and select the Input Group Type

Select **Source** and **Port** from the list.

Option of port will change automatically as per the selected source.

If you select the **Source** as **“Door”** and **Port** as **“DC_USER_ALLOWED”** or **“DC_USER_DENIED”**, Then a new parameter **“User”** will appear.

By clicking on the pick list button you can select the users.

You can select the user by selecting their respective checkbox.

Maximum 10 users can be selected.

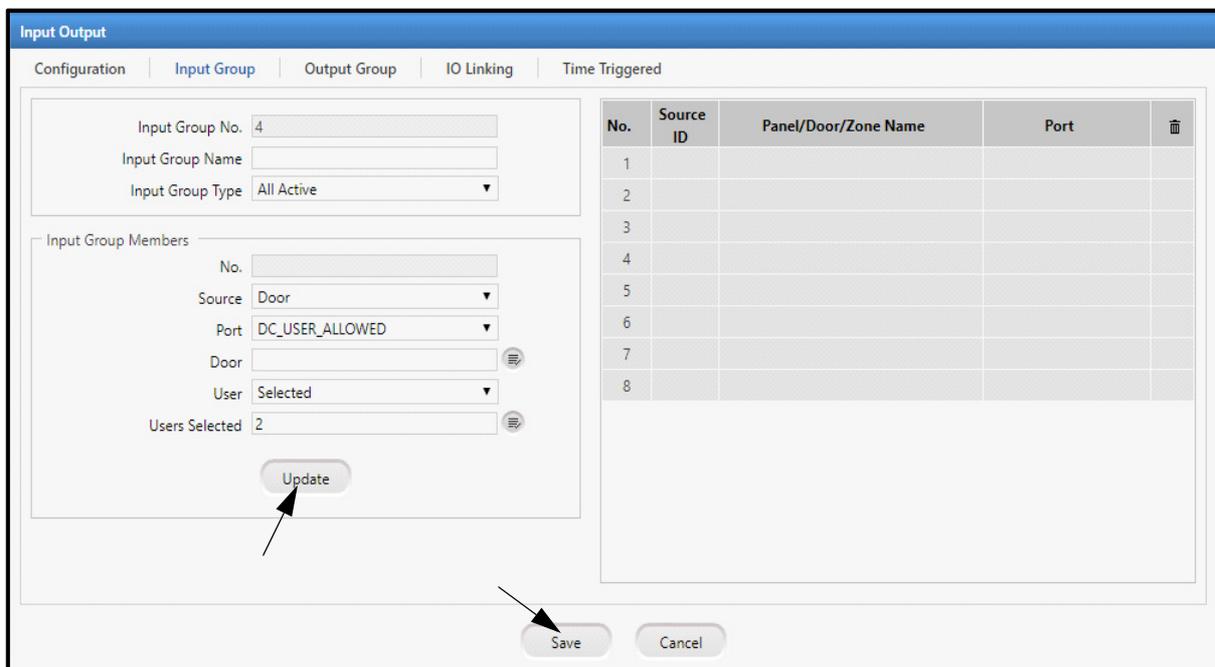
User ID	User Name	
1024	Utsav Pal	<input type="checkbox"/>
1025	Rushi shah	<input type="checkbox"/>
1026	Meet Patel	<input type="checkbox"/>

User ID	User Name	
1024	Utsav Pal	<input type="checkbox"/>
1025	Rushi shah	<input checked="" type="checkbox"/>
1026	Meet Patel	<input checked="" type="checkbox"/>

You can also search the user by “User ID” and “User Name”.

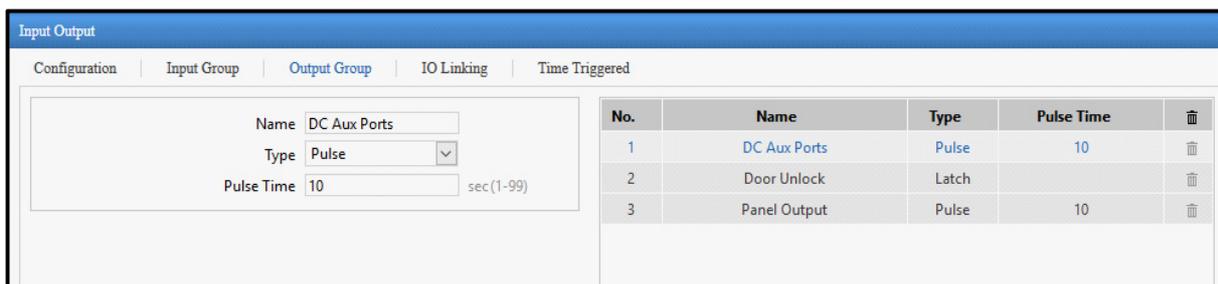


After selecting the users, click Update and Save.



Output Group

This section enables the user to club output ports of Panels and Panel Doors into groups before they can be used in the Input/Output linking programs. Maximum 99 Output Groups can be added.



Specify a user-friendly name for the new Output group.

Type: Select the appropriate Output Group type from the four available options:

- **Pulse:** With this type of output, the user needs to define the **Pulse time** in seconds. The output will be continuously active for the defined pulse time say 5 sec.
- **Interlock:** With 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:** With 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. Eg: During fire alarm, door should be unlocked permanently so Latch output can be used.
- **Toggle:** With this option, the output group toggles its state whenever an input group is activated.

Click the **Add** button and the created group gets appears in the grid.

IO Linking

Input Output Group linking is a feature which enables the user to define programs that activates single or multiple output ports (output Group) based on a trigger received from single or multiple input ports (Input Group) on the Panels and Doors.

To create a new link follow the steps given below:

Link Name: Specify a user-friendly name to the linking program and select the Active checkbox to activate the linking program.

Input Group Name: Click Select Input Group pick-list and select an input group from the list.

Output Group Name: Click Select Output Group pick-list and select an output group from the list.

Time Zone 1-3: Click Select Time Zone pick-list and select the time zone from the list. The Time Zones define the time slots in which the I/O linking Program can be activated.

The screenshot shows the 'Input Output' configuration window with the 'IO Linking' tab selected. On the left, there are input fields for 'Link Name' (Aux Linking), 'Active' (checked), 'Input Group Name' (Aux Input Group), 'Output Group Name' (DC Aux Ports), and three 'Time Zone' fields (Time Zone 1, 2, 3). On the right, there is a table with the following data:

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	🗑️

Click the **Add** button and the created link gets appears in the grid.

Time Triggered

This function enables the user to control the activity of an Output or Output group without manual intervention. The time triggered functions are used for activating events like door unlocks and siren activation which are set as per the start time and for the configured time duration. This functionality is designed to energize outputs for predefined periods at the configured time. Maximum 99 Time Triggered functions can be defined on a single COSEC Panel200.

The screenshot shows the 'Input Output' configuration window with the 'Time Triggered' tab selected. The configuration form on the left includes the following fields:

- Name: Siren Activate
- Active:
- Schedule Time: 13 :00
- Duration: 10 sec(1-65535)
- Days: Sun, Mon, Tue, Wed, Thu, Fri, Sat, Holiday
- Output Port: DC Aux Ports

The table on the right displays the following data:

Name	Time	Duration	Days	O/P	
Siren Activate	13:00	10	_ M T W T F _ _	DC Aux Ports	

To create a new function follow the steps given below:

Name: Specify a user-friendly name to the time triggered function and select the **Active** checkbox to activate the function.

Schedule Time: Set the schedule time at which the function is to be activated.

Duration: Specify the duration in seconds for which the function will remain active.

Days: Select the days on which the schedule is to be activated.

Output Port: Click Select Output Group pick-list to select the output ports from the list.

Click the **Add** button to schedule a time triggered function.

Zone Configuration



Zone Configuration is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

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, each Zone having multiple door controllers. User needs to define the Access Zones before defining the door controllers and assigning the Access Zones.

The page displays a grid containing a list of created access zones and its details.

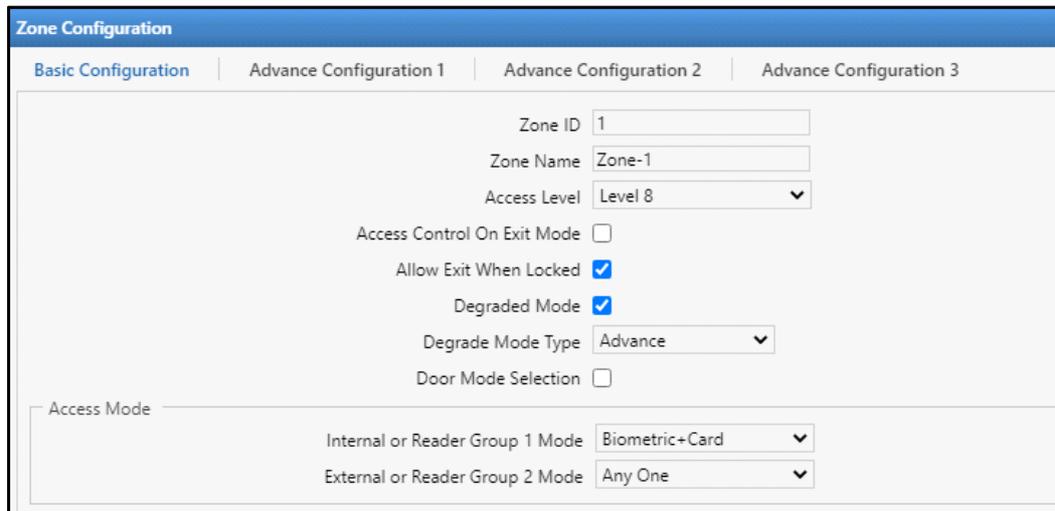
Sr. No.	Zone Name	Access Level	Access Mode 1	Access Mode 2	
1	Zone-1	8	Any One	Any One	

Zone-1 is predefined on the Panel200. You can define additional Zones with unique names.

Click the **Add** button to define a new access zone. While editing or adding an access zone you can also click View List button at the top right corner of the page to go to the main page.

Basic Configuration

In basic configuration of Access control; none of the Access Control functionalities will be applicable for the zone. System will not check the user access level on Time and Attendance zone.



The screenshot displays the 'Zone Configuration' window with the 'Basic Configuration' tab selected. The configuration fields are as follows:

- Zone ID: 1
- Zone Name: Zone-1
- Access Level: Level 8 (dropdown)
- Access Control On Exit Mode:
- Allow Exit When Locked:
- Degraded Mode:
- Degrade Mode Type: Advance (dropdown)
- Door Mode Selection:
- Access Mode:
 - Internal or Reader Group 1 Mode: Biometric+Card (dropdown)
 - External or Reader Group 2 Mode: Any One (dropdown)

Zone ID: The Zone ID is auto generated by the system.

Zone Name: Enter the name of the zone.

Access Level: Select the access level from the drop-down list. The valid access level range can be assigned to a zone from the range 01 to 15.

Access Control on Exit Mode: Select this check-box to enable access control checking for users on exit mode. The following policies will be checked for the user:

- 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 this check-box to enable the user to exit when the door is locked.

Degraded Mode: Select this check box to allow a valid user to access the facility even if the door controller is not in communication with the Panel. Make sure you have enabled Degraded Mode and configured the Degraded Wait Timer under Advanced Profile > Settings.

Degraded Mode Type: If you have enabled Degraded Mode, you can select the Degraded Mode Tye — 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, as well as Access Policies will not be checked if configured. For Exit, user will be allowed to exit only after credential 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 this check-box to allow the user to select the punch type i.e. IN/OUT while punching on the door.

Access Mode

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

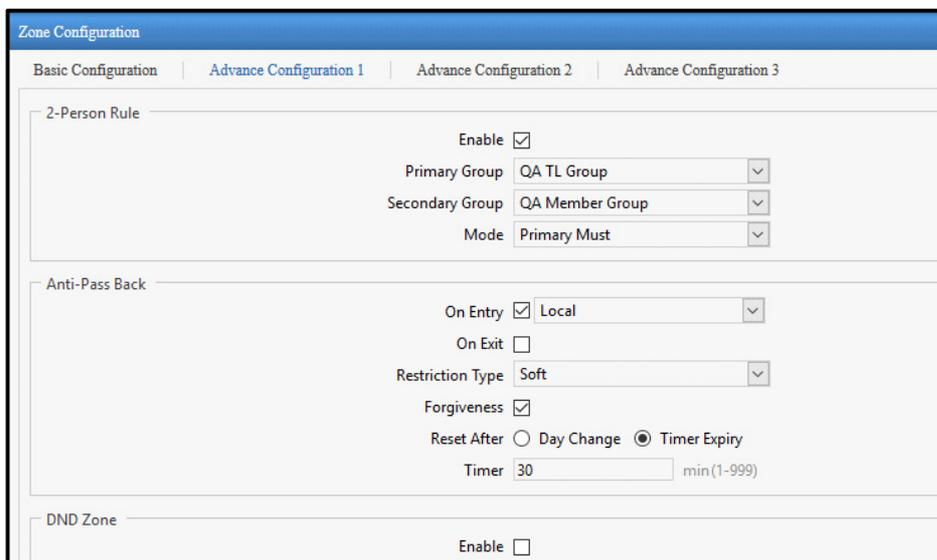
External or Reader Group2 Mode: Select the access mode from the drop-down list.

Click **Save** button to save the Basic Configuration.

Advance Configuration 1

2-Person Rule

This functionality requires two people to present valid credentials to access a secure area. This is typically used in high security areas or in areas where industrial safety is required. Select the **Enable** check-box to enable this feature for the zone.



The screenshot shows the 'Zone Configuration' window with the 'Advance Configuration 1' tab selected. The '2-Person Rule' section is expanded, showing the following settings: 'Enable' is checked; 'Primary Group' is set to 'QA TL Group'; 'Secondary Group' is set to 'QA Member Group'; and 'Mode' is set to 'Primary Must'. The 'Anti-Pass Back' section is also expanded, showing: 'On Entry' is checked and set to 'Local'; 'On Exit' is unchecked; 'Restriction Type' is set to 'Soft'; 'Forgiveness' is checked; 'Reset After' is set to 'Timer Expiry'; and the 'Timer' is set to '30 min(1-999)'. The 'DND Zone' section is collapsed, showing 'Enable' is unchecked.

Primary Group: Select a Primary Group from the drop-down list. This is mandatory because a member from the secondary group has to be always accompanied by a member from the primary group to be considered as a valid transaction. However, any two members from the primary group are treated as a valid user for accessing a Door.

Secondary Group: Select a Secondary group from the drop-down list. A member from this group can be allowed access if accompanied by a member from a Primary Group. If Secondary Group is selected as None then both members from Primary group are required to access the door.



The Groups selected as Primary and Secondary are configured from Access Policies > 2-Person Rule.

Mode: Select the desired mode from the following options:

- **Primary Must** - In this mode, the 2-Person Rule will grant access only when at least 1 user from the 2 person group is from the primary group. i.e. the access is granted if both users are from primary group or 1 from primary and second from secondary group. The only situation when the access will be denied is when both the users are from secondary group.

- **Primary & Secondary Must** - In this mode, the 2-Person Rule will grant access only in one condition, one user from primary group and the other from secondary group. In all other situations the access will be denied.



2-Person Rule is enabled for both entry and exit readers if both are installed.

Anti-Pass Back

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 ID will be accepted a second time at another designated entry reader.

On Entry: Select this checkbox so that the system monitors the entry reader for APB violation. Select the desired option — Local or Global.

- **Local:** In the event of the Local APB, the system applies the Anti-Pass back rule at the Zone level.
- **Global:** In the event of the Global APB, the system applies the rule across all zones at the PANEL level.

On Exit: Select this checkbox also so that the system monitors the entry as well as the exit readers for APB violations.

Restriction Type: Select the restriction type as Hard or Soft option from the drop down.

- **Hard APB:** The access will be denied if the exit is not registered first. It does not allow a second entry using the same card without an exit.
- **Soft APB:** The access will be granted even if the 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.

E.g.: If Anti Pass back in exit mode is configured for the internal port then the system shall display 'Access Allowed' 'Entry Was Not Registered' for Soft Anti Pass Back and for Hard Anti Pass back display 'Access Denied, Entry Not Recorded'.

Forgiveness: Select this checkbox to enable the system to reset the APB status and select the desired reset option:

1. **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 his card for entry in the next morning.
2. **Reset After Timer Expiry:** This will reset the APB status of all the users after the expiry of the Forgiveness timer.
 - **Forgiveness Timer (Mins):** Enter the time duration in minutes after which Anti-Pass Back status will get reset and the pass will be in original state.



Between Anti-Pass Back and Occupancy Control, Occupancy Control has higher priority. So, Forgiveness based on timer expiry won't work when occupancy control feature is enabled.



Forgiveness timer and user IN/ OUT punches will reset; if timer is already running and device gets rebooted.

DND Zone

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.

Select the **Enable** check-box to enable this feature for the zone.

The DND is activated using a special card or through the Menu on the COSEC door.

Enter the **Access level** for DND Zone within a range of 1-15. DND Access Level must be higher than the Zone Access Level so that the unwanted users are restricted to access the DND zone.

Advance Configuration 2

First-IN User Rule

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

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

Once the period is over then system deactivates the access to the designated zone. The system now waits for another valid first in user credential with valid working hours to return the door to normal mode and allow access to users.

Enable: Select this check-box to enable this rule for the zone.

First-IN User Group: Select a First-IN User Group from the drop-down list. These groups are created from *Access Policies > First-IN User Rule*. Eg: The users of “First IN-TL” group can unlock the doors of the selected zone.

Reset After: Select the option to Reset timer — **Working Hours Expiry** or **Timer Expiry**.

- If **Working Hours Expiry** is selected; then first-in user’s punch will remain valid till the working hours of first-in user. Then first-in user has to punch again so that other users can access the premise.
- If **Timer Expiry** is selected; then you must specify the **Timer** in seconds. Say timer is set to 3600sec. So the first-in user punch will remain valid for 1hr. After that first-in user has to punch again so that other users can access the premise.



A VIP user is allowed to access the First-IN enabled 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.

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 on the controlled area.

Enable: Select this check-box to enable the feature for the zone.

A screenshot of a configuration panel titled "Occupancy Control". It contains an "Enable" checkbox which is checked, and a "Max Occupancy Limit" field with the value "4" and a range "(0-999)".

Maximum Occupancy limit: Set the maximum number of users allowed within the selected zone. Suppose max limit is set to 4; then 5th person trying to enter the zone will be denied access to the zone.

Dead Man Zone

This condition allows the tracking of safety and security of a user while performing a specific task, by making it mandatory for the user to show his/her card/finger/face within the pre-defined time period.

A screenshot of a configuration panel titled "Dead Man Zone". It contains an "Enable" checkbox which is checked, a "Warning Timer" field with the value "3" and unit "sec(1-999)", and an "Alert Timer" field with the value "10" and unit "min(3-999)".

Enable: Select this check-box to enable this feature for the zone.

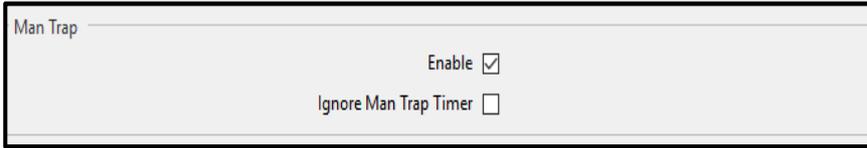
Warning Timer (min): This specifies the minimum time in minutes, within which any user inside the dead man zone should show his card/finger/face to reset the timer and thus prevent the alarm.

Alert Timer (min): This specifies the maximum time in minutes, for which the user is allowed to remain inside the dead man zone.

Man Trap

Mantrap, interlock or airlock systems 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.

Enable: Select this check-box to enable this feature for the zone.



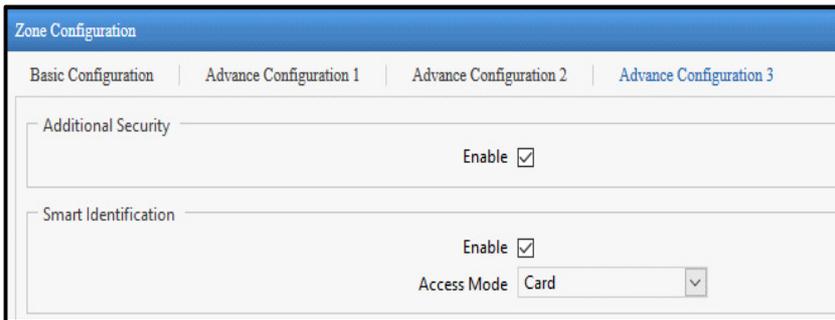
The screenshot shows a configuration window titled "Man Trap". It contains two settings: "Enable" with a checked checkbox and "Ignore Man Trap Timer" with an unchecked checkbox.

Ignore Man Trap Timer: Select the Ignore Man Trap Timer checkbox 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.

Advance Configuration 3

Additional Security

Enable: Select this check-box to enable the Additional Security feature for the Zone.

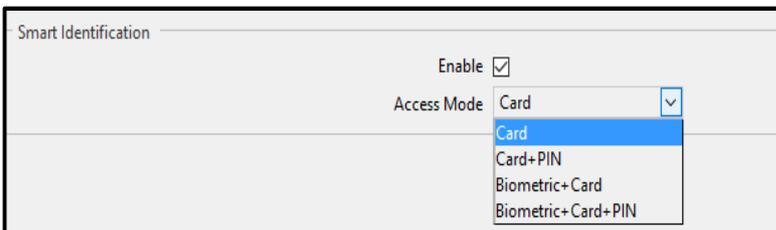


The screenshot shows the "Zone Configuration" interface, specifically the "Advance Configuration 3" tab. It features two sections: "Additional Security" with an "Enable" checkbox checked, and "Smart Identification" with an "Enable" checkbox checked and an "Access Mode" dropdown menu set to "Card".

This Additional Security Check is possible only with Smart Cards which will prevent the duplicacy of 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.

Smart Identification

Enable: Select this check-box to enable the Smart Card Identification feature for the zone.



The screenshot shows the "Smart Identification" configuration window. It includes an "Enable" checkbox checked and an "Access Mode" dropdown menu. The dropdown menu is open, showing options: "Card", "Card+PIN", "Biometric+Card", and "Biometric+Card+PIN".

Access Mode: Select the access mode applicable for Smart Card such as Card, Card+PIN, etc. This enables to identify a user across multiple offices using Smart Card, though not enrolled in these office systems.

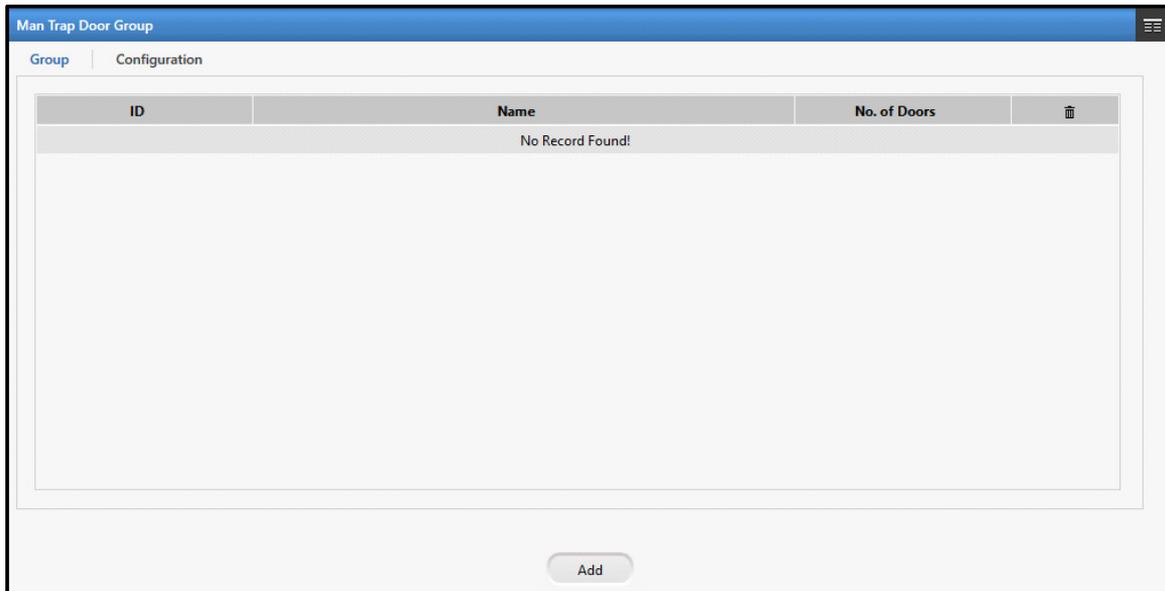
Click **Save** to apply the changes.

Man Trap Door Group



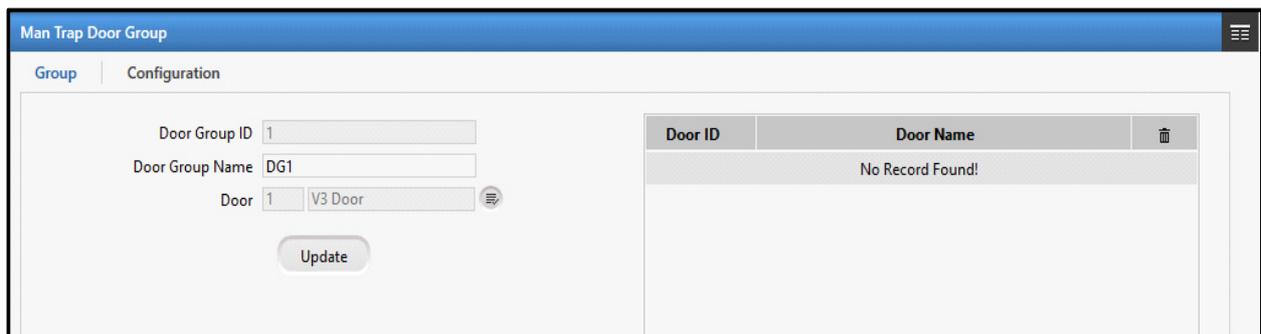
Man Trap Door Group is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

The Man Trap Door Group page enables to configure a group of panel doors. You can create maximum **15** door groups. And maximum **9** panel doors (except IO controllers) can be added in a door group.



Click on **Add** button to configure a door group.

Group

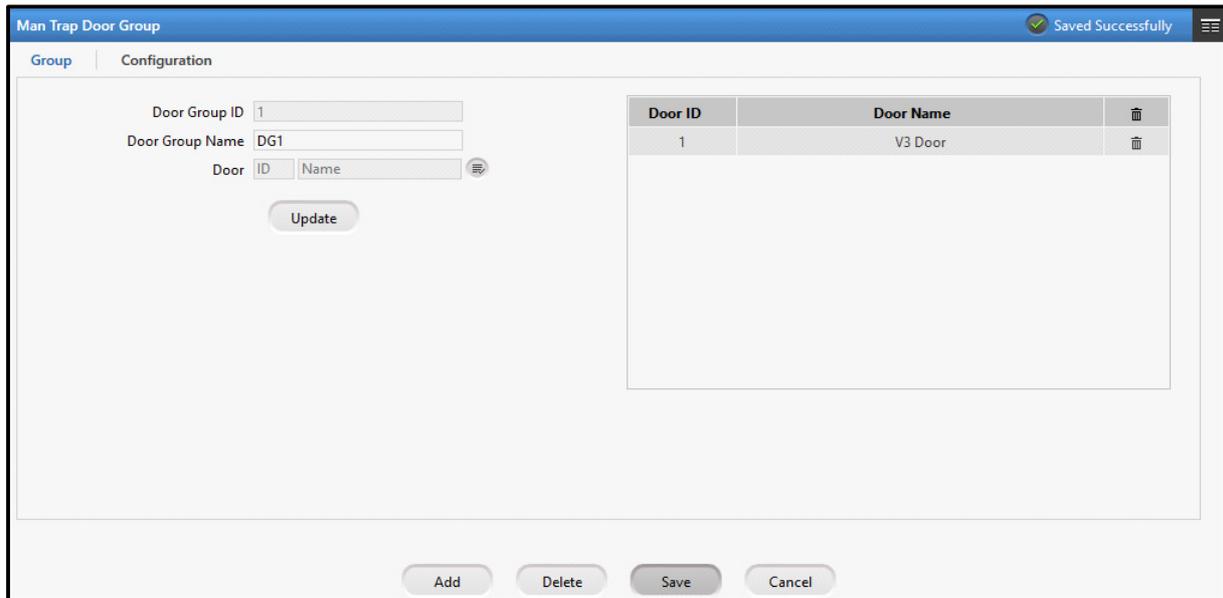


Door Group ID: The Door Group ID is auto-generated by the system.

Door Group Name: Enter the name of the door group.

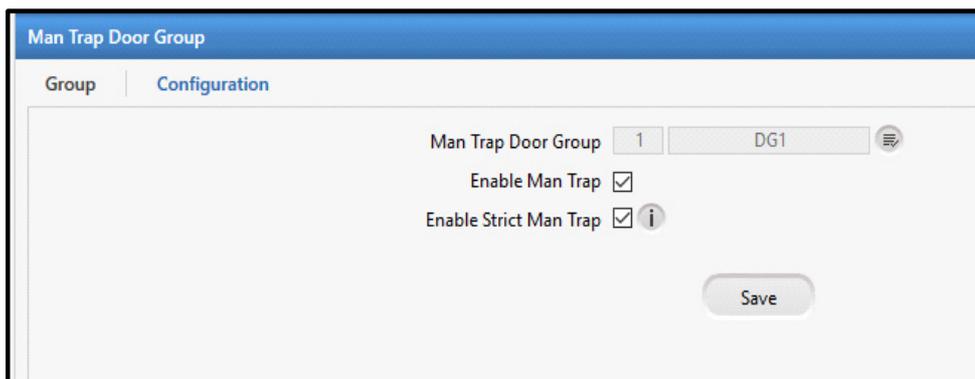
Door: Click the door pick-list button and select the door to be added to the group. You cannot add one door to multiple groups. The doors are configured from *Devices > Door Configuration*.

Click on **Update** to add the selected door to the group. Similarly you can add other doors to the group. Then click **Save** button to save the configured door group.



Configuration

When the Man Trap Door Group is configured then you can configure Man Trap feature on the desired door group.



Man Trap Door Group: Click the pick-list button and select the door group on which man trap is to be configured.

Enable Man Trap: Select this check-box to enable the Man Trap feature on 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 completion of timer then user will be allowed to access the door.



The Man Trap Wait Timer can be set from Panel Configuration > Access Features > Set2.

Enable Strict Man Trap: Select this check-box to enable Strict Man Trap. By this 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. If the user tries to access the second door then he will be denied the access to the door.

Click on **Save** button. The Man Trap Rule will be activated on Door Group.

Network Settings



Network Settings is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

Network Settings page enables configuration of the LAN Settings, Wi-Fi Network Settings, Wi-Fi Access Point Settings, Mobile Broadband Settings, Bluetooth Settings, DDNS Settings and Matrix DNS Settings of the Panel200.

LAN Settings

You can change the IP Address, Subnet Mask, Default Gateway, Preferred DNS and Alternate DNS for the Panel200. The MAC address of the Panel200 is displayed.

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

Field	Value
IP Address	191.168.11.140
MAC Address	00:1b:09:07:db:9a
Subnet Mask	255.255.254.0
Default Gateway	191.168.11.1
Preferred DNS	
Alternate DNS	

At the bottom, there is a 'Test Network Connection' section with an 'Enter URL' input field and a 'Test' button.

To test the network connection of Panel200, enter the URL and click Test button.

Wi-Fi Network Settings



Wi-Fi functionality is available only if your PCB Hardware Version is V2R3 and onwards.

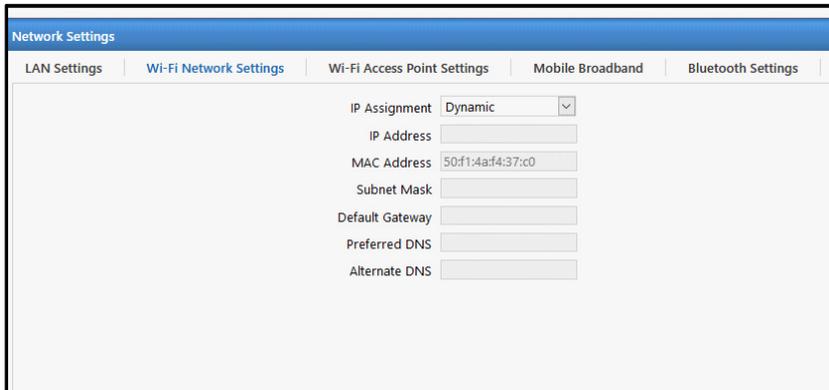
IP Assignment: You can select the IP Assignment mode as either Static or Dynamic.

The screenshot shows the 'Network Settings' interface with the 'Wi-Fi Network Settings' tab selected. The settings are as follows:

Field	Value
IP Assignment	Dynamic
IP Address	
MAC Address	50:f1:4a:f4:37:c0
Subnet Mask	
Default Gateway	
Preferred DNS	
Alternate DNS	

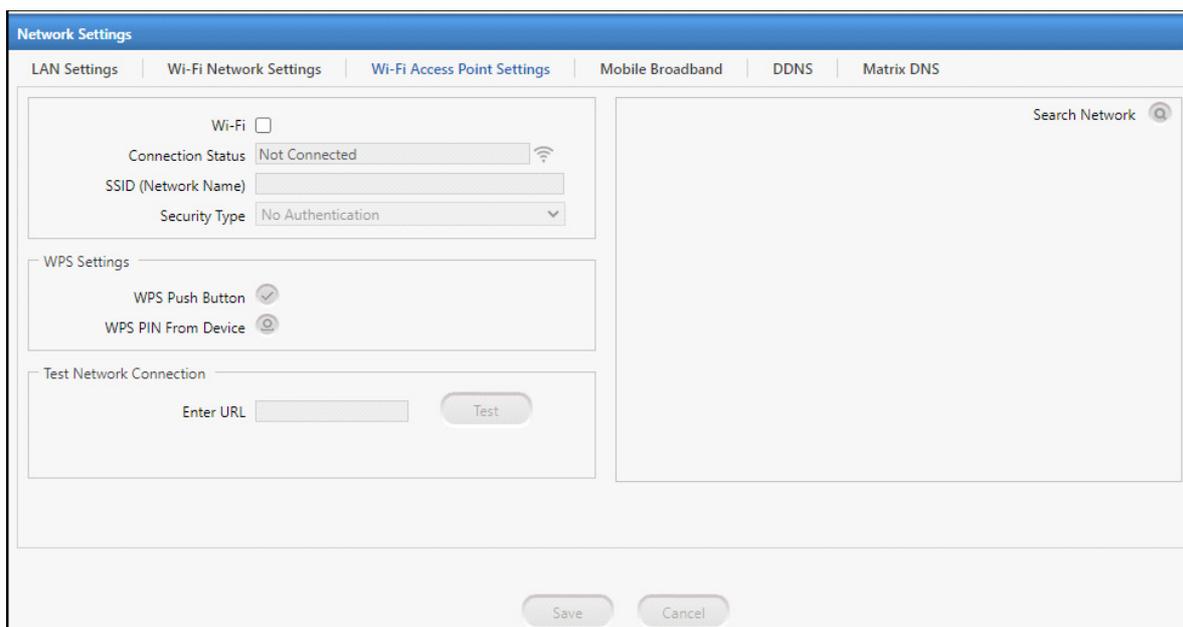
- In **Static** mode specify the IP Address, Subnet mask, Default Gateway, Preferred DNS and Alternate DNS for Wi-Fi access.

- In **Dynamic** mode 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 then keep the IP Assignment mode as Dynamic. When Wi-Fi connection is established, all the Dynamic network settings will be assigned to the Panel200 as shown below.

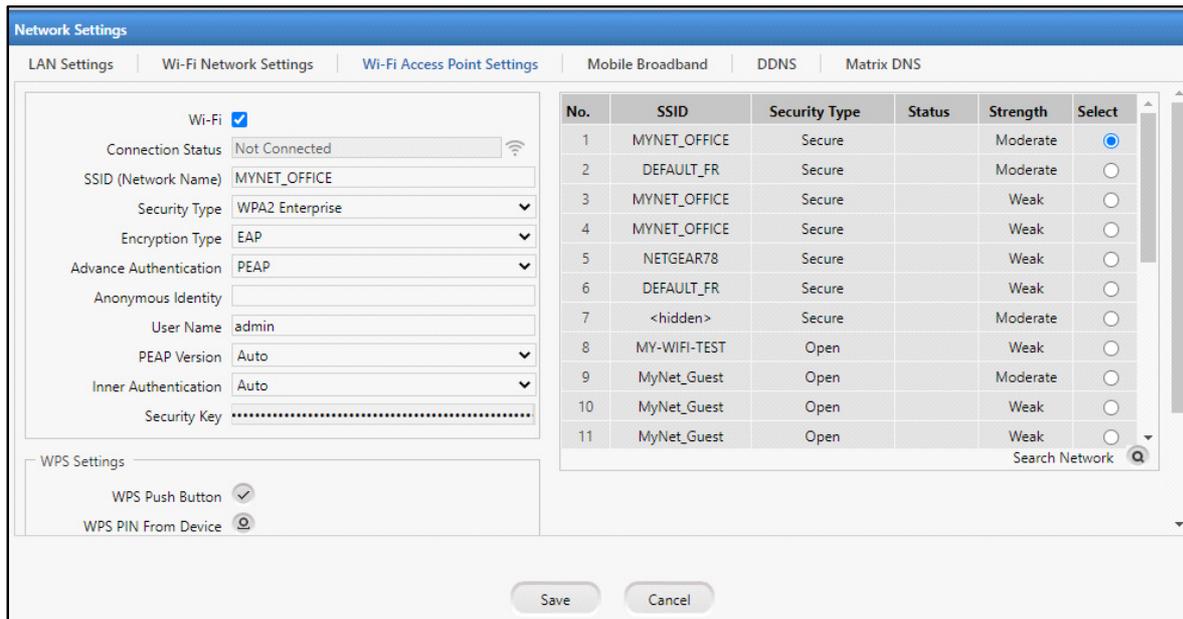


Wi-Fi Access Point Settings

The Wi-Fi Access Point supports wireless connection to communicate between the Standalone Panel200 and the application software. The user has to explicitly configure the security type and encryption option. Only the SSID (Service Set Identifier) field will be automatically detected.

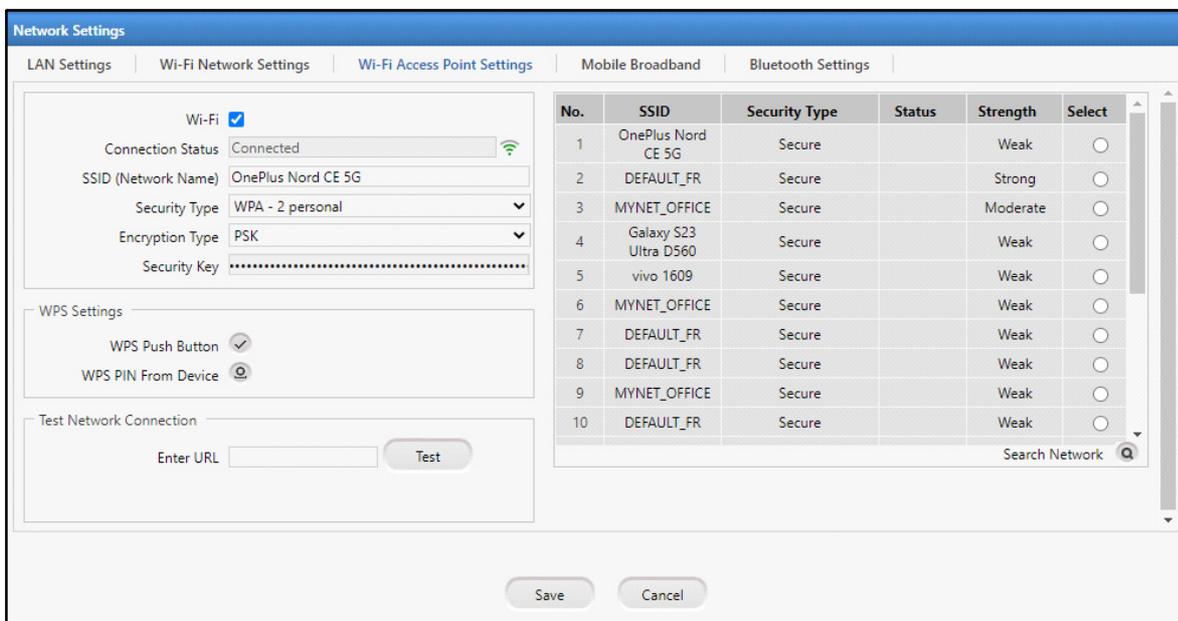


Select the **Wi-Fi** checkbox. Then insert the Wi-Fi dongle in your Panel200 and click on **Search Network** to search the available Wi-Fi networks.

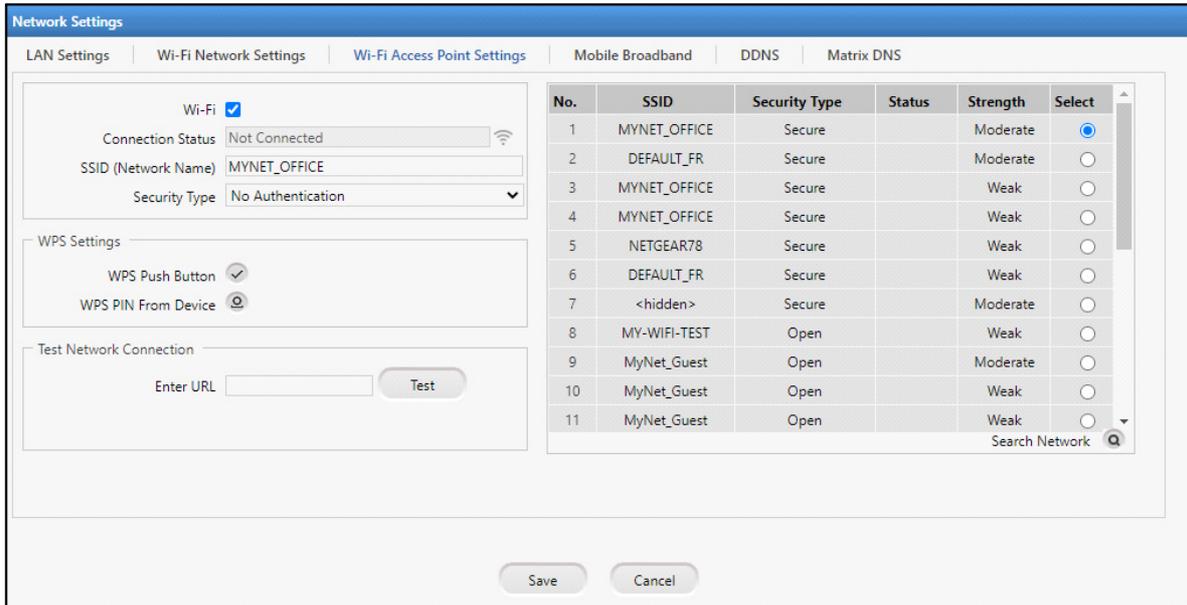


Select a Wi-Fi network from the right grid. The **Connection Status** will display the status of the Wi-Fi network and the Wi-Fi signal strength icon will display the real-time signal strength of the network. The **SSID** and **Security Type** will appear in the respective fields. Depending on the Wi-Fi device you will have to provide Security Key for authentication. Then click **Save** to save the Wi-Fi Access point. When the connection with Wi-Fi is established, **Connection Status** displayed as Connected.

For eg: Using a mobile as hotspot will show WPA-2 personal Security Type. And you have to enter hotspot password in Security Key field.



In some routers no authentication is required as shown below.



WPS Settings

WPS Settings support 2 types of connections:

WPS Push button:

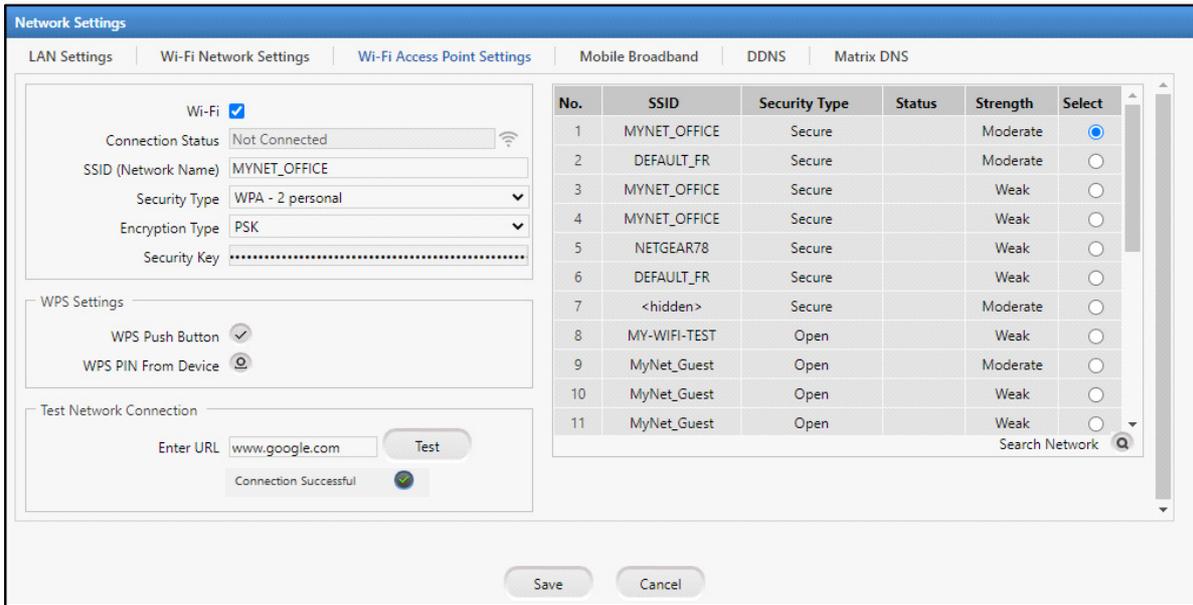
1. If you want to use this option, click the Connect button. The Device will try to establish a connection with the router for 2 minutes.
2. The time period will be displayed.
3. Device treats the connecting state as menu wait state and hence this timer should be reloaded when in this state.

WPS PIN from device:

1. If you want to use this option, click the Connect button. The Device will generate a random 9 digit number and display it in the message.
2. The user must enter this PIN, in the registrar configuration of the router, for establishing connection.
3. Device will establish a connection only for 2 minutes.

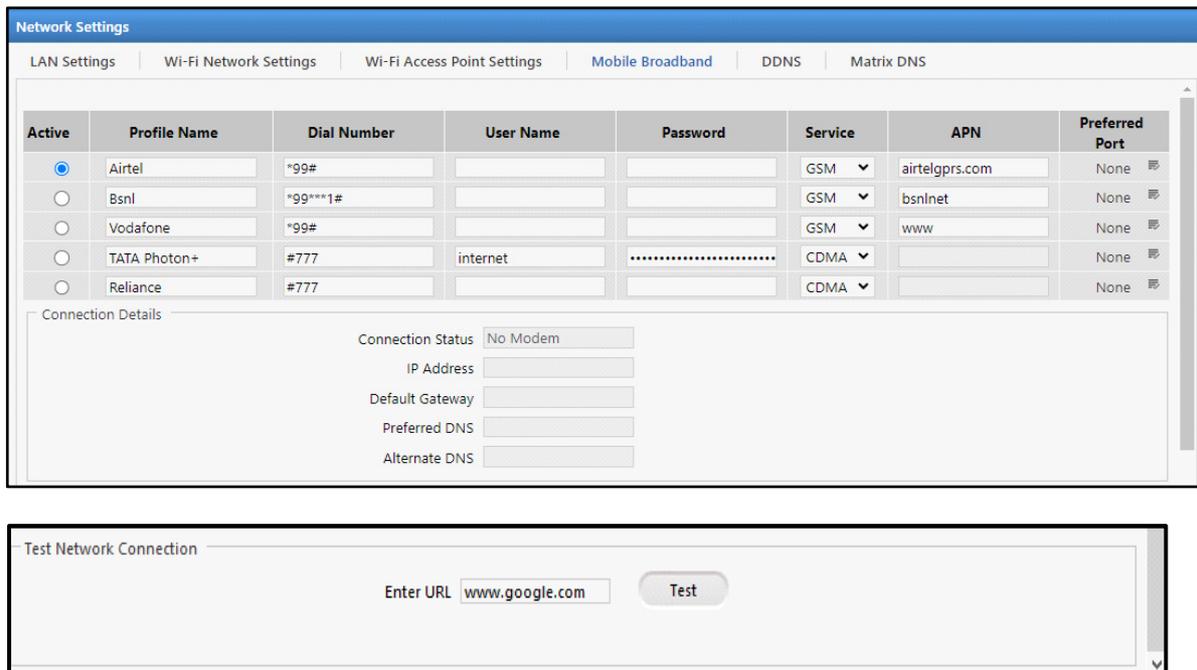
Test Connection

After configuring the above parameters, you can test the network connectivity. Enter the URL and click **Test**.



Mobile Broadband

The mobile broadband using USB dongle connects the system in wireless mode through Internet and transfer data through it. The appropriate broadband USB dongle has to be inserted into the USB port available on the device for broadband communication.



You can configure multiple mobile broadband modem profiles.

The options of dongle are Airtel, BSNL, Vodafone, TATA Photon+ and Reliance-Jio. After connecting the broadband dongle, select the respective profile.

- Specify the **Profile Name**, the **Dial Number** which needs to be dialed to establish connectivity, **User Name** and **Password** for authentication.

- Then service type can be selected from **GSM** and **CDMA**.
- Specify the **APN** (Access Point Name) i.e. the URL to be used to access the respective service provider in case GSM is selected.
- Set the **Preferred Port** as the COM Port on which the device should communicate with the dongle.

The connection details of the selected Profile will display— **Connection Status, IP Address, Default Gateway, Preferred DNS** and **Alternate DNS** address.

Click on **Save** button to save the Mobile Broadband Settings. After configuring the above parameters, you can test the network connectivity. Enter the URL and click **Test**.

Bluetooth Settings



Bluetooth functionality is available only if your PCB Hardware Version is V2R3 and onwards.

Configure the bluetooth settings for Panel200 as shown below.

The screenshot shows the 'Bluetooth Settings' tab in the 'Network Settings' menu. The 'Advertise Bluetooth' checkbox is checked. The 'Name' field contains 'MATRIX'. The 'Range' section has three radio buttons: 'Short (1-2m)', 'Medium (5-7m)' (which is selected), and 'Long (>8m)'. The 'MAC Address' and 'UUID' fields are read-only and display the values 'BCE18A0D760863AABDEFCAFBCA1A8907'.

Advertise Bluetooth: Enable the checkbox to turn-on the bluetooth of Panel200 so that it is visible to the other devices.

Name: Define the name of the bluetooth by which it can be identified for other devices. Default: MATRIX

Range: Select the range for bluetooth as Short, Medium or Long. If Short range is selected then a panel will be visible to the nearby devices which are in the range of 1m to 2m.

MAC Address and **UUID** are read only fields which display the MAC address and UUID of bluetooth.

DDNS



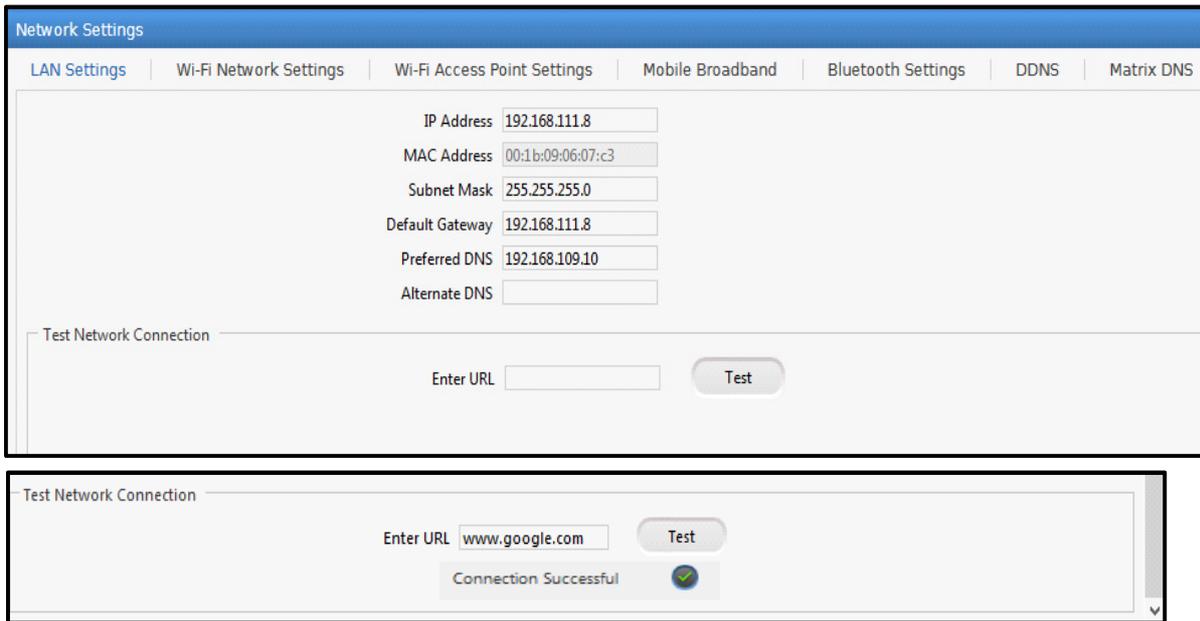
DDNS is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

The DDNS section enables 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 also. Whenever Public IP Address of Panel200 gets changed it automatically gets updated in DDNS server.



This feature will work for LAN interface only.

Before configuring DDNS settings, check the Internet connectivity from LAN settings page by entering URL: www.google.com. Once the connection is successful, the Panel200 is connected with Internet.

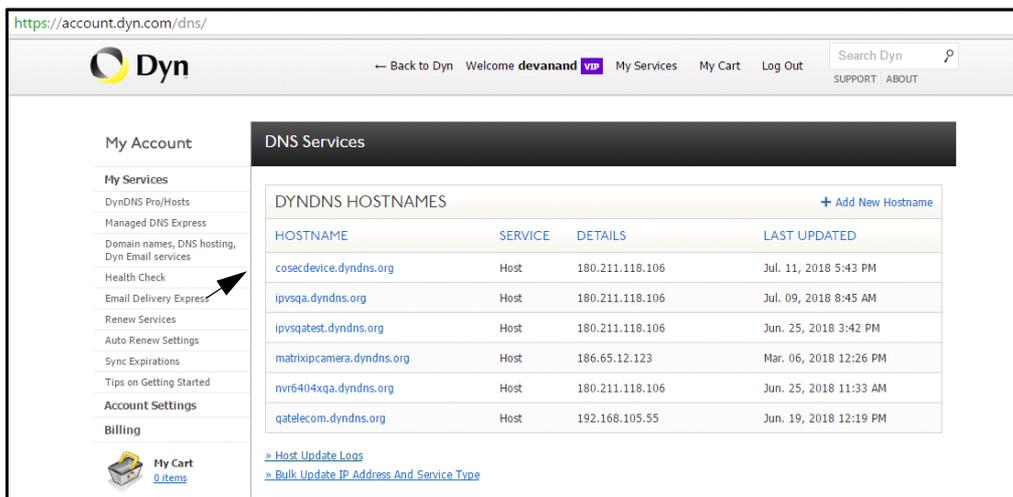


Enable the check-box to activate the registration of host name on DDNS server.

DDNS Server: Select the DynDNS option.

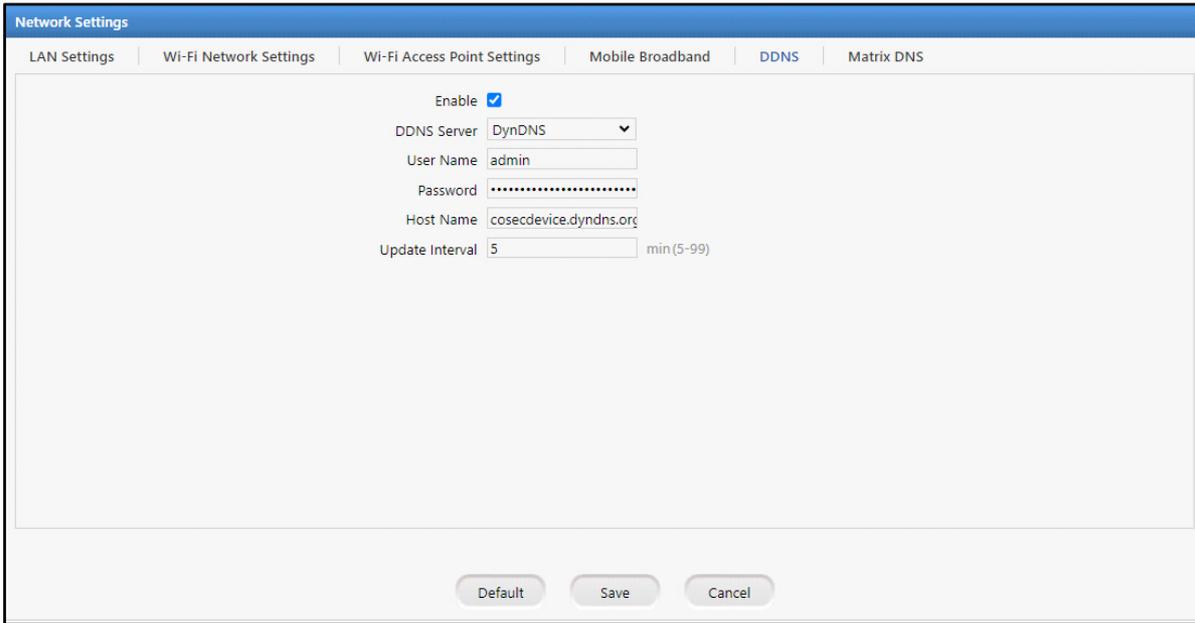
User Name/Password: Enter the user name and password as created by you.

Host Name: Enter the host name as the name registered on DDNS server. Eg: "cosecdevice.dyndns.org"
The Panel200 can be accessed by using this host name. The new host name can also be added if required.

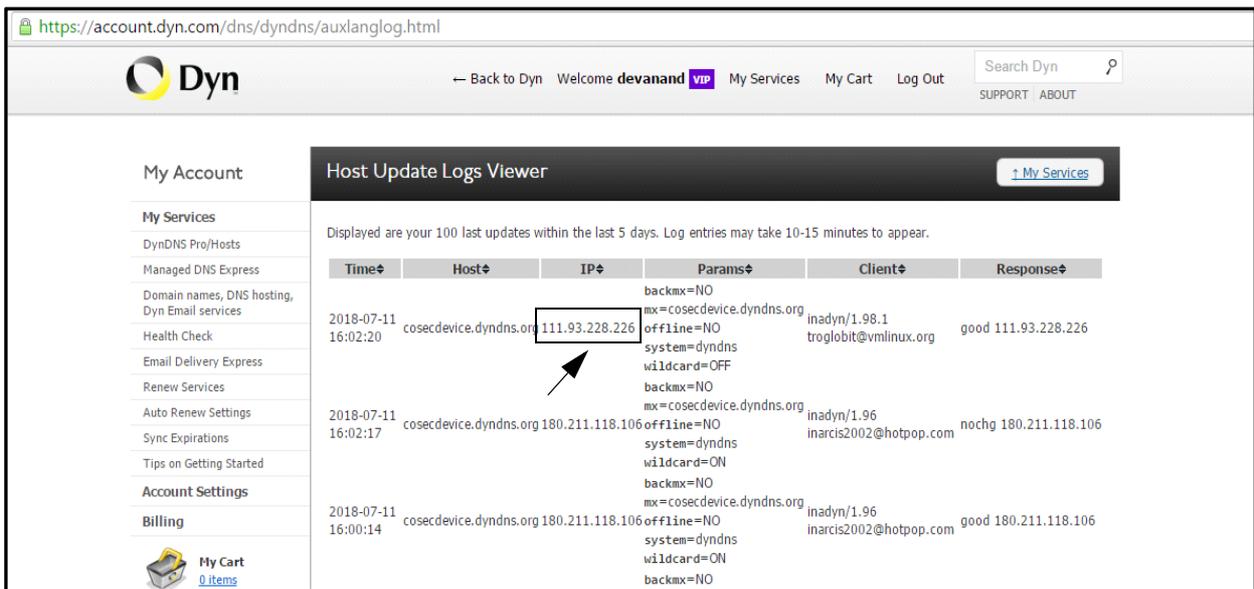


Update Interval: Enter the time in minutes after which device will discover its public IP and update it in selected DDNS server if it is different than the registered one.

Click on **Save** button. The DDNS settings will be saved.



Now you can log into DDNS server by entering URL “account.dyndns.com” and view the registration of host name. The Panel200 is registered by the host name with the public IP as shown below.



You can access the Panel200 by entering host name for eg: “cosecdevice.dyndns.org” in browser.

Matrix DNS



Matrix DNS is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

The Matrix DNS section enables to register Panel200 on Matrix DNS Server by configuring its Hostname. Matrix DNS Server will resolve the IP address of configured host-name and will map the same also.



This feature will work for LAN interface only.

Network Settings

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

Enable

Host Name

Forwarded Port (1-65535)

Update Interval min(5-99)

Default Save Cancel

Enable the check-box to activate the registration of host name on Matrix DDNS server.

Host Name: Enter the host name as the name with which Panel200 can be accessed from the Matrix DNS server.

Forwarded Port: Enter the communication port on which Panel200 will listen. It is 80 by default.

Update Interval: Enter the time in minutes after which device will discover its Public IP and update it in selected Matrix DNS server if it is different than the registered one.

Click on **Save** button. The request will be processed.

Once the host name is registered, the successful registration will be shown as below.

Network Settings Registered Successfully

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

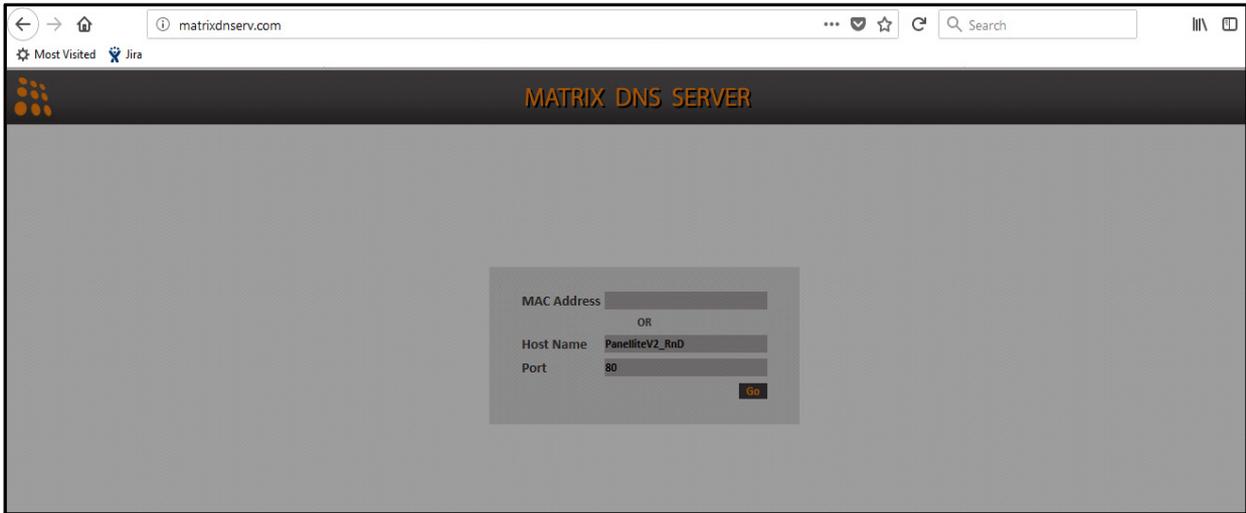
Enable

Host Name

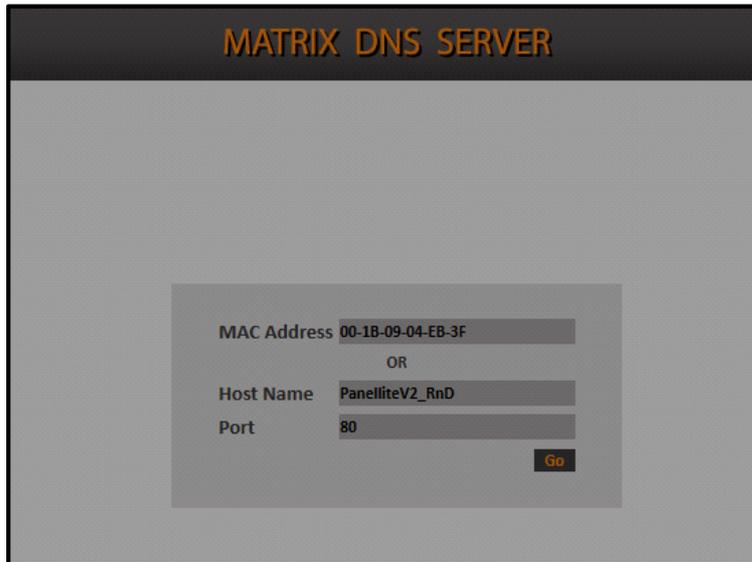
Forwarded Port (1-65535)

Update Interval min(5-99)

Now on Matrix DNS server i.e. URL: www.matrixdnserve.com; you can enter the registered host name.



Once the host name is entered, the MAC address of Panel200 will appear automatically which confirms the registration of Panel200 on Matrix DNS Server.



Matrix DNS Server will resolve the IP Address for configured Host Name. So, now Panel200 can be accessible through same Host Name but with new IP Address.

Date and Time

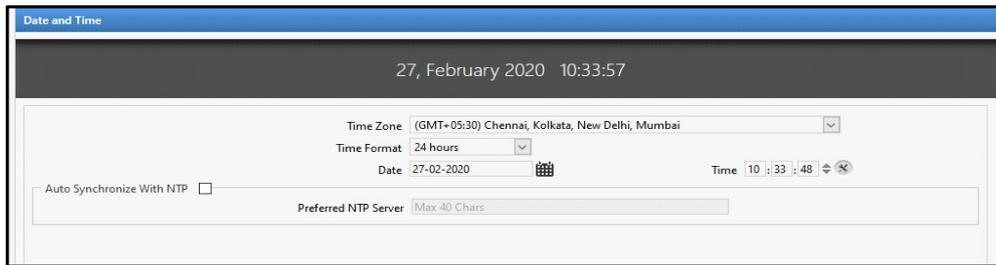
The Date and Time page enables you to view and set date and time parameters for the Panel200 device. The date and time on display displays the current date and time settings on the device.

Time Zone: Select the geographic time zone in which the Panel200 will operate.

Time Format: Select the time format for display as 12 Hours or 24 Hours.

Date/Time: To change date and time manually, select a date using the calendar button and a time by manually entering the value or using up-down arrows.

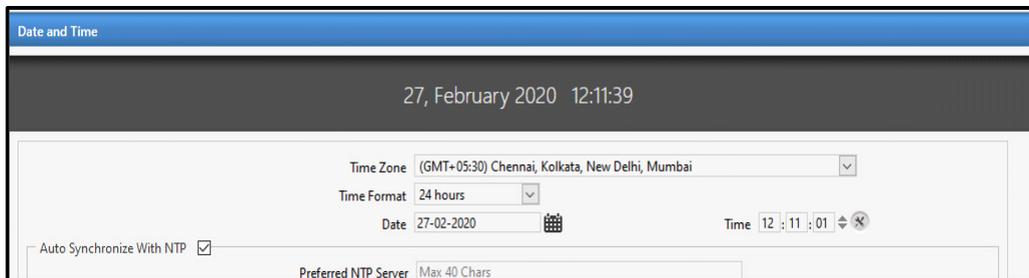
Then click the **Set Date and Time** button to save the manual changes.



The screenshot shows the 'Date and Time' configuration page. At the top, the current date and time are displayed as '27, February 2020 10:33:57'. Below this, there are several settings: 'Time Zone' is set to '(GMT+05:30) Chennai, Kolkata, New Delhi, Mumbai'; 'Time Format' is set to '24 hours'; 'Date' is set to '27-02-2020' with a calendar icon; and 'Time' is set to '10 : 33 : 48' with up-down arrows and a refresh icon. At the bottom, the 'Auto Synchronize With NTP' checkbox is unchecked, and the 'Preferred NTP Server' field is empty with a 'Max 40 Chars' label.

Auto Synchronize with NTP

If Date and Time is to be automatically synchronized as per the Preferred NTP Server (predefined or user-defined NTP server address) selected by user, then you must select the **Auto Synchronize With NTP** check-box.



The screenshot shows the 'Date and Time' configuration page. At the top, the current date and time are displayed as '27, February 2020 12:11:39'. Below this, there are several settings: 'Time Zone' is set to '(GMT+05:30) Chennai, Kolkata, New Delhi, Mumbai'; 'Time Format' is set to '24 hours'; 'Date' is set to '27-02-2020' with a calendar icon; and 'Time' is set to '12 : 11 : 01' with up-down arrows and a refresh icon. At the bottom, the 'Auto Synchronize With NTP' checkbox is checked, and the 'Preferred NTP Server' field is empty with a 'Max 40 Chars' label.

Independent of the mode set from server as Auto or Manual, the user can change the date and time settings from device webpage, which will be reflected on device display.

- When Auto Synchronization with NTP is disabled, Preferred NTP Server field will be disabled.
- When Auto Synchronization with NTP is enabled,
 1. You can specify the Preferred NTP server of your choice. In this case device will first try to get Date and Time from that server address. If it does not get Date and Time in three tries; device will check from 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 device will first check that server. If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen. Valid Values: a-z A-Z 0-9 - . (dot).
 2. You can keep the Preferred NTP server as blank. In this case device will check for Date and Time from the first NTP server.

3. If you have manually entered Date and Time from webpage or Device Menu then those values of Date and Time will be reflected on device webpage and display screen.

Daylight Saving Time (DST)

Select this check-box to **enable** the DST feature.

	Month	Week	Day	Time
Forward Clock	November	First	Sunday	09:00
Reverse Clock	January	Last	Monday	09:00
Duration	05:00			

Save Cancel

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 COSEC Panel200 can be configured to be compatible with this procedure keeping the RTC of the system updated with such changes.

For the Forward Clock, set a month, week, day and time at which the clock is to be set forward. Similarly, set the Reverse Clock. Also, set the Duration in hh:mm format by which the clock is to be set forward or backward.

Example: The above DST Setting implies that on 1st Sunday of November at 09:00 hours, the clock will be forwarded by 05:00 hours. And on last Monday of January at 09:00 hours, the clock will be reversed or set backward by 05:00 hours.

Click **Save** to apply the changes.

Server Settings



Server Setting is configurable only in Panel - Server Mode. (Configuration> Basic Profile> Panel Mode)

The Server Settings enables the device to connect with the COSEC CENTRA or with COSEC VYOM through the available interface.

The screenshot shows the 'Server Settings' configuration window. It is divided into three main sections: 'License Server', 'Web Server', and 'Connectivity Status'.
- **Connectivity Status:** Shows 'via Ethernet' with a green dot.
- **License Server:** Shows 'Disconnected' with a red dot and 'USB Port Disabled' with a red dot. The URL is '192.168.50.100' and the port is '15025'.
- **Web Server:** Shows 'Encryption (HTTPS)' as unchecked, 'Interface Selection' as 'Auto', 'Network Interface' as 'Ethernet', 'URL' as '192.168.103.88' and '80', 'Directory Name' as 'cosec', and 'Request Retry Timer (min)' as '2'. There is a 'Test' button next to the URL fields.
At the bottom, there are 'Default', 'Save', and 'Cancel' buttons.

Connectivity Status: It displays the Centra or Vyom connection status.

Server Connection: Select the server as COSEC CENTRA or COSEC VYOM with which the device is to be connected.



1. For device based license reading; Panel200 must be connected with COSEC Centra.
2. When you change the server; all settings except network settings will be set to default.

COSEC CENTRA

Configuration: Basic

URL: Enter the IP Address or Host Name of the server where Monitor service is running. Then enter the Port number through which the Panel200 is to be connected. It is the TCP listening port. The default port number is 11000.

The device connectivity will show green when monitor service is running at the Centra server and Panel200 is added in COSEC Centra server. You can manually add or Auto add Panel200 in Devices module.

Eg: Here Panel200 is added to the Centra server with IP address 192.168.104.12 and device port 11000.

Configuration: Custom

For Custom configuration you can enter 3 different URL and Port for different interfaces.

Ethernet URL: Enter the IP Address or Host Name of the server. Then enter the Port number through which the Panel200 is to be connected.

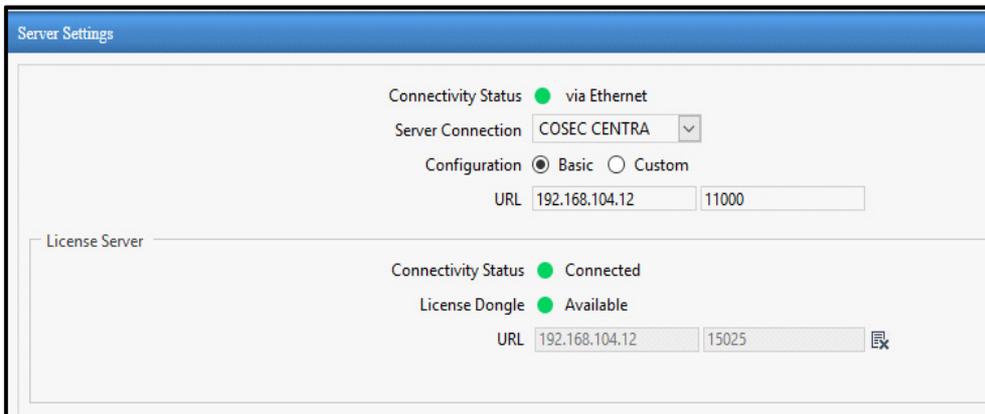
Wi-Fi URL: Enter the IP Address or Host Name of the server. Then enter the Port number through which the Panel200 is to be connected.

Broadband URL: Enter the IP Address or Host Name of the server. Then enter the Port number through which the Panel200 is to be connected.

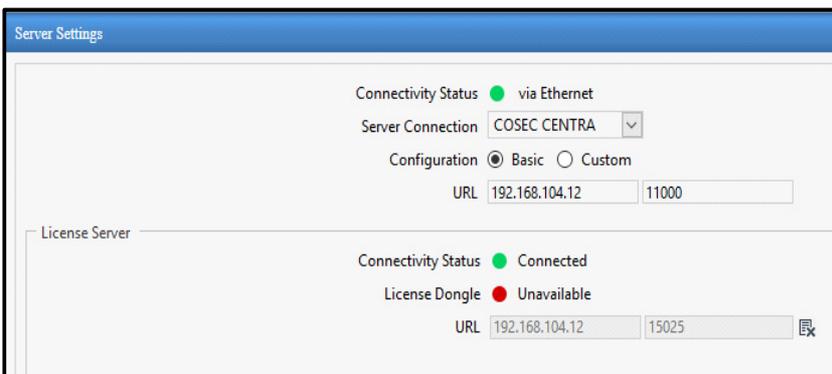
Your device will get connected to the configured server with the available interface.

License Server

Connectivity Status: It displays the connectivity status with license server.



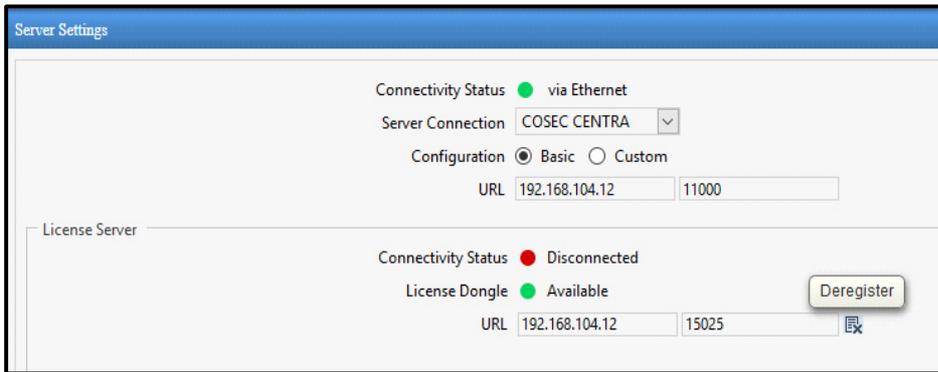
License Dongle: It displays the status if dongle is available on device or not. When dongle is ejected from the Panel200, then it will show red color with Unavailable status.



URL: Enter the IP Address or Host Name of the license server where the Master service is running. Then enter the Port number of the license server.

DeRegister : Click on DeRegister button to stop the communication with the current license server.

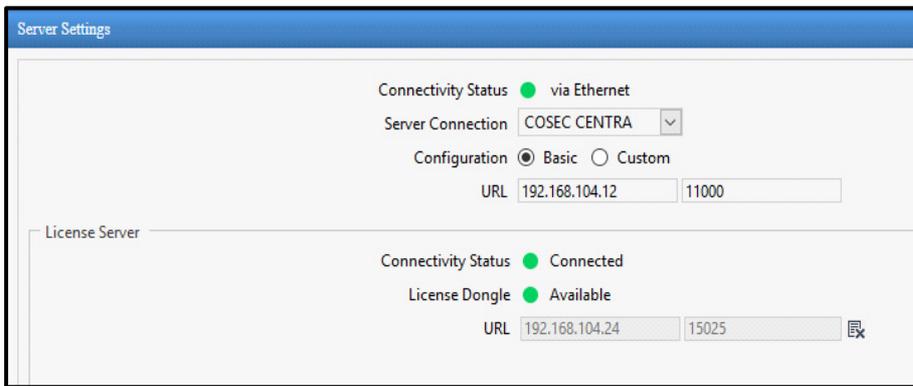
The connectivity status will become disconnected as shown below.



Now enter the IP address of another license server where Master service is running.



Ensure that the new license server is in Device based licensing mode and is not getting license from another device.



Then click **Save** button. Once Panel200 is connected to the license server, connectivity status will show green color. Hence the Master service on the new license server will get license key available in dongle through the Panel200 and will dispatch the same to other services.

COSEC VYOM

URL: Enter the IP Address or hostname of COSEC VYOM where it is hosted. Hostname can be maximum of 253 characters.

Port: Enter the device listening port of Master service. The default port is 15025.

Tenant ID: Enter the tenant ID in which the device is to be connected.

Server Settings

Connectivity Status ● Ethernet: Connecting..

Server Connection COSEC VYOM

URL 192.168.102.226 15025

Tenant ID 1

Redirected Server 192.168.102.226 15025

Server Settings

Connectivity Status ● via Ethernet

Server Connection COSEC VYOM

URL 192.168.102.226 15025

Tenant ID 1

Redirected Server 192.168.102.226 11009

Once the device gets connected with Master service, then Master Service will fetch the Tenant ID and its IP address and Port where device will be redirected. The device will then be added to the monitor service of the tenant.

While adding, ensure that “Auto addition of device” is enabled in the server or you have to add device manually.

Web Server



Web Server configurations are applicable for Panel - Server Mode only.

- **Encryption (HTTPS):** Select the Web Server Encryption check box to establish secure HTTPS connection with Web Server to access Panel 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, select the desired **Network Interface — Ethernet, Wi-Fi** or **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, Panel will communicate will configured Server with available interface with predefined priorities.

- **URL:** Configure the URL (IP Address/ Domain Name) of COSEC Centra or COSEC VYOM with which the device 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 the **Test** button 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.

Once Panel200 is connected, the connectivity status will be displayed in green color.

CCC Settings



CCC Settings are configurable only in Panel - Server Mode. (Configuration > Basic Profile > Panel Mode)

The CCC settings enable the COSEC devices to communicate with third party application and send events using TCP notification.

This functionality will enable the user to send events from the Device to a Command and Control Centre (CCC) as well as receiving commands from a CCC and implementing those commands in the device.

CCC Settings

TCP Notification

IP Address

Port (1024-65535)

Interface Selection Auto Manual

Network Interface ▼

Select the **TCP Notification** checkbox to enable the functionality.

IP Address: Specify the IP Address of the computer on which the TCP Server application has been installed.

Port: Specify the TCP listening port of the TCP server application.



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

Interface Selection: Select the interface option as Auto or Manual.

- Network Interface: For Manual selection; Select the network interface option as Ethernet, WI-FI or Mobile Broadband for the network connectivity. Device will communicate with configured server through selected interface only.
- In Auto selection; Device will communicate will configured server with available interface with predefined priorities.

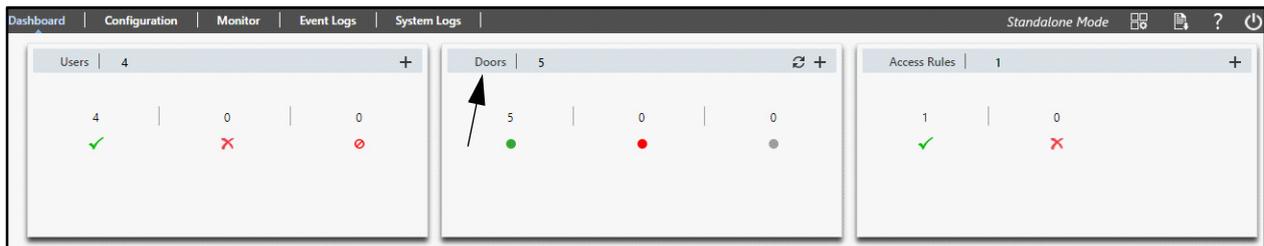
Click on **Save** button to save the settings.

The Devices section enables you to add different type of devices such as PATH Door, PVR Door, VEGA Door, ARGO Door, ARGO FACE Door, ARC Controllers, V1/2/3/4 Door and set the basic and advanced configurations.

You can assign 4 special functions to the arrow keys of Panel Door keypad to facilitate the user to navigate through the device menu and access the door easily.

For more details, [See “Door Configuration” on page 94.](#)

The total number of devices configured in Panel200 are displayed on the Dashboard. The number of Online Devices, Offline Devices and Inactive Devices are also displayed on the Dashboard.



You can also integrate COSEC devices with SATATYA devices to get images and videos triggered by user events at doors.

For more details, [See “Video Surveillance” on page 122.](#)

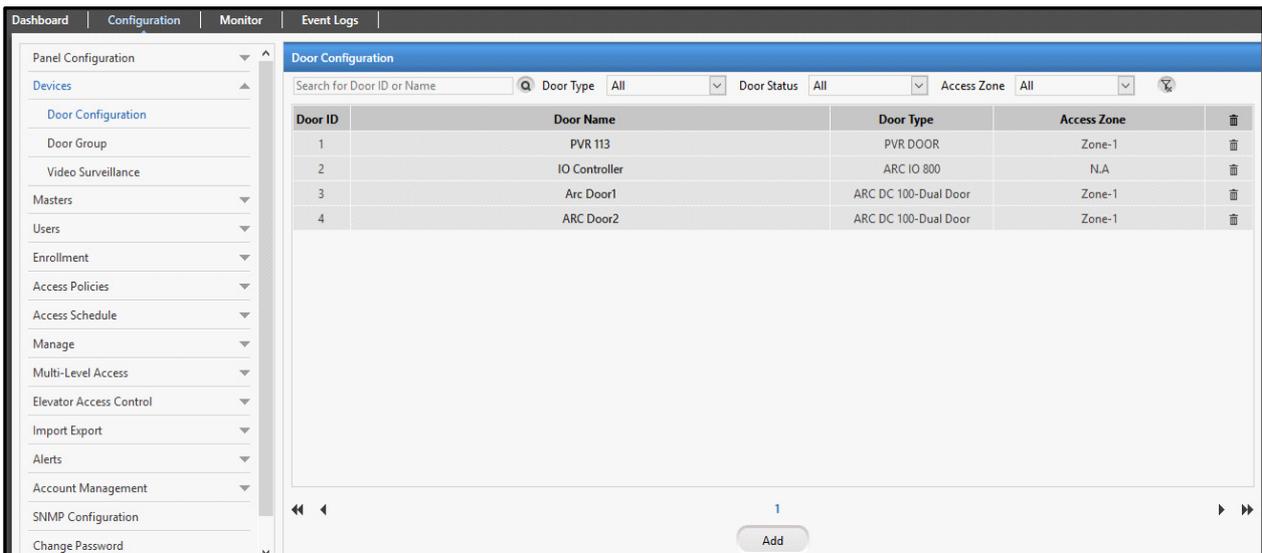
Door Configuration

This page enables user to add slave door controllers to the Panel200 and configure parameters for each door. A Panel200 can control upto 255 doors using Ethernet communication and upto 32 doors using Rs-485 communication. All the configured device details appear in the Device Report. For details, refer to “[Device](#)”.

The grid displays the doors with their details — Name, Type and Access Zone.

You can Search for the desired door using the search filters.

You can also delete a particular door by clicking on Delete icon.

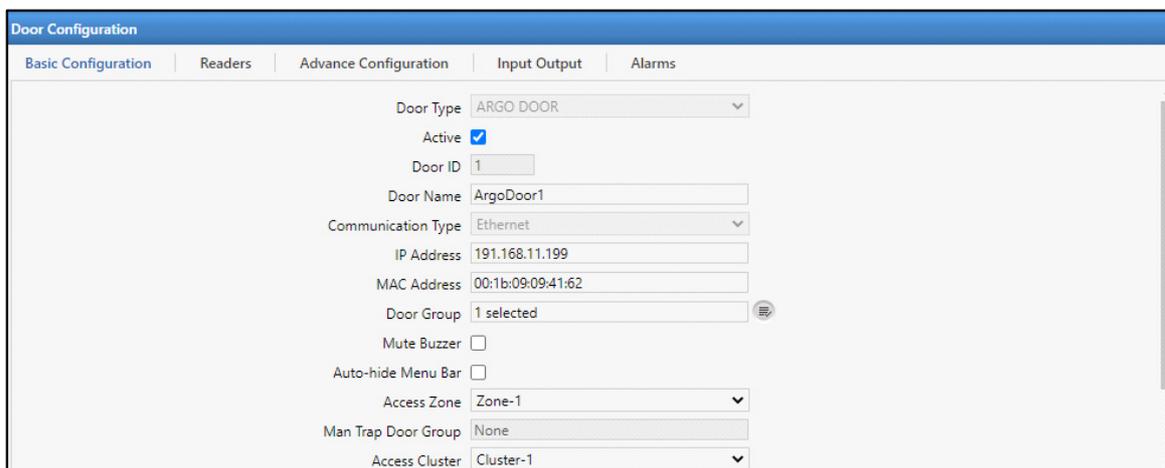


The screenshot shows the 'Door Configuration' page in a web interface. On the left is a navigation menu with options like 'Panel Configuration', 'Devices', 'Door Configuration', 'Door Group', 'Video Surveillance', 'Masters', 'Users', 'Enrollment', 'Access Policies', 'Access Schedule', 'Manage', 'Multi-Level Access', 'Elevator Access Control', 'Import Export', 'Alerts', 'Account Management', 'SNMP Configuration', and 'Change Password'. The main area displays a table with the following data:

Door ID	Door Name	Door Type	Access Zone	
1	PVR 113	PVR DOOR	Zone-1	
2	IO Controller	ARC IO 800	N.A	
3	Arc Door1	ARC DC 100-Dual Door	Zone-1	
4	ARC Door2	ARC DC 100-Dual Door	Zone-1	

At the bottom of the table, there is a pagination control showing '1' and an 'Add' button.

To add a new door click **Add** button and configure the following parameters.



The screenshot shows the 'Door Configuration' page with the 'Basic Configuration' tab selected. The configuration form includes the following fields:

- 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



In Panel - Server Mode, select a door to view its details. Certain fields may appear as read-only fields in this mode.

There are various variants of all the COSEC devices, hence the features and functionalities supported will depend on the device and the variant installed.

To configure, click each link:

- [“Basic Configuration”](#)
- [“Readers”](#)
- [“Advance Configuration”](#)
- [“Advance Configuration 2”](#)
- [“Input Output”](#)
- [“Special Function”](#)
- [“Alarms”](#)
- [“Face Identification Settings”](#)

Basic Configuration

Door Type: Select the type of door controller to be added. You can select the door type from the drop-down list of V1 DOOR/V2 DOOR/V3 DOOR/PATH DOOR/PVR DOOR/VEGA DOOR/ARC DC100/ARC DC200/ ARC IO 800/ ARGO DOOR/ ARGO FACE DOOR.

Mode (Only for ARC DC 100 and ARC DC 200): Select the mode of ARC DC 100/ARC DC 200. You can select Single Door to control a single door or select Dual Door to control two doors from a single ARC DC 100/ARC DC 200.



ARC as 2 door is supported in both Standalone and Server mode.

Active: Select the check box to enable the device in the network.

Door Name: Enter a user-friendly name for the door. The ID will be auto generated by the system.

Communication Type: Select the type of communication with the Panel200 as Ethernet or RS-485.

IP Address: Enter the IP address of the door. Once the door is connected with the Panel200, the status of the door will be displayed as Online in Monitor.

MAC Address: Specify the MAC Address of the door.

Door Group: It displays the door group in which the selected door is added. The door can be added to the group from Door Group.

If the mode of ARC DC 100/ARC DC 200 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 Door2 respectively.

If the mode of ARC DC 100/ARC DC 200 is selected as Dual Door with Single Readers, then along with the above parameters configure Door Name and Mute Buzzer for Door 1 and Door2 separately. Access Zone is configured earlier.

Connect Doors with: This parameter will appear when you add ARC DC 100/ARC DC 200 in Dual Door mode.

- Select the option as **Single Reader** for both the doors to communicate with only one reader (Reader1).
- Select the option as **Dual Readers** for both the doors to communicate with individual readers, i.e. Door1 with Reader1 and Door2 with Reader2.

Mute Buzzer: Select this check box to mute the door buzzer.

Auto-hide Menu Bar: Select this check box to hide the menu bar automatically on the device display screen.



Auto-hide Menu Bar is applicable for VEGA, ARGO and ARGO FACE 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 this inverse polarity check box to get buzzer output when any event (eg: user allowed) is generated.

This is applicable for ARC Dual Door Dual Reader, Dual Door Single Reader and ARC Single Door.

Access Zone: Select an access zone you wish to assign to the door.

Man Trap Door Group: It displays the man trap door group assigned to the specific door. To create/assign a man trap door group go to *Panel Configuration > Man Trap Door Group*.

Access Cluster: Select the configured Cluster from the dropdown list to which the door is to be assigned.

Allowed Acknowledgment

Display Duration: Specify the duration for which the acknowledgment message should be displayed on the device display screen.

LED-Buzzer Duration: Select the duration for which the buzzer should be triggered from the drop-down list.

Hover-over the icon to view the details of Display Duration and corresponding LED-Buzzer Duration.

Denied Acknowledgment

Display Duration: Specify the duration for which the acknowledgment message should be displayed on the device display screen.

LED-Buzzer Duration: Select the duration for which the buzzer should be triggered from the drop-down list.

Hover-over the  icon to view the details of Display Duration and corresponding LED-Buzzer Duration.



Allowed/Denied Acknowledgment is applicable for PVR, VEGA, Door V3, Door V4, PATH V2, ARC DC200, ARGO and ARGO FACE Door.

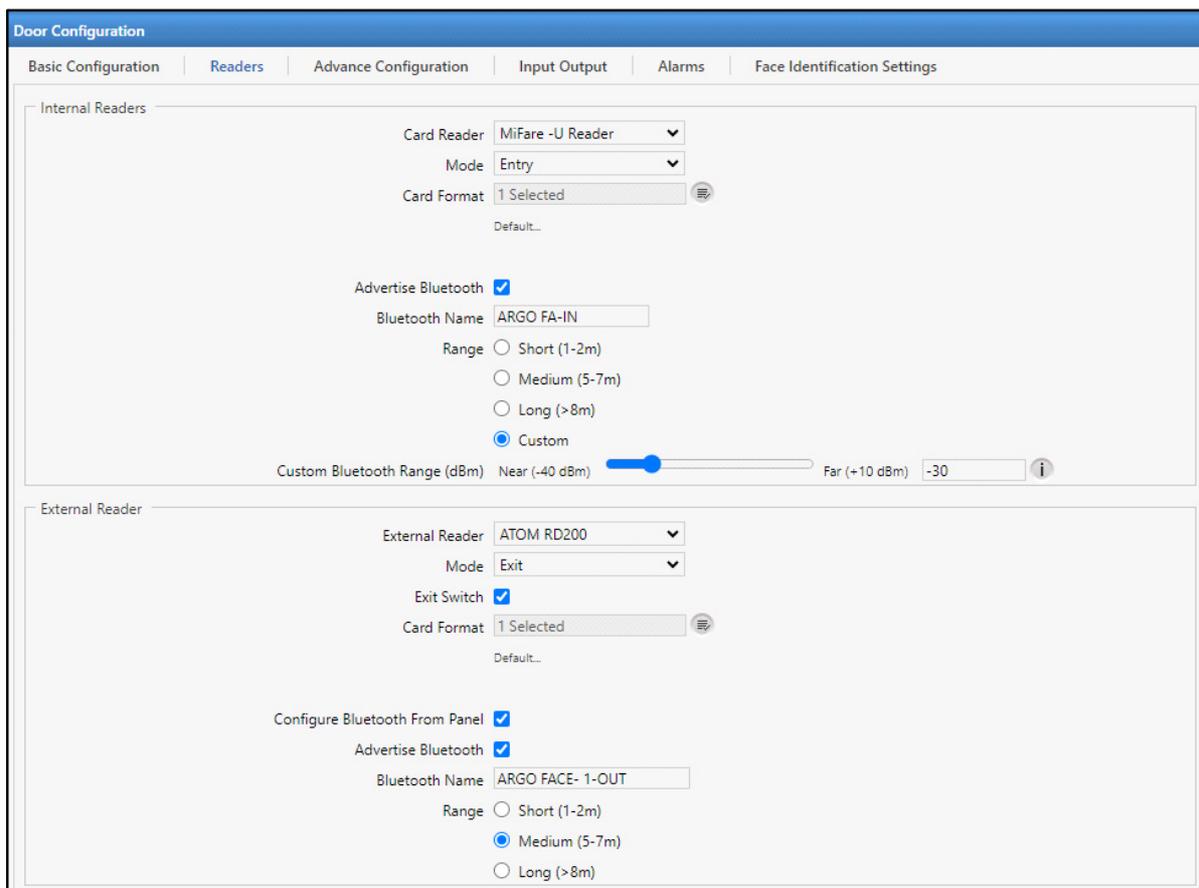
The following is applicable to ARGO, VEGA, ARGO FACE, PATH V2 and ARC DC200 only:

- *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

As per the door type selected there are different parameters for configuring readers.



The screenshot shows the 'Door Configuration' window with the 'Readers' tab selected. It is divided into two sections: 'Internal Readers' and 'External Reader'.

Internal Readers:

- Card Reader: MiFare -U Reader
- Mode: Entry
- Card Format: 1 Selected
- Default... (button)
- 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

External Reader:

- External Reader: ATOM RD200
- Mode: Exit
- Exit Switch:
- Card Format: 1 Selected
- Default... (button)
- Configure Bluetooth From Panel:
- Advertise Bluetooth:
- Bluetooth Name: ARGO FACE- 1-OUT
- Range: Short (1-2m), Medium (5-7m), Long (>8m)

Internal Readers

Configure the following parameters:

Select type of **Card Reader** and **Finger/Palm Vein Reader** from the drop-down list.

Select the **Mode** — **Entry** or **Exit**.

To select the **Card Format**, click the **Select Card Format** button and select the desired format. Then click **OK**.

Select **Advertise Bluetooth** check box to enable Bluetooth of the reader. Then configure the following parameters. By default, if the Device Name is configured then in **Bluetooth Name**, Device Name will be displayed here along with the Mode type. The prefix will be the Device 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.

The system 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, enter 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.



Custom option for Bluetooth Range is applicable to ARGO, VEGA, ARGO FACE, PATH V2 and ARC DC200 only.

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

External Reader

Select the type of External Reader from the drop-down list.



Finger Reader is not applicable for ARGO FACE Door.

Select the Mode — **Entry** or **Exit**.

Select the Exit Switch check-box to enable.

To select the Card Format, click the Select Card Format button and click the desired format and then click OK.



To create card formats click Masters >> Card Format. To know more see, "[Card Format](#)".

When you select **External Reader** as — CB U Reader, ATOM RD300, ATOM RD200 or ATOM RD100, select **Configure Bluetooth from Server** check box to enable Bluetooth feature for the devices with aforementioned external readers.

Select **Advertise Bluetooth** check box to enable Bluetooth of the reader. Then configure the following parameters.

By default, if the Device Name is configured then in **Bluetooth Name**, Device Name will be displayed here along with the Mode type. The prefix will be the Device 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.

The system 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)**.

When **External Reader** is selected as **UHF Reader** from the dropdown list then only **Re-detection Delay** parameter will be visible and configurable.

Re-detection Delay - Enter the value of this parameter to configure the time interval during 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 DC 100 Reader

For **Single Door ARC DC 100** configure the following parameters for **Reader1 Group** and **Reader2 Group**.

RS-485 Reader: Select the type of RS-485 readers from the dropdown list.

Wiegand Reader: Select the Wiegand reader from the dropdown 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 mode 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: Select the desired card format by clicking on the Select Card Format button.

For **ARC DC 100-Dual Door, Dual Reader** configure the following parameters for **Door 1** and **Door 2**.

RS-485 Reader: Select the type of RS-485 readers from the dropdown list.

Wiegand Reader: Select the Wiegand reader from the dropdown 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 entry or exit mode for doors.

Exit Switch: Select the check box to enable Exit Switch feature so that the door can be opened without checking any access policy.

Card Format: Select the card format by clicking on the Select Card Format button.

For ARC DC 100-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 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.



The Mifare- DESfire EV1 card is supported on internal and external readers(PN532 Reader for MiFare) of Door V3, PVR, NGT and Vega controller.

Readers section are not applicable for ARC IO 800.

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

ARC DC 200 Reader

Single Door Dual Reader

For **Single Door ARC DC 200** configure the following parameters for **Reader1 Group** and **Reader2 Group**.

The screenshot shows the 'Door Configuration' window with the following settings:

- Basic Configuration** | **Readers** | Advance Configuration | Input Output | Alarms
- Advertise Bluetooth:
- Bluetooth Name: ARC DC 200
- Range:
 - Short (1-2m)
 - Medium (5-7m)
 - Long (>8m)
 - Custom
- Custom Bluetooth Range (dBm):
 - Near (-40 dBm): [Slider]
 - Far (+10 dBm): -30
- Reader1 Group**
 - 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)

Reader2 Group

RS-485 Interface Protocol: Matrix Proprietary

Matrix Reader Type: ATOM RD300

Wiegand Reader: Short - Range Reader

Mode: Exit

Exit Switch:

Card Format: 1 Selected

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 this 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 Device 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 system 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, enter 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 reader type to be connected on RS-485 interface.



While connecting Matrix ATOM Reader with Matrix COSEC ARC200 DC, 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 dropdown 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.

When **Wiegand Reader** is selected as **Long-Range Reader**, then only **Re-detection Delay** parameter will be visible and configurable.

- **Re-detection Delay:** Enter the value of this parameter to configure the time interval during 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:** Select the desired card format by clicking on the **Select Card Format**  button.
- **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 Device Name is configured then in **Bluetooth Name**, Device Name will be displayed here along with the Mode type. The prefix will be the Device 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 system 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: ARC DC200

Range: Short (1-2m) Medium (5-7m) Long (>8m) Custom

Custom Bluetooth Range (dBm): Near (-40 dBm) Far (+10 dBm) -30 ⓘ

Door 1

RS-485 Interface Protocol: Matrix Proprietary

Matrix Reader Type: EM Prox Reader

Wiegand Reader: Short - Range Reader

Mode: Entry

Exit Switch

Card Format: 1 Selected ⓘ

Default...

Configure Bluetooth From Panel

Advertise Bluetooth

Bluetooth Name: ARC DC200 DDSR-IN

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: ARC DC 200

Range: Short (1-2m) Medium (5-7m) Long (>8m) Custom

Custom Bluetooth Range (dBm): Near (-40 dBm) Far (+10 dBm) -30 ⓘ

Door 1

RS-485 Interface Protocol: Matrix Proprietary

Matrix Reader Type: EM Prox Reader

Wiegand Reader: Short - Range Reader

Mode: Entry

Exit Switch

Card Format: 1 Selected ⓘ

Default...

Configure Bluetooth From Panel

Advertise Bluetooth

Bluetooth Name: ARC DC 200 DD DR -IN

Range: Short (1-2m) Medium (5-7m) Long (>8m)

Door 2

RS-485 Interface Protocol: Matrix Proprietary

Matrix Reader Type: ATOM RD100

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 DD DR-OUT

Range: Short (1-2m) Medium (5-7m) Long (>8m)

- **Advertise Bluetooth:** Select this 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 Device Name is configured then it will be displayed here.

If required, you can configure the bluetooth name as per your requirement.

- **Bluetooth Range:** The system 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, enter 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 reader type to be connected on RS-485 interface.



While connecting Matrix ATOM Reader with Matrix COSEC ARC200 DC, 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 dropdown 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.

When **Wiegand Reader** is selected as **Long-Range Reader**, then only **Re-detection Delay** parameter will be visible and configurable.

- **Re-detection Delay** - Enter the value of this parameter to configure the time interval during 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**: Select the desired card format by clicking on the **Select Card Format**  button.
- **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 Server**, 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 Device Name is configured then it will be displayed here.

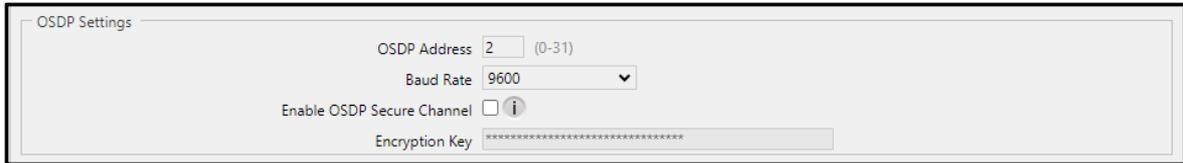
If required, you can configure the name of bluetooth as per your requirement. The **Bluetooth Name** can be a maximum of 20 characters.

- **Bluetooth Range**: The system 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 OSDP Parameters. OSDP Protocol is supported for 3rd Party Readers only.



OSDP Settings

OSDP Address: 2 (0-31)

Baud Rate: 9600

Enable OSDP Secure Channel:

Encryption Key: *****

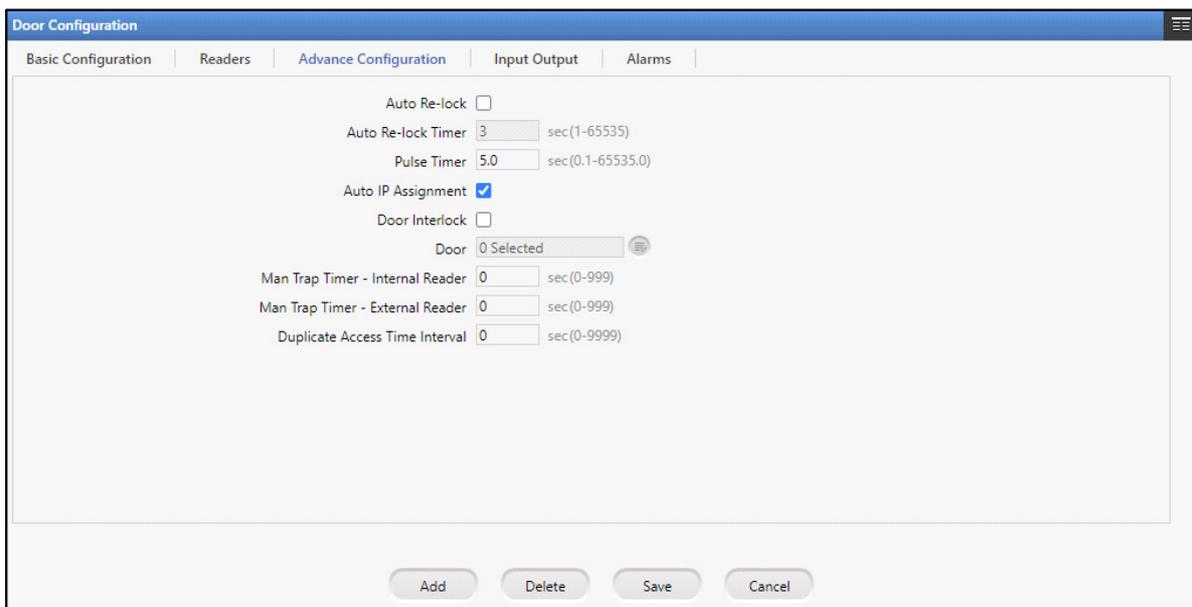
Configure the following parameters:

- **OSDP Address:** Configure the unique identifier assigned to the 3rd Party Reader (Peripheral Device - PD). This allows the Device (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 Device and 3rd Party Reader.
- **Enable OSDP Secure Channel:** If you wish that the Device 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 Device and 3rd Party Readers.

Click **Save**.

For list of Commands and Responses supported in OSDP, refer to, "[Supported OSDP Commands and Responses](#)"

Advance Configuration



Door Configuration

Basic Configuration | Readers | **Advance Configuration** | Input Output | Alarms

Auto Re-lock:

Auto Re-lock Timer: 3 sec(1-65535)

Pulse Timer: 5.0 sec(0.1-65535.0)

Auto IP Assignment:

Door Interlock:

Door: 0 Selected

Man Trap Timer - Internal Reader: 0 sec(0-999)

Man Trap Timer - External Reader: 0 sec(0-999)

Duplicate Access Time Interval: 0 sec(0-9999)

Add | Delete | Save | Cancel



Advance Configuration is not applicable for ARC IO800 device.

- **Auto Re-lock:** Select this check box to allow the door to re-lock immediately when the door status changes to close after normal open irrespective of the defined pulse time. However, it is supported only if a door sense is installed and enabled.
- **Auto Re-lock Timer:** Specify the time 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 this check box to set all door-based alarms as active.
- **Tamper Alarm:** Select this check box to activate the Tamper Alarm.



Alarm and Tamper Alarm are applicable to Door V1, Door V2, Path V1 and ARC DC100.

- **Pulse Timer (sec):** Specify the time in seconds for which a panel 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, PATH V2 and ARC DC200 only.*

- **Auto IP Assignment:** There is option where panel door can be assigned its IP from device webpage. Select the check box to enable this option.
- **Network Protocol:** Select the Network Protocol from the options — 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 this option is enabled, the Occupancy Count of a Zone will be increased/decreased after considering the punch as well as the input from the Auxiliary Input Port.

To reset the Tail-Gating Count, configure the Reset Wait Timer. Select the desired option — **Door Lock** or **Pulse Timer**.

- **Door Interlock:** Select this 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 picklist and select the doors to be assigned for the Interlock to the selected door (PVR door). If Door V3 and Vega Door 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 high security area.

- **Man Trap Timer — Internal Reader (Sec):** This is an alarm wait timer on the panel 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 panel door to ensure that the user exits the panel 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 Mantrap timer.

If user fails to do so, Mantrap violation alarm shall 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 device 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 and ARGO FACE only.

The Duplicate Access Time Interval is not applicable:

- *if Duress Finger is detected by the device.*
- *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 Panel- Server Mode.

In Panel- Server Mode, Temporary User Configuration is displayed as configured in the COSEC Server.

The screenshot shows a web interface titled "Door Configuration" with several tabs: "Basic Configuration", "Readers", "Advance Configuration", "Advance Configuration 2", "Input Output", and "Face Identification Settings". The "Advance Configuration 2" tab is active. It contains the following settings:

- "Temporary Addition of Unknown User" is a dropdown menu currently set to "As Temporary User".
- "Add Name via Device" is a checked checkbox.
- "Confirm before adding Temporary User" is a checked checkbox.

- **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

Door Configuration

Basic Configuration | Readers | Advance Configuration | **Input Output** | Alarms

Door

Enable Door Sense

Supervised

Door Sense Type: NC

Relay

Output Group No. (Unlock): 2

Output Group No. (Lock):

Lock

Lock Sense Turning on Lock Sense should ensure connection of Exit Switch-2 and it will turn off Auxiliary Input 2

Lock Sense Type: NO

Auxiliary Input

Enable Auxiliary Input

Supervised

Aux. Input Sense Type: NO

Add Delete Save Cancel

Door Configuration

Basic Configuration | Readers | Advance Configuration | **Input Output** | Alarms

Auxiliary Input

Enable Auxiliary Input

Supervised

Aux Input Sense Type: NO

Debounce Time: 5 sec (0-99)

Auxiliary Input 2

Enable Auxiliary Input Turning on Auxiliary Input 2 should ensure connection of Exit Switch-2 and it will turn off Lock Sense

Aux Input Sense Type: NO

Debounce Time: 5 sec (0-99)

Auxiliary Output

Enable Auxiliary Output

Output Group No.: 1

Add Delete Save Cancel

Door Sense

Enable Door Sense: Select this to enable the door for two-state monitoring.

Supervised: Select this to enable the door for four-state monitoring where the door is also monitored for door fault and door disconnection.

Door Sense Type: Specify the Sense Type as NC or NO (Default: NC).

Door Relay

Output Group No. (Unlock): Select an Output Group No. (Unlock) from the picklist for door relay.

Output Group No. (Lock): Select an Output Group No. (Lock) from the picklist for door relay.



Door Relay is applicable for all Panel Doors except ARC IO 800.



For ARC DC 100-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 Sense: Select this to enable the lock for two-state monitoring.

Lock Sense Type: Specify the Sense Type as NC or NO (Default: NO).

When Sense type is NO; Lock Open is detected when Lock Sense is changed from NO to NC. Lock Close is detected when Lock Sense is changed from NC to NO.

Lock Sense -ARC Panel Door



This parameter is only configurable for ARC and not for other Panel Doors.

Whenever Lock Sense status is changed; Lock Open/ Lock Close or Manual Lock Override event is generated.

Also, whenever lock status condition is violated respective alarm is generated for Door Lock.

The “Alarm” check box in Door Configuration > Advance Configuration must be enabled for activating the alarms.

The local alarm events i.e Lock Open Too Long, Lock Abnormal and Manual Lock Open alarms are sent to CCC Server.

Lock Open event is generated when Exit Switch is in **Lock Sense Mode** i.e. Lock Sense check box in Input Output page is enabled.

When Lock Sense is enabled for Door1 then Exit Switch gets disabled for Door1. Similarly for Door2 also.

Once the Lock Sense is enabled, lock open event will be generated when lock relay is energized.

Manual Lock Override event is generated when lock is opened manually i.e., by inserting physical key.

Lock Alarms

Whenever Lock related conditions are violated following alarms will be generated and displayed in Monitor> Live Events and Event log.

1. Lock Open Too Long - Minor Alarm

When user has opened the lock but does not close the lock before expiry of the Pulse Timer or Relock Timer.

2. Lock Abnormal - Major Alarm

When user has opened the lock but does not close it before the expiry of Door Abnormal Wait Timer.

3. Manual Lock Override - Critical Alarm

When user has opened the lock manually using mechanical key.

Auxiliary Input

- **Aux Input Port (Applicable only for ARC IO 800):** Select the auxiliary input port from the dropdown list.

- **Enable Auxiliary Input:** Select this check box to enable Auxiliary Input (e.g. Smoke Detectors) depending on normal door state monitoring.
- **Supervised:** Select this check box to enable Auxiliary Input (e.g. Smoke Detectors) depending on supervised door state monitoring.
- **Aux Input Sense Type:** Select the Sense Type as NC or NO (Default: NC).
- **Debounce Time (sec):** Specify the Debounce time in seconds. Default value is 5 sec and range is 0-99 sec. It defines the minimum time 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 Input 2 (Applicable only for ARC DC 200 Single Door)

- **Enable Auxiliary Input:** Select this check box to enable Auxiliary Input (e.g. Smoke Detectors) depending on normal door state monitoring.
- **Aux Input Sense Type:** Select the Sense Type as NC or NO (Default: NO).
- **Debounce Time (sec):** Specify the Debounce time in seconds. Default value is 5 sec and range is 0-99 sec. It defines the minimum time 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 IO 800):** Select the auxiliary output port from the dropdown list.
- **Enable Auxiliary Output:** Select the check box to enable Auxiliary Output (e.g. Fire Alarm) for the selected device.
- **Output Group No.:** Click Select Output Group button to select the Output Group Number to which the auxiliary output is to be assigned based on the output groups created in the Panel.
- **Elevator ID:** Specify the Elevator ID to which the Aux Output Port of the ARC IO 800 is linked.
- **Floor No.:** Specify the floor number to which the Aux Output Port of the ARC IO 800 is linked.



*Only **Auxiliary Input** and **Auxiliary Output** parameters are applicable to **ARC IO 800**.*

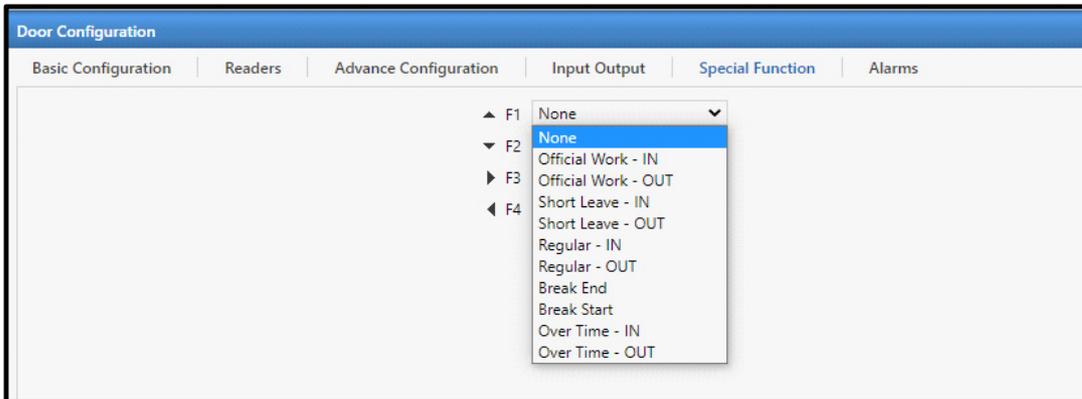
Click **Save** to save the settings or click **Cancel** to discard.

Special Function



Special Function is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

The user can map up to 4 special functions to the arrow keys on a Panel Door keypad. For each arrow key, select a special function from the respective dropdown list.



Special function is applicable for Door V3, Door V4 and PVR Door.

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

Alarms

Alarms are required for the system to indicate unauthorized access, some emergency, system being tampered or occurrence of some fault in the system, etc.

Alarms should be monitored, acknowledged and cleared in real time by an operator who manages the Access Control System.

All the alarms related to door can be enabled or disabled through the Door Configuration.

Select the desired alarms which are to be enabled.

Door Configuration

Basic Configuration | Readers | Advance Configuration | Input Output | **Alarms** | Face Identification Settings

- Tamper Alarm
- Door Held Open
- Door Abnormal
- Door Force Open
- Door Fault
- Panic
- Dead Man
- Occupancy Violated
- Man Trap Timer Violation
- Access Denied - Anti-Pass Back
- Access Denied - Access Route Violated
- Access Denied - Access Route Timer Violated
- Access Denied - Other Reasons
- User Unidentified
- Multiple Unauthorized Attempts
- Face Mask Compulsion

Add Delete Save Cancel



Alarms are applicable only for Door V3, PVR, Door V4, Vega, ARGO, ARGO FACE, Path V2, ARGO FACE and ARC DC200.

Different Doors have different set of Alarms.

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

Face Identification Settings

In Panel- Server Mode, Face Identification Settings is displayed as configured in the COSEC Server. For details, refer to [“Face Identification Settings: Panel- Server Mode”](#).

In Panel-Standalone Mode, the Face Identification Settings can be configured for the ARGO FACE Door. For details, refer to [“Face Identification Settings: Panel- Standalone Mode”](#).

Face Identification Settings: Panel- Standalone Mode

The screenshot displays the 'Face Identification Settings' window within the 'Door Configuration' application. The window has a blue header with the title 'Door Configuration' and a navigation bar with tabs for 'Basic Configuration', 'Readers', 'Advance Configuration', 'Input Output', 'Alarms', and 'Face Identification Settings'. The 'Face Identification Settings' tab is active. The settings are organized into two sections: 'Face Recognition' and 'Face Enrollment'. In the 'Face Recognition' section, 'Enable FR' is checked, 'Server Type' is set to 'Local', and 'Capturing Mode' is set to 'Free Scan'. 'Enable Free Scan TimeOut' is unchecked. The 'Free Scan TimeOut' is set to 30 seconds (range 5-999), 'Identification TimeOut' is 4 seconds (range 1-99), 'Face Matching Score' is 94.00% (range 0.0-100.0), and 'Threshold for Face Detection' is 50.00% (range 0-100). The 'Face Enrollment' section has 'Conflict Check' checked and 'Conflict Matching Threshold (Face)' set to 93.00% (range 1.0-99.99). At the bottom of the window are four buttons: 'Add', 'Delete', 'Save', and '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 Capturing Mode from the dropdown list — Tap and Go or Free Scan.
 - **Tap and Go:** If you select this option, you need to tap on the device screen once. The motion recording screen appears and the device will capture and identify the user's face.
 - **Free Scan:** If you select this option, the device 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:** Enter the Free Scan TimeOut duration. 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 system reloads the Free Scan TimeOut timer again. Hence, device always remains in the scanning mode.
- **Identification TimeOut:** Specify the time in seconds after which the face identification will time out.
- **Face Matching Score:** Specify 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 be found. 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:** Specify the value in percentage for Threshold for Face Detection. This is the percentage of confidence after which the algorithm should conclude that the frame has a face in it which should be detected. When the user image received is above this threshold it will be considered for further processing.



If the Panel's External Memory Storage exceeds 98%, then Panel will stop face sync with associated Panel Doors. Hence, Face Recognition will not function.

If the Panel Door template count reaches 2 Lakhs, even though the Panel Door has memory space the Face Recognition for new users will not function.

If the Panel Door template count is less than 2 Lakhs but the Panel Door 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):** Specify 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.

Face Antispoofing

- **Face Anti-Spoofing:** Select the check box to enable Face Anti-Spoofing.
- **Face Anti-Spoofing Threshold:** Specify the value in percentage for Face Anti-Spoofing Threshold. This will be considered while checking the liveliness of a user's face to consider him/her as a genuine person.



For FR Mode as Local, the default value of Face Anti-Spoofing Threshold will be 90.

If you upgrade the system 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):** Specify the time in seconds within which the user should approach the camera for face mask detection.
- **Mask Detection Time Out (Sec):** Specify the time in seconds after which the mask identification timer will expire.
- **Restriction Type:** Select the Face Mask Compulsion Restriction Type from the dropdown 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. But, 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**.



User Allowed- Face Mask Not Detected and **User Denied- Face Mask Not Detected** alert are not applicable for Panel- Server Mode.

- **Face Mask Coverage:** Enter 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:** Enter 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.

Face Identification Settings: Panel- Server Mode

The screenshot shows the 'Face Identification Settings' tab within the 'Door Configuration' application. The 'Face Recognition' section is active, displaying the following settings:

- Enable FR:
- Allow Access Via QR:
- Server Type: Local (dropdown menu)
- Capturing Mode: Free Scan (dropdown menu)
- 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 Recognition

- **Enable FR:** The check box will appear selected, if enabled in the Server.
- **Allow Access Via QR:** The check box will appear selected, if enabled in the Server.
- **Server Type:** It displays Local or Server Assisted, as configured in the Server.
- **Capturing Mode:** It displays Tap and Go or Free Scan, as configured in the Server.
- **Enable Free Scan TimeOut:** The check box will appear selected, if enabled in the Server.
- **Free Scan TimeOut:** Displays the time as configured in the Server.
- **Identification TimeOut:** Displays the time as configured in the Server.

- **Face Matching Score:** Displays the value in percentage for Face Recognition as configured in the Server. This will be considered while face identification of the user.
- **Threshold for Face Detection:** Displays the value in percentage as configured in the Server. This is the percentage of confidence after which the algorithm should conclude that the frame has a face in it which should be detected. When the user image received is above this threshold it will be considered for further processing.

Adaptive Face Enrollment

- **Adaptive Face Enrollment:** This check box will appear selected, if enabled in the Server. Adaptive Face Enrollment provides automatic real time face enrollment whenever change is experienced in facial features.
- **Threshold Deviation:** Displays the value of deviation from matching threshold in percentage as configured in the Server. Based on the value entered for deviation, template for Adaptive Face Enrollment will be decided.
- **Multi-User Matching Score Deviation:** Displays the value of deviation from matching score between 2 different users while Adaptive Face Enrollment as configured in the Server. Difference between matching scores of templates will be done, when we have templates of two or more users falling under above specified deviation.



Threshold Deviation and Multi-user Matching score deviation will act as two filters to fetch appropriate template for adaptive enrollment.

- **Confirm before Adaptive Face Enrollment:** The check box will appear selected, if enabled in the Server.
- **Adaptive Face Templates Per User:** Displays the number of Adaptive Face Templates that can be enrolled against a user as configured in the Server.

Face Antispoofing

- **Face Anti-Spoofing:** The check box will appear selected, if enabled in the Server.
- **Face Anti-Spoofing Threshold:** Displays the Face Anti-Spoofing threshold value in percentage as configured in the Server to identify user's face liveness for considering him/her as genuine person.

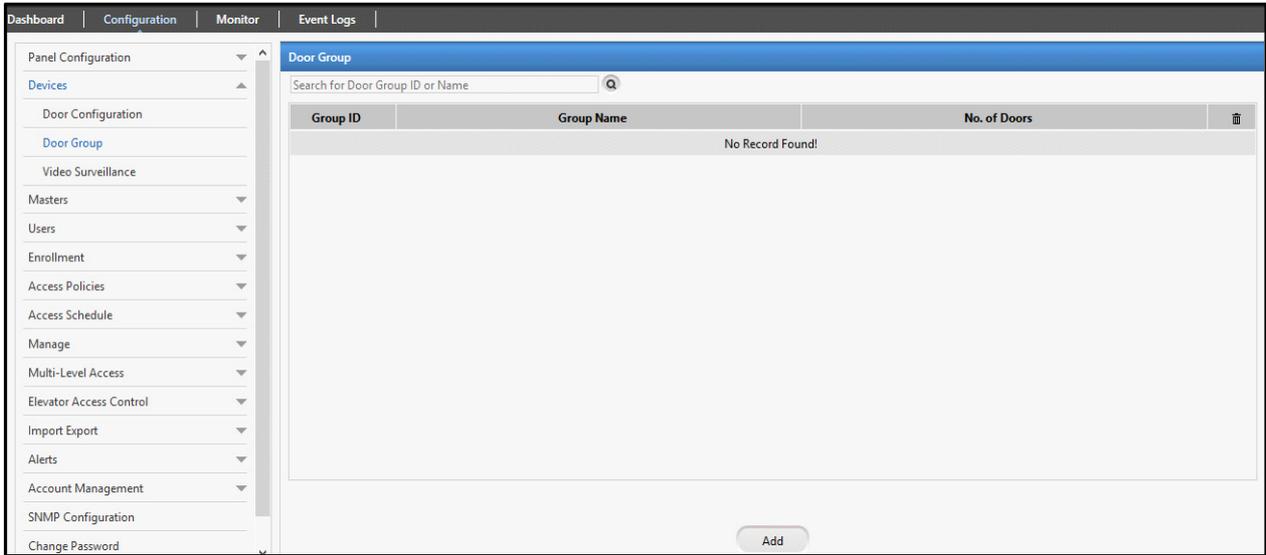
Capture Face of Unidentified User

- **Capture Face of Unidentified User:** The check box will appear selected, if enabled in the Server.
- **Show Feedback for Unidentified Face:** The check box will appear selected, if enabled in the Server.
- **Generate Unidentified Face Event:** The check box will appear selected, if enabled in the Server.

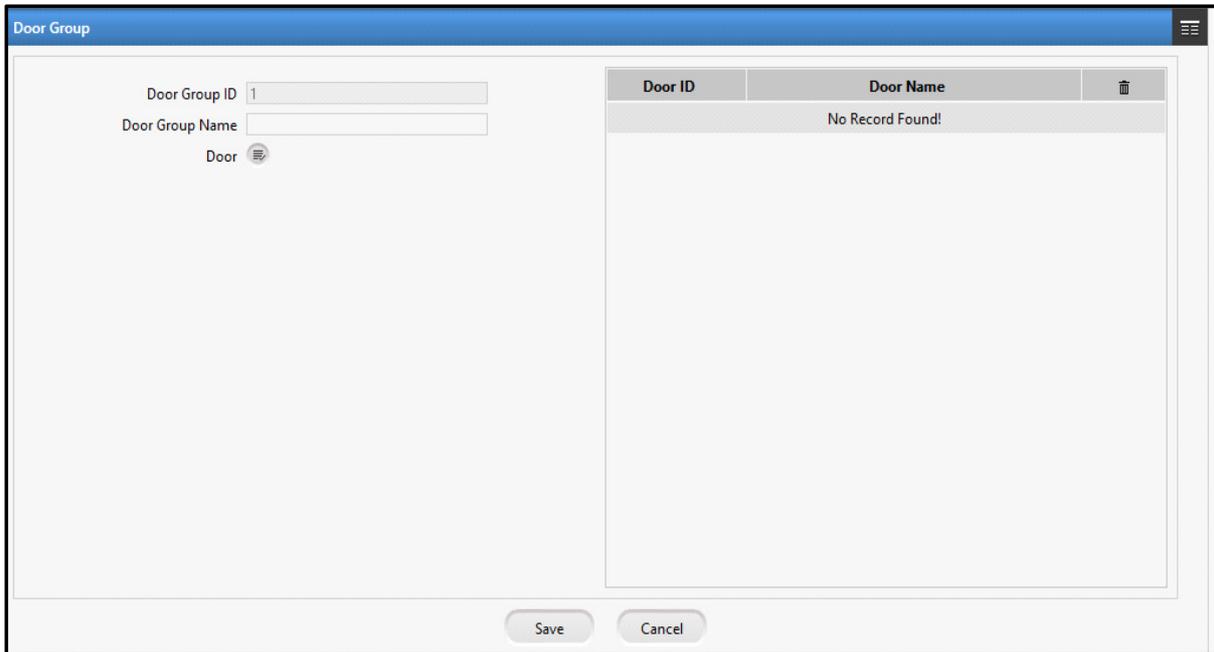
Door Group

This page enables you to configure the Door Group with multiple doors in the group. This door group can be assigned to the user who is to be allowed access on selected doors only.

You can configure maximum **99** device groups and each device group can have upto **255** doors.



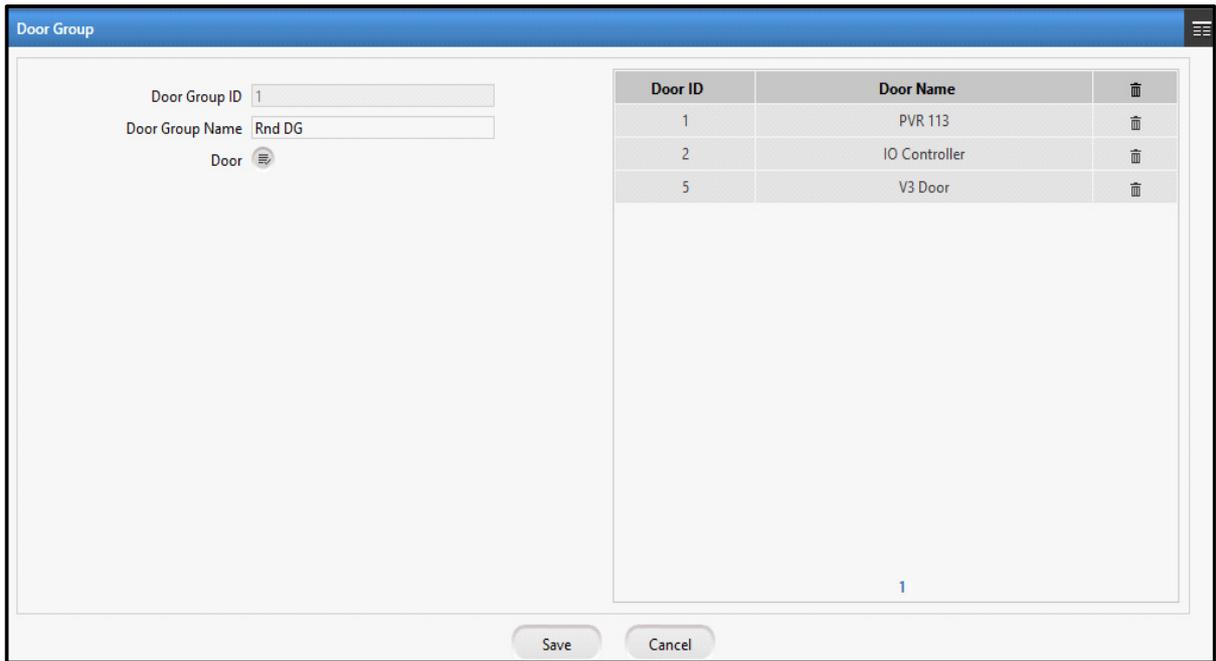
To add a new Door Group click **Add** button and configure the following parameters.



Door Group ID: This is auto generated by the system.

Door Group Name: Specify the name of the door group.

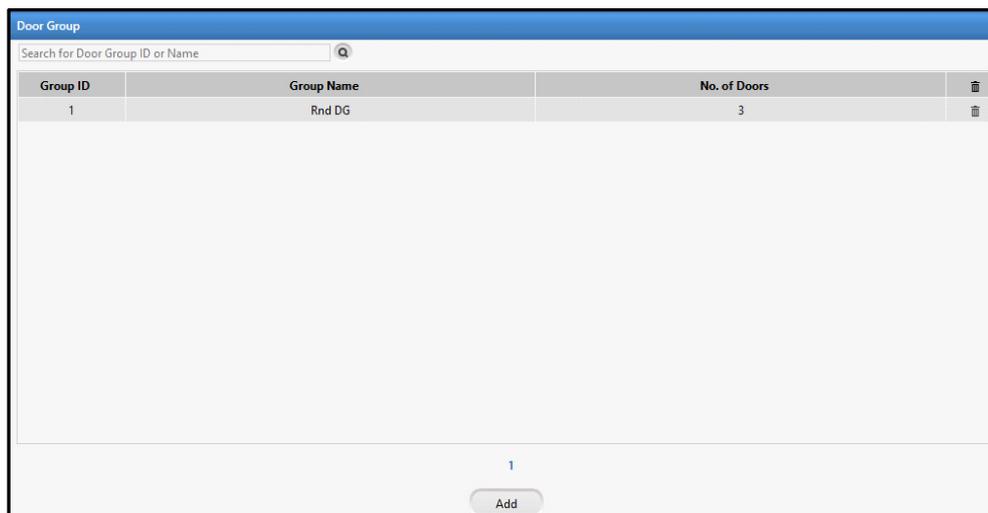
Door: Click the picklist and select the doors to be added in the door group. The list of doors will appear in the grid as shown below.



Click **Save** button to save the door group.



Once the door group is saved, you can view the door groups by clicking on **View List** button.



Video Surveillance



Video Surveillance is configurable only when the Panel is in Standalone Mode. (Configuration > Basic Profile > Panel Mode)

This page enables you to integrate and configure Matrix Network Video Recorder (NVR) and Hybrid Video Recorder (HVR) with Panel200 to get images and videos triggered by the user events at the door. For ARGO FACE Door, you can configure the Built-In Camera to get images triggered by the user events.

Configuration

The screenshot shows the 'Video Surveillance' configuration window. It has a blue header with the title 'Video Surveillance'. Below the header are two tabs: 'Configuration' and 'Satatya Integration'. The 'Configuration' tab is active. The configuration area contains the following fields:

- Door:** A picklist menu showing 'PVR Door'.
- Active:** A checked checkbox.
- Network Connection:** A dropdown menu showing 'Ethernet'.
- IP Address:** A text input field containing '192.168.104.26'.
- Port:** A text input field containing '8000', with '(1024-65535)' displayed to its right.

- **Door:** Click the Door picklist and select the type of door controller for video surveillance integration. The picklist displays all the configured doors.
- **Active:** Select the check box to enable the connection.
- **Network Connection:** Select the desired Network connection from the options — Ethernet, Broadband, Wireless.
- **IP Address:** Enter the IP address of SATATYA NVR/ HVR which is to be configured for surveillance.
- **Port Number:** Enter the port number of NVR/HVR at which COSEC door will connect with SATATYA device. The default port is 8000.

Click on **Save** button to save the configuration.

Sataty Integration



Sataty Integration is not applicable for ARGO FACE Door.

The screenshot shows the 'Sataty Integration' configuration page in a 'Video Surveillance' application. The page has a blue header and a 'Configuration' tab. The configuration fields are as follows:

- ID:** 1
- Name:** PVR NVR Access Deny
- Active:**
- Schedule:** 09 : 00 to 18 : 00
- Days:** Sun, Mon, Tue, Wed, Thu, Fri, Sat, Holiday
- Event:** Access Denied
- Mode:** Both
- Action:** Recording
- Duration:** 5 min (1-60)
- Camera:** A grid of checkboxes for cameras 01 through 40. Camera 02 is selected.

- **ID:** This is a read-only field and the ID is generated automatically.
- **Name:** Specify a user friendly name for the action schedule.
- **Active:** Select the check box to enable the SATATYA integration functionality.
- **Schedule:** Specify the time period in HH:MM format during which the actions should be triggered for the selected event.
- **Days:** Select the check boxes for the desired days of the week for the schedule.

Example: A schedule from 09:00 to 18:00 can be configured for working days (Monday- Friday) to monitor the exit of employees from the working area.

- **Event:** Select a COSEC event from the drop down list for which the corresponding action is to be configured.
- **Mode:** Select the event mode from the drop down list options— Entry, Exit or Both.
- **Action:** Select the action for the SATATYA device from the drop down list.
 - Recording - Specify the duration in minutes.
 - Upload Image - This will be uploaded as per the FTP settings.
 - Video Pop-up - Specify the duration in seconds. The video pop up will be generated on the local client of SATATYA device on the selected camera.
 - PTZ Preset - Specify the PTZ position number as defined on the SATATYA device.
 - Mail Image - Specify the Email-ID.
- **Camera:** Select the relevant camera channels depending on the action selected.

Example: For Access Allowed event on COSEC Device, the video pop up of Camera 12 will be shown for 10 seconds.

Click the **Add** button to complete the process of linking the event to the action. The integration will be updated in the grid.

Camera 25 26 27 28 29 30 31 32
 33 34 35 36 37 38 39 40
 41 42 43 44 45 46 47 48
 49 50 51 52 53 54 55 56
 57 58 59 60 61 62 63 64

Sr. No.	Name	Event	Action	Start Time	End Time	Active	
1							🗑
2							🗑
3							🗑

Sr. No.	Name	Event	Action	Start Time	End Time	Active	
1	PVR NVR Access Deny	Access Denied	Recording	09:00	18:00	Active	🗑
2							🗑
3							🗑

You can update a schedule if required. Select the desired schedule and click the **Update** button to edit the schedule.

Click the **Delete** button in the grid to delete a particular schedule. Similarly you can configure another event-action linkage if required.

Built-In Camera



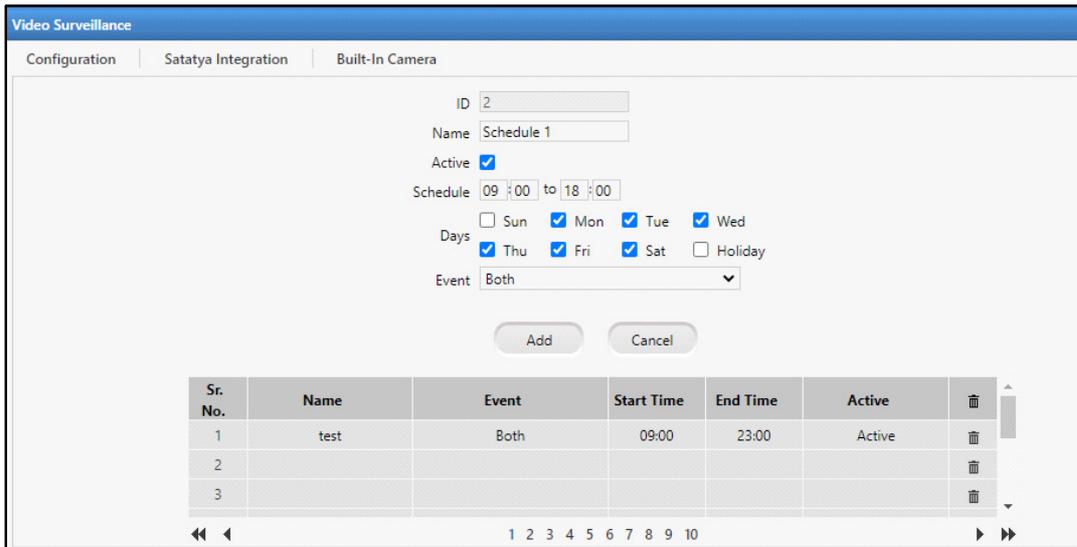
Built-In Camera is applicable for ARGO FACE Door only.

Built-In Camera is applicable for Panel- Standalone Mode.

You can create schedules for capturing snapshots for User Allowed/Denied events. To create schedule,

- Click the desired serial number from the grid for which you wish to create a schedule.

Configure the details as follows:

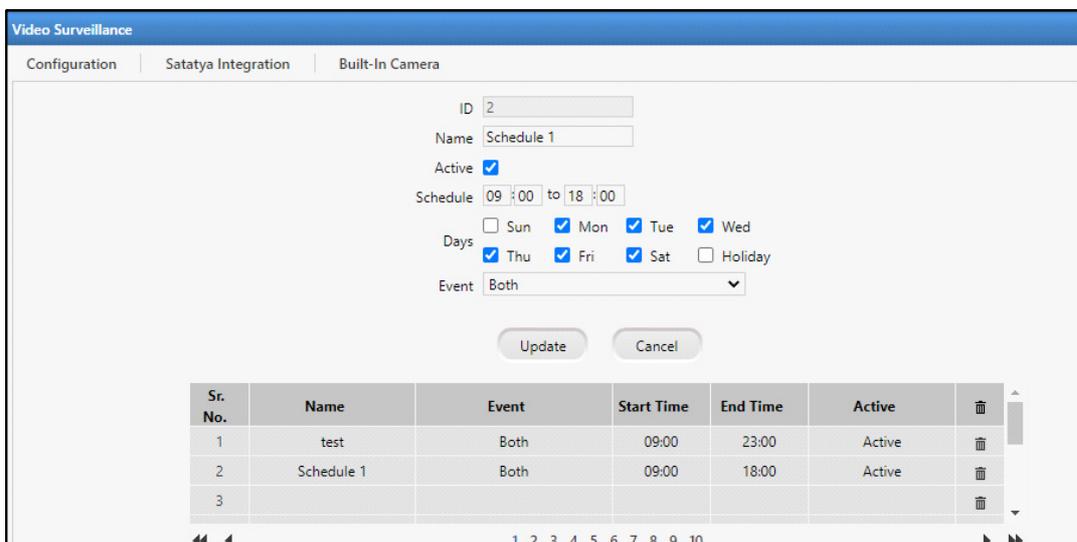


- **ID:** This displays the serial number you have selected.
- **Name:** Specify a user friendly name for the snapshot capturing schedule.
- **Active:** Select the check box to activate the schedule.
- **Schedule:** Specify the time period in HH:MM format during which the device should capture snapshots for the selected event.
- **Days:** Select the check boxes for the desired days of the week for the schedule.

Example: A schedule from 08:00 to 10:00 can be configured for working days (Monday- Friday) to monitor the entry of employees at the main gate.

- **Event:** Select the event from the drop down list for which the device should capture snapshots.

Click **Add** to add the schedule for the selected event. The configured schedule will appear in the grid at the selected serial number. Maximum 99 schedules can be created for one ARGO FACE Door.



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**  of the respective 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 Panel 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.*

Captured Snapshot Count Full alert is applicable for Panel- Standalone Mode.

Capture Snapshot functionality is not supported in Degraded mode.

When the Panel 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.

There are various types of cards that can be assigned to users. Different types of cards have different formats. We need to set the format so that the cards can function.

This page allows you to set the Card Formats, Configure the settings for Personalized Cards as well as set the Wiegand Format.

Card Format: All cards store a sequence of numbers which can be read by card reader devices, when a card is swiped. 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 proximity card is known as its Card Format. For more information, [See “Card Format” on page 128.](#)

Card Personalization: Card Personalization allows users to program the memory mapping of smart cards as per their requirement. Users can configure their own card format by adding user-defined fields as well as modifying length, type and location of pre-defined fields on the different available memory sectors in specific HID iClass and MiFare cards. For more information, [See “Card Personalization” on page 131.](#)

Wiegand Format: Wiegand readers can send outputs not only in the standard formats or the actual information, but also in a custom data format whose structure can be defined. The administrator can use this page to create and save multiple profiles for different Wiegand Output Formats. For more information, [See “Wiegand Format” on page 134.](#)

Card Format



Card Format is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

All cards store a sequence of numbers which can be read by card reader devices, when a card is swiped. This unique card number sequence is then verified against a user enrolled on the COSEC 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 proximity card is known as its card format.

CARD FORMAT

You can select maximum 5 card formats for Internal as well as External Readers. The selected card formats will be displayed.

When you display 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 does 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.

Case 1: Suppose 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 shown on reader. Then only format 3 will be applied on the card.

Case 2: Suppose 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 shown at the reader then as configurable bits are also 26 this format should be applied. However, after truncation process bits are of 24 bit length. So, last 2 bits (MSB) should be discarded/ ignored in bit configuration.

After that bit reversal will be done.

Case 3: Suppose 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 shown at 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.

You can configure upto 9 card profiles.

ID	Name	
1	Default Format	
2		
3		
4		
5		
6		
7		
8		
9		

- **ID:** To configure a card format select the ID number from the grid on right side of the page. This ID will be displayed here.
- **Name:** Specify a name for the card format.
- **Read Order:** The Read Order parameter indicates the sequence in which the card serial number should be read by the card reader. You can specify the Read Order as one of the following:
 - **Forward-** This implies that the bits should be processed in the order of their arrival.
 - **Reverse bitwise-** This implies that all incoming bits will be received and then reversed before processing them further.
 - **Reverse bitwise-** This implies that each incoming byte will be reversed separately and then used for further processing.

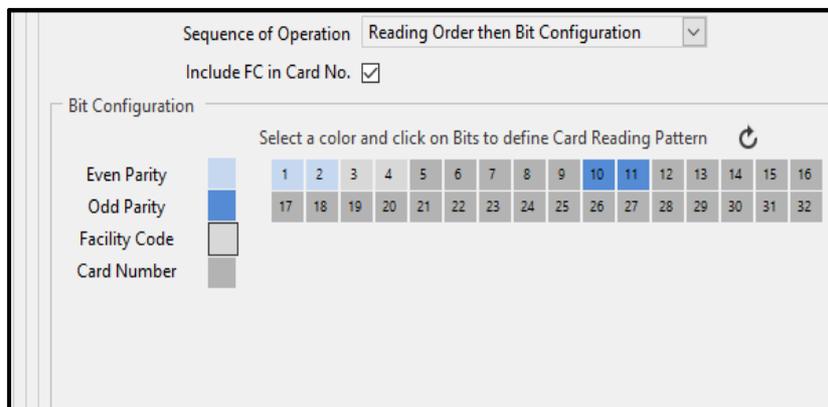
Bit Configuration

Select a color and click on Bits to define Card Reading Pattern

Even Parity	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Odd Parity	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Facility Code																
Card Number																

- **Truncate To (Bits):** Specify the maximum number of bits that will be allowed for the format.

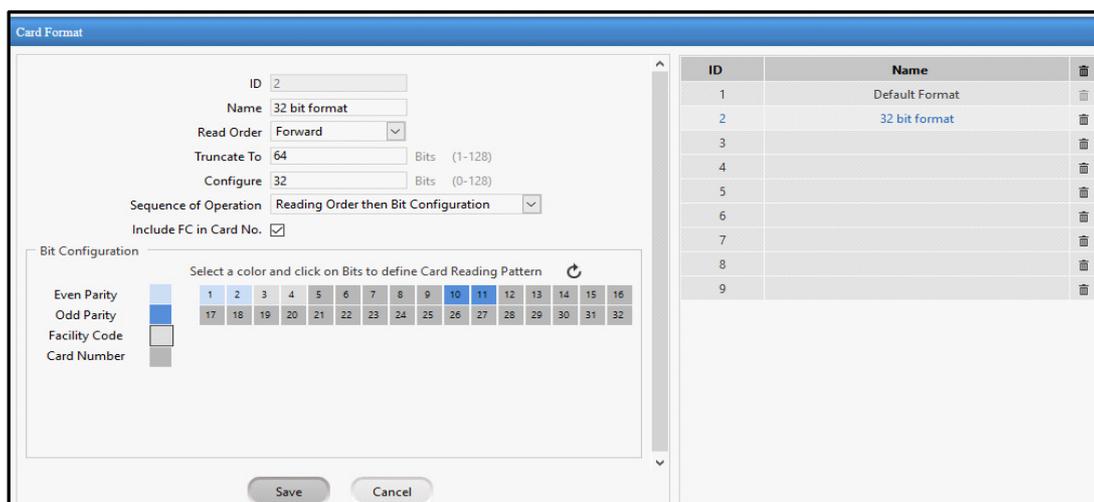
- **Configure (Bits):** Specify the number of bits that will be configured in the card structure. If the number of bits received at the card reader is greater than the number of configured bits, then default card format will be applicable for the reader.
- In **Bit Configuration**, all configurable bits of the card data will appear numerically in a serial order, from left to right, as boxes.
For eg: If you set Configurable bits as 32, then a grid from 1 to 32 will be created. Here, each box represents a bit.
- **Sequence of Operation:** Select the check-box to enable. This will ensure sequence of operation based on which operation is to be performed first and then second between Reading Order and Card Format Configuration.
- **Include FC in Card No.:** Ensure that the Card Number or Card ID includes Facility Code as well.



You can add **Parity** and **Facility Code** to the Card number. For this, In the **Color Selection** area, click to select the colour 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 E.g.: If you select Odd Parity (blue colour) and select 10 and 11 from 32 configurable bits. Then these 2 bits will be set with Odd parity and rest with card number.

Click **Save** to apply the changes.



Card Personalization



Card Personalization is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

This page allows users to program the memory mapping of smart cards as per their requirement. Users can configure their own card format by adding user-defined fields as well as modifying length, type and location of pre-defined fields on the different available memory sectors in specific HID iClass and MiFare cards. A total of maximum 99 fields can be configured for each personalized format out of which 22 fields are pre-defined.

The screenshot shows the 'Card Personalization' interface with two tabs: 'Fields' and 'Configuration'. The 'Configuration' tab is active, displaying a form with the following fields:

- Field Name: 30 Chars
- Field Type: text
- Max Field Length (Bytes):

Below the form are 'Add' and 'Cancel' buttons. A table below the form lists pre-defined fields:

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	🗑️

At the bottom of the table, there are navigation buttons: 1 2 3 4.

Using this feature, user can:

- Add or modify fields such as name, ID, department, shift, fingerprint templates etc. to be written on the Smart Card.
- Configure a field profile based on card type and card mode.

Fields

Field Name: Specify a name for the field.

Field Type: Select a Field Type from the drop-down list.

For Text and Numeric fields, specify the **Max Field Length** in bytes. For a Date field, specify a date type, format and separator. Based on your selection the maximum field length will be automatically determined.

Click the **Add** button. The new field will be added to the grid list below. You can also delete a particular field from the grid itself. To do so, click the Delete icon.

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	8	🗑️
23	Date of Birth	Date	8	🗑️



If some pre-defined field type is changed from text to numeric, the admin should make sure to have only numeric value in such fields. If any mismatch occurs, then while writing or reading information from card, conversion will not be performed and the field shall remain <Blank>.

Configuration

Card Type: Select the **Card Type** from the dropdown list. To view the memory of each card, hover the mouse over the Info icon.

Card Mode: Select the Card Mode as — Default or Custom.

1. **Default:** Select the Card Mode as Default to use the default card format where location of each field is fixed as per card type selected.
 - **Card No.:** If Default Card Mode is selected, specify the Card No. to be used —CSN or UID (Universal Identifier number).
2. **Custom Mode:** If Custom Mode is selected, then you can configure all the pre-defined fields as per the available memory. Maximum 99 new fields can be added.

- **Card No.:** If Custom Card Mode is selected, specify the Card No. to be used — **CSN, UID** or **Custom** card no. as is defined at the time of enrollment. While location of CSN is fixed, it is mandatory to define a Field Profile for Custom Card Nos.

Read CSN: Select to enable this option, if Custom is selected as the Card No. In this case the CSN number will be read if the system is unable to read the Customer number.

Field Profile: If Custom is selected as the Card Mode, for each selected field the location on the card memory can be defined.

Field: Click Field pick-list to select the desired field.

Specify the **Length, Page** and **Block** on the card and number of **Bytes** to be used depending on the field type and the available memory for the selected field.

Click the **Add** button. The configured field will appear on the grid list.

Card Personalization

Fields | Configuration

Card Mode: Custom

Card No.: Custom

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	🗑️
Card id	0-20-1	0-21-0	8	🗑️
Date of Birth	0-21-2	0-22-1	8	🗑️

Save Cancel

Click **Save** to apply the changes.

Wiegand Format



Wiegand Format is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

Wiegand readers can send outputs not only in the standard formats or the actual information, but also in a custom data format whose structure can be defined. The administrator can use this page to create and save multiple profiles for different Wiegand Output Formats. Based on the output required, Wiegand output format in the Device Configuration module should be selected for allowed and denied events.

ID	Name	
1		
2		
3		
4		
5		
6		

The page displays two panels one for configuring the Wiegand format and the second contains a grid that displays the created formats. You can also delete a particular format from the grid itself. You can configure upto 6 different formats

Configure the following parameters for each format:

Name: Specify a name for the format.

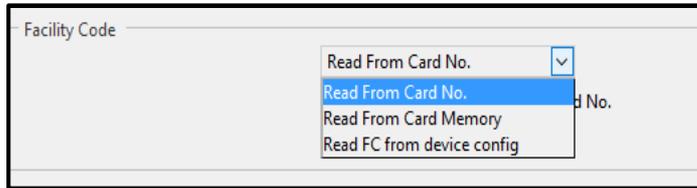
Output bits: Specify the number of bits to be configured in Wiegand Output Format.

Color Selection for Output bits

- You can add Parity, Facility Code, Access Code and Blank to the Card number. Access Code indicates to the 3rd party panel whether the user has been allowed or denied by the device.
- For this, In the Color Selection area, click to select the colour 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 eg: If you select Odd Parity (blue colour) and select 1,2 and 3 from 32 configurable bits. Then these 3 bits will be set with Odd parity.

Facility Code

If **Facility Code** is marked in the output bits, you must specify the source from where it must be read i.e. from Card No., from Card Personalization data or as per Device Configuration.

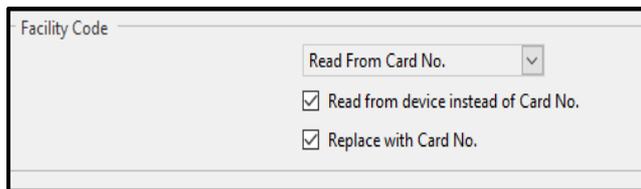


A screenshot of a 'Facility Code' dropdown menu. The menu is open, showing four options: 'Read From Card No.', 'Read From Card No.', 'Read From Card Memory', and 'Read FC from device config'. The first 'Read From Card No.' option is highlighted in blue.

Read from Device instead of Card No.: Select this check-box when you want to send the Facility Code stored in the device.

This option is used when card is not selected as any Access Mode option (Panel Configuration> Zone Configuration> Basic Configuration) and when FC is set as Read From Card No.

Replace with Card No.: Select this check-box when the FC is not obtained then the Card No. will be sent.

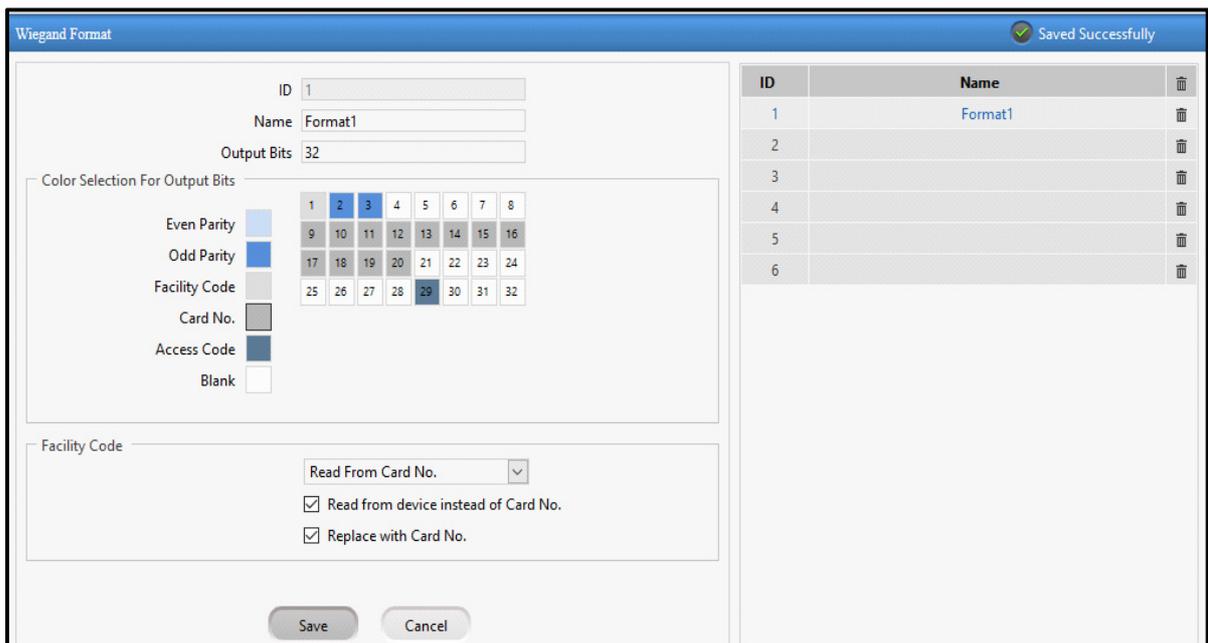


A screenshot of the 'Facility Code' configuration form. It includes a dropdown menu set to 'Read From Card No.', a checked checkbox for 'Read from device instead of Card No.', and a checked checkbox for 'Replace with Card No.'.

Click the **Save** button. The configured Wiegand format will be saved.



1. If a Wiegand Output format is edited and saved, it is automatically sent to all the devices to which this format is assigned.



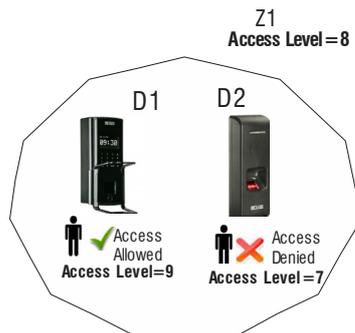
A screenshot of the 'Wiegand Format' configuration window. The window title is 'Wiegand Format' and it has a 'Saved Successfully' notification in the top right corner. The main area contains fields for ID (1), Name (Format1), and Output Bits (32). Below these is a 'Color Selection For Output Bits' section with a grid of 32 colored squares. The colors are: Even Parity (light blue), Odd Parity (dark blue), Facility Code (grey), Card No. (dark grey), Access Code (dark blue), and Blank (white). The 'Facility Code' option is selected for bit 29. At the bottom, there are 'Save' and 'Cancel' buttons.

ID	Name	
1	Format1	🗑️
2		🗑️
3		🗑️
4		🗑️
5		🗑️
6		🗑️

The Users section enables you to add users on the Panel200 and select Group and Zone for the user. You can assign basic and advanced Access Control policies to the users as well as enroll credentials of the user.

You can add maximum 25000 users to Panel200.

A Panel200 can have multiple Zones Z1, Z2, Z3 where each zone can be assigned Access Levels (Z1-L8). Each zone can have multiple doors (Z1- D1, D2). The user can be assigned Access level for working hours, break hours and non-working hours. When the Access Level of User is greater than Access Level of door (zone) then access is allowed to the user otherwise access is denied.



The total number of users configured in Panel200 is displayed as Total Users on dashboard. The number of Active Users, Inactive Users and Blocked Users is also displayed on the Dashboard.



User Configuration

User Configuration enables to configure a user on the Panel200. This page displays a search criteria and grid containing a list of created users along with their details - Name, Access Group, Access Schedule, Credentials and Face Images (Updated At). You can also edit or delete a user from the grid itself.

For details, refer to “[Server Mode](#)” and “[Standalone Mode](#)”.



Certain fields may appear as read-only fields when device is in the Server Mode.



When the 1st schedule is created from Shifts and Schedule; then it will get assigned to all the users and will be displayed in Access Schedule column.

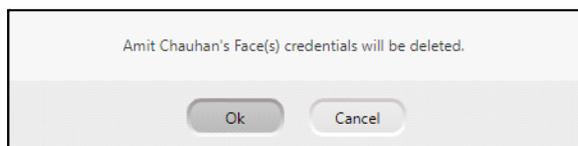
Server Mode

When the Panel is in **Server mode**, the following details are displayed in the grid. These details are fetched from the Server.

User ID	User Name	Access Group	Access Schedule	Card(s)	Finger(s)	Palm(s)	Face Images (Updated At)
2676	Amit Chauhan	Group-1	Schedule Group	1	2	0	38 (28-04-2023 15:43)
w2	w2	Group-1	Schedule Group	0	0	0	9 (28-04-2023 15:35)
1785	Kusha	Group-1	Schedule Group	0	0	0	24 (28-04-2023 15:35)

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 the Delete Images icon, 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.



Face Images (Updated At) is applicable for Panel - Server Mode, when Via Panel is selected as the option for Face Sync In Panel Door in the Server.

The feature Face Sync In Panel Door (Via Panel) is not supported in Panel SDK1. However, the parameter Face Images (Updated At) will be visible with values as 0. The Delete Images option will not be applicable.

If you wish to opt for the Face Sync In Panel Door feature, then you need to upgrade your Panel with SDK2. For assistance please contact our Technical Support Team.

Standalone Mode

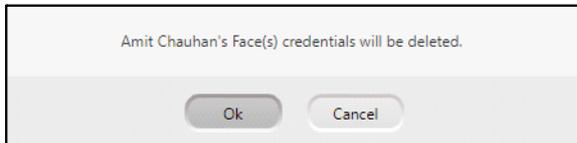
When the Panel is in **Standalone mode**, the following details are displayed in the grid.

User Configuration								
Search by <input type="text" value="Name"/> <input type="text" value="Enter ID/Name"/>								
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

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 the Delete Images icon, 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.

If you wish to delete a User, click **Delete** of the respective user.



*The count of face images in **Face Images (Updated At)** will be updated whenever:*

- *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.*

Panel200 supports a maximum of 25000 users.

To create new user click **Add** button and configure basic and advanced access control parameters.

Profile

User Configuration

Profile | Basic Access Control | Advanced Access Control | Advanced Access Control 2 | Face Recognition

User ID: 3A
User Name: T3A
Reference ID: 3
Active:
Email ID:
Mobile Number:
Access Group: Group-1
Functional Group: Staff
Assign Door: 2 selected
Home Zone: Zone-1
Visit Zone:
VIP:
Absentee Rule:
Absent Days Count: 60 (1-365)

Add Delete Save Cancel

User ID: Specify a unique User ID. It can have an alphanumeric value with a maximum of 15 characters.

User Name: Enter a name that identifies the user. Maximum upto 45 characters.

Reference ID: This is auto-generated.

Active: Select this checkbox to activate this user.

Access Group: Assign an Access Group, click the Select Access Group pick-list and select the desired option..

Functional Group: Select the desired option from the drop-down list..

Assign Door: The doors configured in Panel200 can assigned to the user.

To remove the assignment of particular door; click the Door picklist and delete the door from the list.

You can select the desired Door Group or select individual Door's by clicking the respective pick-list.

Home Zone: Select the home zone to be configured for the user from the dropdown list.

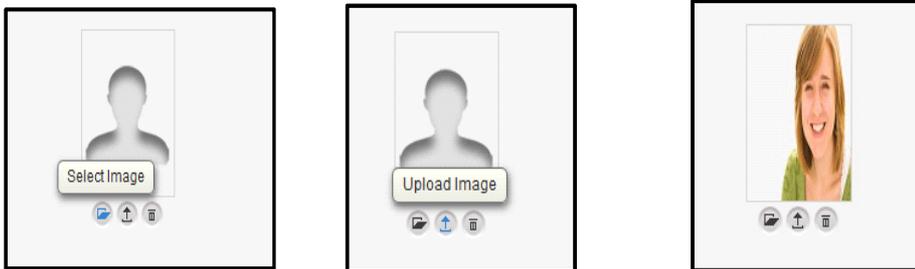
Visit Zone: Select the Visit zone to be configured for the user from the dropdown list.

VIP: Select this check-box, if the unrestricted access is to be given to the user.

Absentee Rule: Select this checkbox to enable the Absentee rule at user level. This rule will allow you to configure maximum no. of days which user will be allowed to be absent, thereafter the user will be denied access. However, this option needs to be first enabled at the Panel level (Panel Configuration> Access Features> Set 1).

Absent Days Count: Specify the day count for the Absentee rule ranging from 1 to 365.

You can upload the image of the user by clicking **Select Image** button and select the image from the desired location. Click **Upload Image** button to upload the image of user and click **Save** to save the Profile of user. Click **Remove** to delete the profile image.



Basic Access Control

Basic Access Control consists of these sections— Credentials, Validity and Access Route.

Credentials

PIN: Specify the PIN for the user. User PIN is a numeric value ranging from 1 digit to a maximum of 15 digits.

PVR Group No.: Specify the PVR group number to be assigned to the user, if applicable. It is a number allotted to a group of users assigned on a device. This enables the device 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: Enter 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 system will display an error.

This Access Card number will be synced with the panel to allow/deny access to users.

PANEL accepts up to two cards per user. So if required and available, enter the **Card 2** number.

Once you save the configurations, hover your mouse over the Facility Code separated CSN value of any Card, the system will display an encoded (converted) value of Facility Code separated CSN.

Enrolled Fingers/Palm/Faces: This option displays the number of fingerprint/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.*

Enrolled Faces is applicable for Panel- Standalone Mode only.

Enable Self-Enrollment: Select the checkbox to enable self-enrollment feature for the user. The Self-Enrollment feature enables the user to enroll himself/herself at a COSEC door controller using a pre-assigned access PIN, without the help of any operator or HR executive.

You must also enable Self-Enrollment from Panel Configuration> Advanced Profile> Enrollment

Profile	Basic Access Control	Advanced Access Control	Advanced Access Control 2	Face Recognition
Credentials				
PIN		16818		
PVR Group No.		143		
Card 1		56321		
Card 2				
Enrolled Fingers		0		
Enrolled Palm		0		
Enrolled Faces		3		
Enable Self-Enrollment		<input checked="" type="checkbox"/>		
Validity				
Enable		<input checked="" type="checkbox"/>		
Valid Upto		31-12-2037		
Access Route				
Route		RnD Route		
Add Delete Save Cancel				

Validity

Enable: Enable this option if the user credential is to be activated for a predefined period.

Valid Upto: Specify the end date of the validity of the user credential.

Access Route

Route: Click **Select Route** button to assign a predefined access route to the user based on which user has to access the configured devices of the route. The Access Route is configured from Access Policies> Access Route.

Click on **Save** to save the Basic Access Control configurations.

Advanced Access Control

Advanced Access Control consists of these sections— Basic, Shift Based Access, Smart Card Access Route and Mobile Based Access.



In Panel - Server Mode, the parameters will be displayed as configured in the COSEC Server. To know more about the parameters refer the COSEC User Guide.

Basic

Restrict Access: Select this checkbox to restrict access for the user on the Panel200. This implies that punches on the panel door will be considered for attendance only and will not open the door for access.

User Configuration	
Profile	Basic Access Control
Basic	
Restrict Access	<input type="checkbox"/>
Bypass Finger	<input checked="" type="checkbox"/>
Bypass Palm	<input checked="" type="checkbox"/>

Bypass Finger/Palm: Select this check-box, if Finger/Palm identification issues are being faced by the user. the system administrator can bypass the Finger/Palm check for the user. The user can punch in or out using any of the assigned pin or card and the same will be considered for attendance calculation.

Shift Based Access

Enable: Select this 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: In case of multiple shifts in the schedule group, 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.



The Shift Schedule and Holiday schedule has to be configured from Access Schedule.

The screenshot shows the 'User Configuration' window with the following sections and settings:

- 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: 05
 - Holiday Schedule: 1
- Smart Card Access Route:**
 - Max Route Level: 75
 - Smart Card Access Route: RnD Smart Route
- Mobile Based Access:**
 - Enable:

Buttons at the bottom: Add, Delete, Save, Cancel

Smart Card Access Route

Max Route Level: Select the route level up to which the user is to be allowed access.

Smart Card Access Route: Click the Smart Routes pick-list and select the desired route to be assigned to the user.

Mobile Based Access

The screenshot shows the 'Mobile Based Access' configuration section with the following details:

- Enable:
- IMEI: 345t3465677853476
- Buttons: Enroll IMEI, i

Enable: Select this check-box to allow the user to access the COSEC device through the Mobile.

IMEI: Specify the IMEI (International Mobile Equipment Identity) number of the mobile. Click Enroll IMEI button to enroll a user to access COSEC device through mobile. On clicking the button, the enrollment for the selected user will be activated for 60 seconds.

Advanced Access Control 2

Advanced Access Control 2 consists of these sections — Elevator Access Control, Access Cluster and Access Rule.



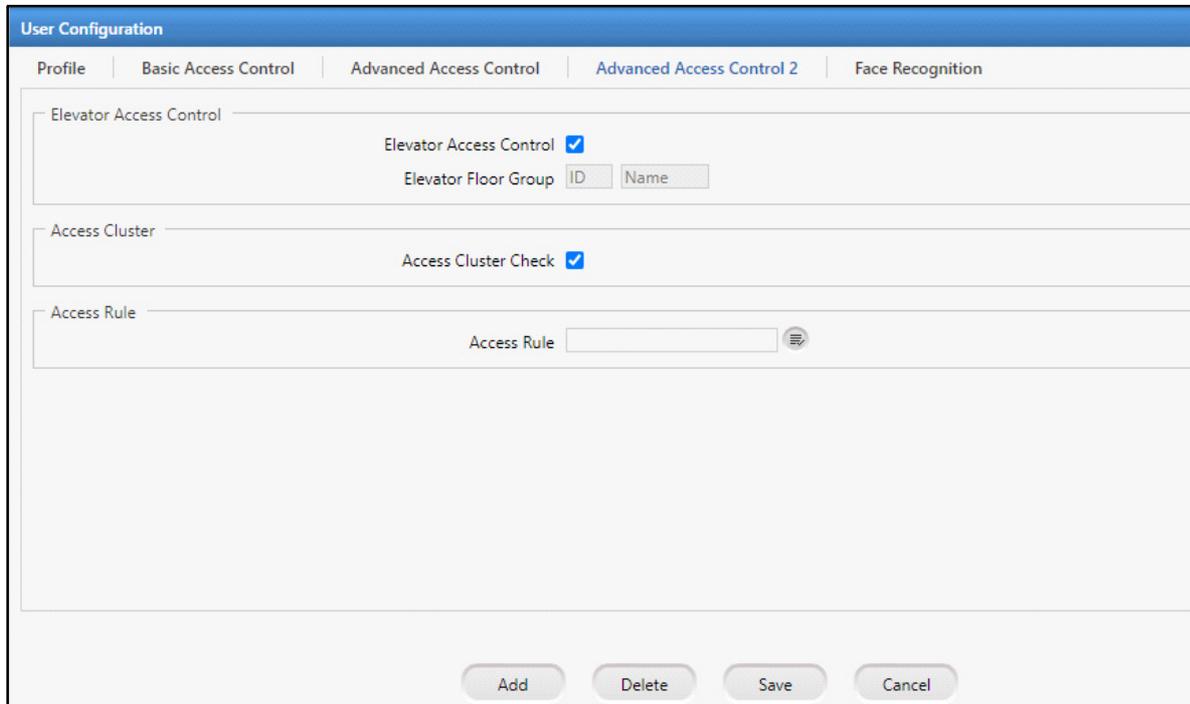
*Advanced Access Control 2 is configurable only when the Panel Mode is in Standalone Mode.
(Configuration > Basic Profile > Panel Mode)*

*In Panel - Server Mode, the parameter Access Rule will be displayed as configured in the COSEC Server.
To know more about the parameters refer the COSEC User Guide.*

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. To know more, refer to the Elevator Floor Group > Users Linking.



The screenshot shows the 'User Configuration' window with the 'Advanced Access Control 2' tab selected. The 'Elevator Access Control' section is expanded, showing a checked checkbox for 'Elevator Access Control' and two input fields for 'Elevator Floor Group' labeled 'ID' and 'Name'. Below this, the 'Access Cluster' section is expanded, showing a checked checkbox for 'Access Cluster Check'. The 'Access Rule' section is expanded, showing a text input field for 'Access Rule' and a pick-list icon. At the bottom of the window are four buttons: 'Add', 'Delete', 'Save', and 'Cancel'.

Access Cluster

Access Cluster Check: Select this checkbox to allow the cluster to the user.

For more details, [See "Access Cluster" on page 185.](#)

Access Rule

Click the Select Access Rule pick-list and select the desired access rule to be assigned to the user. The access of the doors to the user will be as per the configured rule.



Maximum 99 Access Rules can be assigned to a user.

In Panel-Server Mode, you will only be able to click the pick-list and view the Access Rule assigned to the user.

For more details, [See "Access Rule" on page 192.](#)

Face Recognition



For Panel- Server Mode, **Face Recognition** checkbox will be visible as configured from the Server. However, all other parameters will not be displayed.

Face Recognition consists of- Face Recognition and Face Enrollment.

The screenshot shows the 'User Configuration' window with the 'Face Recognition' tab selected. The 'Face Recognition' checkbox is checked. The 'Face Validation Device' is set to '5' and 'ARGO FACE DOOR-00:1b:09'. Below this is the 'Face Enrollment' section with an 'Enrolled Faces' area containing a user icon and a plus sign. A note indicates supported file formats: *.jpg/.jpeg, File size should be less than 200 KB. At the bottom are buttons for 'Add', 'Delete', 'Save', and 'Cancel'.

Face Recognition: Select the checkbox to enable Face Recognition.



If you disable this checkbox, the face images will be deleted from the Panel Doors but will be available with the Panel.

Face Validation Device: The device selected for face validation appears here. The face images uploaded from this page will be validated through the device selected for face validation. Hover-over the  icon to view the details.

Click on  if you wish to change the Face Validation Device. You will be re-directed to select the device 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



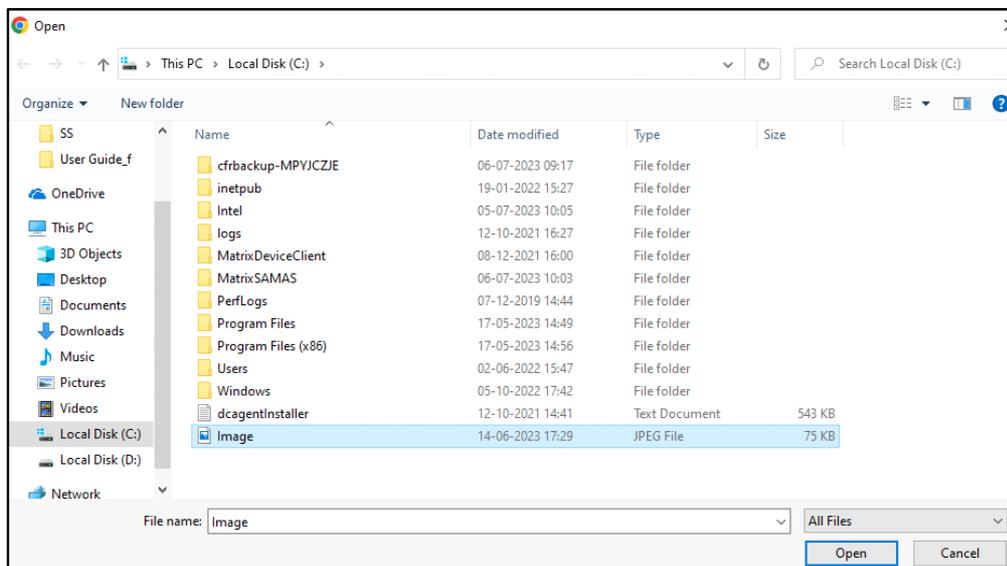
The complete face images will not be visible due to security reasons in this document.

*Make sure the **Face Validation Device** is assigned.*

*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.*

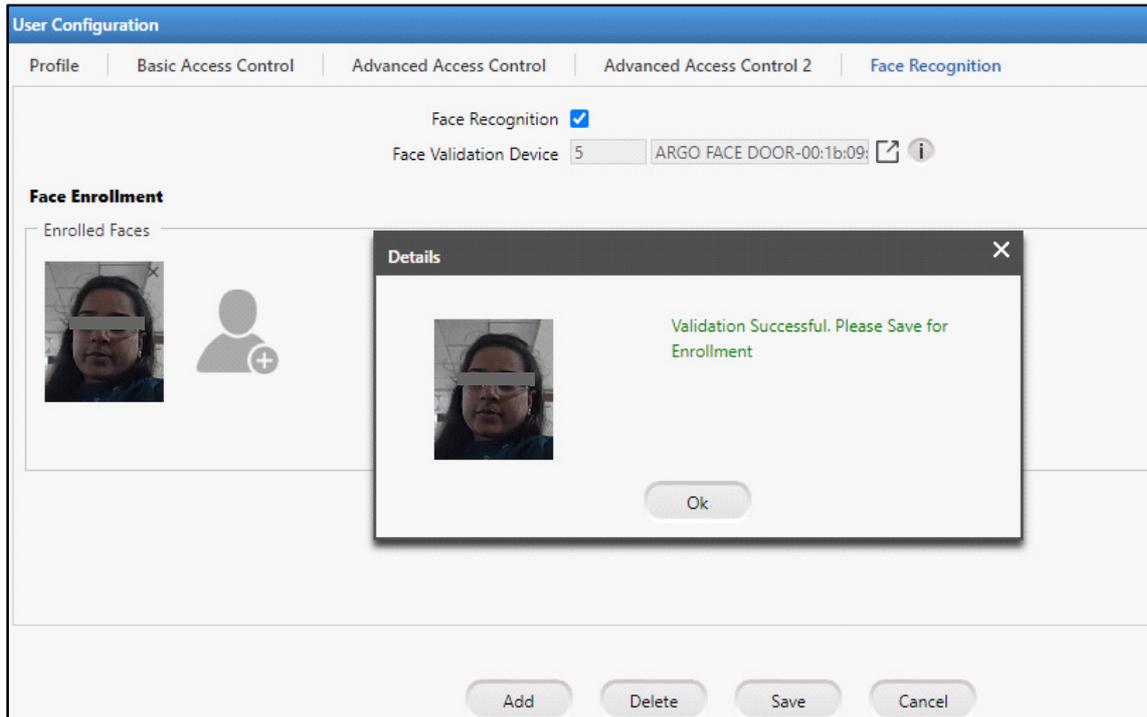
All the enrolled faces of the user will be displayed here. You can also upload images from this page if required. To do so,

- Click **Upload Face Image**  and select the image from the desired location.



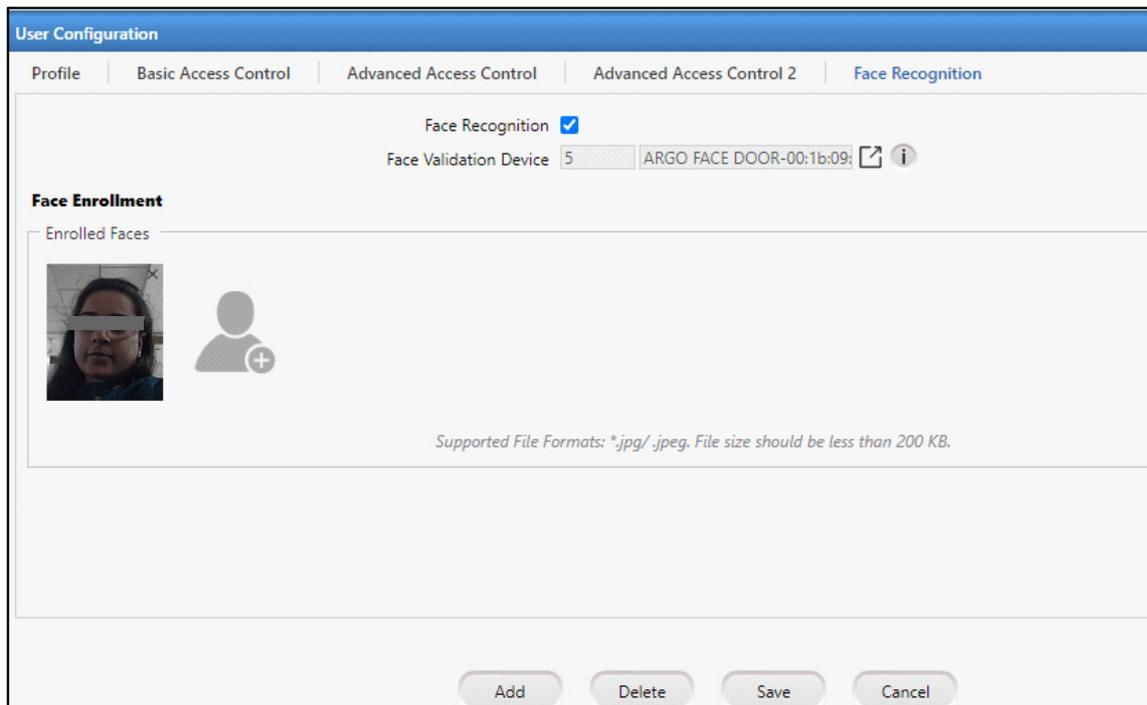
The image will be uploaded and then validated by the configured Face Validation Device. The image preview appears under Face Enrollment.

Once the image validation is done and the image is uploaded successfully, the **Details** pop-up appears.



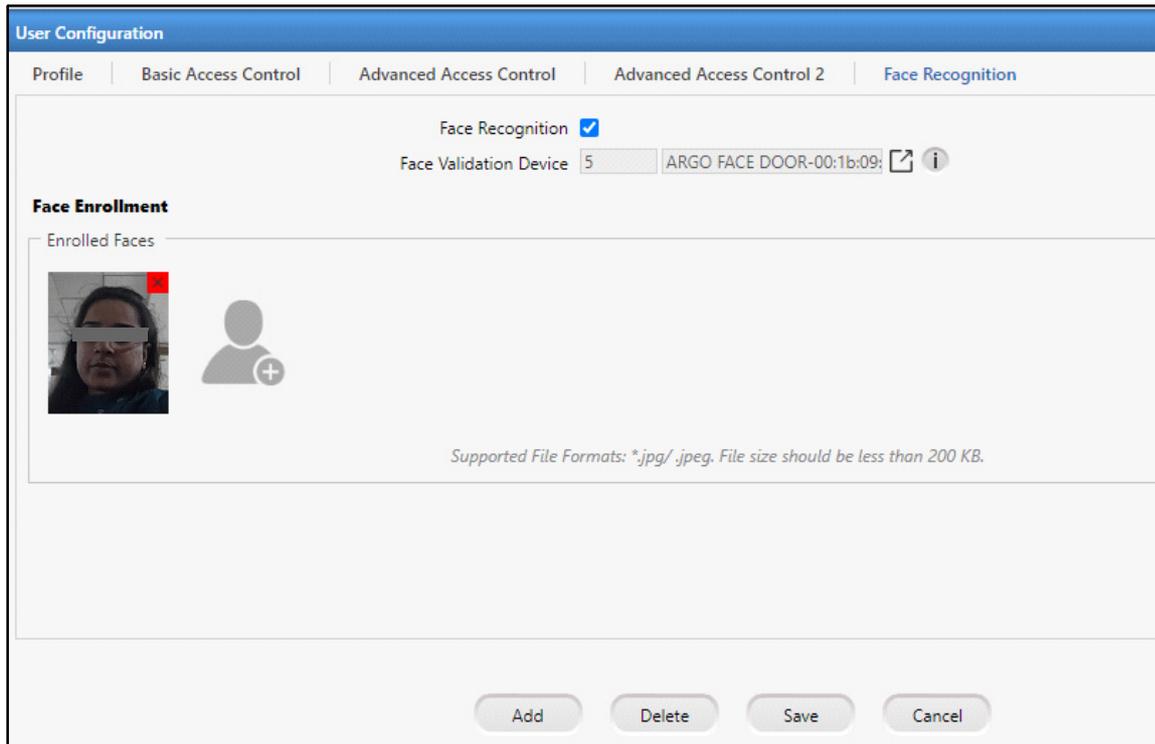
- Click **Ok** to close the pop-up. Click **Save** to enroll the image.

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 Panel Door.

If you do not wish to remove the 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 device selected for Face Validation will sync the available face images with all the other Face Recognition devices (ARGO FACE 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.

Access Group



Access Group is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

This page enables you to view the created access groups as well as create new Access Groups.

An Access Group can be defined as a group of users having similar job functions and who need to be assigned the same privileges throughout the day. In Access Groups, you can configure Time Zone based - Working, Break and Non Working hours - User Access Levels.

The Panel compares Access Level of User with Access Level of the Zone before the user is Allowed or Denied access to the restricted areas. A maximum of 99 Access Groups can be defined in the system.

Group ID	Group Name	User Access Level			🗑️
		Working Hours	Break Hours	Non-Working Hours	
1	Group-1	8	8	8	🗑️

Click **Add** button to add an Access group. The page appears with the configurations and a grid comprising of predefined members. These members cannot be deleted, they can only be updated from the Schedule Based Access Level Override section.

Access Group

Group ID:

Group Name:

Active:

User Access Level

Work Hours: ▼

Break Hours: ▼

Non-Working Hours: ▼

Group ID: It is auto generated by the system.

Group Name: Enter a suitable name for the new access group.

Active: Select the Active check-box to enable the Access Group.



After creating the access group, it can be assigned to the user from “User Configuration”.

User Access Level

Specify the User Access Levels for **Working hours**, **Break Hours** and **Non-Working Hours**, ranging from 01 to 15 from the drop down list.

The access level of the user is compared to the access level of the zone and user is granted access only if user access level is greater than or equal to the access level of the zone.



The access level of zone is assigned from Zone Configuration > Basic Configuration

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

Time Zone: Select a Member on the grid to which a Time Zone is to be assigned. Then click the **Select Time Zone** picklist and select the time zone as configured from Access Policies > Time Zone.

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

Access Level: Specify the Access Level for the Time Zone ranging from 01 to 15 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 the Time Zone.

Click **Update** and **Save** to apply the changes.

Member	ID	Time Schedule	Access Level
1	2	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 activated for the RnD Employees group as shown above.



Either the User Access Levels or 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 on **View list** button to view the configured 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	RnD Employees	9	8	8	🗑️

Add

Functional Group



Functional Group is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

This page enables you to create a new Functional Group and view the created ones.

Group ID	Group Name	
1	Staff	
2	Visitor	
3	Admin	

To create a new Functional Group click the **Add** button.

Group ID	Group Name	
1	Staff	
2	Visitor	
3	Admin	
4	Factory	

Group ID: It is auto generated by the system.

Group Name: Enter a unique, user-friendly name for the Functional Group.

Click **Save** to apply the changes.

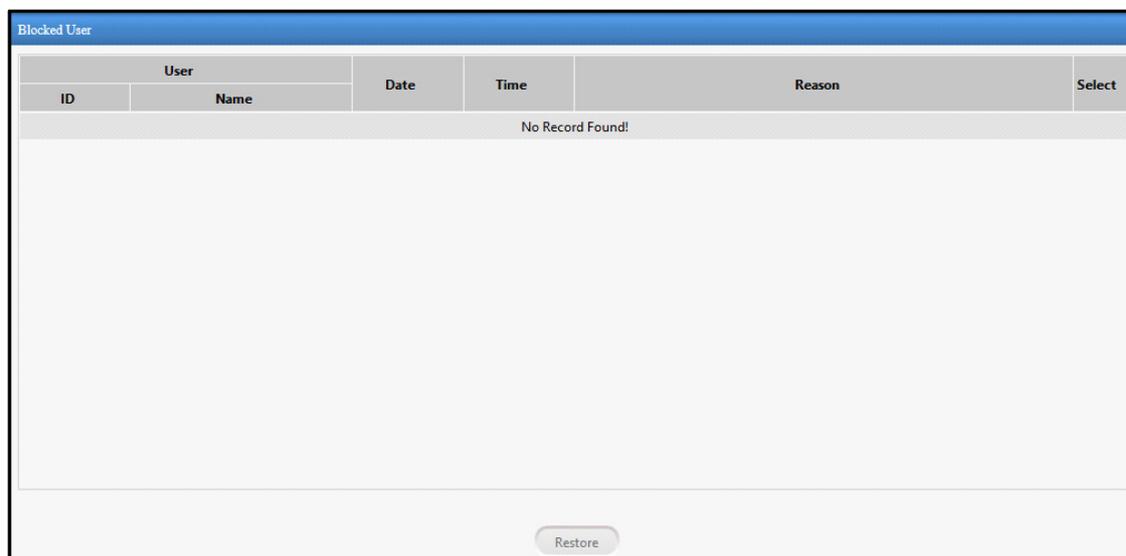
The screenshot shows a web interface titled "Functional Group" with a "Saved Successfully" notification in the top right corner. On the left, there is a form with two input fields: "Group ID" containing the value "1" and "Group Name" containing the value "Staff". On the right, there is a table with the following data:

Group ID	Group Name	
1	Staff	
2	Visitor	
3	Admin	
4	Factory	

An arrow points to the "Factory" group name in the table. At the bottom of the interface, there are three buttons: "Add", "Save", and "Cancel".

Blocked User

Users whose credentials have been temporarily blocked due to inactivity for a prolonged period are referred to as Blocked Users. This could happen in the event of the Absentee rule being applied to the user or unauthorized access attempts exceeding the defined limit.



User		Date	Time	Reason	Select
ID	Name				
No Record Found!					

Restore

Blocking a user only deactivates the credential and does not result in the deletion of user information from the device. The possible reasons for deactivation are:

- Absentee rule being applied to user (Must be enabled from Access Features> Set1. For more information, refer [“Set1”](#))
- Failed Access attempts exceed five
- The Use Count Control rule has been violated (Must be enabled from Access Features> Set1. For more information, refer [“Set1”](#))



The other conditional violations that may lead to blocking of a user can be enabled from Panel Configuration > Access Features > Set 3. For more information, refer [“Set3”](#).

Blocked User					
User		Date	Time	Reason	Select
ID	Name				
3	Isha	06-04-2018	00:00:00	Absentee Rule	<input type="checkbox"/>
4	Aditi	06-04-2018	00:00:00	Absentee Rule	<input type="checkbox"/>

Restore

The Blocked Users will be displayed along with the reason as shown above.
 To restore the user; select the checkbox of the desired user and click **Restore** button to restore the user from blocked status.



Make sure the Alert Service is running to generate Block User Events.



The alert 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.

Enrollment can be defined as a process wherein the Panel accepts and stores the user credentials against a particular user.

This page allows you to start the enrollment process and assign credentials to the users.

User: Once users have been added to the Panel200, the enrollment process can be initiated from this page. It supports enrollment of user cards, finger print templates, palm templates, face templates and special cards. For more information, [See “User” on page 160.](#)

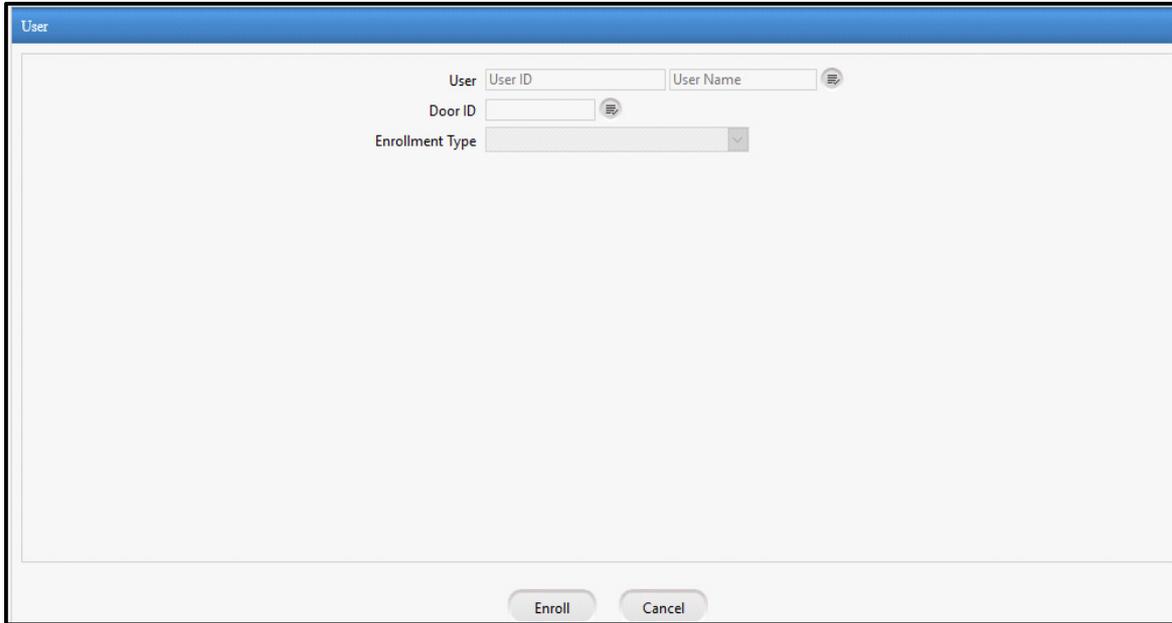
Special Card: A Special Card is a RFID card that can be encoded for a special function and the card-holder can perform a special function at the device just by displaying this special card. For more information, [See “Special Card” on page 163.](#)

SI User: The SI User page enables to enroll a SI (Smart Identification) user for allowing access to the system. For more information, [See “SI User” on page 164.](#)

Authorization: This page enables the system user to authorize the newly enrolled users. For more information, [See “Authorization” on page 166.](#)

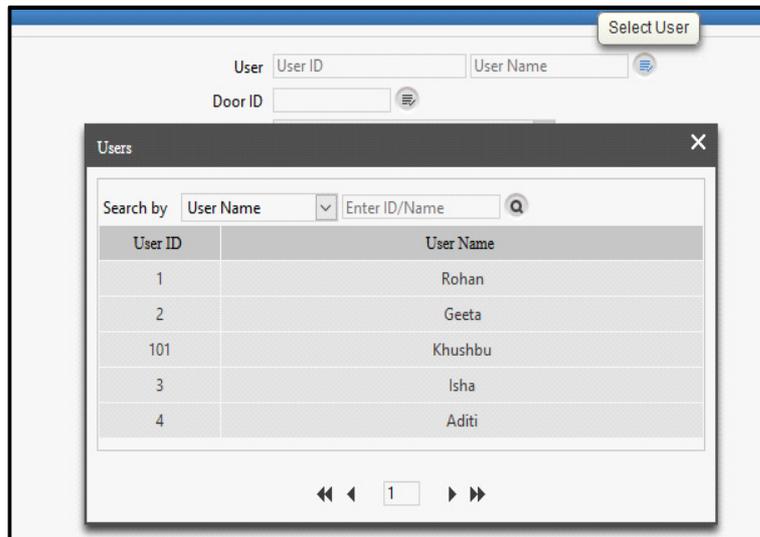
User

Once users have been added to the Panel200, the enrollment process can be initiated from this page. Enrollment can be defined as a process wherein the Panel accepts and stores the user credentials against a particular user. It supports enrollment of user cards, finger print templates, palm templates, face templates and special cards.



The screenshot shows a web interface titled "User" with a blue header. Below the header, there are four input fields: "User ID", "User Name", "Door ID", and "Enrollment Type". The "User ID" and "User Name" fields have a search icon to their right. The "Enrollment Type" field is a dropdown menu. At the bottom of the form, there are two buttons: "Enroll" and "Cancel".

Click Select User button and select the desired user from the picklist, for whom the enrollment is to be done.



The screenshot shows the same "User" form as above, but with a "Select User" button highlighted. A dialog box titled "Users" is open, showing a search bar and a table of users. The search bar has "Search by" set to "User Name" and a search icon. The table has two columns: "User ID" and "User Name". The table contains the following data:

User ID	User Name
1	Rohan
2	Geeta
101	Khushbu
3	Isha
4	Aditi

At the bottom of the dialog box, there are navigation arrows and a page number "1".

Click Select Door button and select the desired Door from the picklist on which the enrollment is to be performed for the user.



Enrollment can also be done using the Device. For details, refer to [“Enrollment”](#).

Select the desired **Enrollment Type** from the dropdown list. The Enrollment Types for a user that can be performed on a device depends on the device type. The following options are available:

- ReadOnlyCard
- SmartCard
- Biometric
- Biometric Then Card
- Mobile Device
- Duress Finger
- Face

1. For **Read Only Cards**, select the **No. of Cards** to be enrolled from the dropdown list.
2. For **Smart Card**, select the **No. of Cards** to be enrolled, select the check box of the respective parameter:
 - 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 dropdown list.

Apart from the above, for Smart Card with Personalized Details, the following additional details can also be configured for the Smart Card:

- Designation
- Branch
- Department
- Blood Group
- Emergency Contact
- Medical History

Select the check box of the respective parameter and enter the desired information in the respective field.

3. For **Biometric**, select the **No. of Fingers/Palms** to be enrolled from the dropdown list.
4. For **Biometric then Card**, select the **No. of Cards** and **No. of Fingers/Palms** to be enrolled from the dropdown list.
5. For **Mobile Device**, in **Access Card Selection**, select the **Access Card** to be enrolled from the dropdown list.

6. For **Duress Finger**, select the **No. of Fingers** to be enrolled from the dropdown list.

7. For **Face**, select the **No. of Faces** to be enrolled from the dropdown list.

Click **Enroll** button to initiate enrollment or **Cancel** to discard the changes on the selected Panel Door.

After the enrollment is successful, the number of credentials enrolled for a user can be viewed from User Configuration page as follows.

User Configuration								
Search by		Name	Enter ID/Name					
User ID	User Name	Access Group	Access Schedule	Card(s)	Finger(s)	Palm(s)	Face Images (Updated At)	
111	1111	Group-1		0	2	0	10 (13-06-2023 10:17)	
222	222	Group-1		0	0	0	0	
9	999	Group-1		0	0	0	12 (13-06-2023 10:28)	

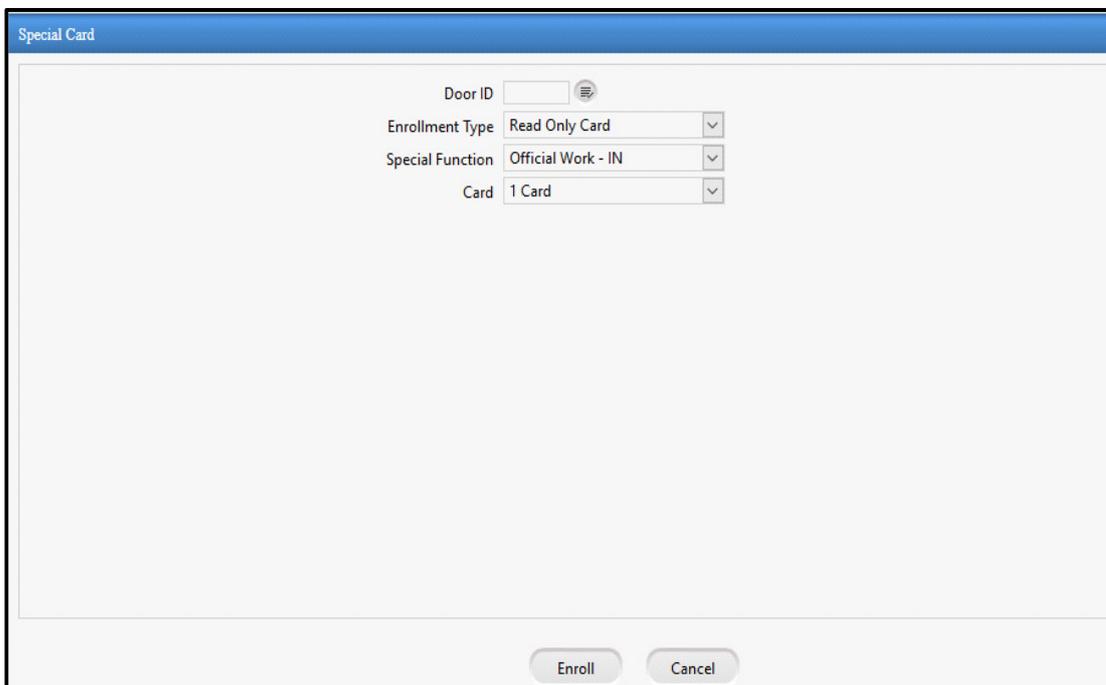
Special Card

A Special Card is a RFID card that can be encoded for a special function and the card-holder can perform a special function at the device just by displaying this special card.

A Special Card is especially 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 controller device does not have keypad or LCD display for manual entry of special codes.

Example: In factories where workers avail short leave; security guard can show the Special card enrolled for Shortleave IN on the Entry door and can give the access to the worker. This same card can be used for multiple workers.

The enrollment for a special card can be initiated from this page.



The screenshot shows a web form titled "Special Card". It contains the following fields:

- Door ID: A text input field with a pick-list icon to its right.
- Enrollment Type: A dropdown menu with "Read Only Card" selected.
- Special Function: A dropdown menu with "Official Work - IN" selected.
- Card: A dropdown menu with "1 Card" selected.

At the bottom of the form, there are two buttons: "Enroll" and "Cancel".

Door ID: Click the Door button and select the desired door from the pick-list on which the special card enrollment is to be performed.

Enrollment Type: Select the desired option - Read Only Card or Smart Card from the drop-down list.

Special Function: Select the desired option from the dropdown list for which the special card is to be enrolled.

Card: Select the Number of Cards to be enrolled for a special function from the dropdown list. Maximum four cards can be enrolled for a single special function.

Click the **Enroll** button to initiate enrollment on the selected Panel Door. The user will be prompted by the selected door controller to display the special card for enrollment.

SI User



SI User is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

The SI User page enables to enroll a SI (Smart Identification) user for allowing access to the system. SI user is a user who is allowed access to another office by means of Smart Card, though s/he is not enrolled onto that particular office system.

SI User

Door ID

Enrollment Type

Smart Identification Options

Reference ID

User ID

User Name

Access Level (1-75)

Validity Date

PIN

Designation

Branch

Department

Blood Group

Emergency Contact

Medical History

Bypass Finger

Enroll Cancel

Configure the following parameters:

Door ID: Enter Door ID or click Select Door button to select the door on which the user is to be enrolled.

Enrollment Type: It displays the enrollment type. By default it is Smart Card.

Smart Identification Options

The following information can be written onto the Smart Card for the SI User during enrollment:

Reference ID: If reference ID is to be used for smart identification, then first select the checkbox and then enter the ID. Maximum 8 digits can be entered.

User ID: If User ID is to be used for smart identification, then first select the checkbox and then enter the ID. User ID can be maximum of 15 characters.

User Name: If User Name is to be used for smart identification, then first select the checkbox and then enter the user name. Maximum length is 15 characters.

Access Level: If Access Level is to be used for smart identification, then first select the checkbox and then specify the level. Valid range is from 1 to 75.

Validity Date: If Validity Date is to be used for smart identification, then first select the checkbox and then select the date after which the user is considered as an invalid user.

PIN: If PIN is to be used for smart identification, then first select the checkbox and then enter the PIN number. Maximum 6 digits PIN number is allowed.

Finger Template: If Finger Template is to be used for smart identification, then first select the checkbox and then select the number of templates to be considered for enrollment from the dropdown list. This option is not available for PVR and ARGO FACE Door.

Designation: If Designation is to be used for smart identification, then first select the checkbox and then enter the designation.

Branch: If Branch is to be used for smart identification, then first select the checkbox and then enter the branch name.

Department: If department is to be used for smart identification, then first select the checkbox and then enter the department name.

Blood Group: If blood group is to be used for smart identification, then first select the checkbox and then select the blood group from the dropdown list to be used.

Emergency Contact: If emergency contact is to be used for smart identification, then first select the checkbox and then enter the contact number.

Medical History: If medical history is to be used for smart identification, then first select the checkbox and then enter the medical history.

Bypass Finger: Select the option, if the finger is to be bypassed.

VIP: If enabled, VIP is written in the card.

ASC: If enabled, the ASC defined in the panel is written on the card.

Facility Code: If enabled, the facility code defined in the panel is written on the card.

Smart Access Route ID and Smart Access User Level: If enabled, users will be allowed access to only specified doors with specified levels in predefined route using a smart card. Enter the corresponding Route ID and User Level.

Click **Enroll** to enroll the user or click **Cancel** to cancel the changes.

Authorization



Authorization is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

This page enables the system user to authorize the newly enrolled users.

User ID	User Name	Status	Authorize <input type="checkbox"/>	Reject <input type="checkbox"/>
No Record Found!				

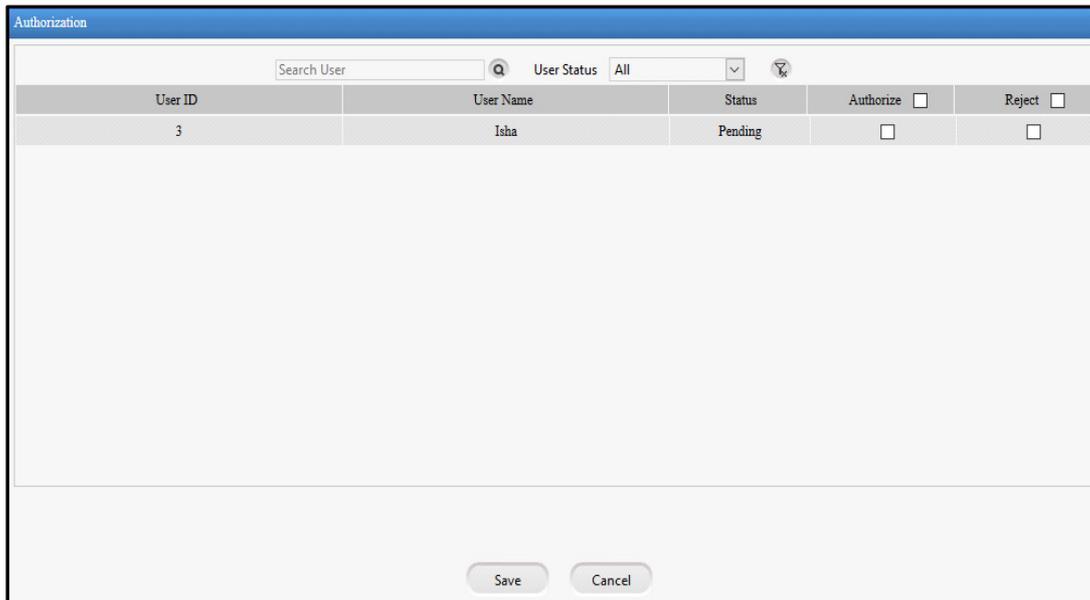
When enrollment of new user is done, then the enrolled credentials require authorization for accessing the panel doors. This user authorization is done from this page.



The Enrolled credential of user needs to be Authorized when “Authorization on Enrollment” is enabled from Panel Configuration> Advanced Profile > Enrollment.

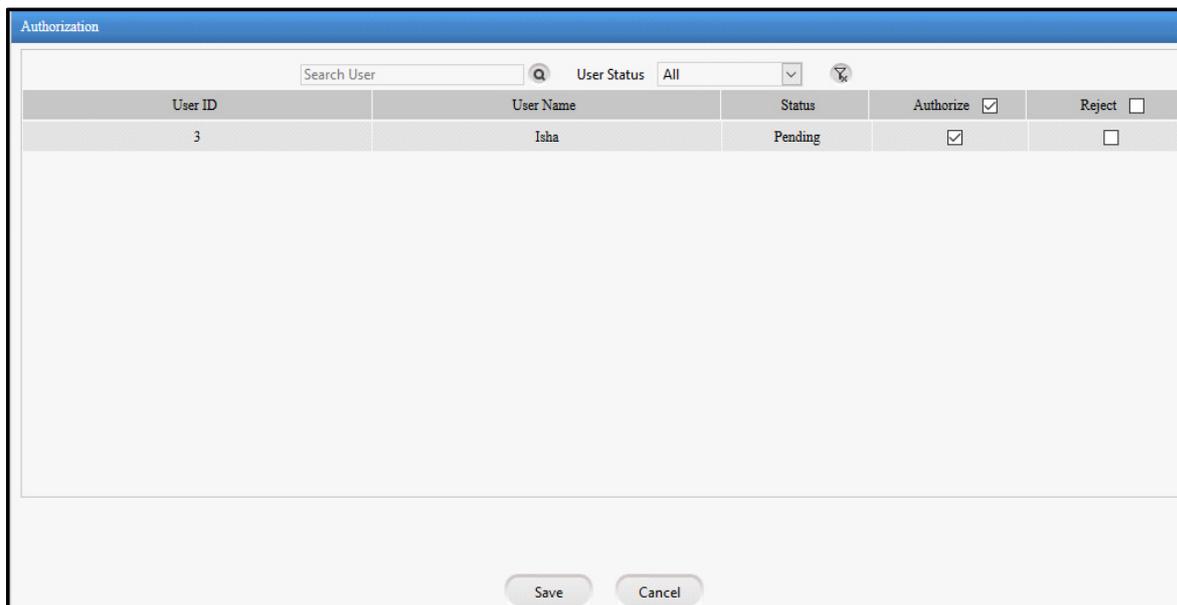
*The “Face Enrollment” request for approval will not appear on this page even if the **Authorization on Enrollment** is enabled from Panel Configuration> Advanced Profile > Enrollment.*

The Status column displays Pending, Authorized and Rejected applications.



You can search the records based on User and User Status. The User Status can be filtered from the options of All, Pending and Rejected.

The system user or the users having Enrollment Authorization rights can select the Authorize or Reject checkboxes for the desired record.



Then click **Save** to apply the authorization. Now the authorized user can use the credentials to access the door.

Access Policies & Access Schedule



Access Policies and Access Schedule are configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

Access Control System can detect and report intrusion, access to warehouse, cash rooms in banks, R&D departments in corporate, troubled conditions, any other place, where unauthorized access needs to be monitored. Access control systems can grant, record, deny, detect and report access to facilities, services, information and other assets that need to be protected from mass access.

The Access Policies section enables you to configure Access control policies such as 2 person Rule, First-IN user rule etc which will restrict the user from accessing the device when the configured rule is violated. The Alarms can also be configured which will be generated on violation of the rule.

All the events related to the Access Policies set by you appear in the Access Policy Report. For details, refer to [“Access Policies”](#).

The number of configured Access Rules are displayed under the Access Rules section on the Dashboard.



2-Person Rule

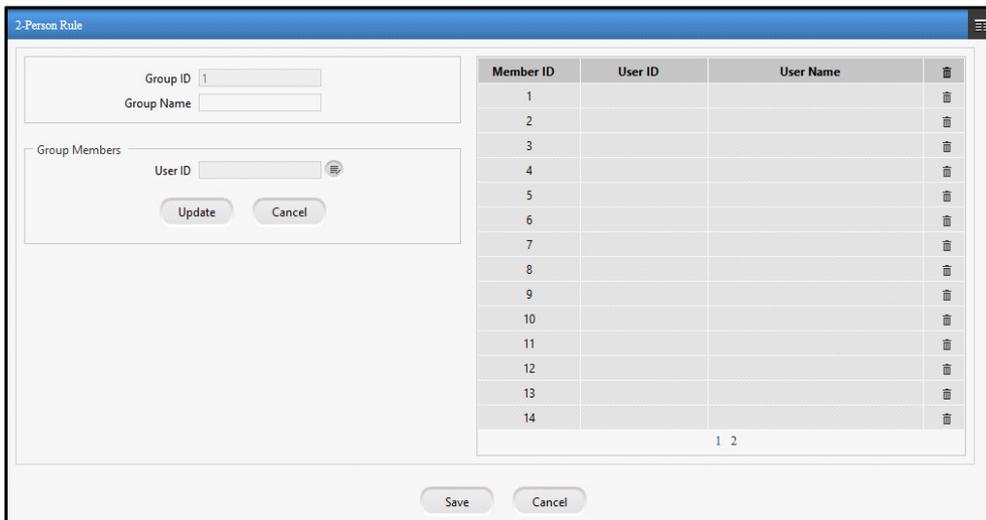
2-Person rule is a feature that enables the system to insist for two valid user entries within specified time to allow access to a secured zone.

This is a control mechanism, designed to achieve a high level of security, especially for critical areas like Cash rooms, R&D Labs, sensitive documents storage etc.

The page will display a list a list of 2-person groups created along with their details.. You can click on the group to edit it or click Delete icon to delete it.



To add a new group click **Add** button and enter the following details.



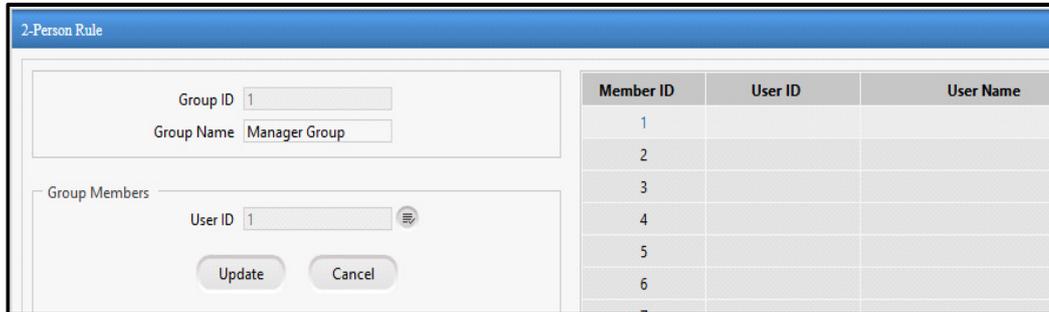
Group ID: It is auto-generated.

Group Name: Specify a user friendly name for the group.

Group Members

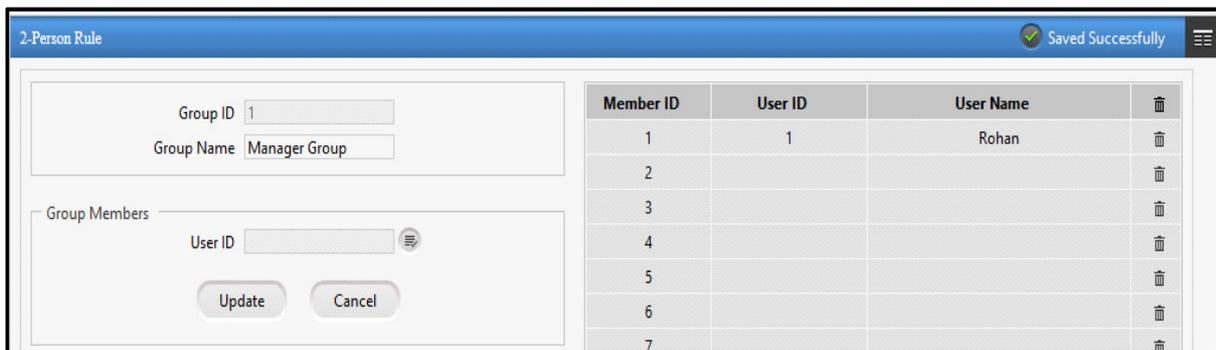
Configure the following, to add members to a group. Click on the Member ID from the right grid to which user is to be added.

User ID: Click the Select User button and select the desired user from the pick-list.



Member ID	User ID	User Name
1		
2		
3		
4		
5		
6		

Click on **Update** to save the members to the grid.
Then Click on **Save** to save the group.



Member ID	User ID	User Name	
1	1	Rohan	🗑️
2			🗑️
3			🗑️
4			🗑️
5			🗑️
6			🗑️
7			🗑️

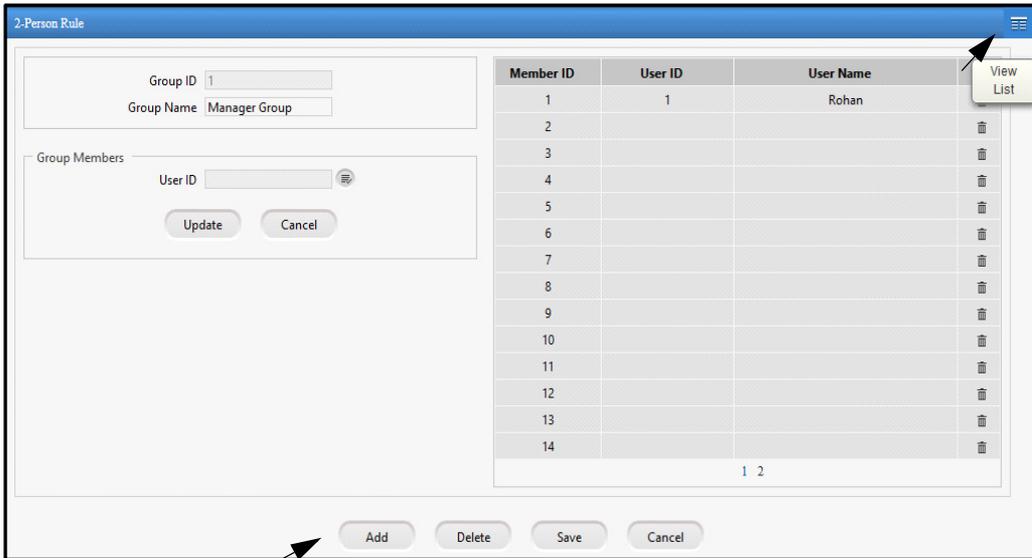
You can add more members to the group in the same way as described above.

The group can be deleted by clicking Delete button.

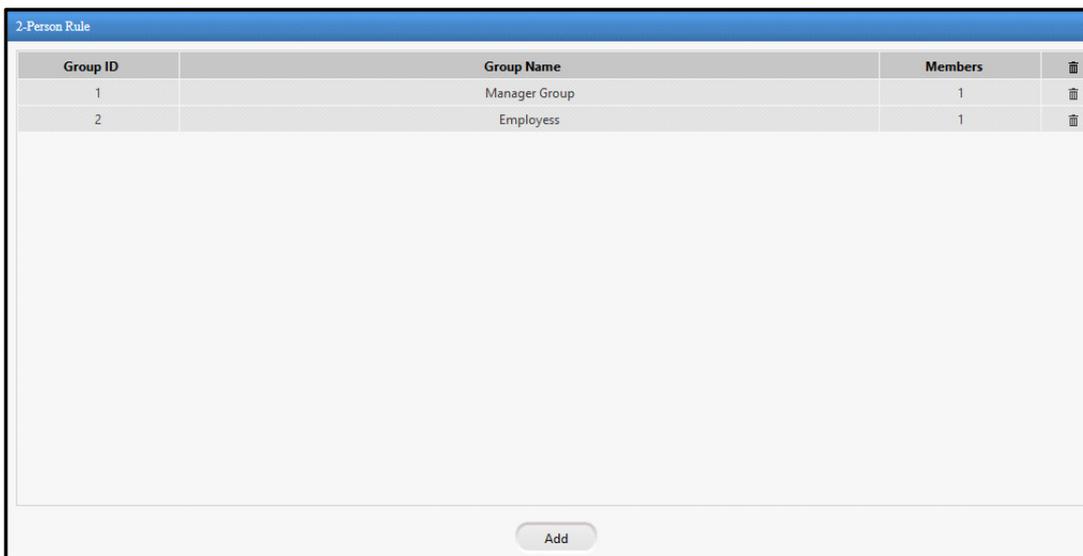


If the first person is an authorized user and the 2nd person is a VIP then, system considers the VIP as an authorized 2nd person to validate the 2 -Person Rule.

To add another group click **Add** button.



To view the added groups click **View list** button.



After creating groups for 2 person rule, you must enable:

1. Enable the rule from Panel
2. Configuration > Access Features > Set1
3. Configure the 2-Person Rule parameters for the Zone from Zone Configuration > Advance Configuration1

Now this rule will be applicable for those doors who are assigned the zone which is enabled for the rule.

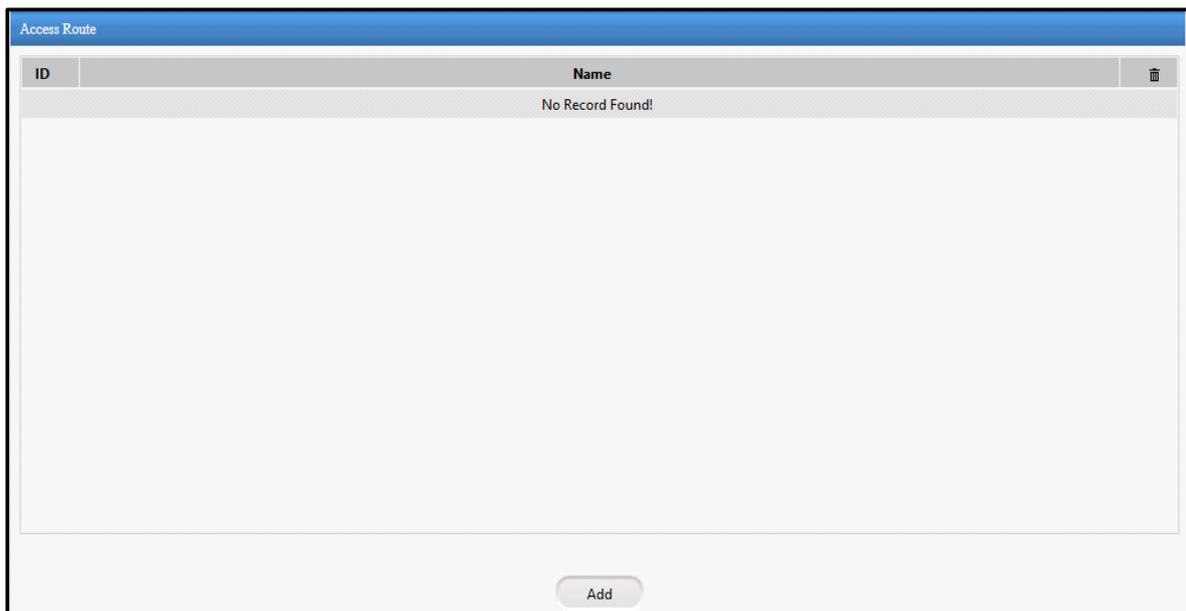
Access Route



Access Route is configurable only when the Panel Mode is in Standalone Mode. (Configuration> Basic Profile> Panel Mode)

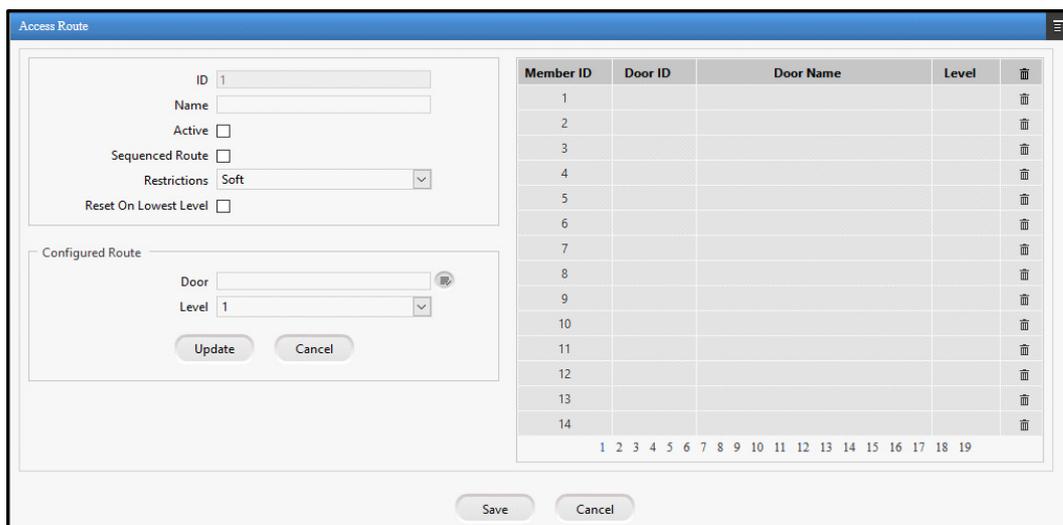
The Access Route functionality enables the administrator to define an access policy which allows the user to access only specified doors (applicable to Panel and Panel doors) with specified levels in predefined route, sequenced or unsequenced.

The page will display a list of created access routes along with their details. You can click on the access route to edit it or click Delete icon to delete it.



To add a new Access Route click **Add** button and enter the following details.

You can add maximum 255 Access routes and maximum 255 doors can be added to a route.



ID: It is auto-generated.

Name: Specify a descriptive name for the Access Route.

Active: Select the checkbox to activate 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 checkbox to enable the sequenced route. If it is disabled then sequence of doors will not to be followed.

In case of the sequenced option, the system checks on the route based on the levels defined. For example, the user has to swipe the 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 the IN as well as the OUT punches. Therefore it is necessary to have exit readers installed on all doors of the access route.

Restrictions: Select the Restriction from the dropdown options.

- **Hard:** Access will be allowed only if the access route is followed.
- **Soft:** Access will be allowed on any door with an access route violation message.

Reset on Lowest Level: Select the checkbox to enable the system 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 functionality 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 entry side.

Configured Route

You need to configure a route for accessing the doors.

Door: To select the Member Doors for the Access Route, click on the Member ID from the right side grid. Select Door button and select the desired panel doors from the pick-list.

Level: Select the Level number for the Door from the dropdown list.

Multiple Doors can be assigned to the same level. However, a single door cannot be assigned to the multiple levels.

If the Sequenced Route is enabled then Configure parameters for “Entry” and “Exit” as shown below.

Entry

The screenshot shows a configuration window with two main sections: 'Entry' and 'Exit'. Each section contains the following fields:

- Enabled:** A checkbox. In the 'Entry' section, it is checked; in the 'Exit' section, it is unchecked.
- Route Timer:** A text input field containing '600' and a unit label 'sec(1-65535)'.
- Level Restriction:** A dropdown menu with 'Soft' selected.
- Perform Action:** A dropdown menu with 'On User Punch' selected.

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.

- Select the **Enabled** checkbox to apply the 'Access Route Timer' between two levels. This option will be disabled by default.
- **Route Timer:** Enter the time duration in seconds till which a user must complete an access route cycle between two levels.
- **Level Restriction:** Select the restriction as 'Soft' or 'Hard' according to which an entry for the next level will be decided for a user.
- **Perform Action:** Select when an action for access route violation needs to be taken. The options are "On Timer Elapsed" and "On User Punch" according to which an alarm should be triggered.

Exit

This option allows user to configure the route timer between two levels (say between Door 2 & Door 3) during exit 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.

Configure the Exit parameters; Enabled, Route Timer, Level Restriction, Perform Action, the same way as you have configured for Entry.

Click on **Update** to save the door and configured route. You can assign upto 255 doors per access route.

The member devices can be deleted by clicking Delete button from the grid.

Click on **Save** to save the configured Access Route.

You can click on **View list** button to view the list of configured Access Routes as shown below.

ID	Name	
1	RnD Route	

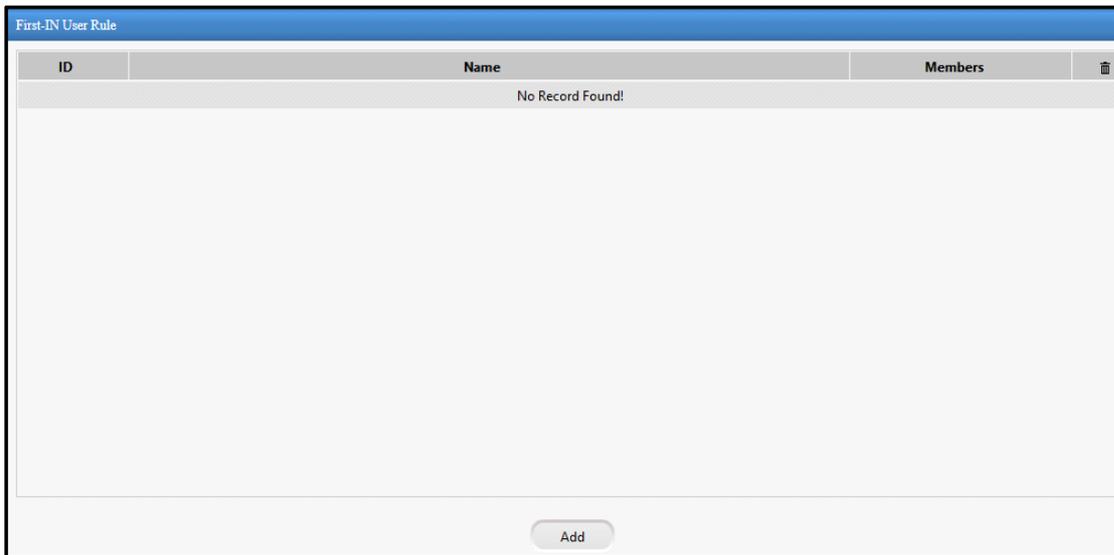


After configuring the Access Route, enable the rule from Panel Configuration> Access Features> Set1 and then make sure it is assigned to the user from User Configuration> Basic Access Control.

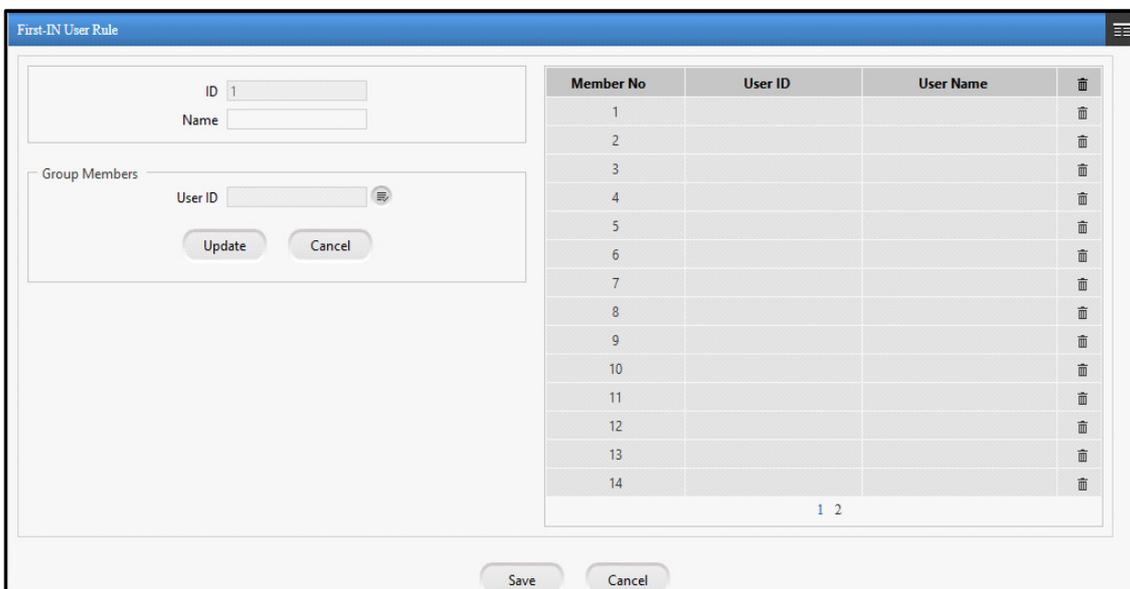
First-IN User Rule

First-IN User rule uses any credentials of the user who is declared as First-IN User to unlock the Access to a particular zone.

The page will display a list of created rules along with their details. You can click on the rule to edit it or click Delete icon to delete it.



To add a new First-IN User Rule click **Add** button and enter the following details.



ID: It is auto-generated.

Name: Specify a user friendly name for the Group of First-In users.

Group Members

User ID: To select the members, click on the Member No. from the right grid to which user is to be assigned. Then click on the Select User button and select the desired user from the picklist.

Click on **Update** to save the member. You can define upto 999 users in each group.

Click on **Save** to save the configured First -In user group.

Member No	User ID	User Name	
1	2	Geeta	🗑️
2	1	Rohan	🗑️
3			🗑️
4			🗑️
5			🗑️
6			🗑️
7			🗑️
8			🗑️
9			🗑️
10			🗑️
11			🗑️
12			🗑️
13			🗑️
14			🗑️



A VIP user is allowed to access the First-In enabled 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.



After configuring the First-In user Rule, you must:

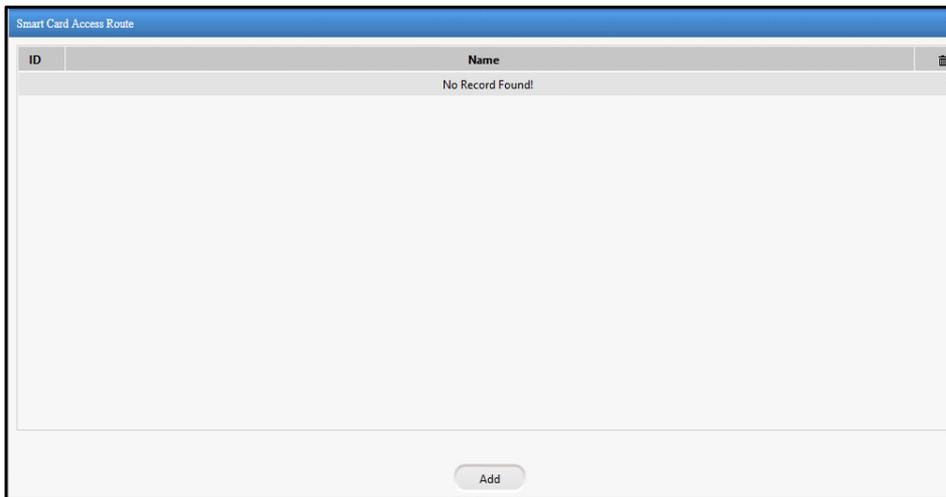
- 1. Enable the rule from Panel Configuration > Access Features > Set1*
- 2. Configure the rule at Zone Configuration > AdvanceConfiguration2.*

Now this rule will be applicable for those doors who are assigned the zone which is enabled for the rule.

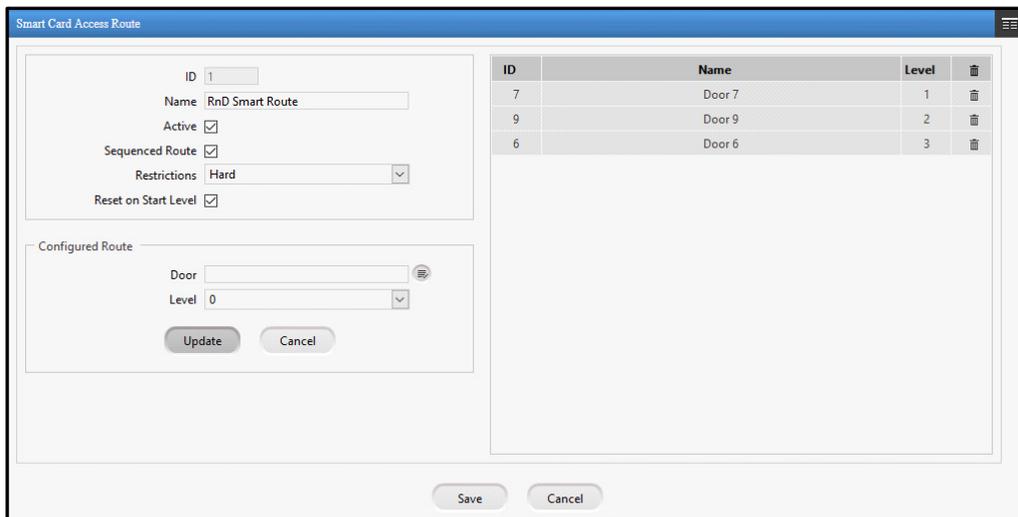
Smart Card Access Route

The Access Route using card functionality enables the administrator to define an access policy which allows the user to access the COSEC Doors in the configured sequence.

The page will display a list of created Smart Card Access Routes along with their details. You can click on the route to edit it or click Delete icon to delete it.



To add a new Access Route click **Add** button and enter the following details.



ID: It is auto-generated.

Name: Specify a descriptive name for the Smart Card Access Route.

Active: Select the checkbox to activate the Smart Card Access Route.

Sequenced Route: Select the checkbox to enable the sequenced route.

Restrictions: Select the Restriction from the drop down options.

- **Hard:** Access will be allowed only if the access route is followed.
- **Soft:** Access will be allowed on any door on the access route with an access route violation message.

Reset on Start Level: Select the checkbox to enable the system 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 functionality 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 entry side.

Configured Route

Door: To select the member Doors for the Access Route click the Select Door button and then select the desired device from the pick-list.

Level: Select the Level number for the Door from the dropdown list.

Click on **Update** to save the devices assigned to the Access Route.

Click on **Save** to save the configured Access Route.

ID	Name	Level	
7	Door 7	1	🗑️
9	Door 9	2	🗑️
6	Door 6	3	🗑️



After configuring the Smart Card Access Route, you must enable the rule from Panel Configuration> Access Features> Set2

Then it must be assigned to the user from User Configuration> Advanced Access Control.

Time Zone

Time Zone allows the system to grant access to the users to certain Access Zone only in a specified time period. This time period can be set as 24-hours or limited set of hours or minutes.

Each time zone represents a particular period of time and time zones may have overlapping time periods. The maximum time period which can be assigned to a time zone is 23:59 hours.

The screenshot shows the 'Time Zone' configuration window with the 'Configuration' tab selected. The 'Group' tab is also visible. The configuration fields are as follows:

- ID: [Empty text box]
- Name: [Empty text box]
- Active:
- Start Time: 00 : 00
- End Time: 00 : 00
- Active Days: Sun Mon Tue Wed Thu Fri Sat Holiday

On the right, there is a table with the following data:

ID	Name	
1	Time Zone 1	

An 'Add' button is located at the bottom center of the window.

Configuration

The Configuration tab enables you to create time zone by clicking **Add** button and configuring the following parameters.

ID: This is auto-generated.

Name: Specify a user friendly name for the Time Zone.

Active: Select the Active checkbox to enable the Time zone.

Start Time: Specify the Start time period (in hh:mm) for the defined time zone.

End Time: Specify the End time period (in hh:mm) for the defined time zone.

Active Days: Select the check-box of the respective days for which the Time Zone is to be activated.

Holiday: Do not select the check-box if you want the provision for Holidays to be overruled.

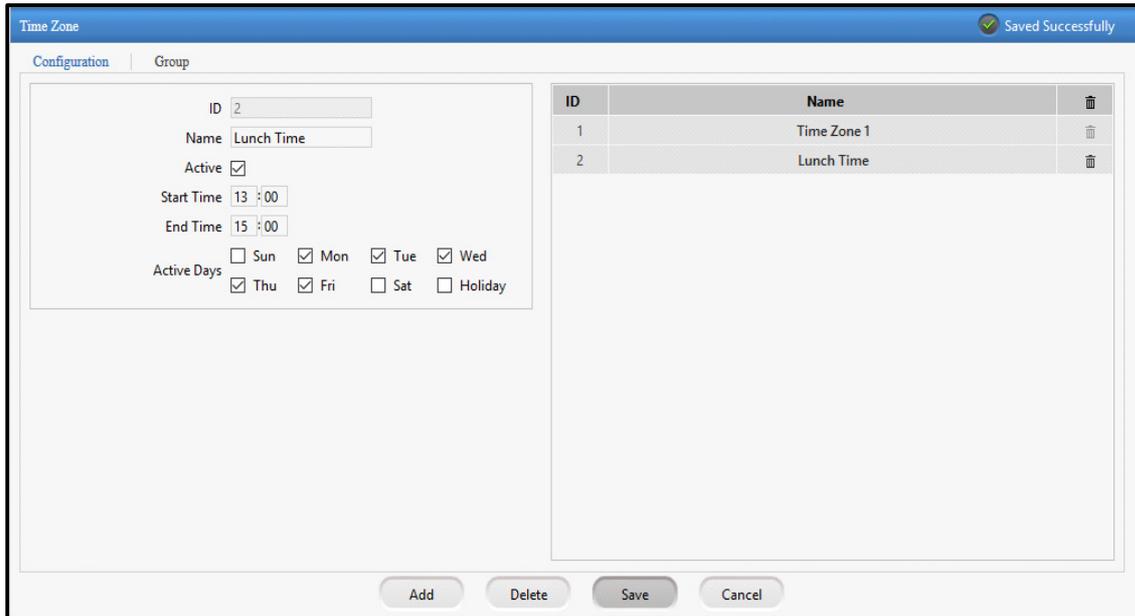
The screenshot shows the 'Time Zone' configuration window with the 'Configuration' tab selected. The 'Group' tab is also visible. The configuration fields are as follows:

- ID: 2
- Name: Lunch Time
- Active:
- Start Time: 13 : 00
- End Time: 15 : 00
- Active Days: Sun Mon Tue Wed Thu Fri Sat Holiday

On the right, there is a table with the following data:

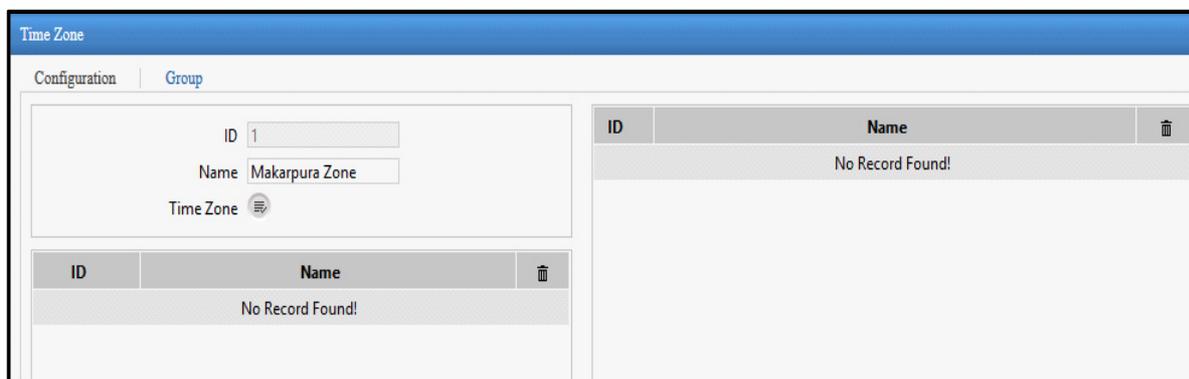
ID	Name	
1	Time Zone 1	

Click on **Save** to save the configured Time Zone. It gets updated in the grid on the right hand side. Also the Time Zone can be deleted by clicking Delete button from the grid.



Group

The Group tab enables you to create time zone groups by clicking **Add** button and configuring the following parameters.



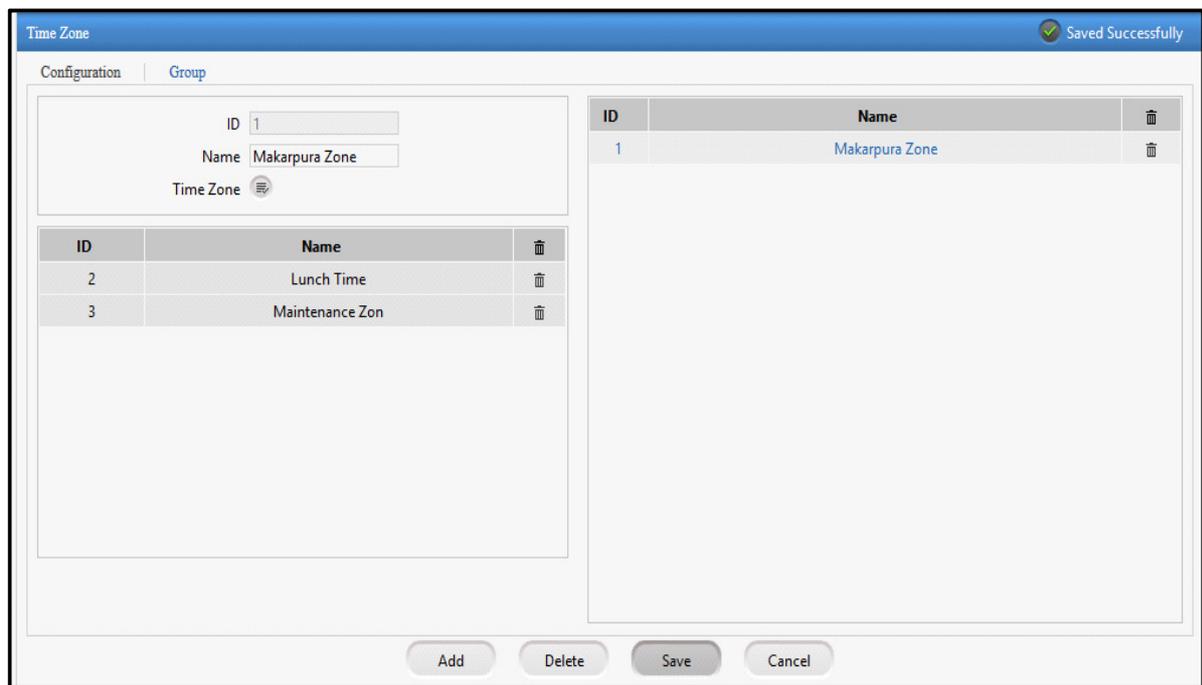
ID: It displays ID of the time zone group.

Name: Enter the name for the time zone group.

Time Zone: Select the time zone using the picklist which is to be included in the group.



Click **Save** to save the time zone group which gets updated in the grid on the right hand side.



After configuring the Time Zone, you can assign to the Schedule Based Access Level override in Users > Access Group.

Access Cluster

The Access Cluster page enables to configure access clusters i.e. zones or group of devices.

In chemical industries; when a user accesses a chemical prone area then he is restricted from going into zones which can harm him or the surroundings. So if the user is accessing one cluster (say chemical area); then he can be restricted to go to second cluster (public area).

ID	Name	Status
1	Cluster-1	Inactive

To add a new cluster click **Add** button.

Name: Specify a name of the access cluster Eg: Cluster A

Active: Select the check-box to enable the cluster.

Cluster Mode: You can select the cluster mode as

- **Allow All Clusters-** Users accessing Cluster A will be allowed to access all other clusters.
- **Allow Selected-** Users accessing Cluster A will be allowed to access only selected clusters. If you select this option, you must configure the Allowed Cluster. Click the pick-list and select the desired clusters to be allowed.
- **Deny All Clusters-** Users accessing Cluster A will be denied access to all other clusters till the restricted duration.

Restricted Duration: Enter the time duration before completion of which; user cannot access another cluster.



First time i.e. after panel is rebooted when user accesses 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.

1. For first cluster, mode selected is **Allow All Clusters** and restricted duration configured is 2hrs and 30 minutes.
2. 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 mins. (Here restricted duration is only for denied clusters)
3. For third cluster, mode selected is **Deny All Clusters** and restricted duration configured is 1 hr.

Access Cluster

ID

Name

Active

Cluster Mode

Restriction Duration

ID	Name	Status
1	Cluster-1	Active

Access Cluster

ID

Name

Active

Cluster Mode

Restriction Duration

Allowed Cluster

ID	Name	Status
1	Cluster-1	Active
2	Cluster-2	Active
3	Cluster-3	Active

ID	Name	
3	Cluster-3	

Access Cluster Saved Success

ID

Name

Active

Cluster Mode

Restriction Duration

ID	Name	Status
1	Cluster-1	Active
2	Cluster-2	Active
3	Cluster-3	Active

Case:1- For first time user is accessing a door of cluster 1.

- Now if user accesses any cluster 1, 2 or 3 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 he will be allowed.
- If user accesses cluster 3 he will be allowed as allowed cluster is cluster3.
- After accessing cluster 3, if user accesses cluster 1 or 2 before 1 hr. i.e. at 3:00 on same day 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 he should be allowed. Note last accessed time should be updated even if door from same cluster is accessed i.e. after accessing door of cluster 3 any other door of cluster 3 is accessed.
- If user accesses cluster 1 or 2 before 1 hr. i.e. before 3 o'clock he will not be allowed. But if user accesses cluster 2 at around 4:00 he will be allowed as restricted hour configured for cluster 3 to deny is 1 hr.



The Access Cluster is enabled for Users from User Configuration> Advanced Access Control2

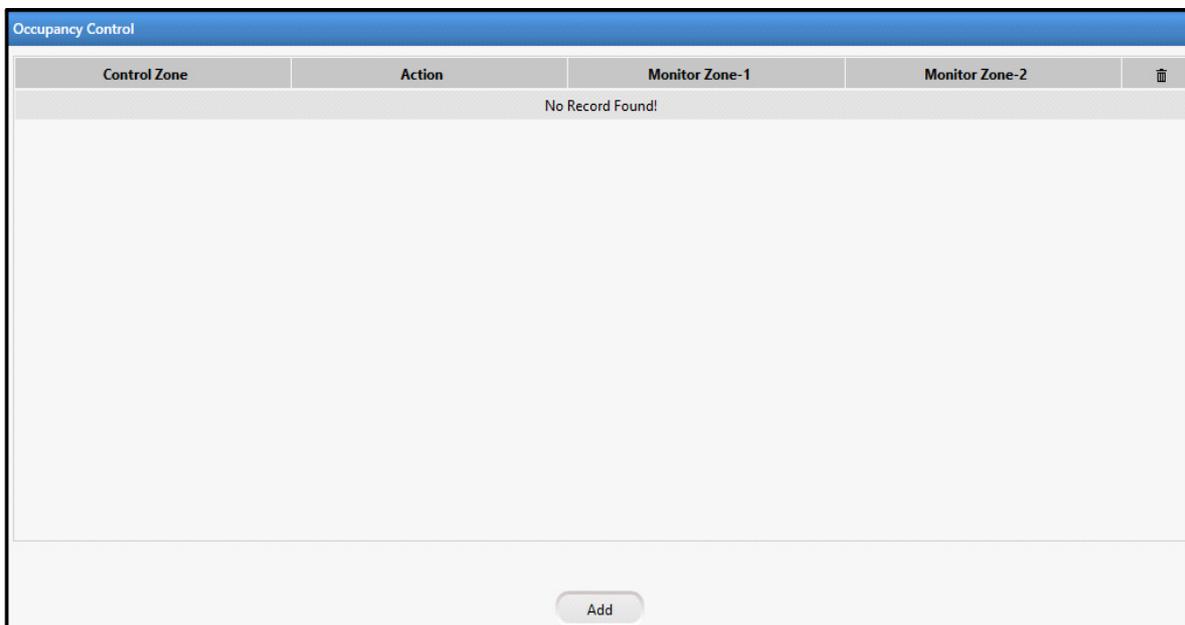
Occupancy Control

Occupancy Control functionality enables the system to monitor and control the number of users permitted within a secured area or controlled zone. This feature can be useful for high security bank vaults, research organizations where single person can't be trusted.

Occupancy rule can be applied on each zone separately or occupancy of one zone (**Monitor zone**) can be monitored to control access into another zone (**Control zone**).

You can add maximum **99** occupancy control rules.

The page will display a list of created rules along with their details. You can click on the rule to edit it or click Delete icon to delete it.



To configure the Occupancy Rule; click **Add** button and configure the following details.

Control Zone: Click the pick-list and select the zone to be made as Control zone where the user access can be controlled based on the selected Action and the condition of monitor zone.

Access Mode: You can select the Access Mode as Entry, Exit or Both based on which Occupancy rule will be checked.

Action: Select the action from the options which is to be executed when there is a violation:

Alarm: Select this option, if you want an alarm to be triggered on violation of the occupancy rule and after the lapse of the Alarm Timer.

- **Alarm Timer:** Configure the **Alarm Timer**. This is the time for which the device will wait, before it declares a violation and on the basis of which the user is allowed to either enter or exit the zone.
- **Restrict:** Select this option, if you do not want the user to enter or exit the zone on violation of the rule.

Monitor Zone-1: Select the desired zone from the pick-list.

- **Avoid Occupancy:** Set the occupancy condition using **Equal To, Greater Than, Less Than** to be avoided for Monitor Zone1. The user limit can vary from 0 to 999.

Monitor Zone-2: Select the monitor zone2 from the picklist.

- **Avoid Occupancy:** Set the occupancy condition using **Equal To, Greater Than, Less Than** to be avoided for Monitor Zone2. The user limit can vary from 0 to 999.

Check Conditions For: Select the option as **Any One Zone** or **Both Zones** to check the **Avoid Occupancy** condition for the respective zone.

Example1:

Let there be 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 - is selected as "Alarm" and Alarm timer is 0 seconds.

Condition - is avoid occupancy equal to 2

When second user comes in monitor zone; he will be allowed access but occupancy will be violated. The occupancy violated Alarm will be triggered when a user tries to access the control zone.

Occupancy Control

Control Zone 1 Zone-1

Access Mode Entry

Action Alarm

Alarm Timer 0 sec (0-999)

Monitor Zone-1 2 Zone-2

Avoid Occupancy Equal To 2 (0-999)

Monitor Zone-2 ID Name

Avoid Occupancy Equal To 0 (0-999)

Check Conditions for Any One Zone

Save Cancel

Example2:

Let there be 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- is selected as "Restrict".

Condition - is avoid occupancy greater than 1

When second user comes in monitor zone; he will be allowed access but occupancy will be violated. When a user tries to access the control zone; he will be restricted access due to violation of occupancy in monitor zone.

Occupancy Control

Control Zone 1 Zone-1

Access Mode Exit

Action Restrict

Alarm Timer 0 sec (0-999)

Monitor Zone-1 2 Zone-2

Avoid Occupancy Greater Than 1 (0-999)

Monitor Zone-2 ID Name

Avoid Occupancy Equal To 0 (0-999)

Check Conditions for Any One Zone

Save Cancel

Example 3:

Let there be 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. For this “Access Control on Exit mode” check-box must be enabled for both the zones from Panel200> Zones> Setup.

Action - is selected as “Restrict”.

Condition - is avoid occupancy 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 occupancy.
- Now when user5 tries to exit from the control zone then access will be denied to him. But on the same time if user8 (VIP user) tries to exit from the control zone then access will be allowed to him.

Example4:

Let there be 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 Access mode from Panel door> Reader section.)

Access mode- is selected as Entry. This is the access mode of user in control zone (Zone-1) for which the Action (Alarm/ Restrict) is to be taken.

Action - is selected as “Restrict”. This will restrict the access to the user in control zone if occupancy is violated in monitor zone.

Condition- is Avoid occupancy equal to 2 in monitor zone-1 (Zone-2)

- When user1 punches on PVR (zone2), he is allowed access.
- When user2 punches on PVR (zone2), he will also be allowed access.

- But when user3 punches on Door V3 in control zone (zone1), he will be restricted access due to violation of occupancy =2 in monitor zone (zone2).
- Now when user4 punches on PVR Door in zone2, he will be restricted access as the maximum occupants limit for zone2 is configured as 2 as shown below and user1 and user2 have already occupied zone2.



The IN- OUT punches are stored in memory of Panel200. Re-booting the panel/panel doors will not reset the occupancy count to zero.

If there are entry punches in a zone so 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.

Example5:

Consider the above example 4 with change in Action as Alarm.

Action - is selected as "Alarm". And Alarm Timer as 2 seconds. Alarm will be triggered after 2 seconds of user access in control zone when the occupancy is violated in monitor zone.

- When user1 and user2 punches on PVR door, they will be access allowed.
- But when user3 punches on Door V3 then he will be access allowed but after 2 seconds alarm will be generated.

Example6:

Let there be 3 zones of Panel200:

- 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. Access mode of all zones is Entry. (Configure Access mode from Panel doors> Reader section.)

Access mode- is selected as Entry. This is the access mode of user in control zone (Zone-1) for which the Action (Alarm/ Restrict) is to be taken.

Action - is selected as "Alarm". And Alarm Timer as 2 seconds. This will raise the alarm after 2 seconds of user access in control zone when the occupancy is violated in monitor zone.

Condition- For Monitor Zone 1 condition is Avoid occupancy equal to 2. For Monitor Zone 2 condition is Avoid occupancy greater than 1.

If **Check Conditions For** is selected as

- **Any One Zone** then occupancy avoidance condition will be checked for any1 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.
- When user1 punches on Door V3-115 (Zone-3), he is allowed access. When user2 punches on Door V3-115 (Zone-3), he will be also be allowed access. But this is violating occupancy >1
- Now when user3 punches on Door V3 (Zone-1) then he will be allowed access but after 2 seconds alarm will be triggered.



Similarly if Action= Restrict; then user3 will be denied on Door V3.

If Check Conditions For = Both Zones, then occupancy in PVR door will also be monitored.

Access Rule

This option allows the administrator to create the 'Conditional Access Rules' for a particular time duration to access the doors. These rules can be assigned to the user from user module.

Click on the option and configure Access Rule as shown below:

The screenshot shows the 'Access Rule' configuration window. It contains the following elements:

- ID:** A text input field.
- Name:** A text input field containing 'User Rule'.
- Active:** A checked checkbox.
- Start Time:** A time picker set to 10:00.
- End Time:** A time picker set to 12:00.
- Active Days:** Checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. Mon, Tue, Wed, Thu, Fri, and Sat are checked.
- Assign Door:** A picklist button.
- Tables:** Two tables with headers 'ID' and 'Name' and 'ID' and 'Door Name'. Both tables display 'No Record Found!'.
- Add:** A button at the bottom center.

Click on the **Add** button to add the new rule.



Maximum 999 Access Rules can be created.

ID: This is generated automatically.

Name: Specify a descriptive name for the Access Rule.

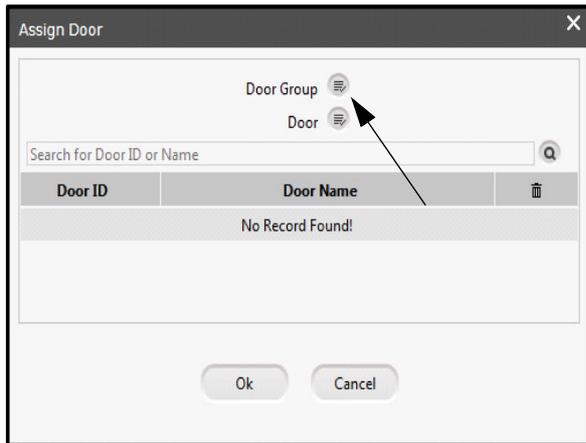
Active: Select the check-box to enable the rule.

Start-End Time: Specify the time duration for the rule by defining the Start and End time in 24hrs clock format. The rule will be enabled at the Start time and Disabled by the end time.

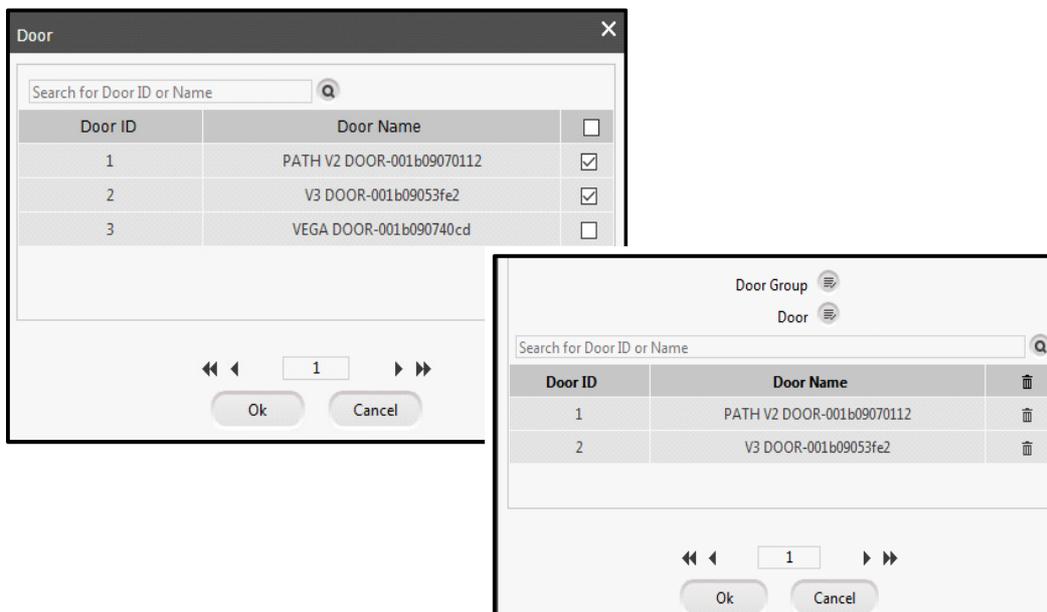
Active Days: Select the respective check-boxes of the days for which the rule is to be configured.

Assign Door: Click on the picklist button to select the Door/Door group.

The required **Doors/Door Group** can be assigned to the rule from the respective picklist button as shown below.



Select the check-box of the desired Door and/or Door Group you wish add.



Click on **Ok** button to save the door configuration. The assigned door/door group will be displayed in the grid.

Click on **Save** button to save the Access Rule configuration. The configured rules will be displayed on the right side panel.

Access Rule

ID

Name

Active

Start Time :

End Time :

Active Days Sun Mon Tue Wed
 Thu Fri Sat

Assign Door

ID	Door Name	
1	PATH V2 DOOR-001b09070112	
2	V3 DOOR-001b09053fe2	
3	VEGA DOOR-001b090740cd	

« « 1 » »

ID	Name	
1	User Rule	
2	Manager Rule	

« « 1 » »

Click on **Delete** button to Delete the configured rule.

Shifts and Schedules

Shift are when the day is divided into set periods of time during which different groups of workers can perform their duties.

Schedule refers to a plan that gives the list of events or tasks and the time at which each needs to be done.

Shifts and Schedules need to be combined for optimum output.

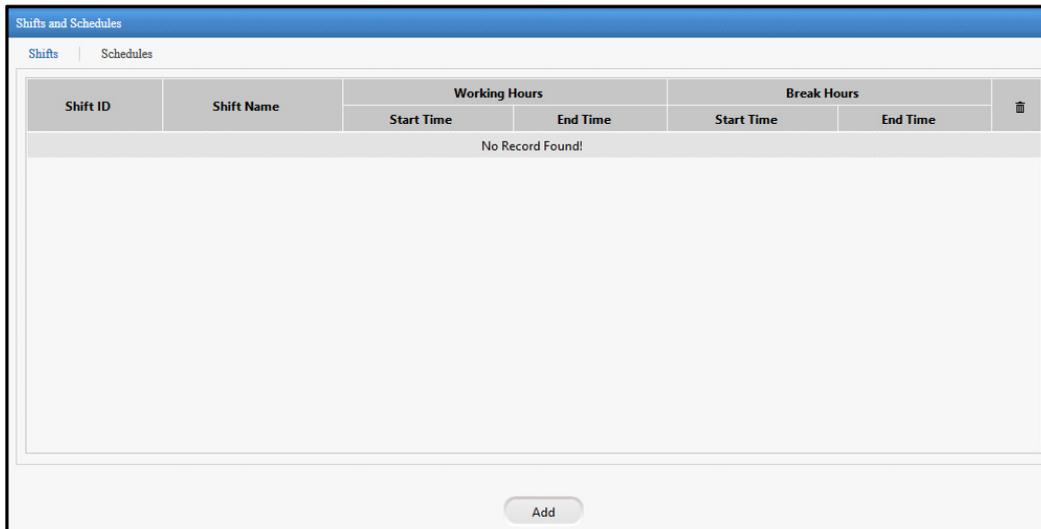
Shift Schedules define the events and the time when the same need to be executed by a defined group of members.

It defines the details like timing, no. of days, shift rotation, rotation count etc for each shift.

It enables the user to group multiple shifts which can then be assigned to the employees. With this you can assign different working hours and Off days for each user by defining different schedules.

Shifts and Schedules allow access to work place according to the user shift schedules only.

Shifts



To configure the Shift, click the Add button. Maximum 1402 Shifts can be added.

Shift Code: Specify a descriptive Shift code. For eg. GS for General Shift.

Name: Specify the user friendly name of the shift.

Shift Type: Select the type of shift from the dropdown list.

- **Normal-** This is a normal shift with one weekoff within a week.
- **Field Break-** This is a shift where a break of around 20 days can be given after a working period of 2 months.
- **Rest Day-** This is a like a normal shift with one weekoff given for rest after 10-12 working days.

Working Hour Details

Start Time: Specify the Start Time of the shift in hh:mm format.

End Time: Specify the End Time of the shift in hh:mm format. The Shift duration or the total working hours of the shift is the difference of end time and start time.

Break Hour Details

Start Time: Specify the Start Time of the break in hh:mm format.

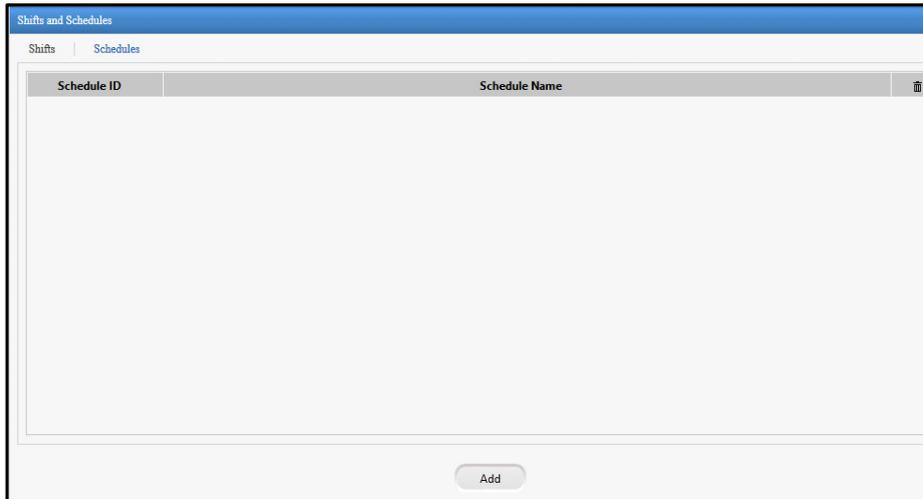
End Time: Specify the End Time of the break in hh:mm format.

Click on **Save** to save the configured Shift. Similarly you can configure other shifts. You can click on **View list** button to view the list of configured shifts as shown below.

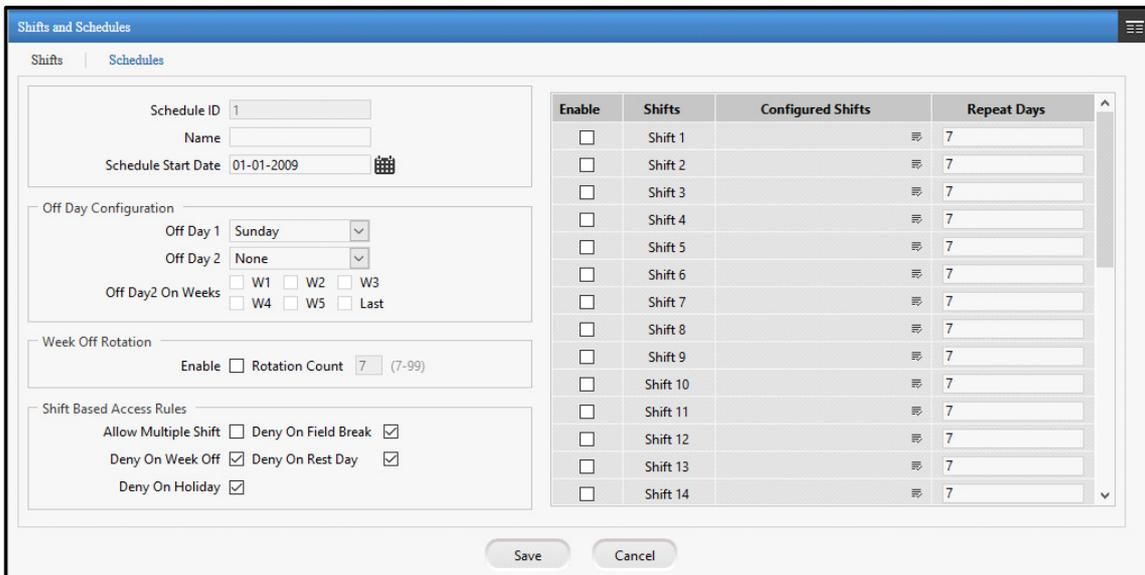
Shift ID	Shift Name	Working Hours		Break Hours		🗑️
		Start Time	End Time	Start Time	End Time	
GS	General Shift	09:00	18:30	13:00	14:00	🗑️

Schedules

Once the shifts are configured, you can add the shifts to a schedule.



To create a new Schedule click on **Add** button.



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

Schedule ID: This is auto-generated by the system.

Name: Specify the user friendly name of the schedule.

Schedule Start Date: Select the Start Date from the calendar from which you want to apply the Schedule.

Off Day Configuration

For configuring second week off, select the Off Day 2 from the drop down list(eg: Saturday). If only one week off is to be given, then select "None" for Off Day2.

Off Day 1: Select the Off Day 1 from the drop down list of Weekdays (eg: Sunday).

Off Day 2: For configuring second week off, select the Off Day 2 from the drop down list(eg: Saturday). If only one week off is to be given, then select "None" for Off Day2.

Off Day2 on Weeks: You can select the week for which Off Day2 is to be assigned. For eg: Saturday is assigned as week off on 2nd and 4th saturday.

Week Off Rotation

Enable: To select the check-box to enable.

Rotation Count: Specify the Rotation Count for rotating single or both week offs as configured. However, Rotation Count cannot be less than 7.

For eg. if Rotation Count is 15 Then the off day on sunday will rotate to monday after the count of 15 days. Similarly it will continue to rotate further to Tuesday and so on. If both the off days are assigned, then both will rotate similarly.

Shift Based Access Rule

Allow Multiple Shift: To allow the User to work in multiple or any of the shifts from the schedule. select the Allow Multiple Shift check-box.

Deny on Field Break: To deny access on field break days select the Deny on Field Break checkbox.

Deny on Week Off: To deny access on Week Off days select the Deny on Week Off checkbox.

Deny on Rest Day: To deny access on Rest Day select the Deny on Rest Day checkbox.

Deny on Holiday: To deny access on Holiday select the Deny on Holiday checkbox.

To add the shifts to the schedule select the respective Enable check-box. To configure the Shift, click the Select Shifts pick-list.

Repeat Days: Specify the number of days for which the shift should be repeated in the schedule.

Enable	Shifts	Configured Shifts	Repeat Days
<input checked="" type="checkbox"/>	Shift 1	GS	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

Click on **Save** to save the configured Schedule. Click on **View List** button to view the list of configured Schedules as shown below.

Schedule ID	Schedule Name	
1	RnD Schedule	

1

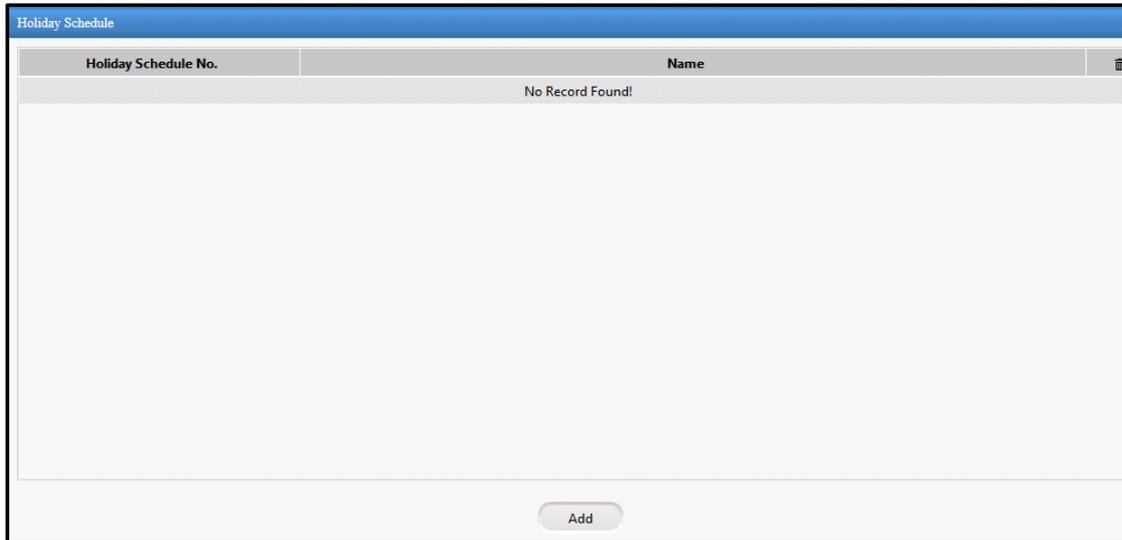
Add



The 1st schedule will get 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.

Holiday Schedule

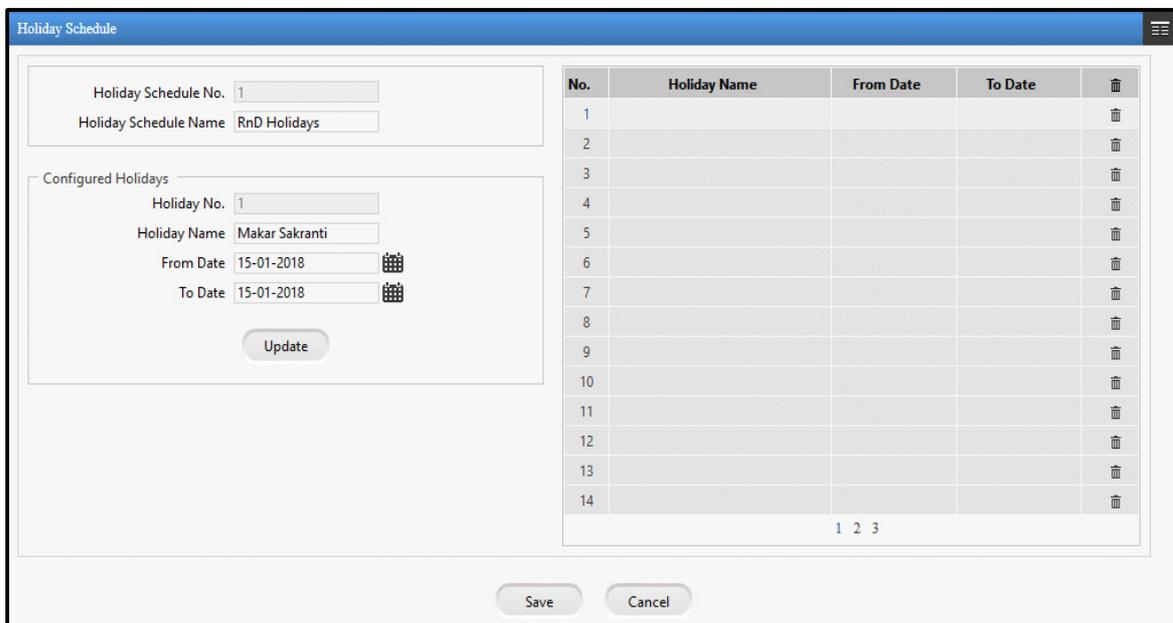
Holiday Schedule is a list of non-working days in a calendar year which are user defined. The user can define up to 32 holidays in a schedule.



The Holiday Schedule can be configured by clicking **Add** button.

Holiday Schedule No.: This is auto-generated by the system.

Holiday Schedule Name: Specify the user friendly name for the Holiday Schedule.



Configured Holidays

Holiday No: To add the holidays to the list select the number from the right grid.

Holiday Name: Specify the name of the holiday.

From Date: Select the Starting date of the holiday from the calendar.

To Date: Specify the Ending date of the holiday from the calendar.

Click on **Update** to save the configured holidays to the grid. Similarly you can add upto 32 holidays for the schedule.

The screenshot shows the 'Holiday Schedule' form. On the left, there are input fields for 'Holiday Schedule No.' (value: 1) and 'Holiday Schedule Name' (value: RnD Holidays). Below these is a section for 'Configured Holidays' with fields for 'Holiday No.', 'Holiday Name', 'From Date', and 'To Date', each with a calendar icon. An 'Update' button is at the bottom of this section. On the right, a table displays the configured holidays:

No.	Holiday Name	From Date	To Date	
1	Makar Sakranti	15-01-2018	15-01-2018	🗑️
2				🗑️
3				🗑️
4				🗑️
5				🗑️
6				🗑️
7				🗑️
8				🗑️
9				🗑️

Click on **Save** to save the Holiday Schedule.

The screenshot shows the 'Holiday Schedule' form after saving. The 'Configured Holidays' section now has an 'Update' button. The table on the right now contains three entries:

No.	Holiday Name	From Date	To Date	
1	Makar Sakranti	15-01-2018	15-01-2018	🗑️
2	Republic Day	26-01-2018	26-01-2018	🗑️
3	Holi-Dhuleti	04-01-2018	05-01-2018	🗑️
4				🗑️
5				🗑️
6				🗑️
7				🗑️
8				🗑️
9				🗑️
10				🗑️
11				🗑️
12				🗑️
13				🗑️
14				🗑️

At the bottom of the form, there is a navigation bar with buttons: Add, Delete, Save, and Cancel.

Click on **View List** button to view the list of holidays.

The screenshot shows the 'View List' view. It displays a table with the following data:

Holiday Schedule No.	Name	
1	RnD Holidays	🗑️

An 'Add' button is located at the bottom center of the view.

 The holiday schedule can be assigned to the user from User Configuration > Advance Access Control > Shift Based Access.

System Maintenance

System Maintenance enables you to take Backup, Upgrade the Firmware, Restore Configuration and manage the System settings.

The firmware of Panel200 can be upgraded manually or automatically. The Event backup and configuration backup can be taken manually or you can schedule the backup.

Firmware Upgrade

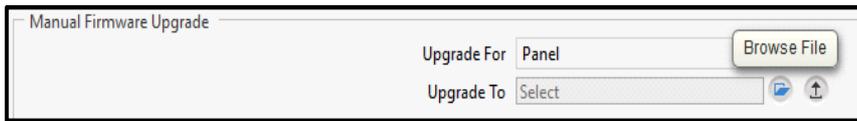
Manual Firmware Upgrade

Upgrade For: Select the device for which the firmware needs to be upgraded from the drop-down list. The firmware of PVR Door, ARGO Door, V3 Door, V4 Door, ARC DC200, PATH V2, ARGO FACE Door and Vega Door(V2)-bluetooth supported Vega will be stored in the memory card of Panel200. The firmware of other panel doors will be stored in the flash of Panel200.



To access Panel's firmware file, contact our Technical Support Team. Once the file is obtained, follow the same steps as mentioned below.

Upgrade To: Click **Browse File** to browse the file and select the firmware. Click on **Upgrade** button to upgrade the firmware.



Manual Firmware Upgrade

Upgrade For: Panel

Upgrade To: Select

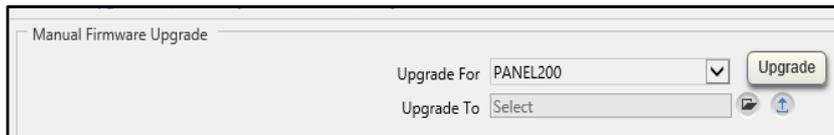
Browse File



Manual Firmware Upgrade

Upgrade For: PANEL200

Upgrade To: COSEC_PANEL200_V01R49.zip

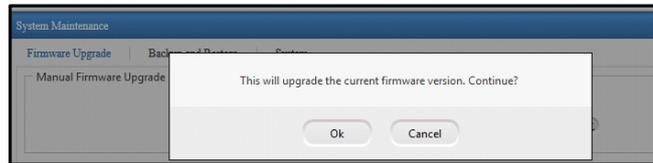


Manual Firmware Upgrade

Upgrade For: PANEL200

Upgrade To: Select

Upgrade

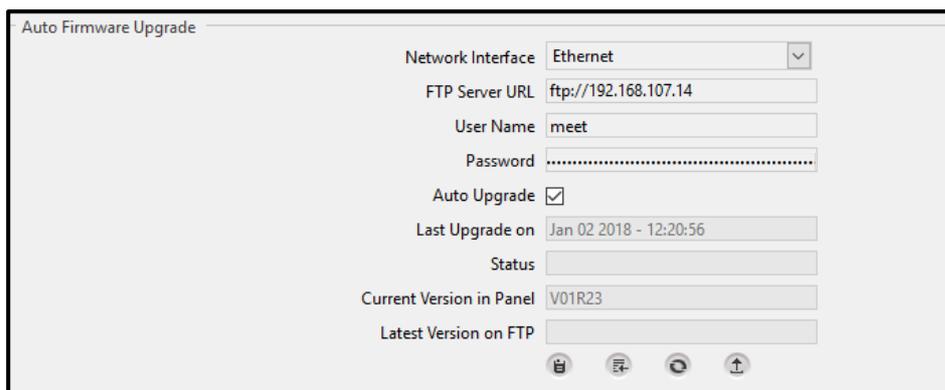


Click **OK** to upgrade the firmware. The panel will be upgraded with the new firmware and will reboot.

Auto Firmware Upgrade

Auto upgrade feature enables to upgrade the firmware of devices located at different places automatically through FTP server in COSEC VYOM.

If there are any mismatches in the present firmware stored in device and firmware on the FTP, latest firmware can be upgraded in device by logging through the FTP Server.



Auto Firmware Upgrade

Network Interface: Ethernet

FTP Server URL: ftp://192.168.107.14

User Name: meet

Password:

Auto Upgrade:

Last Upgrade on: Jan 02 2018 - 12:20:56

Status:

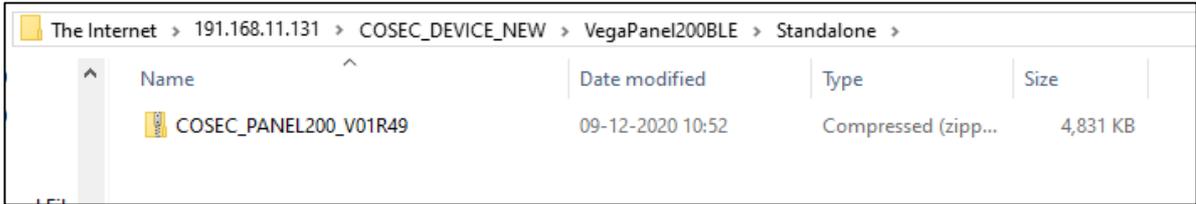
Current Version in Panel: V01R23

Latest Version on FTP:

Network Interface: Select the desired option - Ethernet, Wifi or Mobile Broadband through which the communication needs to be established.

FTP Server URL: Enter the URL as the combined path with FTP Server Address, Port from where you want to upgrade the firmware version.

For example, URL: ftp://192.168.107.15.



Specify the **User Name** and **Password** to login into FTP server. By default Matrix FTP details will be displayed.

Auto Upgrade: Select the Auto Upgrade checkbox to automatically upgrade the firmware of Panel200. If Auto Upgrade is enabled, Device will check the latest version of firmware available on FTP at 00:00 AM every day. It will check whether there is mismatch in the current version stored in device and available at FTP.

Last Upgrade on: It will display the last Date and Time when the device firmware was updated.

Current Version in Panel: It will show the current firmware version stored in the memory of Panel200.

Click **Save** button to save the configured details of FTP server.

Click **Check Version** button to check Current Firmware version in panel and latest firmware version available on the FTP.

Status: It will display the status whether device is connected with FTP server or not.

Latest Version on FTP: It will display the latest firmware version available on the FTP.

Click the **Force Upgrade** button to upgrade the Panel200 with the firmware available at defined FTP server. The Force upgrade can be used when you do not want to wait till 00:00 hrs and upgrade the firmware instantly.

Then click **OK** to upgrade. Then wait for the Panel200 to reboot. After login, you can check the Current version with which the Panel is upgraded.

Click **Default** button to default the FTP Server URL, Username, Password, Status and Latest Version on FTP.

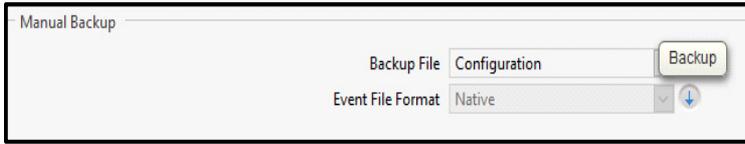
Backup and Restore



SD card must be present in the Panel. Without SD Card Manual or Schedule Backup will not take place.

Manual Backup

Backup File: The backup of the **Event** and **Configuration** can be stored at desired location.



Manual Backup

Backup File: Configuration [Backup]

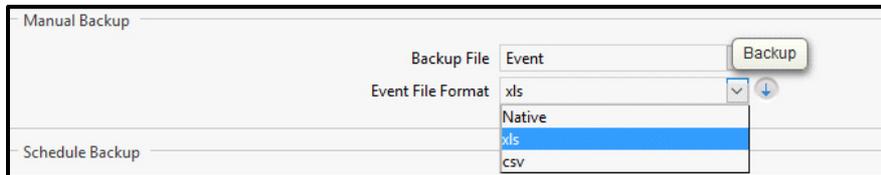
Event File Format: Native [v] [↓]

- The Configuration backup will be generated in a zip file which includes configuration of Panel200, finger templates and palm templates.



Face Templates will not be included in the Backup file.

- The Event backup can be taken in Native, XLS or CSV file format. In Native format, a zip file containing Events folder will be created. If Panel MAC address is 001b0904ac65 then backup file created will be "0904ac65_02102017.zip"



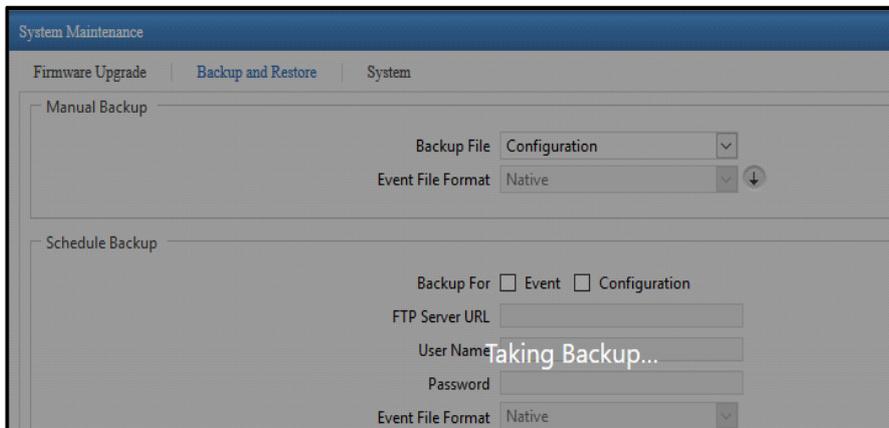
Manual Backup

Backup File: Event [Backup]

Event File Format: xls [v] [↓]

Schedule Backup

- Native
- xls**
- csv



System Maintenance

Firmware Upgrade | Backup and Restore | System

Manual Backup

Backup File: Configuration [v]

Event File Format: Native [v] [↓]

Schedule Backup

Backup For Event Configuration

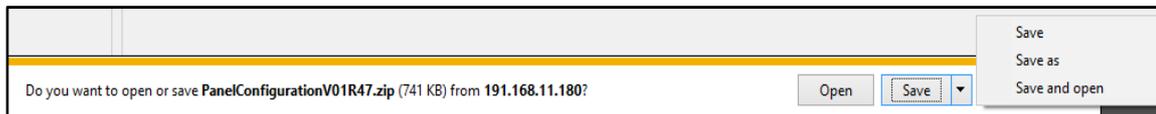
FTP Server URL: []

User Name: []

Password: []

Event File Format: Native [v]

Taking Backup...



Do you want to open or save PanelConfigurationV01R47.zip (741 KB) from 191.168.11.180?

Open [Save] Save and open

Save the file into your desired location of your computer.

Schedule Backup

The screenshot shows the 'Schedule Backup' configuration window. It includes the following fields and options:

- Backup For:** Two checked checkboxes for 'Event' and 'Configuration'.
- FTP Server URL:** A text box containing '191.168.11.136'.
- User Name:** A text box containing 'paresh.hirpara'.
- Password:** A text box with masked characters (dots).
- Event File Format:** A dropdown menu set to 'xls'.
- Monthly Backup On:** A calendar grid with the date '1' selected.
- Schedule Time:** A time picker set to '09 : 00'.

At the bottom of the window are four icons: a save icon, a refresh icon, a back icon, and a forward icon.

Backup For: Select the **Event** and/or **Configuration** checkbox for which backup is to be scheduled.

FTP Server URL: Enter the URL as the FTP Server IP Address, where the backup is to be taken.

Specify the **User Name** and **Password** of the configured FTP server.

Event File Format: Select the file format as **Native**, **XLS** or **CSV** in which backup is to be scheduled.

Monthly Backup On: Select the date in the month on which backup is to be scheduled.

Schedule Time: Enter the time in hh:mm format at which backup will be taken.

Then click **Save** to save the settings.



If the Configuration size is greater than 250 MB; then manual backup or schedule backup might get failed.

Restore

Restore All configurations except: If Network Settings and Users are not required to be restored then select the respective checkbox. The files can be browsed and restored by clicking Restore button. The file can be restored in Native file format only.

The screenshot shows the 'Restore' configuration window. It includes the following fields and options:

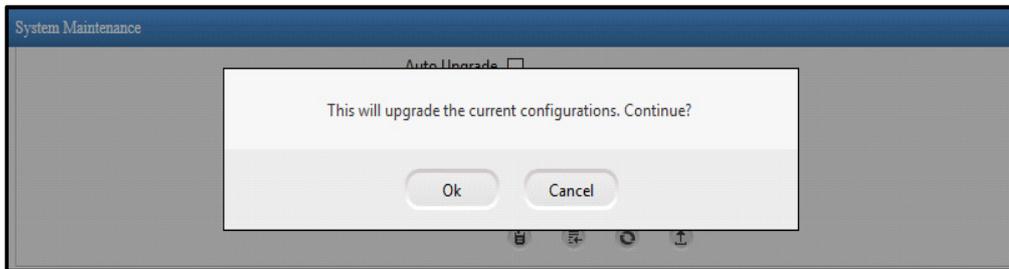
- Restore all configurations except:** Two checked checkboxes for 'Network Settings' and 'Users'.
- Restore File:** A text box containing 'Select'.

A 'Browse File' button is located to the right of the 'Restore File' text box.

The screenshot shows the 'Restore' configuration window. It includes the following fields and options:

- Restore all configurations except:** Two checked checkboxes for 'Network Settings' and 'Users'.
- Restore File:** A text box containing 'PanelConfigurationV01R47.zip'.

A 'Restore' button is located to the right of the 'Restore File' text box.



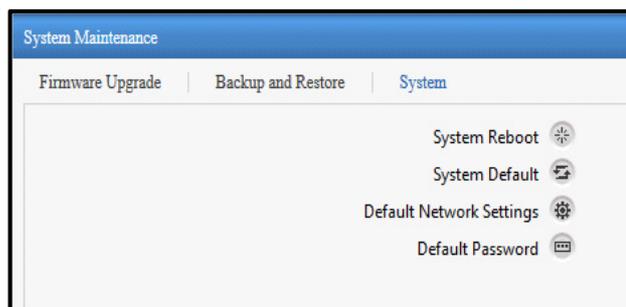
Click on **OK** to update the configuration. Then wait for the panel to reboot.



If the Configuration size of the selected file is greater than 250 MB; then Restore of file may be failed.

If backup of Panel that supports Face Recognition feature is restored in older versions (Panel that does not support this feature), the configuration will not be restored. However, if backup of older versions is restored in Panel that supports Face Recognition feature, all the configuration will be restored and all new parameters will be set to the default values.

System



System Reboot: Click on the respective button to reboot the system.

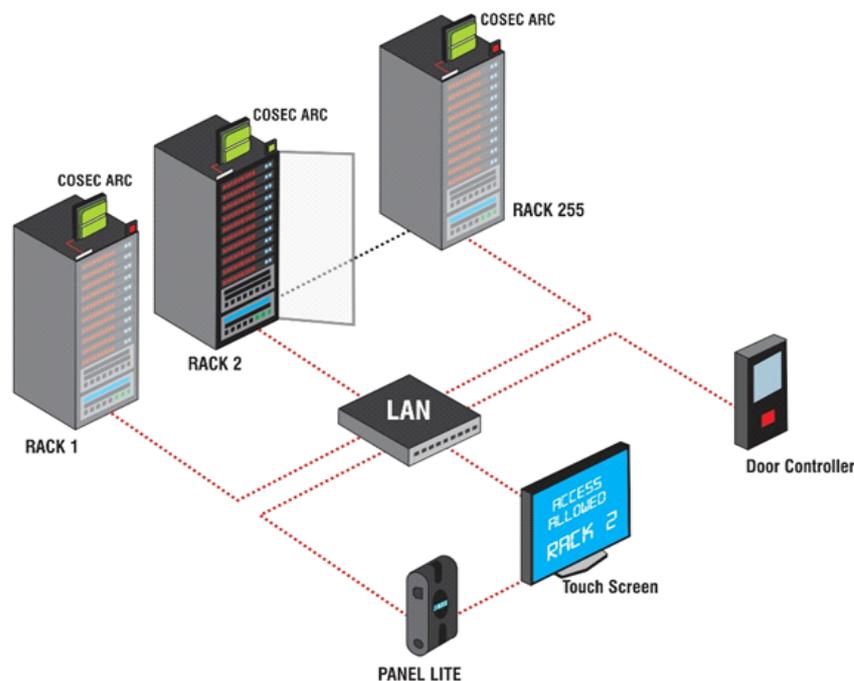
System Default: Click on the respective button to set the system to default settings.

Default Network Settings: Click on the respective button to set the network settings to default.

Default Password: Click on the respective button 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](#)".



To configure Multi-Level Access,

- Click **Multi-Level Access**. The Multi-Level Access page appears.

Multi-Level Access

Monitor Authentication Password

Authentication Device Door Id Door name

Organization Logo .jpg,.png,.bmp files Max 250kb

Organization Name 40 Char

Message 60 chars (eg. Tag Line)

Page Time-Out Duration 20 sec (3-60)

Group Label RACK

Door Unlock Timer 300 sec (1-999)

Save Cancel

The Multi-Level Access page consists of the following tabs.

- “Configuration”
- “Assignment”

Configuration

This tab enables you to configure Multi-Level Access settings.

To configure Multi-Level Access settings,

- Click **Multi-Level Access**. The **Configuration** tab appears by default.

Multi-Level Access

Monitor Authentication Password

Authentication Device Door Id Door name

Organization Logo .jpg,.png,.bmp files Max 250kb

Organization Name 40 Char

Message 60 chars (eg. Tag Line)

Page Time-Out Duration 20 sec (3-60)

Group Label RACK

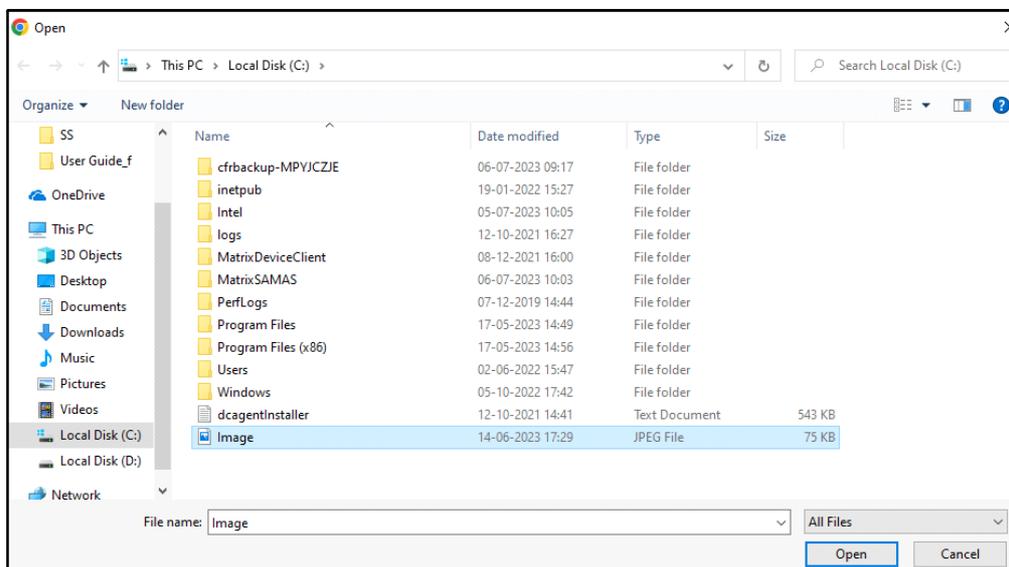
Door Unlock Timer 300 sec (1-999)

Save Cancel

Configure the following parameters:

- **Multi-Level Access:** Select this checkbox to enable the configuration of Multi-Level Access.

- **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 device 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 picklist and select the desired door through which user authentication will 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.

Multi-Level Access Configuration

Multi-Level Access

Monitor Authentication: Password

Authentication Device: 19

Organization Logo: MATRIX

Organization Name: Matrix

Message: 60 chars (eg. Tag Line)

Page Time-Out Duration: 30 sec(3-60)

Group Label: RACK

Door Unlock Timer: 5 sec(1-999)

Save Cancel

- The image preview appears in the box once the image is uploaded.

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

- **Organization Name:** Specify the name of the organization.
 - **Message:** Specify the desired message.
 - **Page Time-Out Duration:** Specify the time in seconds after which the MLAT Access Control page will close if idle.
 - **Group Label:** Specify the desired name for the group of doors. The default name is RACK.
 - **Door Unlock Timer:** Specify the time in seconds after which the door gets locked automatically. Valid range is 1 to 999.
- Click **Save** to save the configuration or click **Cancel** to discard.

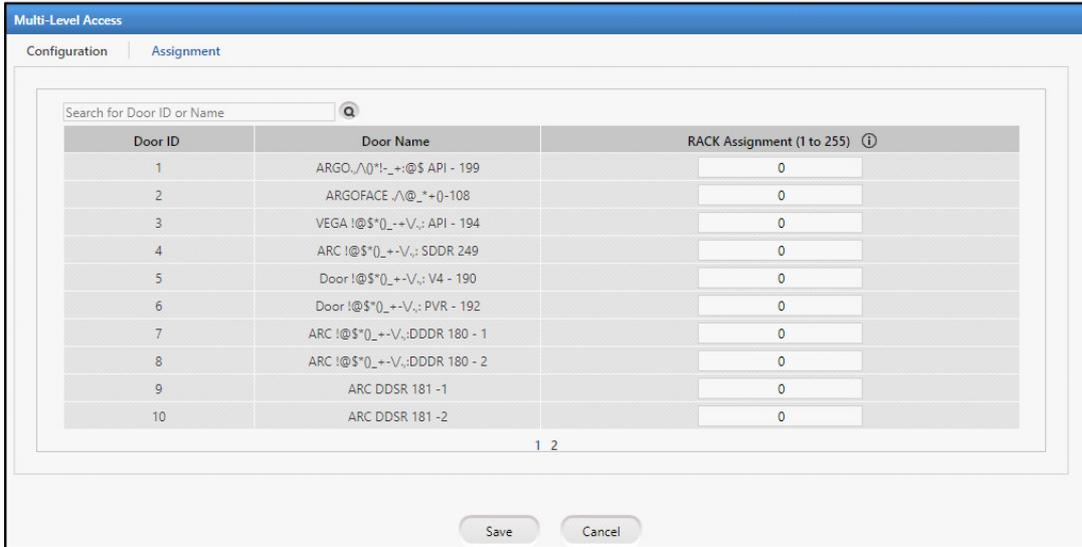
Assignment

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.

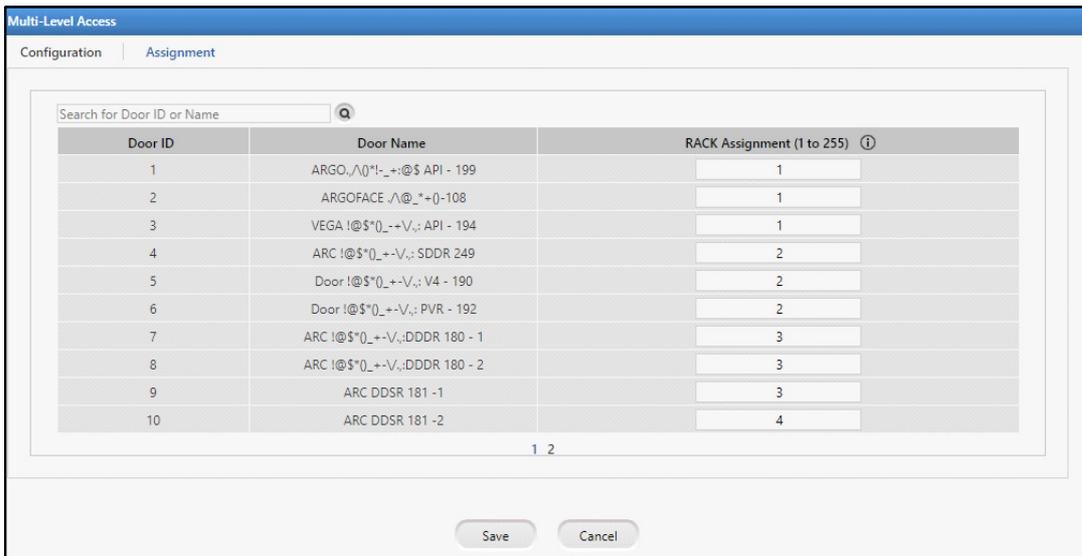
The Assignment page enables you to assign racks to the doors.

To assign racks,

- Click **Multi-Level Access > Assignment**.



- All the doors appear in a list. Enter the desired rack number in RACK Assignment against each door. The maximum Rack Assignments supported are 255.



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

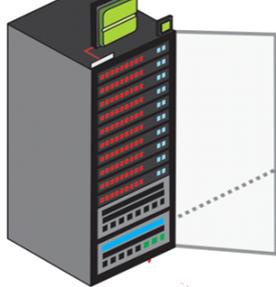
Data Centre Authentication



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 Panel 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 Panel 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 device. 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 authentication device 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 authentication device.

- Make sure you assign the same Access Zone to the users and the authentication device. 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 assigned to the users, then the same will be applicable while accessing MLAT Access Control and MLAT Monitor. For details, refer to “[Access Policies & Access Schedule](#)”.

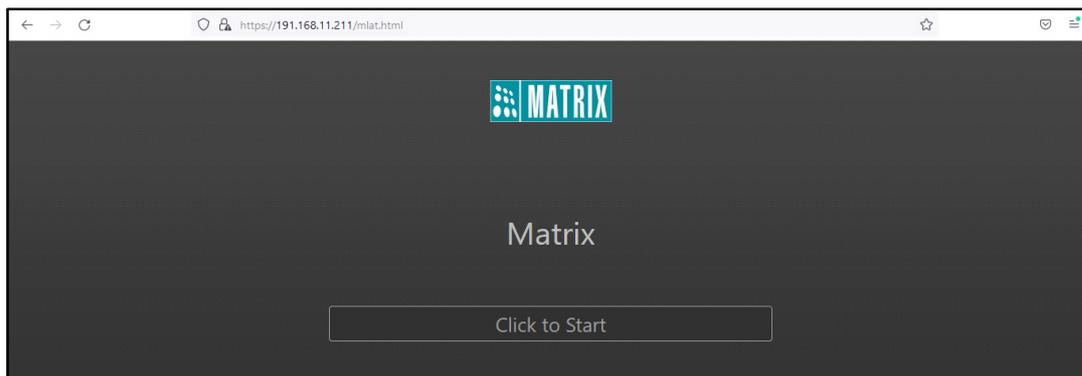
If the Access Policies are applied on the assigned Zone, then the same will be applicable while accessing MLAT Access Control and MLAT Monitor. For details, refer to “[Zone Configuration](#)”.

Make sure the PC from which you wish to access the MLAT Access Control/Monitor is close to the authentication device.

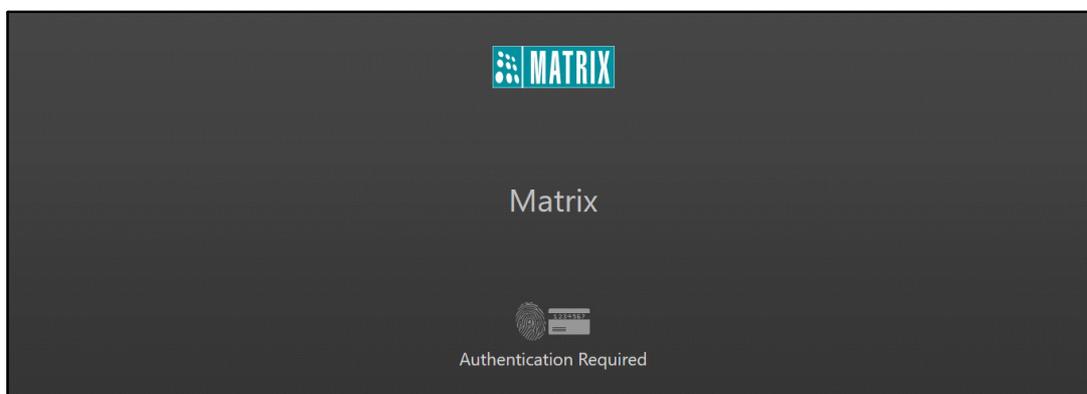
Accessing MLAT Access Control

To access MLAT Access Control,

- Enter Panel IP/mlat.html, for example 192.168.103.26/mlat.html in your web browser. The MLAT Access Control page appears.

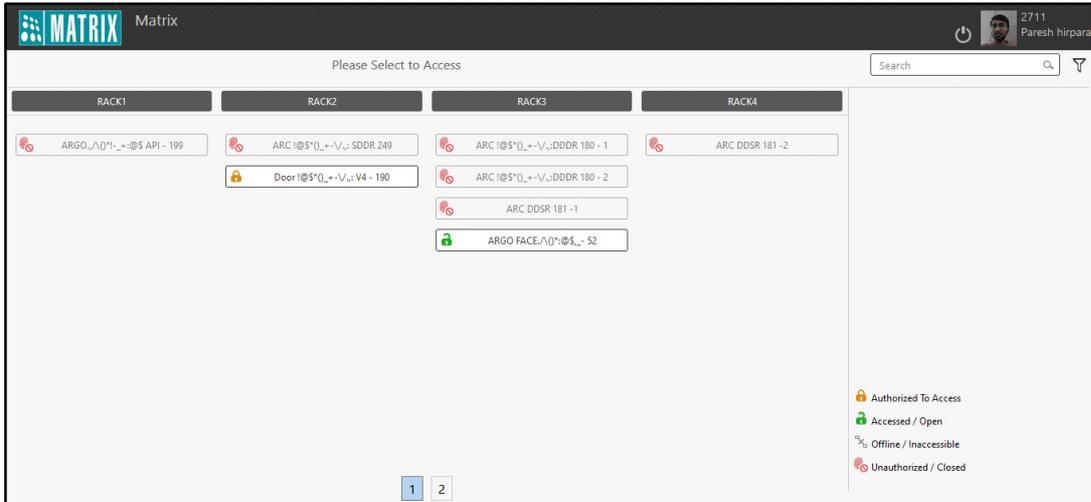


- Click on **Click to Start**. Now you need to show/enter your credentials on the configured authentication device to login.



The authentication device’s display screen is not accessible while accessing the MLAT Access Control page.

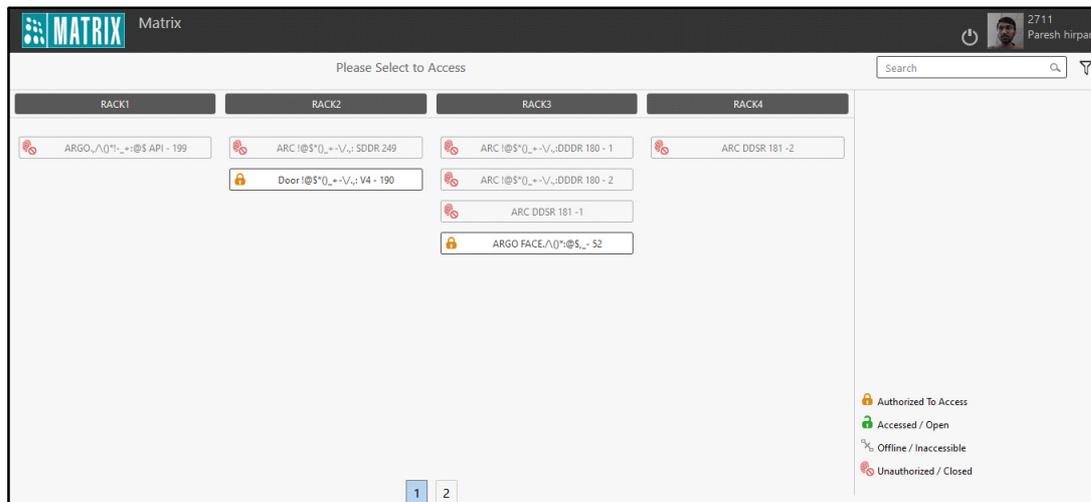
- All the doors assigned to various racks appear here along with their status. All the doors that are not assigned to your Access Route appear disabled.



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.



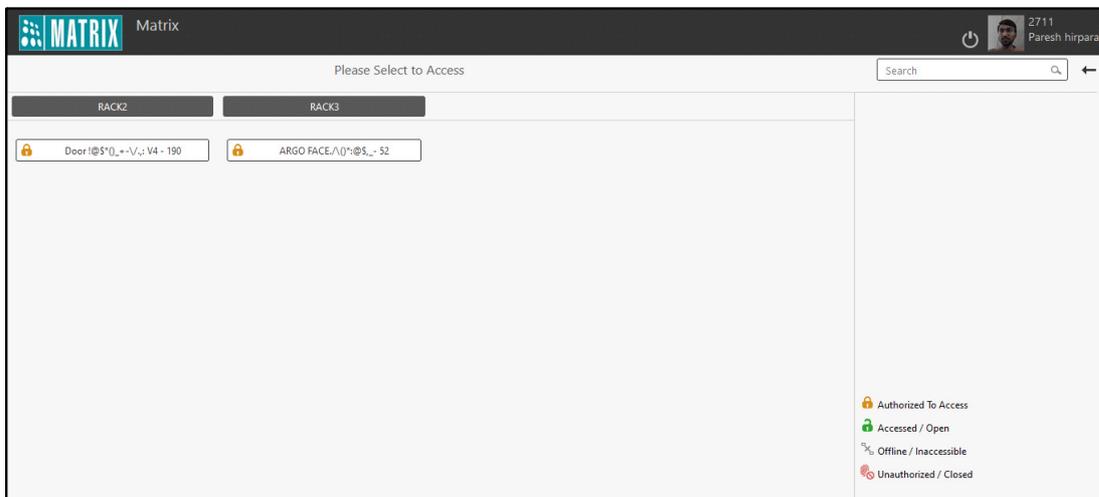
- The door status changes to **Open**. The details of this door appear on the right hand side of the page.



- 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.

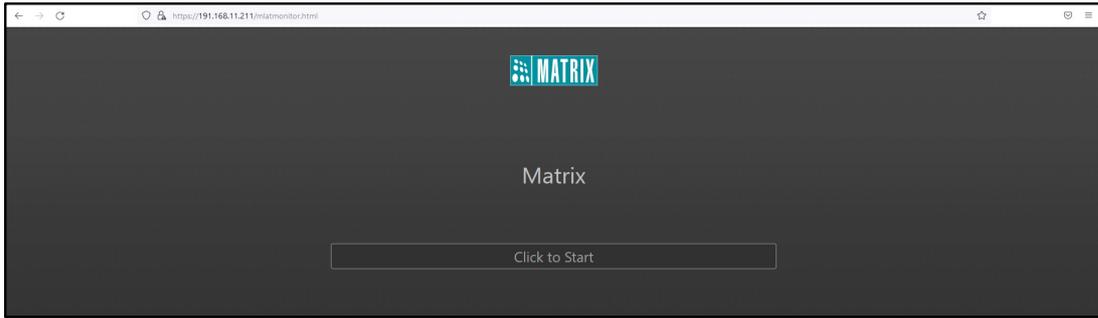


- Click **Filter**  again to view all the doors.

Accessing MLAT Monitor

To access MLAT Monitor,

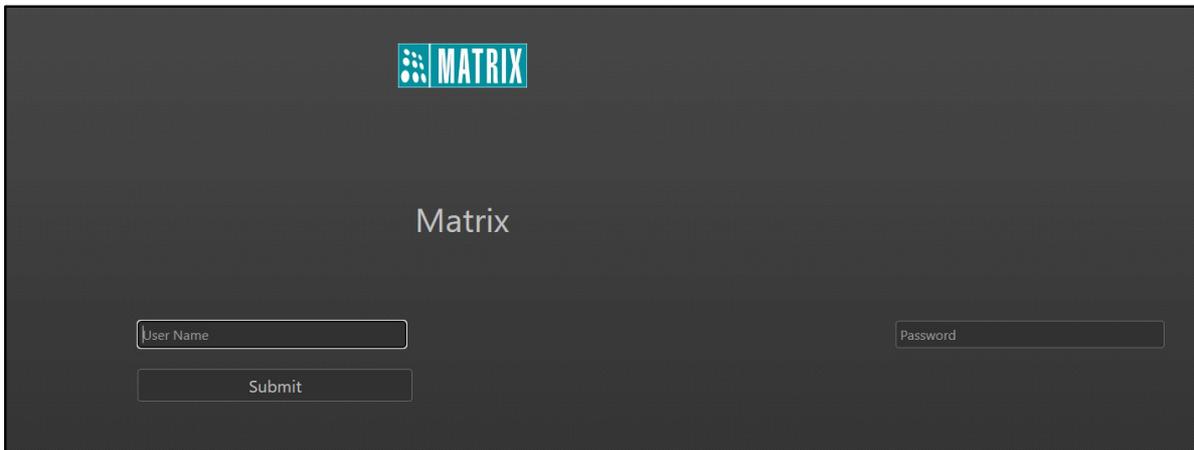
- Enter Panel IP/mlatmonitor.html, for example 192.168.103.26/mlatmonitor.html in your web browser. The MLAT Monitor page appears.



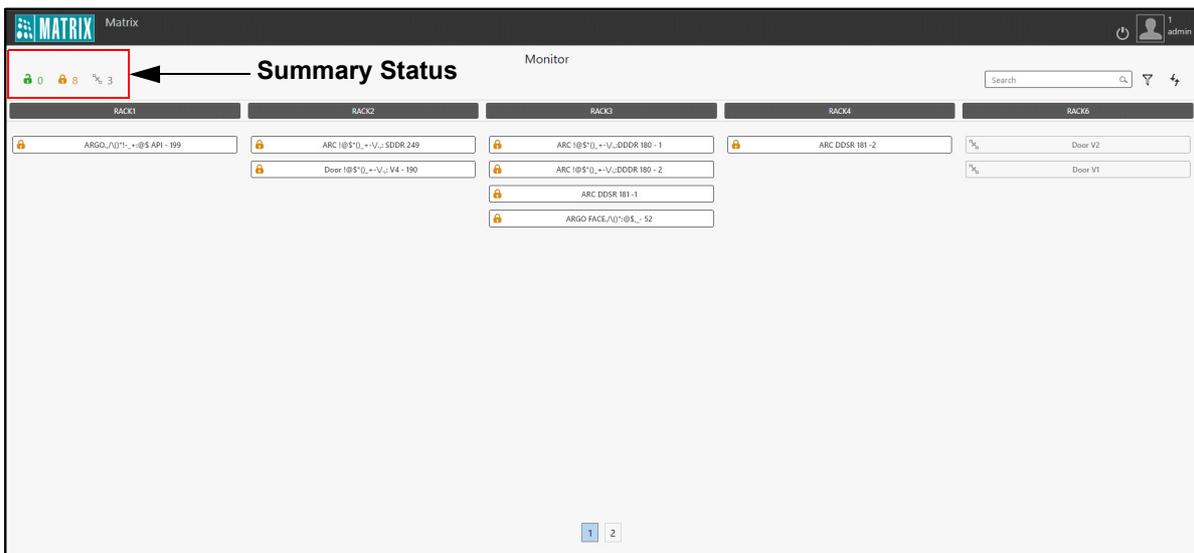
- Click on **Click to Start**.

If the **Monitor Authentication** is configured as User Credential, show/enter the credentials on the configured authentication device to login.

If the **Monitor Authentication** is configured as Password, enter the username and password used to access the Panel 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.

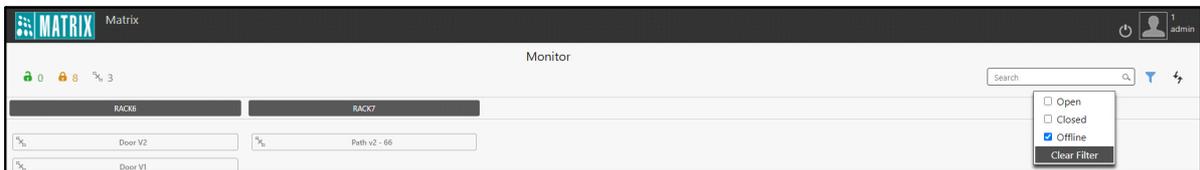
- **Open:** 
- **Closed:** 
- **Offline:** 

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.

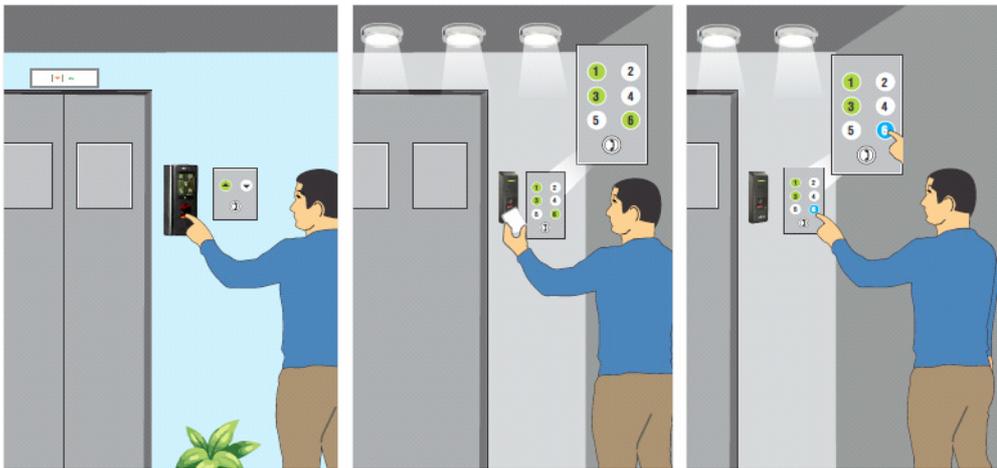


- Select the checkboxes for the Status Type— Open, Closed and Offline as per which you wish to filter the doors. Click **Clear Filter** to clear the filter.



- The doors with the selected status appear as per the assigned racks.
- **Refresh:** Click **Refresh**  to refresh the door status for all the doors.

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.



The Elevator Access Control and their features are available only when the Panel is in Standalone Mode. (Configuration > Basic Profile > Panel Mode)

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 pick-list. Say user Dinesh is linked to RnD Elevators.

When the user Dinesh comes in the Elevator1, then he has to punch on the authentication device 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.

Elevator Configuration

The Elevator Configuration page enables to configure elevators in the standalone Panel200 whose access can be given to authorized users only. You can configure maximum **64** elevators in one panel.



This feature is applicable to PVR Door, Door V3, Door V4, Wireless, Vega, ARC IO 800, ARGO Door, ARGO FACE Door, ARC DC 100 and ARC DC 200 only.

Elevator ID	Elevator Name	Door ID	Door Name	Floors	
No Record Found!					

To configure a new elevator click **Add** button and enter the following parameters.

Elevator ID:

Elevator Name:

Number of Floors: (1-99)

Authentication Device: Argo door

Access Duration For Floors: sec(1-99)

Search by: Enter Index/Name

Floor Index	Floor Name	Free Access Floor ⁱ	IO Controller	Output Port	
1	<input type="text" value="floor1"/>	<input type="checkbox"/>	3 ARCAUTO	<input type="text" value="1"/>	<input type="button" value="↔"/>
2	<input type="text" value="floor2"/>	<input type="checkbox"/>	3 ARCAUTO	<input type="text" value="2"/>	<input type="button" value="↔"/>
3	<input type="text" value="floor3"/>	<input type="checkbox"/>	3 ARCAUTO	<input type="text" value="Port No"/>	<input type="button" value="↔"/>
4	<input type="text" value="floor4"/>	<input type="checkbox"/>	3 ARCAUTO	<input type="text" value="Port No"/>	<input type="button" value="↔"/>
5	<input type="text" value="floor5"/>	<input type="checkbox"/>	3 ARCAUTO	<input type="text" value="Port No"/>	<input type="button" value="↔"/>
6	<input type="text" value="floor6"/>	<input type="checkbox"/>	3 ARCAUTO	<input type="text" value="Port No"/>	<input type="button" value="↔"/>

Elevator ID: The ID is auto-generated by the system.

Elevator Name: Enter a name for the elevator to be configured.

Number of Floors: Enter the number of floors that can be accessed using configured elevator. You can configure maximum **99** floors of Elevator. Then click **Update** to update the rows equal to number of floors in the grid. From the grid you can do the following settings:

- assign a name to each floor,
- mark each floor as free access floor which can be accessed by all the users without any authentication in the working hours.
- link each floor of the elevator to the Output port of IO Controller using the pick-list. Here floor3 and floor4 are linked to IO controller through output port 5 and 6 respectively.

You can also clear the floor details by clicking Clear button from the grid.



Ensure that the same IO controller port should not be assigned to different floors of elevator.

The screenshot shows the 'Elevator Configuration' window. At the top, there are form fields for 'Elevator ID' (1), 'Elevator Name' (Elevator 1), 'Number of Floors' (99), 'Authentication Device' (Argo door), and 'Access Duration For Floors' (10). An 'Update' button is below these fields. A search bar is located below the form fields. The main part of the interface is a table with the following columns: 'Floor Index', 'Floor Name', 'Free Access Floor', 'IO Controller', 'Output Port', and a right-pointing arrow. The table contains 6 rows of data. Below the table are buttons for 'Add', 'Delete', 'Save', and 'Cancel'.

Floor Index	Floor Name	Free Access Floor	IO Controller	Output Port	
1	floor1	<input checked="" type="checkbox"/>	3 ARCAUTO	1	↔
2	floor2	<input checked="" type="checkbox"/>	3 ARCAUTO	2	↔
3	floor3	<input checked="" type="checkbox"/>	3 ARCAUTO	3	↔
4	floor4	<input type="checkbox"/>	3 ARCAUTO	Port No	↔
5	floor5	<input type="checkbox"/>	3 ARCAUTO	Port No	↔
6	floor6	<input type="checkbox"/>	3 ARCAUTO	Port No	↔

Authentication Device: Select the device using the pick-list which is to be assigned as the authentication door in the elevator. It can be any panel door other than IO Controller. 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: Specify the duration in seconds till which the floor numbers in the elevator will be enabled for the user to access. After authenticating if the user does not press the floor number within the specified duration, then he will not be able to access and is required to re-authenticate.

You can search for the desired floors using the search bar. Select the desired option — Index, Name — to filter the floors.

Click **Save** to save the configured elevator. The created elevator gets displayed in the grid on the main page. Click **View List** button on the top right corner to view the list of elevators configured in the panel.

Elevator Configuration

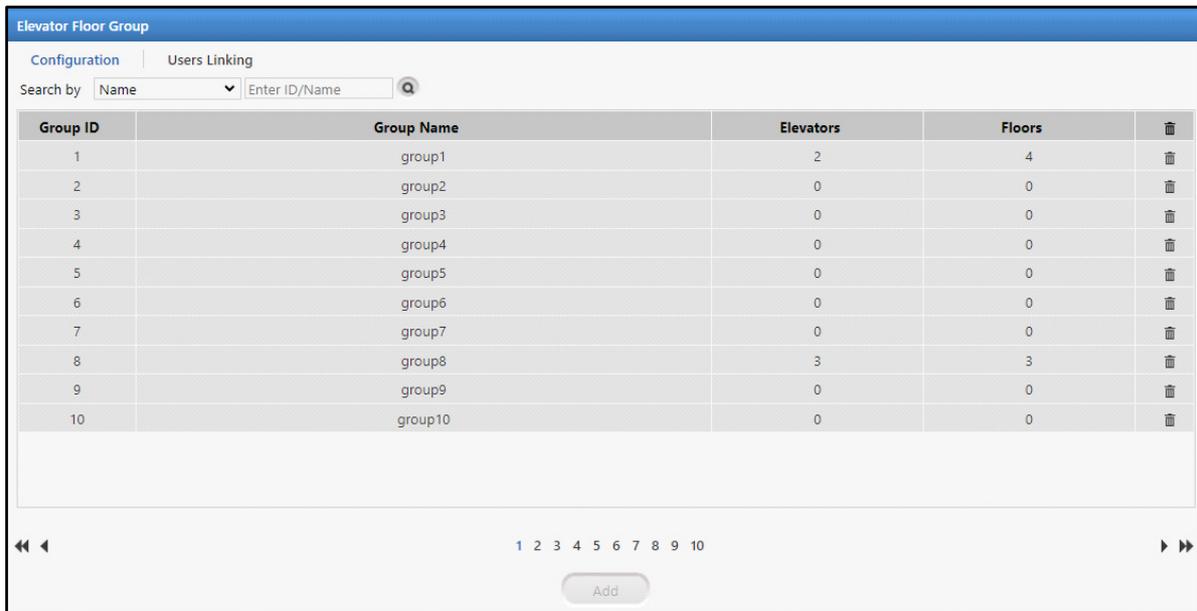
Elevator ID	Elevator Name	Door ID	Door Name	Floors	
1	Elevator 1	1	ARGO	8	

Elevator Floor Group

Elevator Floor Group page enables to group elevators and their desired floors and assign them to users for giving access to the required elevators only. Maximum 999 Elevator Floor Groups can be created.

Configuration

Configuration tab displays a grid containing a list of configured elevator floor groups.



The screenshot shows the 'Elevator Floor Group' configuration page. It has two tabs: 'Configuration' (selected) and 'Users Linking'. Below the tabs is a search bar with a dropdown menu set to 'Name' and a text input field for 'Enter ID/Name'. The main content is a table with the following data:

Group ID	Group Name	Elevators	Floors	
1	group1	2	4	🗑️
2	group2	0	0	🗑️
3	group3	0	0	🗑️
4	group4	0	0	🗑️
5	group5	0	0	🗑️
6	group6	0	0	🗑️
7	group7	0	0	🗑️
8	group8	3	3	🗑️
9	group9	0	0	🗑️
10	group10	0	0	🗑️

At the bottom of the table, there are navigation arrows, a page indicator '1 2 3 4 5 6 7 8 9 10', and an 'Add' button.

To configure a new elevator floor group click **Add** button and enter the following parameters.

Group ID: The group ID is auto-generated by the system.

Group Name: Enter the name for the elevator floor group to be configured.



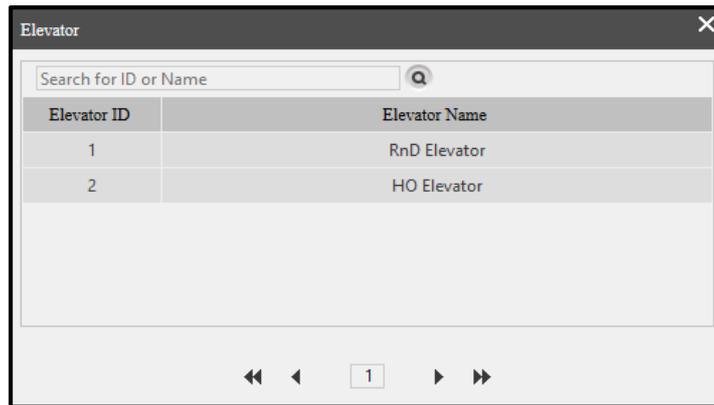
The screenshot shows the 'Elevator Floor Group' configuration page with the 'Configuration' tab selected. The form contains the following fields:

- Group ID:
- Group Name:
- Group Members section with three rows:
 - Elevator: ID Name (with a select icon)
 - Floor: ID Name (with a select icon)
 - Time Zone Group: ID Name (with a select icon)

At the bottom of the form are 'Update' and 'Cancel' buttons. To the right of the form is a table with the following columns: 'Sr. No.', 'Elevator Name', 'Floor Name', 'Time Zone Group Name', and a trash icon. The table currently displays 'No Record Found!'.

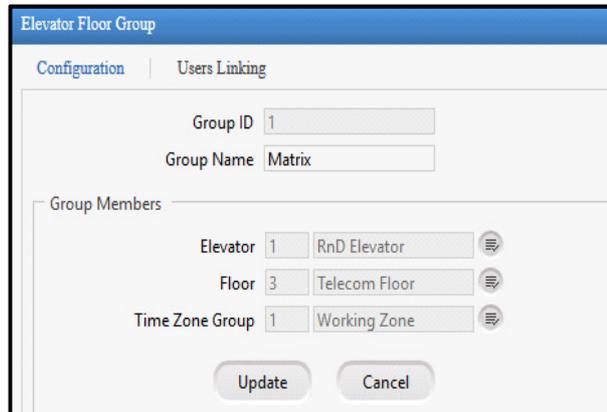
Group Members

Elevator: Click the Select Elevator button and select the desired elevator from the pick-list to include in the floor group. The Elevators are configured from Elevator Configuration. Refer 'Elevator Configuration' for the same. [See "Configuration" on page 228.](#)



Floor: Click the Select Floor button and select the desired floor from the pick-list to include in the floor group.

Time Zone Group: Click the Select Time Zone Group button and select the desired time zone from the pick-list to assign to the elevator floor group. The floors will be accessible during the selected time zone only. If no time zone is selected then the selected floors of the elevator will be accessible throughout the day.



Click **Update** to add the group members in the group. The members will get updated in the grid on the right hand side. You can add more members to the group. Here Marketing floor of HO Elevator can be accessed throughout the day.



Time Zone must be configured from Access Policies > Time Zone> Configuration

Click **View List** button on the top right corner to view the list of configured Elevator Floor Groups. You can search for the desired Elevator Floor Groups using the search bar. Select the desired option — ID, Name — to filter the Elevator Floor Groups.

The screenshot shows the 'Configuration' tab of the 'Elevator Floor Group' interface. At the top, there are two tabs: 'Configuration' (selected) and 'Users Linking'. Below the tabs is a search bar with a dropdown menu set to 'Name' and a search input field containing 'group11'. The main area contains a table with the following data:

Group ID	Group Name	Elevators	Floors	
11	group11	0	0	🗑️
110	group110	0	0	🗑️
111	group111	0	0	🗑️
112	group112	0	0	🗑️
113	group113	0	0	🗑️
114	group114	0	0	🗑️
115	group115	0	0	🗑️
116	group116	0	0	🗑️
117	group117	0	0	🗑️
118	group118	0	0	🗑️

At the bottom of the table, there are page numbers '1 2' and an 'Add' button.

Users Linking

Users Linking tab displays the elevator floor groups and the number of users linked with respective groups.

The screenshot shows the 'Users Linking' tab of the 'Elevator Floor Group' interface. At the top, there are two tabs: 'Configuration' and 'Users Linking' (selected). Below the tabs is a search bar with a dropdown menu set to 'Name' and a search input field containing 'Enter ID/Name'. The main area contains a table with the following data:

Group ID	Group Name	Users
1	group1	5
2	group2	0
3	group3	0
4	group4	0
5	group5	0
6	group6	0
7	group7	0
8	group8	5
9	group9	0
10	group10	0

At the bottom of the table, there are navigation arrows and page numbers '1 2 3 4 5 6 7 8 9 10'.

Click on the group and enter the following parameters for user linking.

Group ID/ Group Name: It displays the Group ID and Group Name for which users are to be linked.

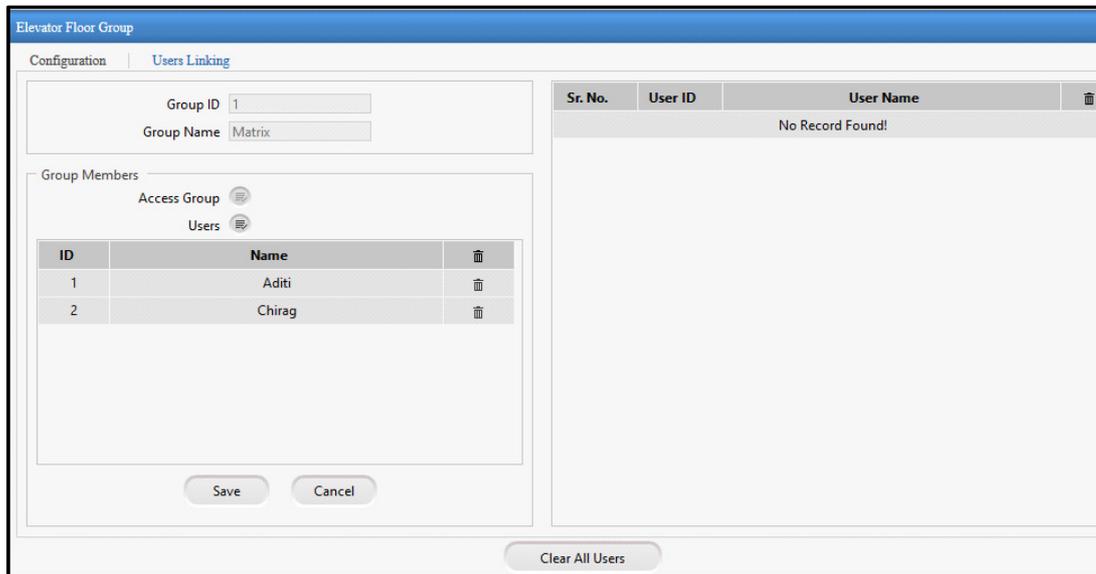
Group Members

You can select the users based on Access Group or individual Users for assigning to Elevator group.

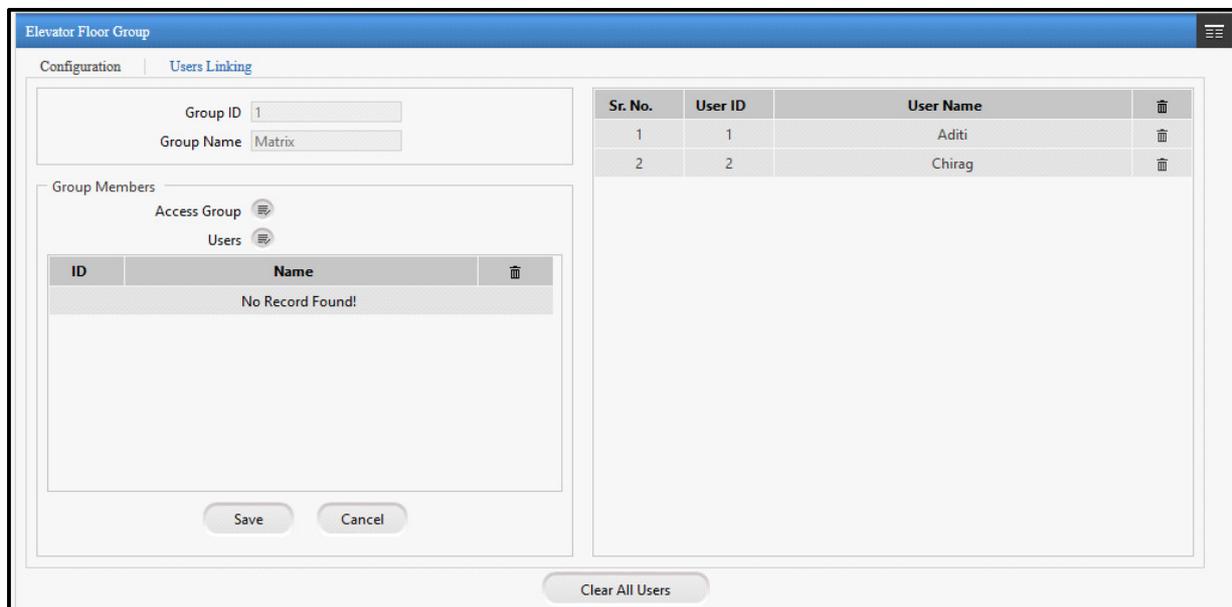
Access Group: Click the pick-list button to select the desired Access Group. The Access group is created from *Users > Access Group*.

Users: Click the pick-list to select the check-boxes for the desired Users which are to be assigned to the Elevator Group.

The selected users will be displayed in the grid below.



Click **Save** to save the members which gets updated in the grid on the right hand side.



You can click **Clear All Users** button to clear all the users and access groups from the elevator floor group.

Click **View List** button on the top right corner to view the list of users linked with Elevator Floor Groups. You can search for the desired users using the search bar. Select the desired option — ID, Name — to filter the users.

Elevator Floor Group		
Configuration		Users Linking
Search by	Name	group11
Group ID	Group Name	Users
11	group11	0
110	group110	0
111	group111	0
112	group112	0
113	group113	0
114	group114	0
115	group115	0
116	group116	0
117	group117	0
118	group118	0

1 2



*The Import, Export and Reports are configurable only when the Panel is in Standalone Mode.
(Configuration > Basic Profile > Panel Mode)*

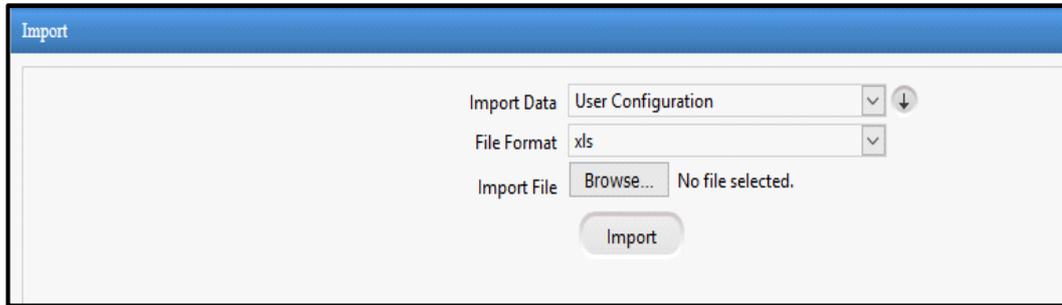
The Panel200 enables you to import data from excel files with predefined format. This would save the end user a lot of time and effort in making individual data entries at the application level.

Similarly the user can also export data to external applications based on the pre-configured data templates. The user has the flexibility to select the output formats as desired.

The Reports section enables you to view different reports based on Alarms, Device, Access Policies, User and Elevator Access Control for the specific time period.

Import

The Import feature helps in importing the data from one device or server to the other device. This feature is useful when the same data needs to be uploaded in multiple devices.

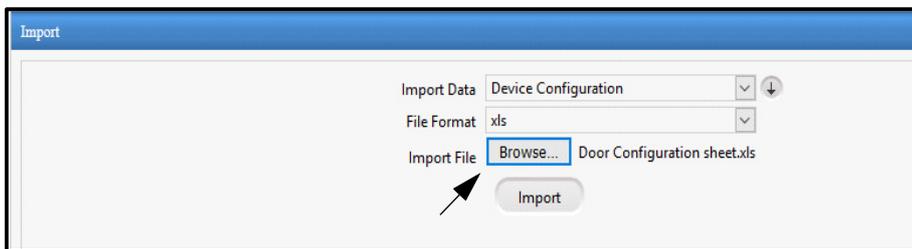


Import Data: Select the type of data from the options of User Configuration, Access Group, Shifts, Schedules etc which is to be imported to the Panel200 through the import file.

Click the **Download Sample Import File** button to download the sample file. You can open or save this sample file. Now in this sample file you can enter the data (say for devices) which can be uploaded into the panel.

File Format: Select the desired import file format option - XLS or CSV.

Import File: Click the Browse button and select the file to be imported.



The excel file imported here has following device configurations as shown below:

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
5	Door 5	1	1	0	192.168.110.1	00:1b:09:02:b0:00					
6	Door 6	1	1	0	192.168.110.2	00:1b:09:02:b0:01					
7	Door 7	1	1	0	192.168.110.3	00:1b:09:02:b0:02					
8	Door 8	1	1	0	192.168.110.4	00:1b:09:02:b0:03					
9	Door 9	1	1	0	192.168.110.5	00:1b:09:02:b0:04					
10	Door 10	1	1	0	192.168.110.6	00:1b:09:02:b0:05					

Then click the **Import** button to import the data from the selected file to the panel. When the data is imported successfully, the message "Import Success" will be displayed.

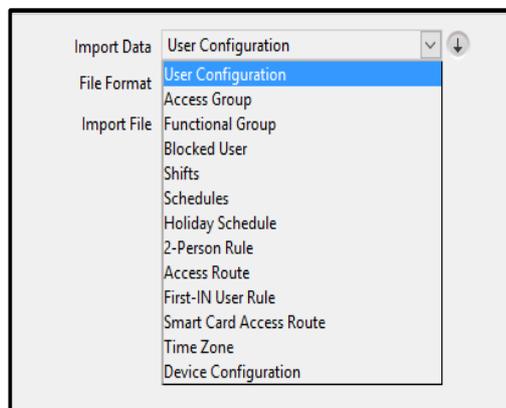


You can view the imported data from Device Configuration page as shown below:

The screenshot shows the 'Door Configuration' page with a blue header. Below the header is a search bar and three dropdown menus: '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	🗑️

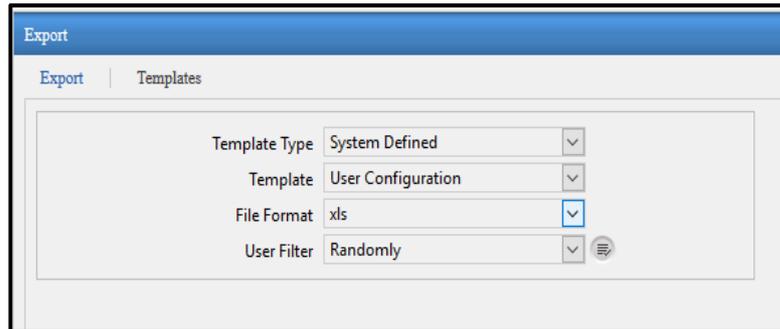
Similarly you can import other types of data as well.



Export

The Export feature helps in exporting the files from one device or server to other device. This feature is useful if you want to download (export) particular type of data from Panel200 and the same needs to be uploaded in other devices.

Export



The screenshot shows the 'Export' window with the following settings:

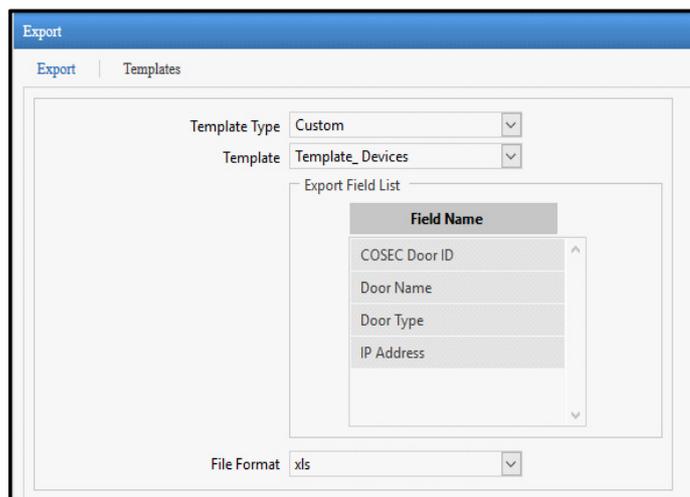
- Template Type: System Defined
- Template: User Configuration
- File Format: xls
- User Filter: Randomly

Template Type: Select the template type as Custom or System Defined in which data is to be exported.

- For System defined template type; data will be exported in the default template format.
- For Custom type of template you must create the desired template from “[Templates](#)” tab.

Template: Depending on the template type; select the template which is to be exported.

- If you select **System defined** template, then you can select the templates for User Configuration, Access Group, Shifts, Schedules etc.
- If you select **Custom** type of template, then user defined templates can be selected from the list. The Export field list of the custom template will be shown as below.



The screenshot shows the 'Export' window with the following settings:

- Template Type: Custom
- Template: Template_Devices
- Export Field List:
 - Field Name
 - COSEC Door ID
 - Door Name
 - Door Type
 - IP Address
- File Format: xls

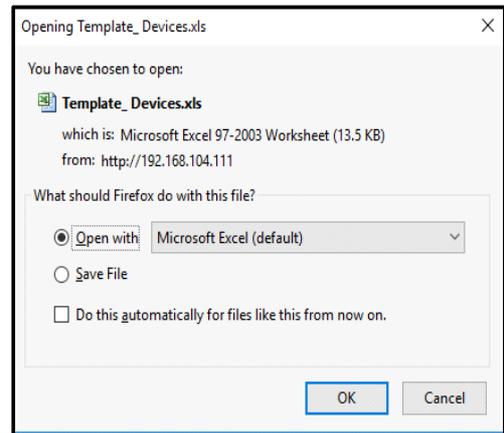
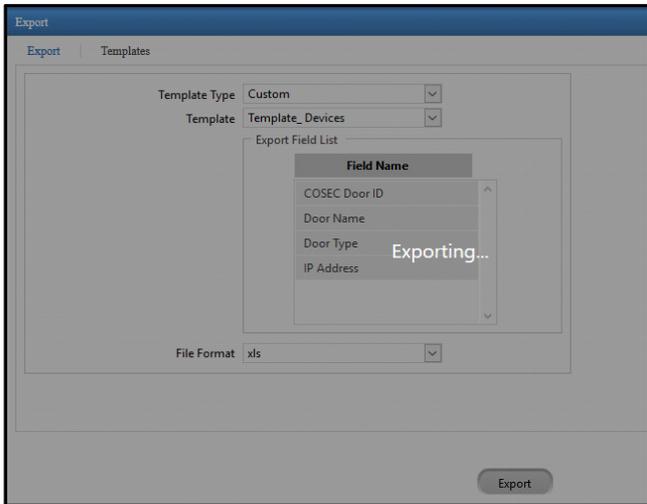
File Format: Select the desired export file format type - CSV, XLS or Text

Text File Separator: If the file format selected is Text or CSV then select the separator for the file.

User Filter: If you have selected System Defined as the Template Type, then select the User Filter as Randomly, Access Group or ALL.

If you have selected Randomly or Access Group then click the pick-list to select the desired user/group.

Then click on the **Export** button to export the data in the selected file format.

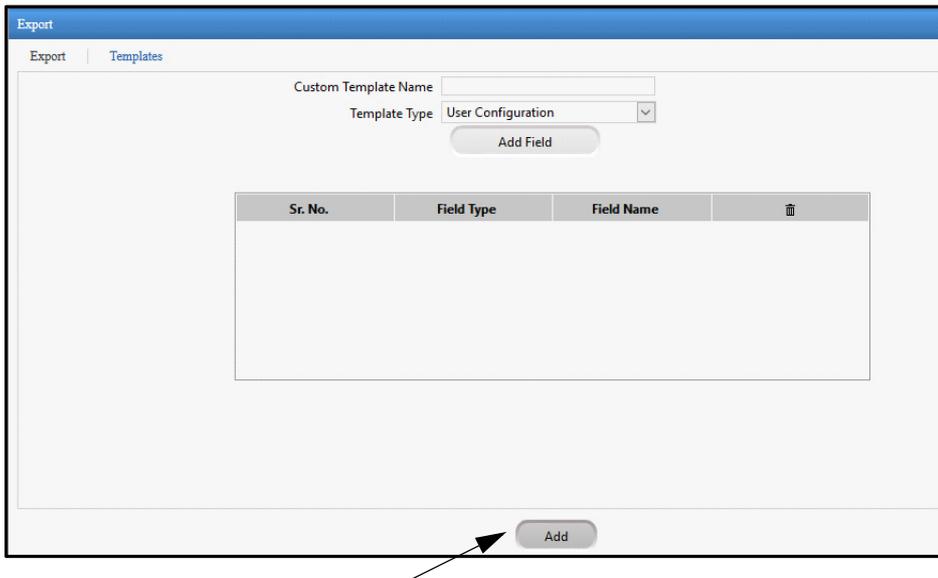


You can open the exported file or save the file at a desired location.

	A	B	C	D	E	F	G
1	COSEC Door	Door Name	Door Type	IP Address			
2	1	PVR Door	7	192.168.104.113			
3	5	Door 5	1	192.168.110.1			
4	6	Door 6	1	192.168.110.2			
5	7	Door 7	1	192.168.110.3			
6	8	Door 8	1	192.168.110.4			
7	9	Door 9	1	192.168.110.5			
8	10	Door 10	1	192.168.110.6			
9							

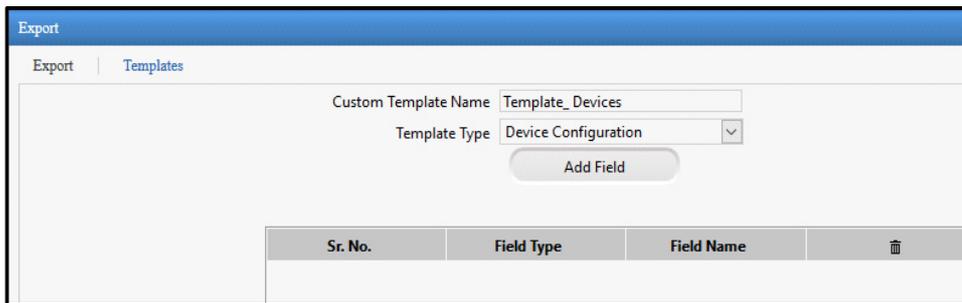
Templates

The user can create customize templates for export data. To do so, Click the **Add** button.

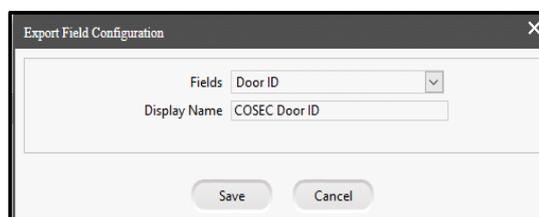


Custom Template Name: Specify a user friendly name for the custom template. For eg. Template_Canteen, Template_DailyEvents etc.

Template Type: Select the type of template from the drop-down list.



Click on **Add Field**. Then select the fields from drop down list and specify respective display names to be added in the template.



After selecting the required fields; click on the **Save** button to save the custom Template.

Custom Template Name

Template Type

Sr. No.	Field Type	Field Name	
1	Door ID	COSEC Door ID	<input type="button" value="🗑"/>
2	Door Name	Door Name	<input type="button" value="🗑"/>
3	Door Type	Door Type	<input type="button" value="🗑"/>
4	IP Address/RS-485 Address	IP Address	<input type="button" value="🗑"/>

The configured Template will appear in the drop-down options for Template.

Reports

Reports enable you to view the Alarm, Device, Rule Violation and User details based on the date filter.



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”.

The screenshot shows a web interface titled 'Reports'. It has several tabs: 'Alarm', 'Device', 'Access Policies', 'User', and 'Elevator Access Control'. The 'Alarm' tab is selected. Below the tabs, there is a 'Select Date' field with a date range from '01-03-2018' to '22-03-2018'. There are calendar icons on either side of the date range. At the bottom, there is a 'Generate Report' button.

Select Date: Select the From and To Date using the calendar buttons.

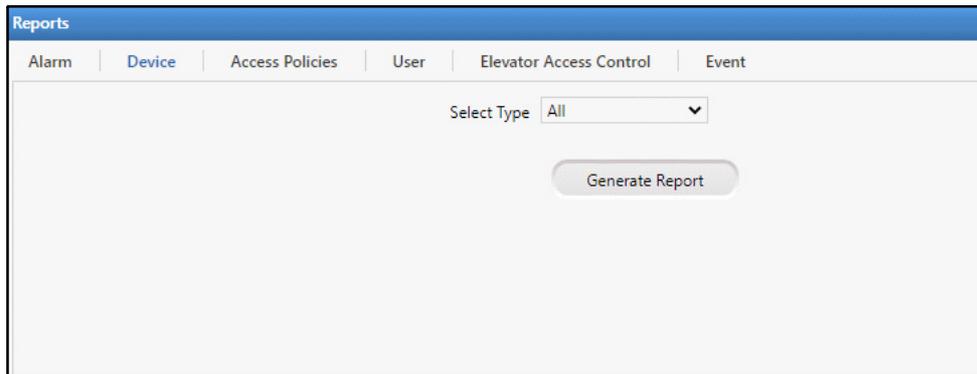
Click **Generate Report**. The Alarm Report for the selected door will be downloaded.

The screenshot shows an Excel spreadsheet titled 'Alarm Reports [Read-Only] [Compatibility Mode] - Microsoft Excel'. The spreadsheet contains the following data:

Sr. No.	Alarm Name	Source	Category
1	Tamper Alarm	Test_Pvr	Critical
2	Tamper Alarm	Test_Pvr	Critical
3	Tamper Alarm	Test_Pvr	Critical
4	Deadman Timer Expired	Test_V2	Critical
5	Duress Alarm	Test_V2	Critical
6	Panic Alarm	Test_V2	Critical
7	FP Memory Full	Test_V2	Minor
8	FP Memory Full	Test_V2	Minor
9	Door Held Open Too Long	Test_V2	Minor
10	Door Abnormal	Test_V2	Major
11	Door Force Open	Test_V2	Critical
12	Door Controller Offline	Test_V2	Major
13	Door Controller Fault	Test_V2	Major
14	Tamper Alarm	Test_V2	Critical
15	Master Power Fail Alarm	Test_V2	Major
16	Master Alarm Input	Test_V2	Critical
17	RTC error	Test_V2	Major
18	Event Buffer Full	Test_V2	Major
19	Tail- Gating Alarm	Test_V2	Major
20	Man Trap Timer Violated Al	Test_V2	Major
21	Access Denied Aalarm	Test_V2	Major
22	Multiple Unauthorized Acce	Test_V2	Major
23	User Unidentified	Test_V2	Major
24	Anti-Pass Back Violated Al	Test_V2	Major

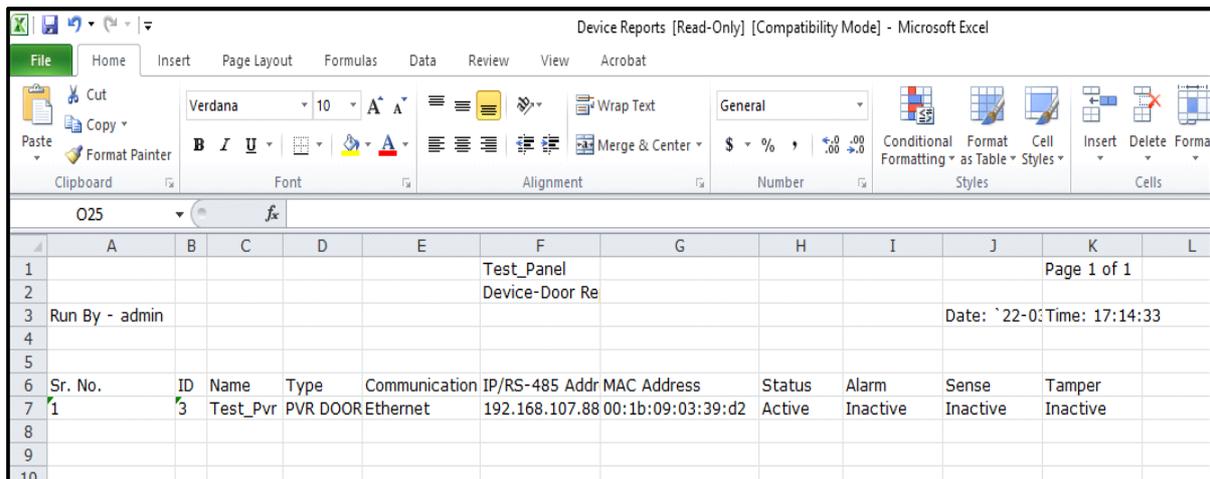
Device

All the configured device details appear in the Device Report. For details, refer to [“Door Configuration”](#).



Select Type: Select the Door Type from the drop-down list for which the report is to be generated.

Click **Generate Report**. The Device Report for the selected door will be downloaded.



The screenshot shows a Microsoft Excel spreadsheet titled "Device Reports [Read-Only] [Compatibility Mode] - Microsoft Excel". The spreadsheet contains the following data:

Sr. No.	ID	Name	Type	Communication	IP/RS-485 Addr	MAC Address	Status	Alarm	Sense	Tamper
1	3	Test_Pvr	PVR DOOR	Ethernet	192.168.107.88	00:1b:09:03:39:d2	Active	Inactive	Inactive	Inactive

Additional information displayed in the spreadsheet includes "Run By - admin", "Date: `22-00:17:14:33", and "Page 1 of 1".

Access Policies

All the configured access policy details appear in the Access Policies Report. For details, refer to [“Access Policies & Access Schedule”](#).

Report

The Report can be generated for a particular Access policy by selecting the option for the following filters.

Reports

Alarm | Device | Access Policies | User | Elevator Access Control

Report | Report Template

Select Date: 23-03-2018 [calendar] 24-03-2018 [calendar]

Type: Custom [v]

Event: Denied [v]

Rule: 2-Person Rule [v]

Report Generation: Door Wise [v]

Door: All [v]

Reports

Alarm | Device | Access Policies | User | Elevator Access Control

Report | Report Template

Select Date: 23-03-2018 [calendar] 23-03-2018 [calendar]

Type: Template Based [v]

Template: Template1 [v]

Event: Allowed [v]

Rule: 2-Person Rule [v]

Report Generation: Door Wise [v]

Door: All [v]

Select Date: Select the From and To Date using the calendar buttons.

Type: Select the **Type** of report from the options of **Custom** or **Template Based**. For Template based, you must create template from “**Report Template**” tab.

1. For Template Based type, you can select the created **template** from drop down options. The other fields will be displayed accordingly.
2. For Custom based, configure the following fields:
 - Select the **Event** as Allowed or Denied. Eg: If event is selected as “Allowed” then report will be generated for Allowed events for the selected Rule.
 - Select the specific Access **Rule** from the drop down list to generate the report based on selected rule. You can also select the option All to include all the rules.
 - Select the Door Wise or User Wise **Report Generation** filter. The Door/User can be selected randomly from the picklist.

Click **Generate Report**. The Access Policy Report for the set filters will be downloaded.

Here Template based report for 2-person rule allowed is displayed as below.

Sr. No.	Door ID	Door Name	User ID	User Name	Rule	Date	Time
1	1	PVR Door	2	Geeta	2-Person Rule Secondary	23-03-2018	17:23:05
2	1	PVR Door	1	Rohan	2-Person Rule Primary	23-03-2018	17:23:05

Report Template

The Report templates can be created based on which report can be generated. You can create maximum 9 templates. Click on the **Add** button to create report template.

Template Name: Enter the name of the template.

Event: Select the Allowed or Denied option for the type of Event in the template.

Select the specific **Rule** violation from the drop down list to generate the report based on selected rule. You can also select the option All to include all the rules in the template.

Select the Door Wise or User Wise **Report Generation** filter. The Door/User can be selected randomly from the picklist.

Click the **Save** button to save the configured template. After saving the template; it appears in the Template drop-down list in Report tab.

Reports

Alarm | Device | Access Policies | User | Elevator Access Control

Report | Report Template

Template Name: Template1

Event: Allowed

Rule: 2-Person Rule

Report Generation: Door Wise

Door: All

Name	Event	Rule
Template1	Allowed	2-Person Rule

Add | Delete | Save | Cancel

User

Select Type: Select the User Type from the drop-down list. For example: Blocked Users

Select Date: Select the From and To Date using the calendar button for Blocked Users.

Reports

Alarm | Device | Access Policies | User | Elevator Access Control | Event

Select Type: Configured Users

Generate Report

Reports

Alarm | Device | Access Policies | User | Elevator Access Control | Event

Select Type: Blocked Users

Select Date: 08-12-2020 | 23-12-2020

Generate Report

 The fields may vary as per the Selected Type of Users.

Click **Generate Report**. The User Report for the set filters will be downloaded.

The screenshot shows a Microsoft Excel spreadsheet with the following data:

Sr. No.	User ID	User Name	Date	Time	Device	Description
1	h1	hardik1	19-03-2018	18:17:11	Test_V21	User Allowed
2	h1	hardik1	19-03-2018	18:23:14	Test_V21	User Allowed
3	h1	hardik1	19-03-2018	18:34:31	Test_V21	User Allowed
4	h1	hardik1	19-03-2018	18:36:21	Test_V21	User Allowed

Additional information from the spreadsheet:

- Run By: admin
- Date: 22-03-2018
- Time: 17:20:29
- Page 1 of 1

Elevator Access Control

The screenshot shows the 'Reports' interface with the following settings:

- Alarm
- Device
- Access Policies
- User
- Elevator Access Control** (Selected)
- Event

Filters:

- Select Date: From Date [Calendar] To Date [Calendar]
- Report Type: Elevator Wise (Dropdown)
- Select Elevator: All (Dropdown)

Generate Report (Button)

Select Date: Select the From and To date using the calendar for specifying the duration for which the report is to be generated.

Report Type: Select the type of report to be generated from the drop-down list. You can generate Elevator Wise or User Wise reports.

Select Elevator/User: Select the elevator or user using the picklist for which the report is to be generated. The elevator picklist contains elevators configured from the ["Elevator Configuration"](#) page. You can also select All to generate report for all the elevators or users.

Click **Generate Report**. The Elevator Access Control Report for the set filters will be downloaded.

Event

The screenshot shows the 'Reports' interface with the 'Event' tab selected. The form includes the following fields and options:

- Source Type:** A dropdown menu set to 'User'.
- User:** A dropdown menu set to 'All'.
- Select Date:** Two date pickers showing '15-06-2024' and '20-06-2024'.
- Credential Type:** A dropdown menu set to 'Selected', with a list of options: PIN, Card, Card+PIN, Finger, Finger+PIN, Finger+Card, and Finger+Card+PIN.
- Credentials:** A section with checkboxes for Access Card 1 and Access Card 2.
- Generate Report:** A button at the bottom of the form.

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 option as **Randomly**, select the check boxes of the desired doors/users.

Select Date: Select the From and To date using the calendar for specifying the duration for which the report is to be generated.

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 Credential 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 on **Generate Report**. The Event Report for the set filters will be downloaded.

Sr. No.	User ID	User Name	Date	Time	Device	Entry/ Exit	Credential	Description
1	i4	i4	24-07-2024	00:01:11	P	ARGO Entry	Card1	User Allowed
2	i4	i4	24-07-2024	00:01:13	P	VEGA Entry	Card1	User Allowed
3	2736	Ishani Patel	24-07-2024	00:01:15	P	ARGO Entry	Card1	User Allowed
4	2736	Ishani Patel	24-07-2024	00:01:17	P	VEGA Entry	Card1	User Allowed
5	2736	Ishani Patel	24-07-2024	00:01:20	P	ARGO Entry	Card1	User Allowed
6	i4	i4	25-07-2024	00:00:52	P	ARGO Entry	Card1	User Allowed
7	2736	Ishani Patel	25-07-2024	00:00:52	P	ARGO Entry	Face	User Allowed
8	2736	Ishani Patel	25-07-2024	00:00:55	P	ARGO Entry	Card1	User Allowed
9	2736	Ishani Patel	24-07-2024	09:32:28	P	ARGO Entry	Face	User Denied - Invalid Route Access
10	2736	Ishani Patel	24-07-2024	09:32:39	P	ARGO Entry	Face	User Denied - Invalid Route Access
11	2736	Ishani Patel	24-07-2024	09:32:44	P	ARGO Entry	Face	User Denied - Invalid Route Access
12	2736	Ishani Patel	24-07-2024	09:33:46	P	ARGO Entry	Face	User Denied - Invalid Route Access
13	2736	Ishani Patel	24-07-2024	09:36:09	P	ARGO Entry	Face	User Denied - Invalid Route Access
14	2736	Ishani Patel	24-07-2024	09:36:39	P	ARGO Entry	Face	User Denied - Invalid Route Access
15	2736	Ishani Patel	24-07-2024	09:39:34	P	ARGO Entry	Face	User Denied - Invalid Route Access
16	2736	Ishani Patel	24-07-2024	09:57:37	P	VEGA Entry	Card1	User Denied - Invalid Route Access
17	2736	Ishani Patel	24-07-2024	09:57:44	P	ARGO Entry	Card1	User Allowed
18	2736	Ishani Patel	24-07-2024	09:57:44	P	ARGO Entry	Card1	User Denied - Invalid Route Access
19	2736	Ishani Patel	24-07-2024	09:57:45	P	VEGA Entry	Card1	User Denied - Invalid Route Access
20	2736	Ishani Patel	24-07-2024	09:57:49	P	PVR 1 Entry	Card1	User Denied - Invalid Route Access
21	2736	Ishani Patel	24-07-2024	09:57:51	P	ARGO Entry	Card1	User Denied - Invalid Route Access
22	2736	Ishani Patel	24-07-2024	09:57:57	P	ARC C Exit	Card1	User Denied - Invalid Route Access
23	2736	Ishani Patel	24-07-2024	09:58:02	P	ARGO Entry	Face	User Denied - Invalid Route Access
24	2736	Ishani Patel	24-07-2024	09:58:05	P	ARGO Entry	Face	User Denied - Invalid Route Access
25	2736	Ishani Patel	24-07-2024	09:59:06	P	VEGA Entry	Card1	User Denied - Invalid Route Access
26	2736	Ishani Patel	24-07-2024	09:59:07	P	ARGO Entry	Card1	User Denied - Invalid Route Access
27	2736	Ishani Patel	24-07-2024	09:59:08	P	ARGO Entry	Card1	User Denied - Invalid Route Access
28	2736	Ishani Patel	24-07-2024	09:59:10	P	ARGO Exit	Card1	User Denied - Invalid Route Access
29	2736	Ishani Patel	24-07-2024	09:59:10	P	PVR 1 Entry	Card1	User Denied - Invalid Route Access
30	2736	Ishani Patel	24-07-2024	10:02:10	P	ARGO Entry	Face	User Denied - Invalid Route Access
31	2736	Ishani Patel	24-07-2024	10:02:17	P	ARGO Entry	Face	User Denied - Invalid Route Access
32	2736	Ishani Patel	24-07-2024	10:09:36	P	ARGO Entry	Face	User Denied - Invalid Route Access
33	2736	Ishani Patel	24-07-2024	10:10:04	P	VEGA Entry	Card1	User Denied - Invalid Route Access
34	2736	Ishani Patel	24-07-2024	10:10:04	P	ARGO Entry	Card1	User Denied - Invalid Route Access
35	2736	Ishani Patel	24-07-2024	10:10:06	P	ARGO Entry	Card1	User Denied - Invalid Route Access
36	2736	Ishani Patel	24-07-2024	10:10:07	P	PVR 1 Entry	Card1	User Denied - Invalid Route Access
37	2736	Ishani Patel	24-07-2024	10:12:17	P	ARGO Entry	Face	User Denied - Invalid Route Access
38	2736	Ishani Patel	24-07-2024	10:26:35	P	ARGO Entry	Face	User Denied - Invalid Route Access
39	2736	Ishani Patel	24-07-2024	11:02:37	P	ARGO Entry	Finger + Card1	User denied - Control zone
40	2736	Ishani Patel	24-07-2024	11:02:42	P	ARGO Entry	Finger + Card1	User denied - Control zone
41	2736	Ishani Patel	24-07-2024	11:02:51	P	ARGO Entry	Finger + Card1	User Allowed
42	2736	Ishani Patel	24-07-2024	11:02:57	P	ARGO Entry	Finger	User Denied - Time Out
43	2736	Ishani Patel	24-07-2024	11:02:59	P	VEGA Entry	Finger + Card1	User Allowed
44	2736	Ishani Patel	24-07-2024	11:03:02	P	ARGO Entry	Card1	User denied - Control zone
45	2736	Ishani Patel	24-07-2024	11:03:04	P	ARGO Entry	Card1	User denied - Control zone
46	2736	Ishani Patel	24-07-2024	11:04:55	P	ARGO Entry	Face	User Denied - Invalid Route Access
47	2736	Ishani Patel	24-07-2024	11:04:57	P	ARGO Entry	Finger + Card1	User Allowed
48	2736	Ishani Patel	24-07-2024	11:04:59	P	ARGO Entry	Face	User Denied - Invalid Route Access
49	2736	Ishani Patel	24-07-2024	11:05:37	P	VEGA Entry	Finger + Card1	User Allowed
50	2736	Ishani Patel	24-07-2024	11:05:41	P	VEGA Entry	Finger + Card1	User Allowed - Panel route access -
51	2736	Ishani Patel	24-07-2024	11:05:46	P	VEGA Exit	Finger + Card1	User denied - Control zone
52	2736	Ishani Patel	24-07-2024	11:05:52	P	VEGA Exit	Finger + Card1	User Allowed
53	2736	Ishani Patel	24-07-2024	11:06:02	P	ARGO Entry	Finger + Card1	User Allowed



Alerts are configurable only when the Panel is in Standalone Mode. (Configuration > Basic Profile > Panel Mode)

The Panel200 can be configured to send the preset alerts to its users in response to certain predefined user events. If such a predefined user event occurs, it will trigger an alert message to be sent to the relevant user or users via SMS or E-mail.

The Alert Server parameters must be configured for sending SMS using one the selected SMS service providers. Also to send an emails, you need to set the email configurations. Before configuring ensure that an SMTP Server has been set up on the network.

Refer Topics: [“Alert Message Configuration”](#) and [“Alert Server Configuration”](#) for details.

Alert Message Configuration

The Alert Message Configuration enables the user to configure Email and SMS alert messages for Access Control events, System events and Alarm events.

This page displays all the active events along with default **Alert, Alert Schedule and Recipients**.

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

To activate alert for a particular event; select that event from the grid. The alert configuration for selected event appears as shown below.

The screenshot shows the configuration for the 'User Denied - 2-Person Rule' event. The 'Event Type' is set to 'Access Control'. The 'Active' checkbox is checked. Alerts for both 'SMS' and 'Email' are selected. The 'Alert Schedule' is set to 'Time Zone', with 'Time Zone 1' selected. The 'Message Preview' section shows the default message for SMS and Email. The SMS message is: '<User Name> (ID: <User ID>): <Entry/ Exit> Denied due to violation of 2-Person rule at <Door Name> on <Date - Time>' (13/130). The Email subject is 'User Denied Access' and the body is: 'Dear User, <User Name> (ID: <User ID>): <Entry/ Exit> Denied due to violation of 2-Person rule at <Door Name> on <Date - Time>' (162/300). At the top right corner, there is a 'View List' button (represented by a list icon) which allows returning to the event grid.

You can go back to the event grid page by clicking **View List** button at top right corner.

Event Type: Select the type of event from the options of Access Control, Alarm and System.



When Authorization on Enrollment is enabled from Panel Configuration > Advanced Profile > Enrollment; then the alert for System Event- "Authorization on Enrollment" will get enabled automatically for the Admin and HRD recipients.

Event: As per the type of event selected; you can select the specific event for which alert message can be configured.

Active: Select the Active checkbox to activate the alert for the selected event.

Alerts: Select the checkbox for SMS and/or Email alerts to be sent whenever the event occurs.

Alert Schedule: Select the alert schedule as Time Zone or Time Zone Group and select the respective Time zone or Time Zone group from the picklist for which alert messages are to be sent.



When client is situated in a time zone other than Alert Service's time zone; Alert Service will take tenant's time zone into consideration while processing scheduled tasks.

Time Zone and Time Zone Group can be configured from Access Policies> Time Zone.

Message Preview

SMS: The SMS format is displayed in the Message box. Click on **Default Message** to send the default SMS.

Email: The Email format is displayed in the Email box. Click on **Default Email** to send the default Email. You can edit Email Subject, Salutation, Additional Message and Signature.

You can add dynamic fields in SMS and Email by writing the field in tags <>

Click on the **Save** button to save the message configuration.

Recipients

Send To: You can send the messages to Individual, Selected Recipients or Both.

- **Individual:** The configured alert will be sent to the user for whom event is generated. Eg: If Access Allowed event for the user James is generated; then the alert message will be sent to James only.
- **Selected Recipients:** Select the desire users by clicking on the **Select Recipients** pick-list. You can select maximum 10 users. You can also search the user by entering the name in the field. Then click **Add Recipient** button.
- **Both:** Click the Select Recipients picklist button and select the users to whom alert is to be sent. You can select maximum 10 users. So alert can be sent to maximum 10 users and 1 individual user for whom event is generated.

Name	Email	Mobile	
Deep	deep.gandhi@gmail.com	9532487512	🗑️

Click **Save** to save the Alert Message Configuration. You can also click the Default button, to assign default values to all the parameters.

Alert Server Configuration

The Alert Server Configuration enables the user to get Email and SMS alerts for Access Control events, System events and Alarm events.

EMAIL

The screenshot shows the 'Alert Server Configuration' window with the 'Email' tab selected. The configuration fields are as follows:

- Enable:
- Encryption (SSL):
- Server Address: smtp.gmail.com
- Port: 465 (1-65535)
- User Name: cosectest7
- Password: [Masked]
- Sender's Email ID: cosectest7@gmail.com

Below the configuration fields is a 'Test Connection' section with an 'Email ID' field containing 'akshaydavda92@gmail.com' and a 'Send Message' button. At the bottom of the window are 'Default', 'Save', and 'Cancel' buttons.

Enable: Select the Enable checkbox to configure Email Server.

Encryption: Select the Encryption checkbox to enable SMTP encryption. In encrypted mode, communication will be done through port number 465.

Server Address: Enter the IP Address or name of the configured SMTP server. Eg: 192.168.103.10

Port: Enter the TCP port number for the SMTP service as set on the SMTP server. The default port is 25.

User Name: Enter the username to access the configured Email Server.

Password: Enter the password to access the configured Email Server.

Sender's Email ID: Enter the Email ID of the sender.

Test Connection

Email ID: Enter the Email ID of the receiver for testing the connection. Click on the **Send Message** button to send the test mail.

SMS

Enable: Select the Enable checkbox to configure SMS server.

Service Provider : Select the Service provider from the options of SMS Gateway Center ,SMS Lane , Business SMS ,Bulk SMS and SNOWEBS. You can also configure 5 new custom service providers by clicking on the Add button. For details, [See “SMS Service Providers” on page 253.](#)

User Name, Password: Enter the Username and Password to use the selected SMS service.



Contact your Network Administrator to know the username and password of the SMS service.

Sender's ID: Enter the registered sender ID.

Check Balance: Click the Check Balance button to know the available SMS balance.

The screenshot shows the 'Alert Server Configuration' dialog box with the 'SMS' tab selected. The 'Enable' checkbox is checked. The 'Service Provider' dropdown is set to 'SMS Gateway Center'. The 'User Name' field contains 'matrixcomsec', the 'Password' field is masked with dots, and the 'Sender's ID' field contains 'MATRIX'. The 'Check Balance' button is active, and the 'Balance SMS Credits' is displayed as 930. Below these fields is a 'Test Connection' section with a 'Mobile Number' field containing '8866614176' and a 'Send Message' button. At the bottom of the dialog are 'Default', 'Save', and 'Cancel' buttons.

Test Connection

Mobile Number: Enter the Mobile Number of the receiver for testing the connection. Click on the Send Message button to send the test SMS.

Click **Save** to save the Alert Server Settings. Click on the **Default** button to assign default values to all the parameters.

SMS Service Providers

You can configure upto 5 new custom service providers by clicking on **Add** button.

The screenshot shows the 'SMS Service Provider' configuration window. It includes the following fields and controls:

- Service Provider Name: Way2Sms
- Service Provider URL: www.way2sms.com
- SMS Base URL: library/send_sms_2.php?
- API Argument: (empty)
- Argument Value: User Name
- Buttons: Add, Cancel
- Table:

API Argument	Argument Value	Custom Value	
uname	User Name		🗑️
- Argument Separator: &
- Request Method: Post
- Buttons: Save, Cancel

- **Service Provider Name:** Enter the name of the new service provider. Eg: Way2Sms
- **Service Provider URL:** Enter the URL of the new service provider. Eg: http://www.way2sms.com/
- **SMS Base URL:** Enter the Base URL of the service provider as given in the API document. This is used for sending the message through SMS. Eg: library/send_sms_2.php?
- **API Argument:** Enter the API argument name as specified in the API document of the service provider. You can add maximum 10 API Arguments. Eg: uname, pwd, To are the arguments specified from the API document in the above URL.
- **Argument Value:** Select the argument value from the dropdown list which is to be associated with the API argument.

Click on the **Add** button to associate API Arguments with the Argument value. The added arguments get displayed in the grid.

- **Argument Separator:** Enter the argument separator to be used in the execution of command.
- **Request Method:** Select the method for sending the message via sms. The options are: Post and Web. If Post is selected, you can send long messages without any limitation. If Web is selected, you can send only short messages.
- **Request Preview:** It displays the preview of URL i.e. Service Provider URL + SMS Base URL + SMS Arguments separated by argument separator in sequence. The complete URL along with arguments will be displayed in Request Preview.
- Eg: http://www.way2sms.com/library/send_sms_2.php?uname=UserName;pwd=Password;To=MobileNumber;Mask=SenderID
- **Check Balance:** Select this check-box to allow balance checking and enter the corresponding API.

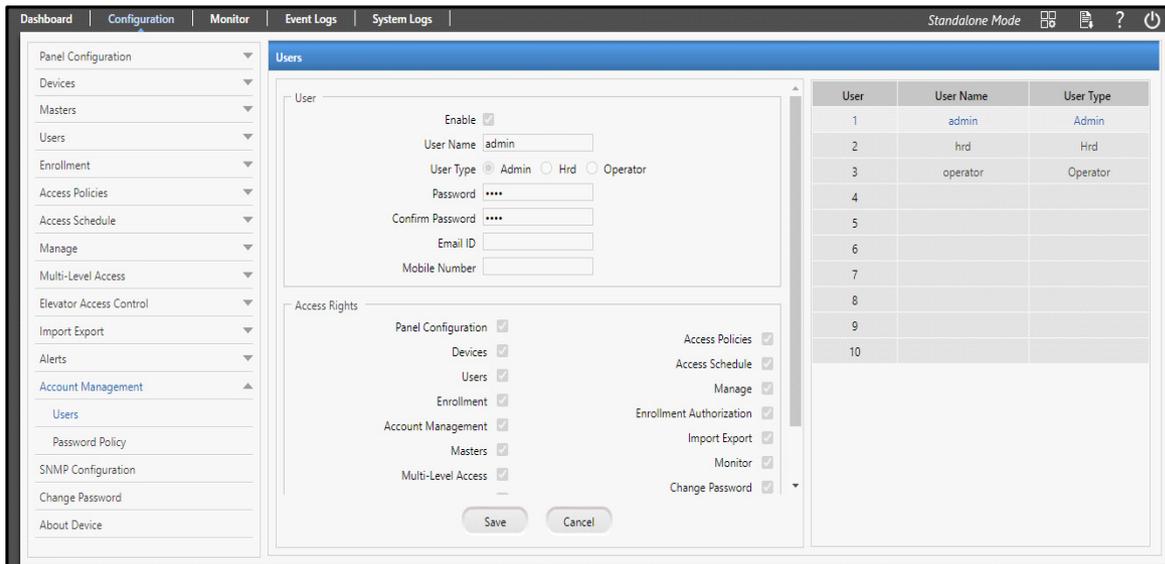
Click on the **Save** button to save the settings.



Account Management is configurable only when the Panel is in Standalone Mode. (Configuration > Basic Profile > Panel Mode)

The Account Management allows you to configure different user accounts such as Admin, HRD and Operator types and assign them different access rights for accessing features of Panel200 as per the requirement.

You can configure password policy i.e. the minimum password length with the required strength as well as password expiration and lockout policy. The password of Panel200 can be changed from Change password page



Users



Users is configurable only when the Panel is in Standalone Mode. (Configuration > Basic Profile > Panel Mode)

Account Management for Users allows defining all the parameters pertaining to a user, such as user name, password, user type (i.e. Admin, HRD, or Operator); and based on the user type, authorizing the user to configure a device.

The Admin, HRD and Operator are the default user accounts. You can create upto 7 user accounts.

User

To create the new user account click on the user number from the right side grid.

User	User Name	User Type
1	admin	Admin
2	hrd	Hrd
3	operator	Operator
4		
5		
6		
7		
8		
9		
10		

Enable: Select this checkbox to enable the user account.

User Name: Specify the name of the user account.

User Type: Select the User Type as Admin, HRD or Operator to be allotted.

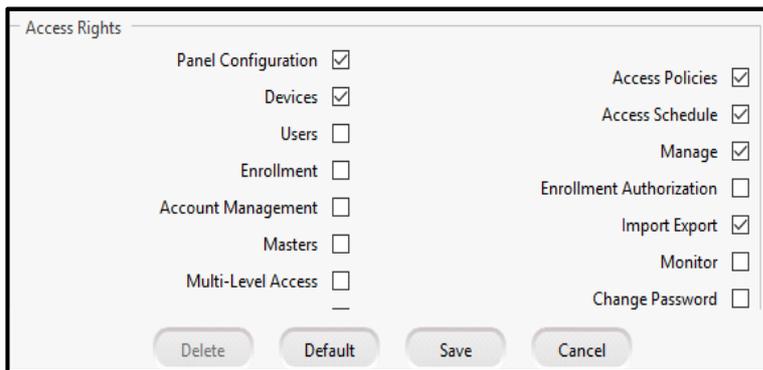
Password: Specify the Password for the user.

Confirm: Enter the password again for confirmation.

Email ID: Enter the Email ID of the user.

Mobile Number: Enter the Mobile number of the user.

Access Rights



The image shows a dialog box titled "Access Rights" with a list of permissions and their corresponding checkboxes. The permissions are arranged in two columns. At the bottom of the dialog, there are four buttons: "Delete", "Default", "Save", and "Cancel".

Permission	Checked
Panel Configuration	<input checked="" type="checkbox"/>
Devices	<input checked="" type="checkbox"/>
Users	<input type="checkbox"/>
Enrollment	<input type="checkbox"/>
Account Management	<input type="checkbox"/>
Masters	<input type="checkbox"/>
Multi-Level Access	<input type="checkbox"/>
Access Policies	<input checked="" type="checkbox"/>
Access Schedule	<input checked="" type="checkbox"/>
Manage	<input checked="" type="checkbox"/>
Enrollment Authorization	<input type="checkbox"/>
Import Export	<input checked="" type="checkbox"/>
Monitor	<input type="checkbox"/>
Change Password	<input type="checkbox"/>

The Access Rights to the user can be assigned depending on the user type. The rights can be assigned by selecting the checkbox against the respective functionality. The users will be able to view the pages based on the assigned Access Rights.

Click on the **Save** button to save the configured user account.

Password Policy



The Password Policy is accessible only when the Panel is in Standalone Mode. (Configuration > Basic Profile > Panel Mode)

You can set the policy for configuration of password from the Password Policy page.

Minimum Password Length	4	(4-16)
Password Strength	Low	
Password Expiration Policy	<input type="checkbox"/>	
Expire Password After	60	day(s) (1-365)
Account Lockout Policy	<input checked="" type="checkbox"/>	
Maximum Invalid Login Attempts Allowed	5	(1-15)
Lock Account For	15	min (1-999)

Minimum Password length: Specify the minimum length of password.

Password Strength: Set the strength of password to be low, Medium or High.

Password Expiration Policy: Select this checkbox if you want the password to get expired after configured number of days.

- **Expire Password After (days):** Specify the number of days after which you want the password to get expired.

Account Lockout Policy: If you want the account to get locked after the invalid login then select this checkbox.

- **Maximum Invalid login Attempts Allowed:** Specify the number of attempts for invalid login after which the account will get locked.
- **Lock Account for (minutes):** Specify the duration of minutes for which the account will remain locked.

Click on the **Save** button to save the configuration of password policy.



SNMP Configuration is configurable only when the Panel is in Standalone Mode. (Configuration > Basic Profile > Panel Mode)

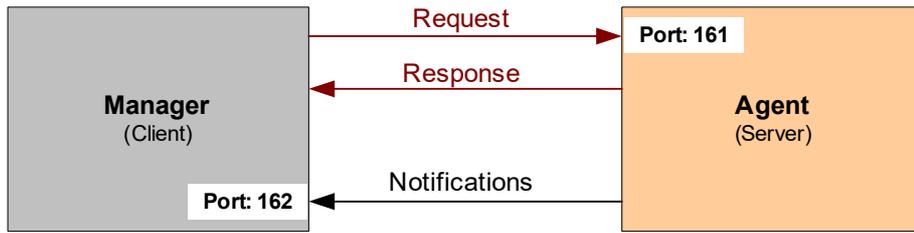
Simple Network Management Protocol (SNMP) is an application-layer protocol used for exchanging management information between network devices. Using SNMP, you can manage and monitor network elements, audit network usage, detect network faults or inappropriate network access.

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

This SNMP Configuration page is used for configuring Panel200 as an SNMP agent and to create Management Information Base (MIB) for SNMP.

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 the **Download MIB** button.
- 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* checkbox is unchecked.

SNMP Settings

The screenshot shows the 'SNMP Configuration' window with the 'SNMP Settings' tab selected. The 'Enable' checkbox is checked. The 'SNMP Listening Port' is set to 161. The 'SNMP Version' dropdown is set to SNMPv1. The 'System Name' dropdown is set to SNMPv1. The 'System Contact' dropdown is set to SNMPv2c. The 'System Location' field is empty. The 'Allow Access to SNMP Manager from' dropdown is set to Any IP Address. The 'Community Name' field is empty. The 'Download MIB' button is highlighted with a mouse cursor.

Enable: Select the checkbox to enable the SNMP settings. When it is enabled; system will process the incoming SNMP messages or outgoing messages.

SNMP Listening Port: It is the UDP port on which system starts listening for incoming SNMP messages. By default, Port is 161 which is standard UDP port assigned for SNMP.

SNMP Version: Select the desired SNMP version as the network infrastructure.

- SNMPv1- Trap message only (no need of acknowledgement).
- SNMPv2c- Trap and Information (acknowledgement required) message both.
- SNMPv3- Privacy enabled

For the SNMPv3, configure the 'Security Settings'. For the configuration, [See "Security Settings" on page 263.](#)

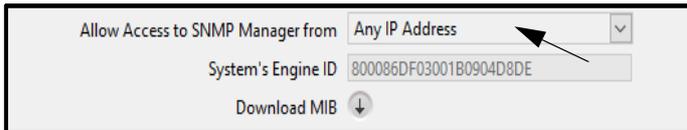
System Name: Enter the System Name which is useful in discovery process of the Agent for SNMPv1 and SNMPv2c. Maximum 40 characters are allowed.

System Contact: Enter the Contact information which is useful in discovery process of the Agent for SNMPv1 and SNMPv2c. Maximum 40 characters are allowed.

System Location: Enter the Location information which is useful in discovery process of the Agent for SNMPv1 and SNMPv2c. Maximum 40 characters are allowed.

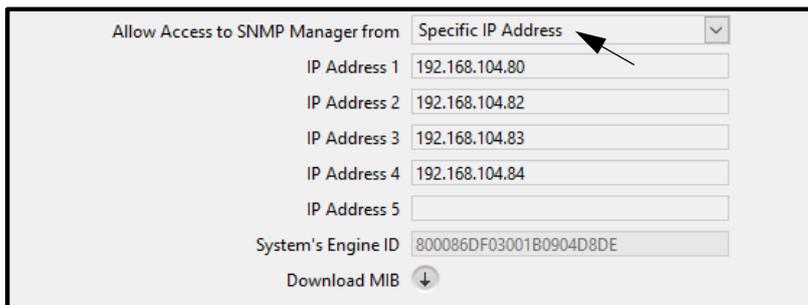
Allow Access to SNMP Manager from: You can Allow/Restrict accessibility of the SNMP Manager. You can select the option as **Any IP Address** or **Specific IP addresses** (specific Managers) to access the system.

- **Any IP Address:** If this option is selected, then any IP Address will be allowed to access the system (SNMP Server).



The screenshot shows a configuration panel titled "Allow Access to SNMP Manager from". A dropdown menu is set to "Any IP Address", indicated by a black arrow. Below it, the "System's Engine ID" is displayed as "800086DF03001B0904D8DE". At the bottom, there is a "Download MIB" button with a downward arrow icon.

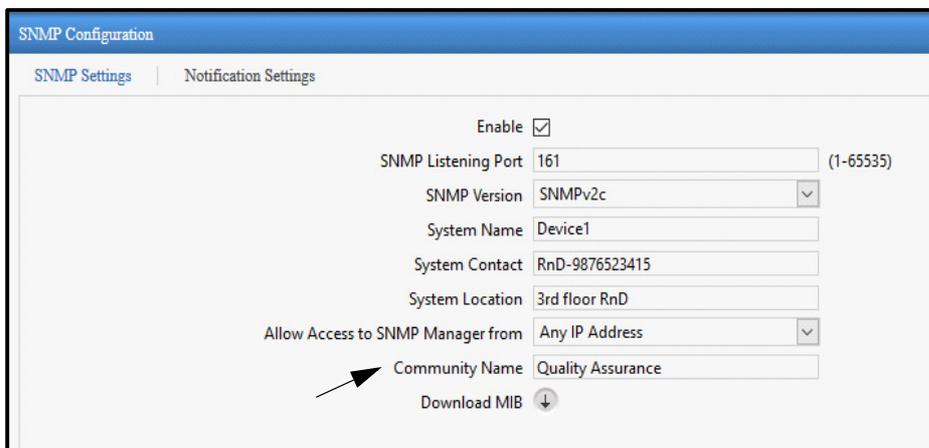
- **Specific IP Addresses:** If this option is selected, then system will process the incoming message only if received Source IP Address is from the configured Manager's IP Address in "**IP Address 1**" to "**IP Address 5**" field.



The screenshot shows the same configuration panel, but the dropdown menu is set to "Specific IP Address", indicated by a black arrow. Below the dropdown, there are five input fields labeled "IP Address 1" through "IP Address 5". The first four fields contain the IP addresses: 192.168.104.80, 192.168.104.82, 192.168.104.83, and 192.168.104.84. The fifth field is empty. The "System's Engine ID" remains "800086DF03001B0904D8DE". The "Download MIB" button is at the bottom.

This is applicable for **GetRequest**, **GetNextRequest**, **GetBulkRequest** only.

Community Name: This Community Name is used only for SNMPv1 and SNMPv2c and works as password. You have to enter this community name in manager login. It is used for both Read-only operations and Trap/Notification in SNMPv1 and SNMPv2c. The System will process the incoming message only when received Community matches with programmed Community String in the system. Maximum 40 characters are allowed.



The screenshot shows the "SNMP Configuration" window with two tabs: "SNMP Settings" and "Notification Settings". The "SNMP Settings" tab is active. It contains the following fields:

- Enable:
- SNMP Listening Port: 161 (1-65535)
- SNMP Version: SNMPv2c
- System Name: Device1
- System Contact: RnD-9876523415
- System Location: 3rd floor RnD
- Allow Access to SNMP Manager from: Any IP Address
- Community Name: Quality Assurance (indicated by a black arrow)
- Download MIB: button with downward arrow icon

System's Engine ID: It is a unique identification of the system when SNMPv3 is used. It is a hexadecimal field with length of 22 characters which is made up of Enterprise number and MAC address of the system.

The screenshot shows a configuration window for SNMP. At the top, there is a checkbox labeled 'Enable' which is checked. Below it are several input fields: 'SNMP Listening Port' with the value '161' and a small '(1-65535)' note to its right; 'SNMP Version' with a dropdown menu set to 'SNMPv3'; 'System Name' with the value 'Device2'; 'System Contact' with the value 'RnD-9876523415'; 'System Location' with the value '3rd floor RnD'; 'Allow Access to SNMP Manager from' with a dropdown menu set to 'Any IP Address'; and 'System's Engine ID' with the value '800086DF03001B0904D8DE'. An arrow points to the 'System's Engine ID' field. At the bottom, there is a 'Download MIB' button with a downward arrow icon.

Security Settings

The screenshot shows a 'Security Settings' window. It contains the following fields: 'User Name' (empty text box); 'Security Type' (dropdown menu set to 'No Authentication - No Privacy'); 'Authentication Algorithm' (radio buttons for 'MD5' and 'SHA', with 'MD5' selected); 'Authentication Password' (empty text box); 'Privacy Algorithm' (radio buttons for 'DES' and 'AES-128', with 'DES' selected); and 'Privacy Password' (empty text box).

User Name: The User Name is used for Authentication and Privacy in SNMPv3. It is used for both Read-only operations and Trap/Notification in SNMPv3. Maximum 40 characters are allowed.

Security Type: You can select from the following options:

1. No Authentication-No Privacy

This should be used when Authentication and Privacy is not required.

2. Authentication without Privacy

This should be used when only Authentication is required. Incoming SNMP Message should be authenticated in this case.

3. Authentication with Privacy

This should be used when both Authentication and Privacy is required. Incoming SNMP Message should be authenticated and encrypted-decrypted in this case.

Authentication Algorithm: It provides the option for message digest algorithm. When Security Type is selected as "Authentication without Privacy" or "Authentication with Privacy"; then you can select Authentication algorithm as:

- **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.

Authentication Password: It is a password used for Authentication with selected Authentication Type.

Privacy Algorithm: When Security Type is selected as “Authentication with Privacy”; then you can select Privacy algorithm as:

- **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: It is a password used for privacy with selected Privacy Type.

Click on the **Save** button to save the SNMP settings.

Notification Settings

Enable Notification: Select this check-box to enable or disable the Trap/Notification. If this check-box is enabled then system will generate Notification message (Trap/Inform) as per version selected and Notification Filter settings 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: Select the notification type as **Trap** or **Inform**. Notification Type is applicable only for SNMPv2c and SNMPv3.

- **Trap** is used when it is required to send notification message without acknowledgement.
- **Inform** is used when it is required to send notification message with acknowledgement. In this case if acknowledgment is not received then system will keep retransmitting Inform message as per Retry parameters.

Destination IP Address: It is the host IP Address i.e. IP address of SNMP Manager (Browser) where you want to receive Trap/Inform messages.

Destination Port: The Port is 162 which is standard UDP port assigned for SNMP Trap/Notification in the PC where SNMP Manager is installed.

Retry Attempts: It is applicable when Notification Type is selected as “**Inform**”. It specifies the number of times the system will retransmit the request if no acknowledge/response is received from Manager. This is applicable only for SNMPv2c and SNMPv3.

Retry Interval: It is applicable when Notification Type is selected as “**Inform**”.

This 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

System offers filters to send the Trap/Inform messages. Select the desired Filters:

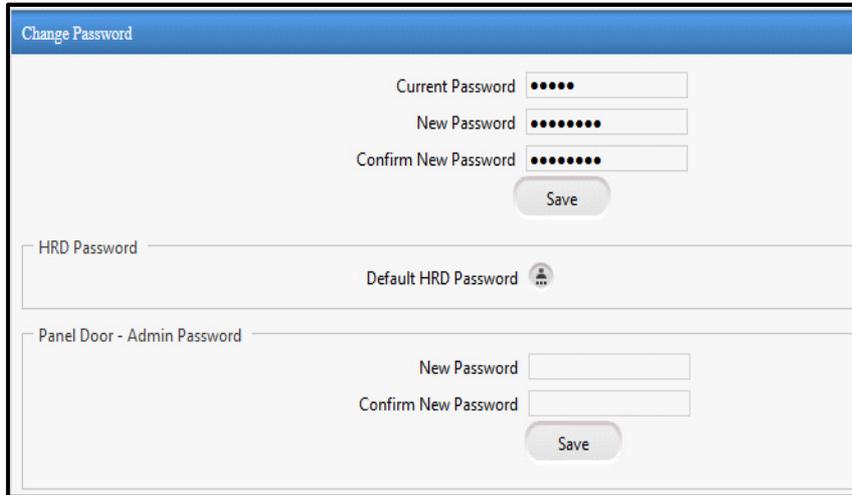
- Door Events
- Alarm Events
- System Events

Each filter option contains severity as:

- Information
- Warning
- Alarm

Change Password

The password of the device can be changed through Change Password tab.



Current Password: Specify the current password of the device.

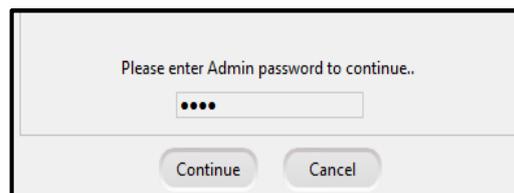
New Password: Enter the new password. The characters allowed are **A-Z a-z 0-9-_.comma:@!+/**

Confirm New Password: Re-enter the new password to confirm.

Click on the **Save** button to save the password.

HRD Password

The administrator can default the HRD password by clicking the Default HRD password icon.



Panel Door-Admin Password

The administrator can change the admin password of Panel Door by specifying new password here.

Panel Door - Admin Password

New Password

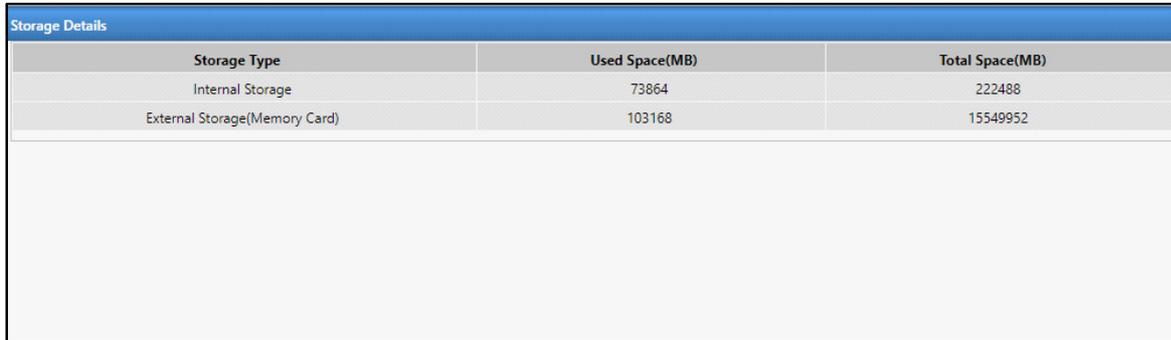
Confirm New Password

Click on the **Save** button to save the settings.

Storage Details

The Storage Details displays the status of internal storage of the Panel and external storage.

- Click **Configuration > 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.



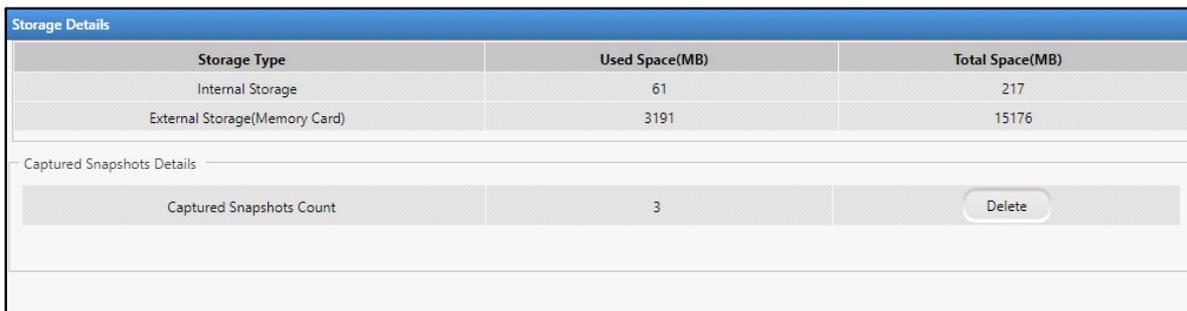
*Applicable when Panel is in Standalone Mode: On encountering 90% or above storage usage for External Storage, the **Device Storage** alert will be triggered, if configured. In [“Alert Message Configuration”](#), select Event Type as **System** and Event as **Device Storage**.*

Captured Snapshot Details



Captured Snapshot Details is applicable for Panel- Standalone Mode only.

The count of captured snapshots for user events if configured appears here.



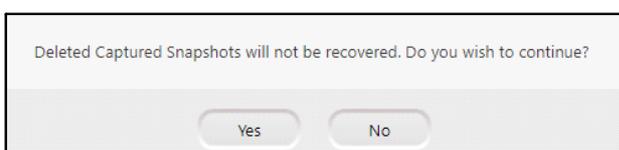
Storage Type	Used Space(MB)	Total Space(MB)
Internal Storage	61	217
External Storage(Memory Card)	3191	15176

Captured Snapshots Details

Captured Snapshots Count	3	Delete
--------------------------	---	--------

You can delete the snapshots, if required.

- Click **Delete** to delete the captured snapshots. The following pop-up appears.



Deleted Captured Snapshots will not be recovered. Do you wish to continue?

Yes No

- Click **Yes** to confirm or click **No** to discard.

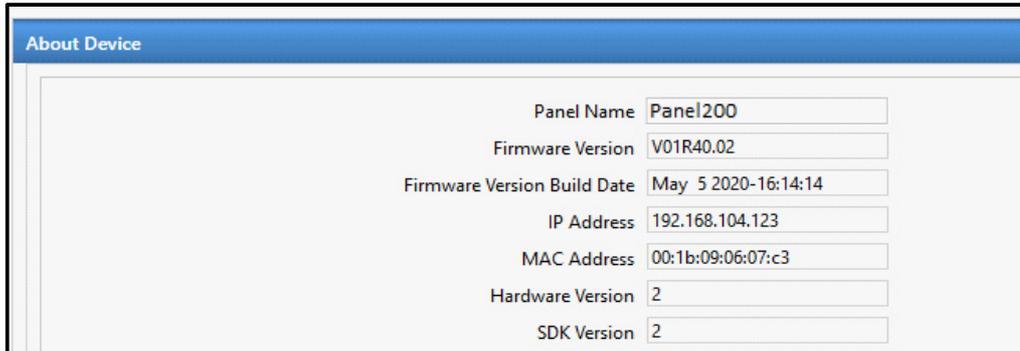


All the captured snapshots will be deleted automatically when:

- *the Panel mode is changed.*
- *the Panel is set to system/factory default.*

About Device

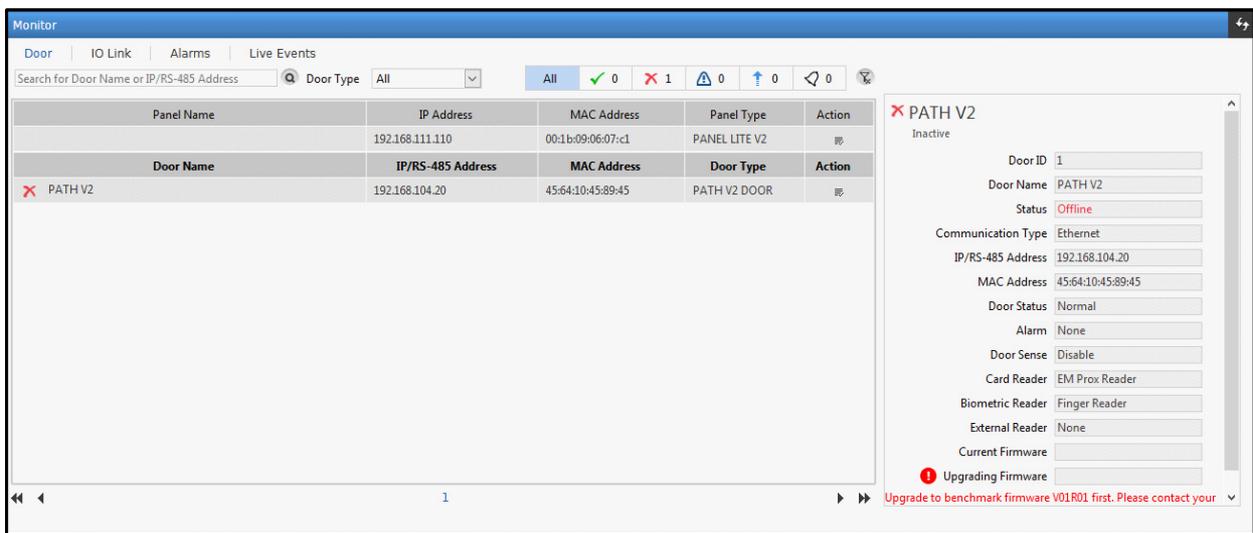
The About Device page shows the name of panel, firmware version available in Panel200, last build date of firmware, IP Address, MAC address, Hardware version and SDK version of Panel200.



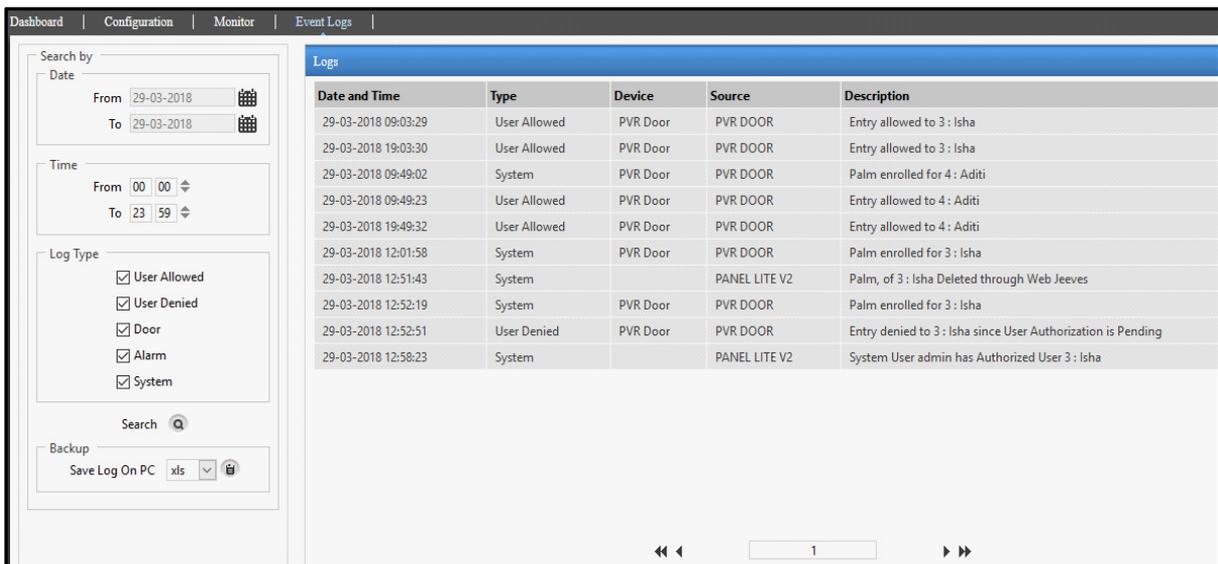
The screenshot displays the 'About Device' page with the following information:

Field	Value
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 Monitor displays the Door status as Online Devices, Offline Devices, Devices in Degrade State, Upgrading Devices and Alarms on Devices. You can also perform different actions on the doors from the monitor.



The log of different events is displayed on Event Log page.



Monitor

Door

Door Selection

The door can be searched by entering the Door Name or its IP/RS-485 address in Search field. The door can also be searched by selecting the Door type from the drop down list.

The screenshot shows the 'Monitor' page in a web interface. At the top, there are navigation tabs: Dashboard, Configuration, Monitor (selected), Event Logs, and System Logs. The 'Monitor' page has sub-tabs: Door, IO Link, Alarms, Live Events, and Time Trigger. Below these is a search bar for 'Door Name or IP/RS-485 Address' and a 'Door Type' dropdown menu set to 'All'. A status bar shows 'All' with a green checkmark, '5' devices, '0' offline devices, '2' in degrade state, '0' upgrading devices, and '0' alarms. The main table lists several doors with columns for Panel Name, IP Address, MAC Address, Panel Type, and Action. A detailed view of the selected device 'PATH V2 DOOR-00:1b:09:0d:1b:e5' is shown on the right, displaying its status as 'Active' and various configuration details.

Panel Name	IP Address	MAC Address	Panel Type	Action
Riddhi	192.168.103.222	00:1b:09:0b:bd:86	COSEC PANEL200	
Door Name	IP/RS-485 Address	MAC Address	Door Type	Action
ARC DC 200-00:1b:09:07:ca:93	192.168.103.158	00:1b:09:07:ca:93	ARC DC 200	
ARGO FACE DOOR-00:1b:09:0a:6f:71	192.168.103.63	00:1b:09:0a:6f:71	ARGO FACE DOOR	
PATH V2 DOOR-00:1b:09:0d:1b:e5	192.168.103.86	00:1b:09:0d:1b:e5	PATH V2 DOOR	
ARC DC 200 DD DR 1	192.168.103.180	00:1b:09:06:07:b2	ARC DC 200	
ARC DC 200 DD DR 2	192.168.103.180	00:1b:09:06:07:b2	ARC DC 200	
ARC DC200 DDSR	192.168.103.45	00:1a:15:20:dcae	ARC DC 200	
ARC SC200 DDSR	192.168.103.45	00:1a:15:20:dcae	ARC DC 200	

Details for PATH V2 DOOR-00:1b:09:0d:1b:e5:

- Active
- Door ID: 4
- Door Name: PATH V2 DOOR-00:1b:09:0d:1b:e5
- Status: Online
- Communication Type: Ethernet
- IP/RS-485 Address: 192.168.103.86
- MAC Address: 00:1b:09:0d:1b:e5
- Door Status: Normal
- Alarm: None
- Door Sense: Disable
- Card Reader: EM Prox Reader
- Biometric Reader: Finger Reader
- External Reader: None
- Current Firmware: V01R34.00
- Upgrading Firmware: V01R34.00

The right side on the Door page displays the details of device. To view details of the device, hover the mouse over the device.

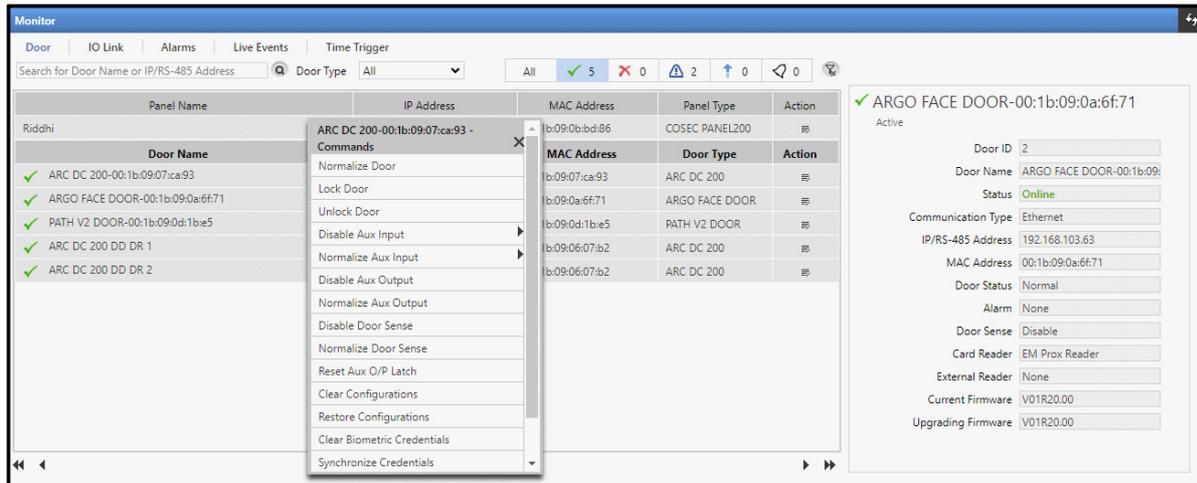
The devices can also be filtered on the basis of their Status. Click on the desired icon - **Online Devices** , **Offline Devices** , **Devices in Degrade State** , **Upgrading Device** , **Alarms on Device** .

By default All Devices are selected and displayed in the list.

The **count** of the different door status represents the total number of doors belonging to the respective status.

The filter can be cleared by clicking on **Clear Filter** button.

Action: Click on the **Select Command** under Action. The list of commands are displayed. You can select the desired command to be executed by the device:



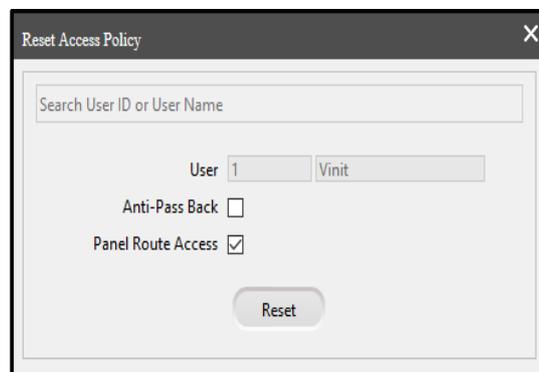
Click the **Select Command** button under Action to send the command to the Panel200. You can **Reset Aux O/P Latch, Reboot Device, Reset Access Policy** and **Reset Anti-Pass Back** by selecting the respective commands.



*Different devices have different sets of commands in **Select Command**.*

When user violates an access policy he/she is denied access to the Panel200 if hard violation is configured for access policies So you can Reset the Access policy to allow access to the user.

When Reset Access Policy is selected; then Reset Access Policy page appears as shown below.



Enter the User ID/Name in Search field. Once the user is selected, you can enable Anti-Pass Back and/or Panel Route Access to reset.

Anti-Pass Back:

- For APB; if user's last punch is Entry punch on device and then APB is reset for that user then user's punch status will become unknown.
- User will be allowed to mark Entry/ Exit punch without considering prior punch. After Entry/ Exit punch APB will work as before.
- Also, whenever APB is reset for any user Occupancy of Device will not be increased/ decreased at that moment. When user punches on device after resetting APB if Entry Punch is found then Occupancy will be increased and if Out Punch is found then Occupancy will be decreased.

Panel Route Access:

- Whenever Panel Route Access is reset; 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.

IO Link

All types of active IO Links configured on the device can be viewed here with name and output type. User can reset only the "Latch" type of IO Links. By default, this page is available only to a user with administrator rights.

Alarms

The Alarm tab displays list of various alarms (which have been activated) with their details. It also provides the user with the option to acknowledge or clear these reported alarms.



For generating Alarm, the Alarm must be enabled from Advance Profile and Door Configuration.

The list displays:

- Date and Time at which the alarm is generated with the description of Alarm.
- Category of the alarm and status.
- To acknowledge the alarm, click the button under Acknowledge column of the respective alarm.
- To clear the alarm, click the button under Clear column of the respective alarm.
- Click **Acknowledge All** button, to acknowledge all the alarms and Click **Clear All** to clear all the alarms.

The example of Critical Alarm is shown below.

Dashboard Configuration Monitor									
Monitor									
Door	IO Link	Alarms							
Sr. No.	Date	Time	Source	Description	Category	Status	Acknowledge	Clear	
1	22-05-2018	14:06:18	Door V3 as Panel Door	Dead Man Zone	Critical	Acknowledged			

Monitor									
Door		IO Link		Alarms		Live Events			
Sr. No.	Date	Time	Source	Description	Category	Status	Acknowledge	Clear	
1	02-01-2018	16:34:29	PVR 113	DC Offline	Major	New			

Monitor									
Door		IO Link		Alarms		Live Events			
Sr. No.	Date	Time	Source	Description	Category	Status	Acknowledge	Clear	
1	02-01-2018	16:34:29	PVR 113	DC Offline	Major	Acknowledged			

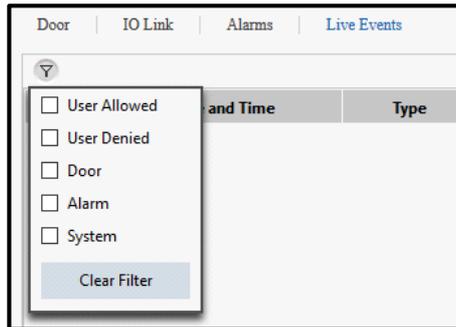
Monitor									
Door		IO Link		Alarms		Live Events			
Sr. No.	Date	Time	Source	Description	Category	Status	Acknowledge	Clear	
1	02-01-2018	16:35:18	PVR 113	DC Tamper	Critical	Acknowledged			

Live Events

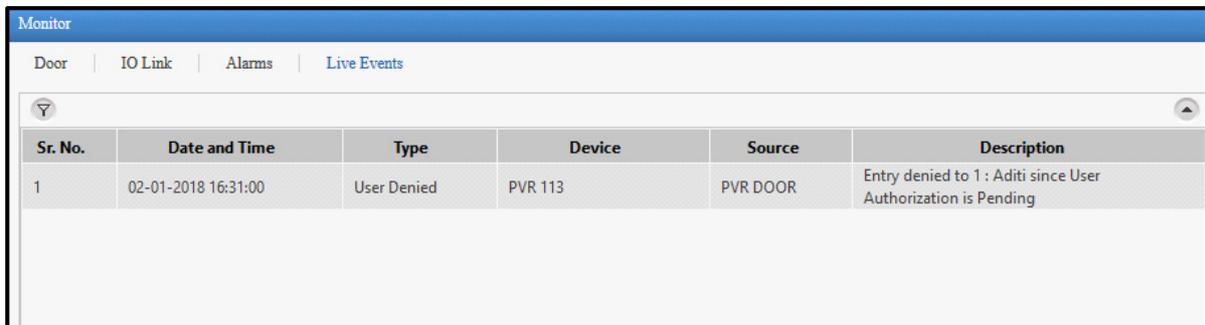
Live Events page enables you to view the events occurring at device end. The events are automatically updated in every 3 second.

Filter

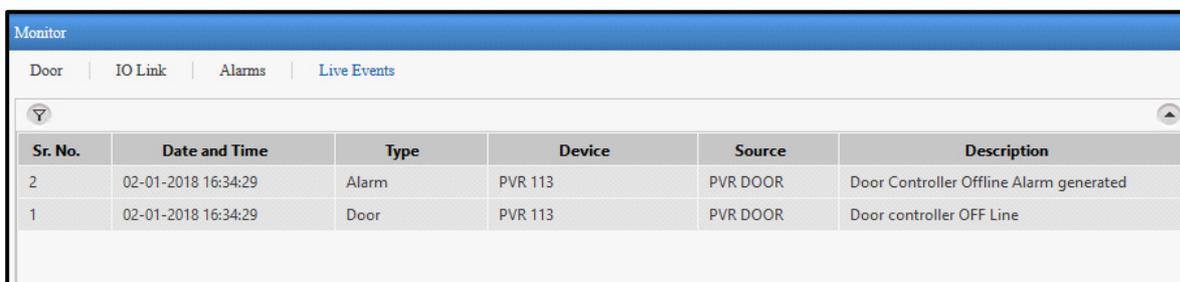
To view a particular type of event on the Live Events page, click the Filter and select the checkbox for the respective event.



The relevant events will appear in the list. The details of events like Date and Time, event type, device, source and description will be displayed.



Sr. No.	Date and Time	Type	Device	Source	Description
1	02-01-2018 16:31:00	User Denied	PVR 113	PVR DOOR	Entry denied to 1 : Aditi since User Authorization is Pending

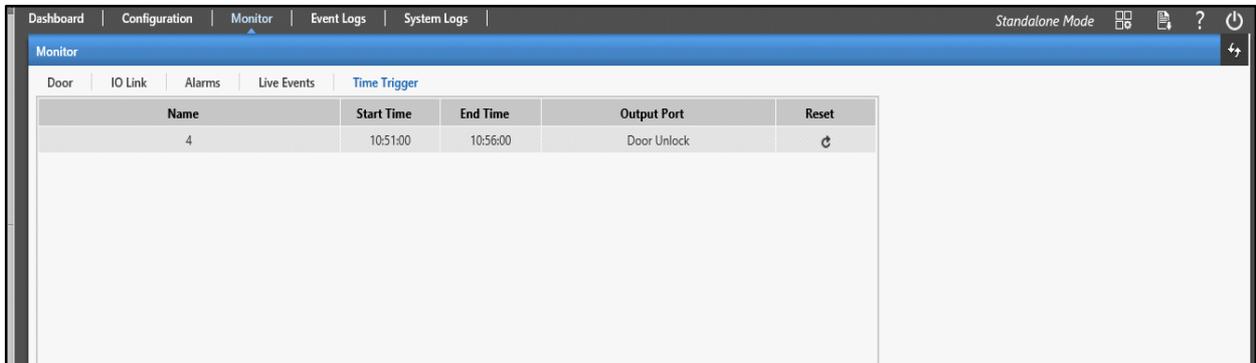


Sr. No.	Date and Time	Type	Device	Source	Description
2	02-01-2018 16:34:29	Alarm	PVR 113	PVR DOOR	Door Controller Offline Alarm generated
1	02-01-2018 16:34:29	Door	PVR 113	PVR DOOR	Door controller OFF Line

Click on the Manual Refresh button to get new live events as per the selected filter.

Time Trigger

Time Trigger function enables user to monitor all types of Time Triggered functions such as Locking/Unlocking of the door as per the predefined time duration, Activation/Deactivation of the alarms etc; which are configured at the device end. User can view the Name, Start time, End time as well as the Output Port of the configured Time Trigger function.



Name	Start Time	End Time	Output Port	Reset
4	10:51:00	10:56:00	Door Unlock	↻

Click on the **Reset** button to reset the respective Time Triggered Function.

Event Logs

Event Log maintains the record 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.



Event Logs are configurable only when the Panel is in Standalone Mode. (Configuration > Basic Profile > Panel Mode)

The screenshot displays the Event Logs interface. On the left, there are search filters for Date, Time, and Log Type. The Date filter is set to 'From 20-06-2024' and 'To 20-06-2024'. The Time filter is set to 'From 00:00' and 'To 23:59'. The Log Type filter has checkboxes for 'User Allowed', 'User Denied', 'Door', 'Alarm', and 'System', all of which are checked. Below the filters is a 'Search' button and a 'Backup' section with a 'Save Log On PC' button and a file format dropdown set to 'xls'. On the right, a table titled 'Logs' displays the following data:

Date and Time	Type	Device	Source	Description
20-06-2024 15:58:49	System		COSEC PANEL200	Master Controller Power ON
20-06-2024 15:58:55	System		COSEC PANEL200	Update of Firmware Successful
20-06-2024 15:58:55	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Entry allowed using Card to 2959 : Jaldeep
20-06-2024 15:59:48	Door	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Door controller ON Line
20-06-2024 16:07:10	System		COSEC PANEL200	Master Controller Power ON
20-06-2024 16:07:16	System		COSEC PANEL200	Update of Firmware Successful
20-06-2024 16:07:16	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Exit allowed using Card to 2959 : Jaldeep
20-06-2024 16:08:09	Door	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Door controller ON Line
20-06-2024 17:02:15	System		COSEC PANEL200	Master Controller Power ON
20-06-2024 17:02:22	System		COSEC PANEL200	Update of Firmware Successful
20-06-2024 17:03:15	Door	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Door controller ON Line
20-06-2024 17:14:13	System		COSEC PANEL200	Master Controller Power ON
20-06-2024 17:14:19	System		COSEC PANEL200	Update of Firmware Successful
20-06-2024 17:15:13	Door	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Door controller ON Line
20-06-2024 17:20:24	Door	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Door controller OFF Line

Search by

Date

- **From:** Select the date from which you wish to view the Event Logs from the calendar.
- **To:** Select the date till which you wish to view the Event Logs from the calendar.

Time

- **From:** Specify the time from which you wish to view the Event Logs for the selected dates.
- **To:** Specify the time till which you wish to view the Event Logs for the selected dates.

Log Type

Select the check boxes for the desired Log Type for which you wish to view the Event Logs.

Click the **Search** button to search for the Event Logs for the configured Date, Time and Log Type. The Event Logs appear in a grid.

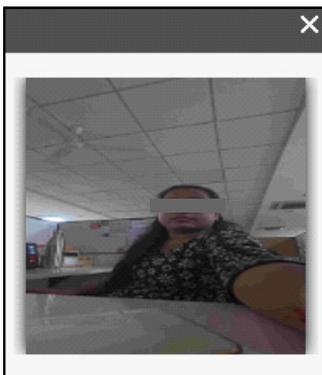
Search by		Logs				
Date		Date and Time	Type	Device	Source	Description
From	18-06-2024	19-06-2024 12:55:16	System		COSEC PANEL200	Master Controller Power ON
To	20-06-2024	19-06-2024 12:55:16	System		COSEC PANEL200	System Defaulted from ACMS
Time		19-06-2024 12:58:55	Door	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Door controller ON Line
From	00 00	19-06-2024 13:03:12	System		COSEC PANEL200	Master Controller Power ON
To	23 59	19-06-2024 13:03:19	System		COSEC PANEL200	Update of Firmware Successful
Log Type		19-06-2024 13:03:19	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Entry allowed using Pin to 2959 : Jaldeep
<input checked="" type="checkbox"/> User Allowed		19-06-2024 13:03:19	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Entry allowed using Card1 to 2959 : Jaldeep
<input checked="" type="checkbox"/> User Denied		19-06-2024 13:03:19	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Entry allowed using Pin + Card1 to 2959 : Jaldeep
<input checked="" type="checkbox"/> Door		19-06-2024 13:03:19	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Entry allowed using Finger to 2959 : Jaldeep
<input checked="" type="checkbox"/> Alarm		19-06-2024 13:03:19	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Entry allowed using Pin + Finger to 2959 : Jaldeep
<input checked="" type="checkbox"/> System		19-06-2024 13:03:19	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Entry allowed using Card1 + Finger to 2959 : Jaldeep
Search		19-06-2024 13:03:19	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Entry allowed using Palm to 2959 : Jaldeep
Backup		19-06-2024 13:03:19	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Entry allowed using Pin + Palm to 2959 : Jaldeep
Save Log On PC	xls	19-06-2024 13:03:19	User Allowed	VEGA DOOR-00:1b:09:09:5c:96	VEGA DOOR	Entry allowed using Pin + Card1 + Palm to 2959 : Jaldeep

The details displayed are — Date and Time, Type, Device, Source, Description and Snapshot Image .



The Snapshot Image Icon will appear enabled only for Captured Snapshot events and is applicable for Panel- Standalone Mode only.

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.*

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 on the button to **Save** the file on desired location of the PC.

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 \(osdp_SCRYPT\)”](#)

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 14 bytes repeated 1 or more times.	0x00 = First Reader 0x01 = Second Reader etc.	Reader Number	
	0x00 = first LED 0x01 = second LED 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 A zero value means no duration
	0x00 – 0xFF	OFF time	An 8 bit OFF duration of the flash, in units of 100 ms A zero value means no duration
	Refer to "Color Values"	ON color	The color to set during the ON time
DATA 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 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 A zero value means no duration
	0x00 – 0xFF	OFF time	An 8 bit OFF duration of the flash, in units of 100 ms 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:

- osdp_ACK as described in [“Positive Acknowledgment \(osdp_ACK\)”](#)
- osdp_NAK as described in [“Negative Acknowledgment \(osdp_NAK\)”](#)

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 5 bytes repeated 1 or more times.	0x00 = First Reader 0x01 = Second Reader etc.	Reader Number	
	0x00 = no tone (off) – use of this value is deprecated. 0x01 = off 0x02 = default tone 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 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 "Error Codes"	Error Code	Refer to "Error Codes"
	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 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 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 The Model field is assigned by and managed by the Vendor.
	0x00 – 0xFF	Version	Manufacturer's version of this product The Version Number field is assigned by and managed by the Vendor.
	0x00 – 0xFF	Serial Number (LSB)	4-byte serial number 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 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 " Function Codes ".
	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 0x01 – tamper	Tamper Status	Status of tamper circuit
	0x00 – normal 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 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.

The key encoding uses the following data representation:

- Digits 0 through 9 are reported as ASCII characters 0x30 through 0x39
- The clear/delete/'*' key is reported as ASCII DELETE, 0x7F
- The enter/'#' key is reported as ASCII return, 0x0D

Special/function keys are reported as upper case ASCII:

- A or F1 = 0x41, B or F2 = 0x42, C or F3 = 0x43, D or F4 = 0x44
- F1 & F2 = 0x45, F2 & F3 = 0x46, F3 & F4 = 0x47, F1 & F4 = 0x48

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

General	
Maximum Door Controllers	255
Users	25,000
Event Buffers	500,000
Door Type Support	COSEC ARC Series, COSEC PATH Series, COSEC VEGA Series, COSEC DOOR PVR, COSEC DOOR FOP, COSEC ARGO Series, COSEC ARGO FACE Series.

Communication	
Communication Port	Ethernet & RS-485
Ethernet	Yes (255 Door Controllers on Ethernet) 10/100 Mbps
Mobile Broadband	Yes (Dongle Required)
RS-485	Yes (32 Door Controllers on RS-485)
Wi-Fi	Yes (Dongle Required) Inbuilt Wi-Fi Module (IEEE 802.11 b/g/n)
USB	One USB Port (for Data Transfer and for 2G-3G-4G /Wi-Fi Dongle)
SD Card	Yes (8GB)
Inbuilt Bluetooth	Yes

Operation Mode	
Server Mode	For Advanced Features and Capacity Enhancement for Access Control and Connected with COSEC CENTRA
Standalone Mode	Built-in GUI to control Matrix Door Controllers and Users

Software & Hardware	
Software	Built-In Interface in a Standalone Mode with Matrix Door Controllers
CPU	Cortex A8 800 MHz
Flash Memory	256 MB
RAM Memory	256 MB (DDR3 SDRAM @ 800Mhz)
Operating System	Linux based OS
Tamper detection	Yes
RTC	Yes

IN/OUT Port	
AUX -OUT Port	30V DC @ 1A, Form C, SPDT Relay Output
AUX- IN Port	Programmable NO, NC, Supervised (4 states-short, open, activated & non-activated)

Audio-Visual	
LED	Tricolor LED for Power, Status and Alarm
Buzzer	Yes

Physical	
Mounting	Wall or Table Top
Dimensions (W x H x D)	81mm x 125mm x 32.5mm
Input Power	External Power Adapter (12V DC @ 2A)
Weight	135 g (approx.)
Enclosure Material	ABS V0 Grade
Package Contents	1. Main unit 2. Adapter (12VDC, 2A) 3. SD Card (8GB)

Environmental	
Humidity	5% to 90% RH Non-Condensing
Operating Temperature	0°C to + 45°C

Compatibility	
System Integration	API For Software Integration
Architecture	1. Network Architecture - With COSEC CENTRA/VYOM 2. Standalone Architecture

Certification	
FCC, CE, IEC, RoHS, Environment Test	



Due to continuous technology upgradations, product specifications are subject to change without notice.

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

www.matrixcomsec.com