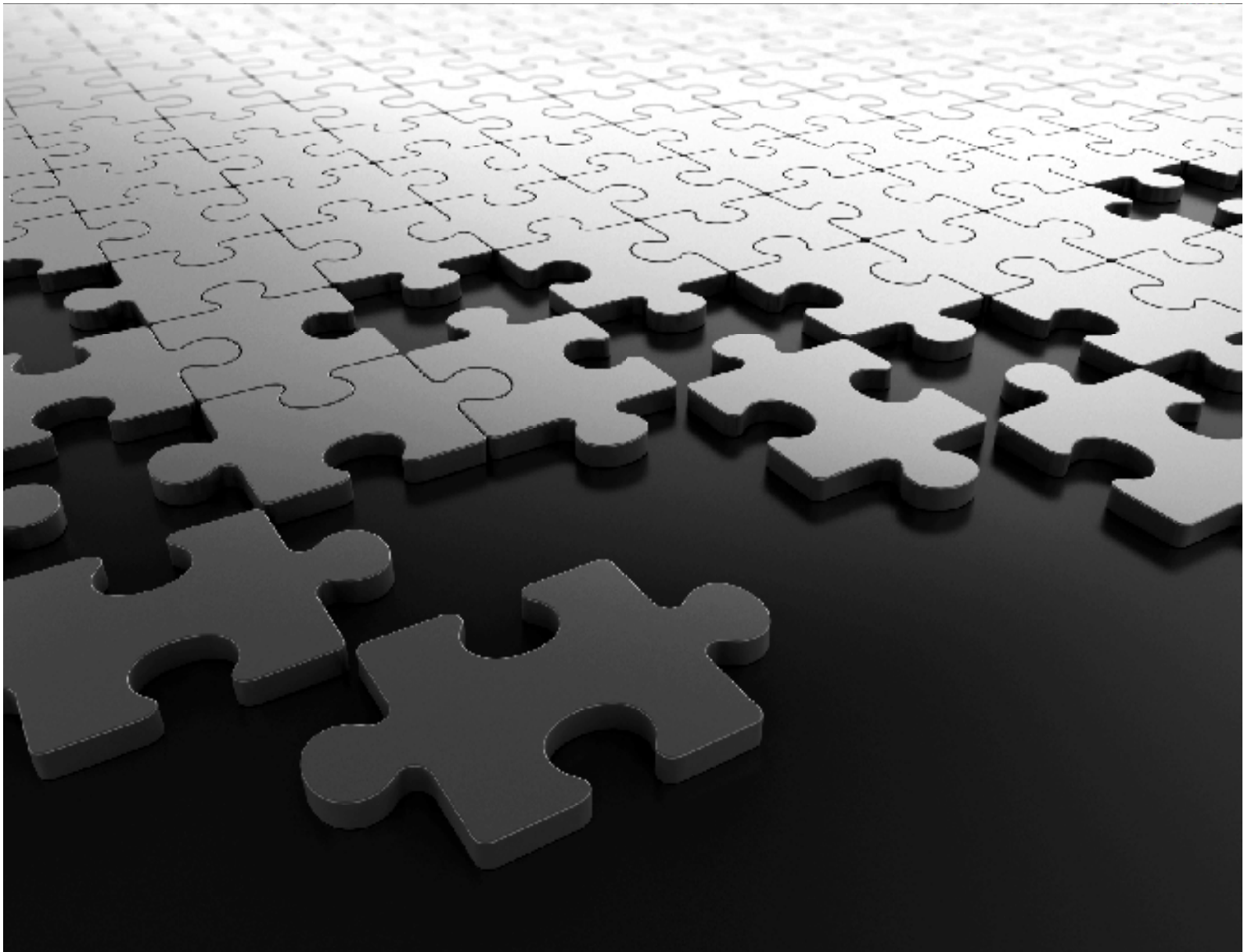


COSEC Panel Lite System Manual



COSEC Panel Lite V2

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:
<http://www.matrixcomsec.com/product-registration-form.html>

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 14

Release date: March 19, 2019

Contents

Introduction	1
Panel Configuration	5
<i>Basic Profile</i>	7
<i>Advanced Profile</i>	12
<i>Access Features</i>	21
<i>Special Functions</i>	27
<i>Input Output</i>	29
<i>Zone Configuration</i>	33
<i>Man Trap Door Group</i>	41
<i>Network Settings</i>	43
<i>Date and Time</i>	53
Devices	55
<i>Door Configuration</i>	56
<i>Door Group</i>	64
<i>Video Surveillance</i>	66
<i>Card Format</i>	68
<i>Card Personalization</i>	70
<i>Wiegand Format</i>	73
Users	75
<i>User Configuration</i>	76
<i>Access Group</i>	82
<i>Functional Group</i>	85
<i>Blocked User</i>	86
<i>User</i>	88
<i>SI User</i>	91
<i>Special Card</i>	93
<i>Authorization</i>	94
Access Policies & Access Schedule	97
<i>2-Person Rule</i>	98
<i>Access Route</i>	101
<i>First-IN User Rule</i>	105
<i>Smart Card Access Route</i>	107
<i>Time Zone</i>	109
<i>Access Cluster</i>	112
<i>Occupancy Control</i>	115

<i>Shifts and Schedules</i>	120
<i>Holiday Schedule</i>	125
System Maintenance & About	127
<i>System Maintenance</i>	128
<i>About Device</i>	136
Elevator Access Control & Multi level Access	137
<i>Elevator Configuration</i>	139
<i>Elevator Floor Group</i>	143
<i>Multi-Level Access</i>	147
Import, Export, Report	151
<i>Import</i>	152
<i>Export</i>	154
<i>Reports</i>	158
Alerts	165
<i>Alert Message Configuration</i>	166
<i>Alert Server Configuration</i>	169
Managing User Account and Password	173
<i>Users</i>	174
<i>Password Policy</i>	176
<i>Change Password</i>	177
SNMP Configuration	179
<i>SNMP Configuration</i>	180
Monitor & Event Log	185
<i>Monitor</i>	186
<i>Event Logs</i>	192

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 rich, Integrated Access Control and Time and Attendance system. Please read this document carefully to get acquainted with the product before installing and operating it.

About this System Manual

This is a common document providing detailed information and instructions for installing and configuring the COSEC Access Control System hardware components as well as the software installation and configuration of the COSEC application. This manual includes sufficient information to install and configure all the components of the Matrix COSEC Access Control System.

The COSEC application is a powerful web based multi-user Access Control cum Time and Attendance system that provides all the features required for medium to large size enterprises. A host of modules are available making the COSEC application a comprehensive, menu-driven software application.

This system manual is a common documentation for all variants of COSEC Controllers - PANEL, DOOR Controllers and their variants. This document is primarily for the hardware and software installation and configuration of the COSEC application components. This manual also includes sufficient information to install and interconnect the controllers on various network topologies. This manual must be read, and its contents clearly understood, before proceeding with any work relating to the COSEC Web Application.

Intended Audience

This System Manual is aimed at:

- **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.
- **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.

- **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 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 Panel lite.
- **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 Panel lite.
- **Event Log**- gives the log of events based on different search criterias.

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 PANEL-LITE 2**, **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.



In general Vega Panel-Lite is interchangeably referred as Panel-lite.

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.

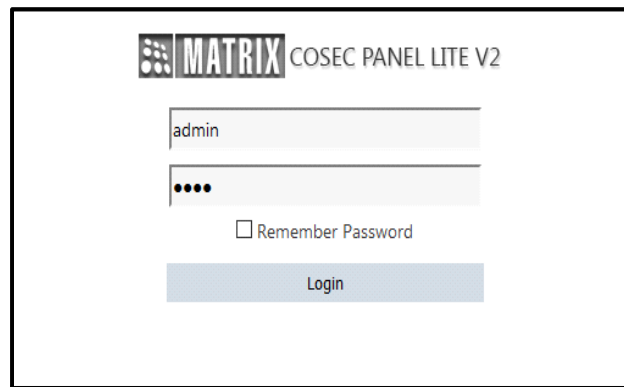
If you need additional information or technical assistance with the COSEC system and other Matrix products, contact our Technical Support Help desk, Monday to Saturday 9:00 AM to 6:00 PM (GMT +5:30) except company holidays.

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

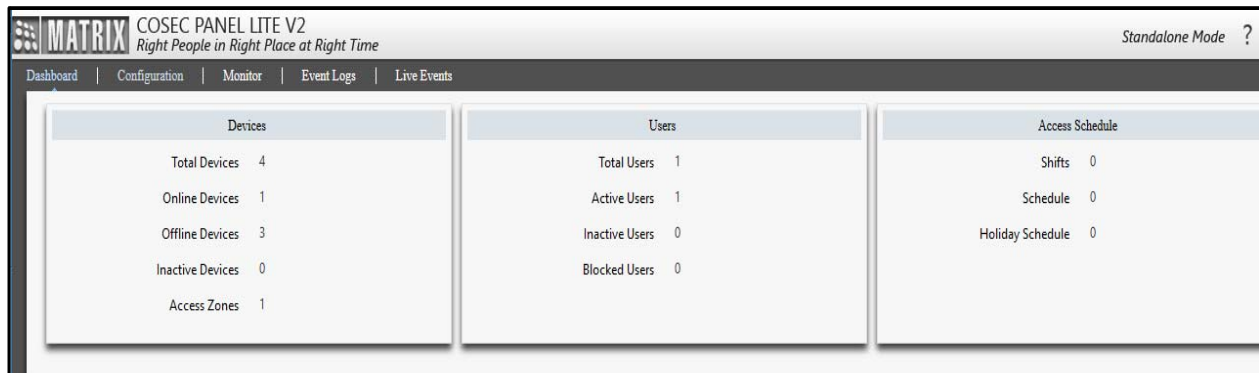


The terms **Panel**, **Panel lite** and **Panel lite V2** are used alternately to refer to **Panel Lite V2** in this manual. The Panel Lite V2 in Standalone Mode is called as Standalone Panel Lite.

The COSEC Panel Lite V2 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 panel lite V2 using default IP in the browser.



Then enter the login credentials for Panel lite V2: Default Username: **Admin**; User defined Password.



Changing Network Configuration

To change the IP address of Panel lite V2; Go to Configuration> Panel Configuration> Network Settings. See *Network Settings for details*.

Changing Panel Mode

To change the mode of Panel Lite V2; Go to Configuration> Panel Configuration> Basic Profile> Panel Mode. The default mode is Standalone Mode.

When you switch to Server Mode; then Server address is to be specified where the Panel lite V2 is to be added.



The Panel lite will reboot when the mode is changed.

Basic Profile

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



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

General

The screenshot shows a web-based configuration interface for a 'Basic Profile'. The interface has a blue header with the title 'Basic Profile' and a navigation bar with tabs: 'General', 'Access Settings', 'Multi-Language', 'Display', and 'Panel Mode'. The 'General' tab is active. The configuration area contains several fields: 'Panel Name' is a text input with 'QA Panel lite'; 'SD Card Status' is a dropdown menu showing 'Normal'; 'Template Per Finger' is a dropdown menu showing 'Single Template/Finger'; 'Max. No. of Fingers Per User' is a dropdown menu showing 'Two'; 'Max. No. of Palms Per User' is a dropdown menu showing 'Ten'; 'Run PVR Door in Guide Mode' is a checkbox; 'Auto Clear Alarm' is a checkbox; 'Alarm Clear Timer' is a text input with '10' and a unit 'sec(10-65535)'; and 'Override IO Linking and Time Triggered during Disarm' is a checkbox.

Panel Name: Enter a unique name for the Panel lite.

SD Card Status: This displays whether the SD card is connected or not.



Do not remove the SD card for proper functioning of panel lite.

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

Max. No. of Fingers/Palms Per User: Select the maximum number of fingers/palms 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.

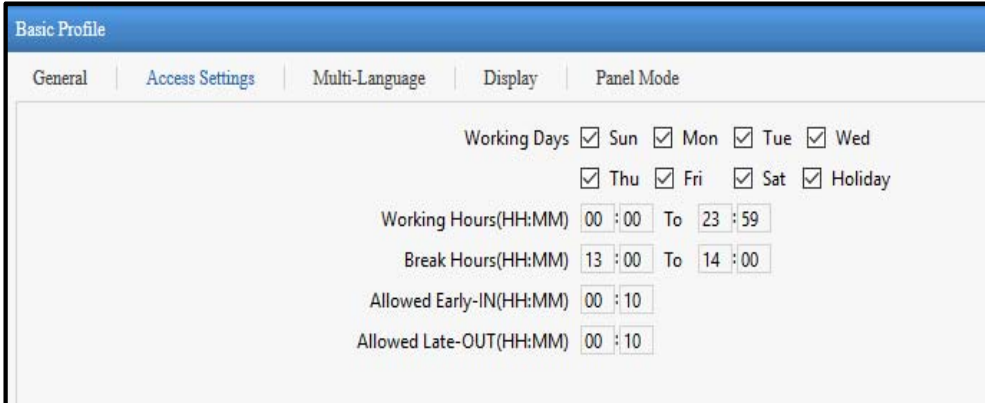
Enable this option to remove all existing palm templates from the Panel Lite and for all future palm enrollment and identification to be performed in the Guide mode only.

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.

Access Settings

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



The screenshot shows the 'Basic Profile' configuration interface. The 'Access Settings' tab is active. Under 'Working Days', all days (Sun, Mon, Tue, Wed, Thu, Fri, Sat, Holiday) are checked. The 'Working Hours(HH:MM)' field is set to 00:00 To 23:59. The 'Break Hours(HH:MM)' field is set to 13:00 To 14:00. The 'Allowed Early-IN(HH:MM)' field is set to 00:10. The 'Allowed Late-OUT(HH:MM)' field is set to 00:10.

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 feature can be configured from the webpage of Panel lite v2 which will sync the same to all applicable panel doors.

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

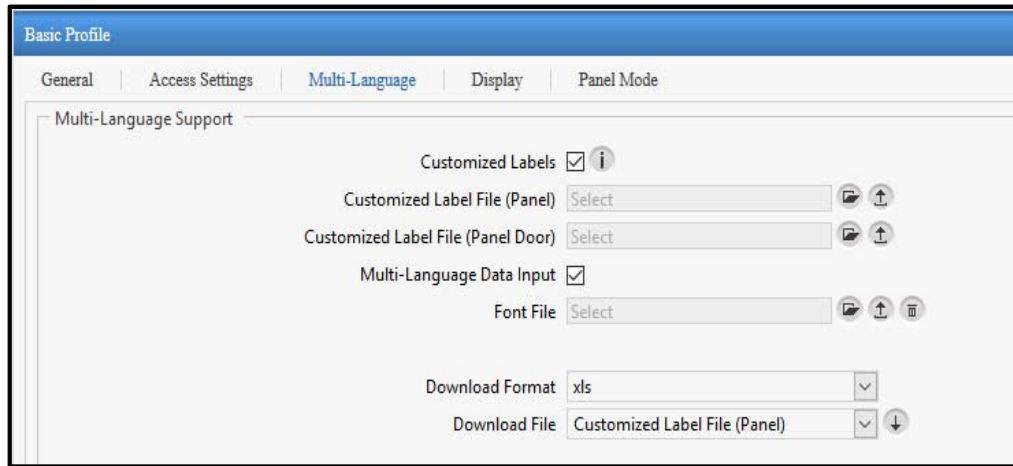
You can enter the custom messages in the desired languages for the variants of panel door [DMD & vega separately] and upload the file. After successful uploading of file, Panel lite will sync the Labels to the respective panel doors.



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 panel lite'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: Check this box 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.
For eg: Select the Sample String File (Panel Door) and Click the download button to download the sample string file for panel door.



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

Display

Basic Profile

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

Enable Display Messages

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

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

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

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

Enable Display Messages: This feature allows the user to enable display messages on door controllers assigned to the panel lite. 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 can function as standalone Panel lite when Standalone Mode is selected.

Basic Profile

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

Panel Mode

Server Mode
 Standalone Mode

Encryption

Encryption Mode

Server/Standalone Mode: Select the appropriate option to switch between the Server and Standalone Modes. The Server mode should be enabled only if the Panel Lite is to be configured using COSEC server application.



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

Encryption Mode: Enable the Encryption mode checkbox to establish secure HTTPS connection between client-server.

Click **Save** to apply the changes.

Advanced Profile

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

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 API

API Entry Access Mode API ONLY

Save Cancel

Generate Events: This check-box 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 Panel Lite V2. 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.

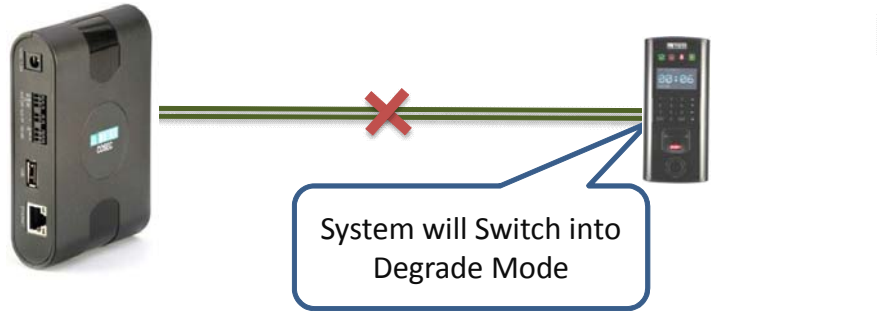
Generate Exit Switch Events: Check this box to enable Panel Doors to generate events for the inputs from the Exit Switch. The exit switch events will be generated when the mode is either exit or both.

Generate Invalid User Events: Check this box 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 Panel Lite. Check this box to enable this feature at the panel level.

- **Degraded Wait Timer (sec):** Specify the time period in seconds before the door controller switches from Network Fault to DEGRADE MODE. The default value is 5 sec.
- The Master controller (here Panel lite V2) 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 Panel lite as Offline, then Door will start the

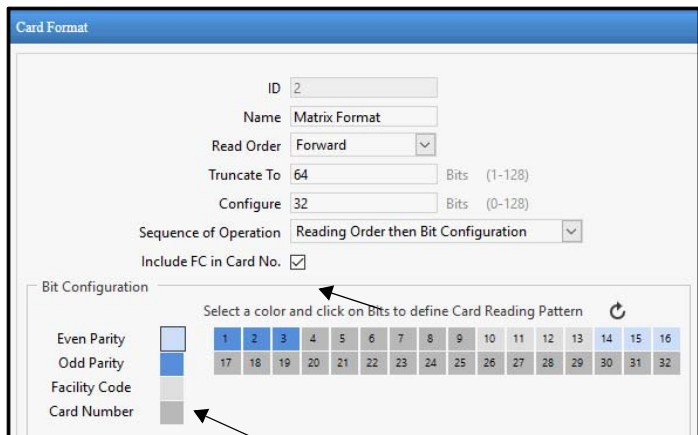
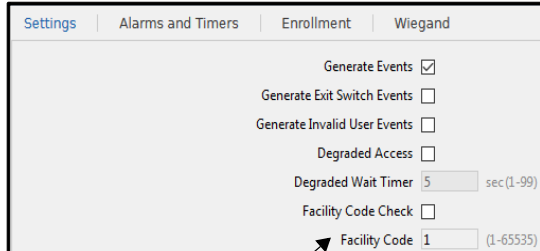
“Degrade wait timer”. If Panel lite does not changes its state to Online before expiry of degrade wait timer, then the Door Controller changes its mode to “Degraded Mode”.



Facility Code Check: Check this box 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 attempted. 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: In order to keep Additional level of security check other than Facility code and card number check, smart cards can be written with additional security code (ASC) that takes security to the next higher level.

- This Additional Security Check is possible only with Smart Cards which will prevent the duplicacy of card and unauthorized access to the facility.

- Check the box 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 check-box to enable smart card identification of the user.

- This enables to identify a user into another office by means of Smart Card, though he is not enrolled into that particular office's system. Eg 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 the SI user must be enrolled with desired SI options from *Enrollment > SI User*.

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

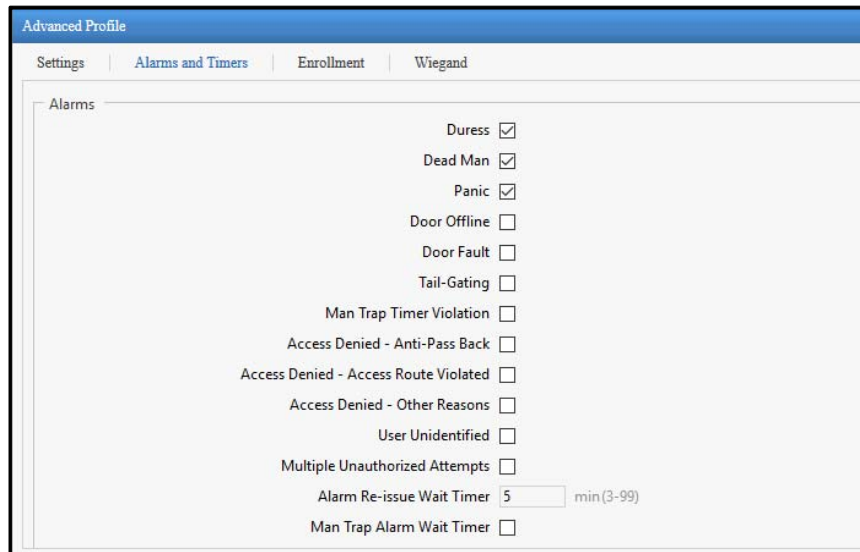
- Set the time in seconds for the **Alarm Auto Acknowledge Wait Timer (sec)**. The wait timer will start and on expiry of the timer, the alarm buzzer will stop automatically.

Allow Door Access Through API: Select this check-box to allow the access to device using COSEC APTA.

- **API Entry Access mode:** Select the entry access mode from the options of API Only, API then Biometrics and API then Card.
- **API Exit Access mode:** Select the exit access mode from the options of API Only, API then Biometrics and API then Card.
- **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 weigand 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.

Alarms and Timers

Alarms



Select the appropriate check-boxes for the respective alarms to be activated on the Panel Lite.

1. Duress Alarm:

Duress Alarm can be generated when a facility/ premises has been accessed by a valid user but under some threat or force entry. In this situation; the user can alert 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

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.

Also door alarm must be active and the door in normal condition (i.e. armed) then Panic alarm will be displayed accordingly.

4. Door Offline Alarm:

The user can enable the system to generate a Door Offline Alarm by enabling the Door Offline check-box. Also door alarm must be active so when door offline then Door Offline alarm will be generated.

5. Door Fault Alarm:

The user can enable the system to generate a Door Fault Alarm by enabling the Door Fault check-box. Also door alarm must be active. So when the door is accessed and held opened for long time, then door fault alarm will be generated.

6. 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 generated.

7. 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 other door present in the same zone/door group within the specified Mantrap timer. If user fails to do so, Mantrap violation alarm will be triggered.



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

8. 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 before entering again; 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.

9. 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.

10. Access Denied-Other Reasons:

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

11. User Unidentified:

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

12. Multiple Unauthorized Attempts:

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

Alarm Reissue Wait Timer (min): Enter the time in minutes for which an acknowledged alarm should wait before being re-issued in the Alarm Reissue Wait Timer (min). The default value is 5 minutes.

Man Trap Alarm Wait Timer: This check-box enables an alarm wait timer on the panel-lite to ensure that the user accesses sequential doors of a man-trap (Zone/ Door group) within a specific time-frame.

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 to be 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.

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 at the panel lite.

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	<input checked="" type="checkbox"/>		
Enrollment Mode	<input type="text" value="Biometric"/>		
Enrollment Using	<input type="text" value="User ID"/>		
Template Using Finger	<input type="text" value="Single Template/Finger"/>		
Max Number Of Fingers	<input type="text" value="Two"/>		
Max Number Of Palms	<input type="text" value="Ten"/>		
Number Of Fingers	<input type="text" value="Two"/>		
Number Of Palms	<input type="text" value="Two"/>		
Number Of Cards	<input type="text" value="One"/>		
Enable Self-Enrollment	<input type="checkbox"/>		
Self-Enrollment Retry Count	<input type="text" value="5"/>		(0-255)
Authorization on Enrollment	<input checked="" type="checkbox"/>		

Enrollment Using Door: Select this check-box to enable a user to be enrolled on the door.

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.

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.

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*

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*

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*

Enable Self-Enrollment: Select this check-box to activate self-enrollment. The Self-Enrollment feature enables the user to enroll himself/herself at a COSEC door controller using an already provided 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 for the user. (*User Configuration > Basic Access Control*) Self-Enrollment can be especially 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.

Authorization on Enrollment: Select this check-box to allow authorization of users who has enrolled biometric credentials or card. 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 VIP user is not yet authorized. However, VIP user will be displayed on Authorization page.

Wiegand

The screenshot shows the 'Wiegand' tab in the 'Advanced Profile' configuration window. The window has a blue header with the title 'Advanced Profile' and four tabs: 'Settings', 'Alarms and Timers', 'Enrollment', and 'Wiegand'. The 'Wiegand' tab is active. The settings are as follows:

Wiegand Interface	Input Mode
Wait For Panel Signal	<input checked="" type="checkbox"/>
Wait For User Verification	<input checked="" type="checkbox"/>
Wait Timer	2 sec
Send From	MSB Bit
Wiegand Out Format	26 Bit

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.

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).

Wait for User Verification: If this option is enabled, user verification will be requested on third party device before triggering any output.

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 Weigand output format, the device will receive all different Wiegand output formats configured from the Wiegand Format page of Masters tab. These formats represent the format in which the output will be sent on Wiegand interface. You can assign six formats for different events or a single format for single event. You can also select the output format by clicking on Select Weigand-Out Format button.

Advanced Profile

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

Wiegand Interface: Input Mode

Wait For Panel Signal:

Wait For User Verification:

Wait Timer: 2 sec

Send From: MSB Bit

Wiegand Out Format: Custom

Wiegand Format

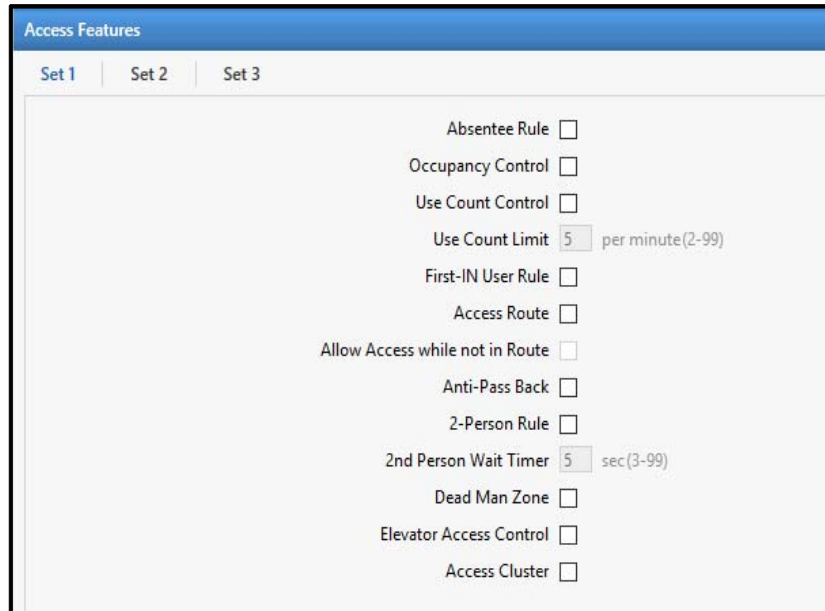
For Allowed Events	ID	Name	
Allowed Code	0		
For Identified Events	ID	Name	
Identified Code	0		
For Denied With Invalid Biometric Events	ID	Name	
Invalid Biometric Code	0		
For Denied With Invalid Card Events	ID	Name	
Invalid Card Code	0		

Click **Save** to apply the changes.

Access Features

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

Set1



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

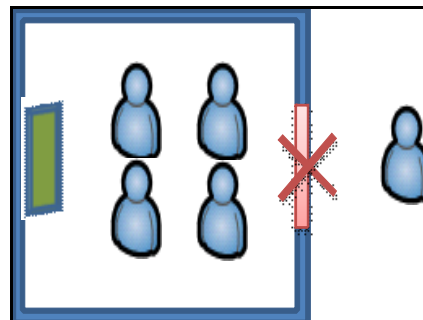


Absentee Rule must be enabled at user level from Users > User Configuration > Profile.

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.



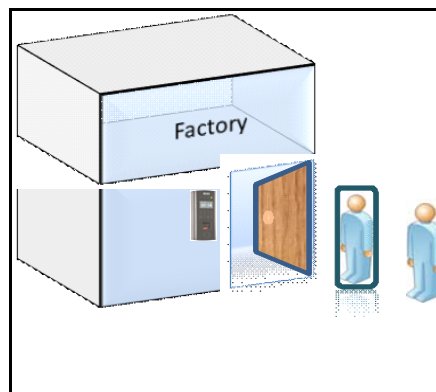
Occupancy Control must be enabled at Zone level from Panel Configuration > Zone configuration > Advance Configuration 2



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

- **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) field provided.
- 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 credential will be required to restore back.

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 effective working hours or the configured time overlaps with the current system 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 effective working hours or the expiry of the configured time.



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.

Access Route: Select this check-box to enable the Access Route feature on Panel lite V2. 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.

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.

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.

2 Person-Rule: Select the check-box to enable this feature at the panel. This functionality requires 2 person 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.

- **2nd Person Wait Timer (sec):** Set the wait time in seconds after which the second person is allowed to punch on the door when the 2-Person Rule is enabled.



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.

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 generated.

- When the user enters into the zone, the warning timer and the Alert timer will be started. If the user comes out of the zone within the Alert time, then the alarm will be reset else generates a warning alarm.
- Dead Man Zone can be activated by special function 23, Activate Dead-man.

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 in any of Elevator Floor group, but he can access those floors only if EAC is enabled for that user.
- 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 Panel lite V2 level.

Set2

The screenshot shows the 'Access Features' configuration window for 'Set 2'. The settings are as follows:

- Duress Detection:
- Duress Code: 10 (range 10-99)
- DND Zone:
- Smart Card Access Route:
- Access Route Type: Level 0 is lowest level (dropdown)
- Man Trap Door Interlock:
- Man Trap Wait Timer: 5 sec (range 3-65535)
- Apply Mantrap on: Zone (dropdown)
- MiFare Custom Key:
- MiFare Custom Key: 0000-0000-0000
- HID iClass Custom Key:
- HID iClass Custom Key: 0000-0000-0000-0000

Duress Detection: Select this check-box to enable duress detection feature. This allows the user to alert 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 (Panel lite) 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"



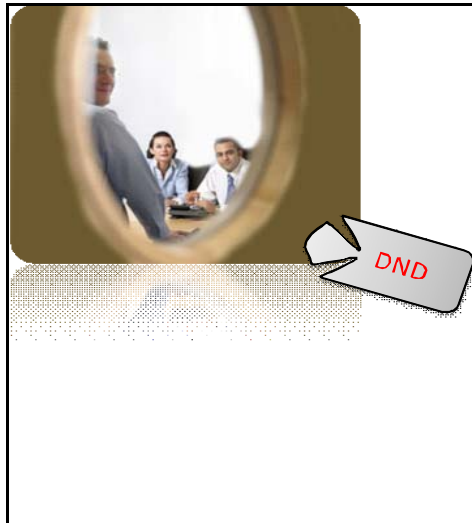
1. Only those users, who are assigned with PIN code, can access this feature.
2. If the door is in Lock state then, user is not allowed, so no duress will be detected.

DND Zone: Select the check-box to enable this feature at the system level. 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 Panel lite 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 are not affected by the do not disturb zone.



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



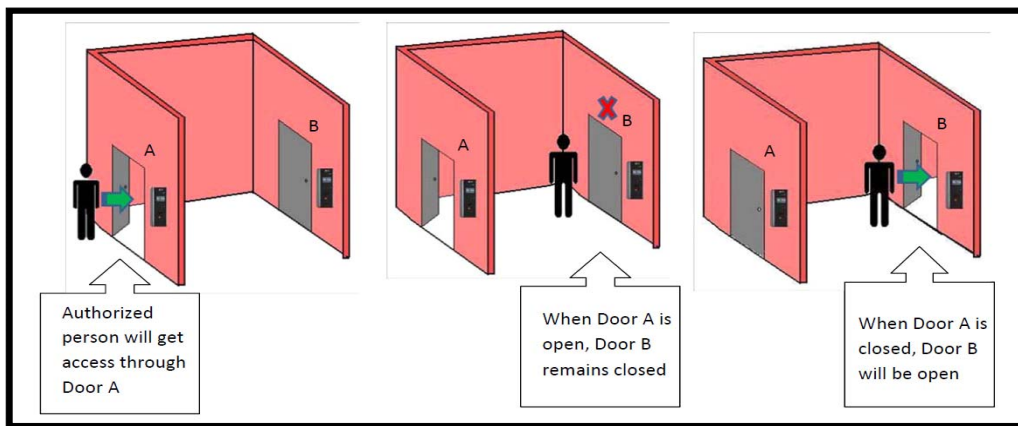
Smart Card Access Route: Select the check-box to enable the Smart Access Route. In this the user is allowed to access only specified doors with specified levels in predefined route, sequenced or un-sequenced.

- **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.

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.



- **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.
- **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.

MiFare Custom Key: Check the box to enable Mifare Card Key configuration. For MiFare Cards, enter 12 hexadecimal digits as custom key.

HID iClass Custom Key: Check the box to enable HID iClass Card Key configuration. For HID Cards, enter a 16-hexadecimal-digit key.

Set3

Set 1	Set 2	Set 3
Block User For		
Tail-Gating <input type="checkbox"/>		
Man Trap Timer Violation <input type="checkbox"/>		
Occupancy Violation <input checked="" type="checkbox"/>		
Anti-Pass Back Violation <input type="checkbox"/>		
Multiple Unauthorized Attempts <input checked="" type="checkbox"/>		
Allowed Unauthorized Attempts <input type="text" value="3"/> (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 panellite.

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

Click **Save** to apply the changes.

Special Functions

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 Panel lite.

There are four major groups of special functions and they are

- User
- Admin / HRD
- Zone Controls
- Alarms

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				

Save Cancel

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. With V13R3 firmware in device; the special functions **Enroll User**, **Enroll Special Card**, **Deleted Credentials** will have **Admin** as the default functional group.

So the 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.

Specify the **Card IDs** in the Card fields which would be registered to activate the special function at the doors. 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.

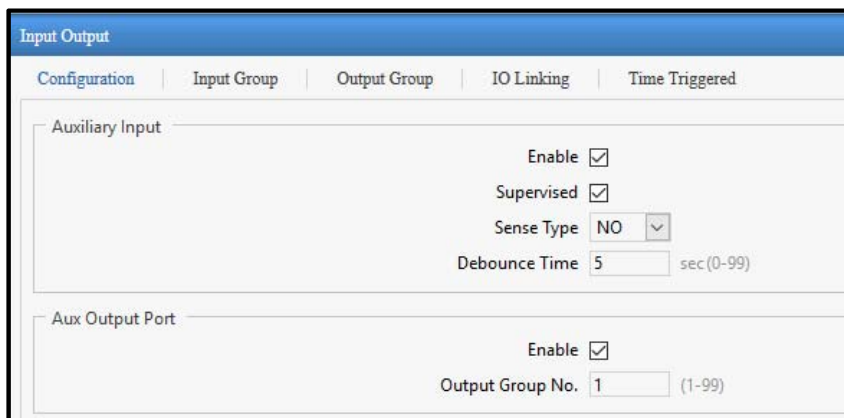
Input Output

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 page with the following settings:

- Auxiliary Input:**
 - Enable:
 - Supervised:
 - Sense Type: NO (dropdown menu)
 - Debounce Time: 5 sec (0-99)
- Aux Output Port:**
 - Enable:
 - Output Group No.: 1 (1-99)

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.

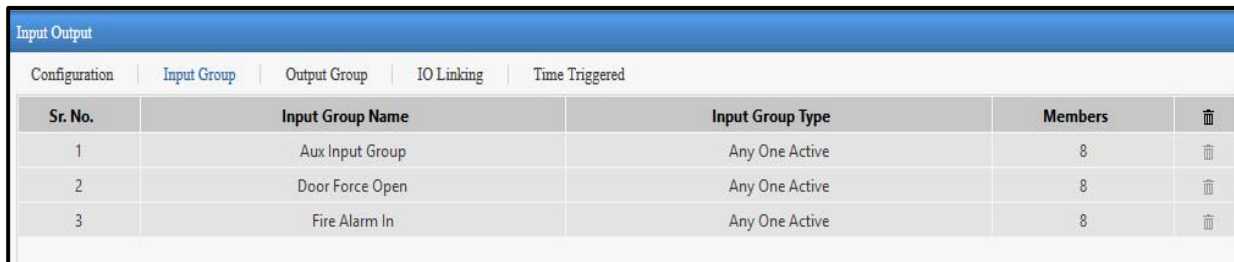
Output Group No.: Specify the Output Group Number to which the auxiliary output is to be assigned based on the output groups defined in the system.

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.

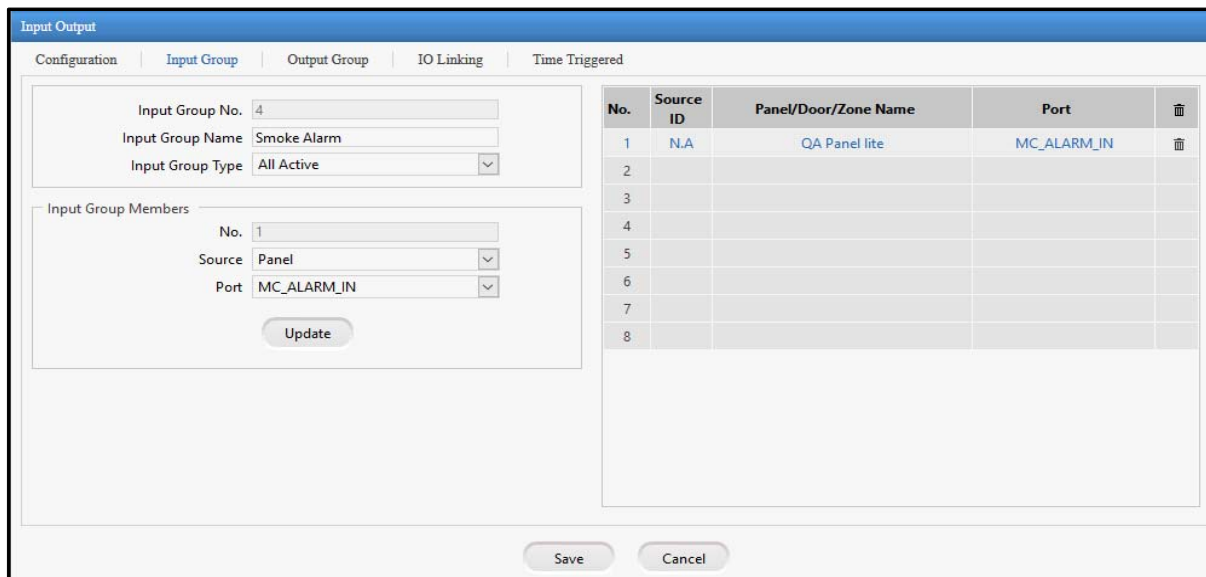


The screenshot shows the 'Input Output' configuration page with the 'Input Group' tab selected. It displays a table with the following data:

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	🗑️

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

Click the **Add** button to create a new Input Group.



The screenshot shows the 'Input Output' configuration page with the 'Input Group' tab selected. The form is used to add a new input group. The fields are filled with the following values:

- Input Group No.: 4
- Input Group Name: Smoke Alarm
- Input Group Type: All Active
- Input Group Members: No. 1, Source: Panel, Port: MC_ALARM_IN

The table on the right shows the existing input groups and their members:


No.	Source ID	Panel/Door/Zone Name	Port	
1	N.A	QA Panel lite	MC_ALARM_IN	🗑️
2				
3				
4				
5				
6				
7				
8				

Specify a Input group name and select the type for the group and define the member ports along with their source device.

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.



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

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 relay output will be in an energized condition for 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 displayed 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.

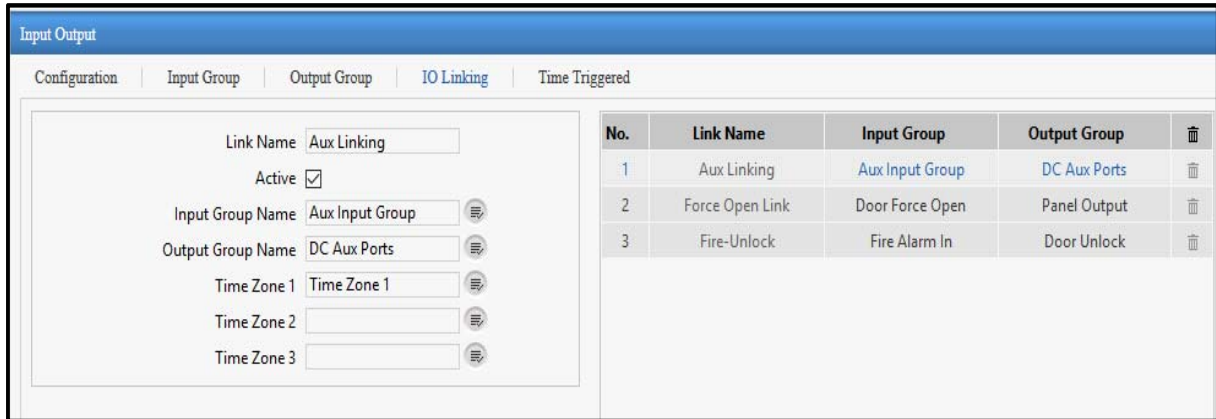
To create a new link follow the steps given below:

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

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

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

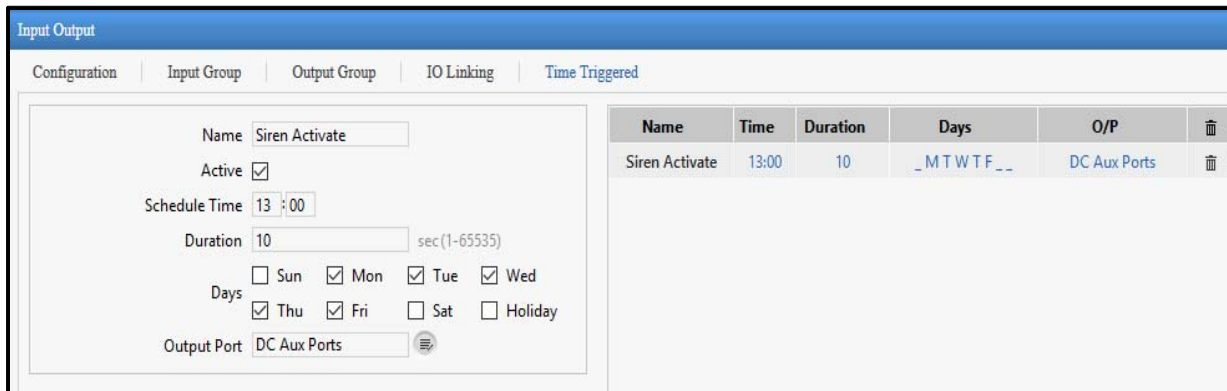
Time Zone 1-3: Click Select Time Zone button and select the time zone from the list. The Time Zones define the time slots in which the I/O linking Program can be activated.



Click the **Add** button and the created link gets displayed 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 Panel Lite.



To create a new function follow the steps given below:

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

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

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

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

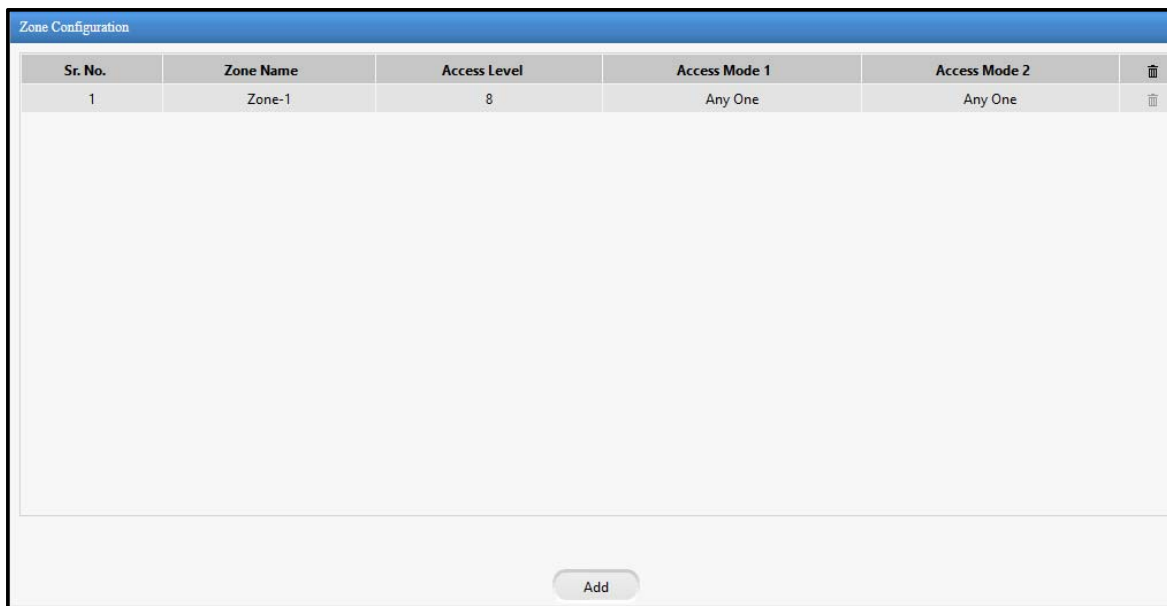
Output Port: Click Select Output Group button to select the output ports from the list.

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

Zone Configuration

Access Zones are areas with well defined boundaries, which are defined to effectively implement an Access Security System with Access Policies. A site can have multiple Access Zones, 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.



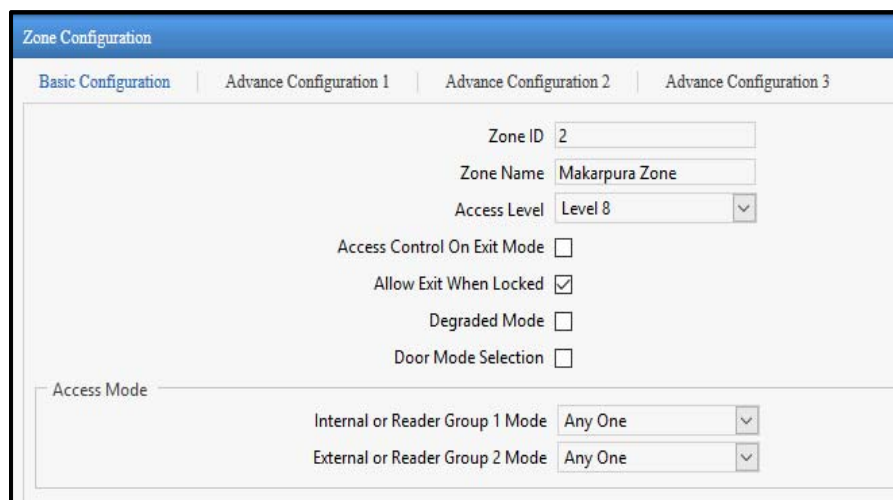
Sr. No.	Zone Name	Access Level	Access Mode 1	Access Mode 2	
1	Zone-1	8	Any One	Any One	

Zone-1 is predefined on the Panel Lite. 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.



Zone Configuration

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

Zone ID:

Zone Name:

Access Level:

Access Control On Exit Mode:

Allow Exit When Locked:

Degraded Mode:

Door Mode Selection:

Access Mode

Internal or Reader Group 1 Mode:

External or Reader Group 2 Mode:

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 master.

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 combinations of Biometric, Card, PIN and Group or None.

External or Reader Group2 Mode: Select the access mode from the combinations of Biometric and Card or None.

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

Advance Configuration 1

2-Person Rule

This functionality requires that two people present valid credentials to access a secure area. This is typically used in high security areas or in areas where industrial safety is an issue. Select the Enable check-box to enable this feature on 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:
- Primary Group: QA TL Group (dropdown)
- Secondary Group: QA Member Group (dropdown)
- Mode: Primary Must (dropdown)

The 'Anti-Pass Back' section is also expanded, showing the following settings:

- On Entry: Local (dropdown)
- On Exit:
- Restriction Type: Soft (dropdown)
- Forgiveness:
- Reset After: Day Change Timer Expiry
- Timer: 30 min (1-999)

The 'DND Zone' section is collapsed, showing the following setting:

- Enable:

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.

Anti-Pass Back

On Entry Local

On Exit

Restriction Type Soft

Forgiveness

Reset After Day Change Timer Expiry

Timer 30 min(1-999)

On Entry: Check this box so that the system monitors the entry reader for APB violation. Select the options from Local or Global from the drop down list.

- **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: Check this box also so that the system monitors the entry as well as the exit readers for APB violations.

Eg: 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'.

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

- **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.

Forgiveness: Check this box to enable the system to reset the APB status. When forgiveness is enabled, then there will be following options to reset the pass.

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 user defined time.
 - **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 get reset; If timer is already running and device gets rebooted.

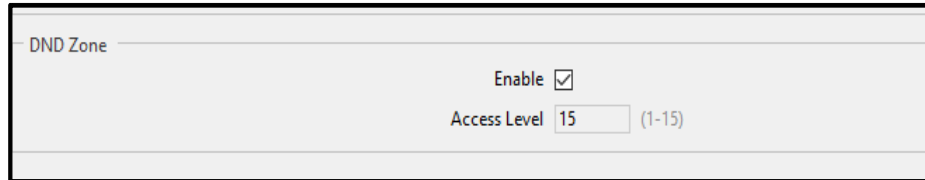
DND Zone

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 on 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.



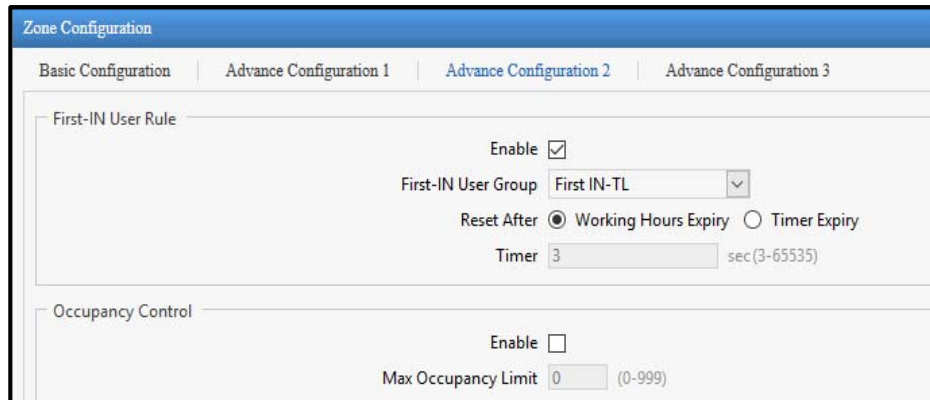
The screenshot shows a configuration window titled "DND Zone". It contains two settings: "Enable" with a checked checkbox, and "Access Level" with a text input field containing the number "15" and a range indicator "(1-15)".

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 with 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 effective working hours.



The screenshot shows the 'Zone Configuration' window with four tabs: 'Basic Configuration', 'Advance Configuration 1', 'Advance Configuration 2' (selected), and 'Advance Configuration 3'. Under the 'First-IN User Rule' section, the 'Enable' checkbox is checked. The 'First-IN User Group' is set to 'First IN-TL'. The 'Reset After' options are 'Working Hours Expiry' (selected) and 'Timer Expiry'. The 'Timer' is set to '3' seconds. Below this, the 'Occupancy Control' section has the 'Enable' checkbox unchecked and the 'Max Occupancy Limit' set to '0'.

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 on 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 after **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 option** 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 on the zone.

Occupancy Control

Enable

Max Occupancy Limit (0-999)

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

Dead Man Zone

This condition allows the tracking of safety and security of a user while a specific task is being performed, by requiring the user to show his card within the pre-defined dead man time period.

Dead Man Zone

Enable

Warning Timer sec(1-999)

Alert Timer min(3-999)

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

Man Trap

Enable

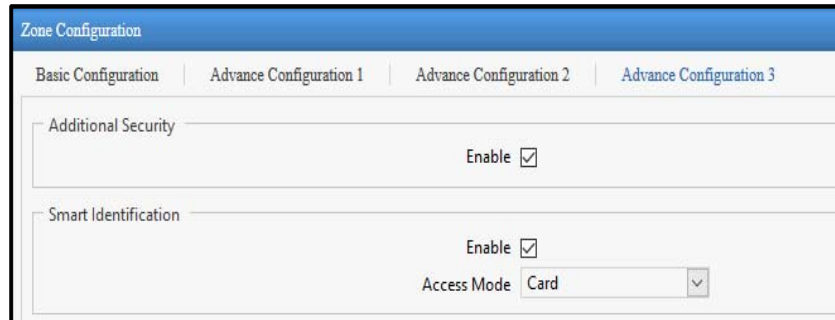
Ignore Man Trap Timer

Ignore Man Trap Timer: Enable the Ignore Man Trap Timer to ignore the Wait Timer in access zone, i.e. 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.

Advance Configuration 3

Additional Security

Enable: Select this check-box to enable the additional security feature for the Zone.



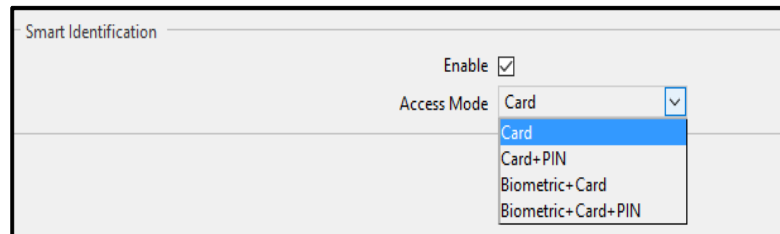
The screenshot shows the 'Zone Configuration' window with four tabs: 'Basic Configuration', 'Advance Configuration 1', 'Advance Configuration 2', and 'Advance Configuration 3'. The 'Advance Configuration 3' tab is active. It contains two sections: 'Additional Security' with an 'Enable' checkbox checked, 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 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 on the zone.



The screenshot shows the 'Smart Identification' section of the configuration interface. It includes an 'Enable' checkbox that is checked and an 'Access Mode' dropdown menu. The dropdown menu is open, showing four options: 'Card' (highlighted in blue), 'Card+PIN', 'Biometric+ Card', and 'Biometric+ Card+PIN'.

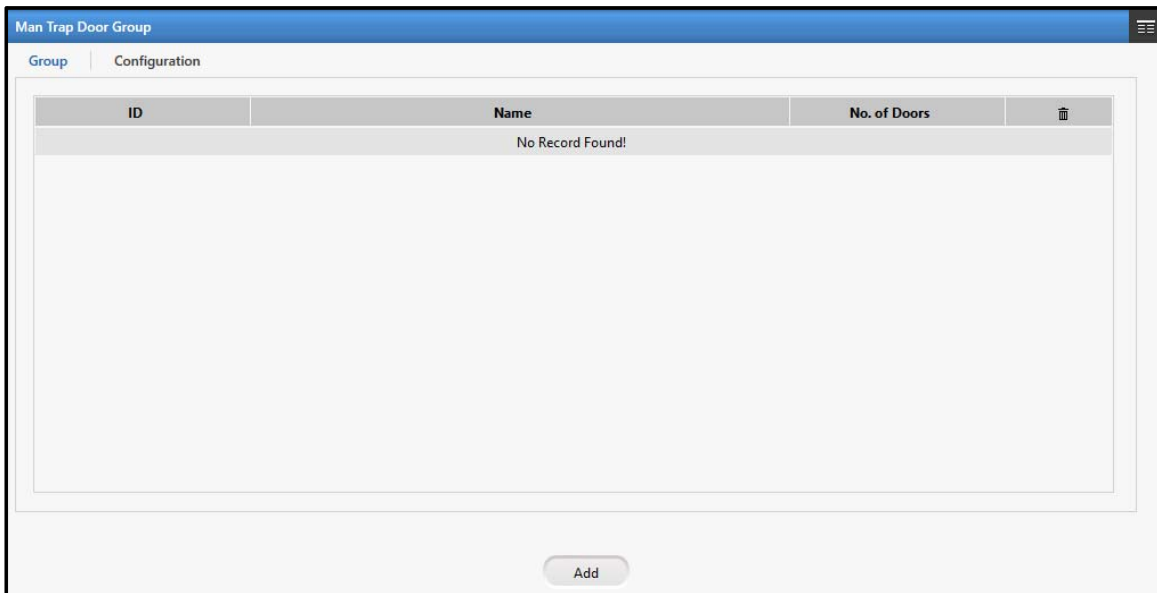
Access Mode: Select the access mode applicable for smart identification such as card, card + pin etc.

This enables to identify a user into another office by means of Smart Card, though he is not enrolled into that particular office's system.

Click **Save** to apply the changes.

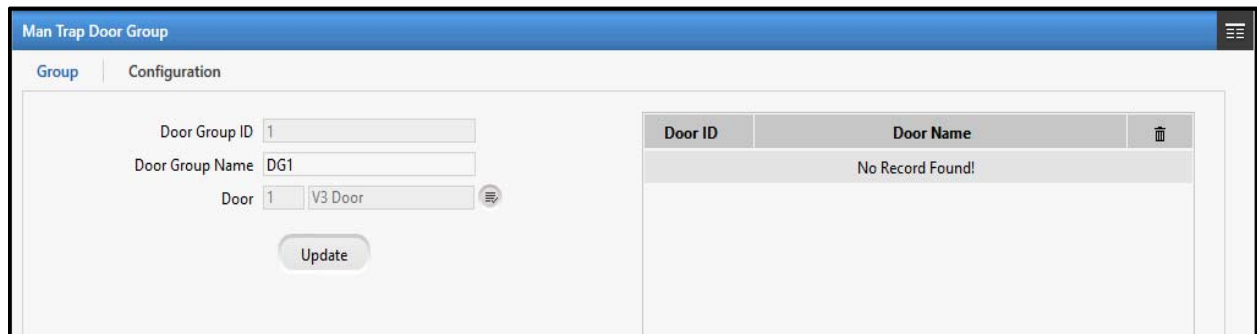
Man Trap Door Group

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

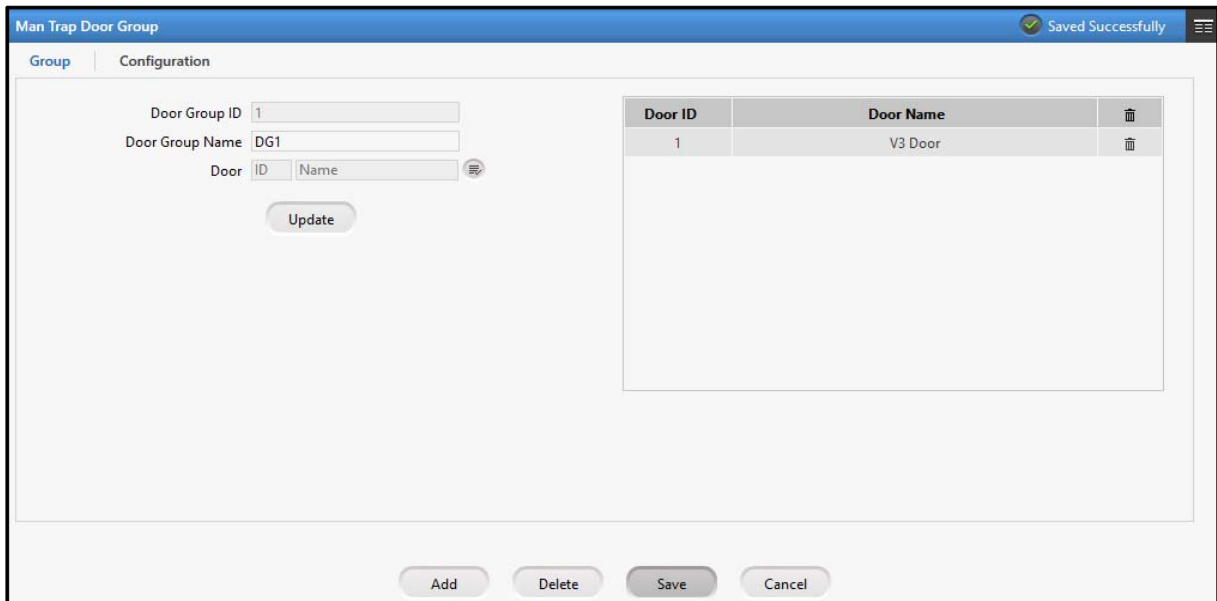


Door Group ID: The door group ID is auto-generated by the system.

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

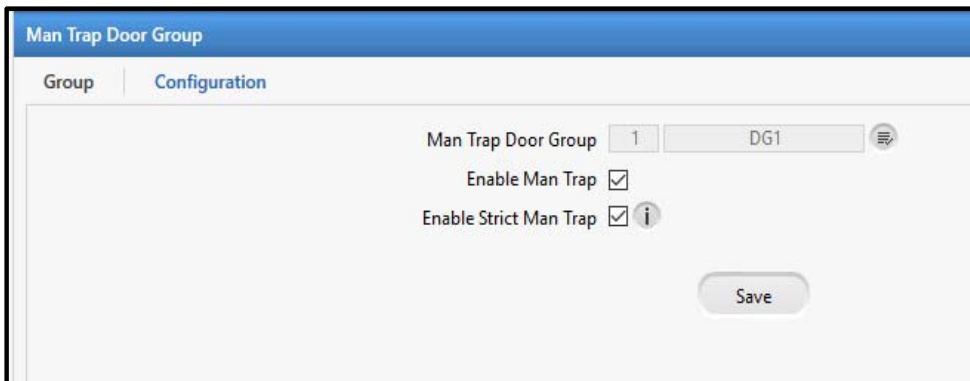
Door: Click the door pick-list button and select the door to be added to the group. You cannot add one door to multiple groups. The doors are configured from *Devices > Door Configuration*.

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 page enables configuration of the LAN Settings, Wi-Fi Settings and Mobile Broadband settings of the Panel-lite.



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

LAN Settings

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

Network Settings

LAN Settings | Wi-Fi Network Settings | Wi-Fi Access Point Settings | Mobile Broadband

IP Address: 192.168.104.111
MAC Address: 00:1b:09:04:65:d1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.104.1
Preferred DNS: 192.168.50.100
Alternate DNS:

Test Network Connection

Enter URL: 192.168.104.12 [Test]

Connection Successful

To test the network connection of panel lite, enter the URL and click Test button. The

Wi-Fi Network Settings

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

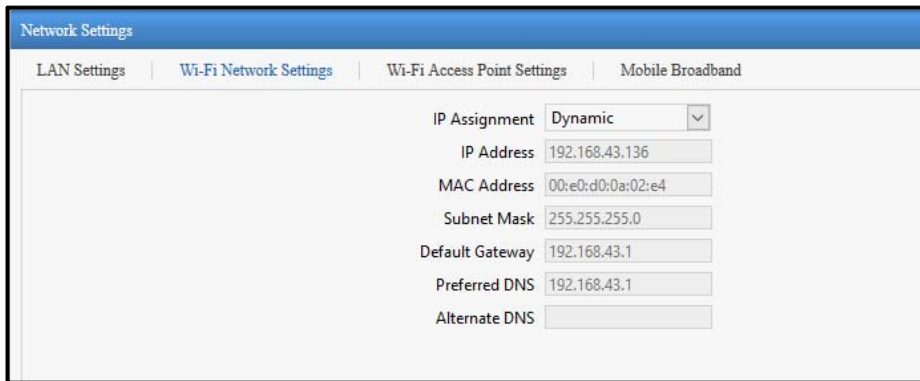
Network Settings

LAN Settings | **Wi-Fi Network Settings** | Wi-Fi Access Point Settings | Mobile Broadband

IP Assignment: Static
IP Address: 192.168.10.1
MAC Address:
Subnet Mask: 255.255.255.0
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 panel lite 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 panel lite as shown below.

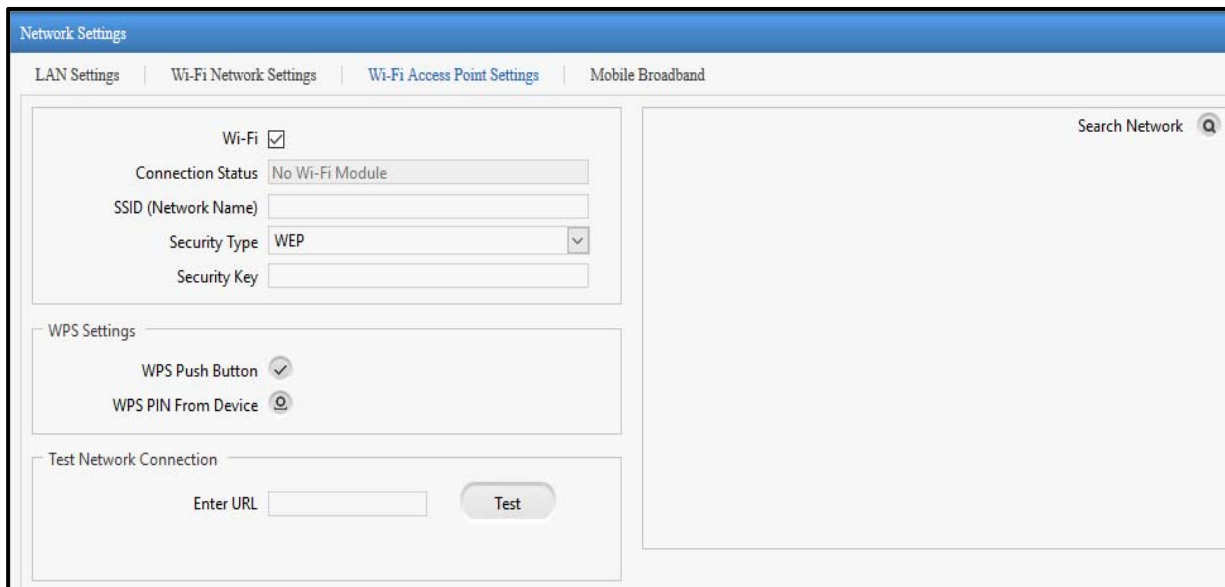


The screenshot shows the 'Network Settings' window with the 'Wi-Fi Network Settings' tab selected. The settings are as follows:

Setting	Value
IP Assignment	Dynamic
IP Address	192.168.43.136
MAC Address	00:e0:d0:0a:02:e4
Subnet Mask	255.255.255.0
Default Gateway	192.168.43.1
Preferred DNS	192.168.43.1
Alternate DNS	

Wi-Fi Access Point Settings

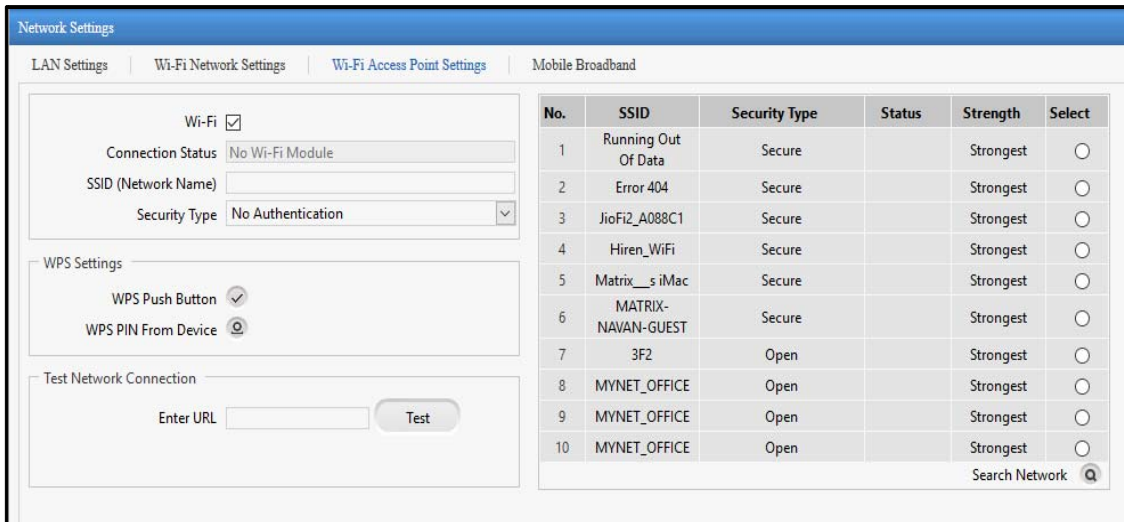
The Wi-Fi Access Point supports wireless connection to communicate between the Standalone panel-lite and the application software. The user has to explicitly configure the security type and encryption option also. Only the SSID(Service Set Identifier) field will be automatically detected.



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

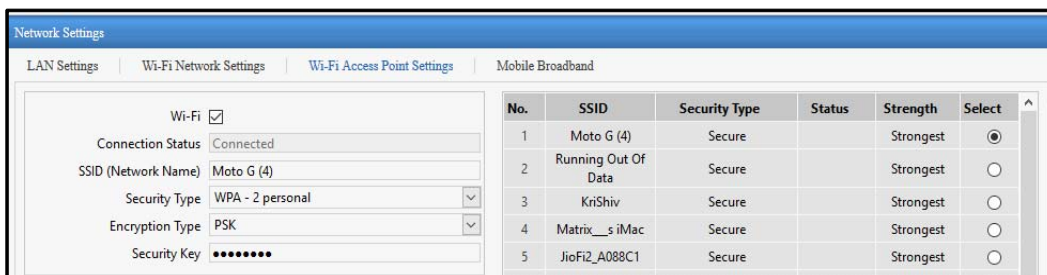
Setting	Value
Wi-Fi	<input checked="" type="checkbox"/>
Connection Status	No Wi-Fi Module
SSID (Network Name)	
Security Type	WEP
Security Key	
WPS Settings	
WPS Push Button	<input checked="" type="checkbox"/>
WPS PIN From Device	<input type="checkbox"/>
Test Network Connection	
Enter URL	
Test	<input type="button" value="Test"/>

Enable the **Wi-Fi**. Then insert the Wi-Fi dongle in your panel lite and click on **Search Network** to search the available wi-fi networks.

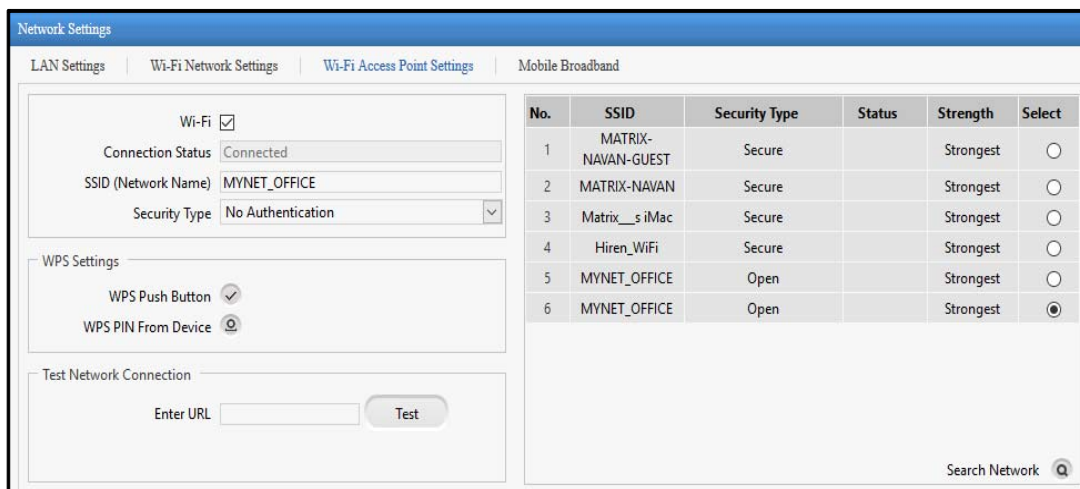


Then select a Wi-Fi network from the right grid. Its **SSID** and **Security Type** will appear in the respective fields. Depending on the Wi-Fi device you will have to provide security key for authentication. Then click **Save** to save the Wi-Fi Access point. When the connection with Wi-Fi is established, **Connection Status** will show 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:

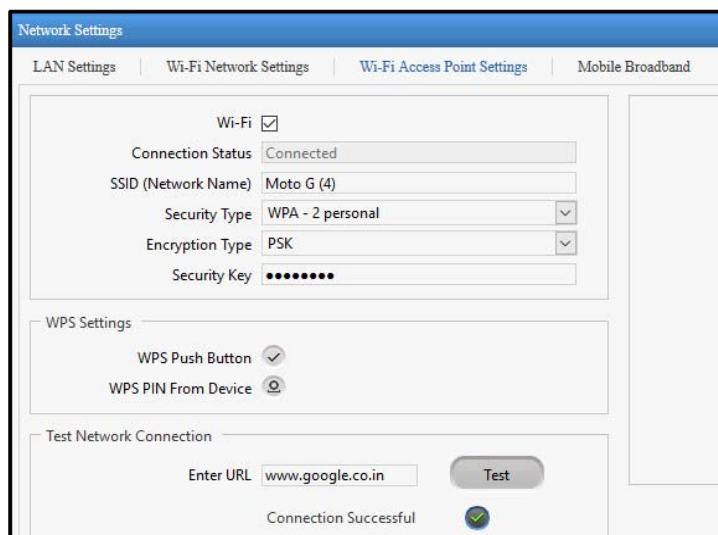
WPS Push button:

1. Once this option is selected and on click of connect button, 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. Once this option is selected and on click of connect button, 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



The screenshot displays the 'Network Settings' interface with the following sections:

- LAN Settings** | **Wi-Fi Network Settings** | **Wi-Fi Access Point Settings** | **Mobile Broadband**
- Wi-Fi**
- Connection Status:** Connected
- SSID (Network Name):** Moto G (4)
- Security Type:** WPA - 2 personal
- Encryption Type:** PSK
- Security Key:** ••••••••
- WPS Settings:**
 - WPS Push Button:**
 - WPS PIN From Device:**
- Test Network Connection:**
 - Enter URL:** www.google.co.in
 - Test** button
 - Connection Successful** with a green checkmark icon.

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.

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

Connection Details

Connection Status: No Modem

IP Address:

Default Gateway:

Preferred DNS:

Alternate DNS:

Test Network Connection

Enter URL:

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 Dialing Number which needs to be dialed to establish connectivity, Username 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 shows the Connection Status, IP address, Default Gateway, Preferred DNS and Alternate DNS address.

Click on Save button to save the Network Settings.

DDNS

The DDNS section enables to register Panel lite V2 on DDNS Server by configuring its Hostname. DDNS Server will resolve the IP address of configured host-name and will map the same also. Whenever public IP Address of Panel lite V2 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 Panel liteV2 is connected with Internet.

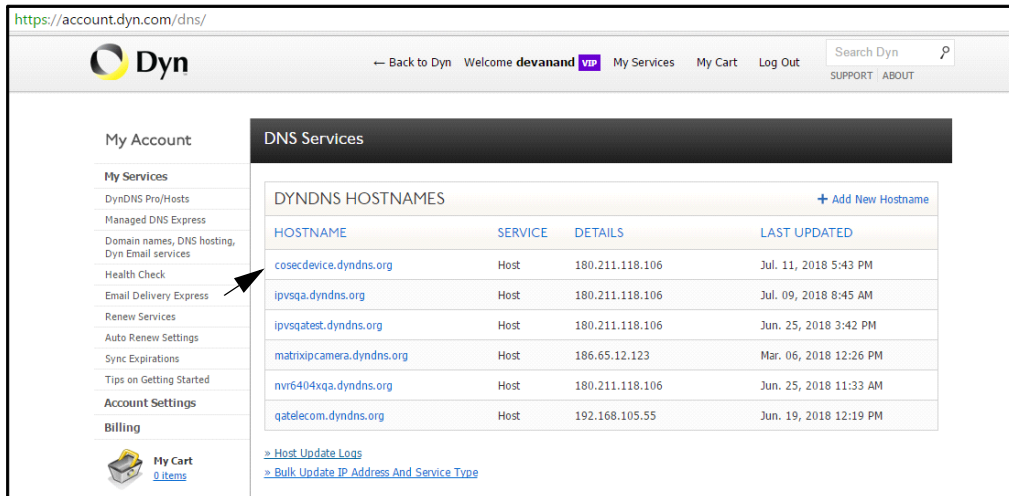
The image shows two screenshots of the 'Network Settings' page, specifically the 'LAN Settings' tab. The top screenshot shows the 'Test Network Connection' section with the 'Enter URL' field set to 'www.google.com' and a 'Test' button. Below the button, the status is 'Connecting' with a circular refresh icon. The bottom screenshot shows the same page after a successful test, with the status 'Connection Successful' and a green checkmark icon. The network configuration fields (IP Address, MAC Address, Subnet Mask, Default Gateway, Preferred DNS, and Alternate DNS) are visible in both screenshots and contain the same values: IP Address: 172.16.2.37, MAC Address: 00:1b:09:04:eb:3f, Subnet Mask: 255.255.0.0, Default Gateway: 172.16.0.1, Preferred DNS: 192.168.52.1, and Alternate DNS: (empty).

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

DDNS Server: Select the DynDNS option for DDNS server.

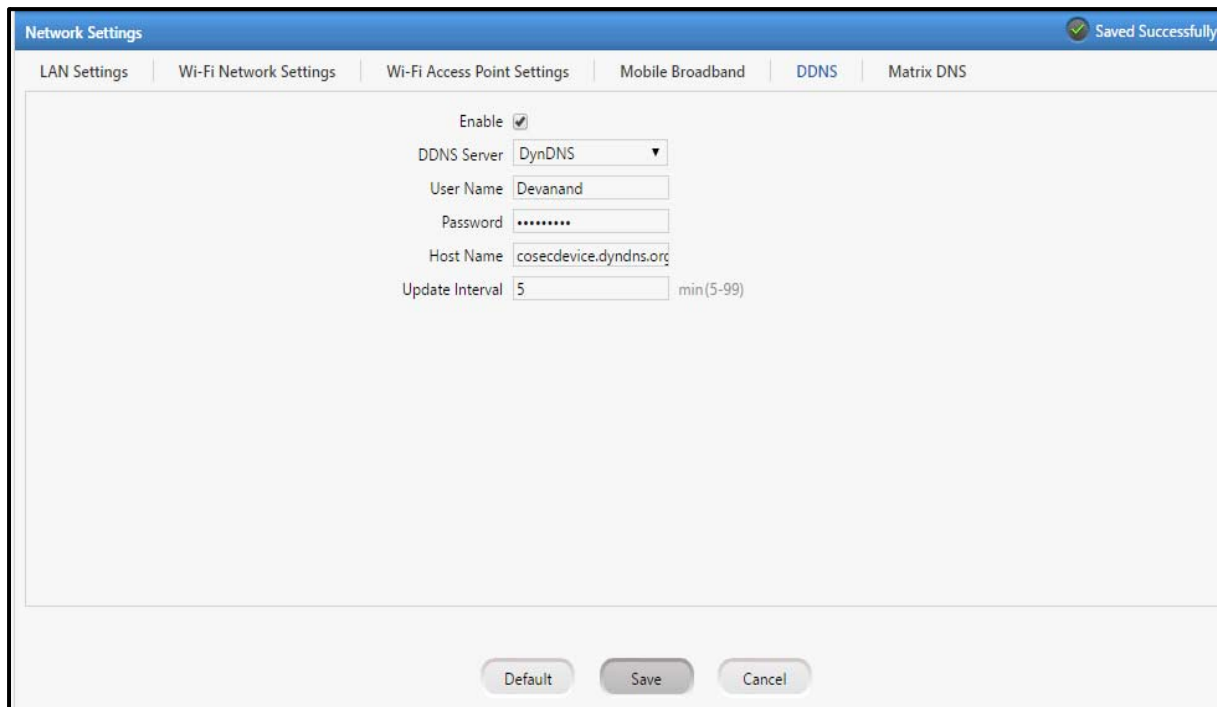
User Name/Password: Enter the user-name as “Devanand” and password as “matrix123”.

Host Name: Enter the host name as the name registered on DDNS server. Eg: “cosecdevice.dyndns.org”
The Panel lite V2 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 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 Panel Lite V2 is registered by the host name with the public IP as shown below.

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

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

My Account

- My Services
 - DynDNS Pro/Hosts
 - Managed DNS Express
 - Domain names, DNS hosting, Dyn Email services
 - Health Check
 - Email Delivery Express
 - Renew Services
 - Auto Renew Settings
 - Sync Expirations
 - Tips on Getting Started
- Account Settings
- Billing
- My Cart 0 items

Host Update Logs Viewer [↑ My Services](#)

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

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

You can access the Panel Lite V2 by entering host name for eg: “cosecdevice.dyndns.org” in browser.

Matrix DNS

The Matrix DNS section enables to register Panel lite V2 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 DDNS **Matrix DNS**

Enable

Host Name

Forwarded Port (1-65535)

Update Interval min(5-99)

Default Save Cancel

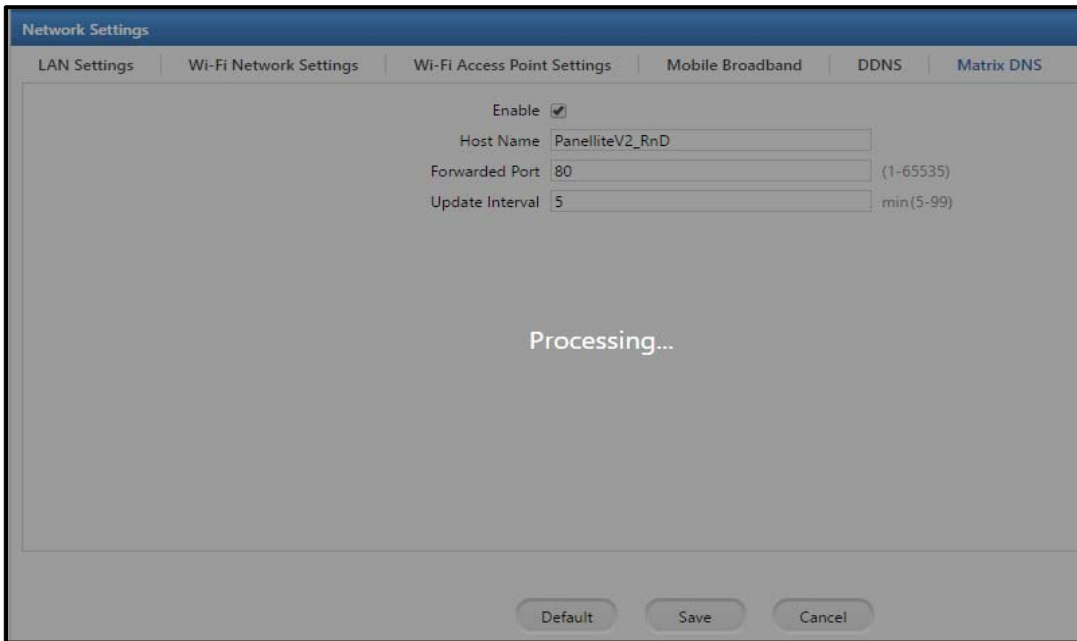
Enable the check-box to activate the registration of host name on Matrix DDNS server.

Host Name: Enter the host name as the name with which Panel lite V2 can be accessed from the Matrix DNS server.

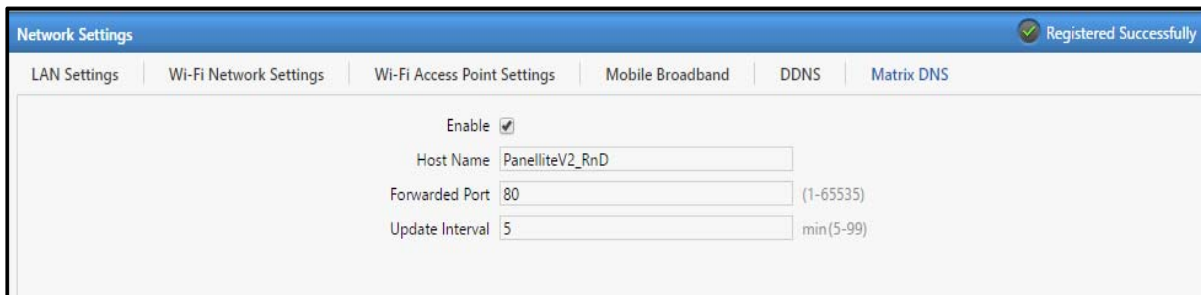
Forwarded Port: Enter the communication port on which Panel Lite V2 will listen. It is 80 by default.

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 registered one.

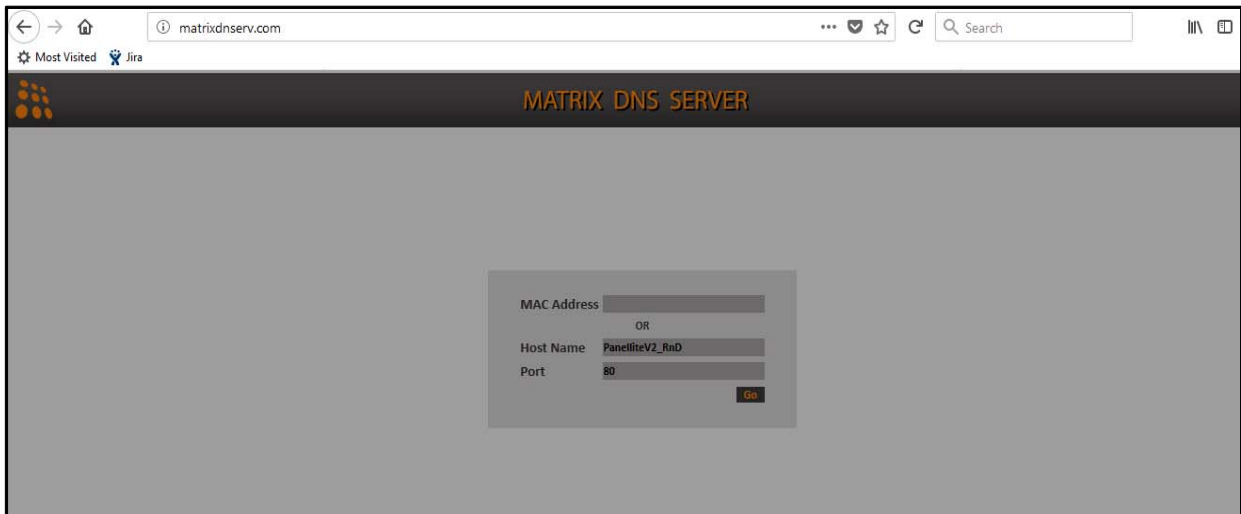
Click on **Save** button. The request will be processed as shown below.



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



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 Panel Lite V2 will appear automatically which confirms the registration of Panel Lite V2 on Matrix DNS Server.



Matrix DNS Server will resolve the IP Address for configured Hostname. So, now Panel Lite V2 can be accessible through same hostname but with new IP Address.

Date and Time

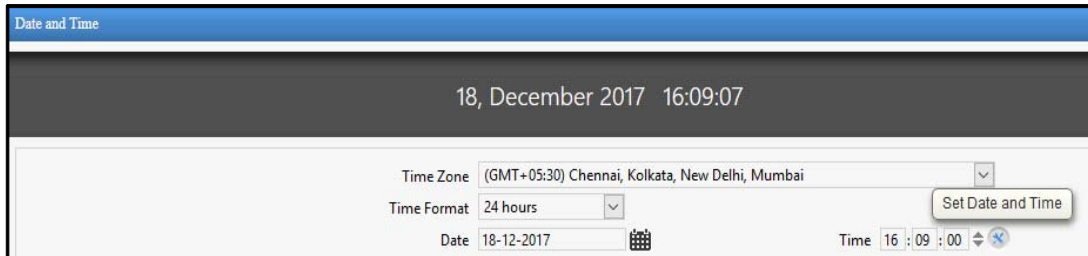
The Date and Time page enables you to view and set date and time parameters for the Panel Lite device. The date and time on display shows the current date and time settings on the device.

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

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

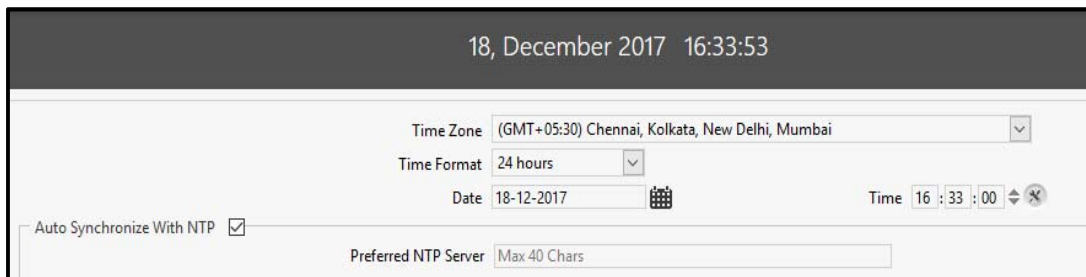
Date/Time: To change date and time manually, select a date using the calendar button and a time by manually entering the value or using up-down arrows.

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



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 enable **Auto Synchronize With NTP** check-box.



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 first. If it receives updated Date and Time then Updated Date and Time will be reflected on device webpage and display screen.
 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 Panel Lite 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 backwarded by 05:00 hours.

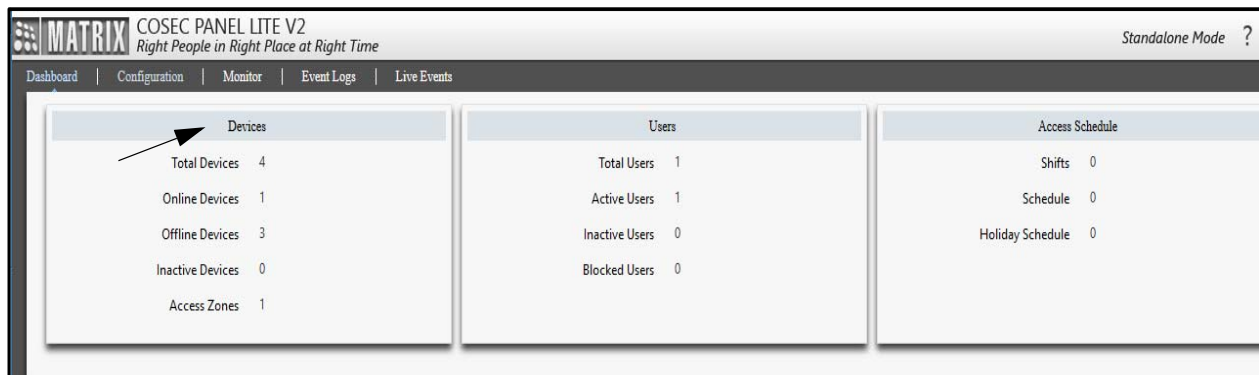
Click Save to apply the changes.

The Devices section enables you to add different type of devices such as PATH Door, PVR Door, VEGA Door, ARGO Door, ARC Controllers, V3 Door and set the basic and advanced configurations.

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

See Door Configuration section for details.

The total number of devices configured in Panel lite is shown as Total Devices on dashboard. The number of Online Devices, Offline Devices and Inactive Devices is also displayed on the Dashboard as shown below.



The screenshot shows the dashboard for MATRIX COSEC PANEL LITE V2. The top navigation bar includes Dashboard, Configuration, Monitor, Event Logs, and Live Events. The main content area is divided into three columns: Devices, Users, and Access Schedule. An arrow points to the 'Devices' column.

Devices		Users		Access Schedule	
Total Devices	4	Total Users	1	Shifts	0
Online Devices	1	Active Users	1	Schedule	0
Offline Devices	3	Inactive Users	0	Holiday Schedule	0
Inactive Devices	0	Blocked Users	0		
Access Zones	1				

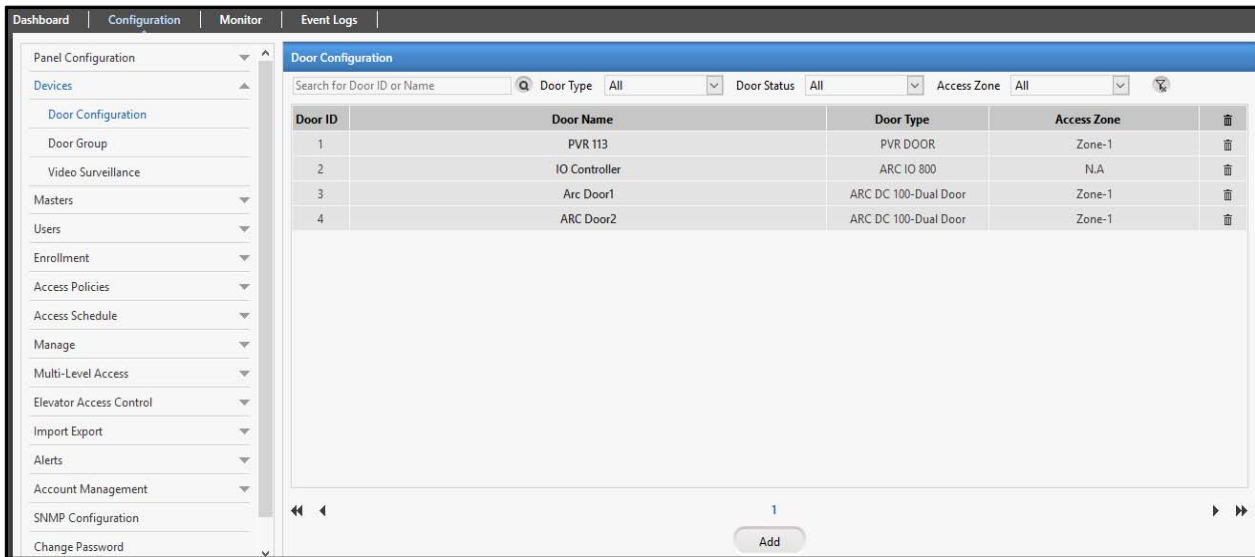
You can also integrate COSEC devices with SATATYA devices to get images and videos triggered by user events at doors.

See Video Surveillance section for details.

Door Configuration

This page enables user to add slave door controllers to the Panel Lite and configure parameters for each door. A Panel Lite can control up to 255 doors using ethernet communication and up to 32 doors when communication type is RS-485.

The page displays a search criteria to find a required door and a grid containing a list of added devices along with its details. You can also delete a particular door by clicking on Delete icon.

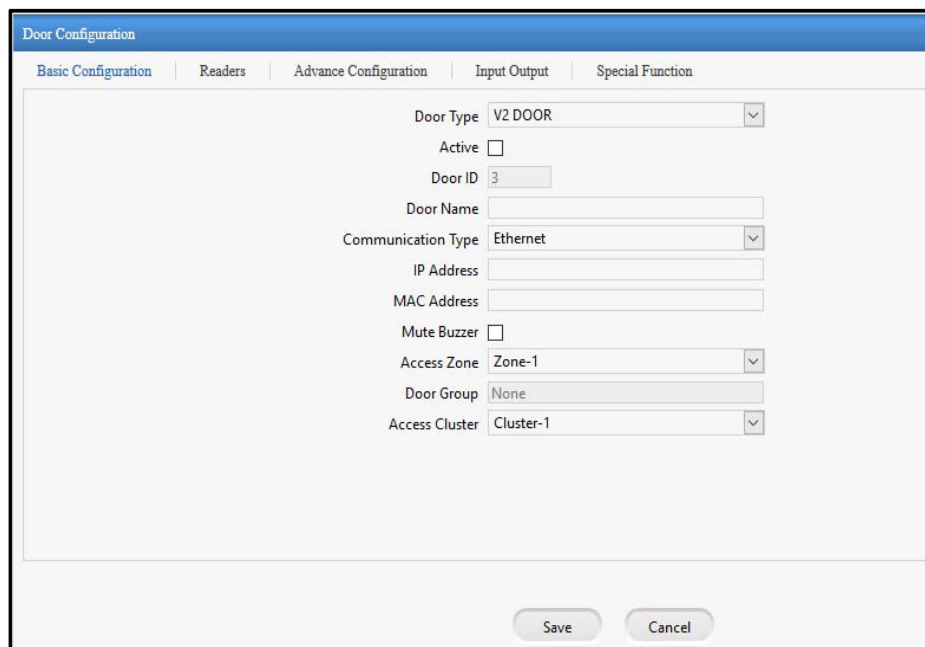


The screenshot shows the 'Door Configuration' page in a web interface. On the left is a navigation menu with options like 'Panel Configuration', 'Devices', 'Door Configuration', 'Door Group', 'Video Surveillance', 'Masters', 'Users', 'Enrollment', 'Access Policies', 'Access Schedule', 'Manage', 'Multi-Level Access', 'Elevator Access Control', 'Import Export', 'Alerts', 'Account Management', 'SNMP Configuration', and 'Change Password'. The main area is titled 'Door Configuration' and features a search bar for 'Door ID or Name', and filters for 'Door Type', 'Door Status', and 'Access Zone'. Below these is 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 area, there is a page indicator '1' and an 'Add' button.

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



The screenshot shows the 'Door Configuration' form with the following fields and values:

- Door Type: V2 DOOR
- Active:
- Door ID: 3
- Door Name: (empty)
- Communication Type: Ethernet
- IP Address: (empty)
- MAC Address: (empty)
- Mute Buzzer:
- Access Zone: Zone-1
- Door Group: None
- Access Cluster: Cluster-1

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



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

Basic Configuration

Door Type: Select the type of door controller to be added. You can select the door type from the options of V1 DOOR/V2 DOOR/V3 DOOR/PATH DOOR/PVR DOOR/VEGA DOOR/ARC DC 100/ARC IO 800/ARGO DOOR.

Mode (Only for ARC DC 100): Select the mode of ARC DC 100. 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 as 2 door is supported in both Standalone and Server mode.

Active: Check the box to activate the device on 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 Panel Lite as Ethernet or RS-485.

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

MAC Address: Specify the MAC Address of the door.

Connect Doors with: This parameter will appear when you add ARC DC 100 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: Use this option to mute or unmute the door buzzer.

Inverse Polarity for External Buzzer: When external reader is connected to ARC controller via Wiegand Interface and external buzzer is required to connect with ARC; then enable this inverse polarity checkbox 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.

The screenshot shows the 'Door Configuration' web interface with the following settings:

- Door Type: ARC DC 100
- Mode: Single Door
- Active:
- Door ID: 2
- Door Name: ARC as Single door
- Communication Type: Ethernet
- IP Address: 192.168.104.60
- MAC Address: f7:65:77:43:32:42
- Mute Buzzer:
- Inverse Polarity for External Buzzer:
- Access Zone: Zone-1
- Door Group: None
- Access Cluster: Cluster-1

Access Zone: Select an access zone to assign to 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 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 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.

Access Cluster: Select the configured Cluster from the drop down options to which the door is to be assigned.

Readers

As per the door type selected there are different parameters for configuring readers. Below parameters are not applicable for ARC DC 100 door type.

Internal Readers

Select the card reader and finger reader/palm vein reader types for internal readers.

Specify the reader mode as entry or exit.

Select the **card format** from the configured formats for internal reader. This is applicable for all direct doors other than Direct V1 DOOR and all Panel doors including Direct V1 DOOR.

External Reader

Select the external reader type and mode as Entry or Exit.

You can select the checkbox to enable the use of exit switch.

Select the **card format** from the configured formats for external reader.

CARD FORMAT

You can select maximum 5 card formats for Internal as well as External reader

The selected card formats will be then displayed.

When you show 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.

Case1: 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.

ARC DC 100 Reader

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

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

Weigand Reader: Select the weigand reader from the dropdown list. The available options are:

- 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 it is must to show Card 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 checkbox to enable exit switch feature for Reader2 Group so that the door can be opened without checking for any access policies.

Card Format: Select the 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 respectively.

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

Weigand Reader: Select the weigand reader from the dropdown list. The available options are:

- 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 it is must to show Card 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 checkbox to enable exit switch feature so that the door can be opened without checking for any access policies.

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 is not applicable for ARC IO 800.

Advance Configuration

Auto Re-lock: Select this checkbox to allow the door to relock 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 Relock operation.

Alarm: Select this checkbox to set all door-based alarms as active

Tamper Alarm: Select this checkbox to activate the Tamper Alarm.

Pulse Timer(sec): Specify the time in seconds for which a panel door will remain in an open state on receiving a valid credential.

Auto IP Assignment: There is option where panel door can be assigned its IP from device webpage.To enable this check the Auto IP Assignment box.

Network Protocol: Select the Network protocol from the options of 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 on the panel door, the occupancy count of a zone will be incremented or decremented considering both the punch as well as the auxiliary input port of the panel door (say, input from a beam-counter).

- **Reset Wait Timer:** Set the wait timer for resetting the tailgating count (Reset Wait Timer) based on the **door lock status** or the door **pulse wait timer** (as configured).

Door Interlock: Select this check-box to activate the Door Interlock for the selected door (say 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). Suppose Door V3 and Vega Door are selected for Interlock with PVR door. So When PVR opens; V3 and Vega door will remain close.



For Degrade mode Door Interlocking feature will not work.

Whenever a door is in abnormal state and for that door interlocking is enabled then user access in other doors of the interlocking group is allowed.

The Man Trap timer Internal/External reader- allows to fix a maximum time within which the user has to cross the high security corridor.

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 any 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 other user will be allowed to any other internal reader in the same zone/group.



Advance Configuration is not applicable for ARC IO800 device.

Input Output

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



For ARC DC 100-Dual Door configure the above Door Sense and Door Relay parameters for both Door 1 and Door 2 respectively.

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

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 generating 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 pulse timer expiry/ 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 to enable Auxiliary Input (e.g. Smoke Detectors) depending on normal door state monitoring.

Supervised: Select this to enable Auxiliary Input (e.g. Smoke Detectors) depending on supervised door state monitoring.

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

Debounce Time(sec): Specify the Debounce time in seconds. Default value is 3 sec and range should be 0-99 sec. It defines the minimum time for which an input interface must be maintained 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 Enable checkbox 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 defined on the system.

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.



For ARC IO 800 configure only the above Auxiliary Input and Auxiliary Output parameters.

Special Function

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.



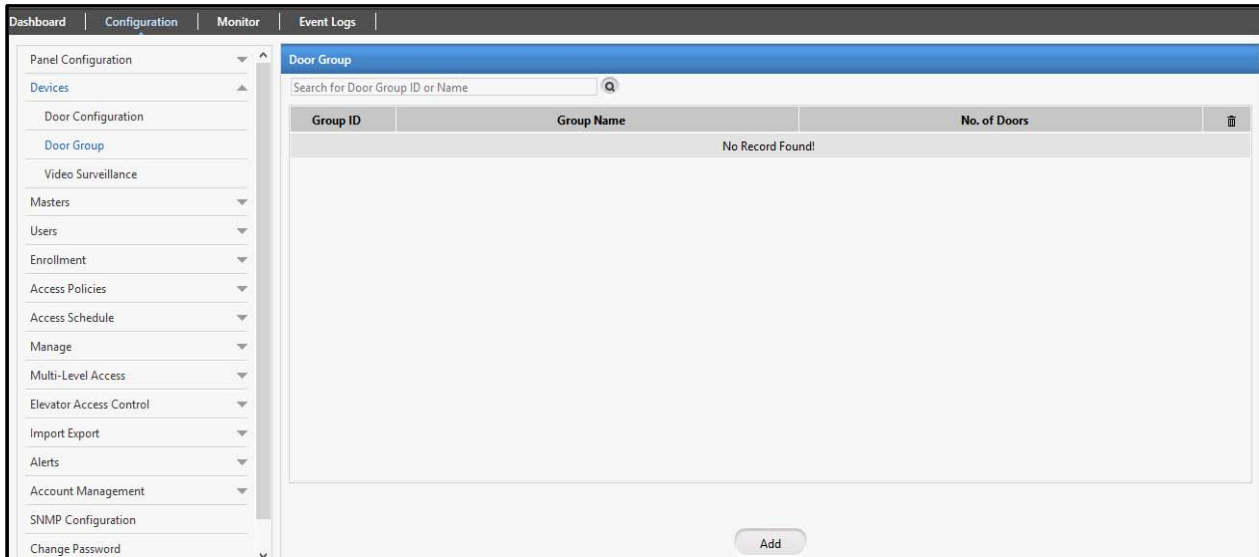
Special function is not applicable for devices ARC DC 100, VEGA DOOR, PATH DOOR, ARGO DOOR and ARC IO 800.

Click Save to apply the changes.

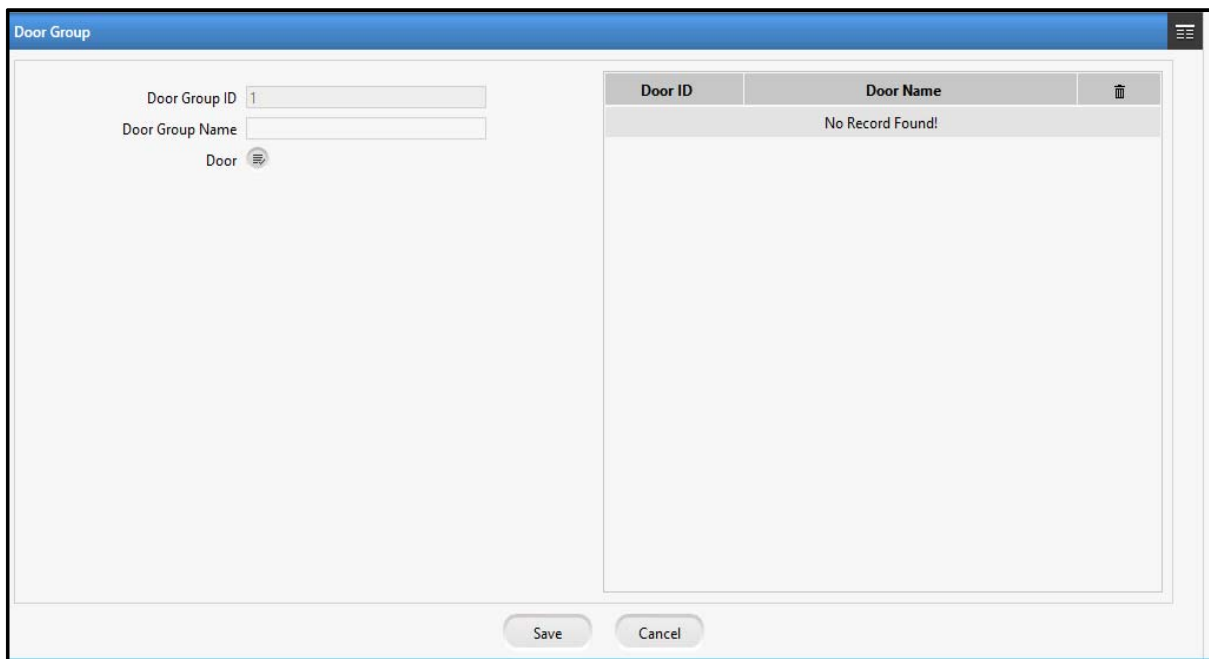
Door Group

This page enables 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.



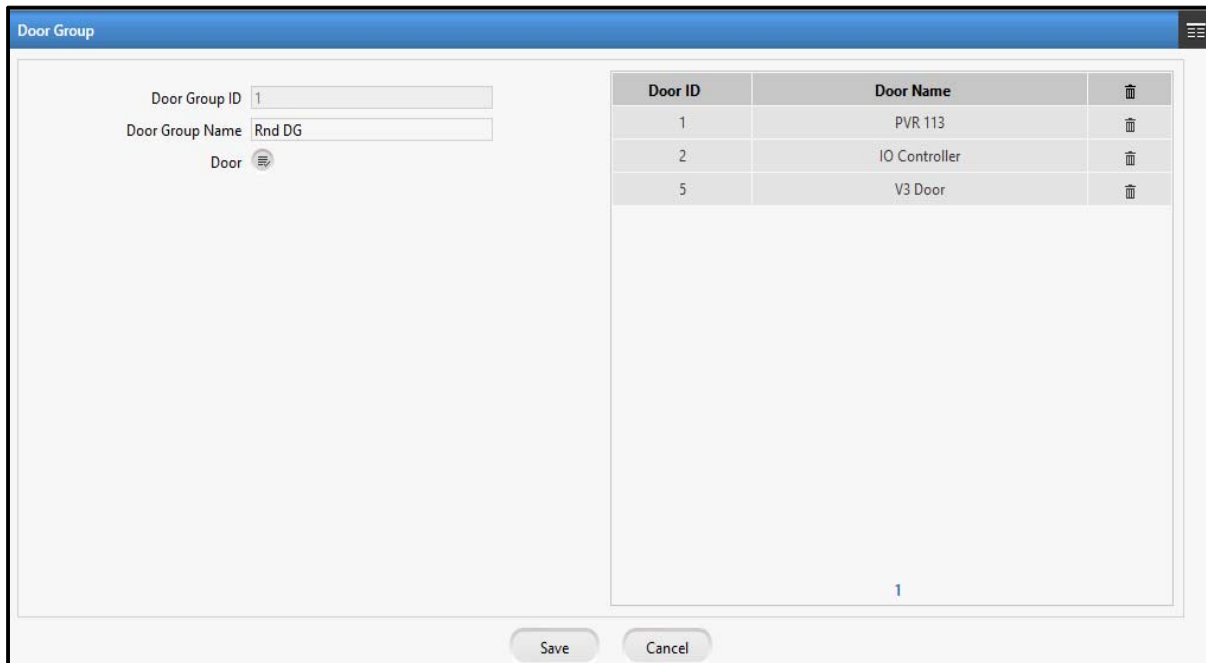
To add a new Door Group click **Add** button and configure the following parameters.



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

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

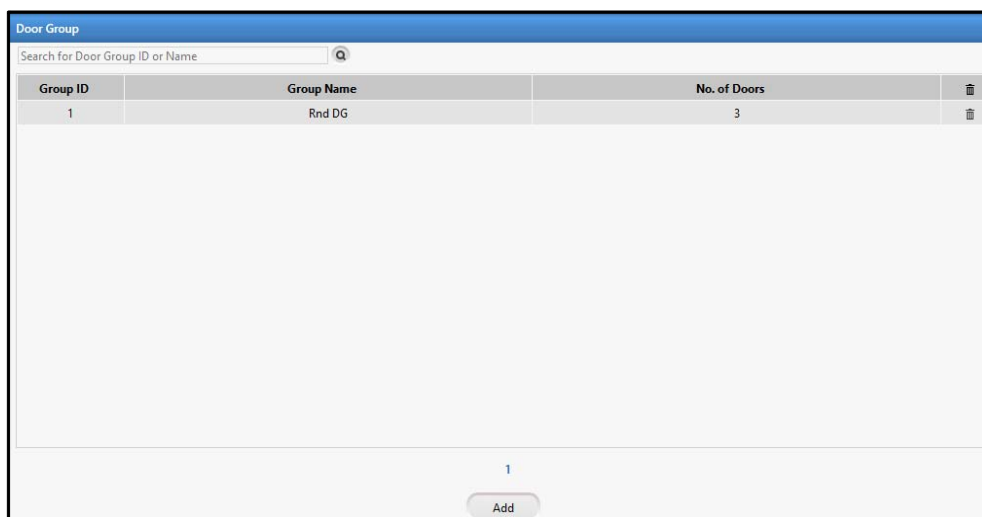
Door: Click the picklist and select the doors to be added in the door group. The list of doors will appear in the grid as shown below.



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



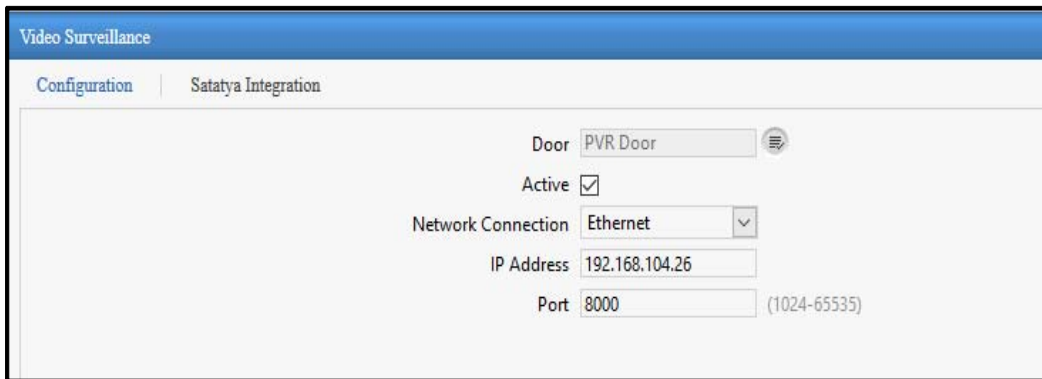
Once the door group is saved, you can view the door groups by clicking on **View List** button.



Video Surveillance

This page allows configuring Matrix Network Video Recorder (NVR) and Hybrid Video Recorder (HVR) with Panel lite V2 and get images and videos triggered by the user events at the door.

Configuration



The screenshot shows the 'Video Surveillance' configuration interface. It has two tabs: 'Configuration' and 'Satatya Integration'. The 'Configuration' tab is active. The form contains the following fields:

- Door: PVR Door (dropdown menu)
- Active:
- Network Connection: Ethernet (dropdown menu)
- IP Address: 192.168.104.26 (text input)
- Port: 8000 (text input) with a hint (1024-65535)

Door: Select the type of door controller for configuring video surveillance. The picklist shows all the configured doors.

Active: Check the box to activate the connection.

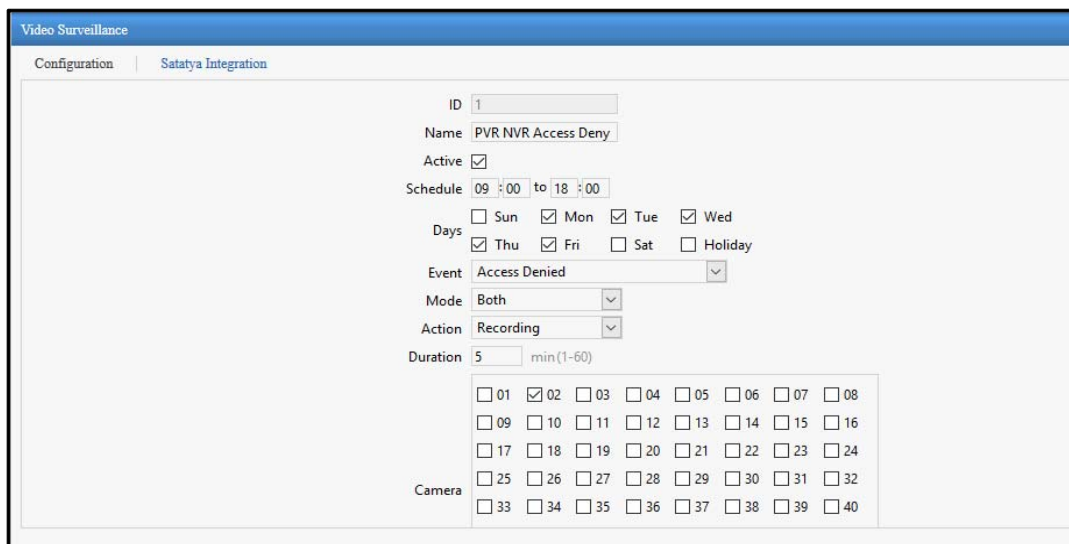
Network Connection: Select the Network connection from the options of Ethernet, Broadband, Wireless.

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.

Satatya Integration



The screenshot shows the 'Video Surveillance' configuration interface, specifically the 'Satatya Integration' tab. The form contains the following fields:

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

Name: Specify a user friendly name for the integration function.

Active: Check the Active box to enable the SATATYA integration functionality.

Schedule: Specify a schedule for the function by specifying the start and the end time (24 Hours format).

Days: Check the boxes for the applicable days of the week to run 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 resultant action is to be configured.

Mode: Select the event mode from the options of Entry, Exit and Both from the drop down list wherever applicable.

Action: Select the action for the Satatya device from the drop down list. The options available are:

- 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.

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 also configure another event-action linkage if required.

Card Format

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.

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.

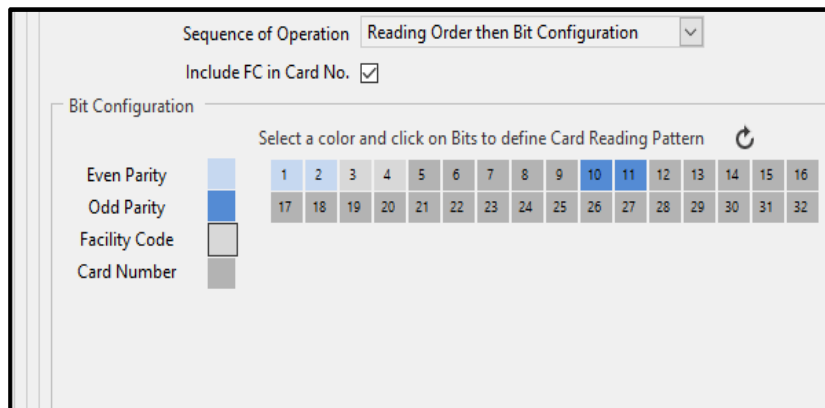
Configure (Bits): Specify the number of bits that will be configured in the card structure. If the number of bits received at the card reader is greater than the number of configured bits, then default card format will be applicable for the reader.

In the **Bit Configuration** section, 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 sequence of operation based on which operation is to be performed first and then second between Reading Order and Card Format Configuration.

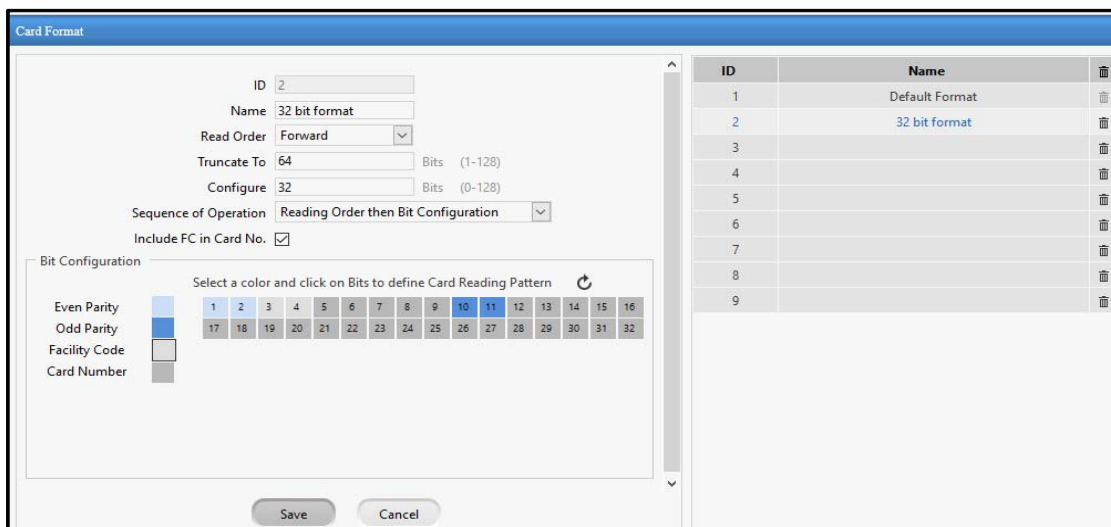
Include FC in Card No. Enable the Include FC in Card No. checkbox to ensure that the Card Number or Card ID includes Facility Code as well.



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 eg: 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

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' application window with two tabs: 'Fields' and 'Configuration'. The 'Configuration' tab is active, displaying a form for adding a new field. The form includes 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 window, there are page 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 using the drop-down list.

The screenshot shows the 'Card Personalization' application window with the 'Configuration' tab active. The form is configured for a Date field with the following settings:

- Field Name: Date of Birth
- Field Type: Date
- Date Type: ASCII
- Date Format: ddmmyy
- Separator: /
- Max Field Length (Bytes): 8

'Add' and 'Cancel' buttons are visible at the bottom of the form.

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.

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

Select a **Card Type** using the dropdown list. You can view the memory size of each card on hovering your mouse on the icon.

Card Mode

- 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, you can specify if the Card No. to be used is the original CSN, or UID (Universal Identifier number).
- Custom Mode:** If Custom mode is selected then location of all pre-defined fields will be allowed to be changed as per available memory sectors on the card. Maximum 99 newly created fields will be accepted for such card types.
 - Card No.:** If Custom Card Mode is selected, you can specify if the Card No. to be used is the original **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: If Card number is selected as Custom, then you can enable Read CSN option. This will allow to read CSN number in case the custom number gets failed to read.

For the Custom Card Mode, location on the card memory can be defined for each selected field. For this, select a **Field** using the picklist button.

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 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 weigand format and the second contains a grid consisting of created formats. You can also delete a particular format from the grid itself.

The parameters for configuring are as follows:

Name: Specify a name for the format. You can specify upto 6 formats.

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 not 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.

Facility Code

- Read From Card No.
- Read From Card No.
- Read From Card Memory
- Read FC from device config

Read from Device instead of Card No.: If access mode is kept as "Biometrics"/"Biometrics + PIN" and if FC is set to be read from card no. then FC will never be obtained, so in such cases which does not have card as any form of access mode, then FC stored in device can be sent by checking this box.

Replace with Card No.: When FC is not obtained then you can select the alternate option of card number to send for FC by enabling this check box.

Facility Code

Read From Card No.

Read from device instead of Card No.

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 will be automatically sent to all the devices to which this format is assigned.
2. The maximum bits of Facility Code and Card No. should be as defined in Card Personalization page of the Devices module. They should be selected one at a time.
3. At a time, Access Code should be of 1 bit only but user can select it to be of more than 1 bit and till maximum 20 bits.

Wiegand Format Saved Successfully

ID: 1
Name: Format1
Output Bits: 32

Color Selection For Output Bits

Even Parity	1	2	3	4	5	6	7	8
Odd Parity	9	10	11	12	13	14	15	16
Facility Code	17	18	19	20	21	22	23	24
Card No.	25	26	27	28	29	30	31	32
Access Code								
Blank								

Facility Code

Read From Card No.

Read from device instead of Card No.

Replace with Card No.

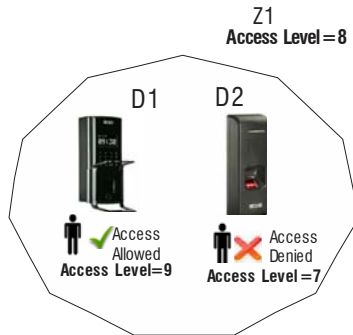
Save Cancel

ID	Name	
1	Format1	
2		
3		
4		
5		
6		

The Users section enables you to add users on the Panel lite V2 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 Panel lite V2.

A Panel lite V2 can have multiple Zones Z1, Z2, Z3 where each zone is assigned Access Levels (Z1-L8). Each zone can have multiple doors (Z1- D1, D2). The user is 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 denied.



The total number of users configured in Panel lite is shown as Total Users on dashboard. The number of Active Users, Inactive Users and Blocked Users is also displayed on the Dashboard as shown below.

Dashboard	Configuration	Monitor	Event Logs																													
<table border="1"> <thead> <tr> <th colspan="2">Devices</th> </tr> </thead> <tbody> <tr> <td>Total Devices</td> <td>8</td> </tr> <tr> <td>Online Devices</td> <td>1</td> </tr> <tr> <td>Offline Devices</td> <td>7</td> </tr> <tr> <td>Inactive Devices</td> <td>0</td> </tr> <tr> <td>Access Zones</td> <td>1</td> </tr> </tbody> </table>	Devices		Total Devices	8	Online Devices	1	Offline Devices	7	Inactive Devices	0	Access Zones	1	<table border="1"> <thead> <tr> <th colspan="2">Users</th> </tr> </thead> <tbody> <tr> <td>Total Users</td> <td>5</td> </tr> <tr> <td>Active Users</td> <td>5</td> </tr> <tr> <td>Inactive Users</td> <td>0</td> </tr> <tr> <td>Blocked Users</td> <td>2</td> </tr> </tbody> </table>	Users		Total Users	5	Active Users	5	Inactive Users	0	Blocked Users	2	<table border="1"> <thead> <tr> <th colspan="2">Access Schedule</th> </tr> </thead> <tbody> <tr> <td>Shifts</td> <td>1</td> </tr> <tr> <td>Schedule</td> <td>1</td> </tr> <tr> <td>Holiday Schedule</td> <td>1</td> </tr> </tbody> </table>	Access Schedule		Shifts	1	Schedule	1	Holiday Schedule	1
Devices																																
Total Devices	8																															
Online Devices	1																															
Offline Devices	7																															
Inactive Devices	0																															
Access Zones	1																															
Users																																
Total Users	5																															
Active Users	5																															
Inactive Users	0																															
Blocked Users	2																															
Access Schedule																																
Shifts	1																															
Schedule	1																															
Holiday Schedule	1																															

User Configuration

User Configuration enables to configure a user on the Panel Lite. This page displays a search criteria and grid containing a list of created users along with the details of user credentials, Access Group and Access Schedule. You can also edit or delete a user from the grid itself.



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.

Both Panel Lite and Panel Lite V2 supports a maximum of 25000 users.

User ID	User Name	Access Group	Access Schedule	Card(s)	Finger(s)	Palm(s)	
1	Rohan	Group-1		0	0	1	
2	Geeta	Group-1		0	0	1	
101	Khushbu	Group-1		0	0	1	

Add

To create new user click **Add** button and configure basic and advanced access control parameters.

Profile

User ID: Specify a unique User ID. It can have an alphanumeric value with a maximum of 10 characters.

User Name: Enter a name in this field that identifies the user. Maximum upto 45 characters allowed.

Active: Select this checkbox to activate this user.

Access Group: Assign an Access Group, Functional Group, Home Zone and Visit Zone to the user from the available options configured on the Panel Lite.

Functional Group: Select the functional group for the user from the dropdown list.

Assign Door: The doors configured in Panel Lite V2 will be assigned to the user.

To remove the assignment of particular door; click the picklist and delete the door from the list.

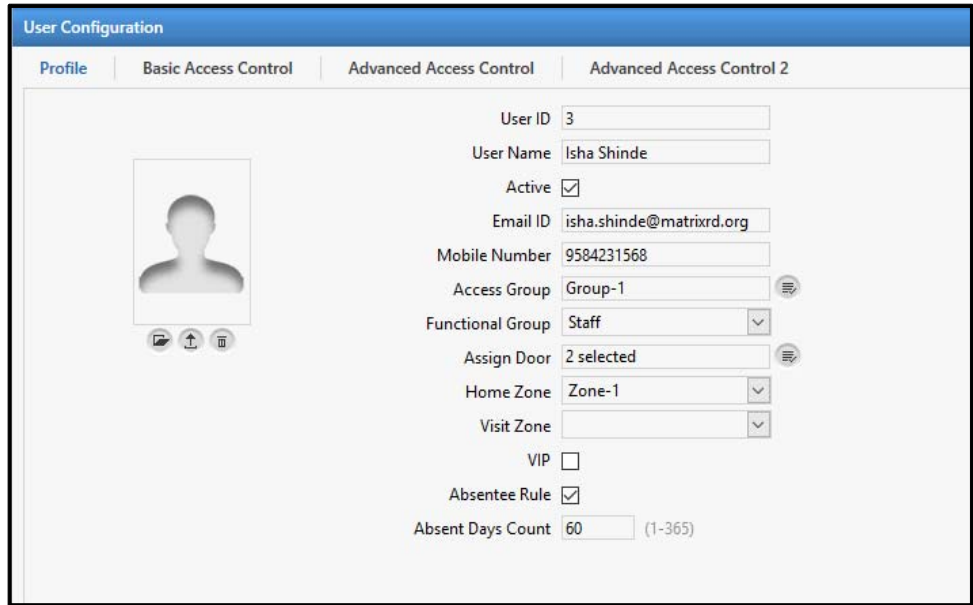
The **Door Group** picklist and **Door** picklist enables you to select the door groups or individual doors respectively for assigning to the user.

Home Zone: Select the home zone to be configured for the user from the dropdown list.

VIP: Check this option if the user is to be given unrestricted access rights.

Absentee Rule: Check this box to enable the Absentee rule at user level. This rule will allow you to configure maximum no. of days for user to be absent after which the user will be disabled/denied. However, this option needs to be first enabled at the Panel level. See *Absentee Rule*.

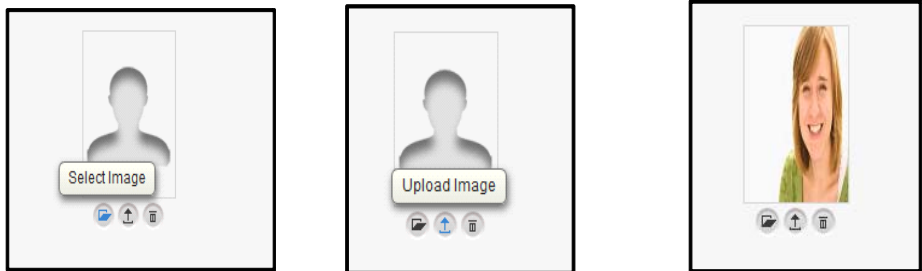
Absent Days Count: Specify the day count for the Absentee rule ranging from 1 to 365



The screenshot shows the 'User Configuration' window with the 'Profile' tab selected. The user details are as follows:

Field	Value
User ID	3
User Name	Isha Shinde
Active	<input checked="" type="checkbox"/>
Email ID	isha.shinde@matrixrd.org
Mobile Number	9584231568
Access Group	Group-1
Functional Group	Staff
Assign Door	2 selected
Home Zone	Zone-1
Visit Zone	
VIP	<input type="checkbox"/>
Absentee Rule	<input checked="" type="checkbox"/>
Absent Days Count	60 (1-365)

You can upload the image of user by clicking **Select Image** button and browsing the image. Then click **Upload Image** button to upload the image of user.



Then click on **Save** to save the Profile of user.

Basic Access Control

Credentials

PIN: Specify the PIN no. for the user. User PIN should be a numeric value ranging from 1 digit to a maximum of 6 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: Specify a card ID no. to be assigned to the user. The maximum value for the card ID is 20 digits. Specify a second card ID in the Card 2 field, if required.

Enrolled Fingers/Palm: This option displays the number of fingerprint/palm templates enrolled against the selected user.

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 an already provided access PIN, without the help of any operator or HR executive.

You must enable Self-Enrollment from Panel Configuration > Advanced Profile > Enrollment

The screenshot shows the 'User Configuration' window with the 'Basic Access Control' tab selected. The 'Credentials' section contains the following fields: PIN (16818), PVR Group No. (143), Card 1 (56321), Card 2 (empty), Enrolled Fingers (0), and Enrolled Palm (0). The 'Enable Self-Enrollment' checkbox is checked. The 'Validity' section has an 'Enable' checkbox checked and a 'Valid Upto' date of 31-12-2037. The 'Access Route' section shows a 'Route' of RnD Route. At the bottom, there are four buttons: Add, Delete, Save, and 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 in this field.

Access Route

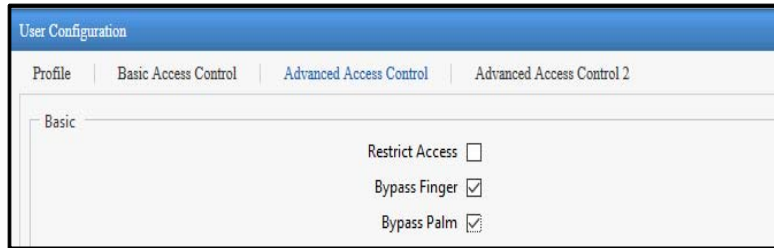
Route: Click **Select Route** button to assign a predefined access route to the user based on which user has to access the configured devices of the route. The Access Route is configured from Access Policies > Access Route.

Click on **Save** to save the Basic Access Control configurations.

Advanced Access Control

Basic

Restrict Access: Enable this to restrict access for the user on the Panel Lite. This implies that punches on the panel door will be considered for attendance only and will not open the door for access.



Bypass Finger/Palm: This option can be enabled in the event of the Finger/Palm Vein image not being in order and the system thus has problems identifying the user. In such cases, 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: Enable user access based on the shift working time of the user. If the Shift Based Access option is not enabled, then the default Access Settings will be applied as defined on the Panel Lite.

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 'Advanced Access Control 2' tab selected. The 'Smart Card Access Route' section is highlighted with a red box. It contains the following fields:

- Max Route Level: 75 (dropdown menu)
- Smart Card Access Route: RnD Smart Route (dropdown menu)

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: Select the Smart Card Based Access Route to be assigned to the user.

Mobile Based Access

The screenshot shows the 'Mobile Based Access' section with the following fields:

- Enable:
- IMEI: 345t3465677853476
- Enroll IMEI button

Enable: Enable this check-box to allow the user to access the COSEC device through the Mobile.

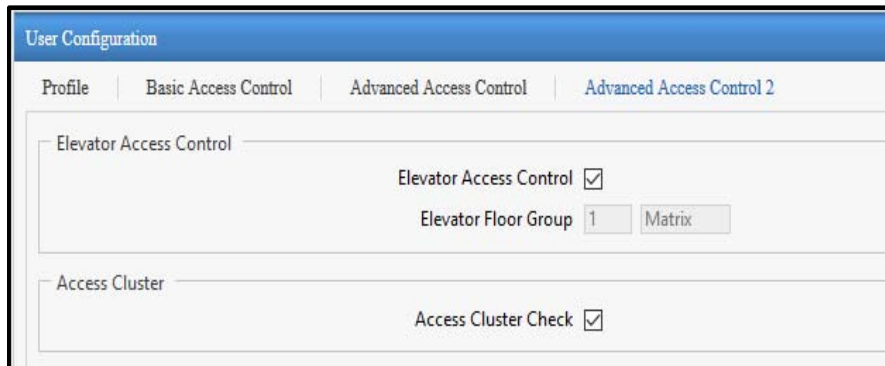
IMEI: Specify the IMEI (International Mobile Equipment Identity) number of the mobile to be registered. Click Enroll IMEI button to enroll a user for access COSEC device through mobile. On clicking the button, the enrollment for the selected user will be activated for 60 seconds.

Advanced Access Control 2

Elevator Access Control

Elevator Access Control: Enable the checkbox to allow the user to access the elevator. If disabled the user will not be allowed to access.

Elevator Floor Group: It displays the elevator floor group assigned to the user from Users Linking tab of Elevator Floor Group page.



The screenshot shows a web interface titled "User Configuration" with a blue header. Below the header are four tabs: "Profile", "Basic Access Control", "Advanced Access Control", and "Advanced Access Control 2". The "Advanced Access Control" tab is selected. The interface is divided into two main sections: "Elevator Access Control" and "Access Cluster".

In the "Elevator Access Control" section, there is a checkbox labeled "Elevator Access Control" which is checked. Below it, there is a label "Elevator Floor Group" followed by a dropdown menu showing "1" and a button labeled "Matrix".

In the "Access Cluster" section, there is a checkbox labeled "Access Cluster Check" which is checked.

Access Cluster

Access Cluster Check: Enable the checkbox to allow the user to access the cluster.

Click **Save** to apply the changes.

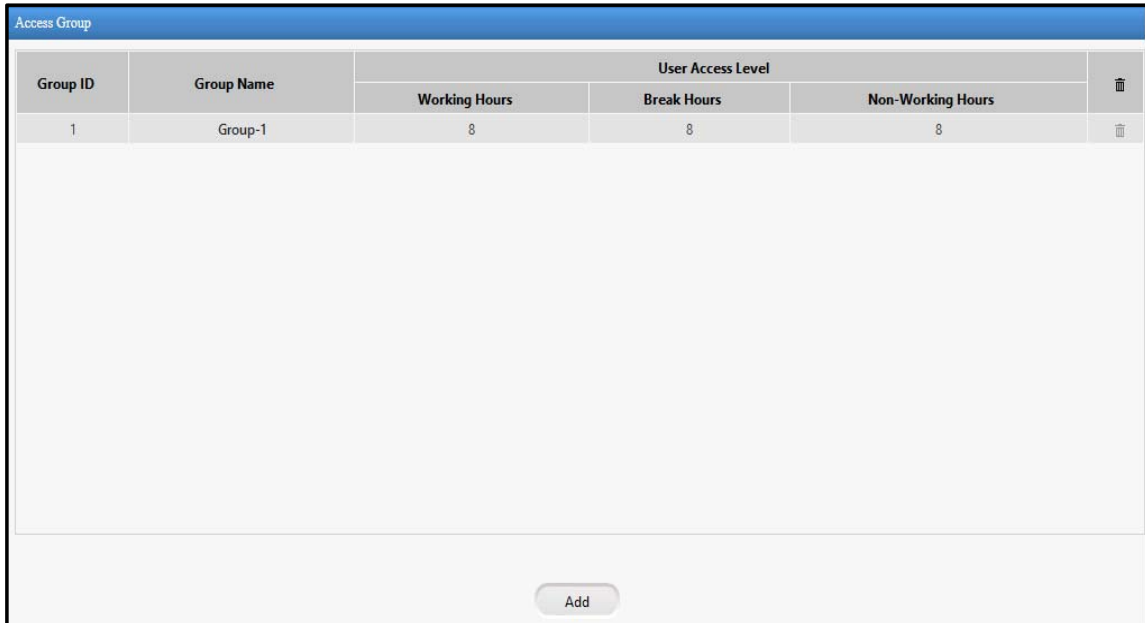
See *Access Policies > Access Clusters* for detailed configuration.

Access Group

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 needing equal privileges throughout the day. Access Groups have Time Zone based Access Levels programmed, and when assigned to a user, enable the determination of user Access Level at any particular time.

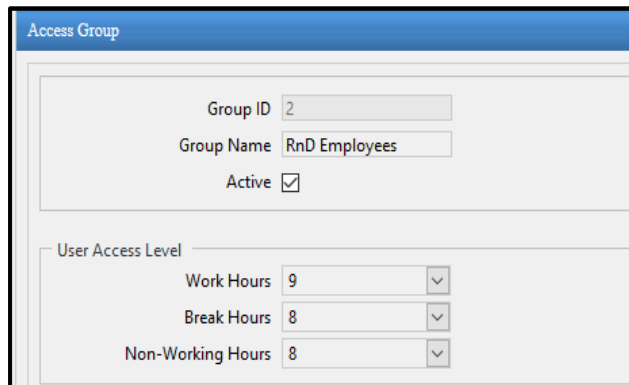
The Panel Lite compares Access Level of User with Access Level of the Zone before the user is Allowed or Denied to access the restricted areas. A maximum of 99 Access Groups can be defined in the system.



Group ID	Group Name	User Access Level			🗑️
		Working Hours	Break Hours	Non-Working Hours	
1	Group-1	8	8	8	🗑️

Add

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: ▼

The **Group ID** is auto generated by the system.

Group Name: Enter a suitable name for the new access group.

Select the **Active** checkbox to activate 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

Schedule Based Access Level Override

Time Zone: Lunch Time

Access Level: 9

Active:

Update Cancel

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: Enable this check-box to activate 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 the Schedule Based Access Levels will work 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.

Group ID	Group Name	User Access Level			Delete
		Working Hours	Break Hours	Non-Working Hours	
1	Group-1	8	8	8	Delete
2	RnD Employees	9	8	8	Delete

Functional Group

This page enables you to create a new Functional Group and view the created ones.

The screenshot shows the 'Functional Group' management interface. 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	

At the bottom of the interface, there are three buttons: 'Add', 'Save', and 'Cancel'.

To create a new functional group click **Add** button.

The screenshot shows the 'Functional Group' management interface after clicking the 'Add' button. The form on the left now has 'Group ID' set to '4' and 'Group Name' set to 'Factory'. The table on the right remains the same as in the previous screenshot:

Group ID	Group Name	
1	Staff	
2	Visitor	
3	Admin	

The 'Add' button is now disabled, and the 'Save' and 'Cancel' buttons are still visible at the bottom.

The **Group ID** is auto generated by the system.

Group Name: Enter a unique, user-friendly name for the Functional Group.

Click **Save** to apply the changes.

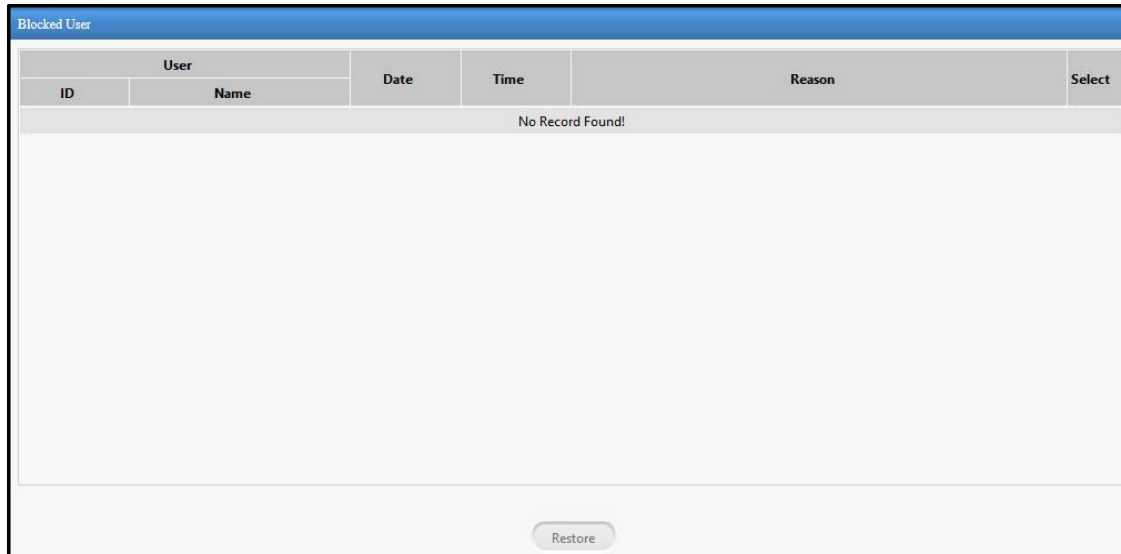
The screenshot shows the 'Functional Group' management interface after clicking the 'Save' button. The form on the left now has 'Group ID' set to '1' and 'Group Name' set to 'Staff'. The table on the right now has four rows, with the new group 'Factory' added at the bottom:

Group ID	Group Name	
1	Staff	
2	Visitor	
3	Admin	
4	Factory	

A 'Saved Successfully' message with a green checkmark icon is displayed in the top right corner of the interface. The 'Add', 'Save', and 'Cancel' buttons are still visible at the bottom.

Blocked User

Users whose credentials have been temporarily blocked due to inactivity for prolonged periods 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!					

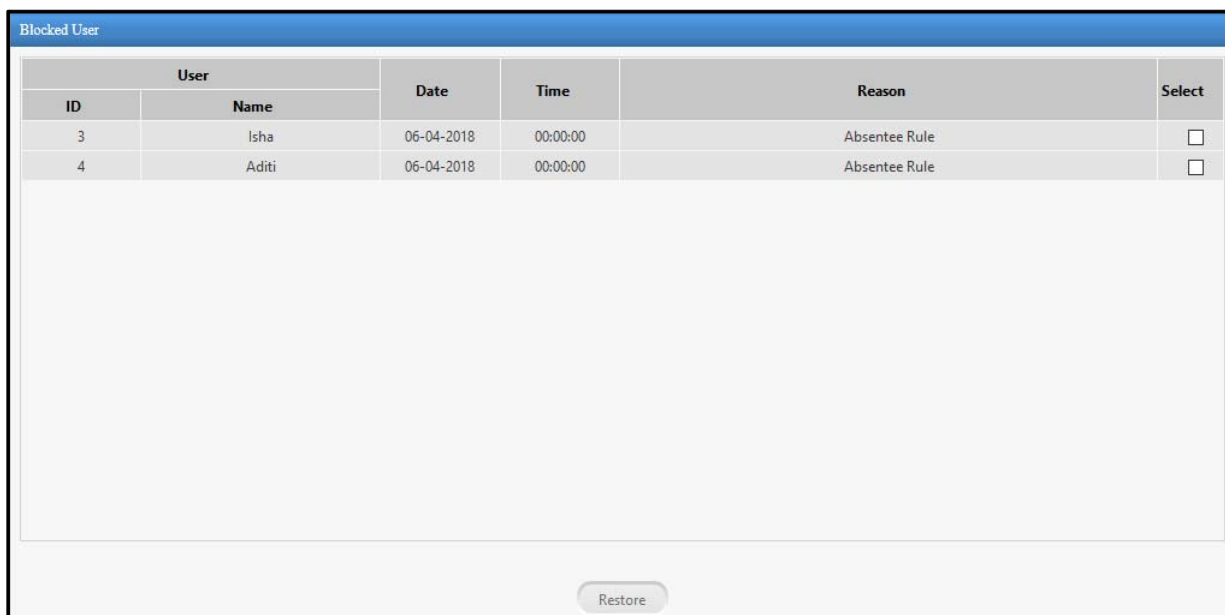
Restore

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)
- Failed Access attempts exceeded five
- The Use Count Control rule has been violated (Must be enabled from Access Features> Set1)



The other conditional violations that may lead to blocking of a user can be enabled from Panel Configuration > Access Features > Set 3



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 user and click **Restore** button to restore the user from blocked status.



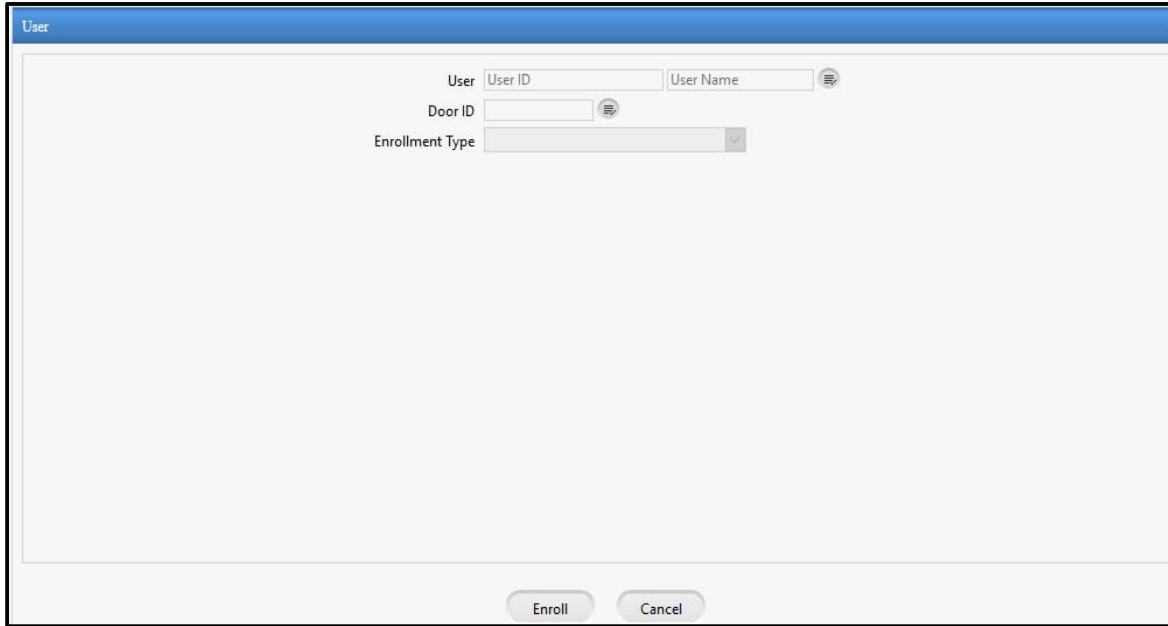
The Alert Service must be running to generate the Block User event.



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.

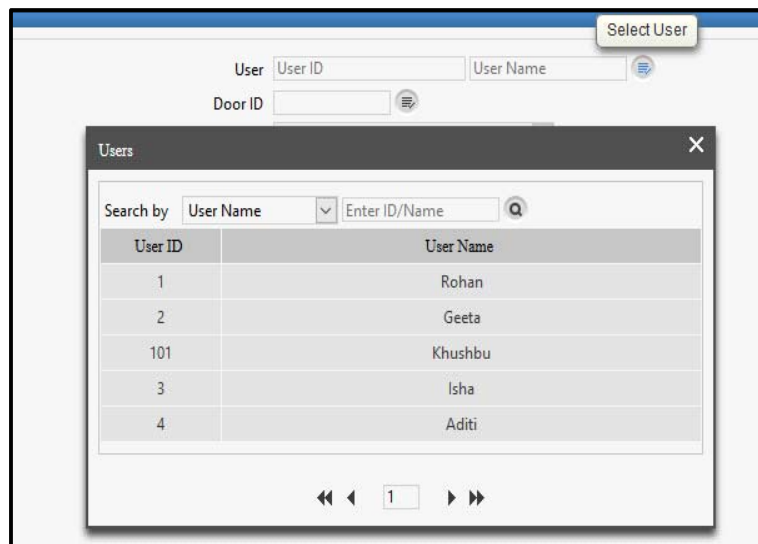
User

Once users have been added to the Panel Lite, the enrollment process can be initiated from this page. Enrollment can be defined as a process wherein the Panel Lite accepts and stores the user credentials against a particular user. It supports enrollment of user cards, finger print templates, palm 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 magnifying glass 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".

Select a **User** from the user picklist, for whom the enrollment is to be done.



The screenshot shows the same "User" enrollment form as above, but with a "Select User" picklist open. The picklist is titled "Users" and has a search bar with "Search by" set to "User Name" and a search input field containing "Enter ID/Name". Below the search bar is a table with the following data:

User ID	User Name
1	Rohan
2	Geeta
101	Khushbu
3	Isha
4	Aditi

At the bottom of the picklist, there are navigation arrows and a page number "1".

Select a Panel **Door** from the door picklist, on which the enrollment is to be performed for the user.

User 3 Isha

Door ID 1

Enrollment Type: Biometric

No. of Palms: Read Only Card, Smart Card, Biometric, Biometric Then Card

Specify the **Enrollment Type** from the dropdown list and specify the **number of credentials** to be enrolled for the selected type as follows:

1. For **Read Only Cards**, select the Number of Cards to be enrolled from the dropdown list.

User 3 Isha

Door ID 1

Enrollment Type: Read Only Card

No. of Cards: 1 Card

2. For **Smart Card**, select the number of smart cards to be enrolled. Check the boxes against the appropriate Details on Smart Card parameters. The following information can be written onto the Smart Card:

User ID

User Name

Facility Code (FC)

Additional Security Code (ASC)

Finger Template: Select the number of templates to be written on to the card from the dropdown list.

User 3 Isha

Door ID 1

Enrollment Type: Smart Card

No. of Cards: 1 Card

Smart Card Options: FC ASC
 User ID User Name

Smart Card With Personalized Details

Designation

Branch

Department

Blood Group N.A.

Emergency Contact

Medical History

Apart from the above, the following Additional Details on Smart Card can also be written:

Designation

Branch

Department

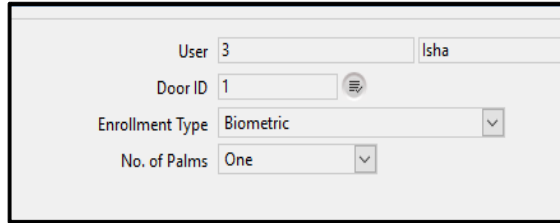
Blood Group

Emergency Contact

Medical History

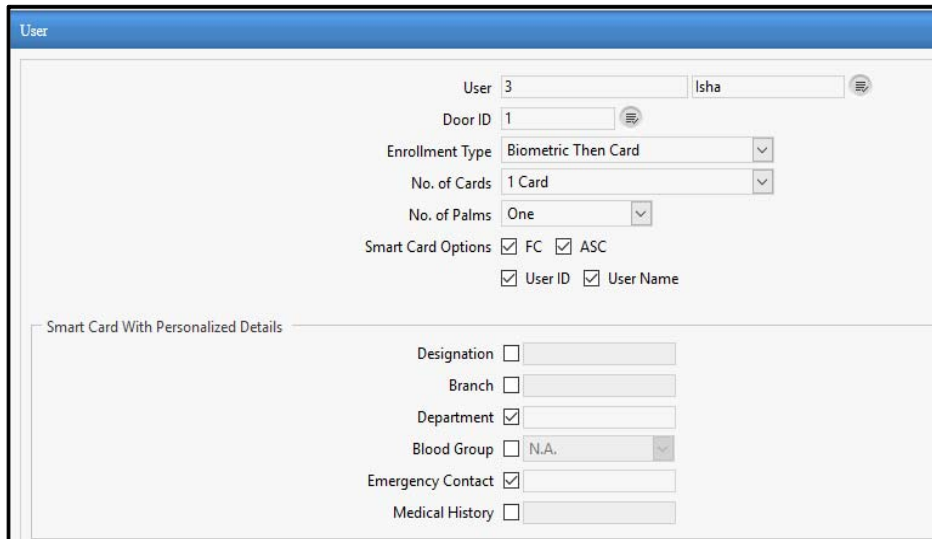
Check the box against the relevant personal detail entry and provide the relevant information in the respective fields.

- For **Biometric**, select the Number of Fingers/Palms to be enrolled from the dropdown list.



The screenshot shows a form for user configuration. The 'User' field contains '3' and 'Isha'. The 'Door ID' field contains '1'. The 'Enrollment Type' dropdown is set to 'Biometric'. The 'No. of Palms' dropdown is set to 'One'.

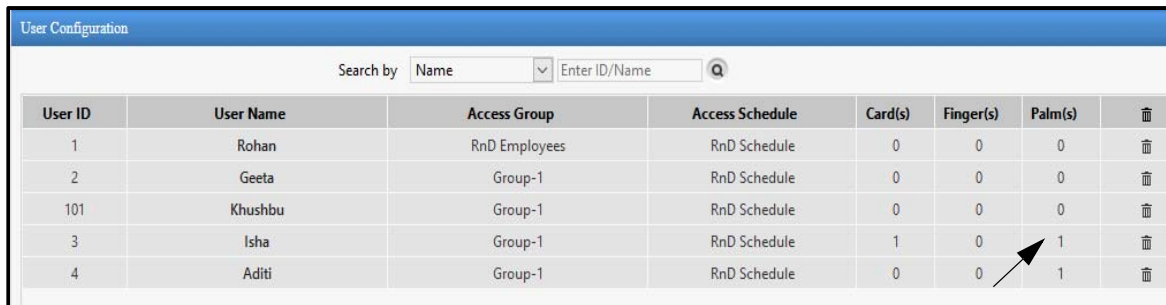
- For **Biometric then Card**, select the Number of Cards and Number of Fingers/Palms to be enrolled from the dropdown list.



The screenshot shows a form for user configuration. The 'User' field contains '3' and 'Isha'. The 'Door ID' field contains '1'. The 'Enrollment Type' dropdown is set to 'Biometric Then Card'. The 'No. of Cards' dropdown is set to '1 Card'. The 'No. of Palms' dropdown is set to 'One'. Under 'Smart Card Options', the checkboxes for 'FC', 'ASC', 'User ID', and 'User Name' are all checked. Below this, there is a section titled 'Smart Card With Personalized Details' with checkboxes for 'Designation', 'Branch', 'Department', 'Blood Group', 'Emergency Contact', and 'Medical History'. The 'Department' checkbox is checked, and the 'Blood Group' dropdown is set to 'N.A.'.

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 credentials for enrollment.

After the enrollment is successful, the number of credentials enrolled for a user can be viewed from User Configuration page as shown below.



The screenshot shows the 'User Configuration' page with a search bar and a table of user credentials. The table has columns for User ID, User Name, Access Group, Access Schedule, Card(s), Finger(s), Palm(s), and a delete icon. An arrow points to the 'Palm(s)' column for user ID 3, which has a value of 1.

User ID	User Name	Access Group	Access Schedule	Card(s)	Finger(s)	Palm(s)	
1	Rohan	RnD Employees	RnD Schedule	0	0	0	
2	Geeta	Group-1	RnD Schedule	0	0	0	
101	Khushbu	Group-1	RnD Schedule	0	0	0	
3	Isha	Group-1	RnD Schedule	1	0	1	
4	Aditi	Group-1	RnD Schedule	0	0	1	

SI User

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 he is not enrolled into that particular office's system.

The screenshot shows a web-based form titled "SI User". At the top, there is a "Door ID" field with the value "1" and a "Select Door" button. Below it is an "Enrollment Type" dropdown menu set to "Smart Card". A section titled "Smart Identification Options" contains several fields, each with a checkbox and an input field:

- Reference ID: []
- User ID: 12318
- User Name: Sonam
- Access Level: 1 (1-75)
- Validity Date: 29-03-2018 [Calendar icon]
- PIN: []
- Designation: Engineer
- Branch: []
- Department: []
- Blood Group: N.A. [Dropdown arrow]
- Emergency Contact: 8644425317
- Medical History: []
- Bypass Finger: []

At the bottom of the form are two buttons: "Enroll" and "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, Smart Card type of enrollment is displayed.

Smart Identification Options

Select the below appropriate parameters for writing in the smart card for SI user enrollment.

Reference ID: If reference ID is to be used for smart identification, then first enable the checkbox and then enter the ID. Maximum 8 digits of ID can be entered.

User ID: If User ID is to be used for smart identification, then first enable the checkbox and then enter the ID. User ID can be maximum of 10 characters.

User Name: If User Name is to be used for smart identification, then first enable 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 enable the checkbox and then specify the level. Its value can be from 1 to 75.

Validity Date: If Validity Date is to be used for smart identification, then first enable 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 enable 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 enable 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 doors.

Designation: If Designation is to be used for smart identification, then first enable the checkbox and then enter the designation.

Branch: If Branch is to be used for smart identification, then first enable the checkbox and then enter the branch name.

Department: If department is to be used for smart identification, then first enable the checkbox and then enter the department name.

Blood Group: If blood group is to be used for smart identification, then first enable 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 enable the checkbox and then enter the contact number.

Medical History: If medical history is to be used for smart identification, then first enable the checkbox and then enter the medical history.

Bypass Finger: Enable 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.

Click **Enroll** to enroll the user or click Cancel to cancel the changes made.

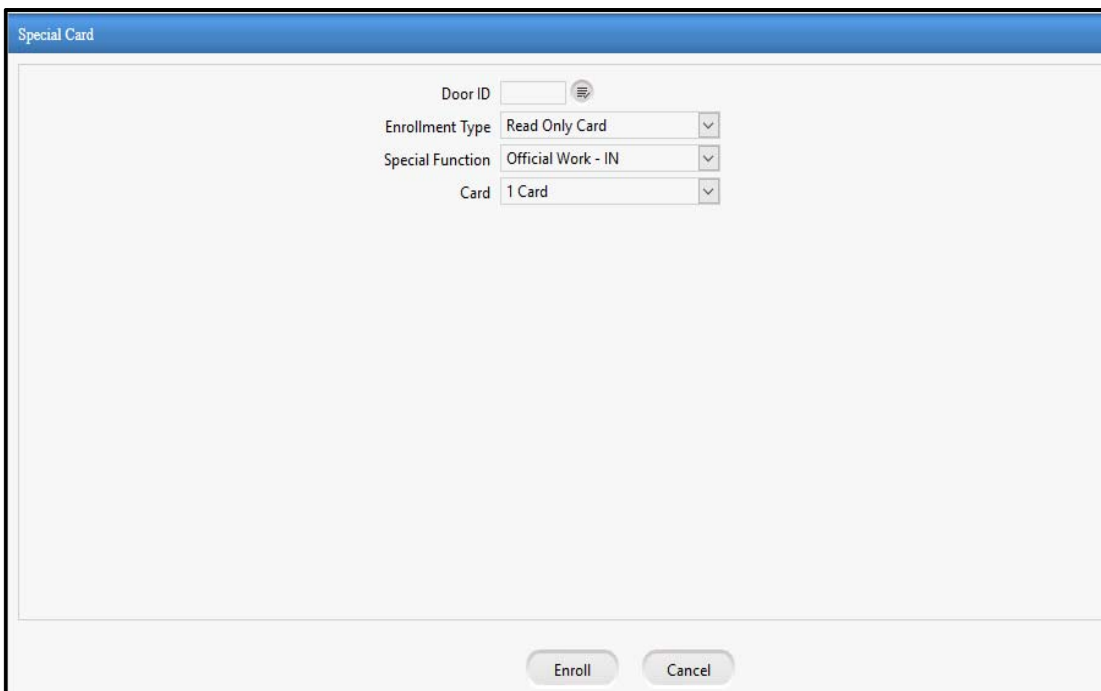
Special Card

A Special Card is an RFID card can be encoded for a special function and the card-holder can perform a special function at the device just by showing 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 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.

The enrollment for a special card can be initiated from this page.



The screenshot shows a web form titled "Special Card" with a blue header. The form contains the following fields:

- Door ID: A text input field with a picklist icon on the 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".

Select a **Door** using picklist on which the special card enrollment is to be performed.

Enrollment Type: Specify whether a Read Only Card or Smart Card is to be enrolled.

Special Function: Select a Special Function 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.

Authorization

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 biometric credential and card requires authorization for accessing the panel doors. This user authorization is done from this page.



The Enrolled credential of user goes to Authorization when “Authorization on Enrollment” is enabled from Panel Configuration > Advanced Profile > Enrollment

The Status column shows Pending, Authorized and Rejected applications.

User ID	User Name	Status	Authorize <input type="checkbox"/>	Reject <input type="checkbox"/>
3	Isha	Pending	<input type="checkbox"/>	<input type="checkbox"/>

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 check the box to Authorize or Reject the record.

The screenshot shows a window titled "Authorization" with a search bar and a dropdown menu for "User Status" set to "All". Below is a table with the following data:

User ID	User Name	Status	Authorize <input checked="" type="checkbox"/>	Reject <input type="checkbox"/>
3	Isha	Pending	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

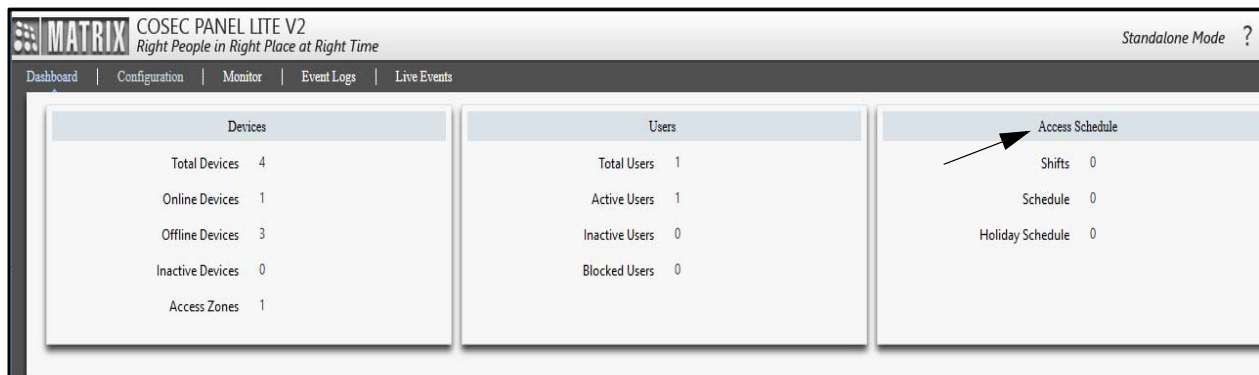
Then click **Save** to apply the authorization. Now the authorized user can use the credentials to access the door.

Access Policies & Access Schedule

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 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 rule.

The number of configured Shifts, Schedule and Holiday Schedules are displayed on the Access Schedule section of Dashboard as shown below.

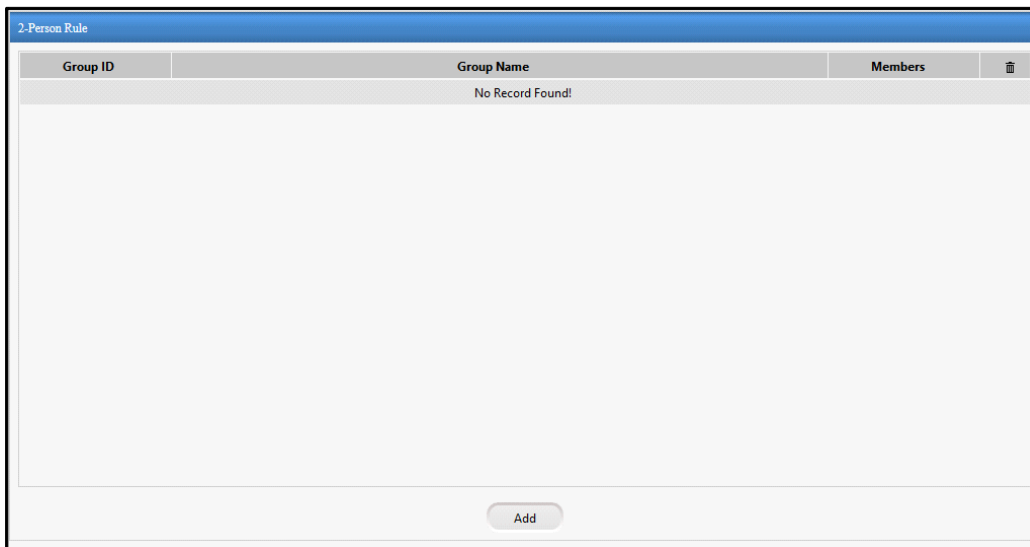


2-Person Rule

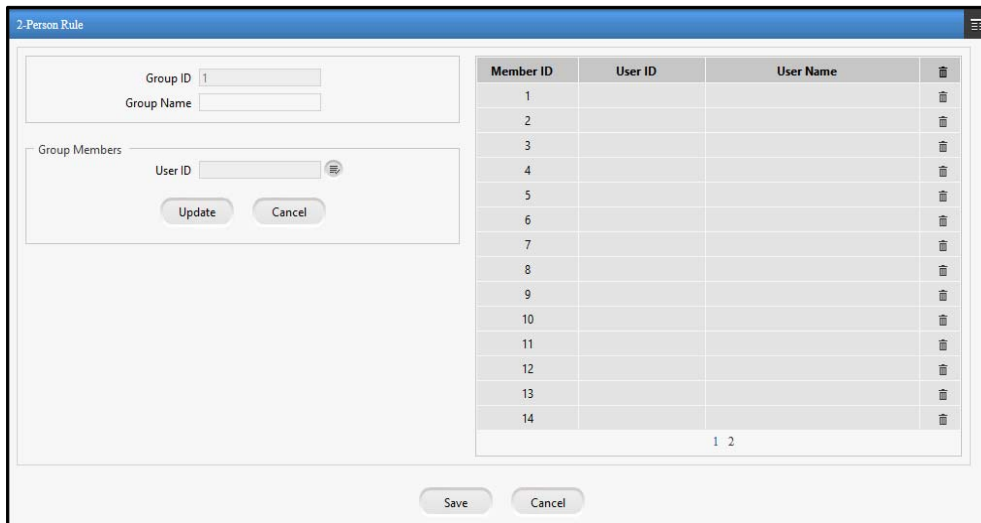
2-Person rule is a feature that enables the system to insist for two valid user entries within specified time to allow access to a secured zone.

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 of created 2-person groups along with its 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.



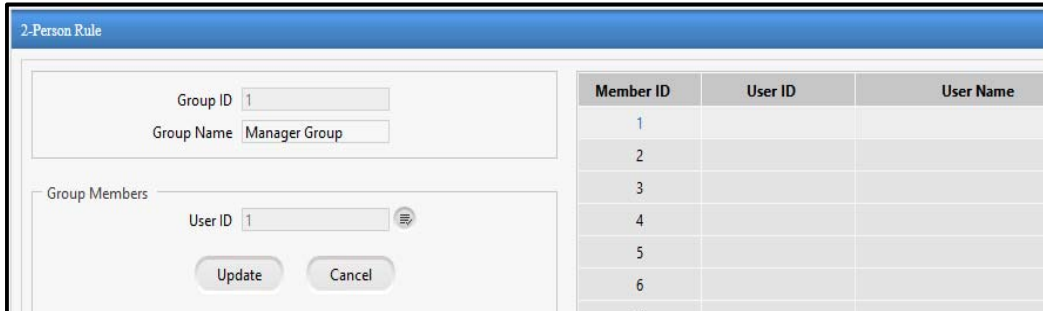
The **Group ID** will be autogenerated.

Group Name: Specify a user friendly name for the group.

Group Members

To add the members to the group click on the Member ID to which user is to be added.

User ID: Now click the user picklist to select the user.

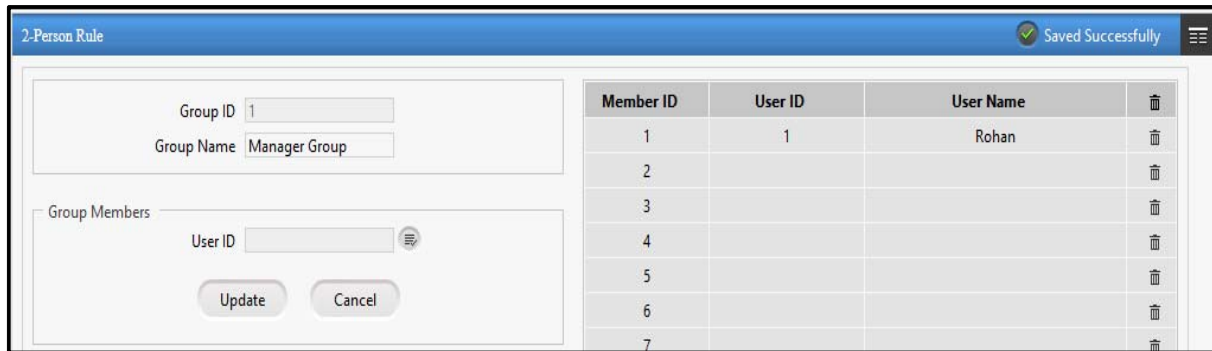


The screenshot shows the '2-Person Rule' interface. On the left, there are input fields for 'Group ID' (value: 1) and 'Group Name' (value: Manager Group). Below these is the 'Group Members' section, which includes a 'User ID' picklist (value: 1) and two buttons: 'Update' and 'Cancel'. On the right, there is a table with the following structure:

Member ID	User ID	User Name
1		
2		
3		
4		
5		
6		

After selecting the user click on **Update** to save the members to the grid.

Then Click on **Save** to save the group.



The screenshot shows the '2-Person Rule' interface after saving. A green checkmark and the text 'Saved Successfully' are visible in the top right corner. The 'Group ID' is 1 and the 'Group Name' is 'Manager Group'. The 'Group Members' section shows the 'User ID' picklist is empty. The table on the right is updated as follows:

Member ID	User ID	User Name	
1	1	Rohan	🗑️
2			🗑️
3			🗑️
4			🗑️
5			🗑️
6			🗑️
7			🗑️

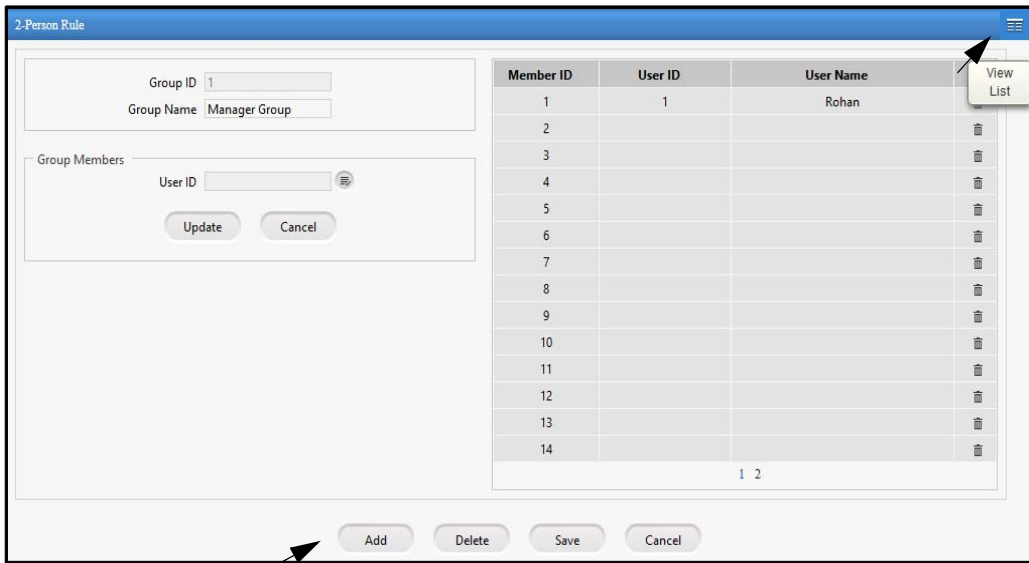
You can add more members to the group in the same way as described above.

The members or the group can be deleted by clicking Delete button.

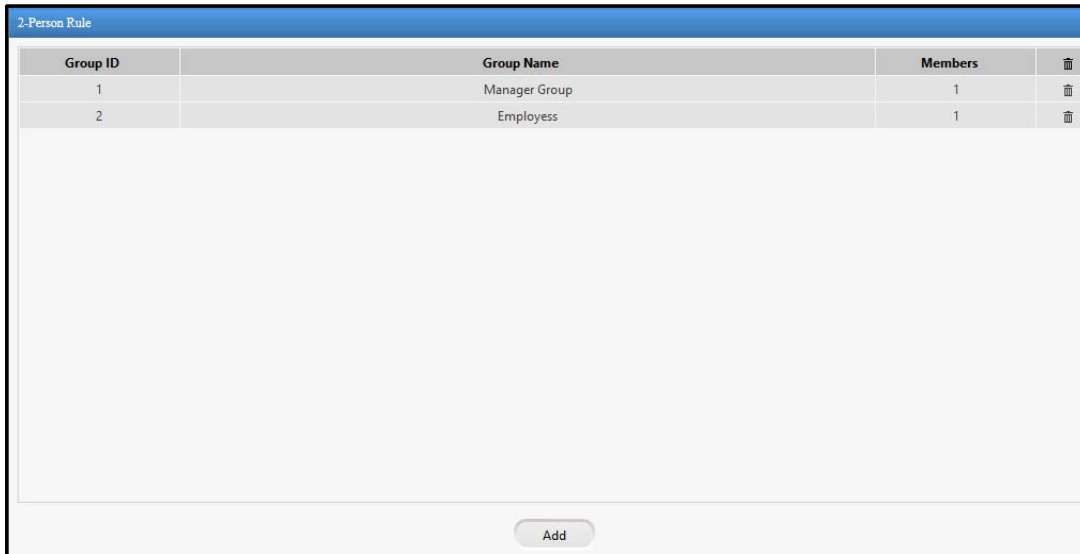


If the first person is an authorized user and the 2nd person is a VIP then, system considers the VIP as an authorized 2nd person to validate the 2 -person rule.

To add another group click **Add** button.



To view the added groups click **View list** button.

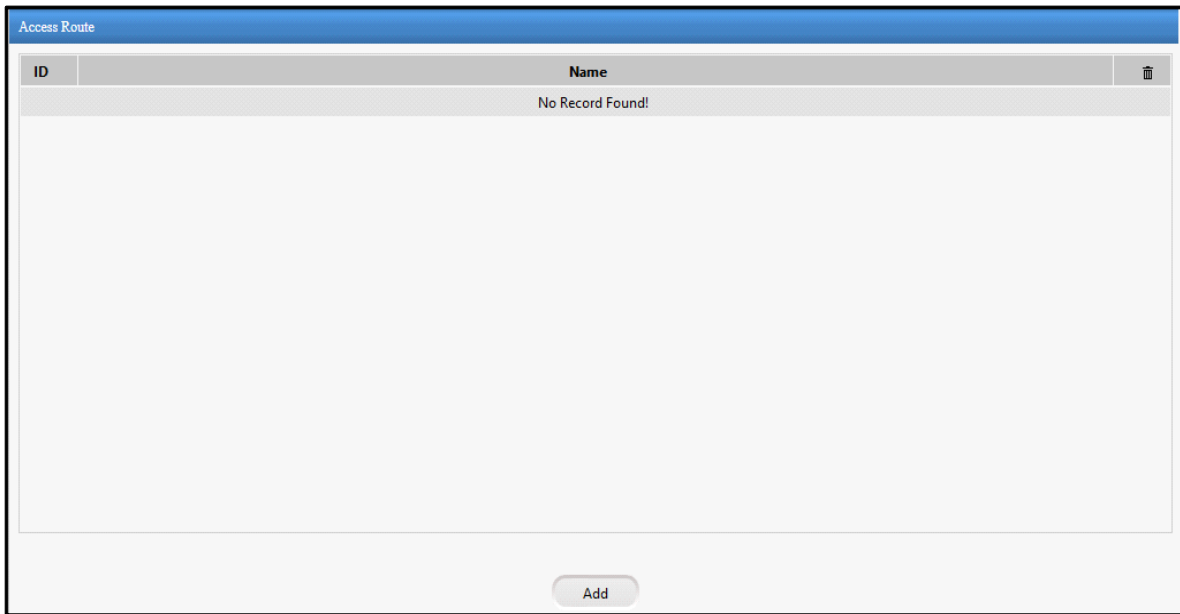


After creating groups for 2 person rule, you must enable the rule from Panel Configuration> Access Features> Set1
 Then configure the rule at Zone Configuration > AdvanceConfiguration1.
 Now this rule will be applicable for those doors who are assigned the zone which is enabled for the rule.

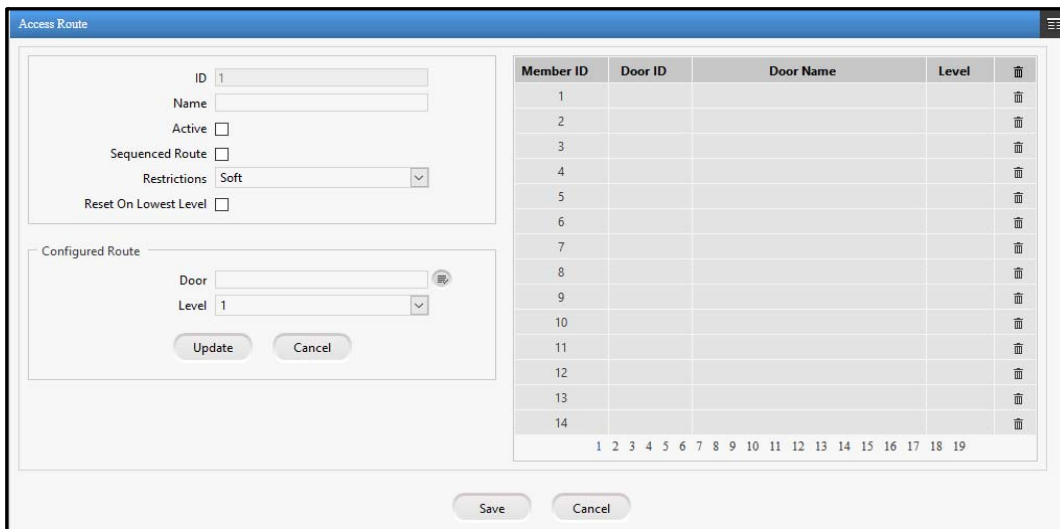
Access Route

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 its 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.



The ID will be autogenerated.
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 be required to follow.

In case of the sequenced option the system checks on the route based on the levels defined. For e.g. the user has to swipe the credential on a 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 of Soft and Hard.

- **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 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 in the event of the user 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 happen only on entry side.

Configured Route

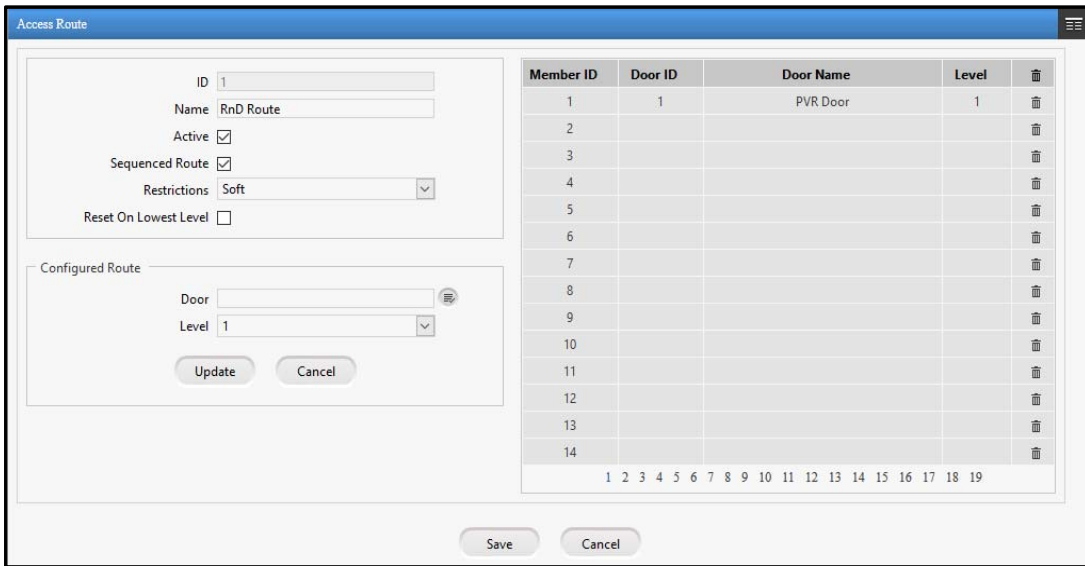
Door: To select the Member Doors for the Access Route, click on the Member ID from the right side grid to which door is to be assigned.

Then click on the Picklist button to select the appropriate Panel door from the Device Picklist.

Level: Select the Level number for the Door from the dropdown list.

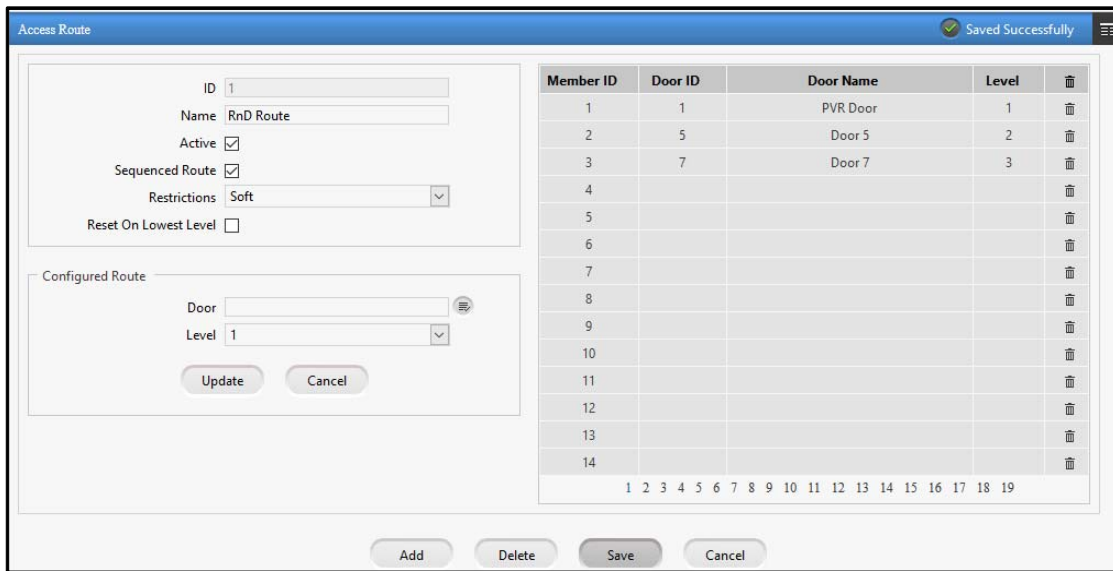
Multiple Doors can be assigned to a single level. However, the same door cannot be assigned to multiple levels.

Click on **Update** to save the door. You can define 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	

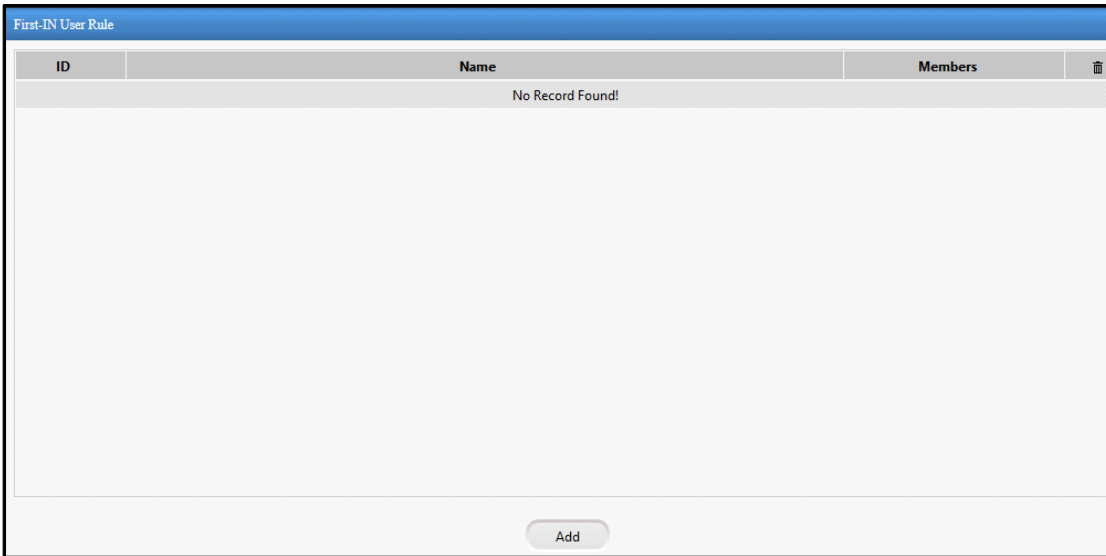


After configuring the Access Route, you must enable the rule from Panel Configuration> Access Features> Set1
Then it must be assigned to the user from User Configuration> Basic Access Control.

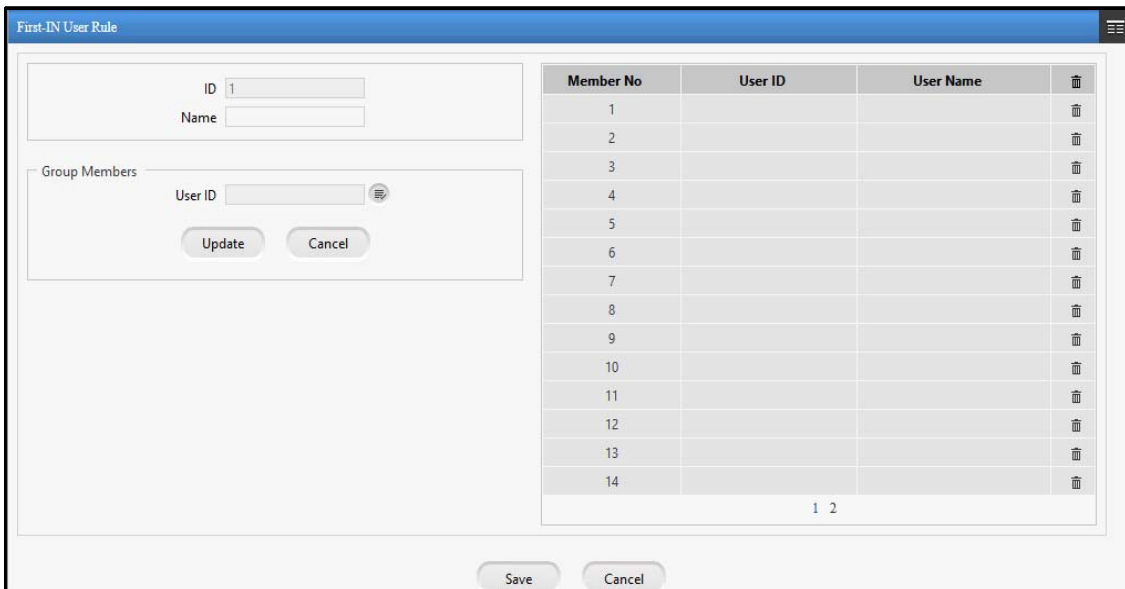
First-IN User Rule

First-IN User rule uses a card or biometric credential of the user who is declared as First-IN User to unlock the Access locked to a particular zone.

The page will display a list of created rules along with its 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.



The **ID** will be autogenerated.

Name: Specify a user friendly name for the Group of First-In users.

Group Members

User ID: To select the user members, click on the Member No. to which user is to be assigned. Then click on the Picklist button to select the user from the Picklist.

Click on **Update** to save the user member. You can define upto 25 person per 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 enable the rule from Panel Configuration> Access Features> Set1

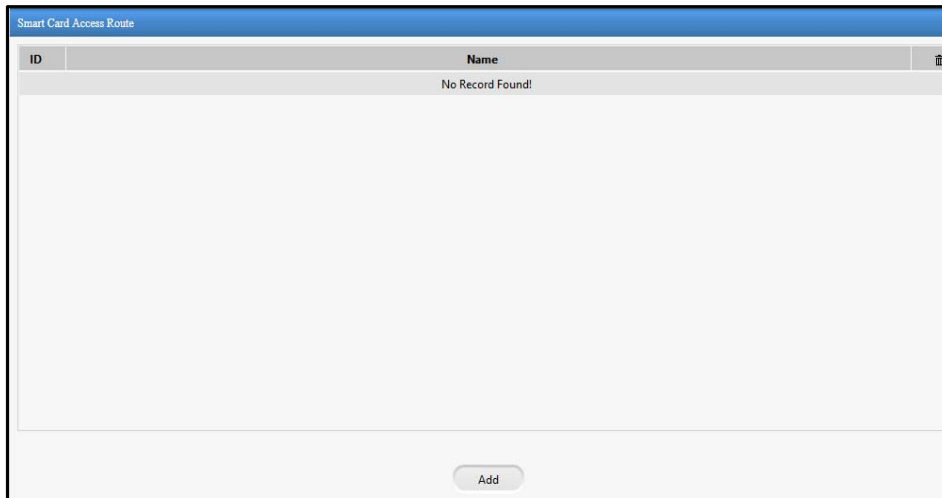
Then configure the rule at Zone Configuration > AdvanceConfiguration2.

Now this rule will be applicable for those doors who are assigned the zone which is enabled for the rule.

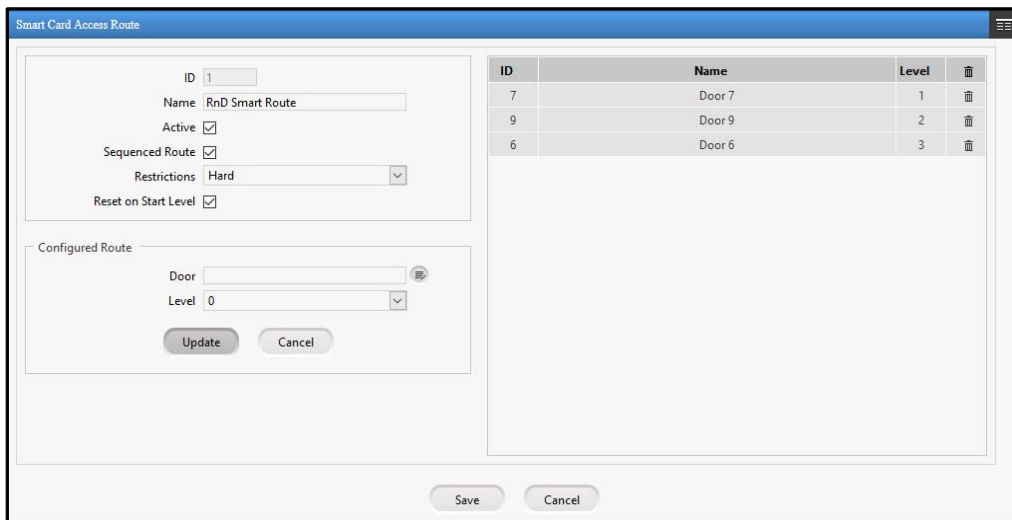
Smart Card Access Route

The Access Route using cards 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 its 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.



The **ID** will be autogenerated.

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 sequence.

The Smart Access Route can be defined as sequenced or un-sequenced by checking or unchecking the Sequence Route box.

Restrictions: Select the Restriction from the drop down options of Soft and Hard.

- **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: Check the box to enable the system to reset the current level status to allow access on the lowest level.

This option is useful in the event of the user 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 happen only on entry side.

Configured Route

Door: To select the member Doors for the Access Route click on the Picklist button to select the Device.

Level: Select the Level number for the Door from the dropdown list.

Click on **Update** to save the devices 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 to a full 24-hours or any 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 interface. The 'Configuration' tab is active, displaying fields for ID, Name, Active checkbox, Start Time (00:00), End Time (00:00), and Active Days (Sun, Mon, Tue, Wed, Thu, Fri, Sat, Holiday). An 'Add' button is visible at the bottom. To the right, a table lists existing time zones:

ID	Name	
1	Time Zone 1	

Configuration

The configuration tab enables to create time zone by clicking **Add** button and providing the following parameters.

The **ID** will be autogenerated.

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.

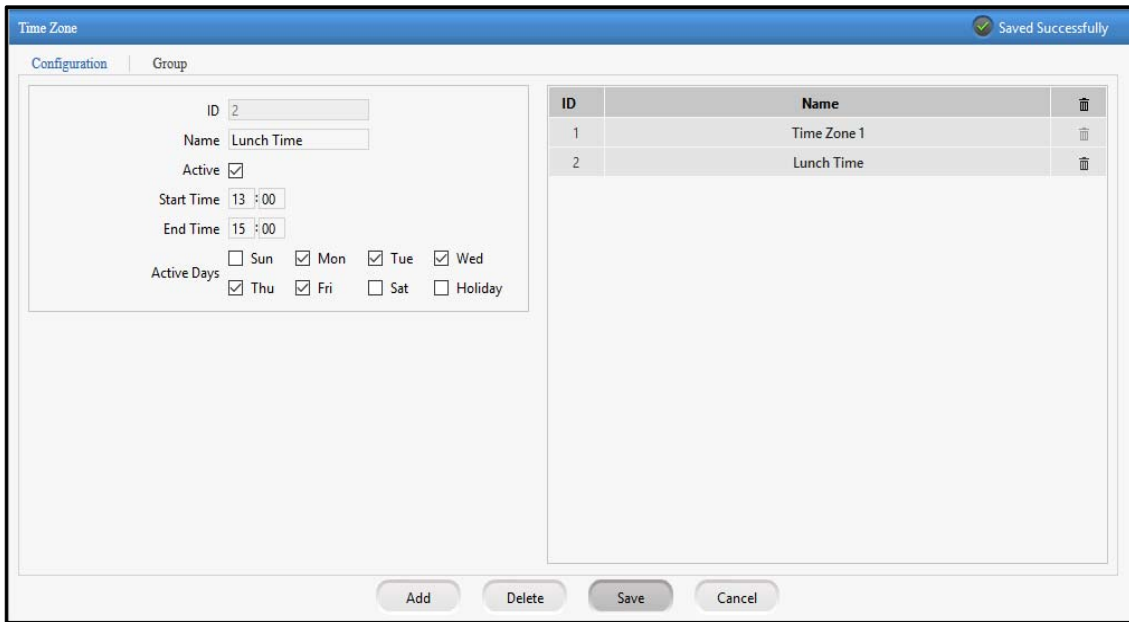
Active Days: Select the days checkbox for which the Time Zone is to be activated.

There is provision for the Holidays to be overruled if required. This can be done by not checking the Holiday box.

The screenshot shows the 'Time Zone' configuration interface with the 'Configuration' tab active. The fields are filled with the following values: ID: 2, Name: Lunch Time, Active: checked, Start Time: 13:00, End Time: 15:00, and Active Days: Mon, Tue, Wed, Thu, Fri. The table on the right shows the existing 'Time Zone 1' entry.

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 to create time zone groups by clicking **Add** button and providing the following parameters.



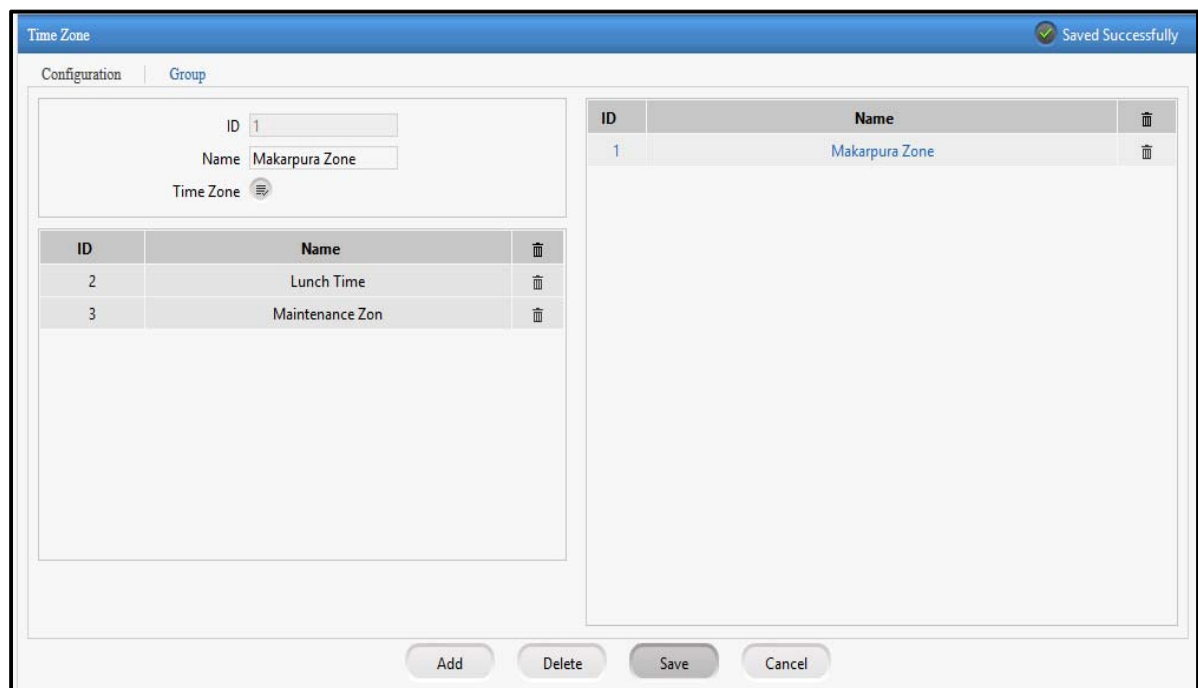
ID: It displays ID of the time zone group.

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.

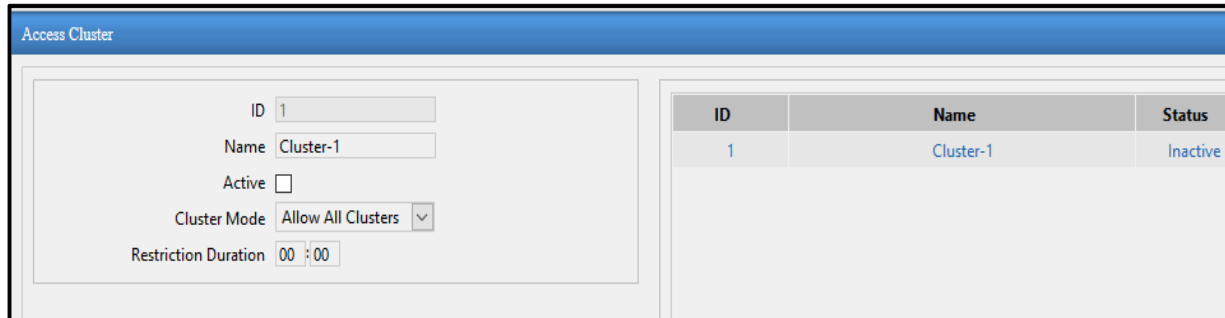


After configuring the Time Zone, you can assign to the Schedule based Access level override in Users > Access Group.

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: Enable the Active check-box to activate 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.
- **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).

Suppose 3 clusters are configured in Panel lite.

1. For first cluster, mode selected is **Allow All Clusters** and restricted duration configured is 2hrs and 30 mins.
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

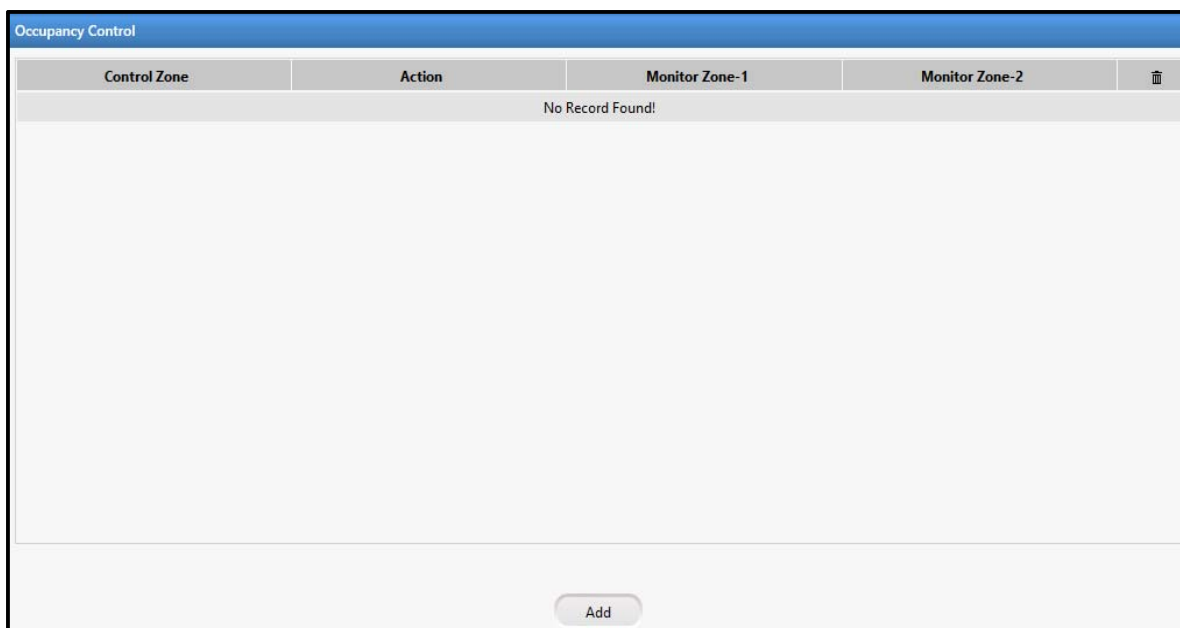
Occupancy Control

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 its 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 enter the following details.

Control Zone: 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 condition in Monitor zone fails.

- **Alarm:** On violation of occupancy rule; Alarm will be generated after the elapse of Alarm timer.
 - **Alarm Timer:** It defines the time for which device will wait for satisfaction of occupancy rule. Alarm timer (0 to 999 seconds) is user configurable. On violation of occupancy rule "Occupancy violated" alarm will be generated after the alarm timer elapses and user is allowed to either enter or exit the zone.
- **Restrict:** On violation of occupancy rule user won't be allowed to enter or exit the zone.

Check Conditions For: Select the option as **Any One Zone** or **Both Zones** to check the **Avoid Occupancy** condition for the respective zone.

Monitor Zone-1: Select the monitor zone1 from the picklist.

- **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.

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 access allowed but occupancy will be violated. The occupancy violated Alarm will be generated 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 access allowed 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 Panel Lite V2> 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 access allowed.
- When user2 punches on PVR (zone2), he will also be access allowed.
- 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 are already occupied in zone2.



The IN- OUT punches are stored in memory of Panel lite. 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. This will raise the alarm 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 Panel lite V2:

- 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 zone then Alarm will be generated after the duration of Alarm Timer when the user punches in Control zone.
- If **Both Zones** is selected then occupancy avoidance condition will be checked for both the zones. And alarm will be generated in control zone if occupancy is violated in both the monitor zones.
- When user1 punches on Door V3-115 (Zone-3), he is access allowed. When user2 punches on Door V3-115 (Zone-3), he will be also be access allowed. But this is violating occupancy >1
- Now when user3 punches on Door V3 (Zone-1) then he will be access allowed but after 2 seconds alarm will be generated.



Similarly if Action= Restrict; then user3 will be access denied on Door V3.

If Check Conditions For = Both Zones, then occupancy in PVR door will also be monitored.

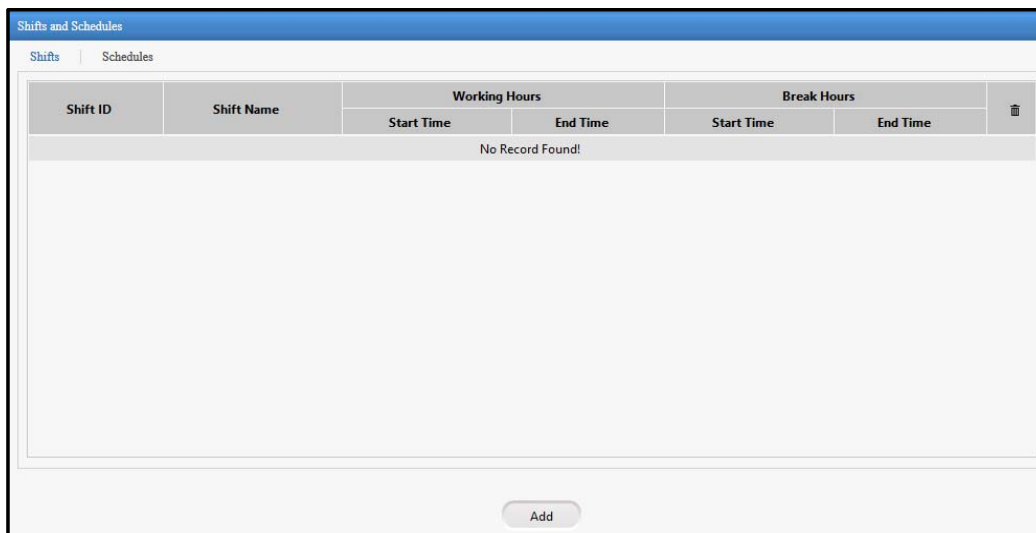
Shifts and Schedules

Shift Schedules are detailed chart indicating the working hours and break hours of employees. It defines the details like timing, no. of days, shift rotation, rotation count etc for each shift configured.

It enables the user to group multiple shifts into a single entity called Schedule 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



The Shifts can be configured by clicking **Add** button.

Shift Code: Specify a descriptive Shift code. For eg. GS for General Shift.

Name: Specify the user friendly name of the shift.

The screenshot shows the configuration form for a new shift. The form is titled 'Shifts and Schedules' and has tabs for 'Shifts' and 'Schedules'. The form fields are as follows:

- Shift Code:
- Name:
- Shift Type: ▼
- Working Hour Details:
 - Start Time:
 - End Time:
- Break Hour Details:
 - Start Time:
 - End Time:

Shift Type: Select the type of shift from the options of Normal, Field Break and Rest Day.

- **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 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.

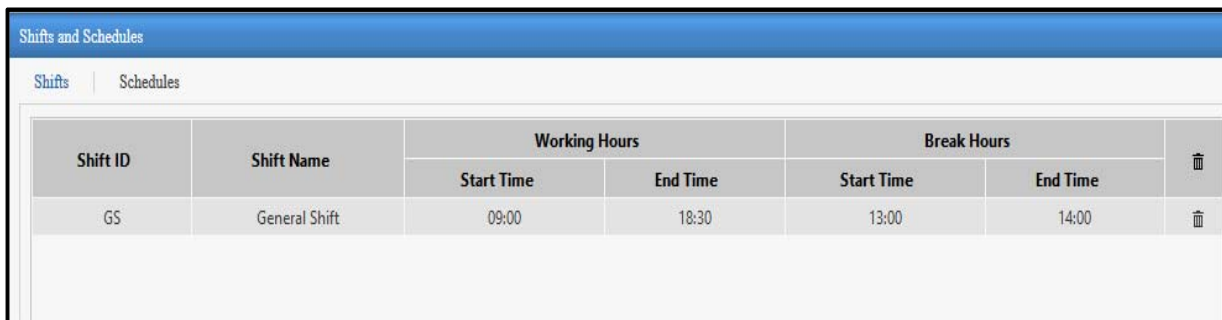
End Time: Specify the End Time of the shift in hh:mm format. The Shift duration or the total working hours of the shift is the difference of end time and start time.

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.

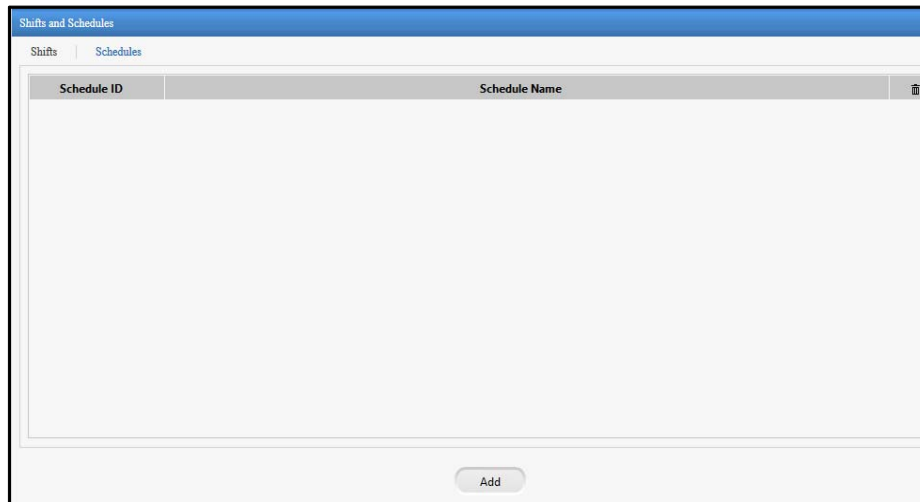
Click on **Save** to save the configured Shift. Similarly you can configure other shifts. You can click on **View list** button to view the list of configured shifts as shown below.



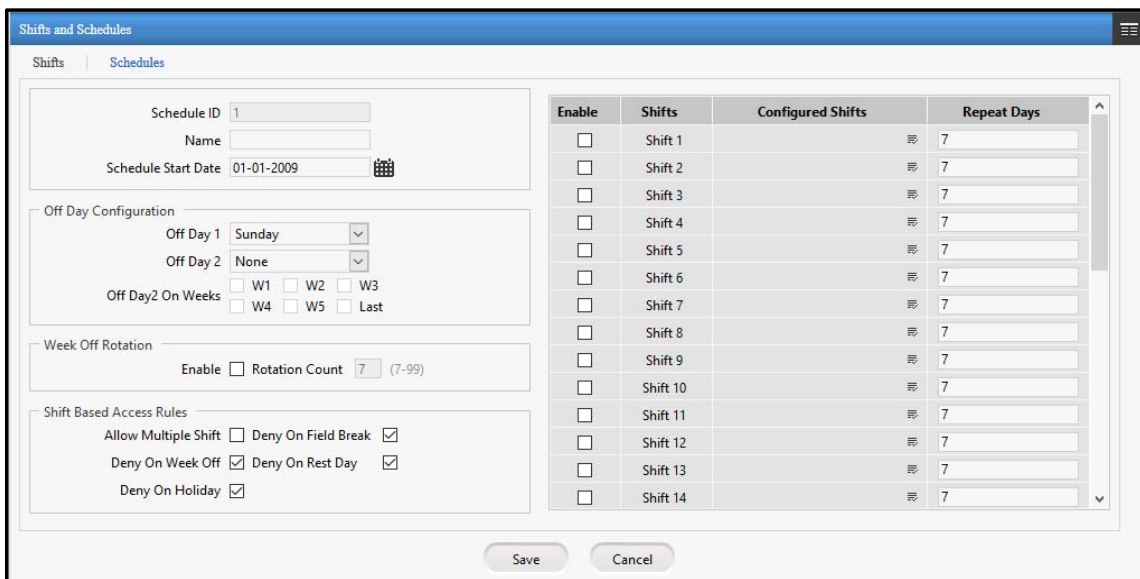
Shifts and Schedules						
		Working Hours		Break Hours		
Shift ID	Shift Name	Start Time	End Time	Start Time	End Time	🗑️
GS	General Shift	09:00	18:30	13:00	14:00	🗑️

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

The **Schedule ID** will be 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 the Schedule will be started.

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 enable the Off Day rotation enable the check-box.

Rotation Count: Specify the Rotation Count for rotating single or both week offs as configured. However, Rotation Count can not 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 check the Allow Multiple Shift box.

Deny on Field Break: To deny access on field break days check the Deny on Field Break box.

Deny on Week Off: To deny access on Week Off days check the Deny on Week Off box.

Deny on Rest Day: To deny access on Rest Day check the Deny on Rest Day box.

Deny on Holiday: To deny access on Holiday check the Deny on Holiday box.

To add the shifts to the schedule check the Enable box in the grid. Select the configured shift from the shift picklist.
Repeat Days: Specify the number of days for the selected shift to repeat 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

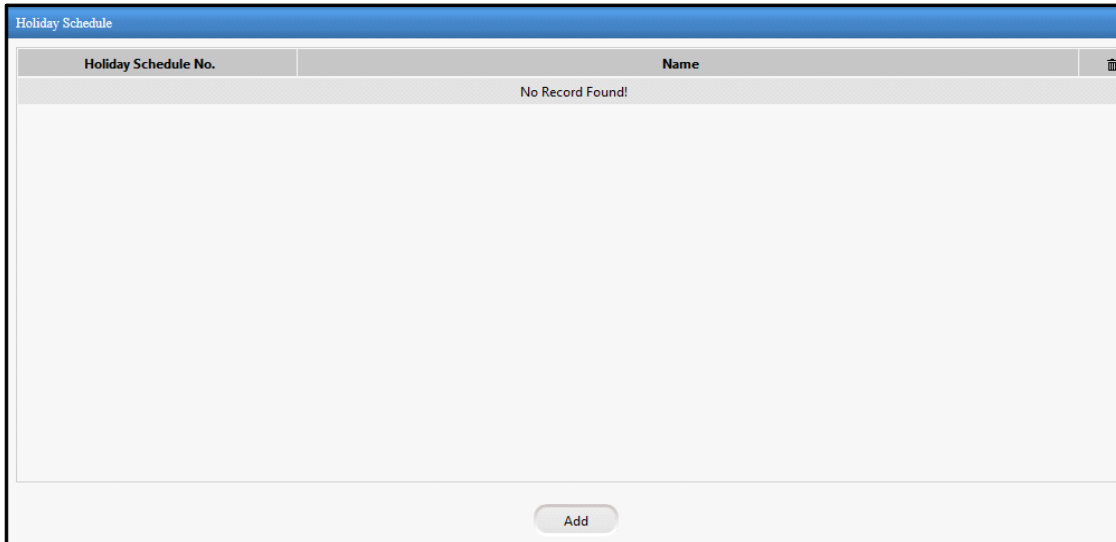
Add



The 1st schedule will get assigned to all the users and will be displayed on User configuration page. But you have to enable it for the desired user from User Configuration > Advance Access Control > Shift Based Access.

Holiday Schedule

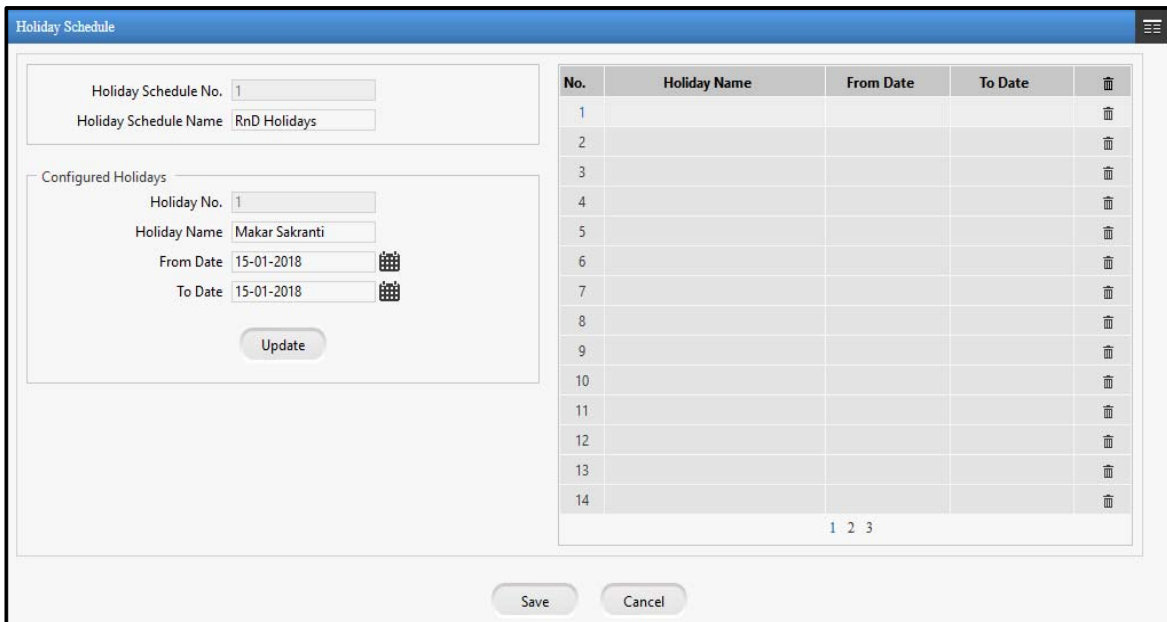
Holiday Schedule is a list of non-working days in a calendar year which are user defined. The user can define up to 32 holidays in a schedule.



The Holiday Schedule can be configured by clicking **Add** button.

The **Holiday Schedule No.** will be 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 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 holiday:

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 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 are buttons for 'Add', 'Delete', 'Save', and 'Cancel'. The 'Save' button is highlighted.

Click on **View List** button to view the list of holidays.

The screenshot shows the 'View List' button. It displays a table with the following data:

Holiday Schedule No.	Name	
1	RnD Holidays	🗑️

An 'Add' button is located at the bottom of the table.



The holiday schedule can be assigned to the user from User Configuration > Advance Access Control > Shift Based Access.

System Maintenance & About

The Panel lite V2 firmware version can be viewed from About page. It also shows IP address and MAC address of the Panel lite.

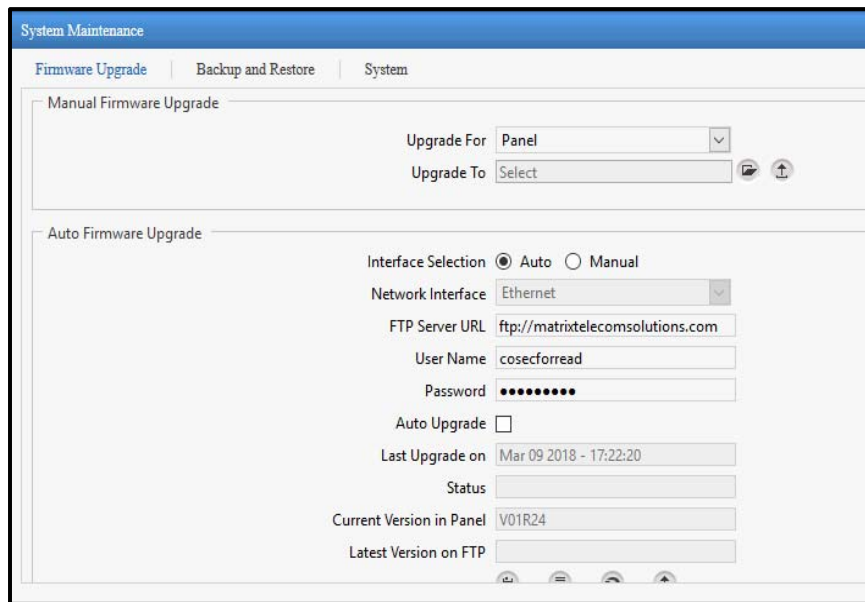
The firmware of panel lite can be upgraded manually or automatically from the System Maintenance page. The Event backup and configuration backup can be taken manually or you can schedule the backup.

See respective sections for details.

System Maintenance

System Maintenance enables to take Backup and Updation of Firmware, Restore configuration and manage System Settings.

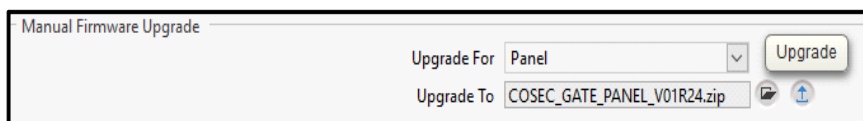
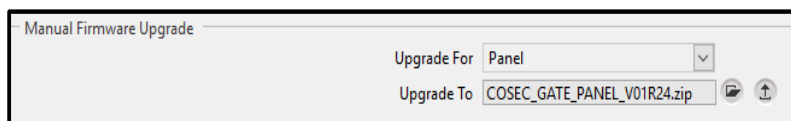
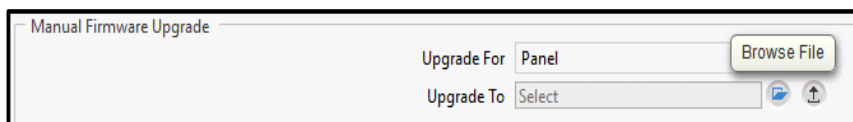
Firmware Upgrade

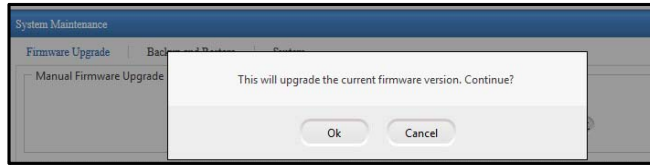


Manual Firmware Upgrade

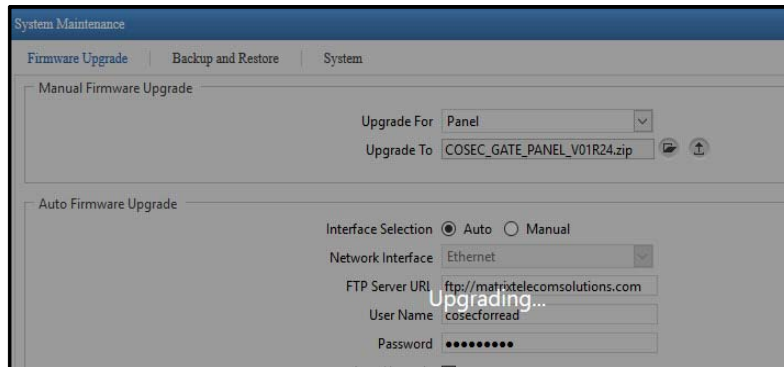
Upgrade For: Select the device for which the firmware is to be upgraded from the drop-down list. The firmware of PVR Door, ARGO Door, V3 Door and Vega Door(V2)-bluetooth supported Vega will be stored in the memory card of Panel lite V2. The firmware of other panel doors will be stored in the flash of panel lite V2.

Upgrade To: Click **Browse File** to browse the file and select the firmware. Click to **Upgrade** button to upgrade the firmware.





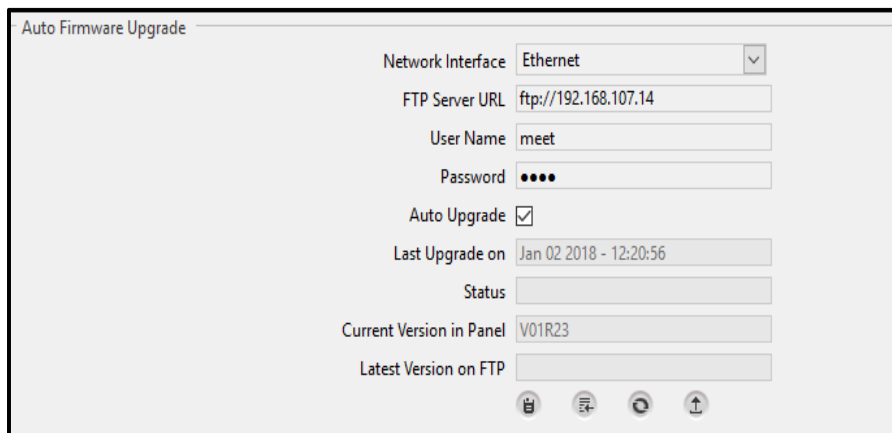
Click **OK** to upgrade the firmware. The panel lite will be upgraded with the new firmware and will reboot.



Auto Firmware Upgrade

Auto upgrade feature enables to upgrade the firmware in 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 FTP Server.



Network Interface: Select the Interface from the options of Ethernet, WiFi and Broadband with which the communication is to be established.

FTP Server URL: Enter the URL as the combined path with FTP server address, port and folder name, from where you want to upgrade the firmware version.

You must specify the URL path up- till COSEC_ DEVICE folder. i.e. if your COSEC_ DEVICE folder is at path ftp://192.168.107.15/Softwares/COSEC_DEVICE then your URL would be ftp://192.168.107.15/Softwares



The firmware must be placed and available from the configured FTP in the folder structure as COSEC_DEVICE> Vega Panellite> Standalone



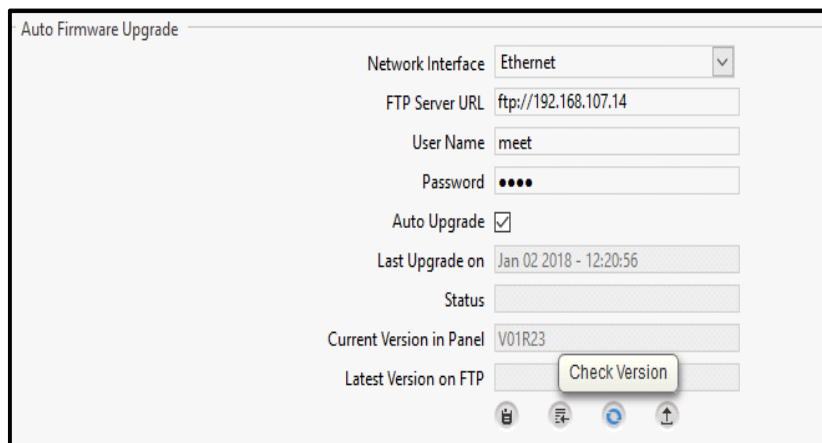
Specify the **User Name** and **Password** to login into FTP server. By default Matrix FTP details will be displayed.

Auto Upgrade: Enable the Auto Upgrade checkbox to automatically upgrade the firmware of panel lite. If Auto Upgrade enabled, Device will check the latest version of firmware available at 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 firmware was installed on device.

Current Version in Panel: It will show the current firmware version stored in the memory of Panel lite.

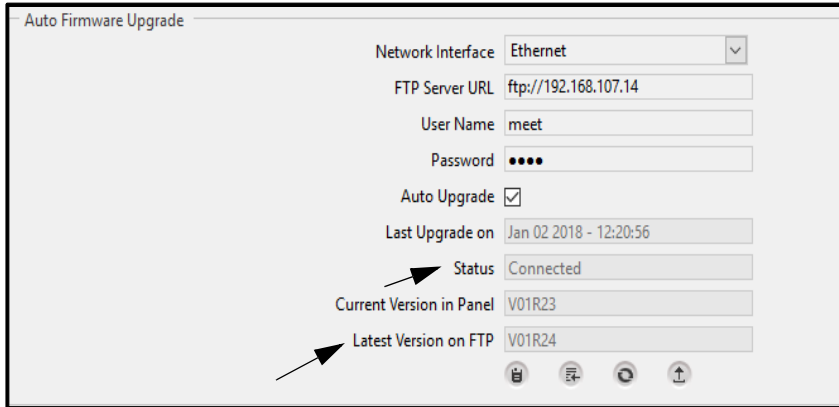
Click **Save** button to save the configured details of FTP server.



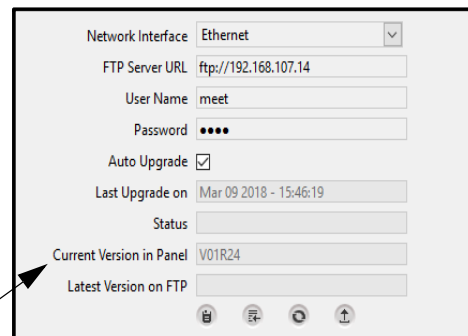
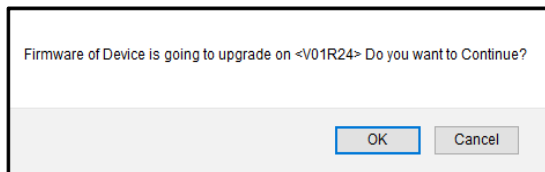
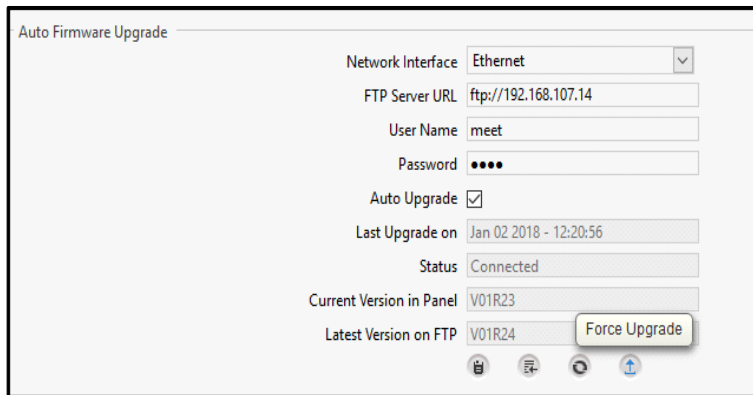
Click **Check Version** button to check Current Firmware version in panel lite and Latest firmware version available at FTP.

Status: It will display the status whether device is connected with FTP server or not.

Latest Version on FTP: It will show the latest firmware version available at FTP.

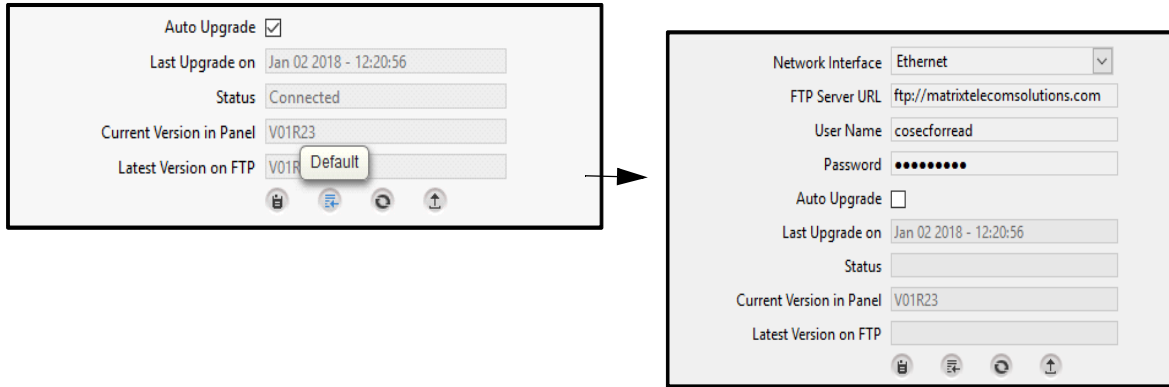


Click **Force Upgrade** to upgrade the panel lite with whichever firmware available at defined FTP server. The Force upgrade can be used when you do not have to wait till 00:00 hrs and upgrade the firmware instantly.



Then click **OK** to upgrade. Then wait for the panel lite to reboot. After login, you can check the Current version in Panel lite which will be upgraded.

Click **Default** button to default the FTP Server URL, Username, Password, Status and Latest Version on FTP.



Backup and Restore

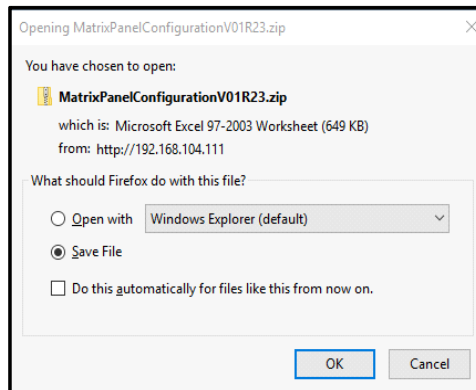
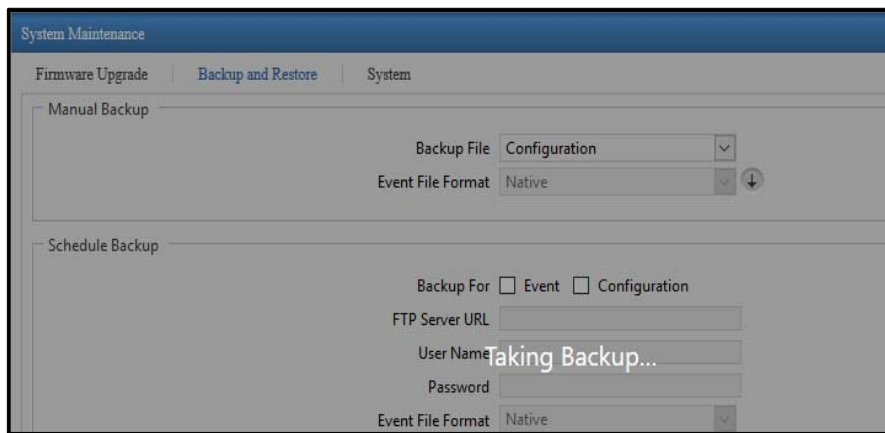


SD card must be present in the Panel. Without SD Card Manual or Schedule Backup will not take place.

Manual Backup

Backup File: The backup of the **Event** and **Configuration** can be stored at desired location.

- The Configuration backup will be generated in a zip file which includes configuration of Panel lite, finger templates and palm templates.
- 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"



Schedule Backup

The screenshot shows the 'Schedule Backup' configuration window. It includes the following fields and options:

- Backup For:** Event Configuration
- FTP Server URL:** ftp://192.168.107.14
- User Name:** meet
- Password:** ••••
- Event File Format:** xls (dropdown menu)
- Monthly Backup On:** A calendar grid with the 10th day selected.
- Schedule Time:** 18 : 15

At the bottom of the window, there are four icons: a trash can, a document with a checkmark, a refresh symbol, and a list icon.

Backup For: Enable the **Event** and/or **Configuration** checkbox for which backup is to be scheduled.

FTP Server URL: Enter the URL as the combined path with FTP server address, port and folder name, 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 > 250 MB; then manual backup or schedule backup may be 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:

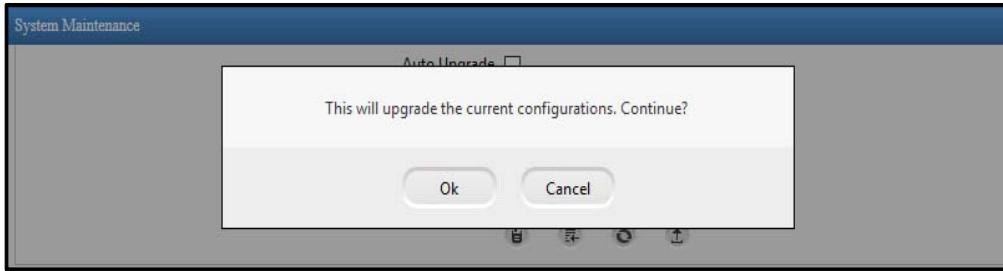
- Restore all configurations except:** Network Settings Users
- Restore File:** Select (with browse and refresh icons)

A 'Browse File' button is visible to the right of the 'Users' checkbox.

The screenshot shows the 'Restore' configuration window after a file has been selected. It includes the following fields and options:

- Restore all configurations except:** Network Settings Users
- Restore File:** MatrixPanelConfigurationV01R23.zip (with browse and refresh icons)

A 'Restore' button is visible to the right of the 'Users' checkbox.

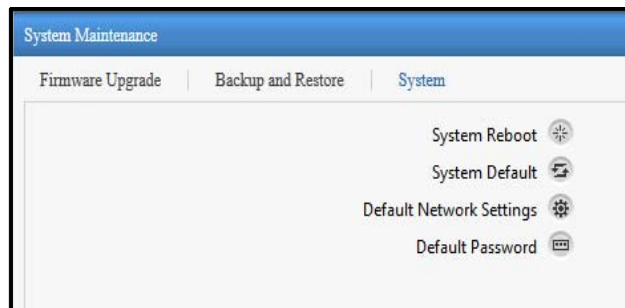


Click on **OK** to update the configuration. Then wait for the panel lite to re-boot.



If the Configuration size of the selected file is > 250 MB; then Restore of file may be failed.

System



System Reboot: To reboot the system.

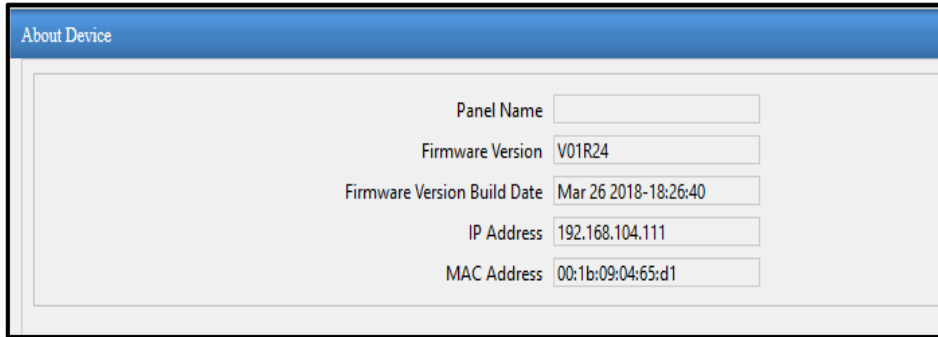
System Default: To set the system to default settings.

Default Network Settings: To set the Network settings to default.

Default Password: To set the password to default.

About Device

The About Device page shows the name of panel lite, firmware version available in panel lite, last build date of firmware, IP Address and MAC address of Panel lite.

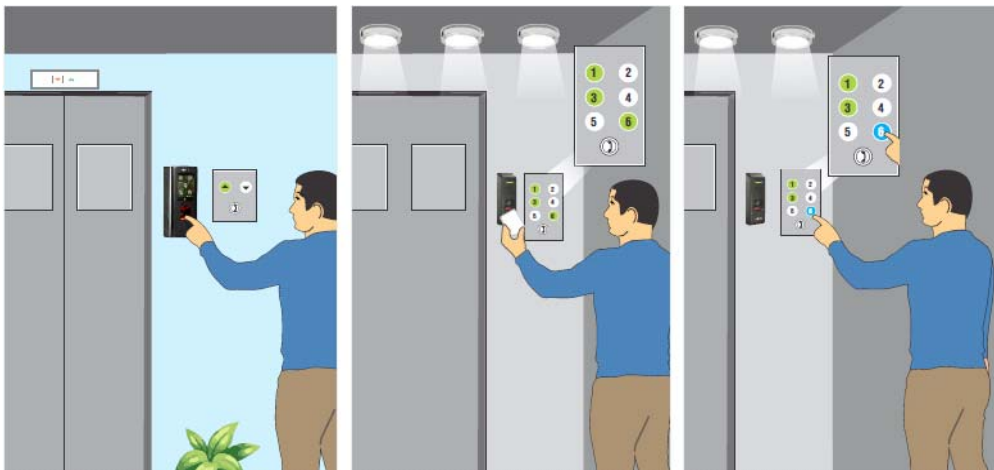


The screenshot displays a web interface titled "About Device" with a blue header. Below the header, there are five rows of information, each consisting of a label and a text input field. The labels are "Panel Name", "Firmware Version", "Firmware Version Build Date", "IP Address", and "MAC Address". The corresponding values in the input fields are: an empty field for Panel Name, "V01R24" for Firmware Version, "Mar 26 2018-18:26:40" for Firmware Version Build Date, "192.168.104.111" for IP Address, and "00:1b:09:04:65:d1" for MAC Address.

Field	Value
Panel Name	
Firmware Version	V01R24
Firmware Version Build Date	Mar 26 2018-18:26:40
IP Address	192.168.104.111
MAC Address	00:1b:09:04:65:d1

Elevator Access Control & Multi level Access

Elevator can be considered as doorways to many organizations, buildings and restricted areas. A person accessing the elevator can gain access to any floor he wishes. Hence, to increase the security and control for different floors in a building Elevator Access Control feature must be used.



EAC Configuration and Working

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 enabling of floor1 and floor2 is done 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 must be given to IO LINK and the desired port can 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 panel lite whose access can be given to authorized users only.



This feature is applicable to PVR Door, V3 Door, Wireless, Vega, ARC IO 800, ARGO Door and ARC DC 100 only.

*You can configure maximum **24** elevators in one panel lite.*

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: 1

Elevator Name: RnD Elevator

Number of Floors: 4 (1-64)

Authentication Device: 1 PVR 113

Access Duration For Floors: 10 sec (1-99)

Update

Floor Index	Floor Name	Free Access Floor ⓘ	IO Controller		Output Port	
1	15 chars	<input type="checkbox"/>	ID	Name	Port No	↔
2	15 chars	<input type="checkbox"/>	ID	Name	Port No	↔
3	15 chars	<input type="checkbox"/>	ID	Name	Port No	↔
4	15 chars	<input type="checkbox"/>	ID	Name	Port No	↔

Save Cancel

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 till which the configured elevator is accessible. You can configure maximum **64** 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,
- 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.

Elevator Configuration
☰

Elevator ID:

Elevator Name:

Number of Floors: (1-64)

Authentication Device:

Access Duration For Floors: sec(1-99)

Floor Index	Floor Name	Free Access Floor (i)	IO Controller	Output Port	
1	<input type="text" value="Reception Area"/>	<input checked="" type="checkbox"/>	ID: <input type="text"/> Name: <input type="text"/> <input type="button" value="⌵"/>	Port No: <input type="text"/> <input type="button" value="⌵"/>	↔
2	<input type="text" value="Canteen Floor"/>	<input checked="" type="checkbox"/>	ID: <input type="text"/> Name: <input type="text"/> <input type="button" value="⌵"/>	Port No: <input type="text"/> <input type="button" value="⌵"/>	↔
3	<input type="text" value="Telecom Floor"/>	<input type="checkbox"/>	2 <input type="text"/> IO Controller <input type="button" value="⌵"/>	5 <input type="text"/> <input type="button" value="⌵"/>	↔
4	<input type="text" value="Surveillance FI"/>	<input type="checkbox"/>	2 <input type="text"/> IO Controller <input type="button" value="⌵"/>	6 <input type="text"/> <input type="button" value="⌵"/>	↔

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.

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 assign IO controller Output port to the desired floor of elevator by selecting the IO controller and the port from pick-list.



Ensure that the same IO controller port should not be assigned to different floors of elevator.

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	RnD Elevator	1	PVR 113	4	🗑️

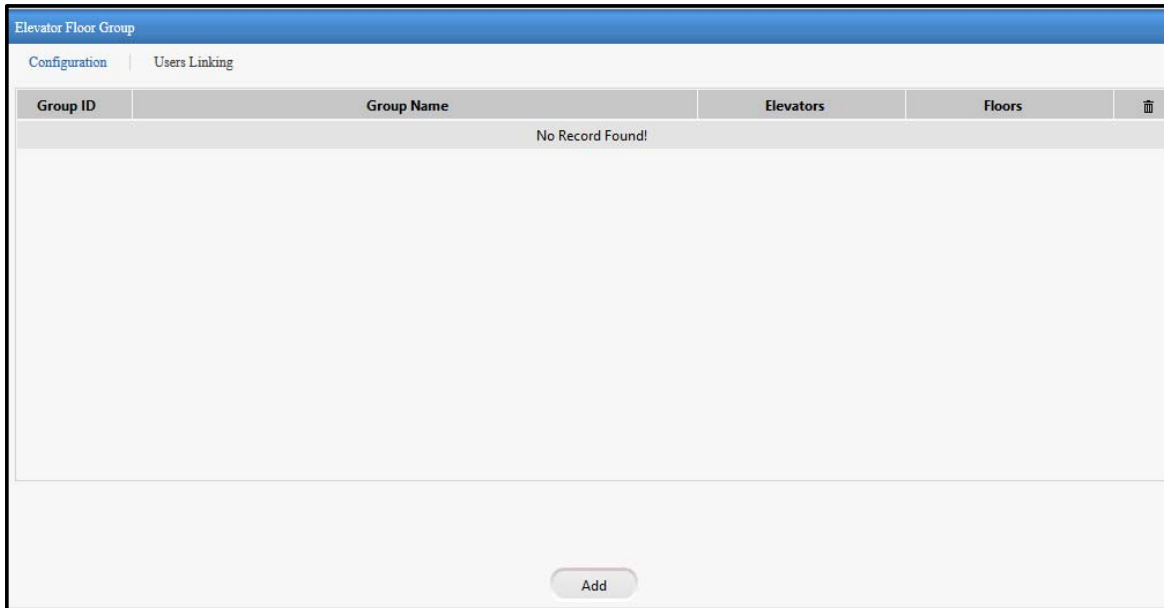
Add

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.

Configuration

Configuration tab displays a grid containing a list of configured elevator floor groups.



To configure a new elevator floor group click **Add** button and enter the following parameters.

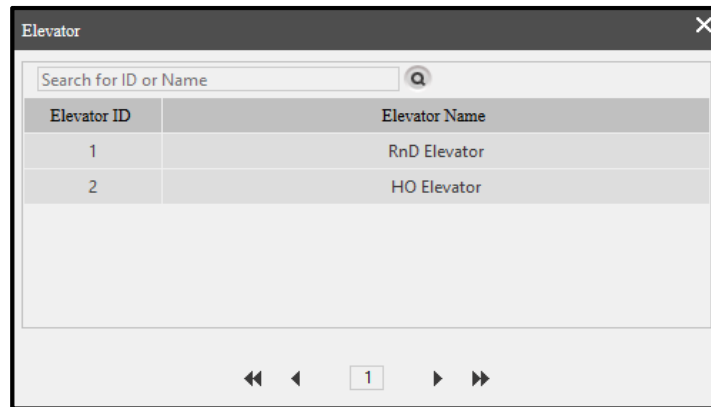
Group ID: The group ID is auto-generated by the system.

Group Name: Enter the name for the elevator floor group to be configured.



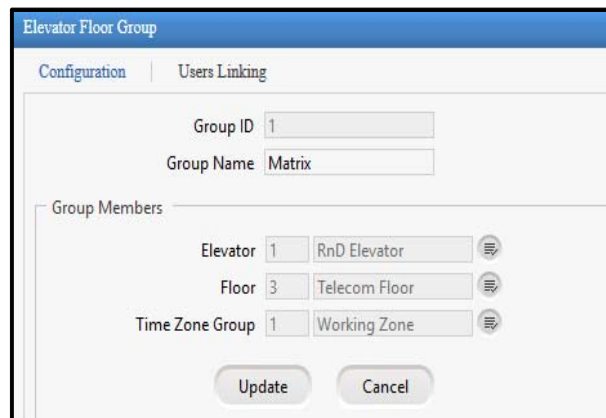
Group Members

Elevator: Select the elevator using the pick-list to include in the floor group. The Elevators are configured from Elevator Configuration.



Floor: Select the floor of the elevator using the pick-list to include in the floor group.

Time Zone Group: Select the time zone group 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

You can also click View List button on the top right corner to view the list of elevator floor groups configured in the panel lite.

Elevator Floor Group				
Configuration		Users Linking		
Group ID	Group Name	Elevators	Floors	
1	Matrix	2	2	

Users Linking

Users Linking tab displays the elevator floor groups and the number of users linked with respective groups.

Elevator Floor Group		
Configuration		Users Linking
Group ID	Group Name	Users
1	Matrix	0

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.

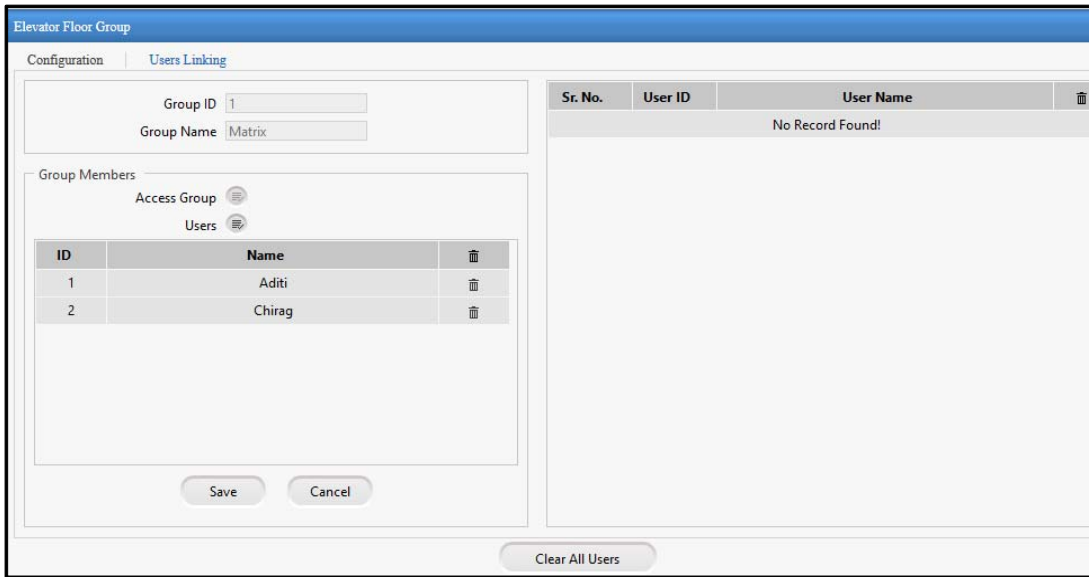
Group Members

You can select the users based on Access Group or individual Users for assigning to Elevator group.

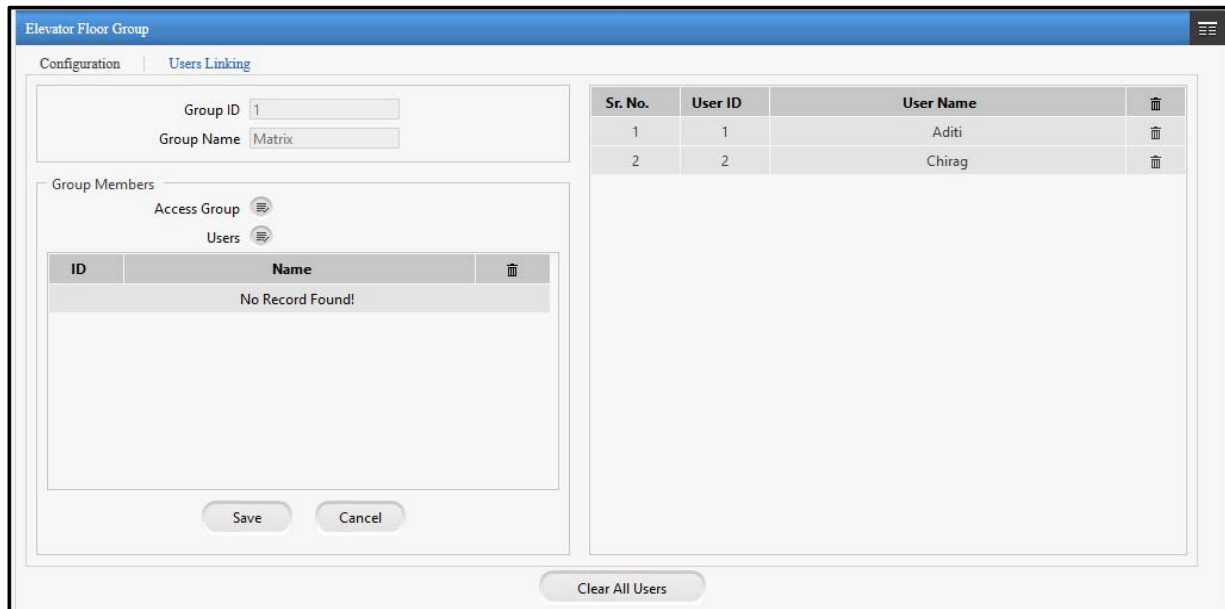
Access Group: Select the access group using the picklist. The Access group is created from *Users> Access Group*.

Users: Select the individual users using the pick-list and checking the respective boxes to be assigned to the elevator group.

The selected users get displayed in the grid below.



Click **Save** to save the members which gets updated in the grid on the right hand side.



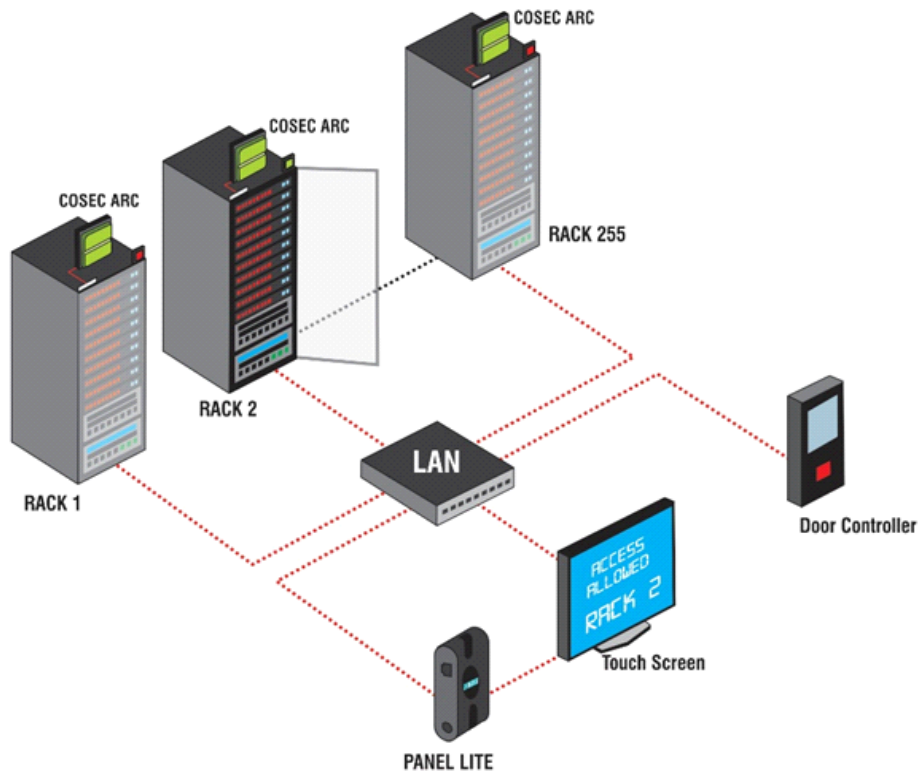
You can click **Clear All Users** button to clear all the users and access groups from the elevator floor group.

You can also click **View List button** on the top right corner to view the number of users assigned to a group.

Group ID	Group Name	Users
1	Matrix	2

Multi-Level Access

Multi-Level Access enables the user to access multiple doors using single biometric/card reader.



Configuration

The screenshot shows the configuration interface for Multi-Level Access. The interface is divided into two tabs: Configuration and Assignment. The Configuration tab is active, showing the following settings:

- Multi-Level Access:
- Monitor Authentication: User Credential
- Authentication Device: 1 PVR Door
- Organization Logo: .jpg,.png,.bmp files Max 250kb
- Organization Name: Matrix Comsec
- Message: Expect More
- Page Time-Out Duration: 3 sec (3-60)
- Group Label: RACK
- Door Unlock Timer: 1 sec (1-999)

At the bottom of the interface, there are Save and Cancel buttons.

Multi-Level Access: Select this checkbox to enable the access to multiple doors/area using a single biometric device to authenticate users.

Monitor Authentication: You can monitor the live status of all the doors of Panel from MLAT Monitor. For authenticating the users for accessing MLAT Monitor; you can select following two options:

- **User Credential:** Select the User Credential option if all normal users are to be given the MLAT monitor access. The user can show their credential on configured Authentication Device and monitor the status of doors.
- **Password:** Select the Password option if only System users are to be given the MLAT monitor access. The system users will have to provide their username and password on the authorization page after which they can monitor the status of doors.

Authentication Device: Select a device through which biometric identification is to be done.

Organization Name: Specify the name of the Organization.

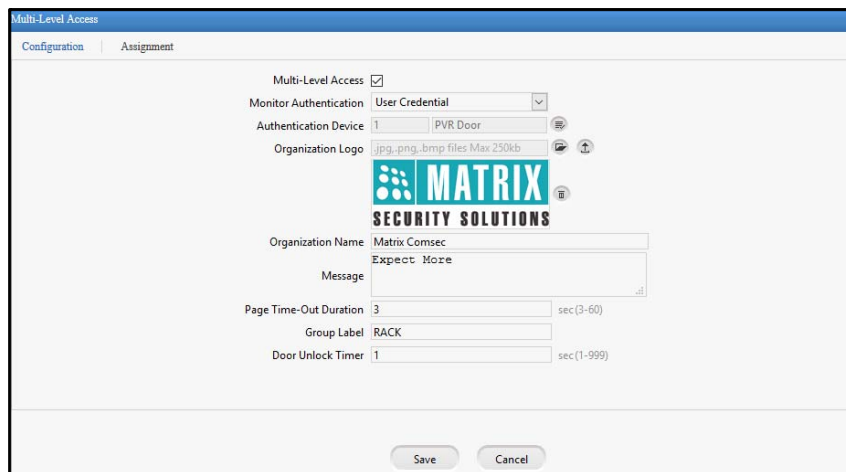
Message: You can give a tag line in the message.

Page Time-Out Duration (sec): Specify the time in seconds after which the idle page will become time-out.

Group Label: You can give a name to the group of doors in an area. The default name is Rack.

Door Unlock Timer: Specify the door unlock time in seconds after which the door gets locked automatically. Time can be specified in the range of 1-999.

Organization Logo: After saving other configurations you can select and upload the logo of the Organization. The maximum size allowed is 250 KB.



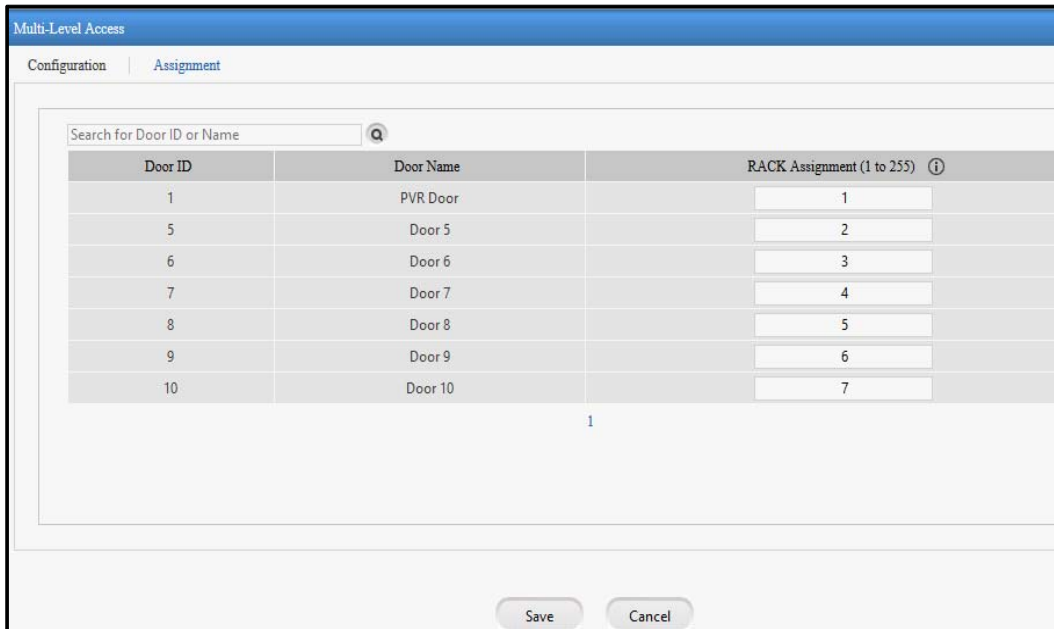
The screenshot shows a web-based configuration interface for 'Multi-Level Access'. The interface has two tabs: 'Configuration' (selected) and 'Assignment'. The configuration fields are as follows:

- Multi-Level Access:** A checked checkbox.
- Monitor Authentication:** A dropdown menu set to 'User Credential'.
- Authentication Device:** A dropdown menu set to '1' with 'PVR Door' displayed next to it.
- Organization Logo:** A file upload area showing a logo for 'MATRIX SECURITY SOLUTIONS'.
- Organization Name:** A text input field containing 'Matrix Comsec'.
- Message:** A text input field containing 'Expect More'.
- Page Time-Out Duration:** A numeric input field set to '3', with a unit of 'sec (3-60)'.
- Group Label:** A text input field containing 'RACK'.
- Door Unlock Timer:** A numeric input field set to '1', with a unit of 'sec (1-999)'.

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

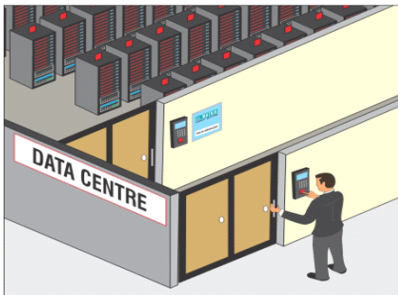
Assignment

The user can assign racks to the door controllers. For each door, enter the Rack number to be assigned. Upto 255 Rack assignment is supported.



Click **Save** to apply the changes.

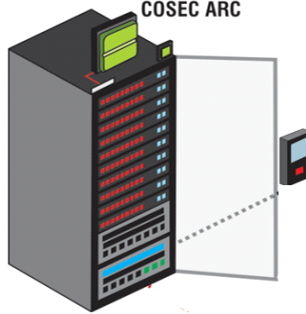
Data Centre Authentication



Data Centre Access Allowed



COSEC ARC



Rack Access Allowed



The Panel lite V2 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.

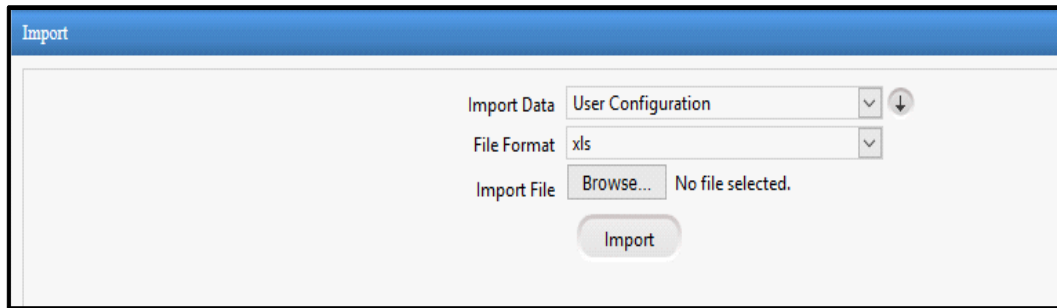
Similarly the user can also export data to external applications based on the pre-configured data templates. The user has the flexibility to select the output formats as desired.

The Reports section enables to view different reports based on Alarms, Device, Access Policies, User and Elevator Access Control for the selected date range.

See the respective sections for details.

Import

The Import feature helps in importing the data from one device or server to the other device. This feature is useful if you want to upload particular type of data in one go.

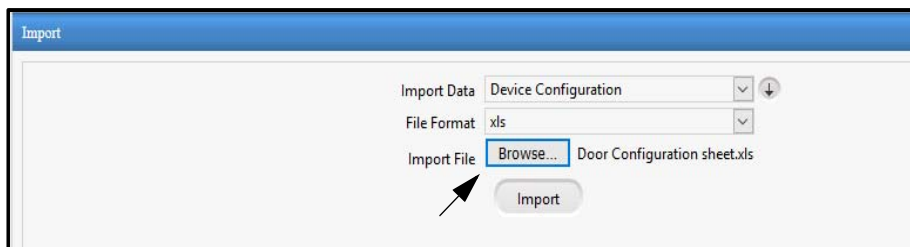


Import Data: Select the type of data from the options of User Configuration, Access Group, Shifts, Schedules etc which is to be imported to the panel lite through the import file.

Click on 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 to the panel lite.

File Format: Select the option of XLS or CSV for the format of file to be imported (uploaded to panel lite).

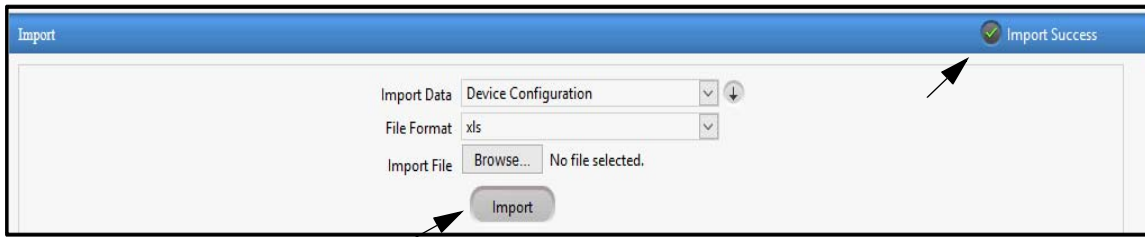
Import File: Click on Browse and select the file to be imported.



The excel file imported here has following device configurations as shown below:

	A	B	C	D	E	F	G	H	I	J	K	L
	Door	Door Name	Door Type	Status	Communication Type	IP Address/RS-485 Address	MAC Address	Mute Buzzer	Access Zone	Card Reader	Biometric Reader	External Reader Mode
1	5	Door 5	1	1	0	192.168.110.1	00:1b:09:02:b0:00					
2	6	Door 6	1	1	0	192.168.110.2	00:1b:09:02:b0:01					
3	7	Door 7	1	1	0	192.168.110.3	00:1b:09:02:b0:02					
4	8	Door 8	1	1	0	192.168.110.4	00:1b:09:02:b0:03					
5	9	Door 9	1	1	0	192.168.110.5	00:1b:09:02:b0:04					
6	10	Door 10	1	1	0	192.168.110.6	00:1b:09:02:b0:05					

Then click on **Import** to import the data from the selected file to the panel lite. After successful importing of data; Import Success will be displayed.

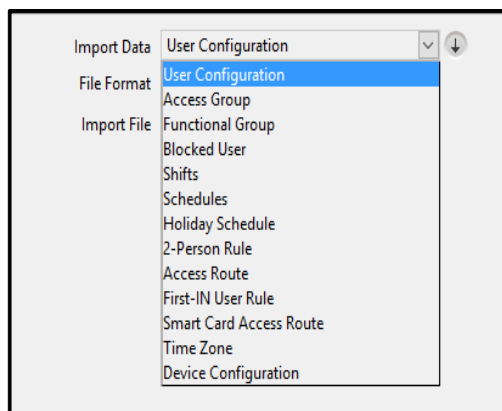


The imported data of devices can be viewed from Device Configuration page as shown below:

The screenshot shows the 'Door Configuration' page. At the top, there is a search bar for 'Door ID or Name' and three dropdown menus for '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	🗑️

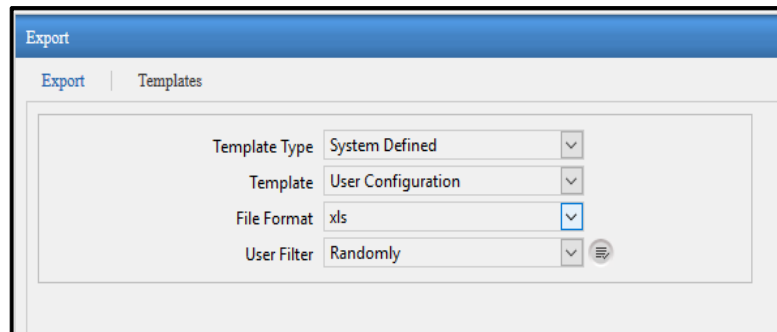
Similarly you can import other types of data as well.



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 panel lite in one go which can be then used to upload in some other device.

Export



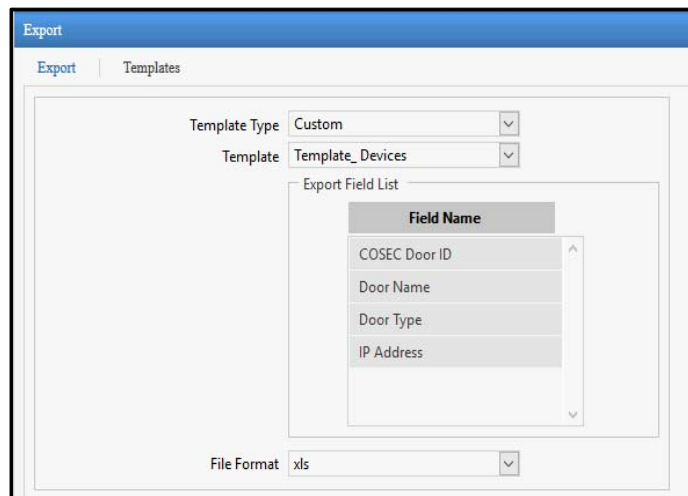
The screenshot shows the 'Export' window with two tabs: 'Export' and 'Templates'. The 'Export' tab is active. It contains four dropdown menus: 'Template Type' set to 'System Defined', 'Template' set to 'User Configuration', 'File Format' set to 'xls', and 'User Filter' set to 'Randomly'. There is a small menu icon to the right of the 'User Filter' dropdown.

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 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.



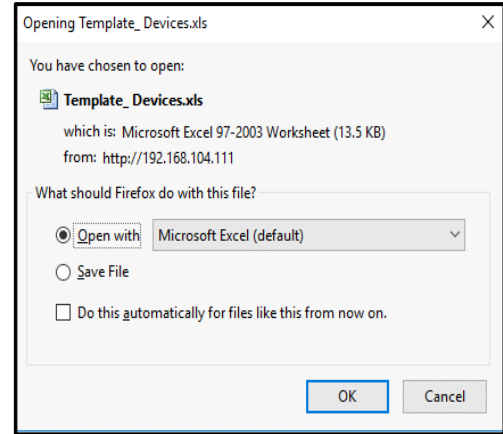
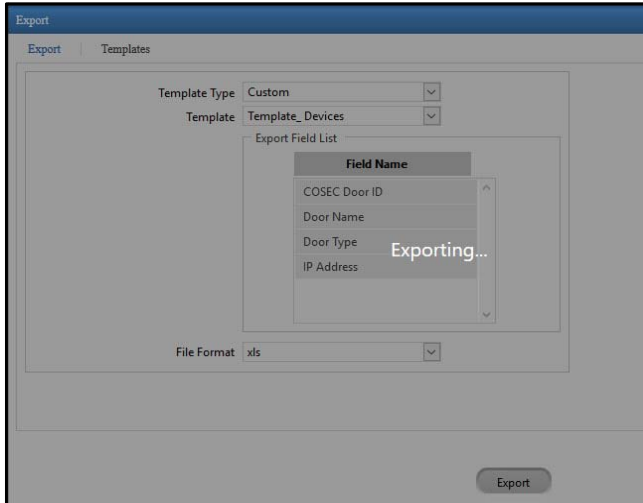
The screenshot shows the 'Export' window with the 'Export' tab active. The 'Template Type' is set to 'Custom' and the 'Template' is set to 'Template_Devices'. Below these, there is an 'Export Field List' section with a list of field names: 'COSEC Door ID', 'Door Name', 'Door Type', and 'IP Address'. The 'File Format' is set to 'xls'.

File Format: Select the option of CSV, XLS or Text for the format of file to be exported.

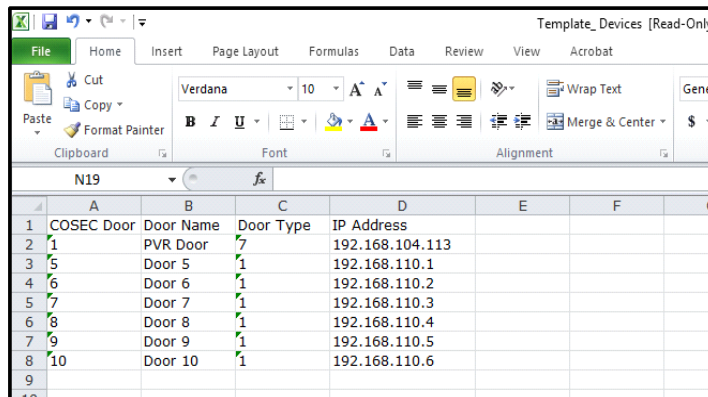
Text File Separator: If the file format selected is Text or CSV then select the separator for the file.

User Filter: Select the user based on the filter options of Randomly, Access Group and ALL.

Then click on **Export** to export the data in the selected file format.



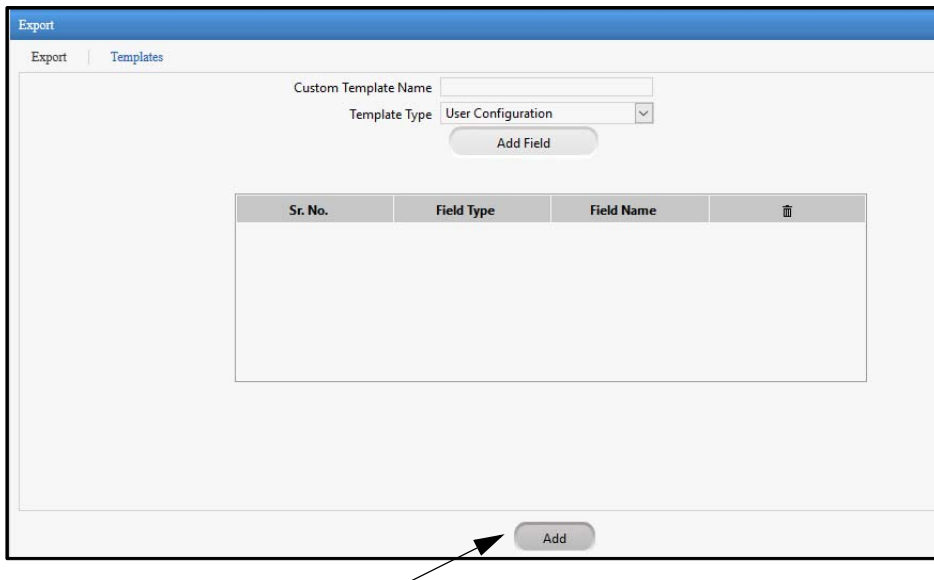
You can open the exported file or save the file at desired path.



	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							
10							

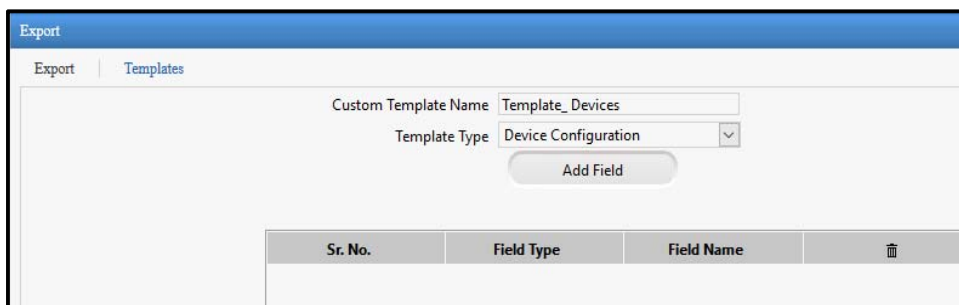
Templates

The user can define templates for export of data in a customizable format by selecting the Templates tab. Then click **Add** button to create the template.

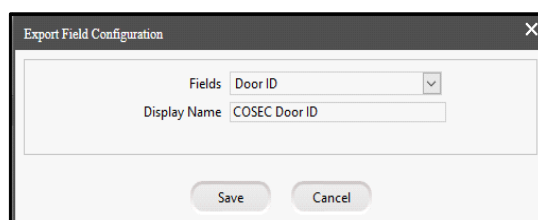


Custom Template Name: Specify a user friendly name for the custom template. For eg. Template_Canteen, Template_DailyEvents etc.

Template Type: Select the type of template from the options of User Configuration, Access Group, shifts, Schedules, Device Configuration etc.



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 **Save** to save the custom Template.

Custom Template Name

Template Type

Sr. No.	Field Type	Field Name	
1	Door ID	COSEC Door ID	
2	Door Name	Door Name	
3	Door Type	Door Type	
4	IP Address/RS-485 Address	IP Address	

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

Select the From and To **Date** using the calendar button.

The screenshot shows a web interface titled "Reports" with tabs for "Alarm", "Device", "Access Policies", "User", and "Elevator Access Control". Below the tabs, there is a "Select Date" section with two input fields: "01-03-2018" and "22-03-2018", each with a calendar icon to its right. A "Generate Report" button is centered below the date fields.

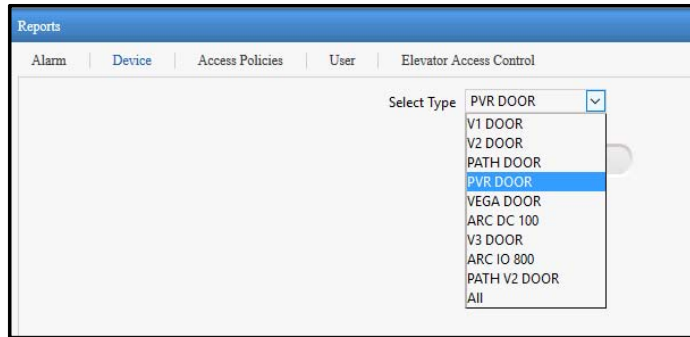
Click on **Generate Report** to view the Alarm Report for the selected dates. You can open or save the report at desired location.

The screenshot shows an Excel spreadsheet titled "Alarm Reports [Read-Only] [Compatibility Mode] - Microsoft Excel". The spreadsheet contains the following data:

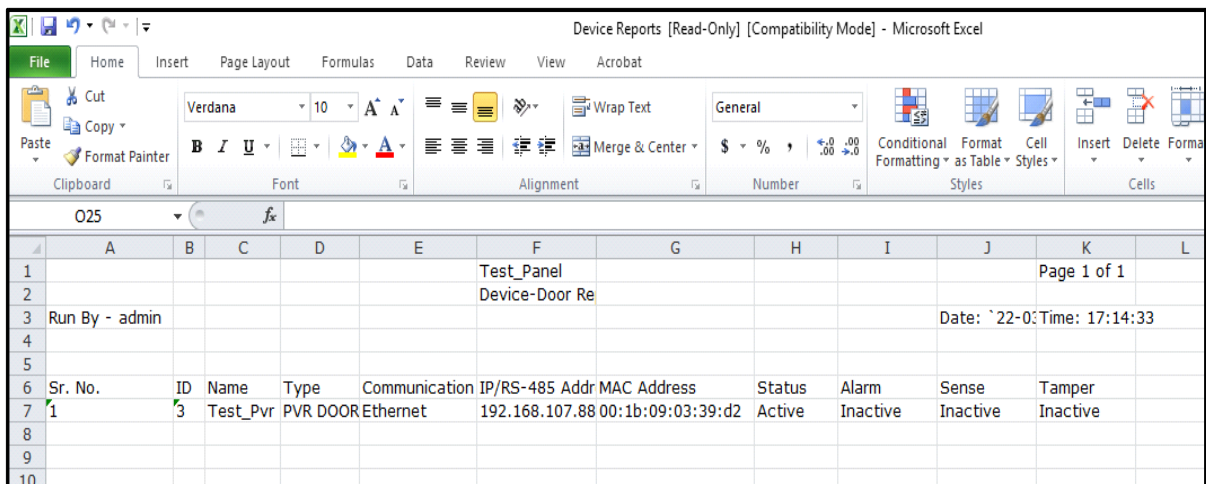
Sr. No.	Alarm Name	Source	Category
1	Tamper Alarm	Test_Pvr	Critical
2	Tamper Alarm	Test_Pvr	Critical
3	Tamper Alarm	Test_Pvr	Critical
4	Deadman Timer Expired	Test_V2	Critical
5	Duress Alarm	Test_V2	Critical
6	Panic Alarm	Test_V2	Critical
7	FP Memory Full	Test_V2	Minor
8	FP Memory Full	Test_V2	Minor
9	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 Aalrm	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

Select the type of door from the dropdown list for which the report is to be generated.



Click on Generate Report to view the Device Report for the selected door.



The screenshot shows a Microsoft Excel spreadsheet titled 'Device Reports [Read-Only] [Compatibility Mode]'. The report data is as follows:

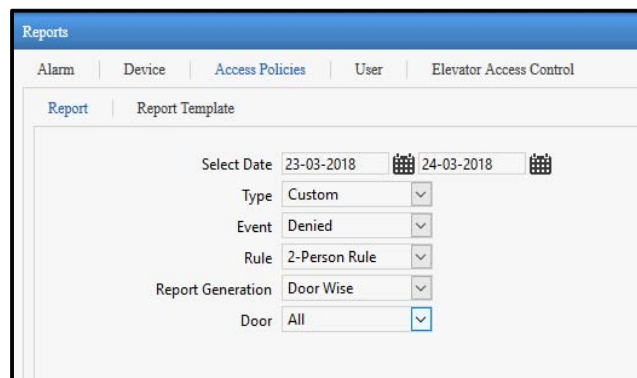
Sr. No.	ID	Name	Type	Communication	IP/RS-485 Addr	MAC Address	Status	Alarm	Sense	Tamper
1	3	Test_Pvr	PVR DOOR	Ethernet	192.168.107.88	00:1b:09:03:39:d2	Active	Inactive	Inactive	Inactive

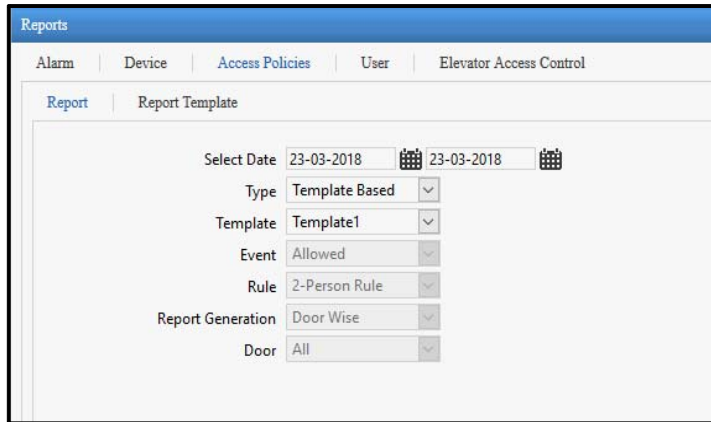
Access Policies

Report

The Report can be generated for a particular Access policy by selecting the option for the following filters.

Select the From and To **Date** using the calendar button for which report is to be generated.





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 type select 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 on **Generate Report** to view the Report for the selected dates.

Here Template based report for 2-person rule allowed is shown 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 **Add** to create report template.

Name	Event	Rule
No Record Found!		

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.

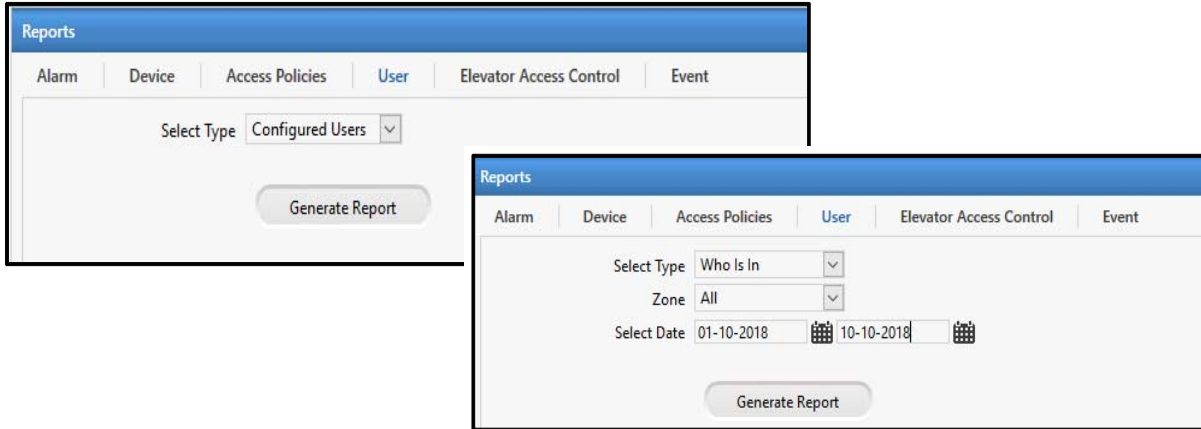
Click on **Save** button to save the configured template. After saving the template; it will appear in Template picklist in Report tab.

Name	Event	Rule
Template1	Allowed	2-Person Rule

User

Select the **type** from the options of Configured Users, Blocked Users, Enrollment Info, Door Wise User, User Wise Door and Who Is In.

Select the From and To **Date** using the calendar button for Blocked Users and Who Is In.



Click on **Generate Report** to view the User Report for the selected type and dates.

The screenshot shows a Microsoft Excel spreadsheet titled 'User Reports [Read-Only] [Compatibility Mode] - Microsoft Excel'. The report content is as follows:

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

Elevator Access Control

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 dropdown list. You can generate elevator wise and 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 on **Generate Report** to view the report for the selected elevators or users.

The Panel lite V2 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 off 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 of the selected SMS service providers. To set email configurations. Before configuring ensure that an SMTP Server has been set up on the network.

See 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

1 2 3

To activate alert for a particular event; select that event from the grid. The alert configuration for selected event appears as shown below.

Alert Message Configuration

Event Type: Access Control

Event: User Denied - 2-Person Rule

Active:

Alerts: SMS Email

Alert Schedule: Time Zone

Time Zone: 1 Time Zone 1

Message Preview

Recipients

SMS Default Message

Message: <User Name> (ID: <User ID>): <Entry/ Exit> Denied due to violation of 2-Person rule at <Door Name> on <Date - Time> (13/130)

Email Default Email

Subject: User Denied Access

Email: 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)

Default Save Cancel

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 for 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 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 **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:** Click the Select Recipients picklist button and select the users to whom alert is to be sent. 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.

Message Preview | Recipients

Send To Individual Selected Recipients Both (Individual and Selected Recipients)

Recipient

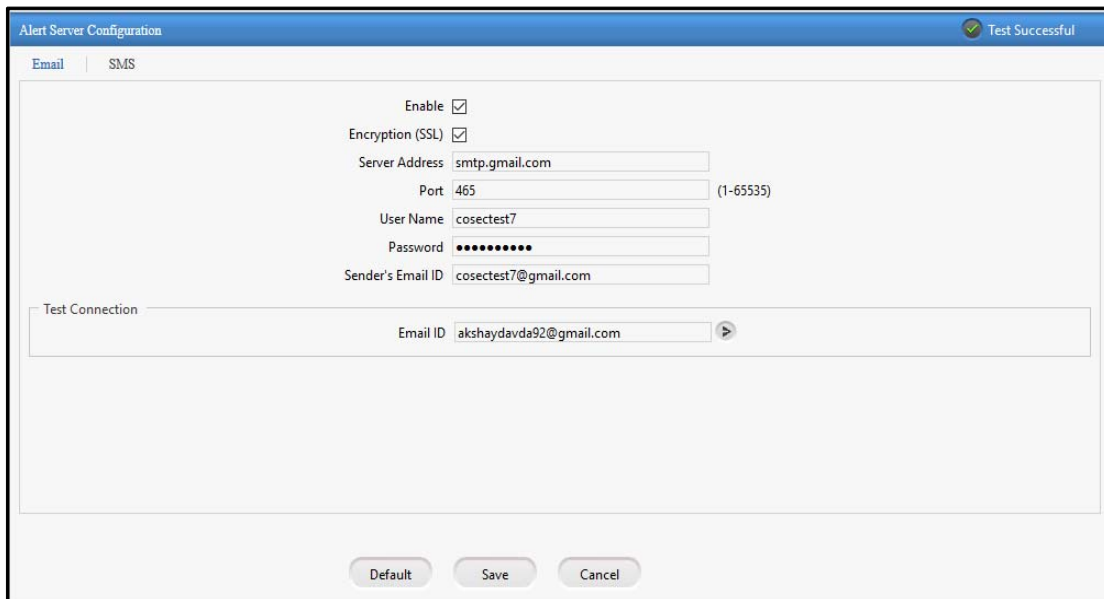
Name	Email	Mobile	
Deep	deep.gandhi@gmail.com	9532487512	<input type="button" value="🗑"/>

Click **Save** to save the Alert Message Configuration. You can also click Default to set all the parameters to its default value.

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 window title bar includes a 'Test Successful' indicator. 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 these fields is a 'Test Connection' section with an 'Email ID' field containing 'akshaydavda92@gmail.com' and a right-pointing arrow button. At the bottom of the window are three buttons: 'Default', 'Save', and 'Cancel'.

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 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.

UserName, 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' window with the 'SMS' tab selected. The 'Enable' checkbox is checked. The 'Service Provider' dropdown is set to 'SMS Gateway Center'. The 'User Name' is 'matrixcomsec', the 'Password' is masked with dots, and the 'Sender's ID' is 'MATRIX'. The 'Check Balance' button is active, showing a balance of 'Balance SMS Credits: 930'. The 'Test Connection' section has a 'Mobile Number' field with '8866614176'. At the bottom are 'Default', 'Save', and 'Cancel' buttons.

Test Connection

Mobile Number: Enter the Mobile Number of the receiver for testing the connection. Click on Send Message button to send the test SMS.

Click **Save** to save the Alert Server Settings. You can also click Default to set all the parameters to its default value.

This screenshot shows the same 'Alert Server Configuration' window but with different settings. 'Enable' is checked. 'Service Provider' is 'Bulk SMS'. 'User Name' is 'matrixcomsec', 'Password' is masked, and 'Sender's ID' is '0447797801008'. 'Check Balance' shows '0|191.32'. The 'Mobile Number' in the 'Test Connection' section is '8866614176'.

You can configure upto 5 new custom service providers by clicking on **Add** button.

- **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?](#)
- **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
- **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 **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 for firing a 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.
- **Check Balance:** Select to allow balance check, if the service provider needs to use it. And enter the corresponding API.
- Click **Save** button to save the settings.

Managing User Account and Password

The Account Management allows you to configure user accounts of Admin, HRD and Operator types and give them different access rights of accessing features of Panel lite V2 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 Panel lite can be changed from Change password page.

See the respective sections for details.

Users

User Account Management 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 grid.

The screenshot shows a web interface for managing users. On the left, there is a form for creating a new user. The form includes fields for 'User Name' (Aditi), 'User Type' (radio buttons for Admin, Hrd, and Operator, with Operator selected), 'Password' (masked with dots), 'Confirm Password' (masked with dots), 'Email ID' (aditigupta@gmail.com), and 'Mobile Number' (9532148657). Below the form is an 'Access Rights' section with various checkboxes for permissions like Panel Configuration, Devices, Users, Enrollment, Account Management, Masters, Multi-Level Access, Access Policies, Access Schedule, Manage, Enrollment Authorization, Import Export, Monitor, and Change Password. At the bottom of the form are buttons for 'Delete', 'Default', 'Save', and 'Cancel'. On the right, there is a table with columns 'User', 'User Name', and 'User Type'. The table contains 10 rows, with the first three rows populated: (1, admin, Admin), (2, hrd, Hrd), and (3, operator, Operator). The remaining rows (4-10) are empty.

User	User Name	User Type
1	admin	Admin
2	hrd	Hrd
3	operator	Operator
4		
5		
6		
7		
8		
9		
10		

Enable: Check the box 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 to the created user.

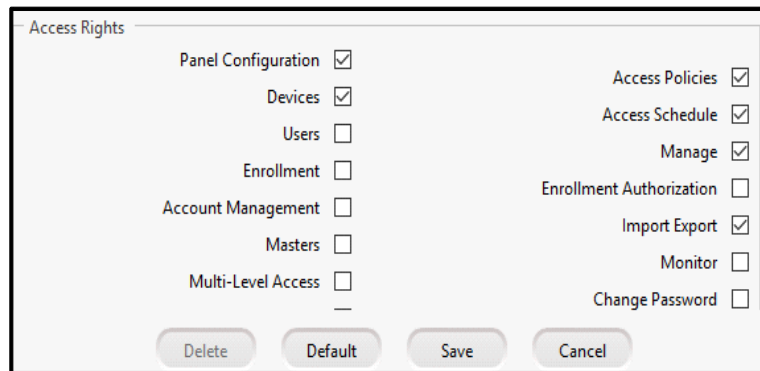
Password: Specify the Password for the user.

Confirm: Type the password again for confirmation.

Email ID: Enter the Email Id of the user.

Mobile Number: Enter the Mobile number of user.

Access Rights



The screenshot 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".

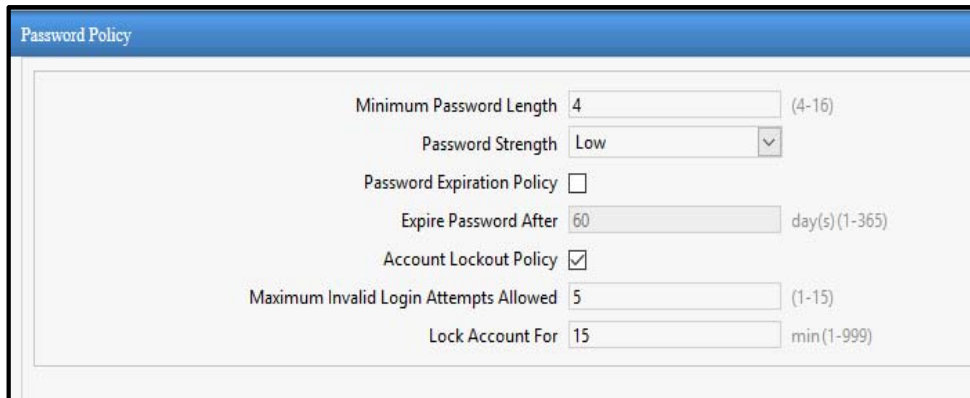
Permission	Checked
Panel Configuration	<input checked="" type="checkbox"/>
Devices	<input checked="" type="checkbox"/>
Users	<input type="checkbox"/>
Enrollment	<input type="checkbox"/>
Account Management	<input type="checkbox"/>
Masters	<input type="checkbox"/>
Multi-Level Access	<input type="checkbox"/>
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.

Click on **Save** to save the configured user account.

Password Policy

You can set the policy for configuration of password from the Password Policy page.



Minimum Password Length	<input type="text" value="4"/>	(4-16)
Password Strength	<input type="text" value="Low"/>	▼
Password Expiration Policy	<input type="checkbox"/>	
Expire Password After	<input type="text" value="60"/>	day(s) (1-365)
Account Lockout Policy	<input checked="" type="checkbox"/>	
Maximum Invalid Login Attempts Allowed	<input type="text" value="5"/>	(1-15)
Lock Account For	<input type="text" value="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: Check the box if you want the password to get expired after certain days.

- **Expire Password After (days):** Specify the number of days after which the password will get expired.

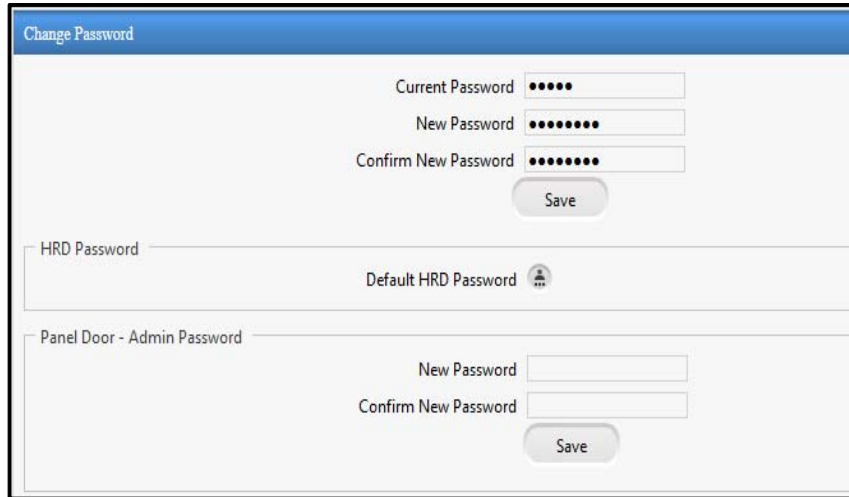
Account Lockout policy: If you want the account to get locked after the invalid login then enable the Account lockout policy.

- **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 **Save** to save the configuration of password policy.

Change Password

The password of the device can be changed through Change Password tab.



Current Password: Specify the current password of the device.

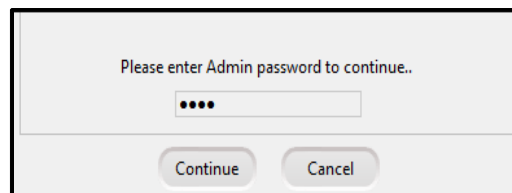
New Password: Enter the new password to be changed. The characters allowed are **A-Z a-z 0-9-_.comma:@!+/**

Confirm New Password: Re-enter the new password to confirm.

Click on **Save** to save the password.

HRD Password

The administrator can default the HRD password by clicking on 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

Save

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

In SNMP (Simple Network Management Protocol), when a manager requests information; SNMP agent (server) sends that information to the manager.

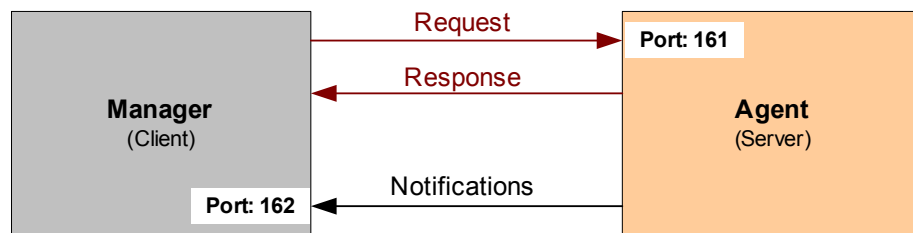
Also, an Agent can send Trap messages to the manager without any GetRequest command. In Trap messages there is no need of acknowledgement.

When specific event occurs; a TRAP or Inform message will be sent to manager from Agent. The message can be Information, Warning or Error.

This SNMP Configuration page is used for configuring panel lite V2 as an SNMP agent and to create Management Information Base (MIB) for SNMP.

The 2 components of SNMP are:

1. Management Node (Agent)- Panel lite V2.
2. Management Host (Manager)- Browser which monitors Panel lite V2.
3. Management Information Base (MIB)- Information which is exchanged between Agent and Manager.

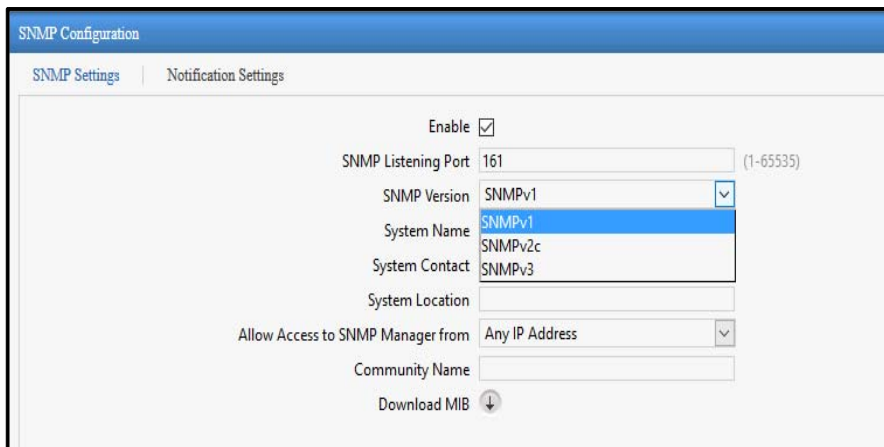


SNMP Configuration

This SNMP Configuration page is used for configuring panel lite V2 as an SNMP agent and to create Management Information Base (MIB) for SNMP.

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.

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 menu is open, showing options for SNMPv1, SNMPv2c, and SNMPv3, with SNMPv1 selected. The 'System Name' dropdown menu is also open, showing options for SNMPv1, SNMPv2c, and SNMPv3, with SNMPv1 selected. The 'System Contact' dropdown menu is open, showing options for SNMPv1, SNMPv2c, and SNMPv3, with SNMPv3 selected. The 'System Location' field is empty. The 'Allow Access to SNMP Manager from' dropdown menu is set to 'Any IP Address'. The 'Community Name' field is empty. There is a 'Download MIB' button with a download icon.

Enable: To activate the SNMP settings; enable this checkbox. When it is enabled; system will process the incoming SNMP messages or outgoing messages.

You can **download MIB** file even if Enable checkbox is unchecked.



The user is required to download the MIB file from the panel lite and upload the same MIB in the Manager so that it will be loaded in the tree.

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

System Name: Enter the System Name which is useful in discovery process of the Agent for SNMPv1 and SNMPv2c. Maximum 40 characters is allowed.

"For this, system should support "SNMPv2-MIB".

System Contact: Enter the Contact information which is useful in discovery process of the Agent for SNMPv1 and SNMPv2c. Maximum 40 characters is allowed.

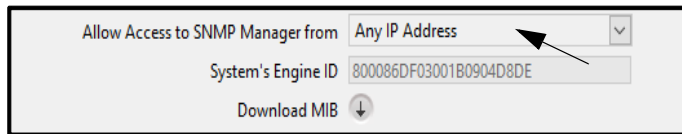
"For this, system should support "SNMPv2-MIB".

System Location: Enter the Location information which is useful in discovery process of the Agent for SNMPv1 and SNMPv2c. Maximum 40 characters is allowed.

"For this, system should support "SNMPv2-MIB".

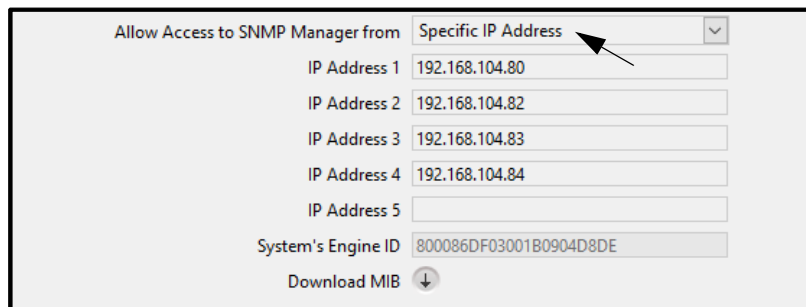
Allow Access to SNMP Manager from: Select the option as **Any IP Address** to allow all IP Addresses (Managers) to allow accessing the system using SNMP or only **Specific IP addresses** (specific Managers) to access the system.

- **Any IP Address:** If this option is selected, then Manager with 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 "800086DF03001B0904D8DE". At the bottom, there is a "Download MIB" button with a downward arrow icon.

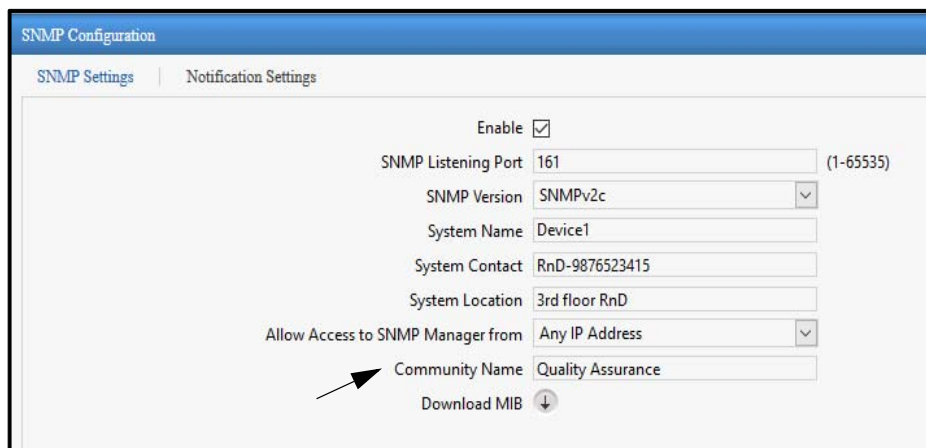
- **Specific IP Addresses:** If this option is selected, then system will process the incoming message only if received Source IP Address is from the configured Manager's IP Address in "**IP Address 1**" to "**IP Address 5**" field.



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" is "800086DF03001B0904D8DE". At the bottom, there is a "Download MIB" button with a downward arrow icon.

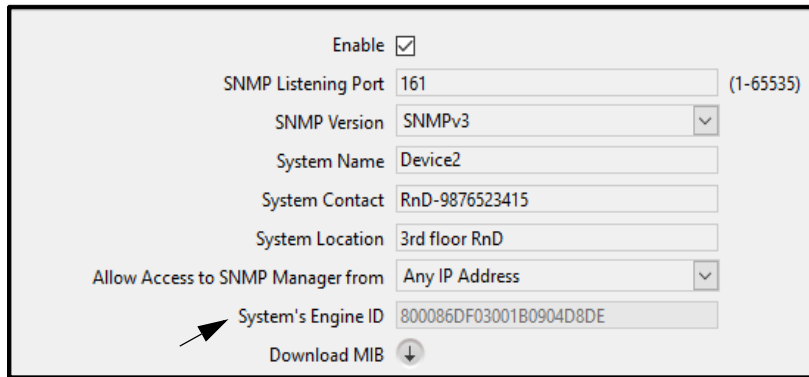
This is applicable for **GetRequest**, **GetNextRequest**, **GetBulkRequest** only.

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 is allowed.



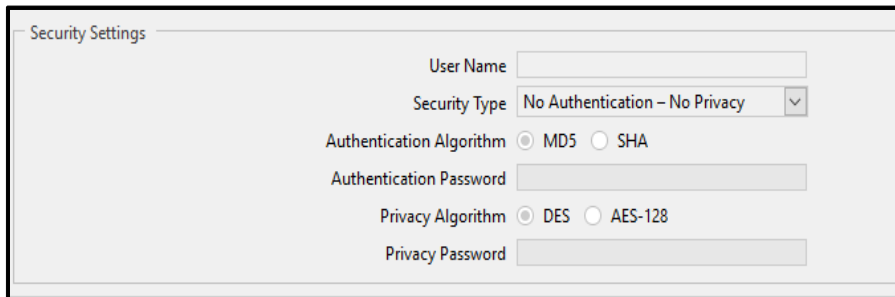
The screenshot shows the "SNMP Configuration" window with two tabs: "SNMP Settings" and "Notification Settings". The "SNMP Settings" tab is active. The "Enable" checkbox is checked. The "SNMP Listening Port" is "161" (with "(1-65535)" next to it). The "SNMP Version" dropdown is set to "SNMPv2c". The "System Name" is "Device1". The "System Contact" is "RnD-9876523415". The "System Location" is "3rd floor RnD". The "Allow Access to SNMP Manager from" dropdown is set to "Any IP Address". The "Community Name" is "Quality Assurance". At the bottom, there is a "Download MIB" button with a downward arrow icon. A black arrow points to the "Community Name" field.

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 an 'Enable' checkbox which is checked. Below it are several input fields: 'SNMP Listening Port' with the value '161' and a note '(1-65535)'; 'SNMP Version' set to 'SNMPv3'; 'System Name' with 'Device2'; 'System Contact' with 'RnD-9876523415'; 'System Location' with '3rd floor RnD'; 'Allow Access to SNMP Manager from' 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 is allowed.

Security Type: It provides the Security Type currently used for SNMPv3. You can select 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-decrypt 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 **Save** to save the SNMP settings.

Notification Settings

Enable Notification: Enable 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 is occurred.

- 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 wants 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 running.

Retry Attempts: It is applicable when Notification Type is selected as "**Inform**". It specifies the number of count 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. Below Category/Filter is provided:

- Door Events
- Alarm Events
- System Events

Each filter option contains severity as:

- Information
- Warning
- Error

The Monitor displays the door status as Offline, Online, Upgrade and Degrade mode. Also different types of Actions can be performed on the door.

The screenshot shows the 'Monitor' page with a table of door configurations and a detailed view for 'Door V3'.

Panel Name	IP Address	MAC Address	Panel Type	Action
RnD Panel Lite	192.168.104.111	00:1b:09:04:65:d1	PANEL LITE V2	

Door Name	IP/RS-485 Address	MAC Address	Door Type	Action
✓ Door V3	192.168.104.114	00:1b:09:05:3f:e2	V3 DOOR	
✓ Arc Dual Door1	192.168.104.112	00:1b:09:04:80:ca	ARC DC 100	
✓ Arc Dual Door2	192.168.104.112	00:1b:09:04:80:ca	ARC DC 100	

Door V3
Active

- Door ID: 1
- Door Name: Door V3
- Status: Online
- Communication Type: Ethernet
- IP/RS-485 Address: 192.168.104.114
- MAC Address: 00:1b:09:05:3f:e2
- Door Status: Normal
- Alarm: None
- Door Sense: Disable
- Card Reader: EM Prox Reader
- Biometric Reader: Finger Reader
- External Reader: None
- Firmware Version: V01R33

The log of different events is displayed on Event Log page.

The screenshot shows the 'Event Logs' page with search filters and a table of logs.

Search by

Date: From 29-03-2018 To 29-03-2018

Time: From 00:00 To 23:59

Log Type:

- User Allowed
- User Denied
- Door
- Alarm
- System

Search: []

Backup: Save Log On PC xls []

Date and Time	Type	Device	Source	Description
29-03-2018 09:03:29	User Allowed	PVR Door	PVR DOOR	Entry allowed to 3 : Isha
29-03-2018 19:03:30	User Allowed	PVR Door	PVR DOOR	Entry allowed to 3 : Isha
29-03-2018 09:49:02	System	PVR Door	PVR DOOR	Palm enrolled for 4 : Aditi
29-03-2018 09:49:23	User Allowed	PVR Door	PVR DOOR	Entry allowed to 4 : Aditi
29-03-2018 19:49:32	User Allowed	PVR Door	PVR DOOR	Entry allowed to 4 : Aditi
29-03-2018 12:01:58	System	PVR Door	PVR DOOR	Palm enrolled for 3 : Isha
29-03-2018 12:51:43	System		PANEL LITE V2	Palm, of 3 : Isha Deleted through Web Jeeves
29-03-2018 12:52:19	System	PVR Door	PVR DOOR	Palm enrolled for 3 : Isha
29-03-2018 12:52:51	User Denied	PVR Door	PVR DOOR	Entry denied to 3 : Isha since User Authorization is Pending
29-03-2018 12:58:23	System		PANEL LITE V2	System User admin has Authorized User 3 : Isha

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' interface with a search bar and a 'Door Type' dropdown menu. A list of doors is displayed, including 'Door V3'. A detailed view for 'Door V3' is shown on the right, displaying various attributes such as Door ID, Door Name, Status (Online), Communication Type (Ethernet), IP/RS-485 Address, MAC Address, Door Status (Normal), Alarm (None), Door Sense (Disable), Card Reader (EM Prox Reader), Biometric Reader (Finger Reader), External Reader (None), and Firmware Version (V01R33).

The devices can also be filtered on the basis of their Status. You can select the icon of **Online Devices**, **Offline Devices**, **Devices in Degrade State**, **Upgrading Device**, **Alarms on Device**. By default All Devices are selected and shown in the list.

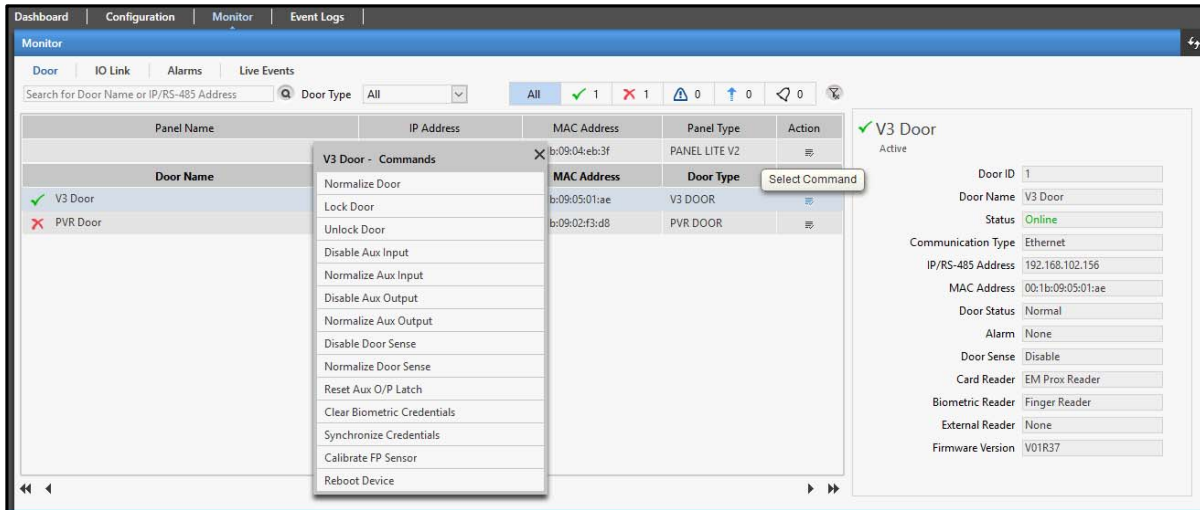
Door Name	IP/RS-485 Address	MAC Address	Door Type	Action
✗ v3	192.168.104.156	11:55:66:99:88:77	V3 DOOR	⋮
⬆ PVR 113	192.168.104.113	00:1b:09:03:f2:b0	PVR DOOR	⋮
✗ ARC Door	192.168.104.112	00:1b:09:04:80:ca	ARC DC 100	⋮
✓ IO Controller 1	192.168.104.51	00:04:A3:08:55:89	ARC IO 800	⋮
✗ Vega Door	192.168.104.99	21:35:34:65:43:54	VEGA DOOR	⋮

The **count** of the different door status represents the total number of doors belonging to the respective status. For example: If Online devices shows count as 3; then total 3 doors are online.

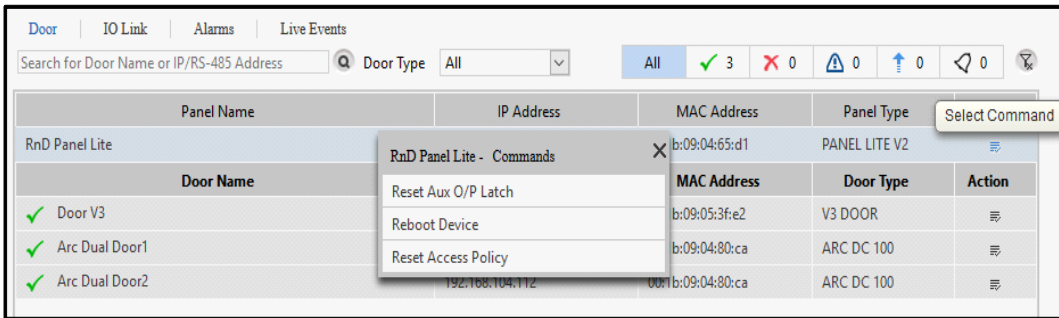
The screenshot shows the 'Monitor' interface with the 'Online Devices' filter selected. The search bar is empty, and the 'Door Type' dropdown is set to 'All'. The status bar shows 'All' with a count of 3 Online Devices, 0 Offline Devices, 0 Degrade State Devices, 0 Upgrading Devices, and 0 Alarms on Device. The list of doors is filtered to show only Online Devices: 'Door V3', 'Arc Dual Door1', and 'Arc Dual Door2'.

The filter can be cleared by clicking on **Clear Filter** button.

Action: By clicking on Action; a list of commands will be shown. You can give the desired commands to the device:



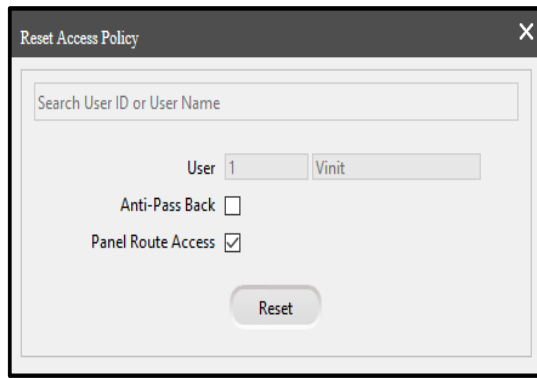
The right side on the Door page shows the details of device depending on the door type which is hovered.



The command can be sent to the Panel lite V2 by clicking on **Select Command** button as shown above. You can **Reset Aux O/P Latch, Reset Device and Reset Access Policy** by selecting the respective commands.

When user violates an access policy he is denied access on the Panel lite V2 if hard violation is configured for access policies So you can reset the Access policy to allow the access to the user.

When the Reset Access Policy is selected; then Reset Access Policy page appears as shown below.



Enter the User Id/Name in search field. When the user is selected; you can enable the Anti-Pass Back and Panel Route Access policies 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

Alarms displays various alarms which have been activated on the system. It also provides the user with the option to acknowledge or clear these reported alarm conditions.



For generating Alarm, the Alarm must be enabled from Advance Profile and Door Configuration.

- The Date and time at which alarm generated with the description of Alarm is displayed in the list.
- The Category of the alarm and status is displayed in the list.
- To acknowledge the alarm, click the button in **Acknowledge** column for the respective alarm.
- To clear the alarm, click the button in **Clear** column for the respective alarm.

- All the Alarms can be acknowledged by clicking **Acknowledge All** button and cleared by clicking **Clear All** button.

The example of Critical Alarm is shown below.

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			

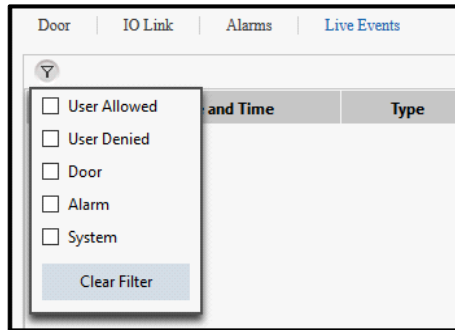
Monitor									
Door		IO Link		Alarms		Live Events			
Sr. No.	Date	Time	Source	Description	Category	Status	Acknowledge	Clear	
1	02-01-2018	16:35:18	PVR 113	DC Tamper	Critical	Acknowledged			

Live Events

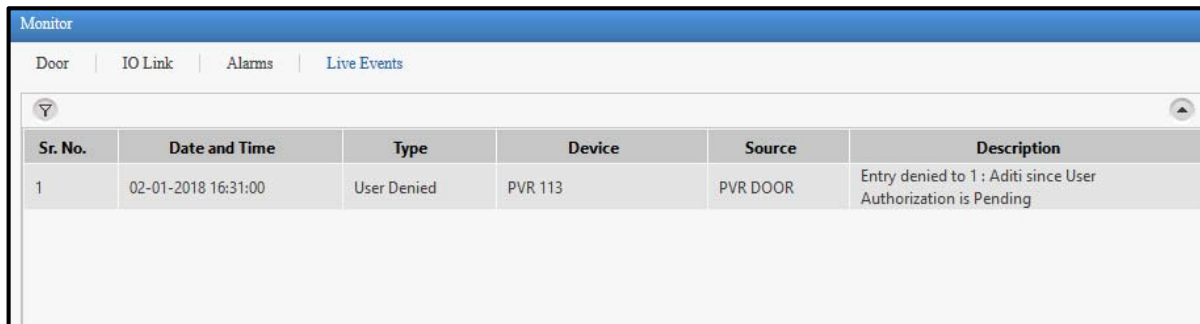
Live Events page enables to view the events occurring at device with auto refresh in 3s.

Filter

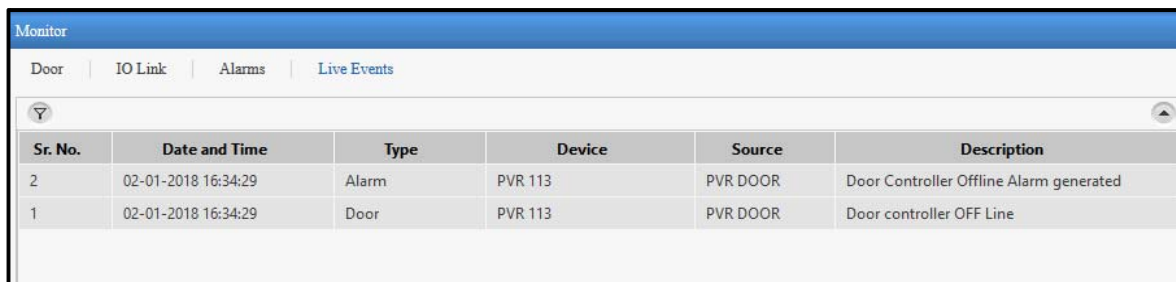
To view the particular event on the Live Events page, click the Filter and select the checkbox for the respective event.



The generated events will appear in the list. The details of events like Date and Time, event type, device, source and description will appear on the page.

A screenshot of the 'Live Events' page showing a table with one event. The table has columns for 'Sr. No.', 'Date and Time', 'Type', 'Device', 'Source', and 'Description'. The event listed is 'User Denied' at '02-01-2018 16:31:00' for device 'PVR 113' and source 'PVR DOOR'. The description is 'Entry denied to 1 : Aditi since User Authorization is Pending'.

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

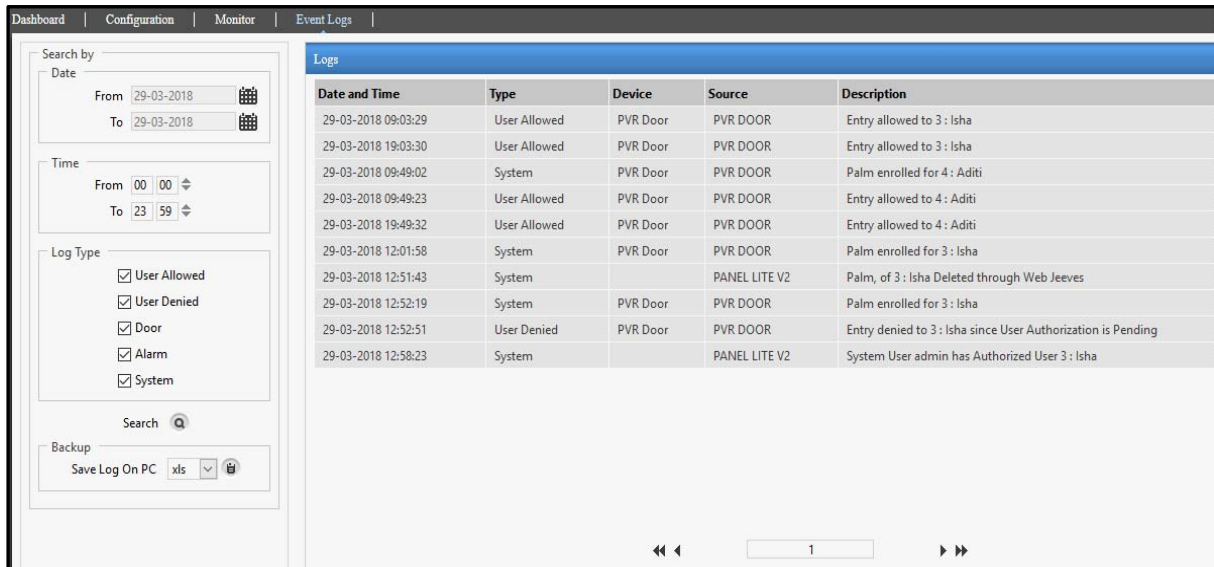
A screenshot of the 'Live Events' page showing a table with two events. The table has columns for 'Sr. No.', 'Date and Time', 'Type', 'Device', 'Source', and 'Description'. The first event is 'Alarm' at '02-01-2018 16:34:29' for device 'PVR 113' and source 'PVR DOOR', with description 'Door Controller Offline Alarm generated'. The second event is 'Door' at '02-01-2018 16:34:29' for device 'PVR 113' and source 'PVR DOOR', with description 'Door controller OFF Line'.

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.

Event Logs

The log maintains a 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 its occurrence.



The screenshot shows the 'Event Logs' section of a web application. On the left, there are search filters for Date (From: 29-03-2018, To: 29-03-2018), Time (From: 00:00, To: 23:59), and Log Type (User Allowed, User Denied, Door, Alarm, System). A 'Search' button is present. Below the filters is a 'Backup' section with a 'Save Log On PC' button and a file format dropdown set to 'xls'. The main area displays a table of logs with the following data:

Date and Time	Type	Device	Source	Description
29-03-2018 09:03:29	User Allowed	PVR Door	PVR DOOR	Entry allowed to 3 : Isha
29-03-2018 19:03:30	User Allowed	PVR Door	PVR DOOR	Entry allowed to 3 : Isha
29-03-2018 09:49:02	System	PVR Door	PVR DOOR	Palm enrolled for 4 : Aditi
29-03-2018 09:49:23	User Allowed	PVR Door	PVR DOOR	Entry allowed to 4 : Aditi
29-03-2018 19:49:32	User Allowed	PVR Door	PVR DOOR	Entry allowed to 4 : Aditi
29-03-2018 12:01:58	System	PVR Door	PVR DOOR	Palm enrolled for 3 : Isha
29-03-2018 12:51:43	System		PANEL LITE V2	Palm, of 3 : Isha Deleted through Web Jeeves
29-03-2018 12:52:19	System	PVR Door	PVR DOOR	Palm enrolled for 3 : Isha
29-03-2018 12:52:51	User Denied	PVR Door	PVR DOOR	Entry denied to 3 : Isha since User Authorization is Pending
29-03-2018 12:58:23	System		PANEL LITE V2	System User admin has Authorized User 3 : Isha

Search Criteria

The event log can be filtered as per the date, time and type of the log.

Select the From date and To date from the calendar button to view the log for selected dates.

Set the From and To time by up-down arrow buttons.

Select the type of log as User allowed, User denied, Door, Alarm and/or System.

Then click on **Search** button to search for the logs.

Display Log

The event log will be displayed along with the date and time of generation. The Type of event, Device, Source and Description is also displayed.

You can view the events on other pages by scrolling the arrows.

Backup

The backup of the event log can be taken in XLS, CSV or text format and saved at the desired location on the PC.



MATRIX COMSEC

Head Office:

394-GIDC, Makarpura, Vadodara - 390010, India.

Ph:(+91)18002587747

E-mail: Support@MatrixComSec.com

www.MatrixSecuSol.com