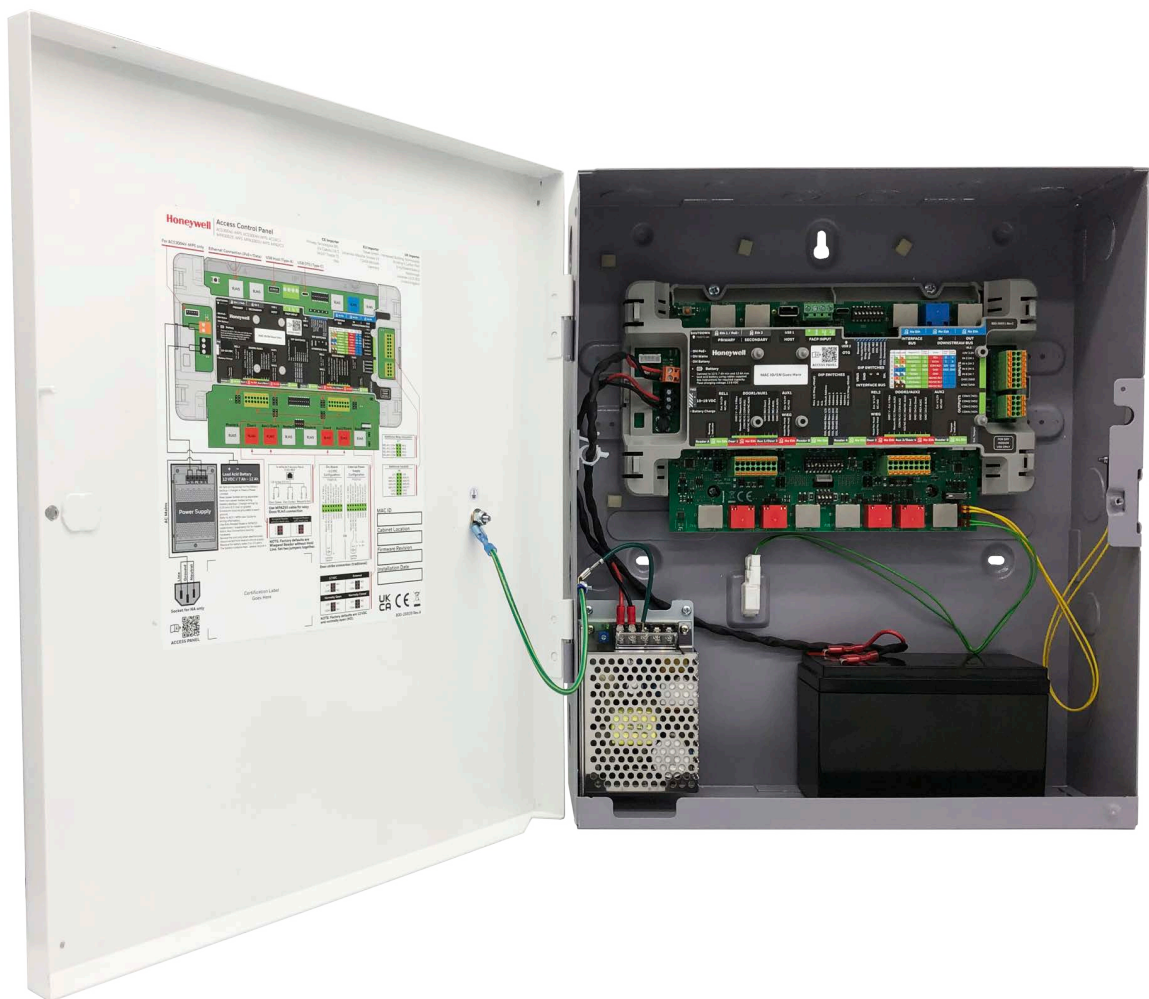


Honeywell | THE FUTURE IS WHAT WE MAKE IT

MPA2C3 Access Control Unit



User Manual

TABLE OF CONTENTS

Chapter 1 - Getting Started.....	13
Overview.....	13
Licensing.....	14
Connecting to the Web Server	14
Setting Up the USB Connection	14
Setting Up an Ethernet Port	17
Navigating through MPA	23
The MPA2 Dashboard.....	23
Accessing the Menu	24
Chapter 2 - Basic settings.....	27
Basic Settings.....	27
Overview	27
Configuring the EVL (Ethernet Virtual Group).....	28
What is an EVL?.....	28
Network Requirements.....	28
DIP Switch Settings (EVL Mode)	28
Configuring the System Via RS-485 Loop	32
DIP Switch Settings (RS485 Mode).....	33
RS-485 Unregister	34
Managing Configuration Data.....	35
Configuring Host/Loop Communications	36
Setting Communication Parameters for WIN-PAK	36
Setting the Communication Mode to Web	39

Configuring for MAXPRO Cloud.....	40
Initial Panel Setup	41
Entering a Panel Name.....	42
Configuring the Network Settings.....	43
Configuring Time Management.....	43
Configuring Spaces	50
Removing a Door from an Access Group.....	51
Configuring Doors.....	53
Accessing the Doors Configurations.....	53
Configuring Door Reader Settings.....	55
About Supervisor Mode	57
About Escort Mode	58
Configuring Door Inputs.....	60
Configuring Door Outputs	63
Configuring Panel I/O and Groups.....	66
Configuring Outputs.....	69
Configuring Output Groups	71
Configuring Card Formats	72
Managing Site Codes	76
Creating a Site Code.....	77
Modifying a Site Code	77
Deleting a Site Code.....	78
Interlock Configuration	78
Creating Interlocks	79
Deleting Interlocks.....	81
Downstream Devices.....	81
Configuring People and Cards	82
Configuring People.....	82
Creating a Person.....	83
Modifying a Person	84
Deleting a Person	85
Configuring Cards.....	85
Adding a New Card	87

Modifying Cards.....	88
Deleting Cards	89
Configuring Access Groups	89
Creating a New Access Group	91

Chapter 3 - Monitoring and Reporting93

Monitoring and Reporting.....	93
Monitoring	94
Monitoring Alarms and Events	94
Monitoring/Managing Doors.....	97
Monitoring Inputs.....	97
Monitoring and Controlling Outputs	99
Monitoring and Controlling Output Group.....	101
Reporting.....	102
Generating Event Reports.....	102
Generating Diagnostic Reports	103
Generating People/Card Reports	104
.....	107
Configuring FACP input functionality	107
FACP input functionality	107
Door Access Modes.....	107

Chapter 4 - FACP Input and Notification107

Door access mode indication	108
Door Access Modes and Door lock behaviors	109
FACP input prerequisites.....	110
FACP input set up procedure- FAIL-SAFE INSTALLATION	111
FACP settings for Interlocks and Reporting only.....	115
Configurations during Reversed Door Access Mode	117
Controlling Doors in Reversed Door Access Mode.....	117
FACP input activation in Alarm-Notifications.....	118
.....	120
Overview	121

Backing Up..... 121

Chapter 5 -121

Chapter 5 - Maintenance121

Upload (From Panel)..... 122

Backing Up (or Uploading) Other Data from the Panel to the Host System.... 122

Card Report..... 122

Diagnostic Report 122

System-wide Backup 123

Download (To Panel)..... 124

Firmware Download (Also see: [Firmware Upgrades](#))..... 124

Downloading a Card Database Report (.CVS file) from the Host System to the Panel..... 125

Backup file Download..... 125

Restoring (Downloading) Panel Only..... 125

Restoring (Downloading) Entire Loop 126

Synchronizing a New Panel with Information on an Existing Panel 127

Replace a Primary Panel in an Existing Loop (Web Mode)..... 127

Overview..... 127

Primary Panel Replacement and System Wide Restore 127

Replace a Secondary Panel (Web Mode) 128

Overview..... 128

Hard Default a Primary in an Existing Loop (Web Mode) 129

Overview..... 129

Hard Default an Existing Secondary Panel (Web Mode)..... 129

Overview..... 129

Primary | Secondary Panel Synchronization (Hard Default) 129

Synchronization Detail Chart..... 130

Restore Entire Loop Detail Chart 131

Panel Resets and Restorations 133

DIP Switch Settings 133

Restoring the Panel to Factory Default Settings 134

Resetting the Panel 135

Firmware Upgrades	135
Panel Requirements	135
Overview	135
Planning for the Firmware Upgrade	136
Updating the MPA2C3 Panel Using the Web Interface	137
Shutting Down and Restart the Panel.....	138
Restart the Panel	138
Panel Requirements	141
Overview	141
Planning for the Firmware Upgrade	141
.....	141

Chapter 6 - Firmware upgrades..... 141

Updating the MPA2C3 Panel Using the Web Interface	142
.....	144
Caches	145

Chapter 7 - Caches and Certificates 145

Generating and Installing Certificates	146
Section 1 - Generating sign-in request and installing certificates	146
Section 2 - Installing the master certificate into the browser	149
Creating MPA2C3 Accounts	155
.....	155

Chapter 8 - MPA2C3 Accounts..... 155

Modifying a User Account	159
Deleting a User Account	159
Admin Password Reset.....	159
Technical Support.....	161
Normal Support Hours	161

Copyright © 2022 Honeywell. All rights reserved.

All product and brand names are the service marks, trademarks, registered trademarks, or registered service marks of their respective owners. Printed in the United States of America. Honeywell reserves the right to change any information in this document at any time without prior notice. Microsoft and Windows are registered trademarks of Microsoft Corporation. Windows Server is a trademark of Microsoft Corporation.

Ordering Information

Please contact your local Honeywell representative or visit us on the web at <https://buildings.honeywell.com/> for information about ordering.

Feedback

Honeywell appreciates your comments about this manual. Please visit us on the web at <https://buildings.honeywell.com/> to post your comments.

Training

Honeywell provides training for better understanding of the product. Please visit <https://myhoneywellbuildingsuniversity.com/>

Digital Manuals and manuals in other languages

Honeywell provides this manual in English and other languages Online:

Get Online Document [Here](#)



The link is also found by scanning the following QR code.

WARNING Installation and servicing should be performed only by qualified and experienced technicians to conform to all local codes and to maintain your warranty.

Regulatory Statements

Waste Electrical and Electronic Equipment (WEEE)

Correct Disposal of this Product (applicable in the European Union and other European countries with separate collection systems).

This product should be disposed of, at the end of its useful life, as per applicable local laws, regulations, and procedures.

INSTALLATION

Install in accordance with the manufacturer's instructions.

Installation and servicing should be performed only by qualified and experienced technicians to conform to all local codes and to maintain your warranty.

POWER SOURCES - This product should be operated only from the type of power source indicated in the guide. If you are not sure of the type of power supplied to your facility, consult your product dealer or local power company.

MOUNTING SYSTEM - Use only with a mounting system recommended by the manufacturer, or sold with the product.

ATTACHMENTS/ACCESSORIES - Do not use attachments/accessories not recommended by the product manufacturer as they may result in the risk of fire, electric shock, or injury to persons.

SERVICING - Do not attempt to service this unit yourself. Refer all servicing to qualified service personnel.

REPLACEMENT PARTS - When replacement parts are required, be sure the service technician has used replacement parts specified by the manufacturer or have the same characteristics as the original part. Unauthorized substitutions may result in fire, electric shock or other hazards. Using replacement parts or accessories other than the original manufacturers may invalidate the warranty.

Warranty and Service

Subject to the terms and conditions listed on the product warranty, during the warranty period Honeywell will repair or replace, at its sole option, free of charge, any defective products returned prepaid.

Be sure to have the model number, serial number, and the nature of the problem available for the technical service representative.

Prior authorization must be obtained for all returns, exchanges, or credits. Items shipped to Honeywell without a clearly identified Return Merchandise Authorization (RMA) number may be refused.

GETTING STARTED

Overview

The MPA2C3 panel is a modular 2 and 4 Door access control system. An MPA2 access control site is configured with a host system and access control units. These units also communicate with each other and with a variety of input and output devices. Each access control unit, or panel, has up to four reader connection. Each connection can support one Wiegand reader and two readers for OSDP (Reader A (IN) and B (OUT)).

MPA2C3 supports up to 4 Wiegand readers. Any Wiegand reader without hold wire can be connected. In a MPA2C3 2 door panel both doors can be controlled with 2 Wiegand readers, configured as IN and OUT Reader. In a MPA2C3 4 door panel each door can be controlled with 1 Wiegand reader, only configured as IN Reader.

MPA2C3 can also support up to 8 OSDP readers. See for a list of compatible OSDP readers. In a MPA2C3 2 or 4 door panel each door can be controlled with 2 OSDP readers, configured as IN and OUT Reader.

Per door peripheral inputs (for Request-to-EXit (REX) and Doorcontacts (DrCnt)) and an output (Locking device) are available.

Additional 8 inputs and 4 outputs are available for internal logical connections (interlocking) or control via the user interfaces or host software. Per Panel a FACP (Fire Alarm Control Panel) input is available to override the controlled door outputs for people to allow to free egress the connected doors.

Panels can be connected in a (Primary/Gateway – Secondary/Downstream) RS485 loop or in a EVL (Ethernet Virtual Loop) configuration.

The User Interface with the MPA2 access control unit is either through a host software system or by connecting to the built in web server through an Ethernet or USB connection. This user manual describes the configuration, monitoring and control via the web server.

For hardware and wiring installation instructions, please see the Installation Guide supplied. The MPA2 is designed to work with most operating systems and browsers, but Honeywell recommends Chrome™ for the best performance.

Note: *All information in this document (descriptions, technical specifications, pictures, illustrations etc) are indicative only, not binding and can be changed without notice. Nevertheless, this document remains valid.*

Licensing

To obtain 4 Door access control system, user need to buy the specific license. Once the license file is applied on the panel then user can use the 4-Door controller. Please contact Honeywell Customer Support team for 4-door license.

Connecting to the Web Server

The MPA2 embedded web server is intended for supplementary and programming purposes only. It has not been evaluated by UL294 evaluation consist of the stand alone mode of this device for use as a monitoring station.

The embedded web server can be accessed through the following three connection types:

- USB (via USB2 WEB MODE)
- Ethernet (via Eth1/PoE+- HOST) through a direct connection
- Ethernet (via Eth1/PoE+- HOST) through a Switch/LAN connection

Note: *1) The panel that you are connecting to the computer is the Primary panel. DIP SW1 Bit 3 on a Primary panel must be set to ON for a successful connection.*

2) When creating a user in MPA2 -> Web server, the administrator should obtain and maintain the consent.

Setting Up the USB Connection

Warning: Do NOT connect the USB cable to the panel until AFTER the drivers are installed.

Note: *Honeywell recommends Chrome™ for the best performance.*

1. Register and log-in to <https://myhoneywellbuildingsuniversity.com/training/support/> Click Download Center > Access Control > MPA > MPA2 Resources and USB Driver Media CD. Click on download link (“Click here to Download” or the Down-



load Icon).

Note: Please add the following to the list of trusted sites in Internet options and set your security level to Low for trusted sites." <https://acshsgdownloadcenter.blob.core.windows.net>
<https://buildings.honeywell.com/>

If the file is blocked by the browser then:

- Navigate to the downloaded MPA2 Resources and USB Driver Media CD.zip file
- Right click on the file and select Properties. In the General Tab click "Unblock"

1. Locate and open the compressed ZIP file. Click on the Driver folder. Double-click on MPA-USB-setup.exe file to launch. Select Run and select Yes to allow the USB Driver to be installed.

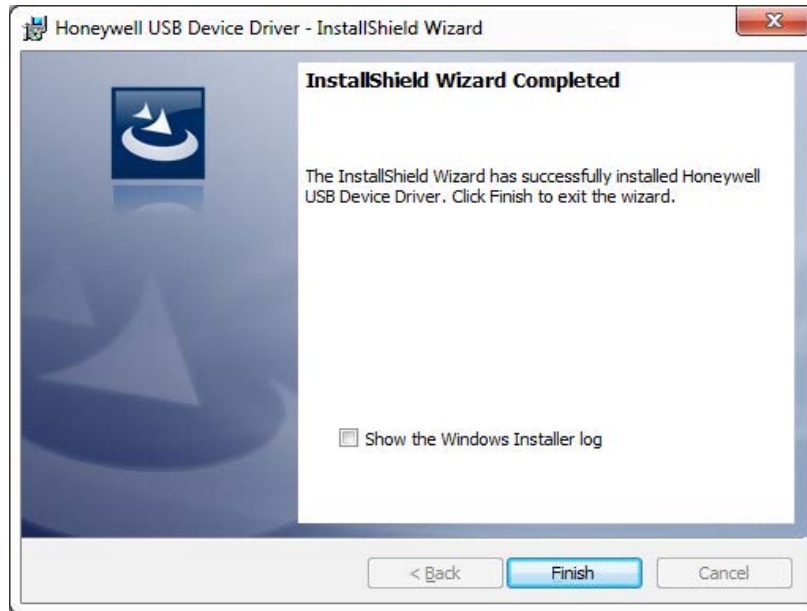


2. Click **Next** to **display** the Ready to Install the Program screen.

Note: *If confirmation dialog boxes pop up before or during the installation, click the appropriate boxes to allow or approve the installation.*



3. Click **Install** to initiate the installation. When the installation is complete, the closing screen appears:



4. Click **Finish**.
5. Connect the computer to the MPA2C3 controller USB2 - WEB MODE connector with a Type-C USB cable.
6. Supply power to the MPA2 controller. Login at <https://192.168.2.150>.

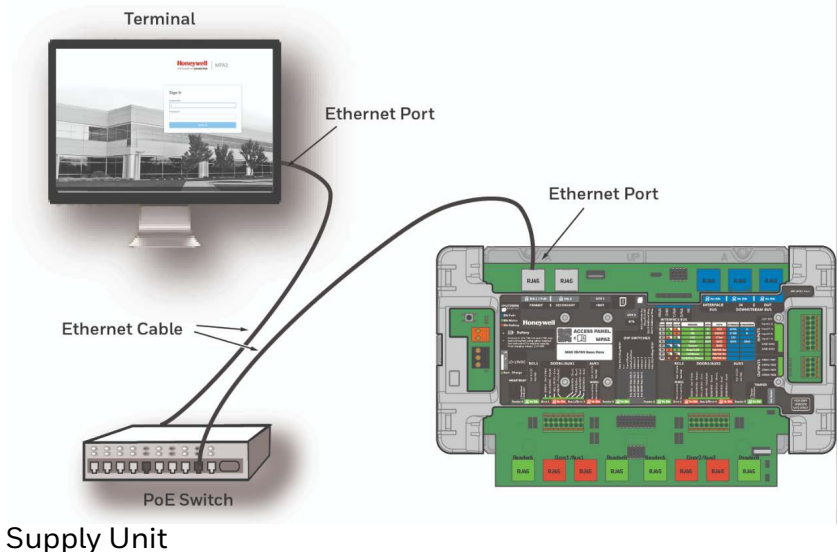
Setting Up an Ethernet Port

There are two options for connecting the panel to a PC via a web server via the Ethernet port Eth1 / PoE+ - HOST:

- Using a Switch /LAN connection
- Using a direct connection

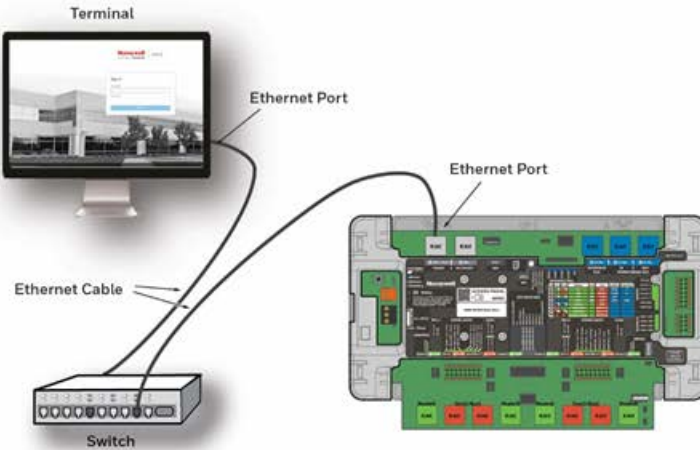
To set up a new Ethernet Port for the panel powered by PoE+

Ethernet switch connection: Connect both the computer's Ethernet port and the panel's Ethernet port (Eth1/PoE+ - HOST) to an Ethernet switch with standard Ethernet patch cables. To set up an Ethernet Port for the panel powered Power

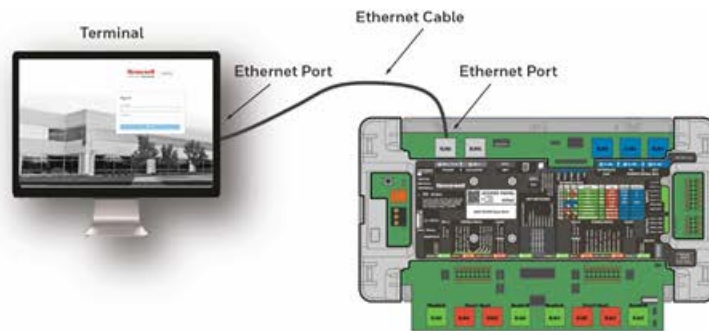


To Set up an Ethernet Port for the Panel Powered by Power Supply Unit

1. Connect your computer's Ethernet port to the panel's Ethernet port using one of the following two methods:
 - a. Ethernet Switch connection: Connect both the computer's Ethernet port and the panel's Ethernet port (Eth1/PoE+ - HOST) to an Ethernet switch with standard Ethernet patch cables.



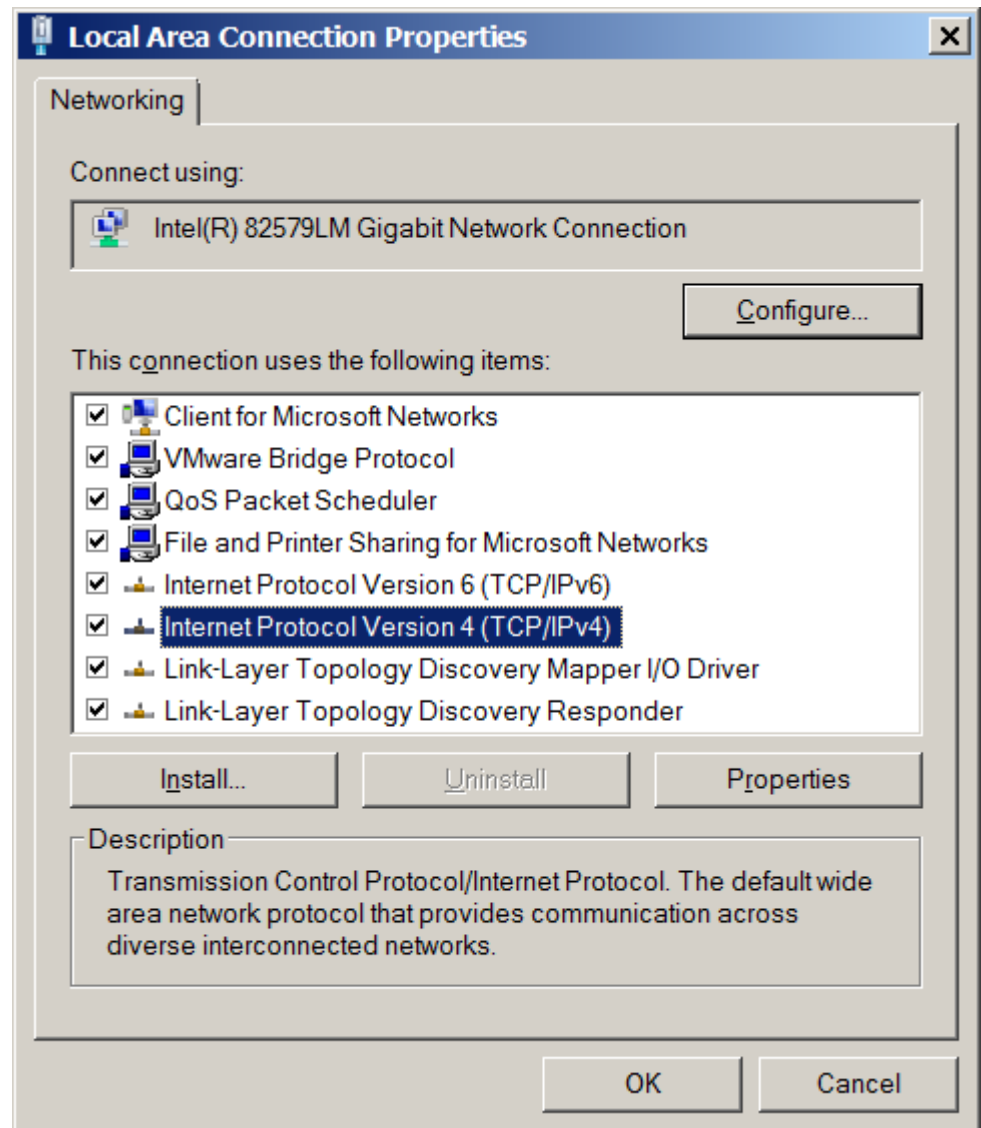
- b. Web server direct connection: Connect the computer's Ethernet port directly to the panel's Ethernet port (Eth1/Poe+-HOST) with either a crossover or an Ethernet cable.



Tip: Turn ON DIP Switch 4 in SW1 to put the panel under default IP 192.168.1.150.

1. Configure the computer's network connection:
 - a. Select **Start > Settings > Control Panel**.
 - b. Click **Network and Dial-up Connections**.

- c. Identify your local Ethernet connection (commonly labeled Local Area Connection), and right-click the icon to display the Local Area Connection Properties screen.

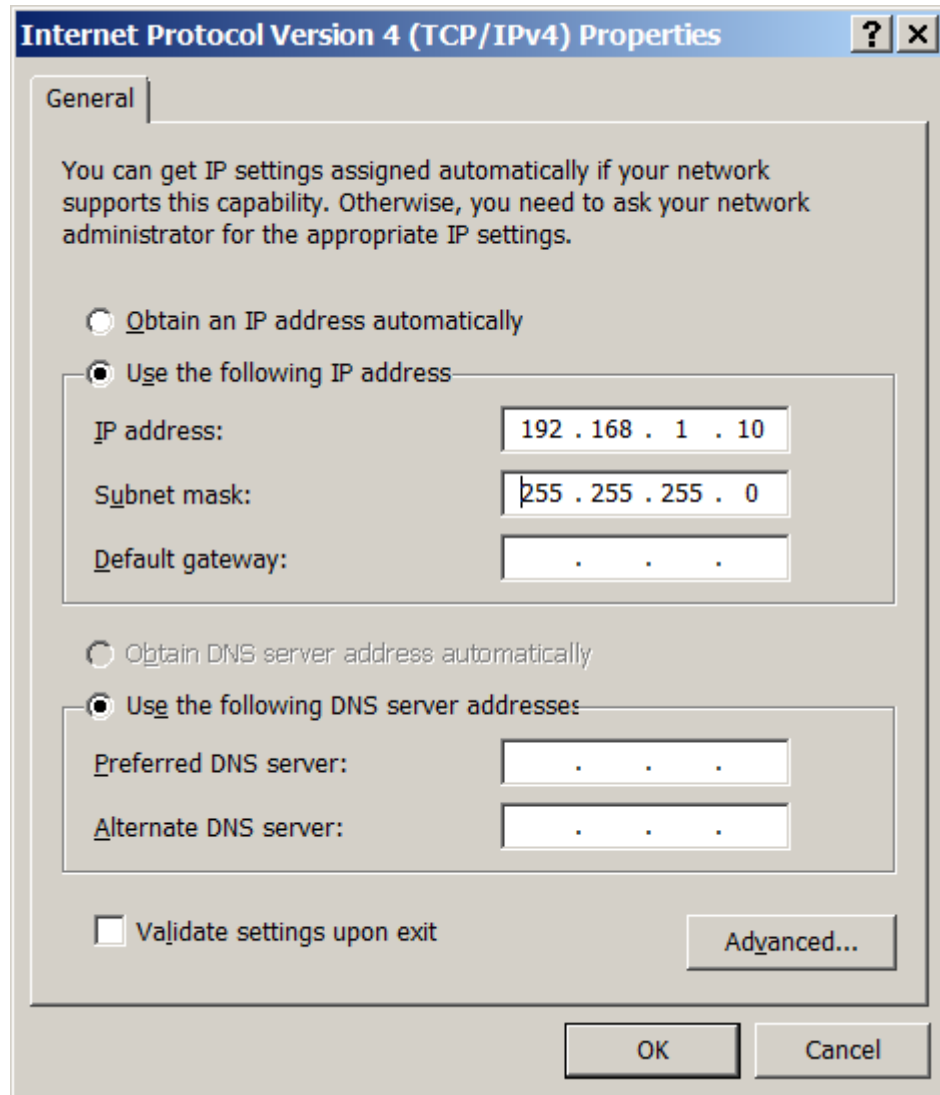


- d. Highlight the Internet Protocol (TCP/IP) connection.
e. Click **Properties** to display your system's current Internet Protocol properties.

Tip: Keep a record of your computer's current network configuration as it appears in this screen. You will need to re-instate this configuration later. Select **Use the following IP address**.

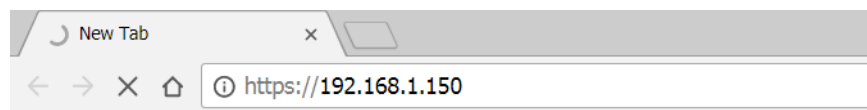
- f. Enter **192.168.1.10** in the IP address field.

- g. Enter 255.255.255.0 in the Subnet mask field.



- h. Click **OK** to accept the entries.

1. Open your browser, and enter **https://192.168.1.150** as the target address.

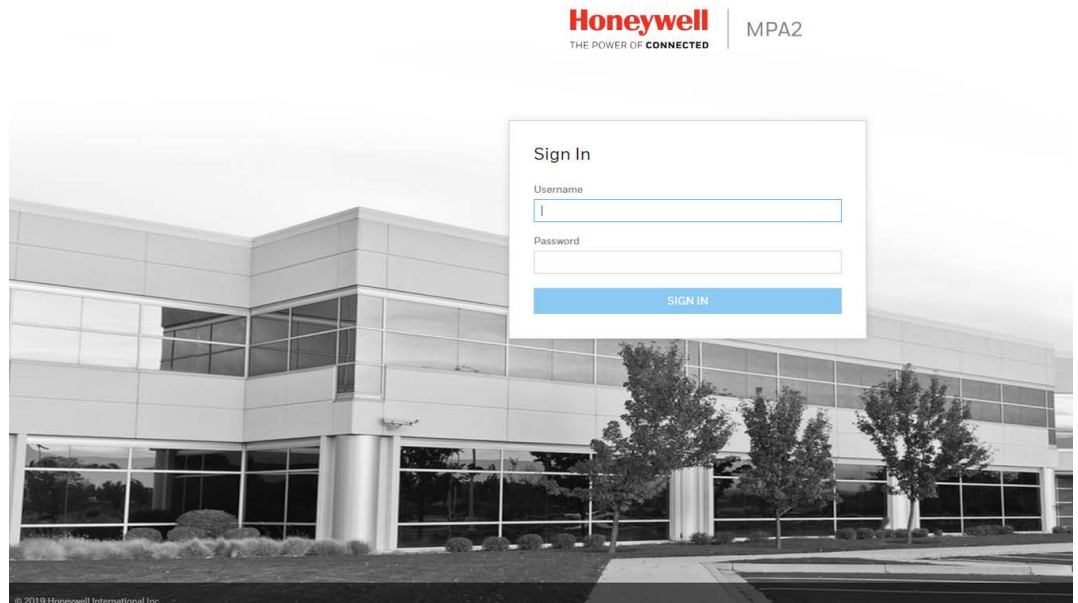


Caution: When connecting to the web using a browser, you must use **https://** for a secure connection. The standard **http://** that is the default in most browsers will not work.

2. Press the Enter key to display the Honeywell MPA2 login screen.

Note: If you are using Google Chrome and you receive a message “Your connection is not private”, follow the below steps to get to the Sign In screen.

- a. Click **Advanced** to expand the popup window.
- b. Click **Proceed to <panel's> IP address (unsafe)**. The Sign In screen appears.



Note: For instructions on certificate errors see the [Chapter 5, Caches and Certificates](#).

1. Enter **admin** in the **User Name** field, and enter **admin** in the **Password** field. Both the user name and password are case-sensitive.

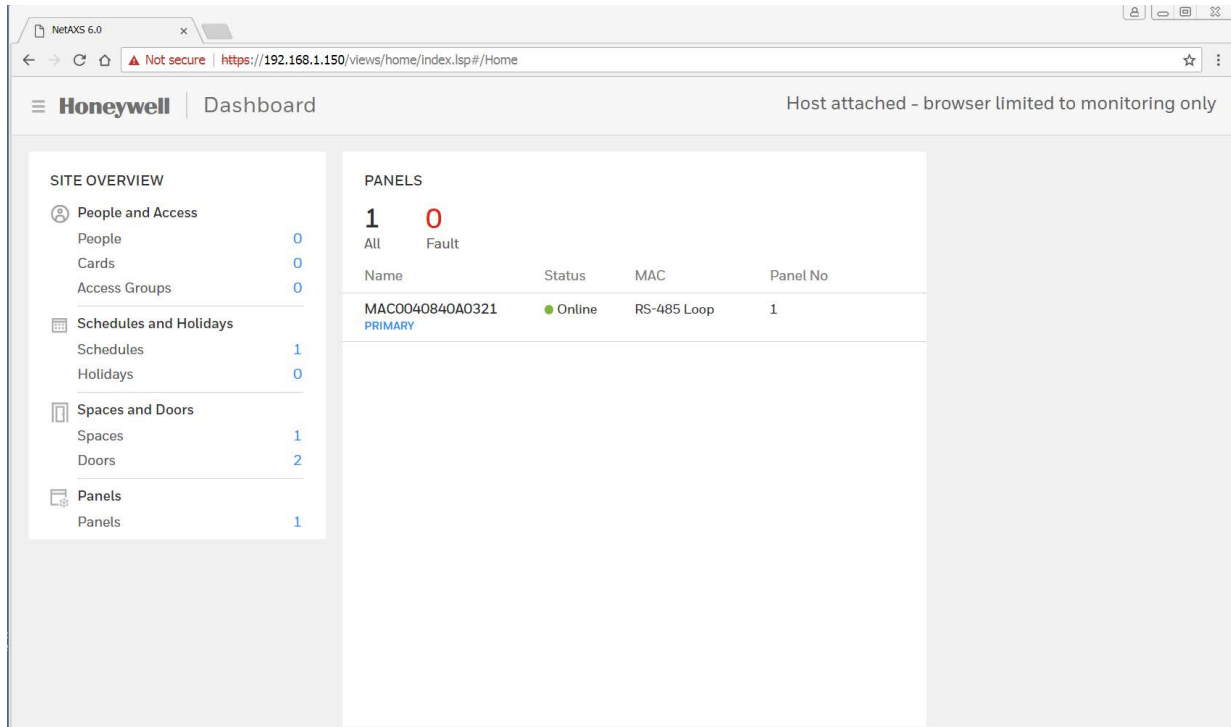
Note: If you fail to log in successfully 5 times, the *Retry Limit* will be exceeded, and the account locks for 30 minutes. Any attempt to log into a locked-out account, within the timeout period, restarts the 30 minute lock-out period.

Note: On initial signing in, you will be asked to change your password to a new password. For more information see [Creating MPA2C3 Accounts](#) section on page 123.

1. Click **Sign In**. By default, the MPA2 opens to the Dashboard.

Navigating through MPA

The MPA2 Dashboard



On the MPA2 Dashboard, you can see the following:

- A list of all the panels in the loop.
- Any offline panels.
- The number of currently existing entries in the database.
- Clicking on the links on the Dashboard will take you directly to the selected database page.

Accessing the Menu

Figure 1-1 In the upper left corner is the **Menu** button, allows you access to all of the MPA functions.

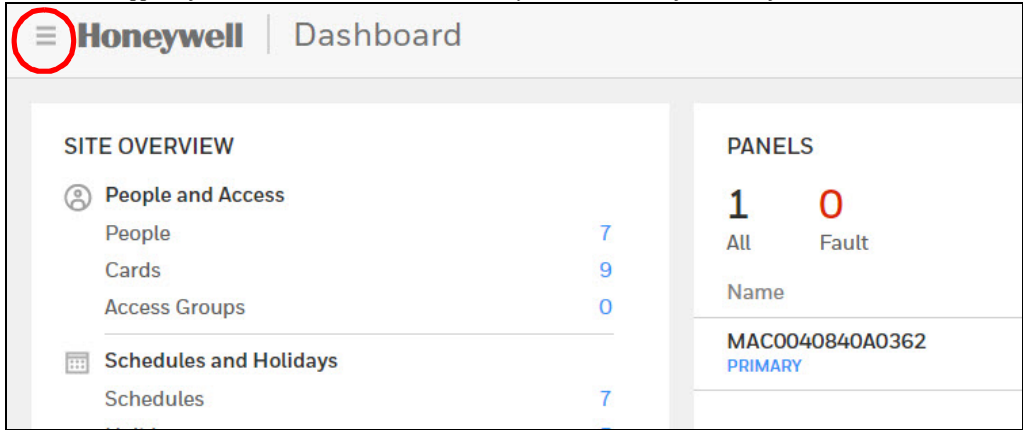


Figure 1-2 Main Menu

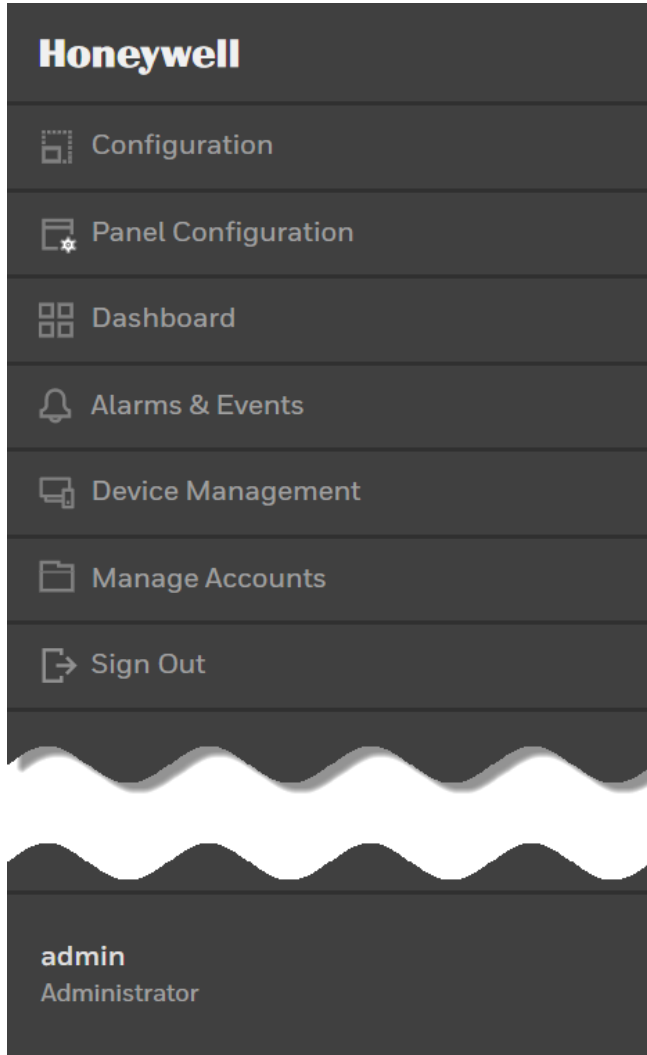


Table 1-1 Main Menu Selections

Icon	Description	For more information, see...
 Configuration	Access configuration options for Spaces, Schedules, Holiday, People and Cards, and Access.	Configuring Spaces on page 40 ; Configuring People and Cards section on page 60; Entering a Panel Name section on page 31
 Panel Configuration	Access panel configuration options.	Configuring the EVL (Ethernet Virtual Group) section on page 18; Configuring the System Via RS-485 Loop section on page 22; Initial Panel Setup section on page 30
 Dashboard	View the Configuration Summary, and the status of all the panels in the loop.	Navigating through MPA section on page 23
 Alarms & Events	View alarms and events	Monitoring Alarms and Events section on page 81; Table 3-6
 Device Management	Manage Spaces, Doors, and Auxiliary Connections (such as Inputs, Outputs, and Output Groups)	Configuring Spaces on page 40 ; Configuring Doors on page 44 ; Configuring Panel I/O and Groups section on page 46
 Manage Accounts	Specify that an account is Administrator, Service, or Operator. Select Language Preference.	Creating MPA2C3 Accounts section on page 123
 Sign Out	Sign out	
 admin Administrator	The current user	

This page is intentionally left blank

Basic Settings

Overview

This chapter explains the MPA2C3 configuration functions as accessed via the web server. These functions should be performed only by the system administrator or service personnel.

Caution: The sequence of MPA2C3 configuration tasks is critical. If you do not follow the sequence described in [Table 2-1](#), the system cannot be successfully configured.

Table 2-1 Configuration Task Sequence

To...	Go here...
Configure the System via EVL (Ethernet Virtual Loop)	Configuring the EVL (Ethernet Virtual Group) section on page 28
OR	
Configure the system via RS485	Configuring the System Via RS-485 Loop on page 22
Initial panel setup	Initial Panel Setup section on page 41
Configuring schedules	Configuring Schedules section on page 45
Configuring spaces	2-Door Inputs Configuration Interface section on page 61
Configuring people and cards	Configuring People and Cards section on page 82
Configuring access groups	Configuring Access Groups section on page 89

Note: Screen captures taken on a **Windows 7** platform. If you use another OS, then the GUI might be different.

Configuring the EVL (Ethernet Virtual Group)

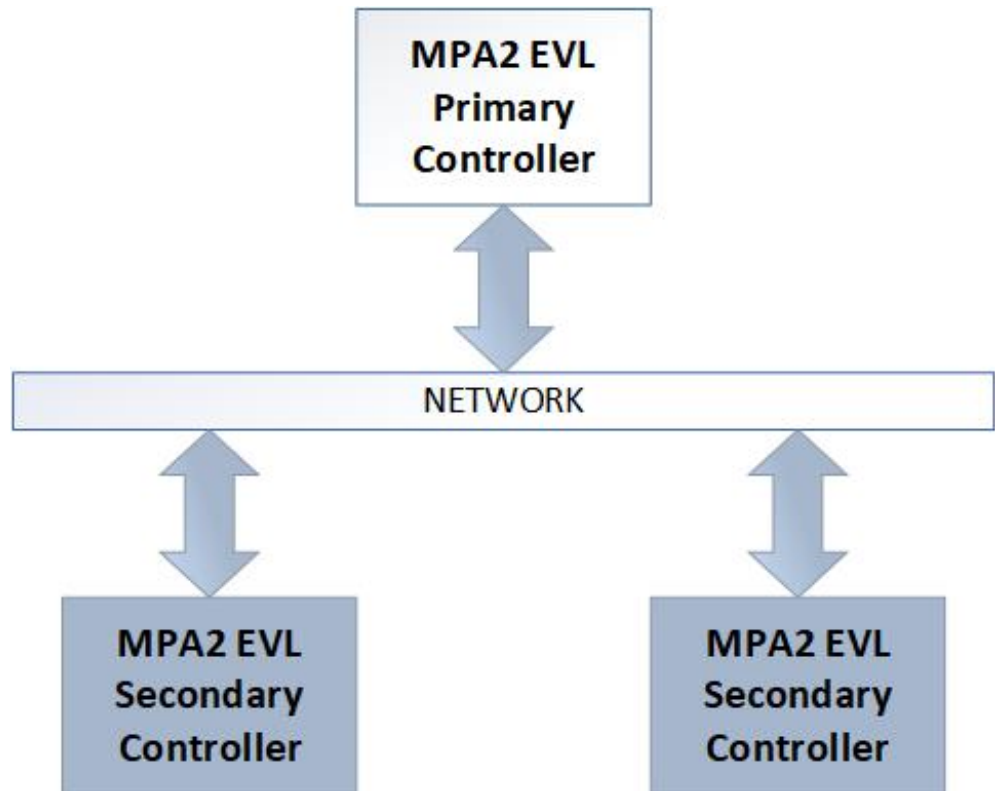
What is an EVL?

An Ethernet Virtual Loop (EVL) allows a group of IP network connected MPA2C3 controllers to be managed as a group, through an embedded Web Server residing on one of the controllers.

Up to 16 controllers may be grouped into an Ethernet Virtual Loop.

The grouping is known as a Virtual Loop since the administration paradigm is similar to an RS-485 loop.

Figure 2-1 EVL System Diagram



Network Requirements

The controllers **must** be connected to a common IP sub-network that provides dynamic address assignment through DHCP.

DIP Switch Settings (EVL Mode)

When a MPA2C3 panel is used in EVL mode, DIP (dual in-line package) SW1 Bit 5-Bit 9 are NOT used to identify the panel. The panel is identified by its MAC address

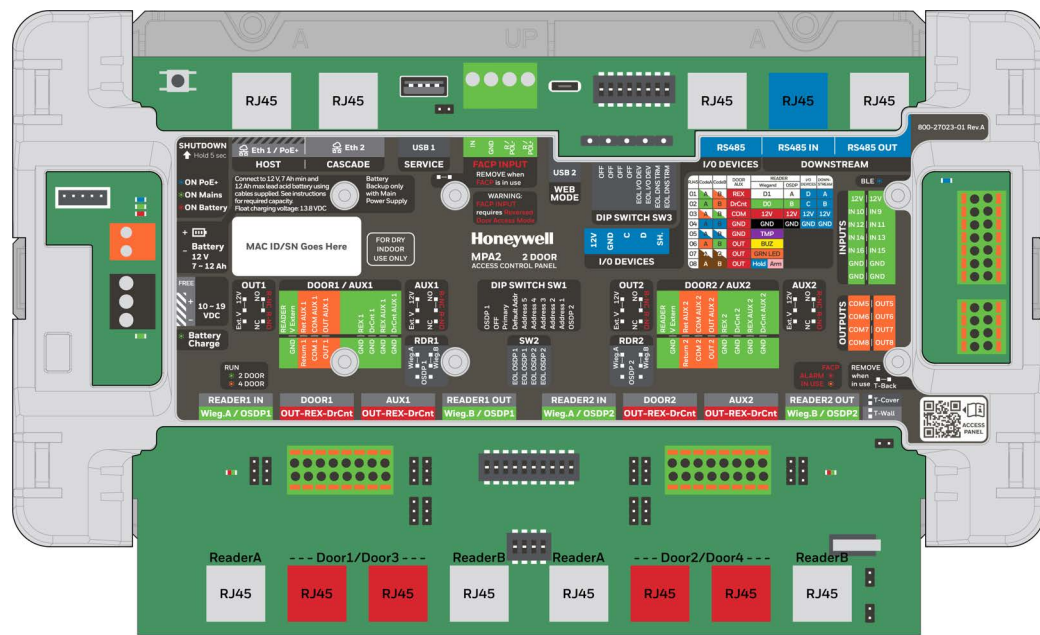
Tip: When setting up an EVL loop, create a list of MAC addresses for all Panels, and what doors they control. This will be useful later when the panels are configured. Example list below.

List of MPA2 EVL system									
Panel	Address	IP Address	MAC Address	Primary / Secondary	2/4 door	Door1	Door2	Door3	Door4
1	1	92.168.1.15	xx:xx:xx:xx:xx:xx	Master	2	Lobby	Office 1		
2	1	DHCP	yy:yy:yy:yy:yy:yy	Secondary	4	Warehouse	Corridor West	Corridor East	Office 2
3	1	DHCP	zz:zz:zz:zz:zz:zz	Secondary	2	Office 3	Back door		

DIP switches 5 through 9 should be set to factory defaults:

- DIP switches 5 through 8: OFF.
- DIP switch 9: ON.

One of the controllers must be set as the Primary controller by setting DIP Switch 3 to ON.



MPA2C3	RS485 Loop Mode							Panel Function
	DIP Switch SW1							
	Bit3	Address	Bit5	Bit6	Bit7	Bit8	Bit9	
Primary	ON	1	OFF	OFF	OFF	OFF	ON	Master
Secondary	OFF	2	OFF	OFF	OFF	ON	OFF	Downstream
		3	OFF	OFF	OFF	ON	ON	
		4	OFF	OFF	ON	OFF	OFF	
		5	OFF	OFF	ON	OFF	ON	
		6	OFF	OFF	ON	ON	OFF	
		7	OFF	OFF	ON	ON	ON	
		8	OFF	ON	OFF	OFF	OFF	
		9	OFF	ON	OFF	OFF	ON	
		10	OFF	ON	OFF	ON	OFF	
		11	OFF	ON	OFF	ON	ON	
		12	OFF	ON	ON	OFF	OFF	
		13	OFF	ON	ON	OFF	ON	
		14	OFF	ON	ON	ON	OFF	
		15	OFF	ON	ON	ON	ON	
		16	ON	OFF	OFF	OFF	OFF	
		17	ON	OFF	OFF	OFF	ON	
		18	ON	OFF	OFF	ON	OFF	
		19	ON	OFF	OFF	ON	ON	
		20	ON	OFF	ON	OFF	OFF	
		21	ON	OFF	ON	OFF	OFF	
		22	ON	OFF	ON	ON	OFF	
		23	ON	OFF	ON	ON	ON	
		24	ON	ON	OFF	OFF	OFF	
		25	ON	ON	OFF	OFF	ON	
		26	ON	ON	OFF	ON	OFF	
		27	ON	ON	OFF	ON	ON	
		28	ON	ON	ON	OFF	OFF	
		29	ON	ON	ON	OFF	ON	
		30	ON	ON	ON	ON	OFF	
		31	ON	ON	ON	ON	ON	

Creating an EVL

Configure other controllers as Secondary controllers by setting DIP switch 3 to OFF. and Creating an EVL

Connect all Controllers to a common IP network. The Secondary IP controllers must have DIP switch 3 set to OFF. and will be configured using the Primary controller.

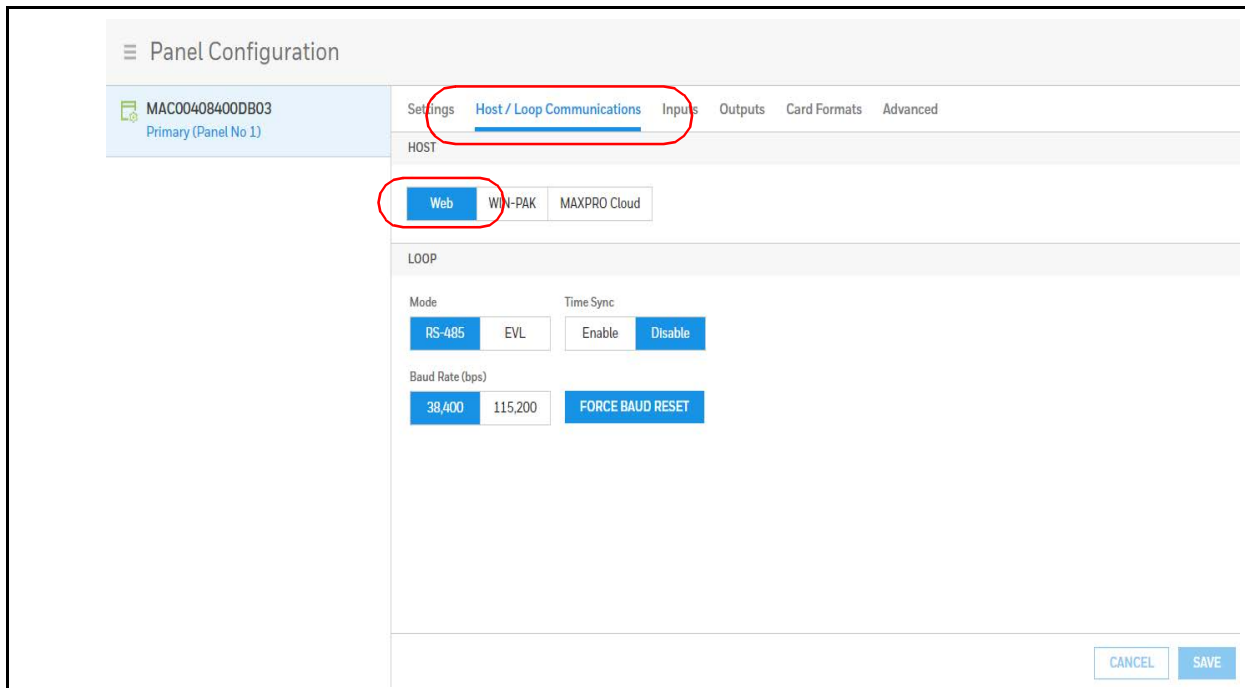
1. Log into MPA2C3 Primary panel from a browser through the USB2 -WEB MODE (<https://192.168.2.150>) or Ethernet connection Eth1 / PoE+ - HOST (<https://192.168.1.150> - SW1- Bit4 ON).

See [Setting Up the USB Connection](#) section on page 6 for instructions.

2. Navigate to Host/Loop Communications Screen:

- **Menu > Panel Configuration > Host/Loop Communications**, or
- Click on **Panels > Host/Loop Communications** on the Dashboard.

Figure 2-2 Selecting Host/Loop Communication Tab



1. Set up Communication attributes (see [figure 2-2](#)):
 - a. Select **Web** as Host Connection Type.
 - b. Select **Ethernet Virtual Loop** as Mode.
 - c. Click **Save**. The panel automatically reboots.
2. Log into the MPA2C3 panel.

See [Setting Up an Ethernet Port](#) section on page 8.

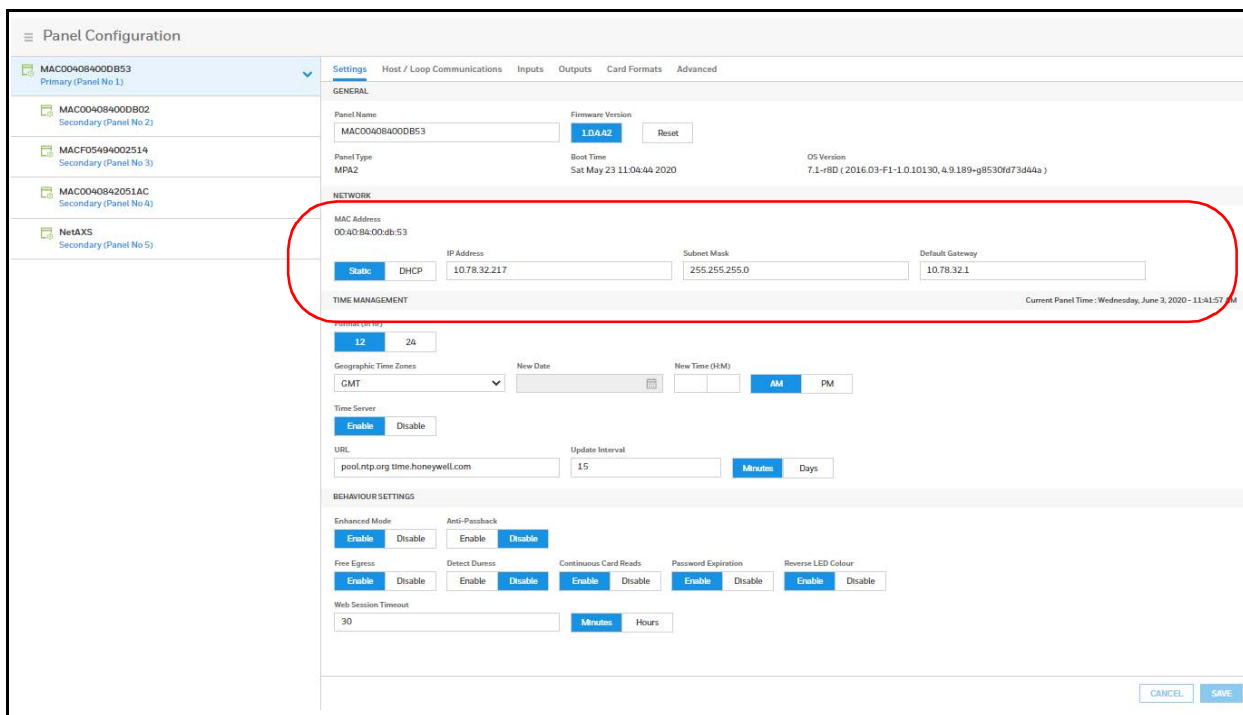
3. Set up Network Configuration (see [figure 2-3](#)):

- d. Navigate to the **Network** field on the **Settings** tab.
- e. Select **DHCP** or enter **Static IP** address assigned to Primary panel.
- f. Click **Save**. The panel automatically reboots.

Note: *It is recommended to set the Primary panel as a static IP address that is different than the default address (192.168.1.150) such as 192.168.1.100.*

The Primary panel must be set to the same subnet as the Secondary panels in order for the EVL to work properly (i.e., if DHCP server is assigning Secondary panels to 129.17.27.XXX, then Primary needs to also be set to 129.17.27.XXX).

Figure 2-3 Network Configuration for EVL



1. Log into the Primary controller from a browser.

See [Setting Up an Ethernet Port](#) section on page 8.

2. Register Secondary EVL controllers (see [figure 2-4](#)):

Note: *Only secondary panels can be Registered and Unregistered.*

- c. Navigate to the EVL tab: **Menu > Panel Configuration > Advanced > EVL Discovery**.

Figure 2-4 EVL Discovery Panel

Panel Configuration

BC033-0040840AB7CD
Primary (Panel No 1)
IP - 192.168.62.33
MAC - 00:40:84:0A:B7:CD

BC034-0040840AD434
Secondary (Panel No 2)
IP - 192.168.48.21
MAC - 00:40:84:0A:D4:34

BC031-0040840A0321
Secondary (Panel No 3)
IP - 192.168.48.77
MAC - 00:40:84:0A:03:21

Panels in the loop appear here.
Panel status is indicated by color: red = offline; green = online.

Settings Host / Loop Communications Inputs Outputs Card Formats **Advanced**

Site Codes REGISTERED & AVAILABLE DOWNSTREAM PANELS OTHER DISCOVERED GATEWAYS

Interlocks BC033-0040840AB7CD PRIMARY IP - 192.168.62.33 MAC - 00:40:84:0A:B7:CD 004084219457 PRIMARY IP - 192.168.48.52 MAC - 00:40:84:21:94:57

Security Certificate BC031-0040840A0321 SECONDARY UNREGISTER 00408421E19C PRIMARY IP - 192.168.48.15 MAC - 00:40:84:21:E1:9C

File Management BC034-0040840AD434 SECONDARY UNREGISTER ALLab1 PRIMARY IP - 192.168.48.61 MAC - 00:40:84:21:57:EA

Downstream Devices BC008-0040840A0366 REGISTER ALLab2 PRIMARY IP - 192.168.48.78 MAC - 00:40:84:20:2D:93

DB002-00408413858A REGISTER ALLabIO PRIMARY IP - 192.168.48.59

Discovered panels appear automatically.

- d. Click **REGISTER** to register a panel. The REGISTER buttons changes to UNREGISTER when the registration is successful.

Figure 2-5 Registered Secondary Controllers

Panel Configuration

BC033-0040840AB7CD
Primary (Panel No 1)
IP - 192.168.62.33
MAC - 00:40:84:0A:B7:CD

BC034-0040840AD434
Secondary (Panel No 2)
IP - 192.168.48.21
MAC - 00:40:84:0A:D4:34

BC031-0040840A0321
Secondary (Panel No 3)
IP - 192.168.48.77
MAC - 00:40:84:0A:03:21

Settings Host / Loop Communications Inputs Outputs Card Formats **Advanced**

Site Codes REGISTERED & AVAILABLE DOWNSTREAM PANELS OTHER DISCOVERED GATEWAYS

Interlocks BC033-0040840AB7CD PRIMARY IP - 192.168.62.33 MAC - 00:40:84:0A:B7:CD 004084219457 PRIMARY IP - 192.168.48.52 MAC - 00:40:84:21:94:57

Security Certificate BC031-0040840A0321 SECONDARY UNREGISTER 00408421E19C PRIMARY IP - 192.168.48.15 MAC - 00:40:84:21:E1:9C

File Management BC034-0040840AD434 SECONDARY UNREGISTER ALLab1 PRIMARY IP - 192.168.48.61 MAC - 00:40:84:21:57:EA

Downstream Devices BC008-0040840A0366 REGISTER ALLab2 PRIMARY IP - 192.168.48.78 MAC - 00:40:84:20:2D:93

DB002-00408413858A REGISTER ALLabIO PRIMARY IP - 192.168.48.59

You have now finished creating an Ethernet Virtual Loop.

Configuring the System Via RS-485 Loop

By default, the Loop Mode is set to RS-485. If it was set EVL and the user set it back to RS-485, the panel will automatically reboot. Panels in a RS-485 loop are wired together in daisy chain fashion Up to 31 controllers may be wired together in a RS-485 loop; that is one primary and up to 30 secondary controllers.

DIP Switch Settings (RS485 Mode)

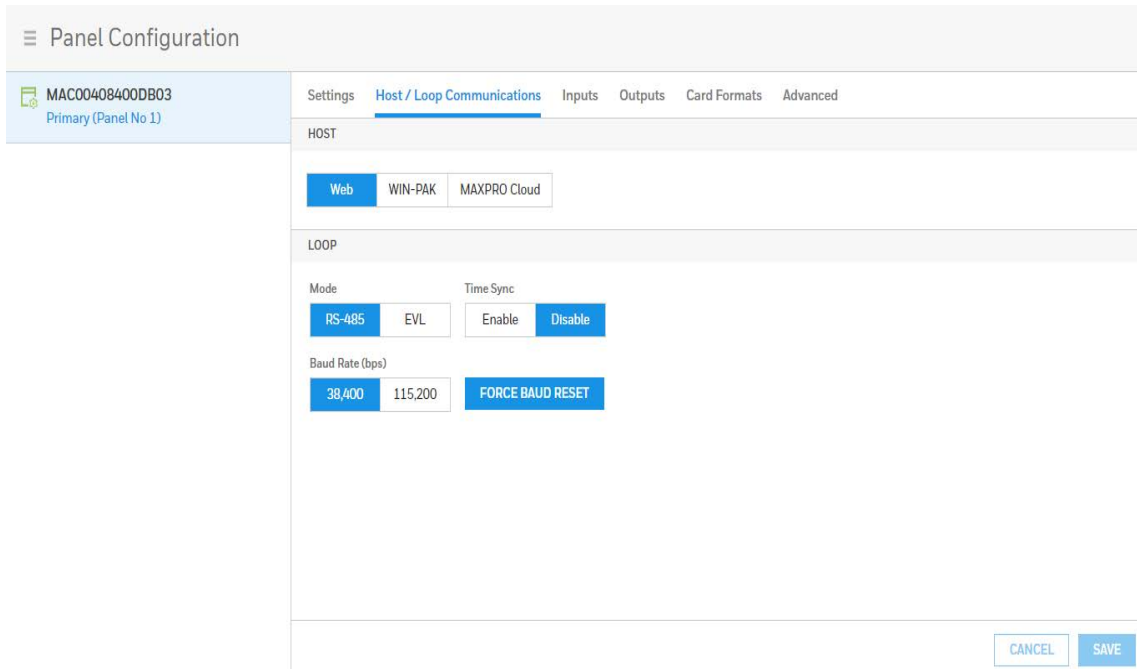
IMPORTANT: Only 1 Primary controller may be in a RS-485 loop. All of the Secondary controllers must have DIP SW1, Bit 3 set to the OFF position. The secondary controllers also need to be addressed with unique addresses by DIP SW1, Bit5 to Bit 9 in the correct positions in the below table.

DIP SW Settings Master Slave Mode RS485

1. Log into MPA2C3 Primary panel from a browser through Ethernet (Eth1 / PoE+ - HOST : default 192.168.1.150), or USB (USB2 - WEB MODE : 192.168.2.150).

See [Setting Up the USB Connection](#) on page 6. See [Setting Up an Ethernet Port](#) on page 8.

2. Navigate to Host/Loop Communications Screen:
 - Menu > Panel Configuration > Host/Loop Communications, or
 - Click on Panels > Host/Loop Communications on the Dashboard.



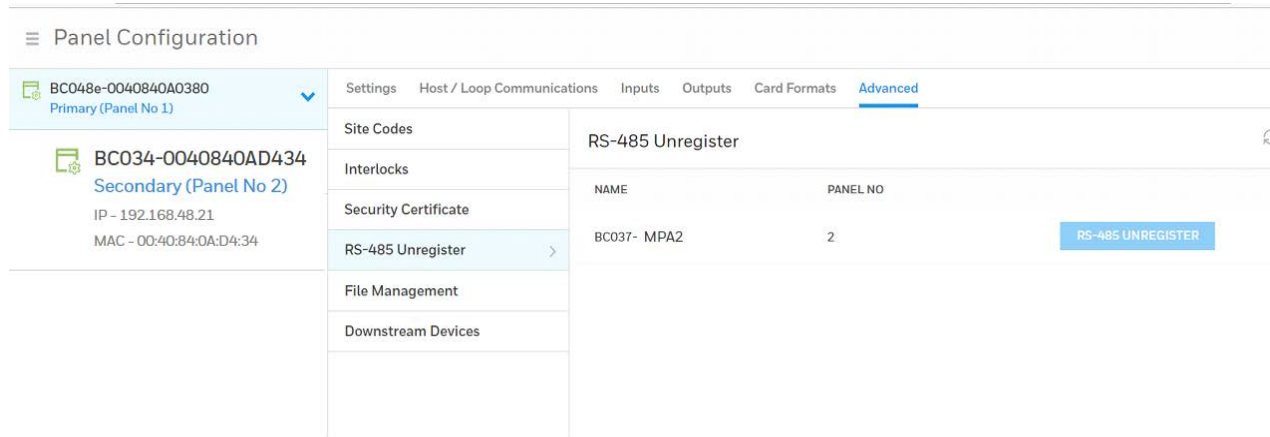
3. Set up Communication attributes
 - a. Select Web as Host Connection Type.
 - b. Select RS-485 as Mode.
 - c. Click Save. The panel automatically reboots.
4. Log into the MPA2C3 panel.

RS-485 Unregister

RS-485 Unregister page will list all of the secondary panels that are physically wired together in a RS-485 communication loop.

Note: Note RS-485 Unregister feature is only available on the primary panel of the RS-485 loop.

Navigate to the RS-485 Unregister tab: Menu > Panel Configuration > Advanced > RS-485 Unregister.



If a secondary panel is offline, it will display as red in the status list. None of its devices (readers, inputs, outputs, etc.) will be accessible until the panel comes back online. Once the panel is back online, its status will change to green and its devices will be accessible.

If the user want to remove the offline secondary panel from the list, the user can unregister it, which will remove it from the panel status list.

Note: Only secondary panels can be Unregistered.

The RS-485 Unregister button does not become available until the panel goes offline. While the panel is online, the button is grayed out, unavailable.

Managing Configuration Data

Configuration data is managed on a system of panels interconnected in a loop.

Configuration data is either common (shared and stored on all online panels when the data is entered) or panel specific (unique to each panel).

Common data includes:

- Schedules
- Cards
- Card Formats

- Holidays
- Access Group Name (access group details are panel-specific)
- Configuration (Site Codes)

Panel-specific data includes:

- Access Group Schedule Reader Assignments
- Space/Door/Reader Configuration
- Panel Configuration (General)
- Panel Configuration (Firmware Version)
- Panel Configuration (Network) (IP addresses apply only to primary panel)
- Panel Configuration (Host/Loop Communications) (applies only to primary panel)
- Panel Configuration (FACP input)
- Web Users (applies only to primary panel)

Configuring Host/Loop Communications

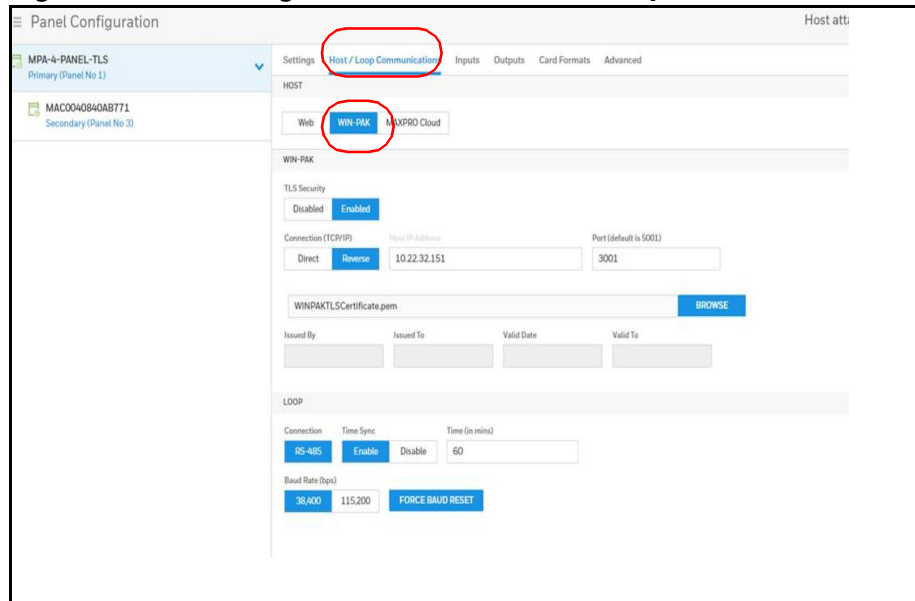
To maintain your MPA2C3 system configuration or to monitor its status, you must connect to the panel using one of three modes:

- **Host mode** (monitor only) – a host software system, such as WIN-PAK™ or MAXPRO Cloud, connects to the panel (through the primary panel, which has an on-board PCI communications adapter). It enables you to monitor the system status.
- **Web mode** (configure and monitor) – the web server connects to the panel and enables you to configure the panel and monitor system status.

Setting Communication Parameters for WIN-PAK

1. Navigate to Host/Loop Communications:
 - **Dashboard > Panels > Host/Loop Communications**, or
 - **Menu > Panel Configuration > Host/Loop Communications**.
2. Click to select **WIN-PAK**.

Figure 2-6 Selecting WIN-PAK on the Host/Loop Communications Tab



3. Configure the following host settings:

Table 2-2 WIN-PAK Host/Loop Communications Mode Settings

Host/Loop	Setting	Description
Host	Connection Type	<p>Specifies the type of physical connection between the host and the Primary panel.</p> <p>If you are connecting from a host software system such as WIN-PAK, select one of the following two connection options:</p> <p>Direct via TCP/IP – Host initiates connection to panel.</p> <p>Reverse TCP/IP – Panel connects directly to the host system using the TCP/IP protocol. You must enter the host IP address in the Host IP Address field. Panel initiates connection to host.</p>
	Host IP Address	Enter the host system (or WIN-PAK server) IP address here if you selected Reverse TCP/IP in the Connection Type field on this screen.
	Port Number	Specifies the port number for the Ethernet port. Port 2101 is Encrypted (default). Port 3001 is Direct TCIP/IP. Reverse TCP/IP port starts at Port 5001 and must be unique in a WIN-PAK system for each primary panel.
	TLS Security	<p>By default enabled to establish TLS encrypted communication between MPA2C3 Primary / Gateway panel and WIN-PAK Host.</p> <p>TLS encryption is available from WIN-PAK 4.9 and higher. After enabling the TLS Security a TLS certificate must be uploaded to the panel. To create the TLS certificate file, browse on the WIN-PAK Server to C:\Program Files (x86)\WINPAKPRO\Honeywell.Winpak.SSLConfigUtility.exe.</p> <p>In the WIN-PAK SSL Configuration Utility dialog box, select Create Self-Signed WIN-PAK Certificate. For more information refer to the WIN-PAK User guide.</p> <p>Disabling encryption creates a vulnerable system for IT attacks and is not recommended.</p>
	TLS File upload	Click Browse select the desired TLS certificate and then click Save and upload the TLS certificate to the panel.

Table 2-2 WIN-PAK Host/Loop Communications Mode Settings

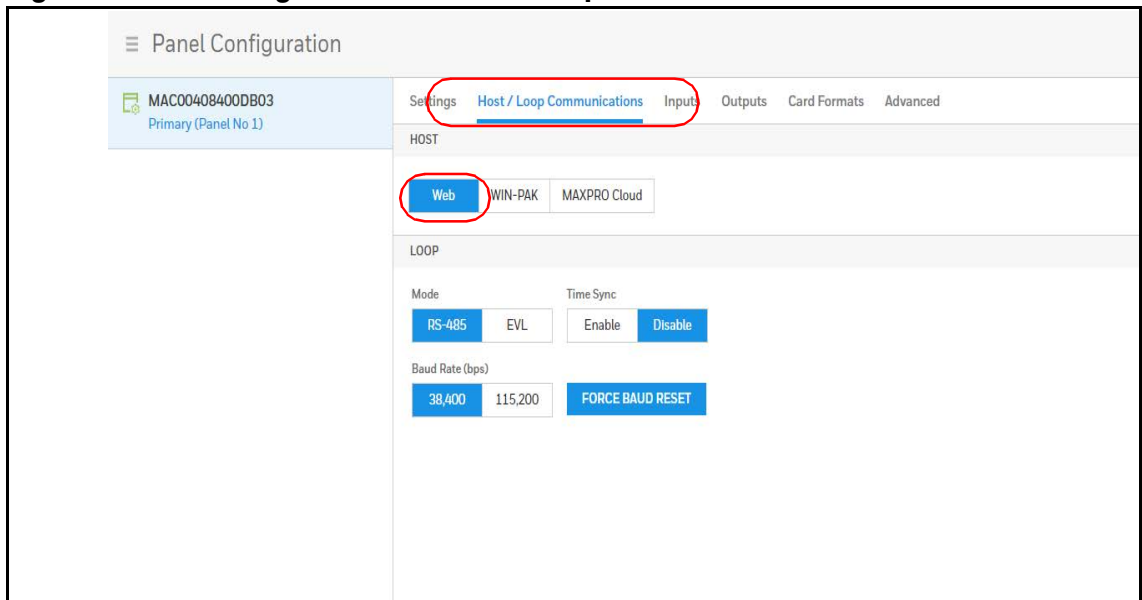
Host/Loop	Setting	Description
Loop	Connection Type	RS-485 -If Primary provides access to RS-485 Loop, to downstream secondary panels .
	Time Sync	Synchronizes the primary’s time with the secondary panels. Enabled – Time-synchronizes the loop by automatically broadcasting the primary’s time to secondary panels. Select from 60-32767 minutes.
	Baud Rate	Specifies the transmission rate (bits per second) among the secondary panels on the loop. Force Baud Reset – Tells all secondary panels to change to the selected loop baud rate. This saves the user from having to go to each panel individually.

4. Click **Save**.

Setting the Communication Mode to Web

- Navigate to Host/Loop Communications:
 - Dashboard > Panels > Host/Loop Communications**, or
 - Menu > Panel Configuration > Host/Loop Communications**.
- Click to select **Web**.

Figure 2-7 Selecting WEB on the Host/Loop Communications Tab



3. Configure the host settings.

Table 2-3 Web Host Communication Mode Settings

Host	Setting	Description
	Mode	RS-485 - If Primary provides access to RS-485 Loop. EVL - If Primary provides access to Ethernet Virtual Loop.
	Time Sync	Synchronizes the primary's time with the secondary panels. Enabled – Time-synchronizes the loop by automatically broadcasting the primary's time to secondary panels. Select from 60-32767 minutes.
	Baud Rate	Specifies the transmission rate (bits per second) among the secondary panels on the loop. Force Baud Reset – Tells all secondary panels to change to the selected loop baud rate. This saves the user from having to go to each panel individually.

4. Click **Save**.

Note: When switching from EVL back to RS-485 mode, all EVL Secondary (DS) controllers are automatically unregistered from the primary so that they may be used again as RS-485 DS controllers.

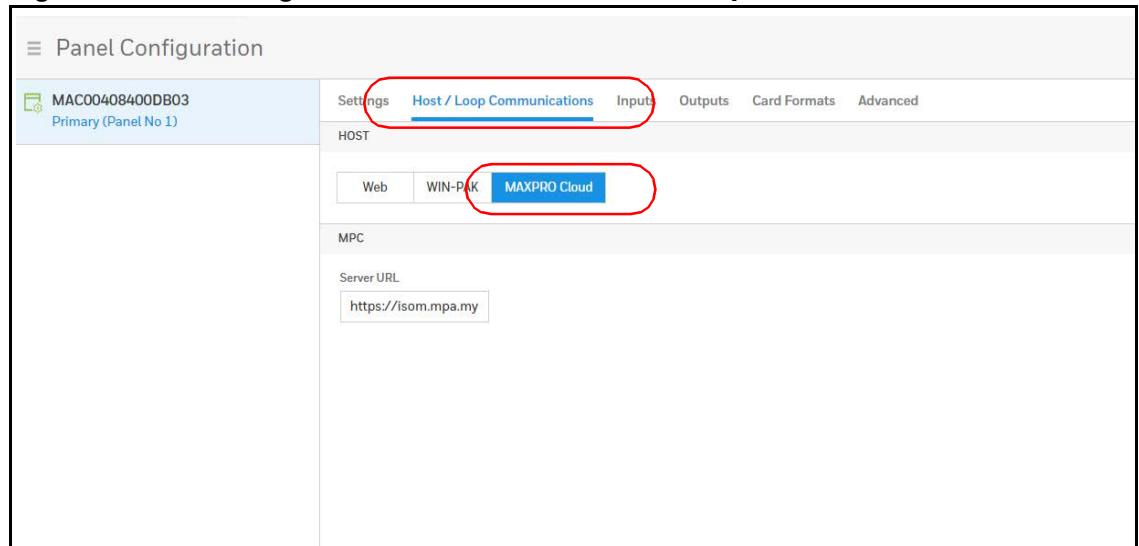
Note: When switching from EVL to RS-485 mode, if the EVL primary can not communicate with the DS controller, then the DS controller remains an EVL controller until it is set back to factory defaults.

Note: Switching to RS-485 mode causes deregistration of EVL Secondary controllers from the primary. Suggestion: Save the configuration database if you might later switch back to EVL mode.

Configuring for MAXPRO Cloud

1. Navigate to **Host/Loop Communications**:
 - **Dashboard > Panels > Host/Loop Communications**, or
 - **Menu > Panel Configuration > Host/Loop Communications**.
2. Click to select **MAXPRO Cloud**.

Figure 2-8 Selecting MAXPRO Cloud on the Host/Loop Communications Tab



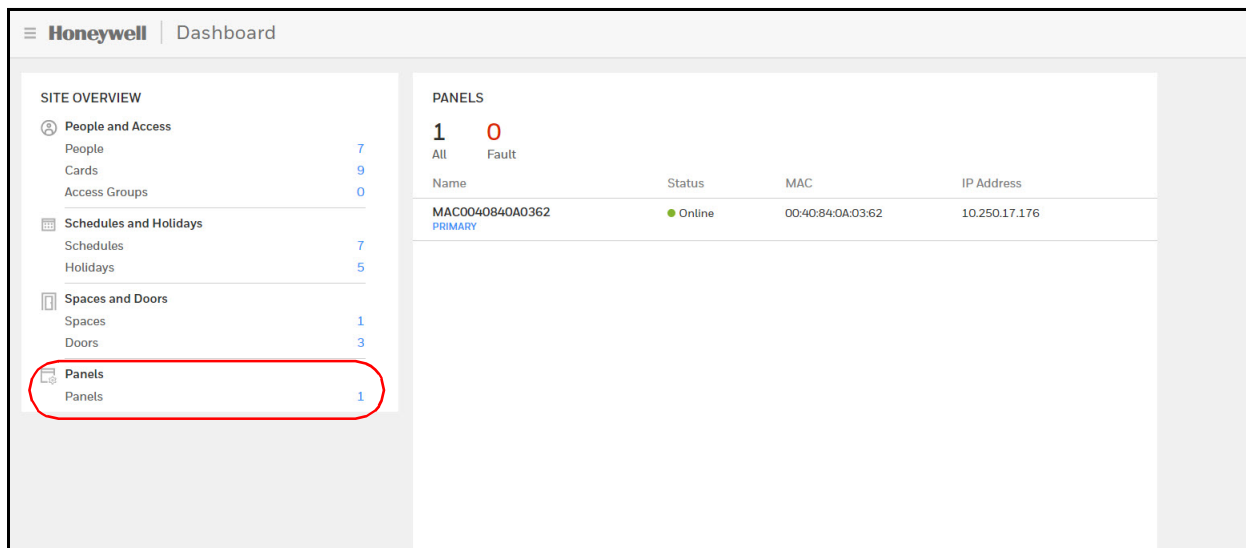
3. Enter the **Server URL**.
4. Click **Save**.

Initial Panel Setup

You can access **Panel** configuration in two ways:

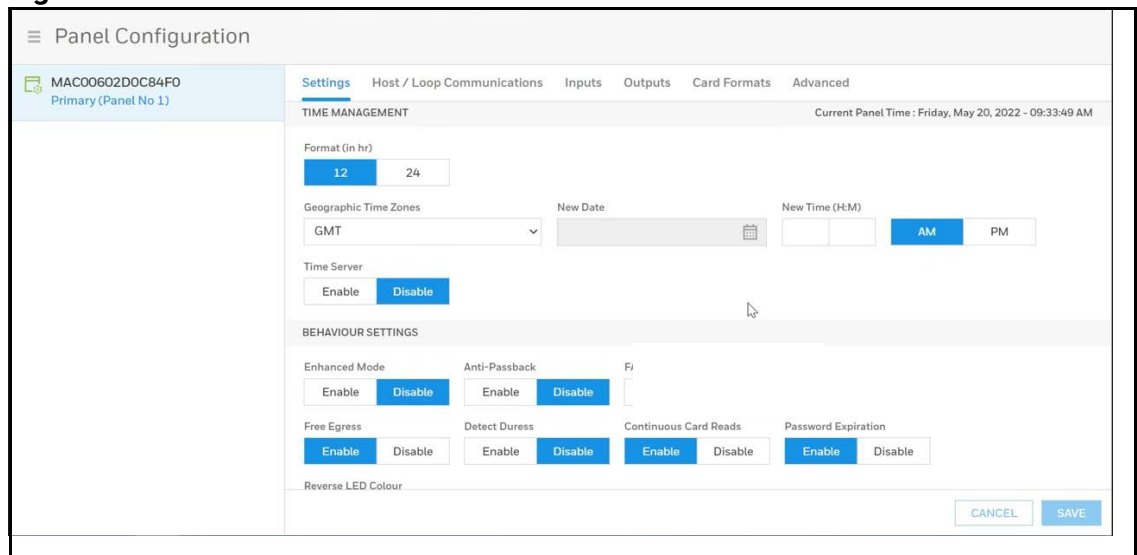
- Click Panels in the Dashboard to access the **Panels** interface, or

Figure 2-9 Navigating to the Panels Interface



- Click Panel Configuration in the Menu.

Figure 2-10 Panels Interface

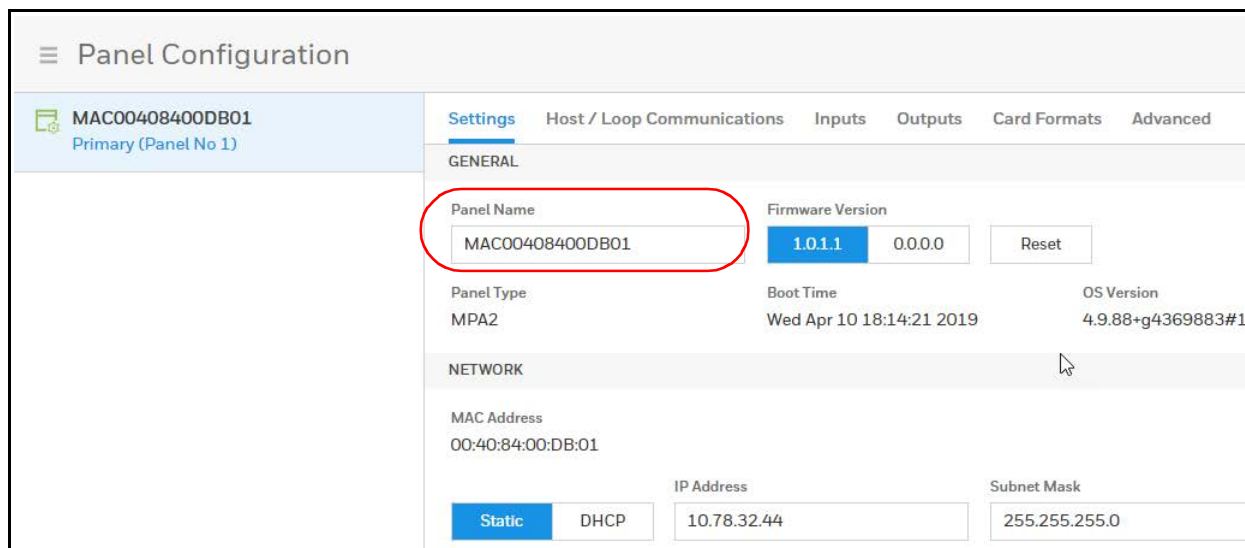


Entering a Panel Name

Note: Panels can be configured only if the Host Communications is set to **Web**.

1. Navigate to the **Settings** panel:
 - **Dashboard > Panels > Settings**, or
 - **Menu > Panel Configuration > Settings**

Figure 2-11 Settings Panel



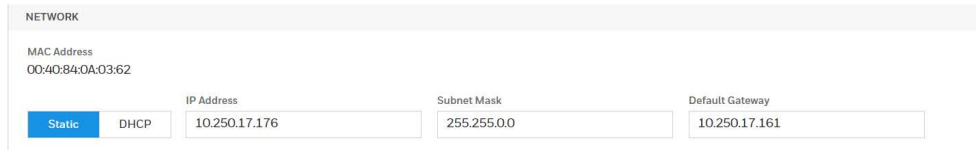
2. Click the **Panel Name** field, and then enter a panel name.
3. Click **Save**.

Configuring the Network Settings

In the Panel Configuration page, you can configure the following network-related settings:

- View the panels MAC Address
- Set network settings to Static or DHCP
- Configure the IP address of the panel
- Configure the Subnet Mask
- Configure the Default Gateway

Scroll down to the Network section.



Note: Only the primary panel will display network information.

The General section allows the user to:

- Configure the panel's name
- View the active and inactive firmware version
- Toggle the firmware version set
- Reset the panel
- View the panel type
- View the last boot time of the panel

Other fields in the Panel Configuration > Settings > General section are Firmware Version, Reset, Panel Type, and Boot Time.

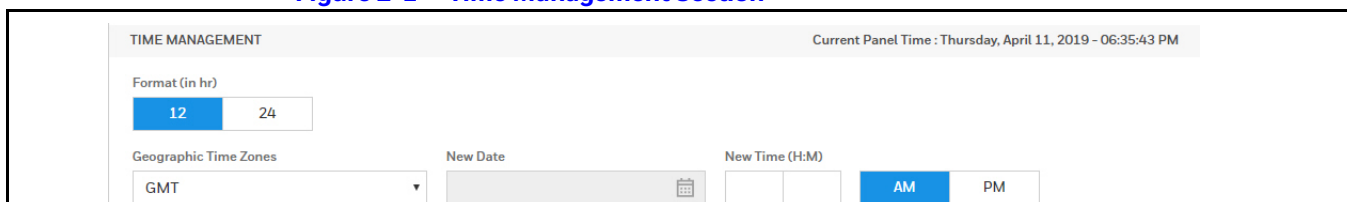
Configuring Time Management

In the **Panel Configuration** page, you can configure the following time-related settings:

- Set the current time.

Scroll down to the **Time Management** section.

Figure 2-1 Time Management Section



Configuring the Current Panel Time

Between the Settings tab and the Host/Loop Communications tab, you can configure the following for the current panel time:

Settings Tab

- Specify the time format (12 hour/24 hour).
- Set a new date.
- Set a new time.
- Set the geographic time zone.
- Enable a time server, and then specify the IP address of the time server being used.
- Specify the update interval.
- Force a time synchronization between the panel and the time server.

Host/Loop Communications Tab

- Synchronizes the primary panel's time with the secondary panels.
- In the Behavior Settings section of Panel Configuration, you can enable/disable the following:
- nted at an OUT reader must then be presented at an IN reader.

Configuring Behavior Settings

BEHAVIOUR SETTINGS

Enhanced Mode:

Anti-Passback:

Free Egress:

Detect Duress:

Continuous Card Reads:

Password Expiration:

Reverse LED Colour

- **Enhanced Mode:** When enabled, it tracks whether the card holder has actually entered/used the door after presenting the card at IN/OUT sequence. If the card holder did not use the door after presenting then in Alarms and Events page, "Card Found Door Not Used" and "Card Found Door Used" events are generated accordingly. If the user opens the door initially then "Card Found Door Used" events are generated accordingly. If the user opens the door intentionally then "Card Found Door Used" event is reported in Alarms page for all the valid cards.

- Anti -Passback-When enabled, a valid card is required for entry and exit. The card holder must use the card in the proper IN/OUT sequence—that is, a card presented at an IN reader must then be presented at an OUT reader, or vice versa.
- Free Egress—Configures the panel for free egress. When enabled (Default), the panel automatically configures inputs REX1-4 to act as egress inputs for Doors 1 to 4, respectively. If disabled, those inputs REX1-4 can be used as general inputs.
- A duress PIN is the PIN a user enters at a keypad when being forced (for example, during a robbery) to open a door. The card holder enters a PIN that is either one number higher or lower than the correct PIN. This PIN opens the door, but it also triggers the designated duress output and produces an alarm event.
- For example, if the PIN is 2222, entering either 2221 or 2223 opens the door, but triggers a duress pulse and generates an alarm. In this way, the card holder notifies others without detection by the unauthorized person.

Note: A PIN ending in 0 (for example, 2320) will only trip a duress output when a 1 is used in place of the 0 (for example, 2321).

Note: The duress output feature requires the following configurations:

Note: Duress must be enabled on the Panel Configuration > Settings > Behaviour Settings tab. See figure 2-10 on page 30.

Note: A schedule/schedule must be selected for Card and PIN in the Doors configuration.

- Continuous Card Reads – Enables continuous card reading while the output is being energized. t caused by the previous card read. This parameter is set to Enabled by default.
- Password Expiration – When enabled, password expiration will be based on the last time a user’s password was updated. The password is good for 180 days. When disabled, the system does not check for password expiration. This is not recommended. Enabled by default. After 180 days when a user logs in, then the system will prompt you to change the password.
- Reverse LED Color – Identifies the color of a reader LED when a grant is authorized. When this parameter is enabled, the LED should be solid red and then turn green after two seconds (by default). Enabled by default. Web Session Timeout– Activates a web session timeout after the specified time period has elapsed. Define the time period either in minutes or in hours. Enter the number in the box, then select either minutes (3-59) or hours (1-12).

Configuring Schedules

The MPA2C3 panel controls access by using schedules, or time schedules. Inputs, outputs, groups, readers, access groups, and cards through access groups are all configured with schedules by which they will be energized or de-energized, enabled or disabled.

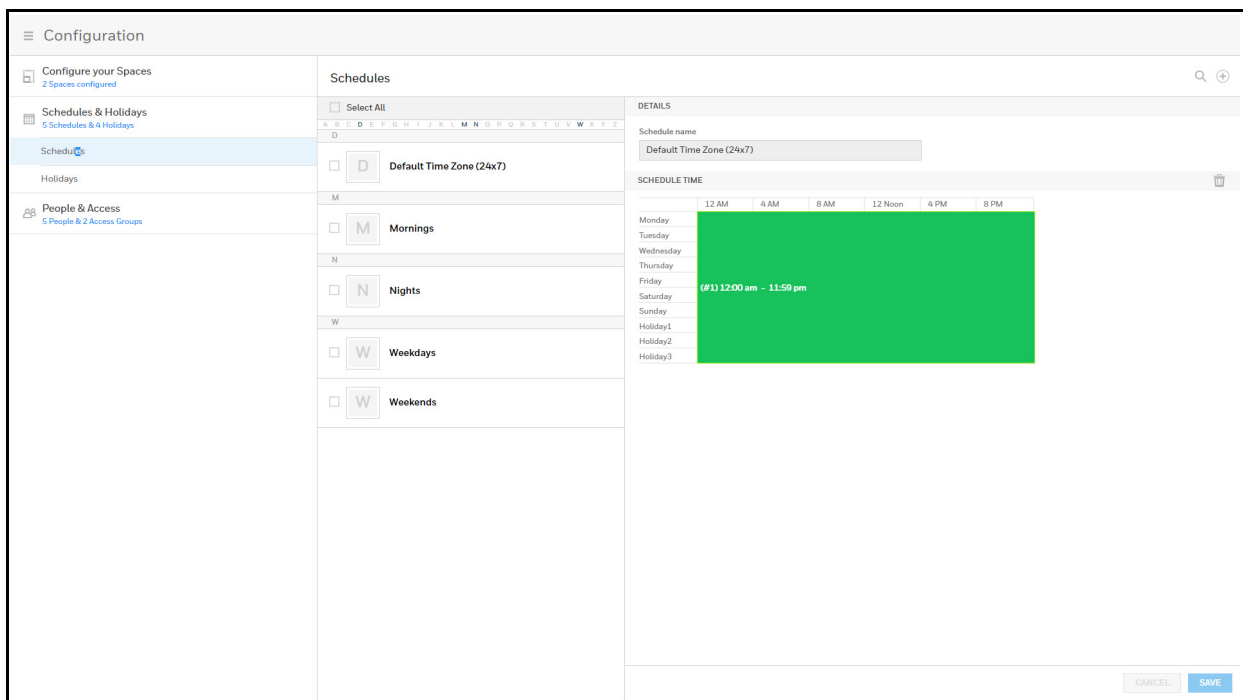
For example, you might assign a group of outputs to be energized from 12:00 AM to 6:00 AM, every day. The 12:00 AM to 6:00 AM, Sunday through Saturday, time period is called a schedule.

The Schedules configuration interface enables you to:

- Create schedules by which the panel controls the operation of the inputs, outputs, groups, readers, access groups, and cards through access groups.
- Modify a schedule.
- Delete a schedule.
- Define the holiday schedule.

Click **Configuration > Schedules & Holidays > Schedules** to display the Schedules interface:

Figure 2-12 Time Management - Schedules



Creating a schedule


1. Click **+** in the Schedules interface to add a new schedule.
2. Enter a schedule name.
3. Click and drag to define the parameters of the schedule, including days of the week and hours.
4. Click **Save**.

Modifying a Schedule

1. In the **Schedules** alphabetical list, click the letter that begins the name for the schedule, and then click to select the name.
2. Click to select the desired schedule.
3. Click to select the rectangle that defines the schedule.
4. Drag to change the shape, and therefore the days and the time of the schedule.
5. Click **Save** to accept the changes.

Deleting a Schedule

Caution: Do not delete a schedule that is currently in use.

1. Click to select the schedule. A delete icon appears .
1. Click the delete icon. A Delete Confirmation message appears.
1. Click **OK**. A Successfully Deleted message appears to indicate the deletion was successful.

Configuring Holidays

Holidays are special days of a week. They are similar, but override standard weekdays. If a day programmed as a Holiday occurs in the panel, the panel treats that day as the Holiday type, regardless of the actual day of the week (Monday-Sunday).

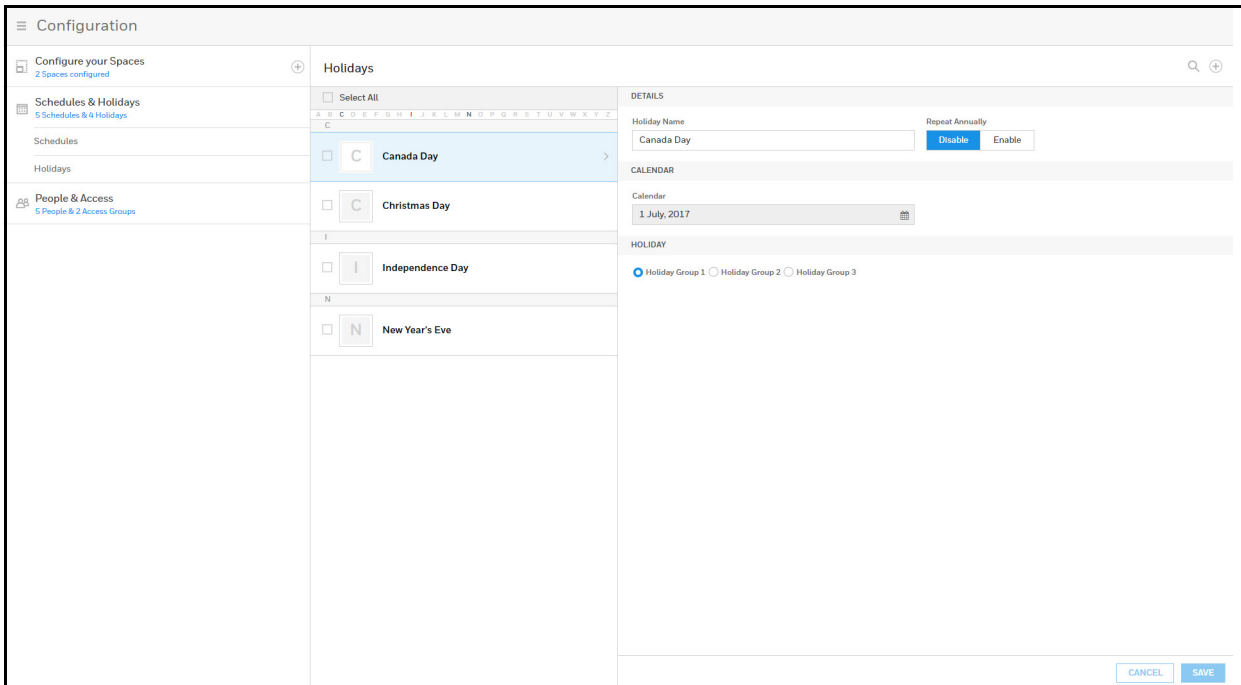
During this Holiday, only Schedules that contain that specific Holiday type work. The Holidays window enables you to further customize how the panel works. For example, you can block access to a building on that day, or grant special access during that day.

In the Holidays configuration window, you can:


- Create a holiday
- Modify a holiday
- Delete a holiday

Click **Configuration > Schedules & Holidays > Holidays** to display the Holidays window:

Figure 2-13 Holidays Window



Creating a Holiday

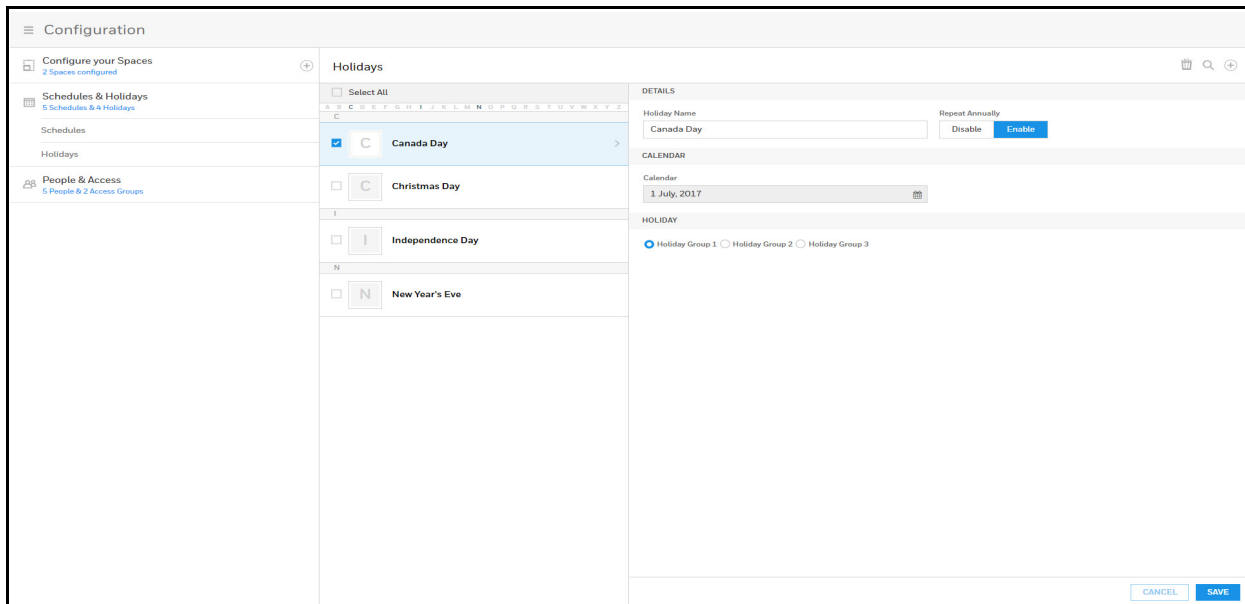
1. Click  in the **Holidays** window to add a new holiday.
2. Enter a new **Holiday Name**.
3. Click to enable/disable annual repetition.
4. Click the calendar icon, then select a day on the calendar.
5. Click to assign the new holiday to a **Holiday Group**. There are 3 holiday groups.
6. Assigning a holiday to a Holiday Group maps that holiday to a schedule configuration. The holiday then follows the rules of that schedule. (See [Configuring Schedules](#) section on page 45).
7. Click **Save**. A message appears to confirm that the new holiday was saved.

Note: Each Holiday added is considered a full day, extending from midnight to midnight.

Modifying a Holiday

1. Click to select the holiday in the Holidays list.

Figure 2-14 Modifying a Holiday

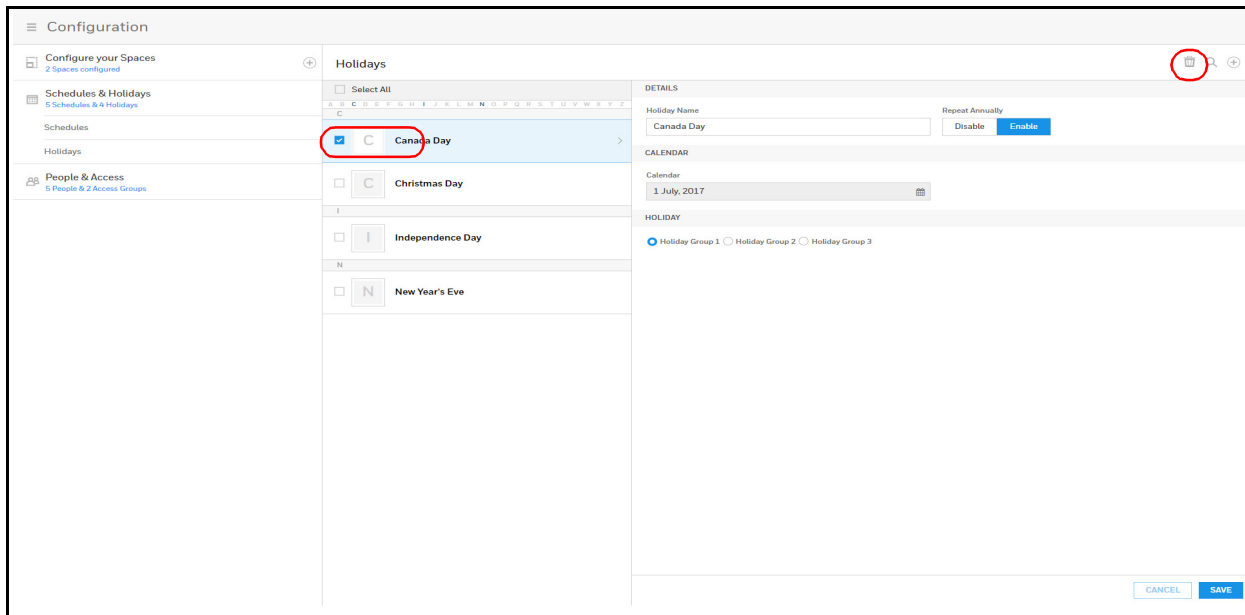



2. Modify the holiday.
3. Click **Save**. A message appears to confirm that the changes were saved.

Deleting a Holiday

1. Click to select the holiday.

Figure 2-15 Deleting a Holiday



A delete icon appears .

2. Click the delete icon. A Delete Confirmation message appears.
3. Click **OK**. A Successfully Deleted message appears to indicate the deletion was successful.

Configuring Spaces

Before you can configure doors, you must assign doors to a space.

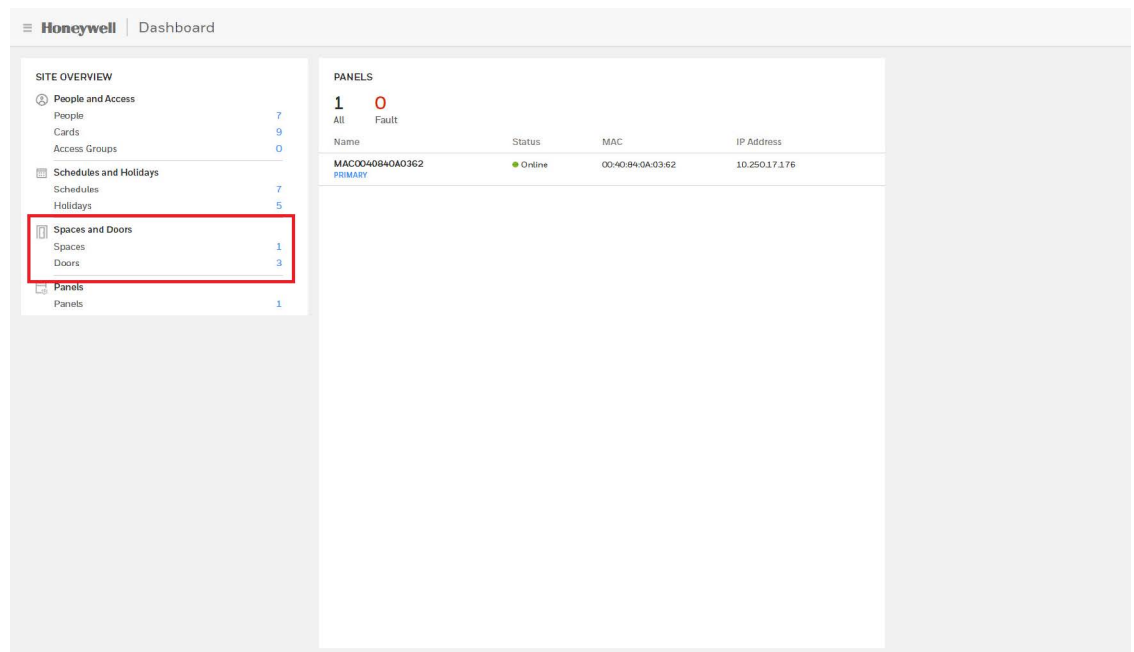
Examples for a space are "Ground Floor", "Lobby" or "West Wing"

1. Navigating to the **Spaces** interface.
 - Click **Spaces** in the **Dashboard** to access the Spaces interface.

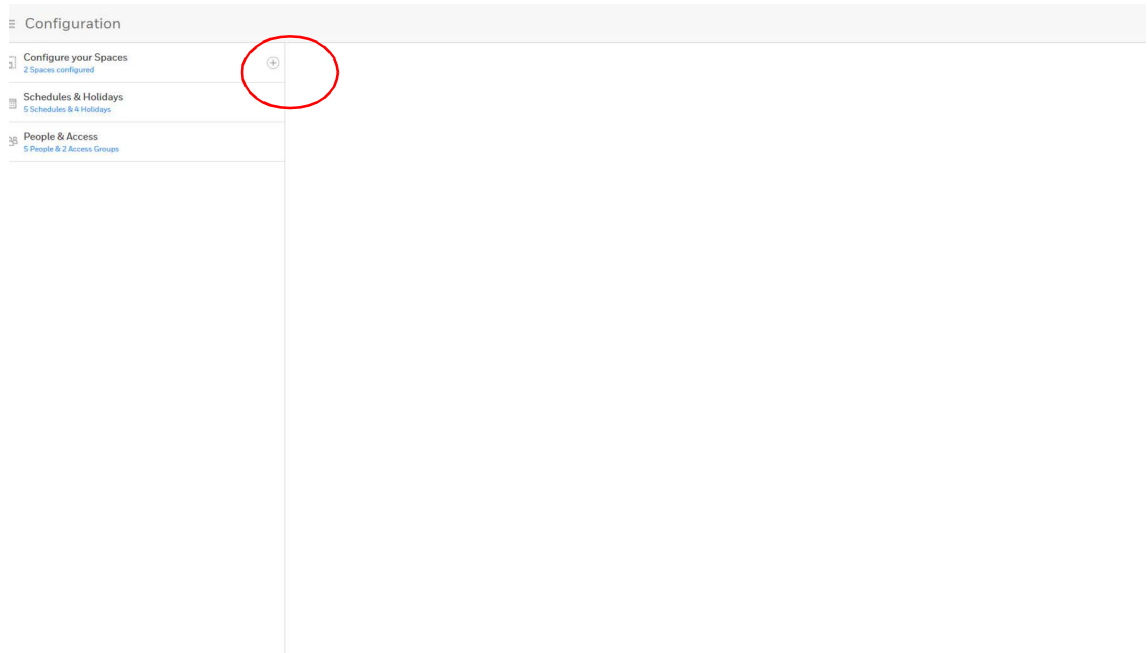
Figure 2-16 Navigating to the Spaces Interface

- Or click **Configuration** in the **Menu**.
2. Click to create a new space.

Figure 2-17 Creating a New Space



The **ASSIGN DOORS TO SPACE** window opens.



Note: If all of your doors are already assigned to space, then you receive a message explaining that *You don't have any doors available*. Therefore, you cannot create a new space.

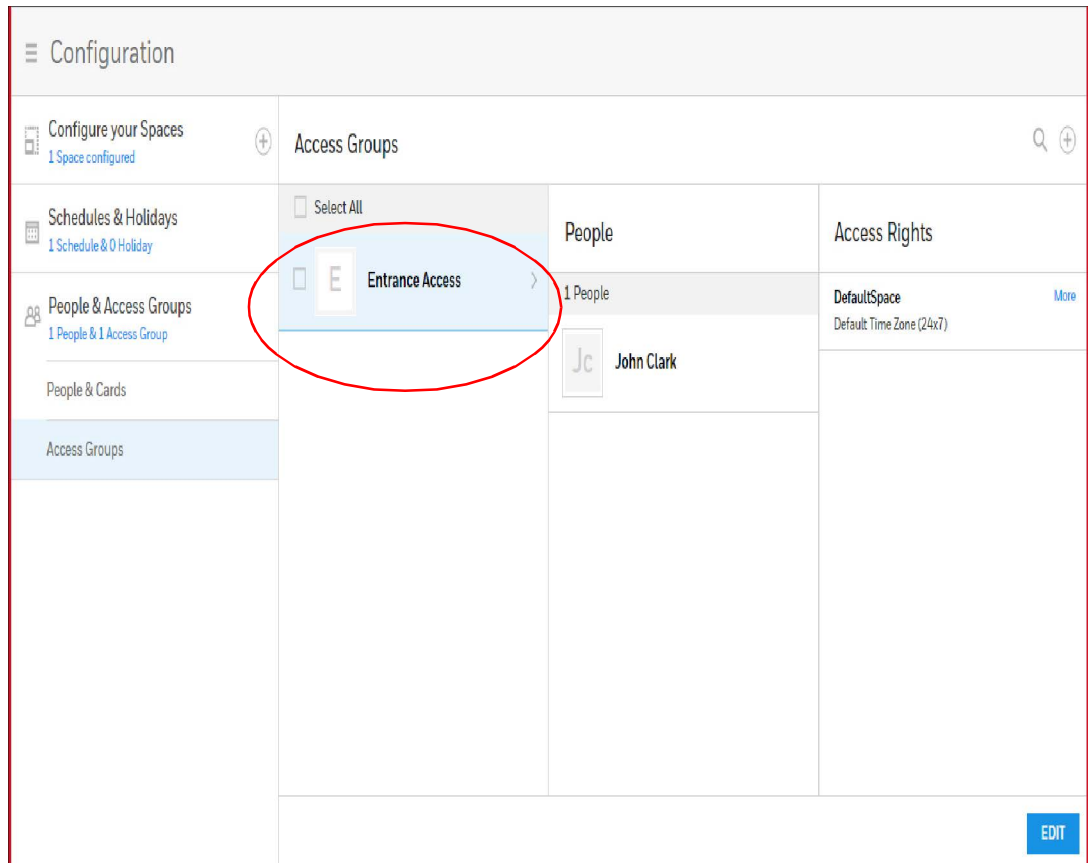
3. Figure 2-19 ASSIGN DOORS TO A SPACE window
4. Enter a space name in the **Name your Space** field.
5. Click in the **AVAILABLE DOORS** pane to select the door. The door appears in the **ADDED DOORS** pane.
6. Click **Save**. A message appears confirming the new Space.

Note: You cannot delete a door that is assigned to an access group. You must first remove that door from the access group.

Removing a Door from an Access Group

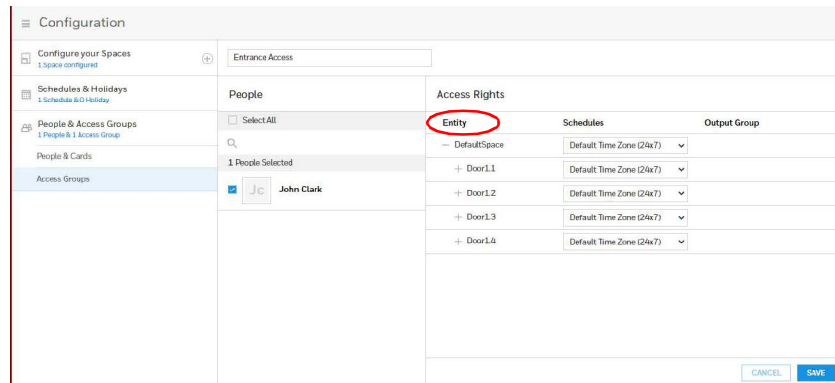
1. Click **People & Access > Access Group > Access**.

Figure 2-18 Figure 2-20 Access Groups Interface



2. Click to select an **Access Group**, then click **EDIT**.

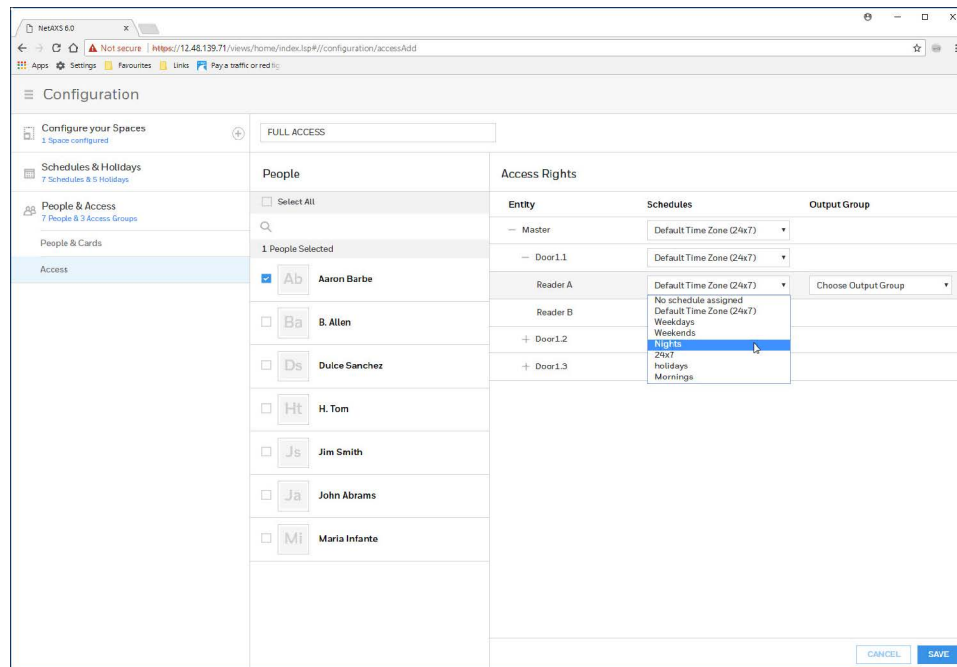
Figure 2-19 Figure 2-21 Editing an Access Group



3. Click + under **Entity** to expand a space and reveal the doors that belong to that space.

4. Click to select a door, then select **No schedule assigned** from the **Schedules**.

Figure 2-20



5. Click Save

Configuring Doors

Each panel supports from 1-4 doors depending on the license applied on the panel. For each door, you must configure the readers, inputs, and outputs. MPA2C3 supports:

- 2 Door Controller: Each door can be controlled by 2 Wiegand readers (Reader A: IN / READER B: OUT) or by 2 OSDP readers (IN and OUT).Door Controller
- 4 Door Controller: Each door can be controlled by 1 Wiegand reader (Reader A: IN) or by 2 OSDP readers (IN and OUT)

Note: You must assign doors to a Space before you can configure the doors. See [Configuring Spaces on pageXXXXX](#)

Accessing the Doors Configurations

1. Navigate to the **Configure your Spaces** tab by doing one of the following:
 - Click **Menu > Configuration**, or
 - Click **Spaces** in the **Dashboard**.

Figure 2-21 Configure your Spaces Tab

- Click **Configure your Spaces** to expand the configured spaces, then click a **Space** to open it, then click on a door in that space to select it.

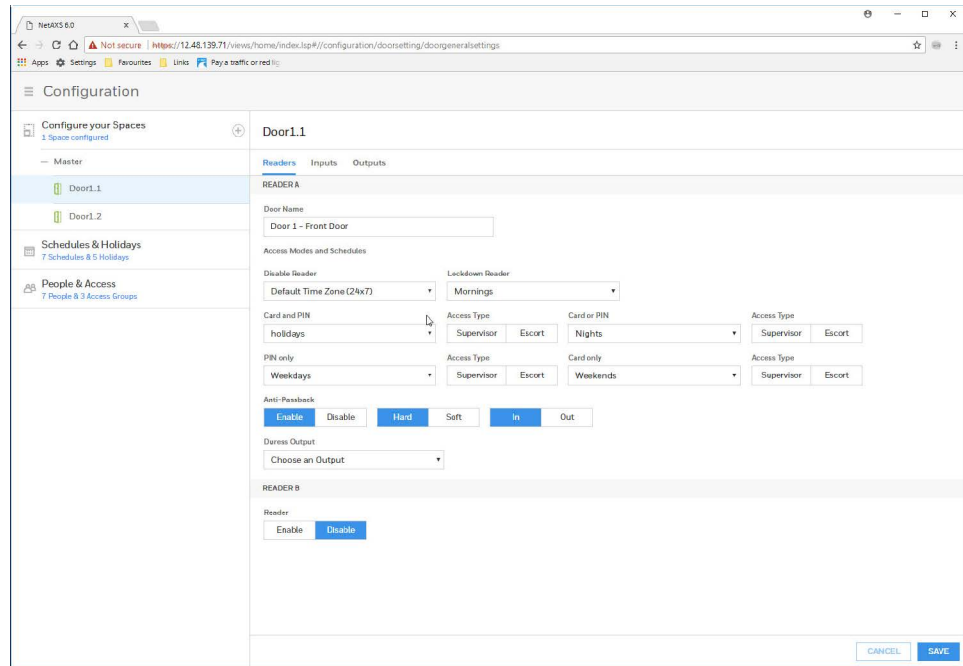


Figure 2-22 Door Configuration - OSDP Mode Enabled

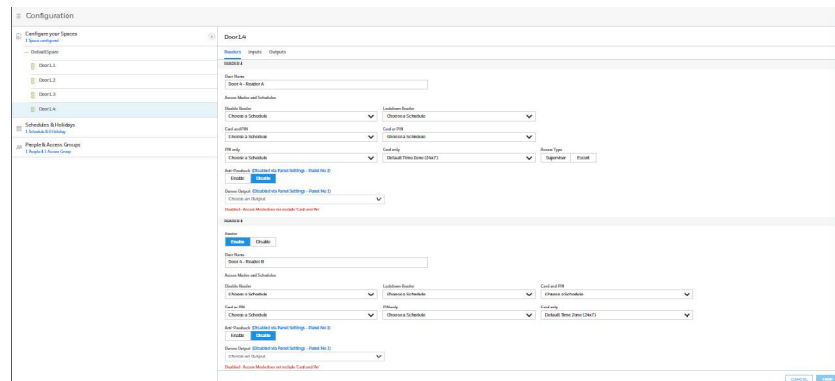
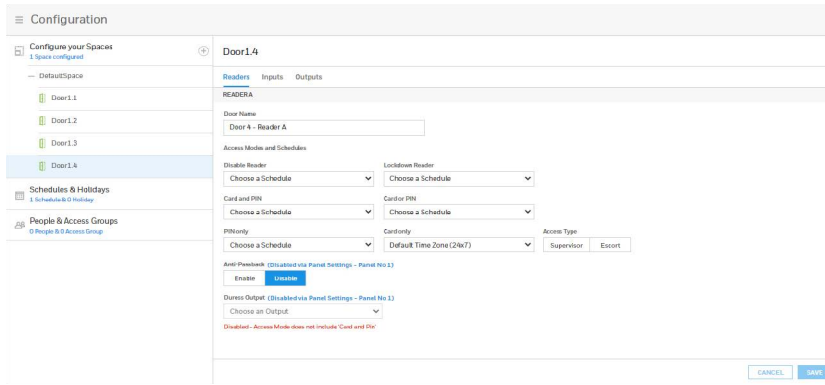


Figure 2-23 Door Configuration - Wiegand Mode Enabled



Configuring Door Reader Settings

The Reader settings tab allows you to configure the following settings for both Readers A and B for each door in a 2 door panel. In a 4 door system you can configure settings in Wiegand mode only for Reader A (IN) and in OSDP mode for both Reader A and B.

- Door Name
- Access Modes and Schedules
- Anti-Passback (enable/disable)
- Duress Output

Below table explains the limitation on Reader type supported for 4 Door Controller
Table 2-4 Table 2-8 Limitations for 4 Door Controller

Table 1:

Reader Type Readers Supported for Door	Reader Type Readers Supported for Door
OSDP	Reader A and B can be used for all the 4 Door
Wiegand	Only Reader A is available and Reader B is disabled

Figure 2-24 Door Configurations

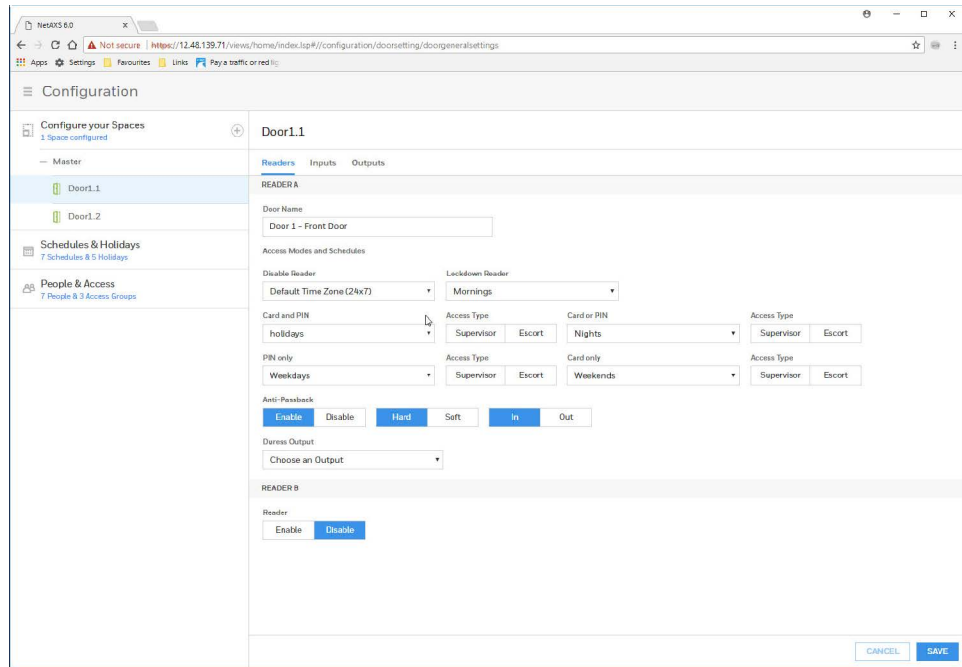


Figure 2-25 Door Configurations - OSDP Mode

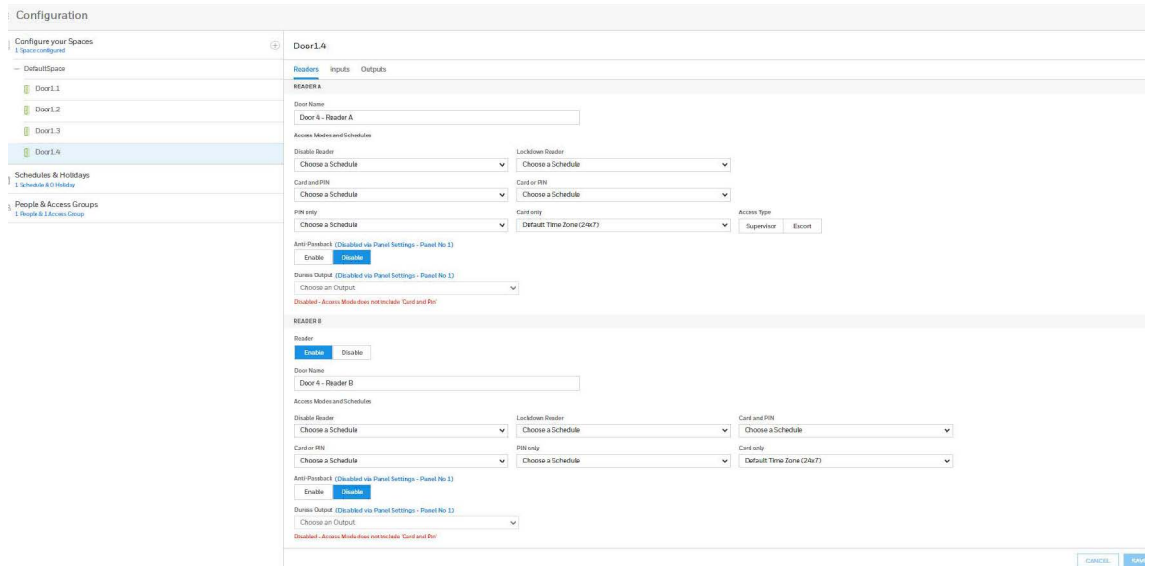


Figure 2-26 Door Configurations - Wiegand Mode

The screenshot shows the configuration page for 'Door 1.4' in Wiegand Mode. The left sidebar contains a tree view with 'Configure your Spaces' (1 Space configured), 'DefaultSpace' (Door 1.1, 1.2, 1.3, 1.4), 'Schedules & Holidays' (1 Schedule & 0 Holiday), and 'People & Access Groups' (0 People & 0 Access Group). The main content area is titled 'Door 1.4' and has three tabs: 'Readers', 'Inputs', and 'Outputs'. The 'Readers' tab is active, showing 'READER A' configuration. The 'Door Name' is 'Door 4 - Reader A'. Under 'Access Modes and Schedules', there are dropdowns for 'Disable Reader', 'Lockdown Reader', 'Card and PIN', and 'Card or PIN'. Below these are 'PIN only' and 'Card only' sections with dropdowns and 'Access Type' buttons for 'Supervisor' and 'Escort'. At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

1. Enter a **Door Name**.
2. Select a schedule for the following settings:
 - Disable Reader
 - Lockdown Reader
 - Card and PIN
 - Card or PIN
 - PIN only
 - Card Only

Note: The order of the above list is the priority order.

3. Select an **Access Type**, if desired, either SUPERVISOR or ESCORT, for Card and PIN, Card or PIN, PIN only, and Card only.

Note: Access Type selection is optional.

About Supervisor Mode

Supervisor mode enables a supervisor to enter without allowing general access. When this mode is enabled, the reader LED changes color four times per second (usually red then green).

About Escort Mode

Escort mode requires a supervisor escort to allow entry by an employee card holder. In Escort mode, the reader LED changes color four times per second (usually red then green).

Table 2-5 Escort Mode LED Color Cycle

Table 2:

Action	LED Cycle	Reaction
Supervisor swipes card	LED goes solid Red for 10 seconds	System waits for the swipe of an employee credential
Employee credential presented within 10 seconds of Supervisor card swipe	LED returns to rapid flashing	Door opens
No employee swipes a card within the 10 seconds	LED returns to rapid flashing	Reader returns to Escort mode
Supervisor swipes card twice	LED turns red after first swipe and turns to rapid flashing after second swipe	Door opens for supervisor (Supervisor gains entry)

Note: Unlike Supervisor mode, the Escort mode when active cannot be disabled during its schedule; a supervisor is required for all employee access during Escort mode schedule.

Note: VIP cards do not need a supervisor card to gain access.

4. Enable or Disable **Anti-Passback**.

Note: You must enable Anti-Passback in Panel Configuration before you can enable it here. See the Behaviour Settings section in [Figure 2-10](#) on [page 31](#).

Anti-Passback: When enabled, a valid card is required for entry and exit. The card holder must use the card in the proper IN/OUT sequence—that is, a card presented at an IN reader must then be presented at an OUT reader, or vice versa—a card presented at an OUT reader must then be presented at an IN reader.

Anti-Passback Violation: If the user's IN/OUT sequence is invalid, then an anti-passback violation event is generated for the type of anti-passback chosen (Hard or Soft) and the card holder is either denied access (Hard) or allowed access (Soft).

Enabled - Enables the anti-passback feature.

Note: The Hard/Soft and In/Out Anti-Passback options appear only after enabling Anti-Passback.

Hard - Validates IN/OUT status before allowing entry. A second swipe of the card at the same type of reader (IN/OUT) causes a

Hard anti passback violation notification and the user is denied entry.

Soft - Validates IN/OUT status before allowing entry. A second swipe of a card at the

same type of reader (IN/OUT) causes a Soft anti-passback violation notification but the user is allowed entry.

Out - Applies to readers located inside the anti-passback-controlled area. Card-holders use these readers when attempting to exit the anti-passback-controlled area.

Note: *With anti-passback, limited use and trace cards do not apply. In - Applies to readers located outside the anti-passback-controlled area. Card holders use these readers when attempting to enter the anti-passback-controlled area.*

5. Select a **Duress Output** value

Configures the output that triggers when a card holder enters a **duress PIN** at a keypad/card reader. A duress PIN is the PIN a user enters at a keypad when being forced (for example, during a robbery) to open a door. The card holder enters a PIN that is either one number higher or lower than the correct PIN. This PIN opens the door, but it also triggers the designated duress output and produces an alarm event.

For example, if the PIN is **2222**, entering either **2221** or **2223** opens the door, but triggers a duress pulse and generates an alarm. In this way, the card holder notifies others without detection by the unauthorized person.

Note: *A PIN ending in 0 (for example, 2320) will only trip a duress output when a 1 is used in place of the 0 (for example, 2321).*

Note: *The duress output feature requires the following configurations:*

- Duress must be enabled on the **Panel Configuration > Settings > Behaviour Settings** tab. See [Figure 2-10](#) on [page 31](#).
- A schedule/schedule must be selected for **Card and PIN** in the Doors configuration.

6. Enable or Disable **Reader B**. The default setting is Disabled. A confirmation message appears. Click **OK** to enable Reader B. Use an Reader B if a door has readers on both sides (inside and outside).

7. Click **Save**.

Note: *Should a conflict arise among the schedules set in the Access Modes and Schedules section, priority is given in the following order:*

- Disable Reader
- Lockdown Reader
- Card and PIN
- Card or PIN

- PIN only
- Card only

Therefore, the Disabled schedule has highest priority, and the Card Only schedule has lowest priority.

Note: Readers must be enabled in two places, in **Panel Configuration** and here. Go **Panel Configuration > Settings > Behaviour Settings** tab. See [Figure 2-10](#) on [page 31](#).

Note: The access mode defined here for the door can be overridden by a card assigned with a VIP card type. (See [Configuring People on page 69](#) for information about assigning a VIP card type.)

Configuring Door Inputs

The Inputs tab allows you to configure the following settings:

- Input Name
- Input Modes
- Shunt and Debounce
- Scheduling

Four inputs are associated with each of the doors on a MPA2C3 panel:

- **Status** – Provides door status information (Doorcnt).
- **Egress** – Allows the door to open or close normally without generating an alarm (REX).
- **Tamper A** – Reports abnormal handling of the reader device or wiring for Reader A.
- **Tamper B** – Reports abnormal handling of the reader device or wiring for Reader B.

The Inputs tab allows you to configure the following settings for each door:

- Define the Status, Egress, and Tamper input modes.
- Specify the Status, Egress, and Tamper shunt time, or the period of time the door's normal state will be ignored.
- Specify the Status, Egress, and Tamper debounce time, or the period of time the input
- must remain in its new state before it is recognized as being in the new state.
- Specify the schedules for the Status, Egress, and Tamper inputs.

Note: For 2-Door and 4-Door, the input configuration is same.

- Enable or disable Auto-Relock for the Status inputs.

1. Click **Inputs** on the **Doors** configuration window to open the Inputs configuration pane.

Figure 2-27 2-Door Inputs Configuration Interface

Figure 2-28 4-Door Inputs Configuration Interface - Weigand /OSDP Mode

2. Enter an **Input Name**.

3. Select **Input Modes**.

Table 2-6

Configura- tion	Description
Normally	<p>Normally Closed means that the input's normal state is closed. (Default setting).</p> <p>Normally Open means that the input's normal state is open.</p>
State	<p>Unsupervised means that the input's electrical circuit is wired in one path without alternative paths supervised by resistors. (Default setting)</p> <p>Supervised means that the input's electrical circuit is wired in one path with alternative paths supervised by resistors. If you select Supervised, then you must select a Resistor value.</p>
Resistor Value	<p>Specifies the resistor values being used in the supervised modes. Select from: 1K ohms, 2.2K ohms, 4.7K ohms, or 10K ohms. The default is 2.2K Ohm.</p> <p style="text-align: center;">Note: <i>when using MPA2S5 Door connection cable, the State for Door contact (DrCnt) must be set to Supervised with 2.2K ohms. The State for Request to Exit button must be set to Unsupervised</i></p>
Auto-Relock	<p>Causes the door to re-lock immediately when the door status switch closes after entry. The output relay that controls the door strike de-energizes when the associated input returns to normal state instead of remaining energized for the duration of the pulse time. To enable Auto-Relock, de-select the Disable check box, and select the associated output from the drop-down list.</p>
Output	<p>Select an Output value for Auto-Relock.</p>

4. Configure Shunt and Debounce times.

Table 2-7

Configura- tion	Description
Shunt Time (h:m:s)	Specifies the amount of time for which the inputs are shunted, or de-activated. The maximum length of time is 1 hour, 45 minutes, 59 seconds. You can express seconds in tenths of a second.
Debounce Time (h:m:s)	Specifies the period of time (MIN = 0 second, MAX = 6553.5 seconds) the input must remain in a new state before generating an alarm. For example, with a 5-second debounce time selected, if a Normal state is changed to Alarm, the state must remain in Alarm for five consecutive seconds before an alarm is generated.

5. Configure Scheduling.

Table 2-1

Configuration	Description
Shunt	Specifies the time period during which the input will be ignored.
Disable Interlocks	Specifies the time period during which the programmed action on this input from another point will be disabled.
Disable Alarm Mes- sages	Specifies the time period during which Alarm and Normal will not be reported, but Short and Cut will be reported. Short alarms are triggered when a short occurs in the input cable. Cut alarms are triggered when a wire is cut.

6. Click **Save**.

Configuring Door Outputs

The Outputs tab allows you to configure the following settings:

1. Discrete or Group selection
2. Output Name and Pulse Duration
3. Latch and Interlocks
4. Special output modes controlled by cards

5. Lock operation definition.
6. Scheduling.

Two outputs are associated with a door on a MPA2C3 panel

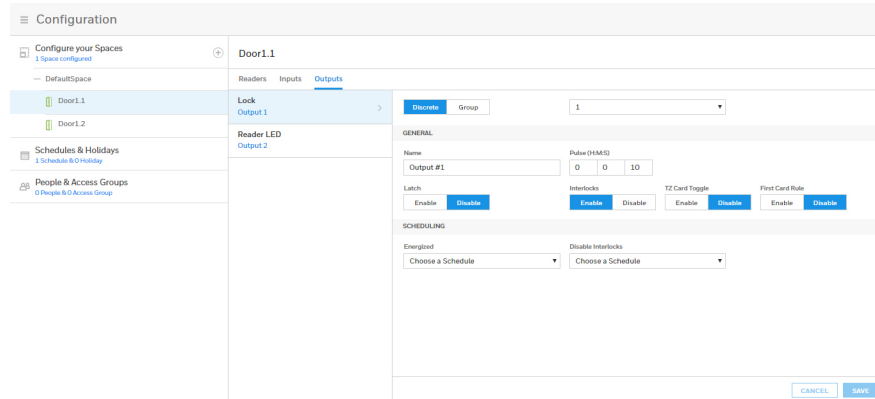
- a. **Lock**- Controls the lock in an electronic state to open or close the door
- b. **Reader LED**-Controls the LED of the Reader(s) in Green state (via LED wire to Wiegand reader, or OSDP command)

The Outputs tab allows you to configure the following settings for the door

1. Select Discrete Output or Output Group and number
2. Define Output Name
3. Specify Pulse duration
4. Disable or Enable Latched output after valid card (instead of pulse)
5. Disable or Enable Interlocks.
6. Disable or Enable Card activity outputs mode such as Time Zone Card Toggle and First Card Rule
7. Specify Lock Operation as Fail Safe or Fail Secure
8. Specify Schedules for Energized output and for Disable Interlocks

Click Outputs in the Doors configuration window to open the outputs configuration pane

Figure 2-29 Door Output Configuration Interface



1. Select Discrete or Group and specify the available number
2. Select General Setting

Configuring Discription

Name	Enter a unique name to identify the lock output
Pulse Time	Configure how long a device assume to be normal status such as a hours, minutes and seconds, Maximum time is 1:45:59
Latch	Toggle the start of the outputs between energized and de-energized upon every activation (code use, interlock, or manual pulse) Interlocks Disable/enable interlocks. See Interlock Configuration , page 77 for more information about Interlocks
TZ Card Toggles	Requires like the First Card Rule, a valid card read within the time zone to enable the time zone (periods in which the doors are unlocked) to take effect. Unlike the First Card Rule, however the user can swipe the card a second time to return the doors to a locked Note: Effective only if the output has a valid schedule for Energized in the Section Scheduling. Both TZ Card Toggle and First Card Rule cannot be enabled at the same time
First Card Rule	First Card Rule requires a valid card read within the time zone to enable the time zone (period in which the doors are unlocked) to take effect. Note: Effective only if the output has a valid schedule for Energized in the section Scheduling. Both TZ Card Toggle and First Card Rule cannot be enabled at the same time.

3. Select Scheduling

Configuration	Description
Energized	Specifies the period during which the output relay is automatically in the state where the door is unlocked (Energized or De-energized-when FACP is in use). Select the Schedule (that you created in Configuring Schedules , page 45) from the drop down list. The Energized state of the output can be affected by the Enabled setting for the TZ Card Toggle or First Card R
Disable Interlocks	Specifies the period during which the Interlock that controls the output will be disabled, Select a Schedule (that you created in Configuring Schedules , page 45) from the dropdownlist.

4. Click Save.

Configuring Panel I/O and Groups

To view a configuration of a group of outputs, click **Group** and select the group number from the drop-down list. The group configuration screen appears. **Note** that you can only view the group configuration from this screen.

To edit the Group configuration, go to **Panel Configuration > Outputs > Groups**.

Figure 2-30 2-Door Output Group

Figure 2-31 4-Door Output Group

Configuring Inputs

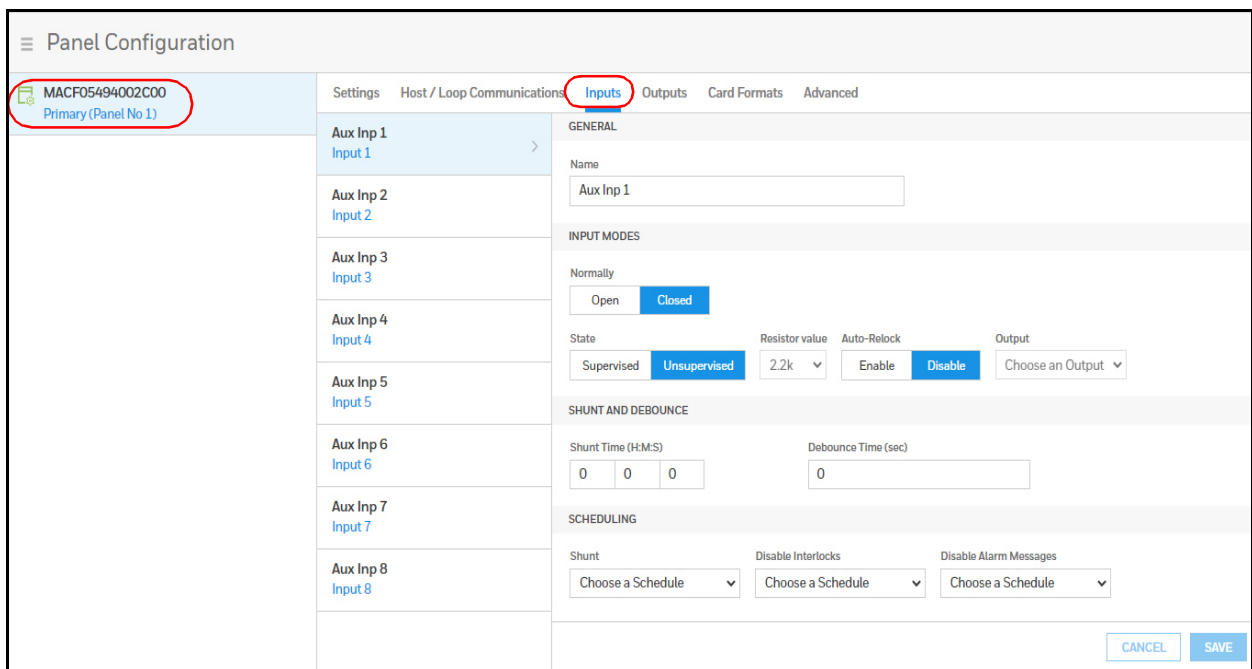
The Inputs tab enables you to:

- Enter a name for the input.
- Configure input modes, including the state.
- Configure shunt and debounce settings.
- Configure input schedules.

1. Navigate to the Input tab:

- Click **Panel Configuration** > **Inputs**, or
- Click **Panels** in the **Dashboard**.

Figure 2-32 Configuring Panel Inputs



4. Click to select an input.

5. Select **Input Modes**.

Table 2-8

Configuration	Description
Normally	Normally Closed means that the input's normal state is closed. (Default setting). Normally Open means that the input's normal state is open.

Table 2-8

Configuration	Description
State	Unsupervised means that the input's electrical circuit is wired in one path without alternative paths supervised by resistors. (Default setting) Supervised means that the input's electrical circuit is wired in one path with alternative paths supervised by resistors.
Resistor Value	Specifies the resistor values being used in the supervised modes. Select from: 1K ohms, 2.2K ohms, 4.7K ohms, or 10K ohms. The default is 2.2K Ohm. Note:when using MPA2S5 Door connection cable, the State for Door contact (DrCnt) must be set to Supervised with 2.2K ohms. The State for Request to Exit button must be set to Unsupervised.
Auto-Relock	Causes the door to re-lock immediately when the door status switch closes after entry. The output relay that controls the door strike de-energizes when the associated input returns to normal state instead of remaining energized for the duration of the pulse time. To enable Auto-Relock, de-select the Disable check box, and select the associated output from the drop-down list.
Output	Select an Output value for Auto-Relock,

6. Configure **Shunt** and **Debounce** times.

Table 2-9

Configuration	Description
Shunt Time (h:m:s)	Specifies the amount of time for which the inputs are shunted, or de-activated. The maximum length of time is 1 hour, 45 minutes, 59 seconds. You can express seconds in tenths of a second.
Debounce Time (h:m:s)	Specifies the period of time (MIN = 0 second, MAX = 6553.5 seconds) the input must remain in a new state before generating an alarm. For example, with a 5-second debounce time selected, if a Normal state is changed to Alarm, the state must remain in Alarm for five consecutive seconds before an alarm is generated.

7. Configure **Scheduling**.

Table 2-10

Configuration	Description
Shunt Schedule	Specifies the time period during which the input will be ignored.
Disable Interlocks	Specifies the time period during which the programmed action on this input from another point will be disabled.

Table 2-10

Configuration	Description
Disable Alarm Messages	Specifies the time period during which Alarm and Normal will not be reported, but Short and Cut will be reported. Short alarms are triggered when a short occurs in the system. Cut alarms are triggered when a wire is cut.

Click **Save**.

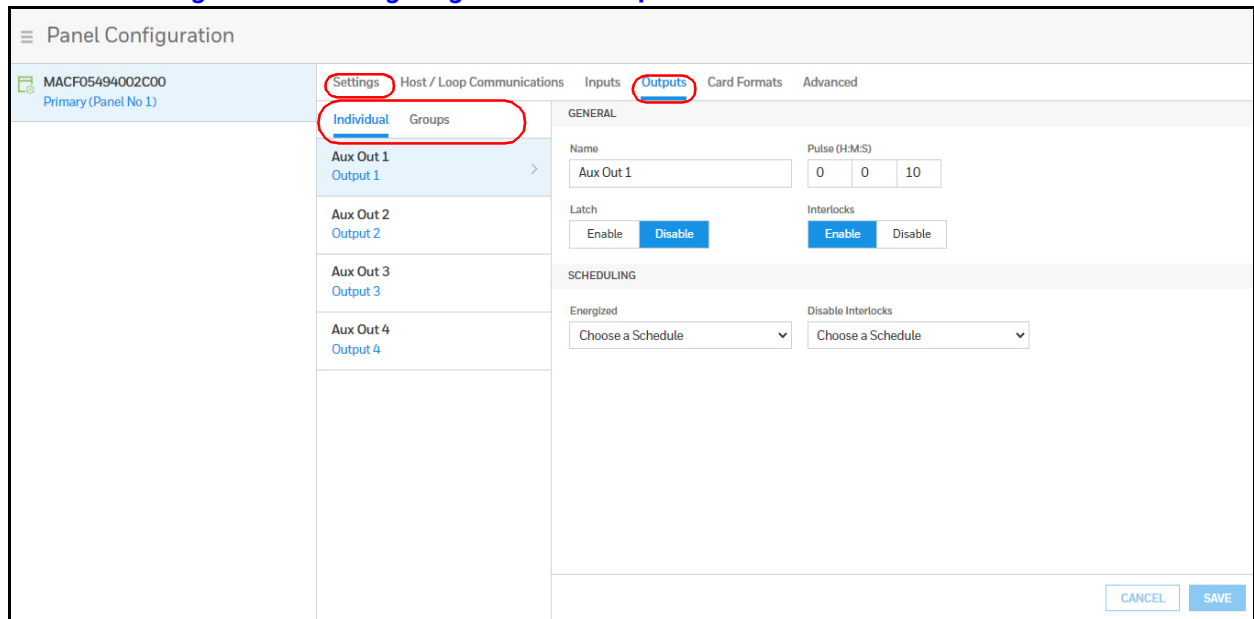
Configuring Outputs

In the Individual Outputs tab, you can configure the following for each output:

- Pulse time
- Disable/Enable Latch and Interlocks
- Energized and Disable Interlocks schedules

1. Navigate to the **Outputs** tab: Click **Panel Configuration > Outputs > Individual**.

Figure 2-2 Configuring Individual Outputs



2. Click to select an individual output from the list.
3. Configure the following for each output:

Table 2-11

Setting	Description
Name	Enter a unique name for the output

Table 2-11

Setting	Description
Pulse Time	Configure how long a device assumes abnormal status, such as a horn sounding or a released door strike. In hours:minutes:seconds. Maximum time is 1:45:59.
Latch	Toggles the state of the outputs between energized and de-energized status upon every activation (code use, interlock, or manual pulse).
Interlocks	Disable/enable interlocks. See <i>Configuring Interlocks on page 53</i> for more about Interlocks.
Energized	Specifies the period during which the output relay is automatically energized. Select a schedule (that you created in Entering a Panel Name section on page 42) from the drop-down list.
Disable Interlocks	Specifies the period during which the interlocks that control the output will be disabled. Select a schedule (that you created in Entering a Panel Name section on page 42) from the drop-down list.

8. Click **Save**.

Configuring Output Groups

Note: You must select at least one output before you can create a group.

The Output Groups tab allows you to configure the following:

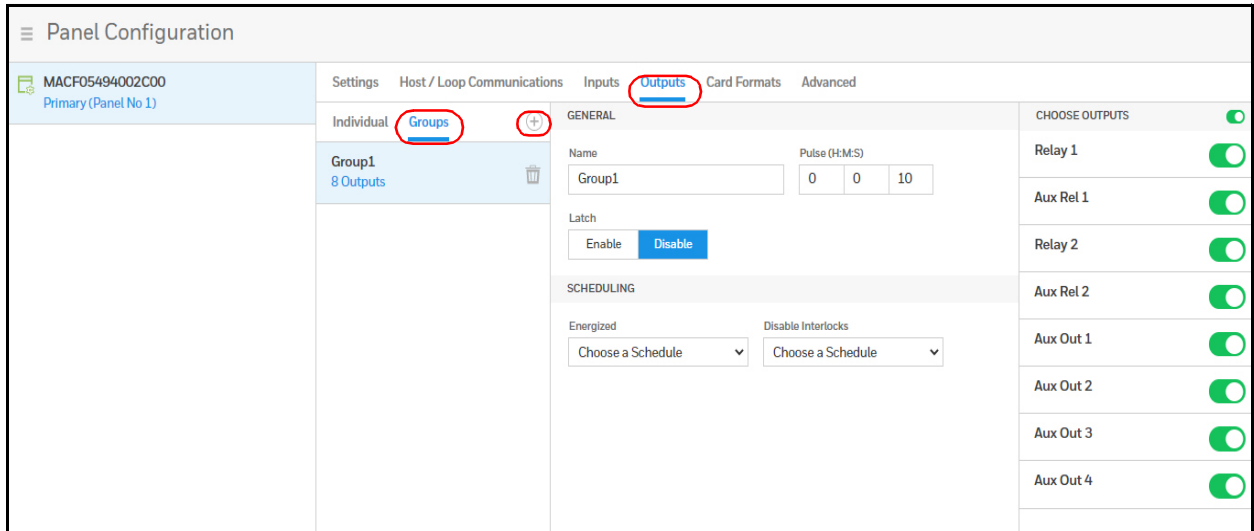
- A group of horns to sound for a set time during a set period
- Energize or de-energize a group of doors during a set period

In the Output Groups tab, you can configure the following for one or more groups:

- Pulse time
- Disable/Enable Latch
- Energized (schedule selection)
- Disable Interlock (schedule selection)

1. Navigate to the **Output Groups** tab: Click **Panel Configuration > Outputs > Groups**.

Figure 2-33 Configuring Output Groups




2. Click to  add a new group.
3. Configure the following for each output group:

Table 2-12

Setting	Description
Name	Enter a unique name for the group
Pulse Time	Configure how long a device assumes abnormal status, such as a horn sounding or a released door strike. In hours:minutes:seconds. Maximum time is 1:45:59.
Latch	Toggles the state of the outputs between energized and de-energized status upon every activation (code use, interlock, or manual pulse).
Energized	Specifies the period during which the group of output relays are automatically energized. Select a schedule (that you created in Entering a Panel Name section on page 42) from the drop-down list.
Disable Interlocks	Specifies the period during which the interlocks that control the group's outputs will be disabled. Select a schedule (that you created in Entering a Panel Name section on page 42) from the drop-down list.

4. Click toggle(s) to select outputs. Click the **Choose Outputs** toggle to select all outputs.
5. Click **Save**.

Configuring Card Formats

A card format tells the panel how the card number will be read. The panel supplies the format to the card readers. Then, the card readers can correctly read the card.

Navigate to Card Formats:

- Dashboard > Panels > Card Formats
- Menu > Panel Configuration > Card Formats

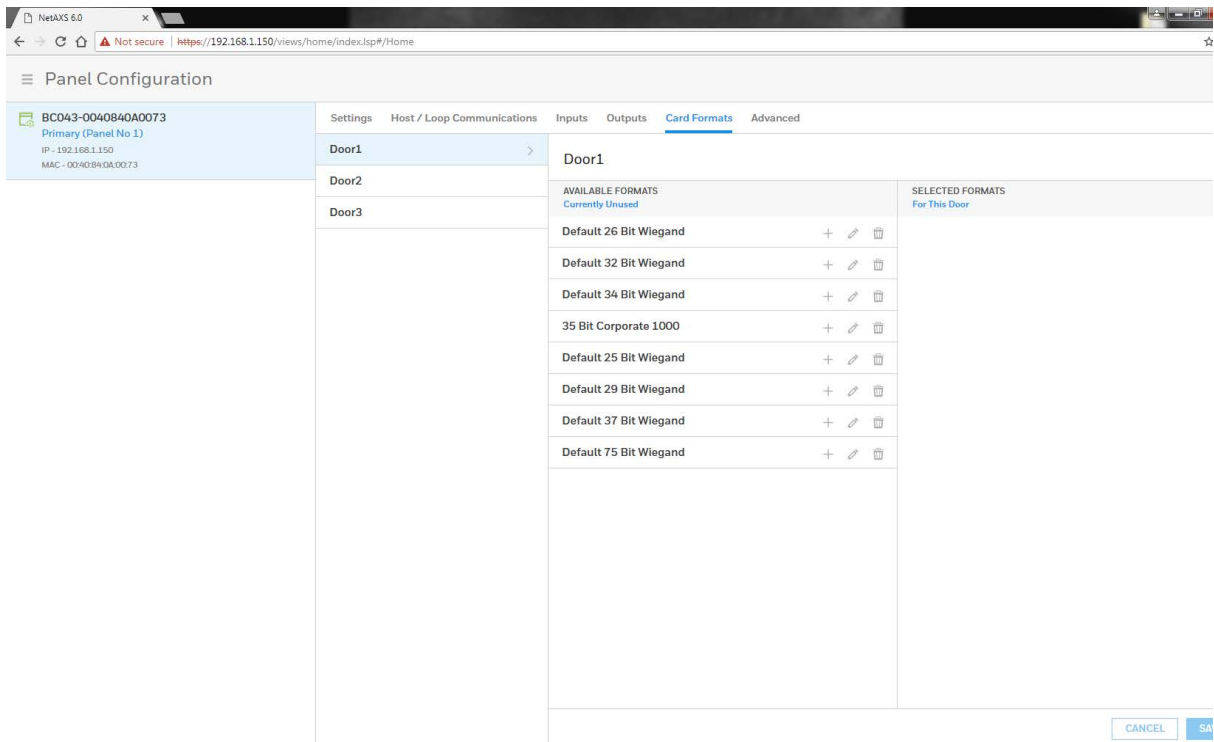


Table 2-13 Card Format Settings


Settings	Description
Available Formats	Lists all the formats in the panel. All formats, new ones as well as the eight default formats, are listed under Available Formats. This information allows all readers by default to use all formats to try and decipher card reads. The reader will then use every Available Format(s) to decipher incoming card reads. Any cards presented with formats that do not match the Available Format(s) are then reported as an Invalid Format event.
Selected Formats	Lists specific formats selected by the user from the Available Formats list that the reader should use to decipher card reads. As soon as a single format is placed in the Selected Formats column, the reader begins to use only the selected format, ignoring any unselected formats in the Available Formats list. Cards presented with formats that do not match the Selected Format(s) are then reported as an Invalid Format event, even if the format is in the Available list. This selection is on a per reader basis-that is, each reader can have its own selected formats. Selections at one reader do not affect another reader.

Note: *The user should never add in more than one format using the same total number of bits. If you need more information, please contact Technical Support.*

1. Click the Add icon (+) of each desired card format under the Available Formats list, and to move the format(s) into the Selected Formats list.

Note: *If you select no formats, the reader will use all available formats (up to 128 per pane) as described for the Available Formats setting in [Table 2-13](#) If you select a subset of formats for a given reader, the reader will interpret only those formats and ignore formats that are not selected, as described for the Selected Formats setting in [Table 2-13](#).*

2. Click Save.

If you want to create a new card format, click Circled Add icon  to display an empty Card Format data layout screen.

Panel Configuration

MACF05494002C00
Primary (Panel No 1)

Settings Host / Loop Communications Inputs Outputs **Card Formats** Advanced

GENERAL

Card Format Name Concatenate Site Code Exponent Reverse Bit Order

BIT MANAGEMENT

Total Bit Count

Even Parity Odd Parity

CID A CID B CID C CID D

Site Code A Site Code B Site Code C Site Code D

Use the field descriptions in [Table 2-14](#) to define the layout and click Save.

Table 2-14 Panel Configuration > Card Formats

Settings	Description
Card Format Name	Displays the name by which the format will be listed in the Card Formats tab. The name is user-defined.
Concatenate Site Code	When enabled, it is used with the Exponent field to combine the site code and Card ID into a new unique number. Mainly used when a site requires the use of more than 8 different site codes.
Exponent	Concatenate Site Code box is checked. To generate a card's new ID, use this box to insert the desired number of zeroes to be added to the right-hand side of the Site Code value. Then add the card ID to calculate the card's new ID. For example, a 26-bit card has a site code of 123 and the card ID is 637. When the Concatenate Site Code is enabled with an exponent of 4, 4 zeroes are added to the right-hand side of the site code. The result is a final value of 1230000. This newly modified site code value is then added to the number that the panel has read as the card's ID-that is, 1230000 + 637 = 1230637. The newly combined number becomes the card's new ID value.
Reverse Bit Order	Returns the message from the reader in reverse bit order (least significant bit first and most significant bit last).
Total Bit Count	Lists the total number of bits on the card.
Even Parity	Lists where on the card that even parity is being observed. Start - First bit in the card where even parity begins. Num - Number of bits to the right of the start bit, including the start bit, to include in the even parity check.

Table 2-14 Panel Configuration > Card Formats (Continued)

Settings	Description
Odd Parity	Lists where on the card that odd parity is being observed. Start - First bit in the card where odd parity begins. Num - Number of bits to the right of the start bit, including the start bit, to include in the odd parity check.
CID A CID B CID C CID D	Lists where on the card the Card ID A is listed. Start - First bit in the card where card ID begins. Num - Number of bits to the right of the start bit, including the start bit, that comprise the card ID. Most formats require only CID A, and not CID B, C, or D. If the Card ID of the card format has multiple parts, CIDs B, C, and D may be used to specify which parts are to be concatenated to form the Card ID.
Site Code A Site Code B Site Code C Site Code D	Lists where on the card the Site Code A is listed. Consult the card manufacturer for detail on the card detail. Start - First bit in the card where the card's Site Code begins. Num - Number of bits to the right of the start bit, including the start bit that comprise the Site Code. Most card formats require only Site Code A.

If you want to change an existing card format's data layout, click the **Edit icon** (pencil) of the desired format in the list of existing formats to display the Card Format data layout screen. Use the descriptions in the table above to edit the layout's fields. Then, click Save to save the edited format.

To Delete a Card Format, select the desired card format than click on the **Delete icon** (trash can). A confirmation popup will appear. Click OK to the popup.

Note: *Note: Only user added card formats can be deleted. The default card formats cannot be deleted.*

Managing Site Codes

Site codes (also called facility codes) identify an enterprise's site with unique numbers for each site. You can create a maximum of eight site codes to serve as secondary IDs (in addition to the card number) on the card for additional validation.

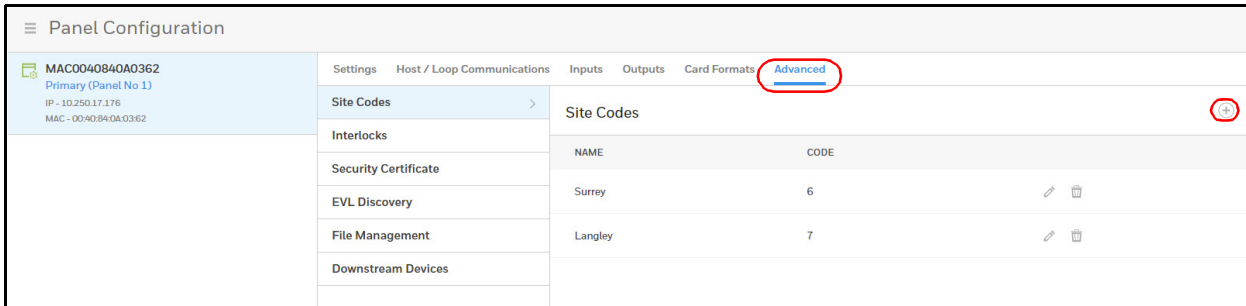
The Site Codes panel enables you to:

- Create one or more site codes.
- View existing site codes.
- Modify an existing site code.
- Delete a selected site code.

Navigate to the Settings panel:

- **Dashboard > Panels > Advanced**, or
- **Menu > Panel Configuration > Advanced**

Figure 2-34 Settings Panel

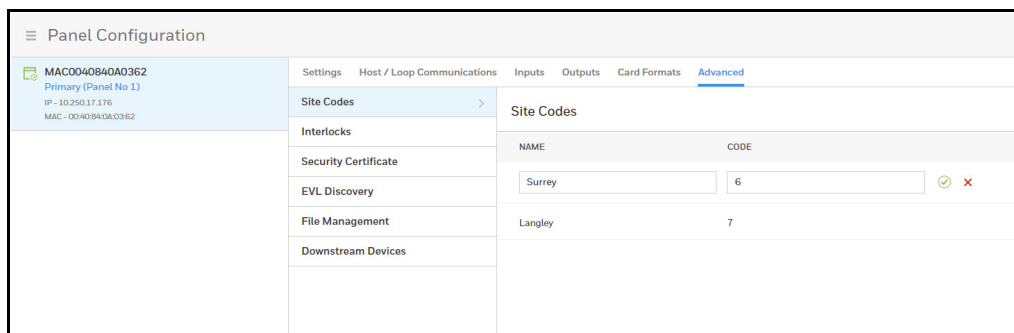


Creating a Site Code

1. Click to enter a new site name.
2. Editable fields appear in the **Name** and **Code** columns.
3. Enter a unique name for the site code in the **Site code name** field. You can use letters, numbers, and some special characters.
4. Enter a unique number (up to five digits, numbers only) for the site code in the **Code** field. Valid site codes are between 1 and 65535.
5. Click on the check mark to the creation of the site code.
6. A message appears confirming that the new site has been Successfully Saved.

Modifying a Site Code

1. Click to modify a site code.



The **Name** and **Code** fields become active.

2. Make your modifications, then click the green check mark to save.

A message appears confirming that the new site has been Successfully Updated.

Deleting a Site Code

Click  to delete a site code.

Please refer to Chapter 4

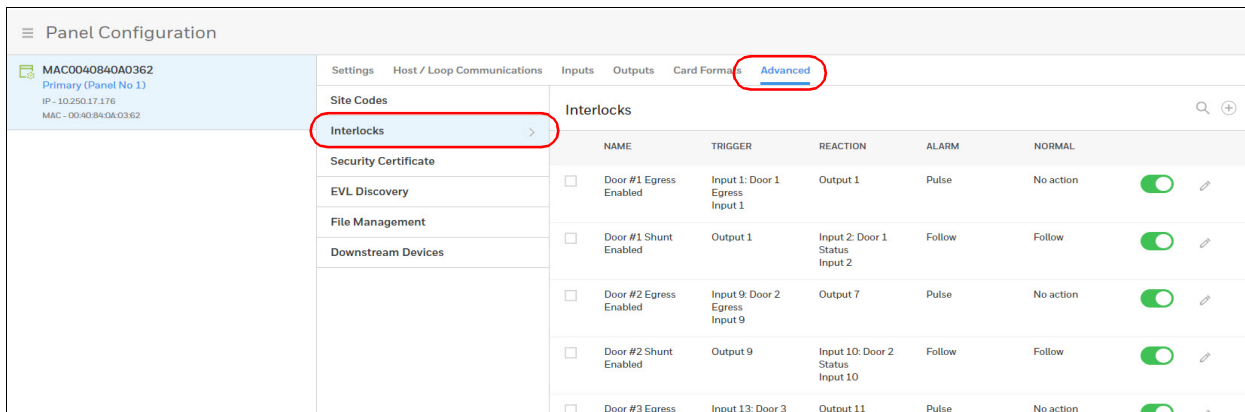
Interlock Configuration






An interlock is a programmed connection between two points. The interlock causes an input point, output point, or group of output points to act in a specified manner when another input point, output point, or group of output points changes its state. An action on the trigger point causes a reaction on the reacting component. For example, when a motion detector (input) detects movement, it causes a horn (output) to sound.

On the Interlocks pane, you can:

- Create and delete interlocks.
 - Enable or disable existing interlocks.
1. Navigating to the Interlocks interface.
- Click **Panel Configuration > Advanced > Interlocks**.

Figure 2-35 Interlocks Configuration Tab



NAME	TRIGGER	REACTION	ALARM	NORMAL	
<input type="checkbox"/> Door #1 Egress Enabled	Input 1: Door 1 Egress Input 1	Output 1	Pulse	No action	<input checked="" type="checkbox"/> 
<input type="checkbox"/> Door #1 Shunt Enabled	Output 1	Input 2: Door 1 Status Input 2	Follow	Follow	<input checked="" type="checkbox"/> 
<input type="checkbox"/> Door #2 Egress Enabled	Input 9: Door 2 Egress Input 9	Output 7	Pulse	No action	<input checked="" type="checkbox"/> 
<input type="checkbox"/> Door #2 Shunt Enabled	Output 9	Input 10: Door 2 Status Input 10	Follow	Follow	<input checked="" type="checkbox"/> 
<input type="checkbox"/> Door #3 Egress	Input 13: Door 3	Output 11	Pulse	No action	<input type="checkbox"/> 

Creating Interlocks

1. Click  to open the **Create Interlock** window.

Figure 2-36 Create Interlocks Interface

CREATE INTERLOCK

Interlock Name

When TRIGGERS	Choose REACTION	Then Execute ALARM ACTION	Upon Resuming NORMALCY
Door 1 Egress	Door 1 Egress	Unshunt	Unshunt
Door 1 Status	Door 1 Status	Shunt	Shunt
Door 1 Tamper A	Door 1 Tamper A	Follow	Follow
Door 1 Tamper B	Door 1 Tamper B	Invert Follow	Invert Follow
Panel Tamper Ext	Panel Tamper Ext	No action	No action
Power Status	Power Status	Timed Shunt	Timed Shunt
Panel Tamper Int	Panel Tamper Int		
Battery Status	Battery Status		
Door 2 Egress	Door 2 Egress		

2. Enter a name for the new Interlock.
3. Select configurations for the **Triggers** (Input, Output, or Group), **Reaction** (Input, Output, or Group), **Alarm Action**, and **Normalcy** (the state to which the trigger returns).

Table 2-15

Configuration	Description
Triggers	<p>Specifies the input, output, or output group for which a change of state will cause a reaction from another input, output, or group.</p> <p>If Trigger = Inputs, then triggers 1-88* will have an interlock link (Int Lnk) number from 1-96.</p> <p>If Trigger = Outputs, then outputs 1-80* will have an interlock link (Int Lnk) number from 97-184.</p> <p>If Trigger = Group, then groups 1-64* will have an interlock link (Int Lnk) number from 185-250.</p> <p>Use the drop-down list to specify the number of the input or output.</p> <p>Additional Input/Output/Group points are achieved with the addition of NX4IN and NX4OUT secondary devices.</p>

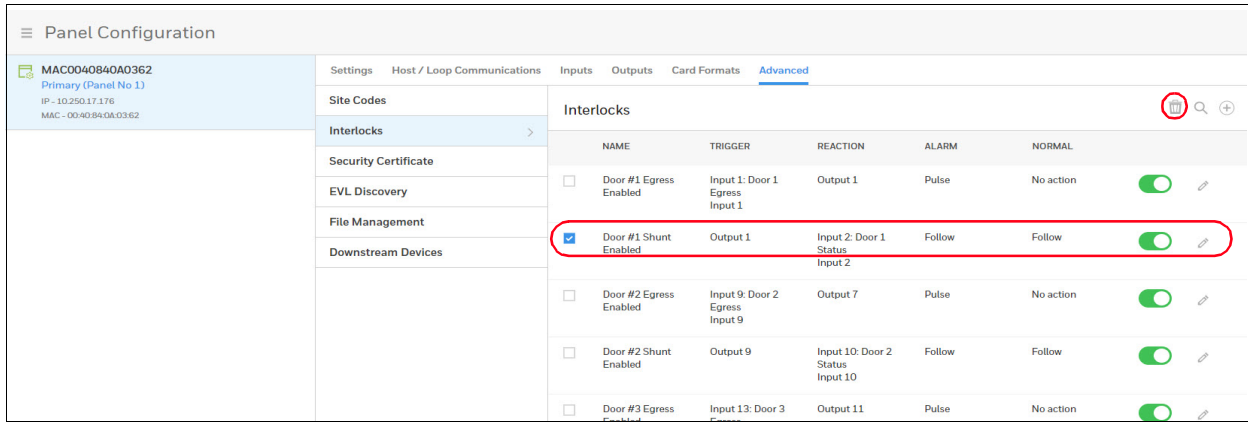
Table 2-15

Configuration	Description
Reaction	Specifies the input, output, or output group that will react to a change of state from the trigger point. Use the drop-down list to specify the number of the input or output.
Interlock Actions	<p>Then Execute (Alarm Action) – Specifies the reacting component’s action when the trigger’s change of state occurs. Select the action from the available options.</p> <p>Upon Resuming (Normalcy) – Specifies the reacting component’s action when the trigger returns to the normal state. Select the action from the available options.</p> <p>Following are the available Input Reactor actions in the drop-down lists:</p> <p>Unshunt – Reactivates the input point.</p> <p>Shunt – Ignores alarms from the input point.</p> <p>Follow – The reacting point (second point) takes on the same state as the triggering point (first point).</p> <p>Invert Follow – The reacting point (second point) takes on the opposite state as the triggering point (first point).</p> <p>No action – The reacting point (second point) does nothing in response to the state change of the triggering point (first point). No change of state.</p> <p>Timed Shunt – Ignores alarms from the input point for a specified amount of time.</p> <p>Following are the available Output Reactor actions in the drop-down lists:</p> <p>De-energize – Remove energy from an output point or group. On a system, the normal state of an output point or group is "de-energized".</p> <p>Energize – The state of an output point or group. Output points and groups are in a normal state when they are "de-energized". An energized state means that the output or group is active.</p> <p>Follow – The reacting point (second point) takes on the same state as the triggering point (first point).</p> <p>Invert Follow – The reacting point (second point) takes on the opposite state as the triggering point (first point).</p> <p>No action – The reacting point (second point) does nothing in response to the state change of the triggering point (first point). No change of state.</p> <p>Pulse – Energizes the output point or group for a specific amount of time.</p> <p>Pulse Off – Becomes unshunted for the programmed shunt time, followed by a return to the shunted state.</p>

Deleting Interlocks

1. Click to select an **Interlock**.

Figure 2-37 Deleting an Interlock



2. Click the **Delete** button . A message appears asking for confirmation.
3. Click **OK**.

Enabling/Disabling Interlocks

- Click the **Enable/Disable** button . A confirmation appears if successful.

Downstream Devices

The NETAXS® I/O devices provide the MPA2C3 panels with additional inputs and outputs. The MPA2C3 panels supports two Interface types:

- NX4IN - Provides 32 supervised, four-state inputs that are limited to 2.2K ohms resistance. The NX4IN must be assigned network addresses 1 and 2.
- NX4OUT - Provides 2 supervised inputs and 16 SPDT relay outputs; each input is limited to 2.2K ohms resistance. The NX4OUT must be assigned network addresses 3-6.

Note: The NX4IN and NX4OUT network addresses are set by the DIP switches on each board. Refer to the NETAXS® NX4IN/NX4OUT Input/Output Configuration Guide for more information about configuring the NX4IN and NX4OUT boards.

Note: MPA2C3 panel supports a maximum of six daisy-chained Interface boards - two NX4IN and four NX4OUT boards. The boards connect to the MPA2C3 panel's RS-485 Interface Bus (J16).

Figure 2-38 Menu > Panel Configuration > Advanced > Downstream Devices

The screenshot shows the 'Panel Configuration' interface. On the left, there is a sidebar with two panels: 'BC048e-0040840A0380 Primary (Panel No 1)' and 'BC037- MPA2 Secondary (Panel No 2)'. The 'Advanced' tab is selected, and the 'Downstream Devices' sub-tab is active. The main area displays a table with the following data:

NAME	TYPE	ADDRESS
I/O RS-485 #1 NX4IN	NX4IN	1
I/O RS-485 #2 NX4IN	NX4IN	2
I/O RS-485 #3 NX4OUT	NX4OUT	3
I/O RS-485 #4 NX4OUT	NX4OUT	4
I/O RS-485 #5 NX4OUT	NX4OUT	5
I/O RS-485 #6 NX4OUT	NX4OUT	6

The **Downstream Devices** tab enables you to:

- View and modify the names of the devices that communicate with the panel.
- View the types and addresses of the devices that communicate with the panel.

Configuring People and Cards

Configuring People

The People tab on the People & Cards interface allows you to do the following:

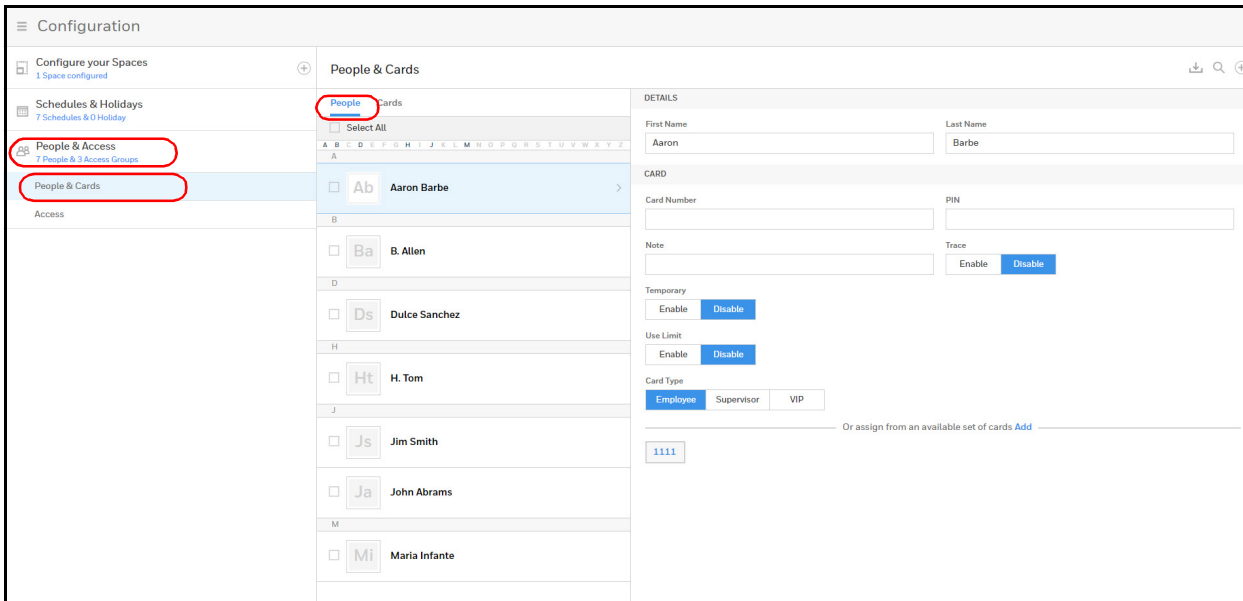
- Create a person, including assigning/adding a card.
- Modify a person.
- Delete a person.

You can configure people to have one of the following card types, with the appropriate available functionality. Select from **Supervisor**, **Employee**, and **VIP**.

Navigate to the People tab on the People & Cards window:

- Click **People** in the **Dashboard** to access the **People & Cards** interface, or
- Click **Configuration** in the **Menu**, then click **People & Access > People & Cards**.

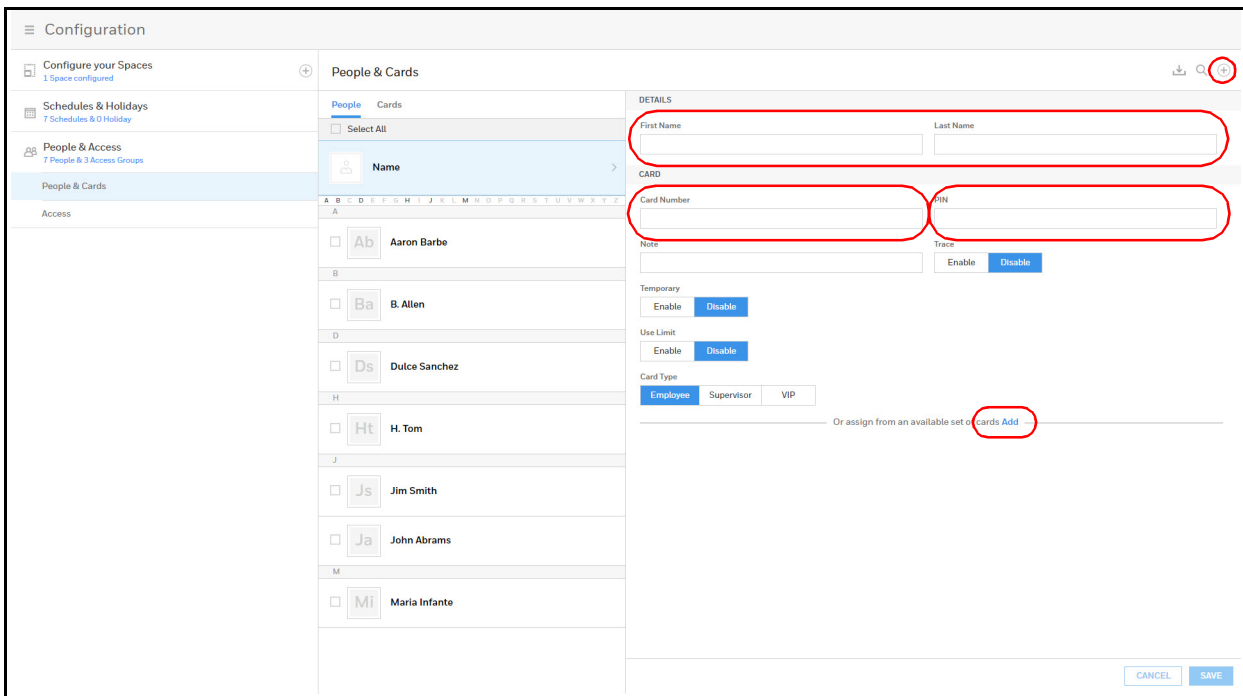
Figure 2-39 People & Cards Configuration Interface



Creating a Person

1. Click to  on the **People** tab to create a new user.

Figure 2-40 Creating a New Person



2. Enter a first and last name.
3. Enter a **card Number**.

4. Or click **Add** near the bottom of the window to assign a card from an available set of cards.
5. Enter a **PIN** (numbers only).
6. Optional: Enter a note, such as Department number, phone extension, or a birthday, for example. Notes can be up to 20 characters.
7. Turn **Trace** on or off.
8. Trace provides a record of the card holder's path through the facility by sending an alarm message to the alarm monitor whenever a card with trace enabled is presented at a reader.
9. Select a type of **Usage**.
10. If you select **Temporary**, then you must select an end date on the calendar.
11. If you select **Limited**, then you must select the maximum number of times the card can be presented.
12. Select an **Access Type**: Employee, Supervisor, or VIP. See [User Access Types and Functionality](#) section on page 123 for more about Access Types.
13. Click **Save**.

Tip: You can assign attributes from an existing set of cards. At the bottom of the **People & Cards** window, click **Add** to open a list of available cards, then select a card to assign to this person.

Modifying a Person

1. Click the box next to the person's name.

Figure 2-41 Modifying a Person

The screenshot shows the 'People & Cards' configuration interface. On the left, a sidebar lists navigation options: 'Configure your Spaces', 'Schedules & Holidays', and 'People & Access'. The 'People & Cards' section is expanded, showing a list of people. The person 'B. Allen' is selected, with a red circle highlighting the checkbox and name. The 'DETAILS' panel on the right contains the following information:

- First Name:** B.
- Last Name:** Allen
- CARD:**
 - Card Number:** [Empty field]
 - PIN:** [Empty field]
 - Note:** [Empty field]
 - Trace:** [Enable] [Disable]
- Temporary:** [Enable] [Disable]
- Use Limit:** [Enable] [Disable]
- Card Type:** [Employee] [Supervisor] [VIP]

At the bottom of the 'DETAILS' panel, there is a text input field with the value '36483' and a link that says 'Or assign from an available set of cards Add'.

2. Make changes to the person, then click **Save**.

Deleting a Person


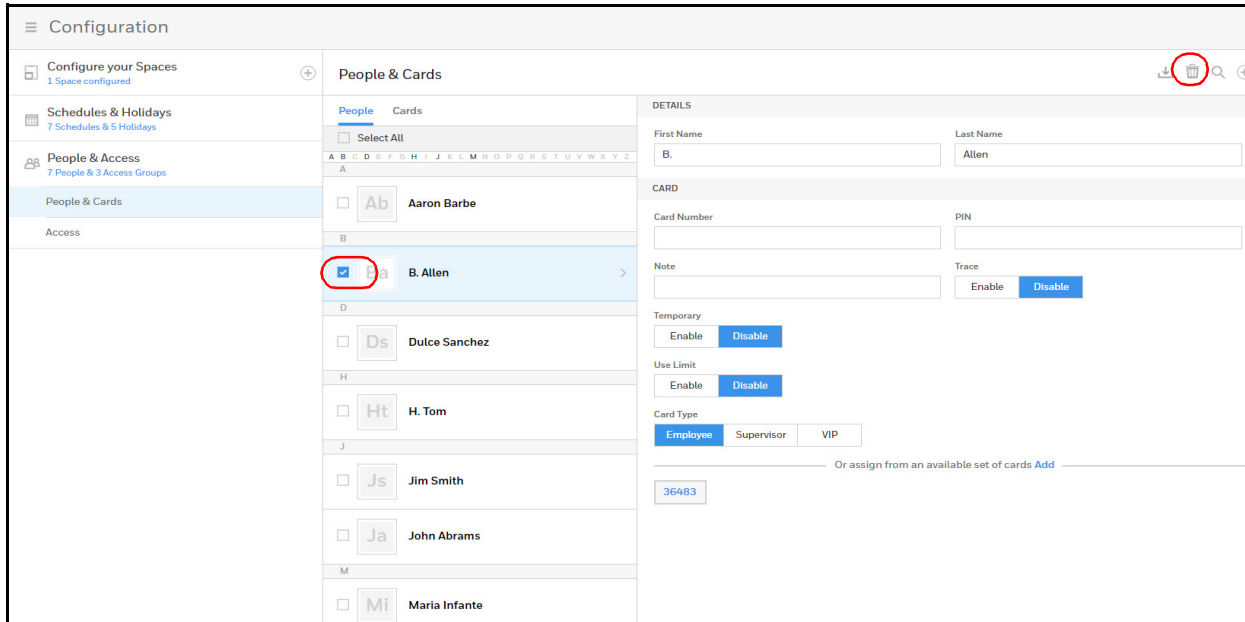

1. Click the box next to the person's name. A delete icon appears .

Figure 2-42 Deleting a Person



2. Click the delete icon . A confirmation message appears.
3. Click **OK** to confirm the deletion.

Configuring Cards

A card is encoded with a unique number and the person's access group grants rights to access system resources. For example, in addition to its unique number, a card allows the person access to certain doors during a certain time of day.

The Cards configuration interface allows you to:

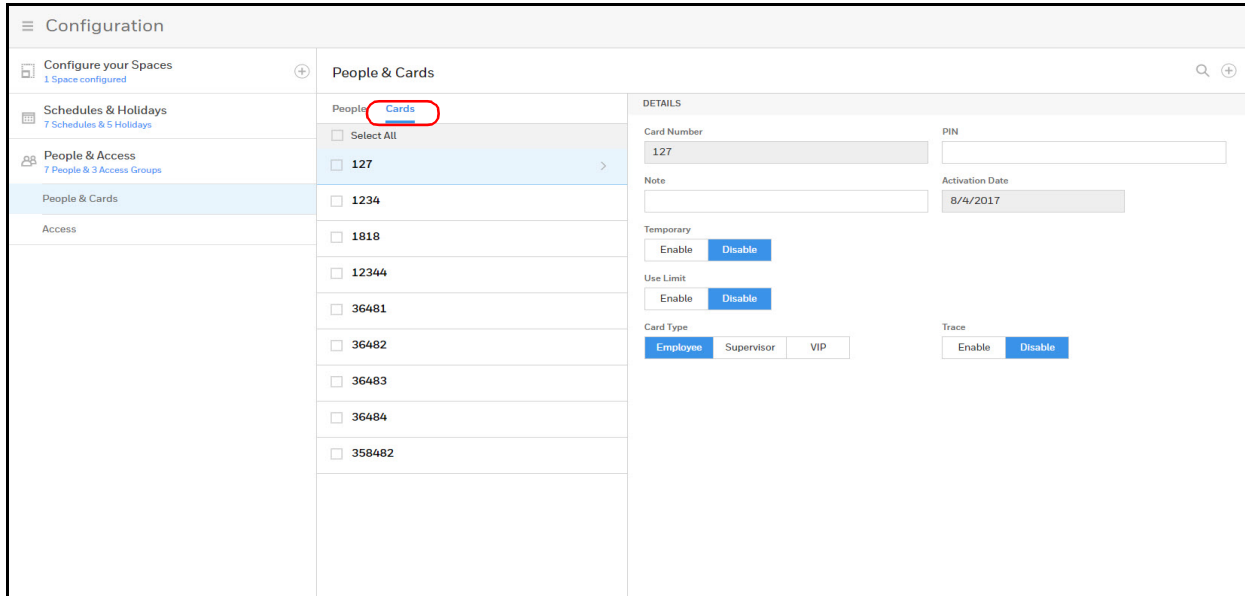
- Create cards encoded with the following information:
- Card Number(s)
- Card Type
- Personal Identification Number (PIN)
- Trace
- Expiration Date
- Use Limit
- Note

Note: People can have more than one card associated to them.

Navigate to the Cards tab on the People & Cards window:

- Click **Cards** in the **Dashboard** to access the **People & Cards** interface, or
- Click **Configuration** in the **Menu**, then click **People & Access > People & Cards > Cards**.

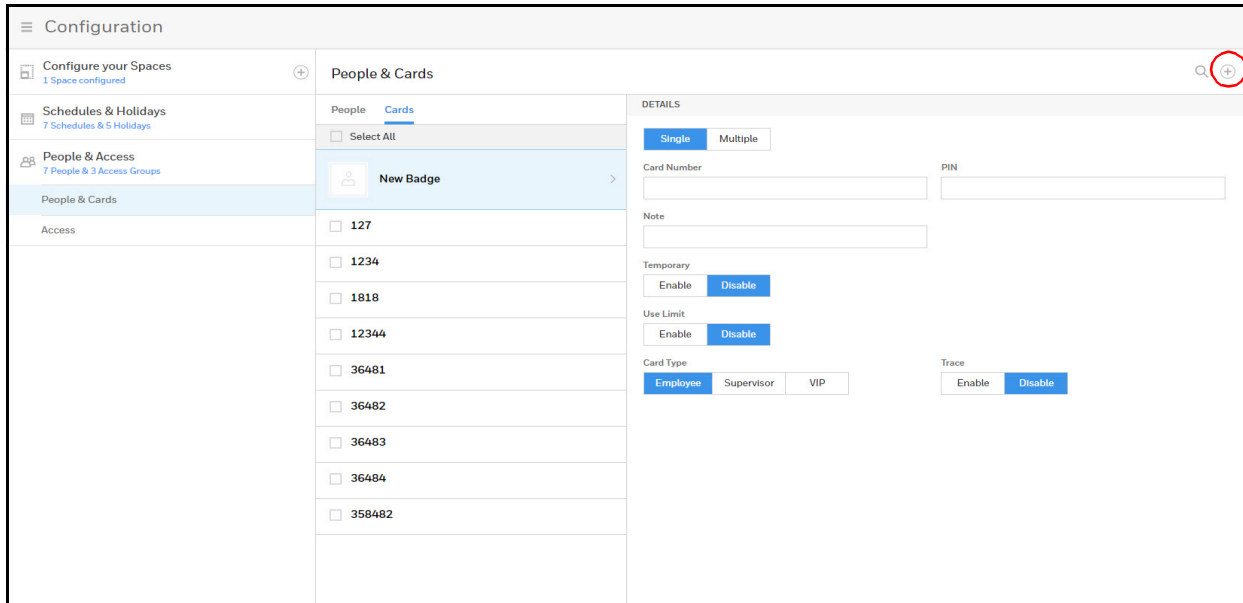
Figure 2-43 Cards Configuration Interface



Adding a New Card

1. Click  in the Cards tab of the **People & Cards** window to open the configuration options.

Figure 2-44 Adding New Cards



2. Enter either a card number (if adding a single card) or a range (if adding multiple cards).
3. Enter a **PIN** if you're adding a single card. See the note on [page 83](#) for PIN number rules.

Note: A PIN is optional; however, if the door reader is configured to require PIN identification (see [Configuring Door Reader Settings on page 47](#)), then you must create a PIN for the card holder here. The PIN has a maximum of six digits.

Note: If you are adding multiple cards, then you cannot enter a PIN/Password.

4. Turn **Trace** on or off.
Trace provides a record of the person's path through the facility by sending an alarm message to the **Alarm & Events screen** whenever a card with trace enabled is presented at a reader.
5. Select a type of **Usage**.
 - a. If you select **Temporary**, then you must select from the calendar an end date for the temporary card.
 - b. If you select **Limited**, then you must enter the maximum number of accesses granted to the temporary card, between 1 to 255.

6. Select an **Card Type**: Employee, Supervisor, or VIP.

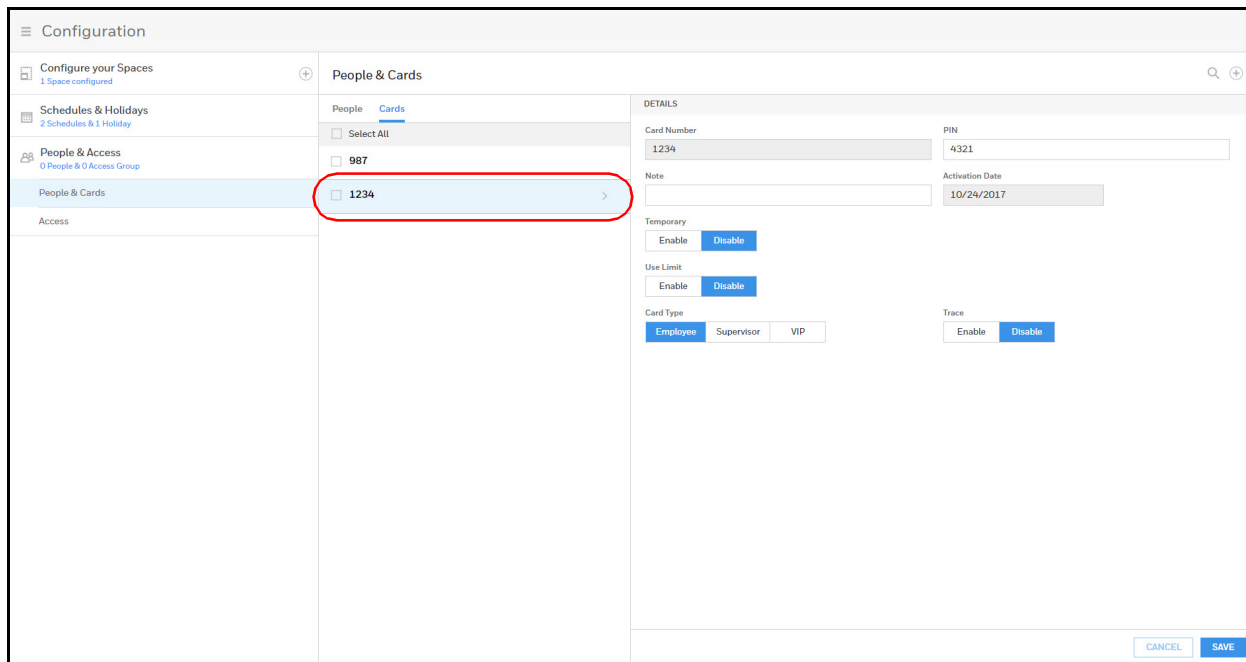
Note: Once a VIP card is added to the database, it can gain access to any door regardless of the access level. VIP card can also bypass Duress, Anti-Passback, Disabled Reader Mode, Duress, Limited Use, Lockdown Reader Mode, Site Code, and Temporary Use.

7. Click **Save**.

Modifying Cards

1. Click to select a card.

Figure 2-45 Modifying a Card



2. Make the changes to the card, then click **Save**.

Deleting Cards


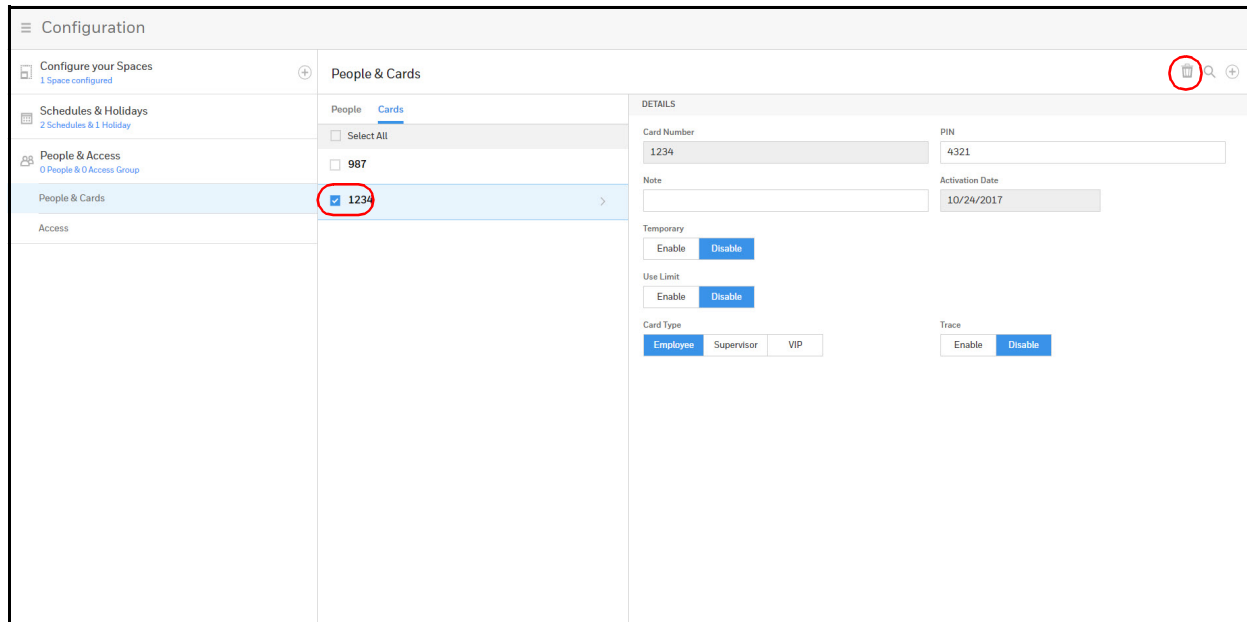

1. Click the box next to the card. A delete icon appears .

Figure 2-46 Deleting a Card



2. Click the delete icon . A confirmation message appears.
3. Click **OK** to confirm the deletion.

Configuring Access Groups

Every card is assigned an access group, which specifies the schedule, or time schedule, during which the card holder can be granted access at a specific door. For example, an access group embedded in an employee's card might allow the employee to enter the facility only through door 2 from 6:00 AM to 6:00 PM, Monday through Friday.

On the Access Groups panel, you can:

- Select Reader A and/or Reader B for each door. Note that if a reader is disabled, then the schedule drop down list for that reader will not be accessible.
- Create an access group.
- Modify an access group.
- Delete an access group.
- Set a Schedule for each door.

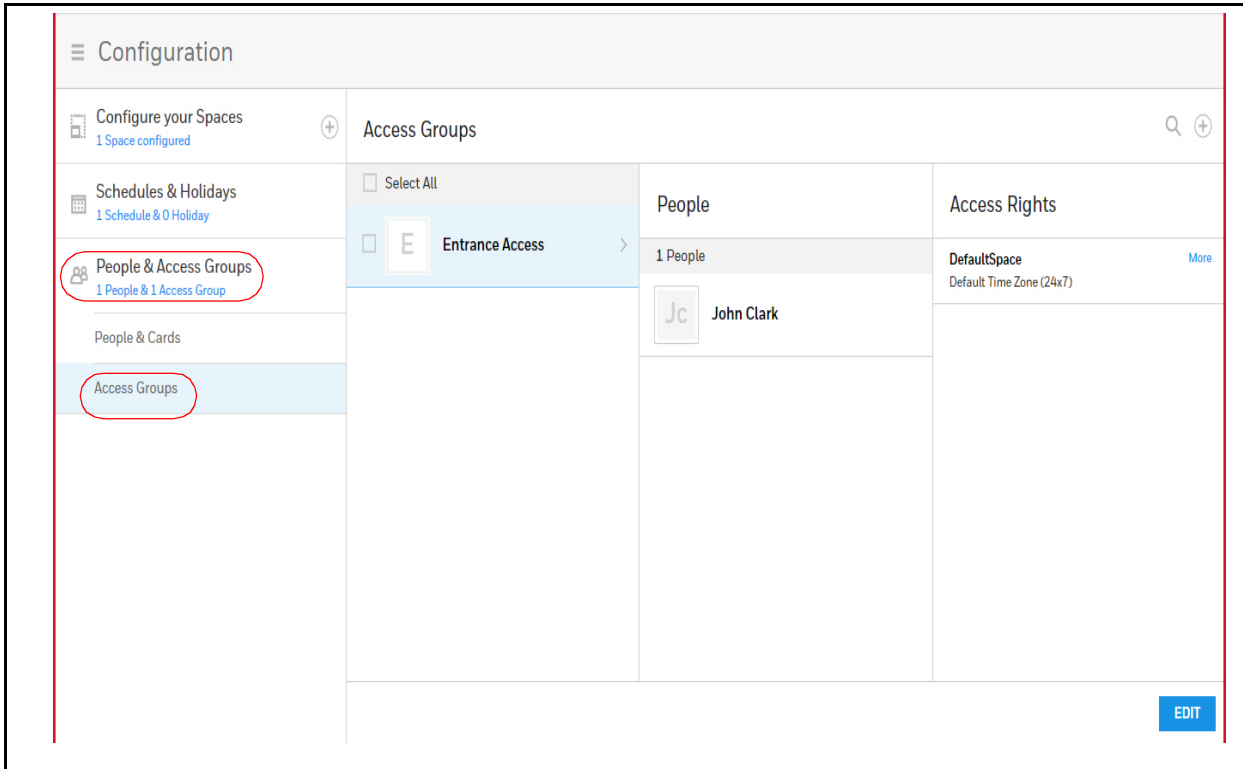
- View other panels with readers in this access group.

Note: Since an access group is defined by door and schedule configurations, you must configure the door (see [Configuring Doors on page 44](#)), people (see [Configuring People section on page 82](#)), and the schedule (see [Entering a Panel Name section on page 42](#)) before configuring an access group.

To navigate to the Access Configuration page, click:

- **Menu > Configuration > People & Access > Access > Create an Access Group**, or
- Access **Groups** in the **Dashboard**, then **Create an Access Group**.

Figure 2-47 Access Group Configuration Page



Creating a New Access Group


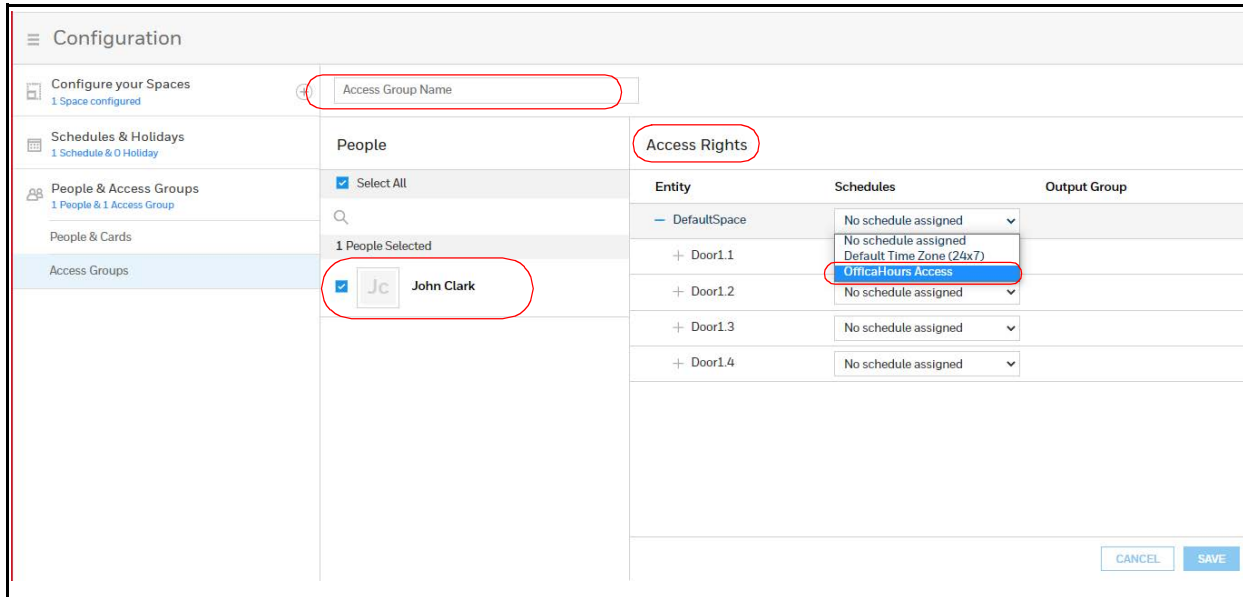
1. Click  to open the new access group configuration panel.

Figure 2-48 Access Group Configuration Page



2. Enter a name in the **Access Group** name field.
3. Click to select **People** for this access group.
4. Click to expand a space/entity to show the doors and readers assigned to that space.
5. Click the drop-down menu to assign a schedule to that door and/or reader.
6. Click **Save** to save the new access group.

Monitoring and Reporting

MPA2C3 allows you to monitor the following:

Alarms

Alarms are events, or system transactions, that are assigned alarm status, including invalid card reads or forced doors.

Events

Events are the recorded system transactions. For example, door statuses, database changes, invalid cards, valid cards.

Doors

Doors are a collection of inputs and outputs connected on the panel that are associated to reader(s).

Inputs

Inputs are terminals located on the panel; the inputs are wired to input devices, such as door-position switches that monitor status of a door.

Outputs

Output relays are relays located on the panel that are connected to output devices, such as a door lock or a siren.

Reports

Future release:Download a CSV file of the People and Cards Report and Alarms &(Web) Events Report. Download a Diagnostic Report as a bin file.

Note: *MPA2C3 has been evaluated for standalone use only. Monitoring features are supplementary only and have not been evaluated by UL.*

Monitoring

Monitoring Alarms and Events

Note: MPA2C3 is listed for access control only. No burglary applications have been investigated.

Alarms

Alarms are system-generated messages that might indicate the need for user attention. To view alarms and events, you have to navigate to the Alarms & Events window.

Events

Events are both panel- and web-generated events. Panel events include the recording of a card read by a reader. Web events include the recording of a user login.

Navigating to the Alarms & Events tab:


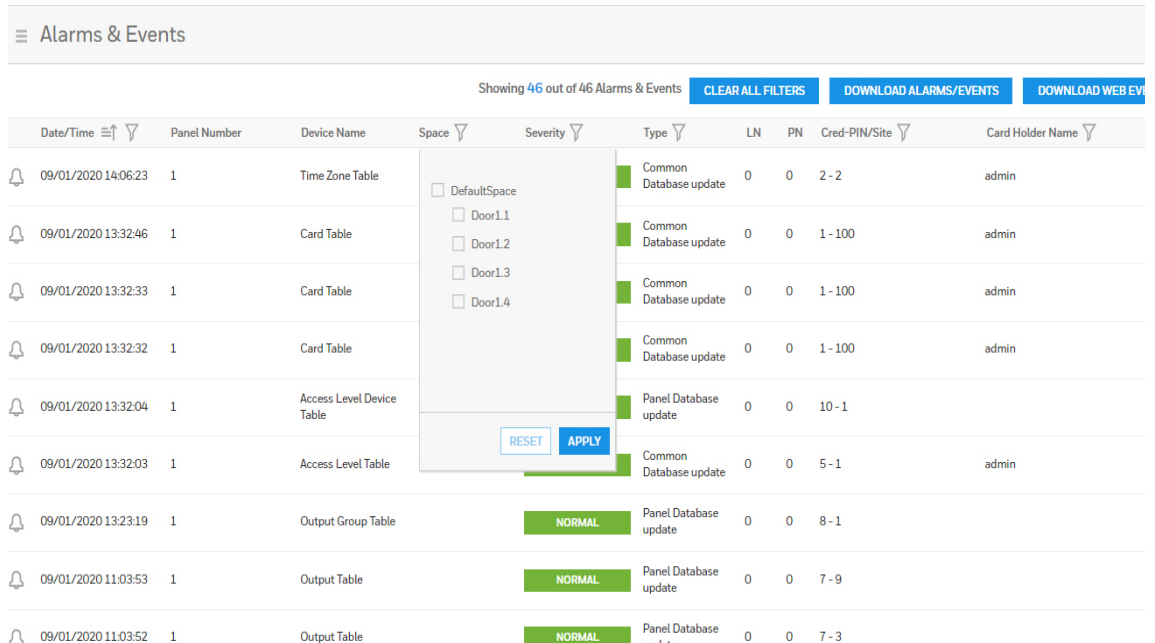
Click  to open the menu, then click **Alarms & Events**. NOTE: Alarms & Events display transactions from all panels in the loop on the same page. The users do not have to go to each panel to see their individual transactions.+

Figure 1-1 2/4-Door Alarms & Events Window



The screenshot shows the 'Alarms & Events' window. At the top, there is a header with a hamburger menu icon and the text 'Alarms & Events'. Below the header, there are three buttons: 'CLEAR ALL FILTERS', 'DOWNLOAD ALARMS/EVENTS', and 'DOWNLOAD WEB EV...'. The main content is a table with the following columns: Date/Time, Panel Number, Device Name, Space, Severity, Type, LN, PN, Cred-PIN/Site, and Card Holder Name. A dropdown menu is open over the 'Space' column, showing a list of checkboxes: 'DefaultSpace', 'Door1.1', 'Door1.2', 'Door1.3', and 'Door1.4'. At the bottom of the dropdown are 'RESET' and 'APPLY' buttons. The table contains several rows of data, including 'Time Zone Table', 'Card Table', 'Access Level Device Table', 'Access Level Table', 'Output Group Table', and 'Output Table'. The 'Severity' column for the last three rows shows 'NORMAL'.

Date/Time	Panel Number	Device Name	Space	Severity	Type	LN	PN	Cred-PIN/Site	Card Holder Name
09/01/2020 14:06:23	1	Time Zone Table			Common Database update	0	0	2-2	admin
09/01/2020 13:32:46	1	Card Table			Common Database update	0	0	1-100	admin
09/01/2020 13:32:33	1	Card Table			Common Database update	0	0	1-100	admin
09/01/2020 13:32:32	1	Card Table			Common Database update	0	0	1-100	admin
09/01/2020 13:32:04	1	Access Level Device Table			Panel Database update	0	0	10-1	
09/01/2020 13:32:03	1	Access Level Table			Common Database update	0	0	5-1	admin
09/01/2020 13:23:19	1	Output Group Table		NORMAL	Panel Database update	0	0	8-1	
09/01/2020 11:03:53	1	Output Table		NORMAL	Panel Database update	0	0	7-9	
09/01/2020 11:03:52	1	Output Table		NORMAL	Panel Database update	0	0	7-3	

Table 3-1 Alarms & Events Fields









Field	Description
	Event/Alarm indicator: Grey = Event Gold = Alarm
Date/Time	Indicates the date and time of the event. Time sort: You can sort the events by most recent or most distant by clicking the up arrow next  to Date/Time in the header Date filter: You can filter by date (the last seven days, the last 30 days, or custom) by clicking the filter icon  next to Date/Time in the header
Panel Number	Indicates the Panel ID if you have more than one panel in a loop.
Device Name	Displays the name of the device that generated the alarm.
Space	Displays the name of the space where the alarm occurred for both 2 Door and 4 Door controllers. Filter by Space: You can filter alarms and events by the space by clicking the filter icon  next to Space in the header.
Severity	Indicates the importance of the event: Normal, Major, or Critical. Normal: Indicates that the panel or device is back online, valid card transactions, the input is back to the normal state, or an output has been used. Major: Indicates an invalid card transaction, such as card not found, invalid format, anti-passback violation, site code violation, time-zone violation. Critical: Indicates that the panel or a device is offline, or that an input is in an alarm state. Filter by Severity: You can filter alarms and events by the severity by clicking the filter icon  next to Severity in the header.

Table 3-1 Alarms & Events Fields

Field	Description
Type	<p>Indicates the type of alarm/event, such as:</p> <ul style="list-style-type: none"> • Normal State • Alarm State • Ajar State • Card Found • Card Not Found • Card Not Found Door Not Used • Card Found Door Used • Input Alarm • FACP Input Alarm <p>Filter by Type: You can filter alarms and events by the type by clicking the filter icon  next to Type in the header. There are 61 event types from which to choose.</p>
LN (Logical Device Number)	<p>A unique number starting at 1 that is assigned to an alarm generating point. This number is never duplicated on a Controller. There is one exception to this: Door Readers.</p>
PN (Physical Device Number)	<p>A number at the board level that is assigned to a specific alarm generating point. MPA2C3 Controller starts at 1 and goes to 8, 1-Door I/O board as a new board goes from 1 to 4, and 2-door I/O board goes from 1 to 8. System alarms, such as a reset, which are not board-specific, will report a value of 0. There is one exception to this: Door Readers.</p>
Cred-PIN/Site	<p>Identifies the card number, and either the PIN or site code number of the card. Reports only events that have an invalid Card Number, invalid Site Code, or invalid PIN. Invalid Cards are reported by themselves. Invalid Site Codes and invalid PINs are reported with the card number that was presented along with them.</p> <p>Filter by Cred-PIN/Site: You can filter alarms and events by the Cred-PIN/Site by clicking the filter icon  next to Cred-PIN/Site in the header, and then entering a card holder number.</p>
Card Holder Name	<p>Reports a Card Holder name on events where the Card Number is an actual card in the system.</p> <p>Filter by Card Holder Name: You can filter alarms and events by the Card Holder Name by clicking the filter icon  next to Card Holder Name in the header, and then entering a card holder name.</p>
Clear All Filters	<p>Click to clear all display filters (Date/Time; Space; Severity; Type; Cred-PIN/Site; Card Holder Name).</p>
Download Alarms/Events	<p>For generating reports. See Reporting section on page 102.</p>
Download Web Events	<p>For generating reports. See Reporting section on page 102. Web Events include logins with invalid passwords and logging in/out, for example.</p>

Monitoring/Managing Doors

The panel supports 2 and 4 doors. The door status screen provides status for each door's egress, status, and tamper and also status of the door lock relay.

The Door Status screen enables you to:

- View the current status of each input (Normal, Alarm, Cut, Short, Unshunt/Shunt).
- Shunt or un-shunt any input. Shunt means that the input's change of state is ignored. This way you can allow a door to be held open without signaling an alarm. The default state of an input point is "unshunted."
- Restore the input to its schedule. A schedule is a specified time period during which the input will be shunted and the alarm deactivated (for schedule management, see [Configuring Time Management](#) section on page 33).
- View the current status of each output (Energized, De-energized).
- Pulse, energize, or de-energize the Door Lock relay.
- Restore the Door Lock to its schedule.

Monitoring Inputs

The panel supports door, panel, and auxiliary inputs. The door inputs provide egress, status, and tamper monitoring. The auxiliary inputs support any monitoring devices connected.

The Input Status screen enables you to:

- View the current status of each input (Normal, Alarm, Cut, Short, Shunt).
- Shunt or unshunt any input. Shunt an input to ignore a change of state. This way you can allow a door to be held open without falsely signaling an alarm. The default state of an input point is "unshunted."
- Restore the input to its schedule. A schedule is a specified time period during which the input will be shunted and the alarm deactivated.

Please Refer Chapter 4 for FACP Monitoring Inputs.

Navigating to the Spaces & Doors tab:


Click  to open the menu, then click **Device Management**.

Figure 1-2 2- Door Device Management Window

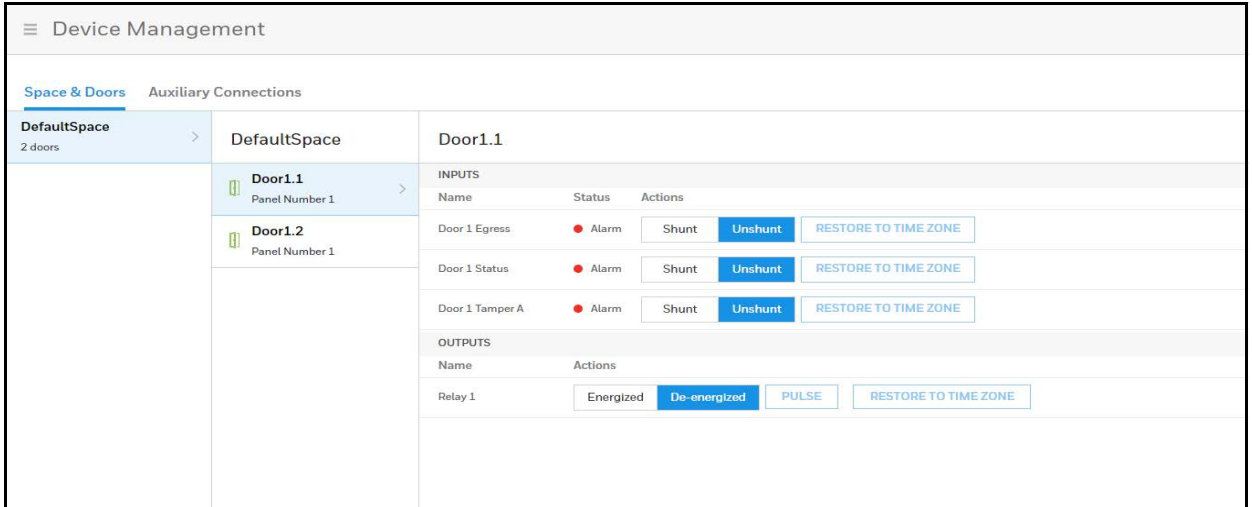
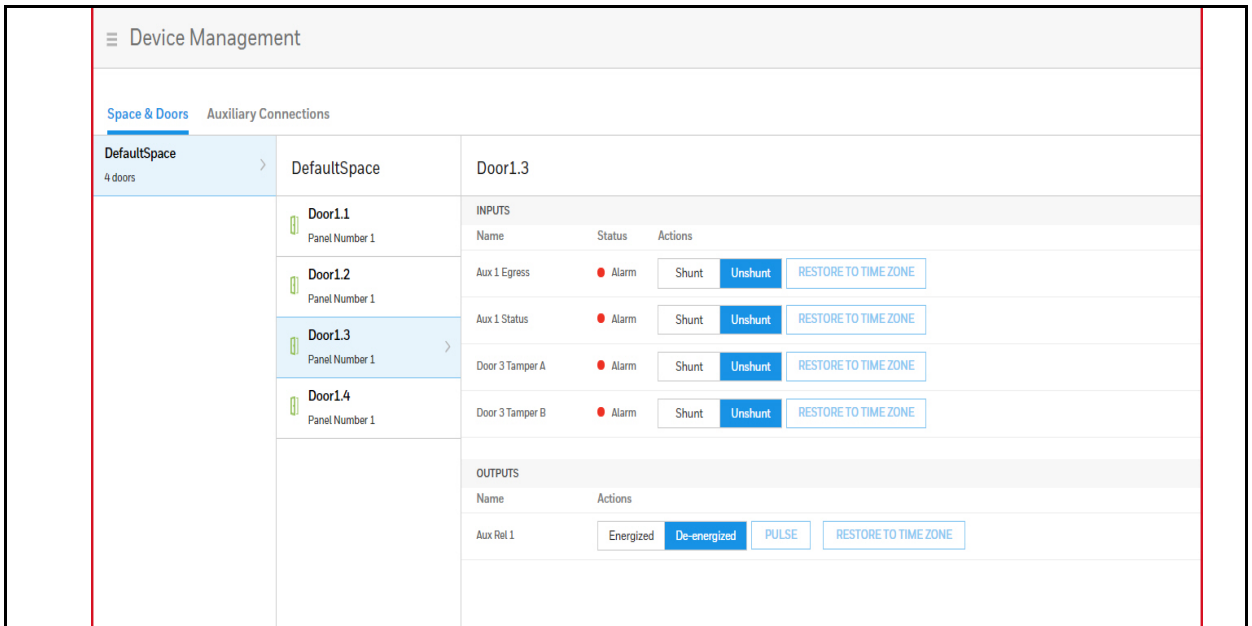


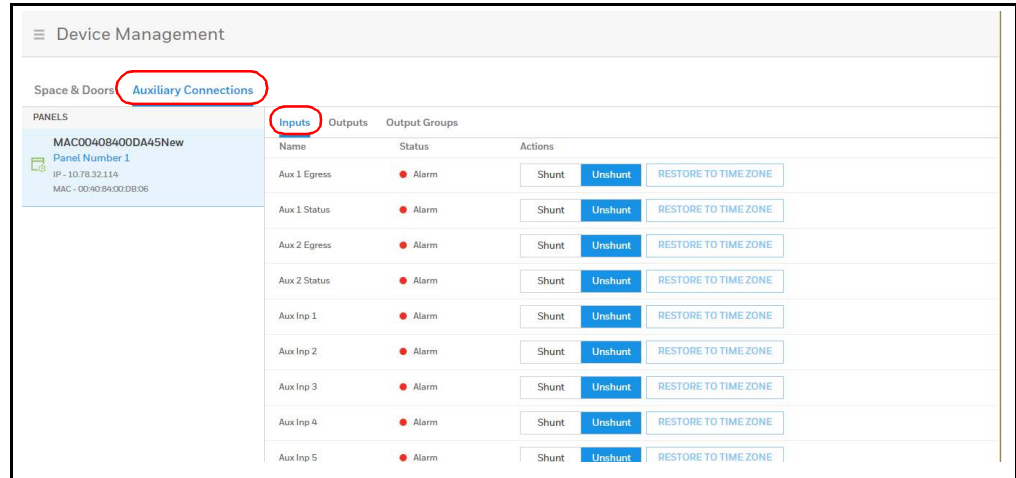
Figure 1-3 4 - Door Device Management Window



Navigating to the Auxiliary Connections-Inputs tab

Click  to open the menu, then click **Device Management > Auxiliary Connections > Inputs**.

Figure 1-4 Device Management Window - Auxiliary Connections - Inputs



Shunting/Unshunting an Input

Shunt an input to manually override a schedule setting.

1. Click either the **Shunt** or **Unshunt** button.
2. Click **OK**.

Restoring the Schedule

1. Click **Restore to Schedule** to restore the input to its shunt state based on its current schedule. A window appears to confirm the action.
2. Click **OK**.

Monitoring and Controlling Outputs

An output is a device that changes state when it is energized, pulsed, or time-zone controlled. For example, a successful card read at a reader pulses a door lock. The lock changes its normally locked state to an unlocked state and the cardholder opens the door.

The panel supports one door output for each of its one to four doors. The panel also supports up to 4 additional auxiliary outputs. For example:

- Door System = 1 Door Output and 3 Aux Output + 4 additional Aux Outputs
- Door System = 2 Door Outputs and 2 Aux Outputs + 4 additional Aux Outputs
- Door System = 3 Door Outputs and 1 Aux Outputs + 4 additional Aux Outputs
- Door System = 4 Door Outputs + 4 additional Aux Outputs

Configuring Outputs

Before you can monitor outputs, they must first be configured. Outputs can be configured individually as discrete outputs (see [Configuring Panel I/O and Groups](#) section on page 46) or collectively as a group of outputs.

Note: *The Pulse and Restore to Schedule buttons only function when an output or a group has a valid pulse time or a schedule assigned.*

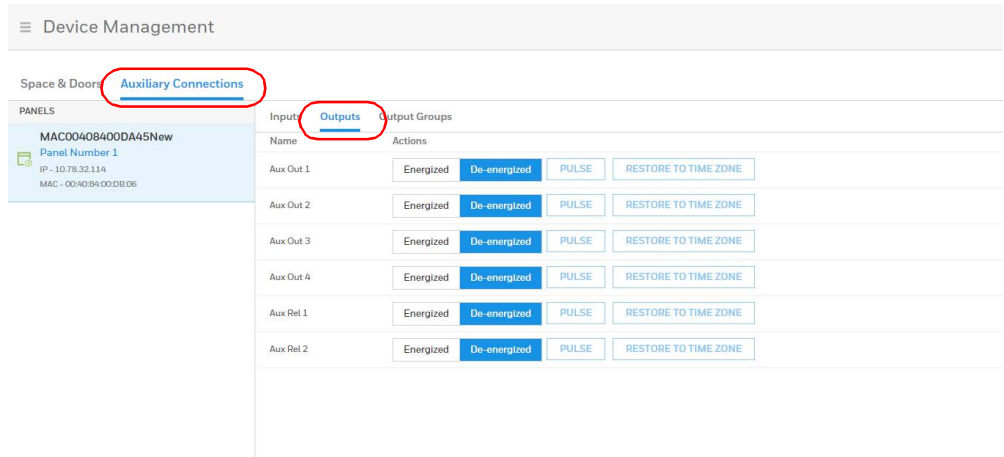
On the Outputs tab, you can do the following:

- View the current status of each output in the Discrete tab (Energized or De-energized).
- View the current status of each group of outputs in the Groups tab.
- Energize or de-energize any output or group indefinitely.
- Pulse any output or group. This energizes the output or group for a configured period of time (see [Monitoring and Controlling Outputs](#) section on page 99).
- Restore the output to its configured schedule. A schedule is a specified time period during which the output will be energized. (see [Entering a Panel Name](#) section on page 31).

Navigating to the Auxiliary Connections-Outputs tab:

Click  to open the menu, then click **Device Management > Auxiliary Connections > Outputs**.

Figure 1-5 Device Management Window - Auxiliary Connections - Outputs



Note: *The Output Status screen dynamically refreshes when the output status changes.*

Table 3-2 Output Management Settings

Field	Description
Energized	Click to energize an output for an indefinite period of time.
De-energized	Click to de-energize an output for an indefinite period of time

Table 3-2 Output Management Settings

Field	Description
Pulse	Click to pulse an output for the configured period of time.
Restore to Time Zone	Click to reset the output to follow its configured time zone.

Monitoring and Controlling Output Group

Configuring Output Groups

Before you can monitor output groups, they must first be configured. See [Configuring Panel I/O and Groups](#) section on page 46), and select **Group** when configuring the output.

Navigating to the Auxiliary Connections-Output Groups tab:

Click  to open the menu, then click **Device Management > Auxiliary Connections > Output Groups**.

Figure 1-6 Device Management - Auxiliary Connections - Output Groups

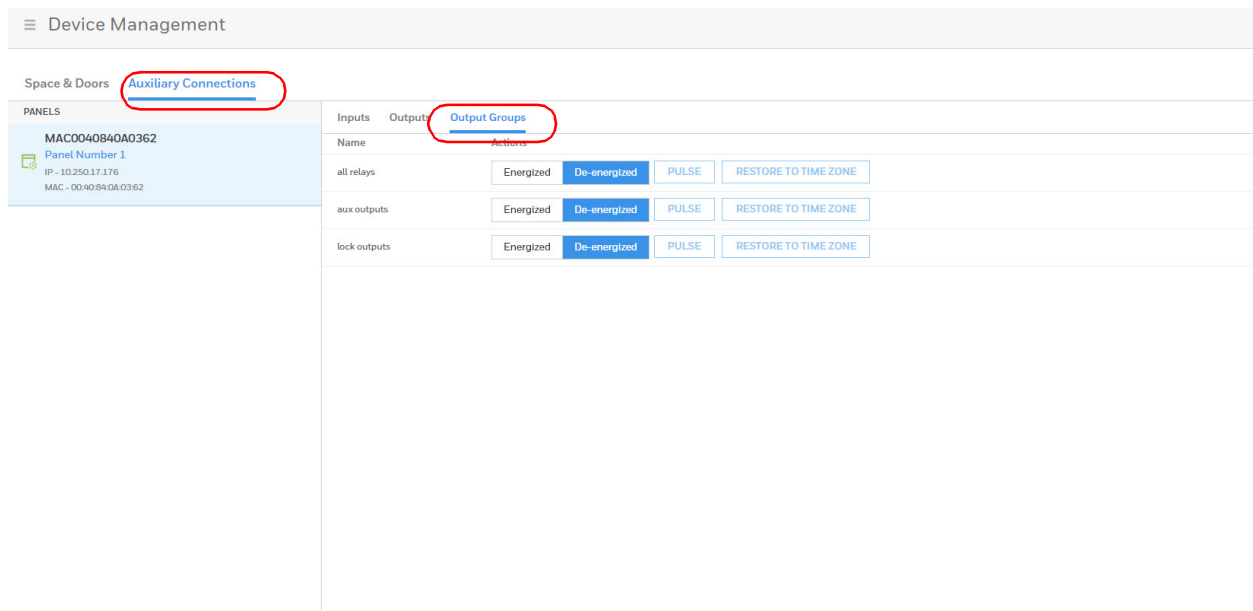


Table 3-3 Output Groups Management Settings

Field	Description
Energized	Click to energize an output for an indefinite period of time.
De-energized	Click to de-energize an output for an indefinite period of time.

Table 3-3 Output Groups Management Settings

Field	Description
Pulse	Click to pulse an output for the configured period of time.
Restore to Time Zone	Click to reset the output to follow its configured time zone.

Reporting

Generating Event Reports

On the Alarms & Events window, you can download **Alarms/Events** or **Web events**.


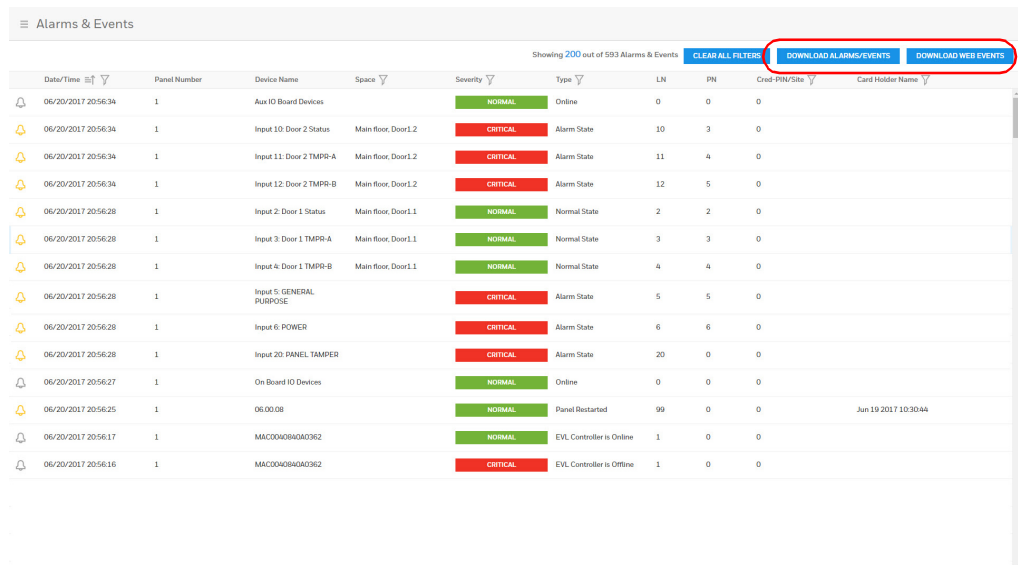
1. Click  to open the menu, then click **Alarms & Events** or **Web Events**.

Figure 1-7 2/4- Door Alarms & Events Window



The screenshot shows the 'Alarms & Events' window. At the top right, there are three buttons: 'CLEAR ALL FILTERS', 'DOWNLOAD ALARMS/EVENTS', and 'DOWNLOAD WEB EVENTS'. The 'DOWNLOAD ALARMS/EVENTS' button is circled in red. Below the buttons is a table with the following columns: Date/Time, Panel Number, Device Name, Space, Severity, Type, LN, PN, Card-PIN/Site, and Card Holder Name. The table contains several rows of event data, including 'Aux IO Board Devices', 'Input 10: Door 2 Status', 'Input 11: Door 2 TMPR-A', 'Input 12: Door 2 TMPR-B', 'Input 2: Door 1 Status', 'Input 3: Door 1 TMPR-A', 'Input 4: Door 1 TMPR-B', 'Input 5: GENERAL PURPOSE', 'Input 6: POWER', 'Input 20: PANEL TAMPER', 'On Board IO Devices', '060008', 'MAC0048A0A0362', and 'MAC0048A0A0362'.

Date/Time	Panel Number	Device Name	Space	Severity	Type	LN	PN	Card-PIN/Site	Card Holder Name
06/20/2017 20:56:34	1	Aux IO Board Devices		NORMAL	Online	0	0	0	
06/20/2017 20:56:34	1	Input 10: Door 2 Status	Main floor, Door1.2	CRITICAL	Alarm State	10	3	0	
06/20/2017 20:56:34	1	Input 11: Door 2 TMPR-A	Main floor, Door1.2	CRITICAL	Alarm State	11	4	0	
06/20/2017 20:56:34	1	Input 12: Door 2 TMPR-B	Main floor, Door1.2	CRITICAL	Alarm State	12	5	0	
06/20/2017 20:56:28	1	Input 2: Door 1 Status	Main floor, Door1.1	NORMAL	Normal State	2	2	0	
06/20/2017 20:56:28	1	Input 3: Door 1 TMPR-A	Main floor, Door1.1	NORMAL	Normal State	3	3	0	
06/20/2017 20:56:28	1	Input 4: Door 1 TMPR-B	Main floor, Door1.1	NORMAL	Normal State	4	4	0	
06/20/2017 20:56:28	1	Input 5: GENERAL PURPOSE		CRITICAL	Alarm State	5	5	0	
06/20/2017 20:56:28	1	Input 6: POWER		CRITICAL	Alarm State	6	6	0	
06/20/2017 20:56:28	1	Input 20: PANEL TAMPER		CRITICAL	Alarm State	20	0	0	
06/20/2017 20:56:27	1	On Board IO Devices		NORMAL	Online	0	0	0	
06/20/2017 20:56:25	1	060008		NORMAL	Panel Restarted	99	0	0	Jun 19 2017 10:30:44
06/20/2017 20:56:17	1	MAC0048A0A0362		NORMAL	EVL Controller is Online	1	0	0	
06/20/2017 20:56:16	1	MAC0048A0A0362		CRITICAL	EVL Controller is Offline	1	0	0	

When you click on one of the download events buttons, a dialog box pops up to advise that the file you are downloading is not secure, and that you save that file in a secure location. It then asks for you to confirm that you want to download filtered Alarms/Events or Web Events.

1. Click **OK** to confirm.

An excel spreadsheet report is generated and appears in the lower toolbar of your browser.

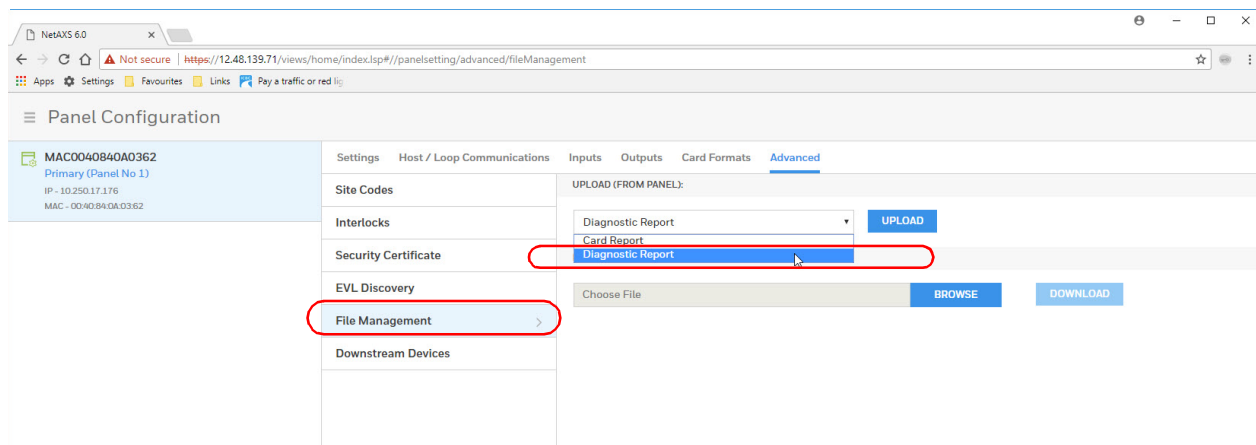
2. Click to open the report in Excel.

Generating Diagnostic Reports

In the File Management window, you can download **Card** and **Diagnostic** reports.

1. Navigate to the File Management window: Click **Panel Configuration > Advanced > File Management**.

Figure 1-8 File Management Window




2. Select **Diagnostic Report** from the drop-down menu, then click **UPLOAD**.
3. When you click on **UPLOAD**, a dialog box pops up to advise that the file you are downloading is not encrypted and that it might contain sensitive configuration and cardholder data. It then asks for you to confirm that you want to upload the report.
4. Click **OK** to confirm.
5. A .bin file is generated which can be saved and sent to Honeywell technical support for diagnosis.
6. Click to save the file in a secure location of your choice.

Generating People/Card Reports

1. Navigate to the People & Cards page: **Configuration > People & Access > People & Cards.**

Figure 1-9 Generating a People/Card Report

The screenshot shows the 'People & Cards' configuration page. On the left, there is a navigation menu with 'People & Cards' selected. The main area is divided into two columns. The left column displays a list of people with checkboxes and initials: Aaron Barbe (Ab), B. Allen (Ba), Dulce Sanchez (Ds), H. Tom (Ht), Jim Smith (Js), John Abrams (Ja), and Maria Infante (Mi). The right column shows the 'DETAILS' form for Aaron Barbe, with fields for First Name (Aaron) and Last Name (Barbe). Below this is the 'CARD' section with fields for Card Number and PIN, and checkboxes for Temporary, Use Limit, and Card Type (Employee, Supervisor, VIP). A download icon (a downward arrow) is circled in red in the top right corner of the page. At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

2. Click the download button  in the top right corner.
3. You see a message confirming that you want to download a People/Cards report.
4. Click **OK**.
5. A comma-separated values (.CSV) report is generated and appears in the lower toolbar of your browser.
6. Click to open the report in Excel.

Configuring FACP input functionality

FACP input functionality

The MPA2C3 has a dedicated fully hardware controlled FACP (Fire Alarm Control Panel) input, intended to unlock all doors when triggered with the highest priority, overriding any current access control setting.

When connected to a Fire system and there is a fire alarm, this function allows people to easily evacuate a premises and allows first responders to easily enter unlocked areas.

To make this function fully effective hardware AND software configuration need to be made on the MPA2C3.

Door Access Modes

By default the MPA2C3 is a normal access control panel, operating in Normal Door Access Mode. The operation and control of the outputs are for access control use. This mode sets the Door Relays (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) in fail-secure operation.

Note: *Door outputs or relays (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) apply to both Push in terminal blocks and all 4 red Door/AUX RJ45 terminals.*

In Normal Door Access Mode all Door Relays (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) are de-energized when the door is supposed to be locked. To unlock a door the Door relay must be in energized state.

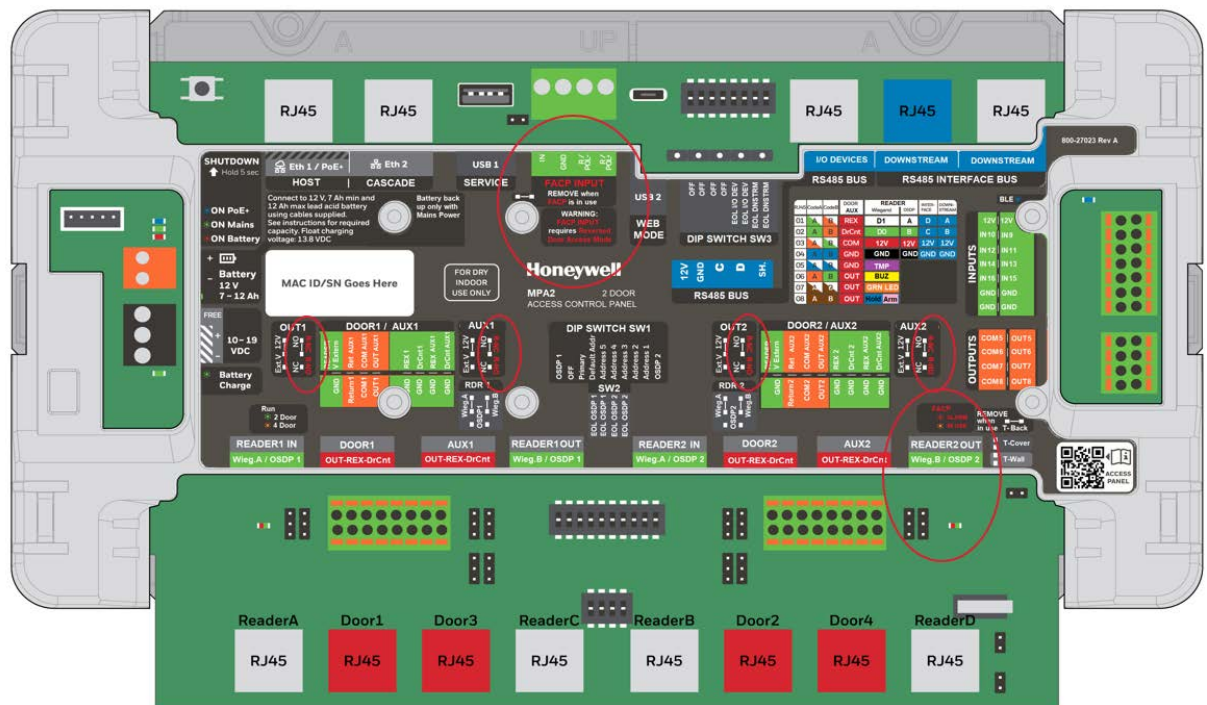
When additionally, the doors must be unlocked when e.g. a Fire Alarm occurs, then MPA2C3 panel must be in Reversed Door Access Mode. This mode sets the Door Relays (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) in fail-safe operation. See further about the conditions and Door Output states in fail-safe operation.

In Reversed Door Access Mode all Door Relays (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) are energized when the doors are supposed to be locked. To unlock a door the Door Relay must be in de-energized state.

Door access mode indication

On the panel's information card Normal Door Access Mode functions are described in wording in WHITE. Where wording in RED is available at some functions (e.g. OUT / AUX R-NO/R-NC jumpers) AND Reversed Door Access Mode has been activated, then the wording in Red must be considered.

In the figure below, identify the wording in RED for Reversed Door Access Mode indicators.



When Reversed Door Access Mode is activated, the amber FACP LED is ON, indicating that FACP LED is in use.

Note: The amber FACP LED (in use) will not turn on automatically when the FACP jumper has been removed.



In the Web User Interface there are many references to Door Access Modes.
 In sections 4.3 and further

Door Access Modes and Door lock behaviors

The below table describes the Door Status per Normal or Reversed Door Access Mode.

MPA2C3		Fail-Secure Installation	FAIL-SAFE INSTALLATION
Scenarios		DOOR STATUS 1-4 OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2))	
PANEL	DOOR ACCESS MODE	NORMAL	REVERSED
NORMAL OPERATION		LOCKED with functional operator control/ card swipes/ schedules	
POWER LOSS	P R I O R I T Y 	Panel Power loss (12v Internal powered lock)	LOCKED, non functional operator control/ card swipes/ door schedules
		External PSU for locks Power loss	UNLOCKED, non functional operator control/ card swipes/ door schedules
		Panel Power loss with External PSU for locks operational	
FACP	FACP input triggered (Fire alarm)		
	FACP input idle.	LOCKED with functional operator control/ card swipes/ schedules	

APPLICATION / USE CASE	Fail-Secure Access Control w/ door strikes - At power loss doors will lock, - For all doors not requiring evacuation mode	Fail-Safe Access Control w/ mag locks: - At power loss doors will unlock, - For inner doors, corridor doors, - Where escape route needed - First responders to easily enter
Other System Prerequisites	Use Power-to-lock Door locking devices, such as door strikes	Use Power-to-Unlock Door locking devices, such as magnetic locks

FACP input prerequisites

The MPA2C3 has a dedicated fully hardware controlled FACP (Fire Alarm Control Panel) input. When triggered the panel overrides immediately and simultaneously the 4 door outputs (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) to a Fail-safe state (door unlocked state*). AUX REL 5,6,7 and 8 are NOT affected hardware wise by the FACP input. See the installation manual for FACP installation.

Note: *Individual doors cannot be selected to be fail-safe or fail-secure. All door outputs are affected.*

When the FACP input is activated:

- All door outputs (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) are in safe condition (safe = off = unlocked door* = free egress).
- None of the door outputs (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) can be controlled by card readers, egress buttons or access control software.
- There is a notification in the Web UI that the FACP input has been activated. Host software will be notified.

To achieve the above functionality the panel needs to be set to the Reversed Door Access Mode. In Reversed Door Access Mode the Door Outputs (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) are reversed.

In Reversed Door Access Mode all Door Relays (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) are energized when the doors are supposed to be locked. To unlock a door the Door relay must be in de-energized state.

Always test the full end to end functionality of the FACP input and the effect to the doors (not only the outputs) after the installation has been completed.

- FACP input not activated: Doors 1 to 2/4 function as access-controlled doors, using cards, egress or software/Web User Interface.

- FACP input activated: Doors 1 to 2/4 are and stay in unlocked state, and controls are not possible using cards, egress or software/Web User Interface

Note: See the MPA2C3 installation manual how to connect the Fire panel output to the MPA2C3 in chapter XYZ, and how to connect the outputs the to fail safe locking devices (power-to-lock), with the correct jumper settings of (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)).

Note: Jumper head on FACP jumper needs to be off when the FACP input is in use and to un-bypass the FACP input.

Note*: Fail safe locking devices (power-to-lock) are devices that unlock when power (voltage) is interrupted to the locking device. This interruption can be done by opening a NC (Normally Closed) contact of a relay (door) output via the controls of the panel or when power to the panel or to the locking device is lost. Main examples for fail safe locking devices are magnetic locks.

FACP input set up procedure- FAIL-SAFE INSTALLATION

The below procedure is to create a fail-safe installation. Any diversion from these steps will make the installation not fail-safe (unlock doors at power fail and at FACP input triggered).

To make sure all door outputs are in a fail-safe mode, the panel needs to be in Reversed Door Access Mode. There are 5 steps to make the FACP input fully functional.

1. Set panel in Reversed Door Access Mode

In Panel configuration/advanced/FACP Input:

- a. Go to section DOOR OUTPUT OPERATION:
 - Select DOOR ACCESS MODE: REVERSED

Panel Configuration

MAC0040840A0362
Primary (Panel No 1)
IP - 10.250.17.176
MAC - 00:40:84:0A:03:62

Settings Host / Loop Communications Inputs Outputs Card Format **Advanced**

Site Codes

Interlocks

Security Certificate

EVL Discovery

File Management

Downstream Devices

FACP Input

DOOR OUTPUT OPERATION

DOOR ACCESS MODE
NORMAL REVERSED

Select Reverse when FACP input is in use and connected

Reversed Door Access mode:

- Select "REVERSED" when FACP Input is in function and FACP jumper has been removed.
- Door outputs OUT1, OUT2, OUT3 (AUX1) and OUT4 (AUX2) are in reversed state.
- Install Magnetic locks or Power-to-lock locking devices in Fail-Safe installations.
- Consider R-NC jumper when connecting Power-to-lock locking devices.
- In Fail-Safe installations the doors unlock immediately at FACP activation and at panel power loss.

FACP Input:

- FACP Input controls Door Outputs OUT1, OUT2, OUT3 (AUX1) and OUT4 (AUX2) immediately.
- FACP Input controls Door Outputs with highest priority, not affected by FACP Input parameters below.
- An FACP Input alarm forces the Doors Outputs to unlocked state.
- An FACP Input alarm makes card read, timezone and operator control nonfunctional.
- FACP Input parameters are for Interlock and Report function only.
- Auxiliary Outputs OUT5, OUT6, OUT7, OUT8 are not affected by the FACP input.

Normal Door Access mode:

- Select "NORMAL" for default access control operation without FACP Function
- Relay outputs OUT1, OUT2, OUT3 (AUX1) and OUT4 (AUX2) are in normal state
- Consider NO or NC jumper when connecting locks, depending on the type of locks used.
- FACP Input cannot and must not be used, keep the FACP Jumper on.

GENERAL For Interlocks and Report only

Name
FACP Input

SHUNT AND DEBOUNCE

Shunt Time (H:M:S) 0 0 0 Debounce Time (sec) 0

SCHEDULING

Shunt Choose a Schedule Disable Interlocks Choose a Schedule

2. Click Save

On the panel the Amber FACP LED will be ON and all Door Relays will be energized state (if the door outputs are in idle locked mode).



3. Reposition the OUT/AUX NO/NC jumper on all Outputs.

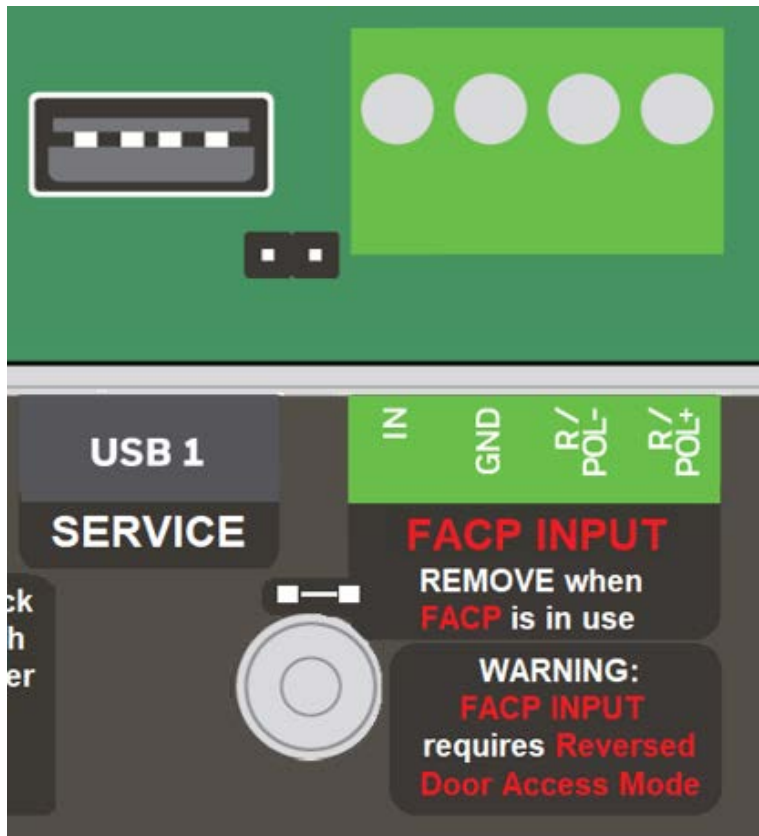
On the Panel, regard all (OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) relay outputs modes on the panel as reversed.

- a. Set the Jumperhead to the Red R-NC (Normally Closed in Reversed Door Access Mode)
- b. This is the correct setting to connect power-to-lock locking devices (such as magnetic locks) to the output.



4. Remove the jumperhead from the FACP jumper.
Hardware activate the FACP input on the panel and unbypass the FACP input.

Note: The amber FACP LED (in use) will not turn on automatically when the FACP jumper has been removed.



5. Connect the fire output wiring to the FACP input.

See the installation manual for the correct wiring of the FACP input.

FACP settings for Interlocks and Reporting only

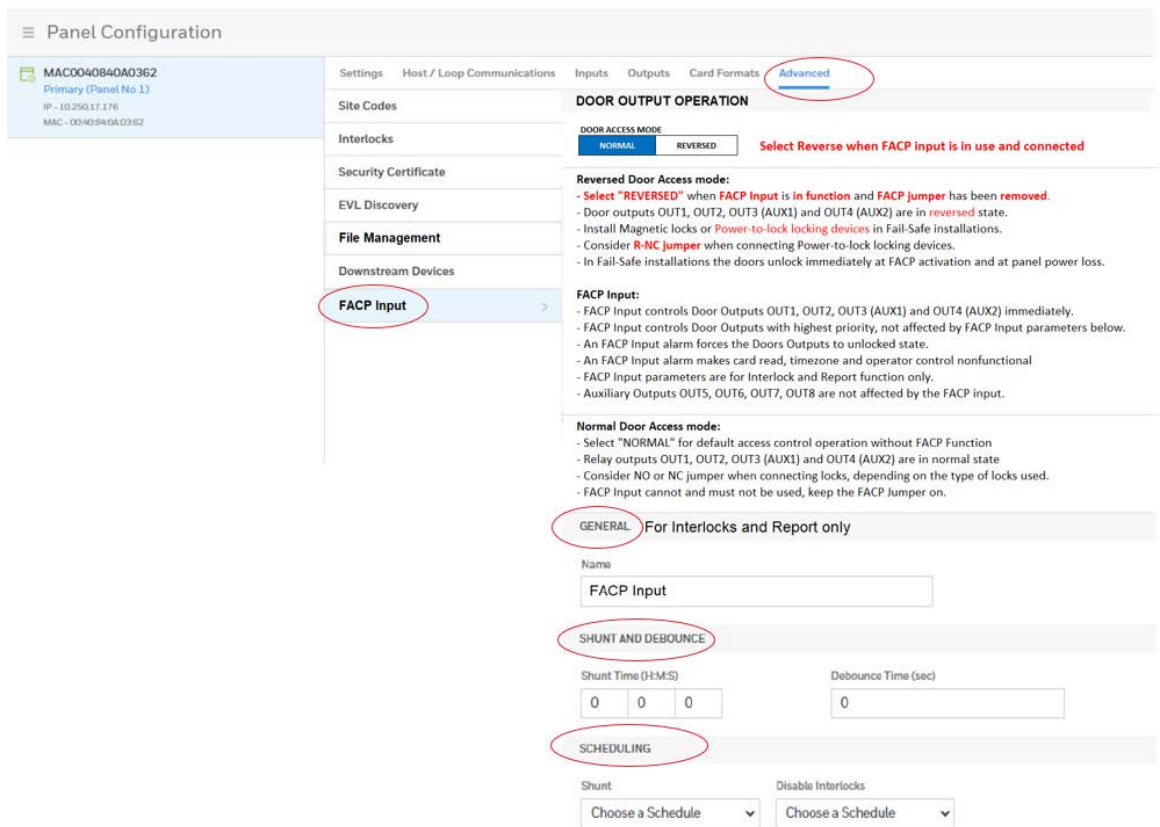
The section GENERAL, SHUNT AND DEBOUNCE and SCHEDULING have no effect on the triggered FACP input unlocking all doors at all. E.G a shunted or debounced value in this section will not shunt or delay all the door outputs to fail-safe state (de-energized)

The GENERAL, SHUNT AND DEBOUNCE and SCHEDULING sections allows you to configure the following settings:

- Input Name
- Shunt and Debounce
- Scheduling

Define the FACP input reporting features.

- Specify the FACP input shunt time, or the period of time the state of the FACP input will be ignored (only for reporting - interlocking).
 - Specify the FACP input debounce time, or the period of time the FACP input must remain in its new state before it is recognized as being in the new state (only for reporting).
 - Specify the FACP input schedules.
1. In Panel configuration/advanced/FACP Input, Go to section General – For Interlocks and Report only.



2. Enter an **Input Name**.
3. Configure Shunt and Debounce times.

Configuration	Description
Shunt Time (h:m:s)	Specifies the amount of time for which the FACP input is shunted, or de-activated for reporting/interlocking. The maximum length of time is 1 hour, 45 minutes, 59 seconds. You can express seconds in tenths of a second.
Debounce Time (h:m:s)	Specifies the period of time (MIN = 0 second, MAX = 6553.5 seconds) the FACP input must remain in a new state before generating an alarm (in reporting and for interlocking only). For example, with a 5-second debounce time selected, if a Normal state is changed to Alarm, the state must remain in Alarm for five consecutive seconds before an alarm is generated.

4. Configure Scheduling.

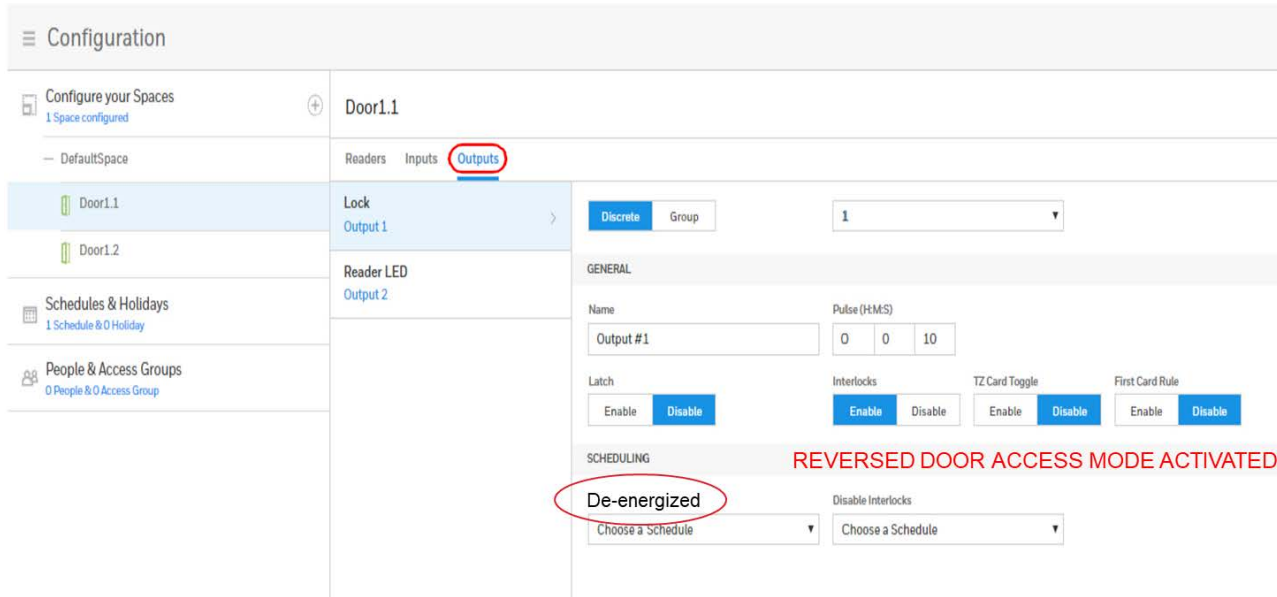
Configuration	Description
Shunt	Specifies the time period during which the state of the FACP input will be ignored for reporting.
Disable Interlocks	Specifies the time period during which the programmed action on the FACP input from another point will be disabled.

Configurations during Reversed Door Access Mode

Because the Reversed Access Door Mode is activated, the door outputs OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) are in reversed state.

In Configuration/Configure your Spaces/Door/Outputs/Scheduling, the De-Energized schedule is now to reflect the schedule to unlock the door during that schedule.

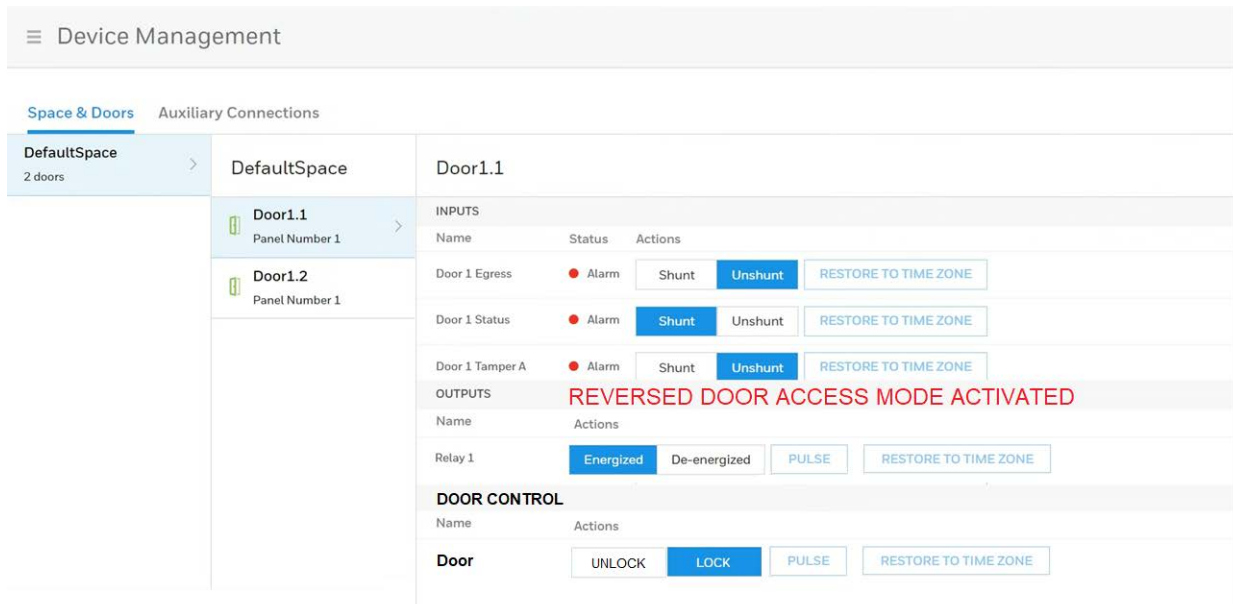
When an MPA2C3 panel is set later for Reversed Door Access Mode, then this will automatically change and scheduled. Please regard the correct locks.



Controlling Doors in Reversed Door Access Mode

Because the Reversed Access Door Mode is activated, the door outputs OUT1, OUT3 (AUX1), OUT2, OUT4 (AUX2)) are in reversed state.

In Device Management, the idle door locked state is now reflected as Door Relay Energized.



To unlock the door from the User interface in Reversed door access mode, the door relay must be set to “De-energized”

The Pulse button will de-energize the Door relay for the specified time.

The Door Control section remain the same, lock and unlock functions are reflecting the door status and not the relay status.

FACP input activation in Alarm-Notifications

Notifications on the panel

When the connected Fire alarm control panel is in alarm and the Fire panel output has activated the FACP input on the panel, on the MPA2C3 panel the RED FACP LED (Alarm) is ON. (Only for service purposes)



Notifications in the Web User Interface

On every screen of the Web User Interface the following message will appear

**%FACP input% activated.
Door outputs of Panel %1, %2 ... %32 are in unlocked state.
Controls have no effect on Door 1, Door 2, Door 3 (Aux1) and Door 4 (Aux2)**

%FACP Input% is the name of the input given in Panel Configuration/Advanced/FACP Input/General.

In multi panel configurations the panel numbers are indicated where the Fire input has been activated.

In Device Management you can see the below screen.

The screenshot shows the 'Device Management' interface. At the top right, a red notification box contains the text: '%FACP input% activated. Door outputs of Panel %1, %2 ... %32 are in unlocked state. Controls have no effect on Door 1, Door 2, Door 3 (Aux1) and Door 4 (Aux2)'. Below this, the 'Space & Doors' section is visible. A red vertical bar with a circled '1' highlights the 'DefaultSpace' (3 doors) in the left sidebar. Another red vertical bar with a circled '2' highlights the 'Door1.1' (Panel Number 1) in the main list. The 'Door1.1' details are shown on the right, including 'INPUTS' (Door 1 Egress, Door 1 Status, Door 1 Tamper A) and 'OUTPUTS' (REVERSED DOOR ACCESS MODE ACTIVATED, DOOR CONTROL CONTROLS HAVE NO EFFECT with a circled '3', Door). The 'DOOR CONTROL' section shows 'Name' and 'Actions' (UNLOCK, LOCK, PULSE, RESTORE TO TIME ZONE).

1. In Spaces & Doors, per Space a red indicator highlights the space where the FACP has been triggered
2. In the highlighted Space another red indicator highlights the doors affected by the FACP input alarm.
3. In Door Control a message in red wording appears:
4. CONTROLS HAVE NO EFFECT

Although you can change the status of the Door or Relay, these changes have no effect and the door will remain in unlocked state.

Other controls such as (Supervisor) Card swipes, Schedules and Auto-relock have no effect and the door will remain in unlocked state.

When the FACP input is back in normal condition, all applied changes will take effect, and the panel continues working as an access control panel.

Maintenance

Overview

This chapter contains:

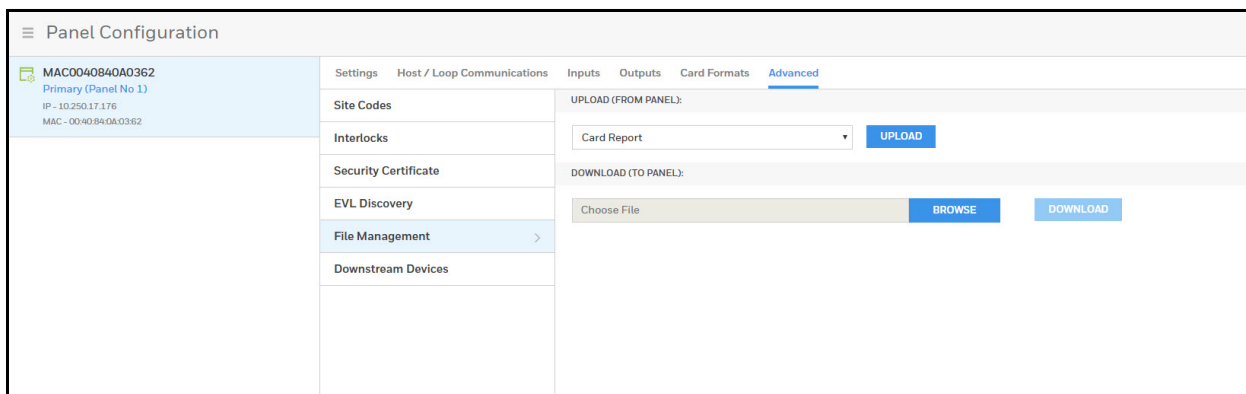
- System-wide backup
- Panel Resets and Restorations
- Firmware Upgrades
- Primary / Secondary Panel Replacement Use Case Scenarios
- Primary / Secondary Panel Hard Default Use Case Scenarios

Backing Up

Navigate to the File Management interface:

1. Select a panel from the **Panel Configuration** interface.
2. Click **Menu > Panel Configuration > Advanced > File Management**.

Figure 1-1 File Management Interface



Upload (From Panel)

I. Primary Panel Upload

From the primary panel's UPLOAD menu under File Management tab, it will list following three options from drop-down list to upload from Panel,

- Diagnostic Report
- Card Report
- System-wide Backup

II. Secondary Panel Upload

From any secondary panel's UPLOAD menu, it will list following two options from drop-down list,

- Diagnostic Report
- Card Report

Backing Up (or Uploading) Other Data from the Panel to the Host System

Card Report

Uploads the Card Number, Last Name, First Name, Trace, VIP, Limited Use, Card Expiration, Temporary, Supervisor, Access Groups, Site Codes, Number of Bits, Pin, Info 1, Info 2, Schedules, Activation Date, Issue Level, APB State, and Control Device card values in a .CSV file.

Note: Card report (short and long) data is stored in a 64-bit format. Microsoft Excel displays up to 32 characters. Therefore, you should save the report and then open it in Notepad, instead of opening the report immediately in the default .CSV format in Excel.

Diagnostic Report

Troubleshooting information can be retrieved from the panel using this function. The report is not readable to the customer and is useful only as a tool to help Honeywell technical support troubleshoot certain unusual problems.

To generate a diagnostic report,

1. Select "Diagnostic Report" from the Upload drop-down menu on File Management screen.
2. Click Upload button.

3. Save the file when prompted to do so.

Note: The Diagnostic Reports saves as a .bin file.

System-wide Backup

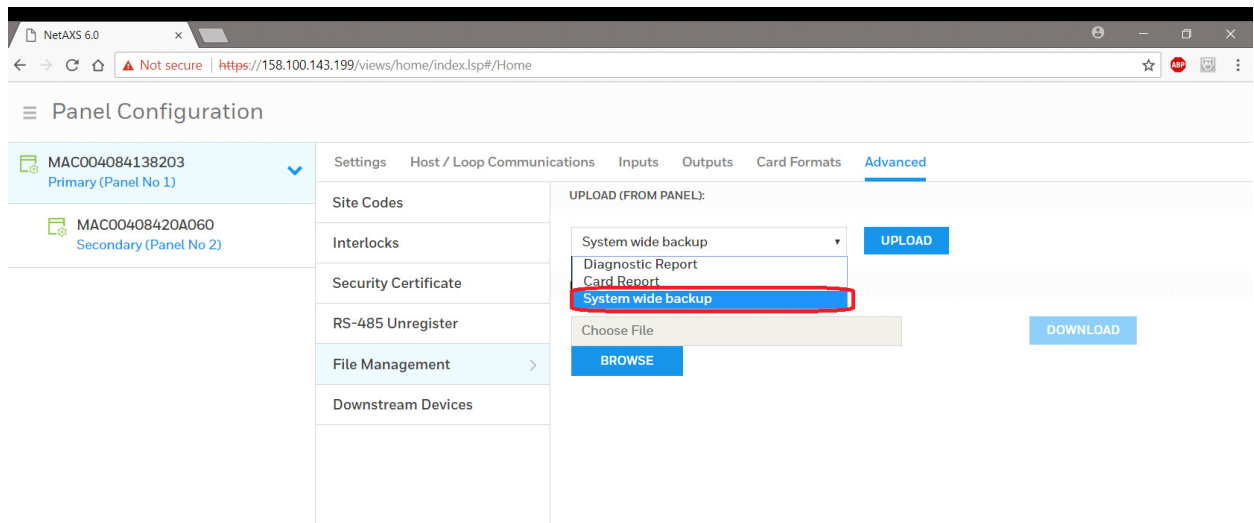
Uploads Card, Common and Panel configuration data in a proprietary internal format.

Common data includes:

- Schedules
- Cards
- Card Formats
- Holidays
- Access Group Name (access group details are panel-specific)
- Configuration (Site Codes)

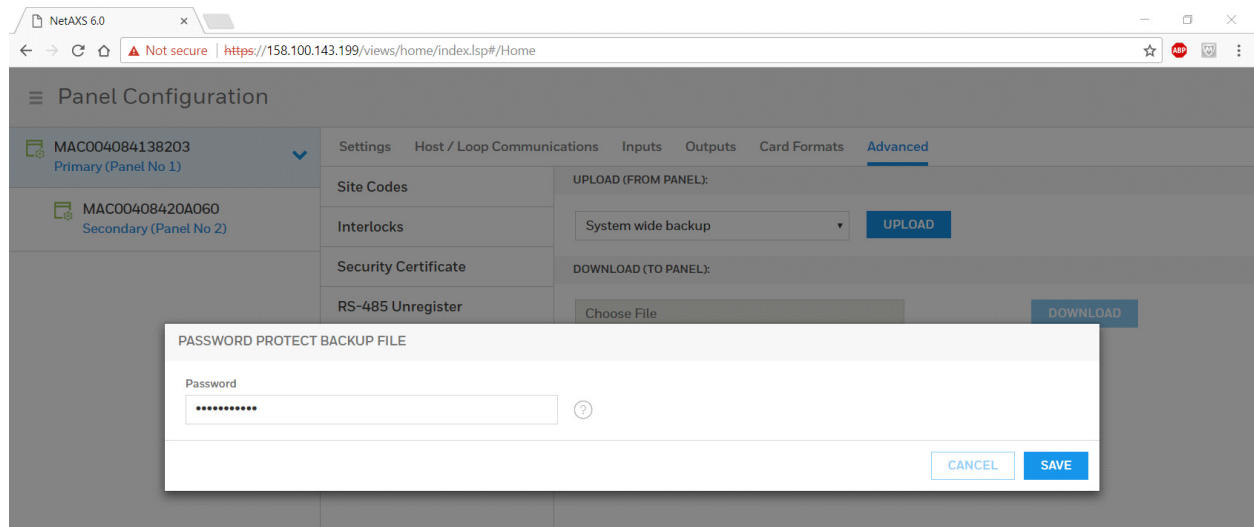
Panel-specific data includes:

- Access Group Schedule Reader Assignments
- Space/Door/Reader Configuration
- Panel Configuration (General)
- Panel Configuration (Firmware Version)
- Panel Configuration (Network) (IP addresses apply only to primary panel)
- Panel Configuration (Host/Loop Communications) (applies only to primary panel)
- Web Users (applies only to primary panel)



Taking System-wide Backup for panel(s) is only allowed from Primary (gateway) panel's file management page.

- Upon selecting system wide backup, UI will show a field to enter password
- Password Must follow rules for valid password checks - need not be same as current user/admin password:



- Click save button the spinner will show while Primary panel is getting configuration data from the Secondary panels.

Note: The Backup file saves as a .bkp file.

Download (To Panel)

Following types of downloads are allowed from File Management sections

- Firmware (.bin file)
- Card Report (.csv file)
- Backup file (.bkp file)

Firmware Download

To restore (or download) firmware to a panel:

1. Select a Panel first, on which you want to download firmware from Panel Configuration menu.
2. Click Browse to locate the firmware file.
3. Click Download.

When the download is completed, the panel is immediately rebooted. A status bar indicates the progress of the reboot.

Downloading a Card Database Report (.CSV file) from the Host System to the Panel

1. Click Browse to locate the .CSV file. This .CSV file is usually the Card Report that was previously uploaded from the panel as a backup.
2. Click Download to download the file. If the file is in the correct report format, then this message appears:

Would you like to append or replace the database? Access Control does not function while replacing a database, and updating may take several minutes.

If the file is not in the correct report format, a message states the error condition.

If the database update is successful, this message appears:

Update Successful. Restarting Access Control.

If the database update is not successful, a message states the error condition.

Backup file Download

Process to Restore the Entire Loop

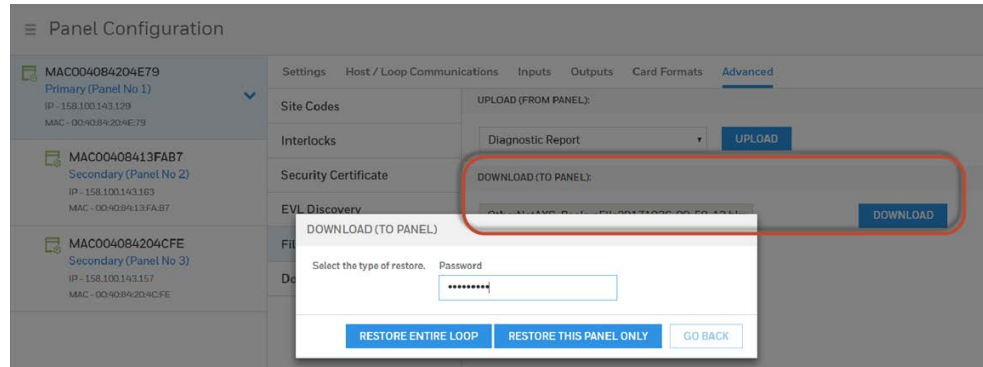
1. Navigate to Primary Panel's Download option, Panel Configuration > Advanced > File Management > Download (To Panel)
2. Click Browse to locate the backup file.
3. Click Download
4. Click "Restore Entire Loop"

When the restore is completed, all the panels are immediately rebooted. A status bar indicates the progress of the reboot.

Restoring (Downloading) Panel Only

1. Choose the Panel you want to restore, Panel Configuration > Advanced > File Management > Download (To Panel)
2. Click Browse to locate the backup file.
3. Click Download
4. Click "Restore This Panel Only" Option

When the restore is completed, the panel is rebooted.



Note: Restoring any panel whose back-up info is not available in the bkp file will not be restored.

Note: During the restore process, the system will prompt for a password that must match the password that was used when the backup file was created.

Panel only restore will restore Panel Configuration data for the specific panel and the Restore Entire Loop option will restore Card, Common and Panel Configuration data to each panel in the loop.

Backup files with a different loop configuration (i.e. EVL) should not be used to restore a loop with the other type of configuration (i.e. RS-485).

Off-line panels while taking back-ups or restores will not be serviced.

Restoring any panel whose back-up info is not available in the bkp file will not be restored.

Restoring (Downloading) Entire Loop

DOWNLOAD (TO PANEL)

Select the type of restore.

RESTORE ENTIRE LOOP

RESTORE THIS PANEL ONLY

GO BACK

1. Click **Browse** to locate the firmware file.
2. Click **Immediate**.
3. Click **Download**.

When the download is completed, the panel is immediately rebooted. A status bar indicates the progress of the reboot.



Synchronizing a New Panel with Information on an Existing Panel

No special operation is required. For any new secondary panel added in a loop, Primary Panel will push card and common configuration to the new panel so basic databases will already be synced up once panel is detected/added.

Note: Synchronization will occur when adding a new panel in a loop or after upgrade from Rev 5 or lower firmware.

The secondary panel will reboot after the panel is synchronized.

Primary panel to the Secondary panel synchronization occurs at the time the Secondary panels are "Registered" with the Primary and will include the common data.

Replace a Primary Panel in an Existing Loop (Web Mode)

Overview

Details the steps to replace a MPA2C3C3 "Primary" panel with existing "Secondary" panels wired via RS-485 or Ethernet Virtual Loop (EVL). The System Wide Restore in the Primary is required with an existing backup.

Primary Panel Replacement and System Wide Restore

IMPORTANT: Ensure a "System Wide Backup" is performed prior to replacing the Primary Panel.

- Step 1. Power up the "New" Primary panel and log into the Web Interface.
- Step 2. Hard Default the "Secondary" panels as they are bound to the original Gateway panel.

Step 3. Navigate to the "Advanced" Tab of the primary panel:

RS-485 Installations: Secondary panels will automatically register with the Gateway.

Confirm the secondary panels are registered.

EVL Installations: Requires Manual Registration of the Secondary Panels.

Navigate to the EVL Discovery and "Register" the Secondary Panels.

IMPORTANT: In order to proceed to Step #4 please wait for all panels to be synchronized. Refer to the "Synchronization Detail Chart"

Step 4. Select the "Restore Entire Loop" option from the "System Wide Backup" once all of the Secondary panels are registered with the Primary.

- Refer to the "Restore Entire Loop Detail Chart"

Replace a Secondary Panel (Web Mode)

Overview

Details the steps to replace a MPA2C3C3 "Secondary" panel in an existing loop of either a wired via RS-485 or Ethernet Virtual Loop (EVL) in Web Mode.

Secondary Panel Replacement and Synchronization

Step 1. Un-register the original Secondary panel in the Primary panel. Navigate to:

- RS-485 Unregister Tab: Panel Configuration > Advanced > RS-485 Unregister.
- EVL Tab: Menu > Panel Configuration > Advanced > EVL Discovery.

Step 2. Install the replacement Secondary panel in the loop.

Step 3. Navigate to the "Advanced" Tab of the primary panel:

- **RS-485 Installations:** Secondary panels will automatically register with the Gateway.
- Confirm the secondary panels are registered.
- **EVL Installations:** Requires Manual Registration of the Secondary Panels.
- Navigate to the EVL Discovery and "Register" the Secondary Panels.

IMPORTANT: In order to proceed to Step #4 please wait for the Secondary panel to be synchronized. Refer to the "Synchronization Detail Chart"

Step 4. Program and add the new Secondary panels doors into the "Spaces".

Step 5. Program the custom settings for Readers, Input Points and Output Points.

Step 6. Perform a "System Wide Backup" when programming is complete.

Hard Default a Primary in an Existing Loop (Web Mode)

Overview

Details the synchronization process of a MPA2C3C3 "Primary | Secondary" panel after hard defaulting an existing "Primary" Panel in a loop of either a wired via RS-485 or Ethernet Virtual Loop (EVL) in Web Mode.

Primary | Secondary Panel Synchronization (Hard Default)

IMPORTANT: Ensure a "System Wide Backup" is performed prior to Hard Default of the Primary Panel.

Step 1. Perform a hard default and log into the Web Interface.

Step 2. Navigate to the "Advanced" Tab of the primary panel:

- **RS-485 Installations:** Secondary panels will automatically register with the Gateway.
 - Confirm the secondary panels are registered.
- **EVL Installations:** Requires Manual Registration of the Secondary Panels.
 - Navigate to the EVL Discovery and "Register" the Secondary Panels.

IMPORTANT: In order to proceed to Step #3 please wait for all panels to be synchronized. The Synchronization will remove the Common Database from the Secondary panels. Refer to the "Synchronization Detail Chart"

Step 3. Select the "Restore Entire Loop" option from the "System Wide Backup" once all of the Secondary panels are registered with the Primary. Refer to the "Restore Entire Loop Detail Chart"

Hard Default an Existing Secondary Panel (Web Mode)

Overview

This section details the synchronization process of a MPA2C3 "Primary | Secondary" panel after hard defaulting an existing "Secondary" Panel in a loop of either a wired via RS-485 or Ethernet Virtual Loop (EVL) in Web Mode.

Primary | Secondary Panel Synchronization (Hard Default)

Step 1. Perform a System Wide Backup

Step 2. Perform a hard default of the Secondary panel.

Step 3. Un-register the original Secondary panel in the Primary panel. Navigate to:

- RS-485 Unregister Tab: Panel Configuration > Advanced > RS-485 Unregister.

- EVL Tab: Menu > Panel Configuration > Advanced > EVL Discovery.

Step 4. Navigate to the "Advanced" Tab of the primary panel:

- **RS-485 Installations:** The Secondary panel will automatically register with the Gateway.
 - Confirm the secondary panels are registered.
- **EVL Installations:** Requires Manual Registration of the Secondary Panel.
 - Navigate to the EVL Discovery and "Register" the Secondary Panels.

IMPORTANT: In order to proceed to Step #5 please wait for the Secondary panel to be synchronized. Refer to the "Synchronization Detail Chart"

Note: *The RS-485 Secondary panels will automatically register with the primary panel and for Ethernet Virtual Loop (EVL) a manual registration is required.*

Step 5. Restore the System Wide Backup and select the "Restore this panel only" option.

(If a backup hadn't been performed the Panel-specific Data will need to be re-programmed.)

- Refer to the "Restore Entire Loop Detail Chart"

Synchronization Detail Chart

Synchronization

Primary panel to the Secondary panel synchronization occurs at the time the Secondary panels are "Registered" with the Primary.

The Synchronization only occurs at the time of panel registration and will include Common Data.

The Secondary panel will reboot after synchronization.

Example:

Primary to Secondary Synchronization in following order with (3) Secondary Panels:

1. The 1st Secondary panel will receive the backup and reboot.
2. The 2nd Secondary panel will receive the backup and reboot
3. The 3rd Secondary panel will receive the backup and reboot.

Common data includes:

- Schedules
- Cards
- Card Formats

- Holidays
- Access Group Name (access group details are panel-specific)
- Configuration (Site Codes)

Access control behavior during synchronization

- Primary Panel access control not affected.
- Newly registered secondary panels will show online in Web Interface and will keep its existing card and common config. Once common data received, secondary's access control and communication processes stop running and the existing common data will be overwritten by new one from primary. Once the common data is received the Secondary panel will reboot.
- Approximately 4 minutes for secondary panel access control to function after registration and synchronization.

Restore Entire Loop Detail Chart

System Wide Backup Restore

Primary panel to the Secondary panel downloads the following:

- Common Data
- Panel-specific data

Example:

System Restore in the following order with (3) Secondary Panels:

1. The 1st Secondary panel will receive the backup and reboot.
2. The 2nd Secondary panel will receive the backup and reboot
3. The 3rd Secondary panel will receive the backup and reboot.
4. The Primary panel will receive the backup and reboot

Common data includes:

- Schedules
- Cards
- Card Formats
- Holidays
- Access Group Name (access group details are panel-specific)
- Configuration (Site Codes)

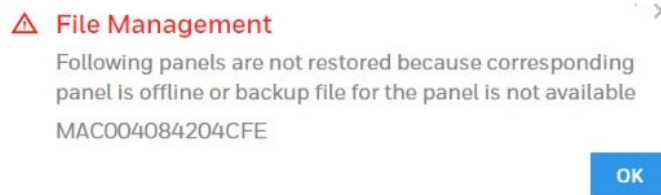
Panel-specific data includes:

- Access Group Schedule Reader Assignments
- Space/Door/Reader Configuration
- Panel Configuration (General)
- Panel Configuration (Firmware Version)
- Panel Configuration (Network) (IP addresses apply only to primary panel)
- Panel Configuration (Host/Loop Communications) (applies only to primary panel)
- Web Users (applies only to primary panel)

Important Points to Note:

System Wide Backup will backup both Card Data and Panel-specific Data with "All" panels on-line. If a Secondary panel is off line the System Wide Backup will not backup the Secondary Panel-specific data.

If the Secondary panel comes back on line the panel will not be serviced at the time of the restore.



The "Panel Only" restore will only restore "Panel-specific data" to the particular panel.

Panel Resets and Restorations

DIP Switch Settings

MPA2C3 SW1 DIP Switch Settings.

S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	Selection
OFF	OFF	ON	OFF	OFF	OFF	OFF	OFF	ON	OFF	Factory Settings
OFF										Reader 1 and Reader 3 = Wiegand
ON										Reader 1 and Reader 3 = OSDP (OSDP 1)
	OFF									Future Use - set to OFF
		OFF								Downstream/Secondary Panel
		ON								Master/Primary Panel
			OFF							Uses the User Provided Ethernet IP Address
			ON							Uses the Default IP Address(192.168.1.150)
				OFF	OFF	OFF	OFF	ON		Address 1
				OFF	OFF	OFF	ON	OFF		Address 2
				OFF	OFF	OFF	ON	ON		Address 3
				OFF	OFF	ON	OFF	OFF		Address 4
				OFF	OFF	ON	OFF	ON		Address 5
				OFF	OFF	ON	ON	OFF		Address 6
				OFF	OFF	ON	ON	ON		Address 7
				OFF	ON	OFF	OFF	OFF		Address 8
				OFF	ON	OFF	OFF	ON		Address 9
				OFF	ON	OFF	ON	OFF		Address 10
				OFF	ON	OFF	ON	ON		Address 11
				OFF	ON	ON	OFF	OFF		Address 12
				OFF	ON	ON	OFF	ON		Address 13
				OFF	ON	ON	ON	OFF		Address 14
				OFF	ON	ON	ON	ON		Address 15
				ON	OFF	OFF	OFF	OFF		Address 16
				ON	OFF	OFF	OFF	ON		Address 17
				ON	OFF	OFF	ON	OFF		Address 18
				ON	OFF	OFF	ON	ON		Address 19
				ON	OFF	ON	OFF	OFF		Address 20
				ON	OFF	ON	OFF	ON		Address 21
				ON	OFF	ON	ON	OFF		Address 22
				ON	OFF	ON	ON	ON		Address 23
				ON	ON	OFF	OFF	OFF		Address 24
				ON	ON	OFF	OFF	ON		Address 25
				ON	ON	OFF	ON	OFF		Address 26
				ON	ON	OFF	ON	ON		Address 27
				ON	ON	ON	OFF	OFF		Address 28
				ON	ON	ON	OFF	ON		Address 29
				ON	ON	ON	ON	OFF		Address 30
				ON	ON	ON	ON	ON		Address 31*
									OFF	Reader 2 and Reader 4 = Wiegand
									ON	Reader 2 and Reader 4 = OSDP (OSDP 2)

1. DIP Switch SW1 bit 4 does NOT require a panel reboot to take effect. This does not affect the USB2 - WEB MODE IP address.

Note: A Primary panel (SW1 bit 3 ON) cannot be set to address 31.

MPA2C3 SW2 DIP Switch Settings

Bit1	Bit2	Bit3	Bit4	Section
OFF	OFF			No EOL resistor for OSDP 1 (Door 1 & 3)
ON	ON			EOL resistor for OSDP 1 (Door 1 & 3)
		OFF	OFF	No EOL resistor for OSDP 2 (Door 2 & 4)
		ON	ON	EOL resistor for OSDP 2 (Door 2 & 4)

MPA2C3 SW3 DIP Switch Settings

Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8	Selection
OFF	OFF	OFF	OFF					Future Use - always in OFF position
				OFF	OFF			NO EOL resistor for RS485 bus I/O Devices (default)
				ON	ON			EOL resistor for RS485 bus I/O Devices
						OFF	OFF	NO EOL resistor for RS485 bus Downstream panels (default)
						ON	ON	EOL resistor for RS485 bus Downstream panels

Note: When you use the DIP switches to reset a panel to the original factory default values, the Event History is lost and any customized databases are removed. So the panel is reset with the original factory default database. This does not affect the Ethernet IP address.

Note: Door 3 and Door 4 is applicable for 4 door panels.

Restoring the Panel to Factory Default Settings

1. Make a note of the existing settings on SW1 DIP switches.
2. While the panel is powered up, turn all of the DIP switches to the OFF position.
3. Power down; then power the panel back up.
4. Wait for the panel to come up. The **RUN LED** should flicker fast.
5. Set the DIP switches back to their original positions.

6. Power down; then power the panel back up. The RUN LED should flash normal.
7. The panel is now reset to the original factory default values.

Resetting the Panel

1. Navigate to the **Settings** panel:
 - **Dashboard > Panels > Settings**, or
 - **Menu > Panel Configuration > Settings**.

Figure 1-2 Settings Panel

The screenshot shows the 'Panel Configuration' interface. On the left, a sidebar lists panel details: 'MAC00408400DA45New', 'Primary (Panel No 1)', 'IP - 10.78.32.114', and 'MAC - 00:40:84:00:DB:06'. The main area is titled 'Settings' and has tabs for 'Host / Loop Communications', 'Inputs', 'Outputs', 'Card Formats', and 'Advanced'. Under the 'GENERAL' section, the 'Firmware Version' is '1.0.3.45' and a 'Reset' button is circled in red. Other fields include 'Panel Name' (MAC00408400DA45New), 'Panel Type' (MPA2), 'Boot Time' (Mon Dec 16 16:56:43 2019), and 'OS Version' (7.0-r16 (2016.03-F1-1.0.10130, 4.9.141+gf1855e7)). The 'NETWORK' section shows 'MAC Address' (00:40:84:00:db:06), 'IP Address' (10.78.32.114), 'Subnet Mask' (255.255.255.0), and 'Default Gateway' (10.78.32.1). The 'TIME MANAGEMENT' section shows 'Format (in hr)' with options '12' and '24'. At the bottom right are 'CANCEL' and 'SAVE' buttons.

2. Click **Reset**.
Click **OK** to reboot the panel.

Firmware Upgrades

Panel Requirements

MPA2C3 panels must first be upgraded to latest firmware. See the release notes for more information.

Note: *The secondary (downstream) EVL panels should be upgraded first, and then the primary (MASTER).*

Overview

The following procedures provide step-by-step instructions for upgrading the MPA2C3 controller.

Upgrading the firmware can involve the following actions:

- Backing up the database from each panel
- Updating the panel firmware (Application only)
- Updating the panel firmware (OS + Application)

IMPORTANT: Recommend to back up the database before and after the firmware upgrade.

Planning for the Firmware Upgrade

Note: *The Secondary panels must be upgrade first in any order and then upgrade the Primary panel last.*

The Secondary panel Firmware upgrade through panel web page is not recommended. Refer the below two sections to upgrade the Secondary panels.

For primary panel, plan 5-7 minutes (approximately) to upgrade the **Application only** and for **OS + Application** plan for 10 to 15 minutes (approximately). In order to reduce the time required to install this version on your "Secondary" panel, each panel can be removed from the loop and configured as a "Primary" panel (disconnect the RS-485 before making it a Primary) by following these steps:

RS-485 Drop line:

- Step 1. Configure Secondary panels as Primary and manually "Reboot"
- Step 2. Upgrade the firmware
- Step 3. Configure the panels back to Secondary and manually "Reboot"
- Step 4. Upgrade the Firmware in the Primary
- Step 5. Confirm Secondary panels are line with the Primary

Note: *If a Secondary panel doesn't come on line with the primary perform a manual "Reboot" of the Secondary panel.*

Ethernet Virtual Loop (EVL):

- Step 1. "Unregister" the Secondary panels
- Step 2. Configure Secondary panels as Primary and manually "Reboot"
- Step 3. Upgrade the firmware
- Step 4. Configure the panels back to Secondary and manually "Reboot"
- Step 5. "Re-register" Secondary panels manually in the Primary panel

Remember to return their configuration back to a downstream panel once the upgrade has been successfully completed.

The firmware and Operating System (OS) can be downloaded from the Honeywell Download Center at the following site: <https://mywebtech.honeywell.com/>.

Updating the MPA2C3 Panel Using the Web Interface

Step 1: Installing the new App File

1. Navigate to the web server **Panel Configuration > Advanced > File Management > Upload (To Panel)**.
2. Under **Download (To Panel)** click **Browse** to locate the application bin file.
3. Select the file and click **Download**. Click **OK** to continue. Once the "Download to primary panel complete; now processing the image" message pops up, click **OK** again.
4. You will see the **Download** to primary panel complete; now processing the image message once again. Click **OK**. This time a reboot will be triggered and you will see the message: "The Panel is now rebooting. Wait 5-7 minutes, then click Refresh and log back in."

Step 2: Installing the new OS File + Application

Note: This procedure is not necessary if the panels are already at the latest OS.

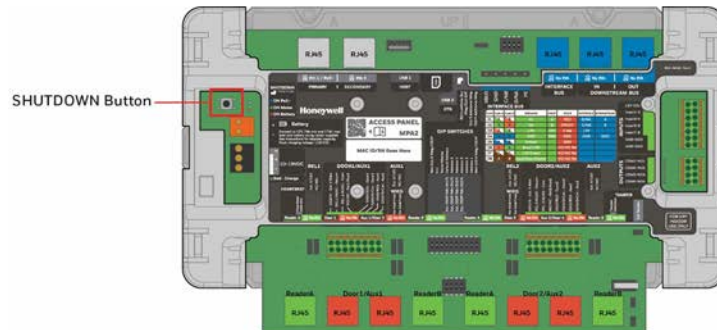
1. Navigate to the web server **Panel Configuration > Advanced > File Management > Upload (To Panel)**.
2. Under **Download**, click **Browse** to locate the latest **OS + Application** file.
3. Select the file and click **Download**. Click **OK** to continue. Once the "Download to primary panel complete; now processing the image" message pops up, click **OK** again.
4. You will see the "Download to primary panel complete; now processing the image message" once again. Click **OK** to continue. This time a reboot will be triggered. It will take approximately **10 to 15 minutes** for the OS + Application to complete the install.
5. Clear Cache and Cookies: This time, before logging back in, use the browser-dependent steps found in *Clearing the Cache and Cookies in the Internet Browsers Used by the MPA2C3 Web Server*, to clear your browser cache and cookies. You can navigate away from the current web screen, clear the files, and then navigate back.

Step 3: Verifying that the Installed Versions are Correct

1. Navigate back to the web server **Menu > Panel Configuration > Settings**.
2. In the Firmware Version section, you should see the latest application versions listed as 1.0.3.x. In the Operating System section, you should see the latest OS version.
3. If you notice any communication issues, and the upgrades are complete, typically this means there is more than one panel set up as a primary on the active loop. You should disconnect each panel from the 485 loop (C-TB9), and cycle power on all the panels on the loop. Once all panels are powered up, reconnect the 485 loop to clear the issue.

After upgrading a MPA2C3 panel, you must clear your browser's cache. See [Clearing the Cache and Cookies in the Internet Browsers Used by the MPA2C3 Web Server](#) for details.

Shutting Down and Restart the Panel



The SHUTDOWN button allows you to shut down the control panel securely. This ensures that the system can save all necessary data and status in the flash memory. Shutting down the panel disables the inputs/outputs, turns OFF the peripheral bus, AUX outputs and the PTCs. However, it cannot remove power from the panel (from the AC power adapter or the batteries).

Shutdown the control panel:

1. Press the SHUTDOWN button for 5 seconds.
2. Running LED is off, Panel is shut down (hibernate state).

Note: After shutdown the power is not removed from the panel, to restart the panel, please press Shutdown button shortly (NOT 5 Seconds)

Note: To completely power off the control unit,

- a. When the unit is powered by PSU, first disconnect the battery cable and then disconnect the AC power cable.
- b. When the unit is powered by PoE+, disconnect the PoE+ cable.

Restart the Panel

Note: Before powering up the access control unit, ensure that the access control unit is

properly wired to the readers, doors, interface bus and downstream devices. Ensure the DIP Switches and jumpers are set for the corresponding readers.

1. Apply Mains power first, then connect the back-up battery or connect PoE+ power to the panel.
2. Check the status of Running LED.
 - Green blinking - license is correct and application is running for a 2 door system
 - Amber blinking - license is correct and application is running for a 4 door system

Note: *If only the battery is connected to the panel without the mains power, then the panel will not start.*

To restart the control panel

Note: *Before powering up the access control unit, ensure that the access control unit is properly wired.*

1. Apply the PoE+ power to the panel or apply the power via PSU with a battery backup to the panel.
2. Check the status of Heartbeat LED.
 - The Heartbeat LED blinks in green for 2-door panels, or
 - The Heartbeat LED blinks in orange for 4-door licensed panels.

Note: *You can also use the ASCII command `_l=pn_R` to reset a panel to the original factory default values, but this command only removes the customized databases and restores the original factory default database. The Event History is retained*

Panel Requirements

MPA2C3 panels must first be upgraded to latest firmware. See the release notes for more information.

Note: *The secondary (downstream) EVL panels should be upgraded first, and then the primary (MASTER).*

Overview

The following procedures provide step-by-step instructions for upgrading the MPA2C3 controller.

Upgrading the firmware can involve the following actions:

- Backing up the database from each panel
- Updating the panel firmware (Application only)
- Updating the panel firmware (OS + Application)

IMPORTANT: Recommend to back up the database before and after the firmware upgrade.

Planning for the Firmware Upgrade

Note: *The Secondary panels must be upgrade first in any order and then upgrade the Primary panel last.*

The Secondary panel Firmware upgrade through panel web page is not recommended. Refer the below two sections to upgrade the Secondary panels.

For primary panel, plan 5-7 minutes (approximately) to upgrade the **Application only** and for **OS + Application** plan for 10 to 15 minutes (approximately). In order to reduce the time required to install this version on your "Secondary" panel, each panel can be removed from the loop and configured as a "Primary" panel (disconnect the RS-485 before making it a Primary) by following these steps:

RS-485 Drop line:

- Step 1. Configure Secondary panels as Primary and manually “Reboot”
- Step 2. Upgrade the firmware
- Step 3. Configure the panels back to Secondary and manually “Reboot”
- Step 4. Upgrade the Firmware in the Primary
- Step 5. Confirm Secondary panels are line with the Primary

Note: *If a Secondary panel doesn't come on line with the primary perform a manual “Reboot” of the Secondary panel.*

Ethernet Virtual Loop (EVL):

- Step 1. “Unregister” the Secondary panels
 - Step 2. Configure Secondary panels as Primary and manually “Reboot”
 - Step 3. Upgrade the firmware
 - Step 4. Configure the panels back to Secondary and manually “Reboot”
 - Step 5. “Re-register” Secondary panels manually in the Primary panel
- Remember to return their configuration back to a downstream panel once the upgrade has been successfully completed.

The firmware and Operating System (OS) can be downloaded from the Honeywell Download Center at the following site: <https://mywebtech.honeywell.com/>.

Updating the MPA2C3 Panel Using the Web Interface

Step 1: Installing the new App File

1. Navigate to the web server **Panel Configuration > Advanced > File Management > Upload (To Panel)**.
2. Under **Download (To Panel)** click **Browse** to locate the application bin file.
3. Select the file and click **Download**. Click **OK** to continue. Once the "Download to primary panel complete; now processing the image" message pops up, click **OK** again.
4. You will see the **Download** to primary panel complete; now processing the image message once again. Click **OK**. This time a reboot will be triggered and you will see the message: "The Panel is now rebooting. Wait 5-7 minutes, then click Refresh and log back in."

Step 2: Installing the new OS File + Application

Note: *This procedure is not necessary if the panels are already at the latest OS.*

1. Navigate to the web server **Panel Configuration > Advanced > File Management > Upload (To Panel)**.
2. Under **Download**, click **Browse** to locate the latest **OS + Application** file.
3. Select the file and click **Download**. Click **OK** to continue. Once the "Download to primary panel complete; now processing the image" message pops up, click **OK** again.
4. You will see the "Download to primary panel complete; now processing the image message" once again. Click **OK** to continue. This time a reboot will be triggered. It will take approximately **10 to 15 minutes** for the OS + Application to complete the install.
5. Clear Cache and Cookies: This time, before logging back in, use the browser-dependent steps found in *Clearing the Cache and Cookies in the Internet Browsers Used by the MPA2C3 Web Server*, to clear your browser cache and cookies. You can navigate away from the current web screen, clear the files, and then navigate back.

Step 3: Verifying that the Installed Versions are Correct

1. Navigate back to the web server **Menu > Panel Configuration > Settings**.
2. In the Firmware Version section, you should see the latest application versions listed as 1.0.3.x. In the Operating System section, you should see the latest OS version.
3. If you notice any communication issues, and the upgrades are complete, typically this means there is more than one panel set up as a primary on the active loop. You should disconnect each panel from the 485 loop (C-TB9), and cycle power on all the panels on the loop. Once all panels are powered up, reconnect the 485 loop to clear the issue.

After upgrading a MPA2C3 panel, you must clear your browser's cache. See *Clearing the Cache and Cookies in the Internet Browsers Used by the MPA2C3 Web Server* for details.

CACHES AND CERTIFICATES

Caches

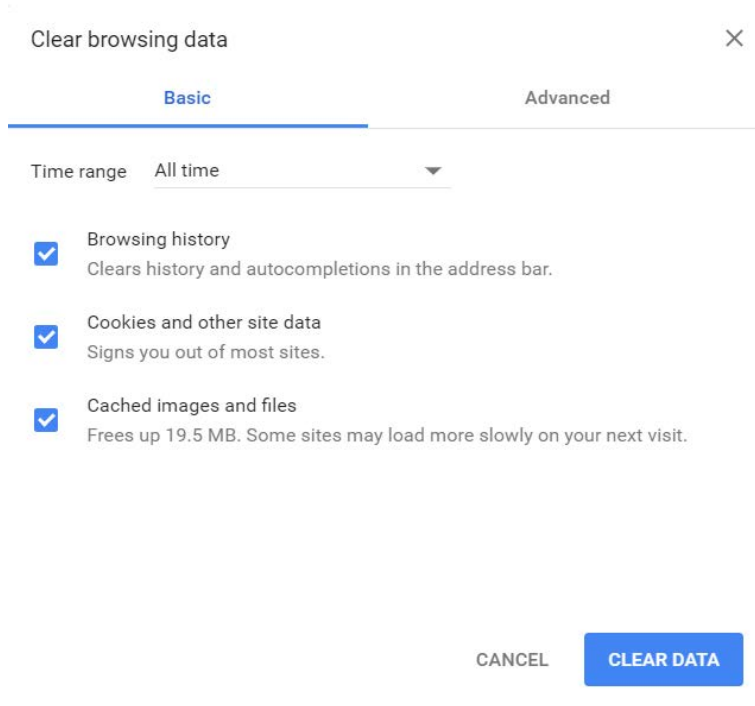
Clearing the Cache and Cookies in the Internet Browsers Used by the MPA2C3 Web Server

The MPA2C3 supports Google Chrome. It is recommended that the cache be cleared following a successful upgrade.

Note: *After upgrading a MPA2C3 panel, you must clear your browser's cache.*

1. Open your Chrome browser and click the menu button (three vertical dots) in the top right corner of the browser window.
2. Select Settings to display the settings screen.

- Click the Advanced link at the bottom of the Settings screen to display the Clear Browsing Data screen:



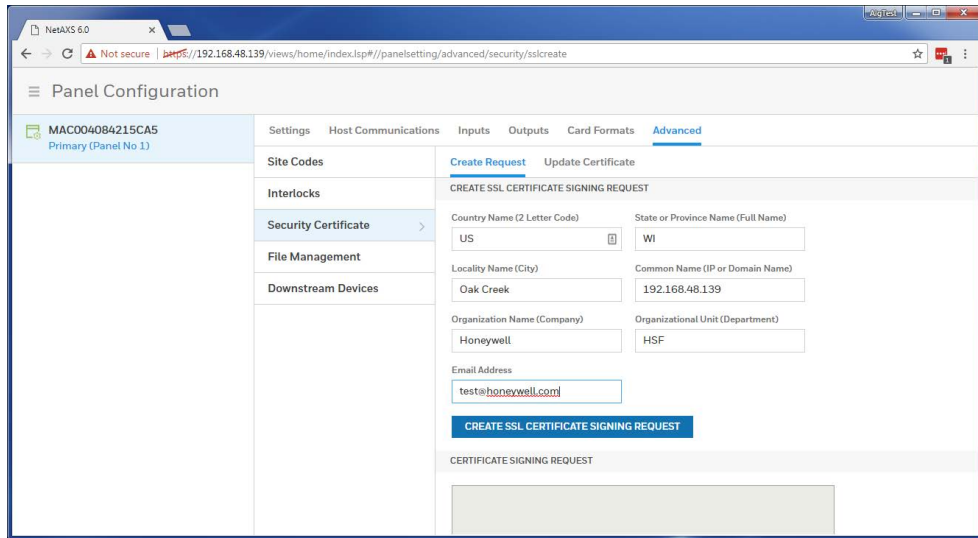
- Ensure that the selections pictured in the above image are chosen.
3. Click **CLEAR DATA**.

Generating and Installing Certificates

Section 1 - Generating sign-in request and installing certificates

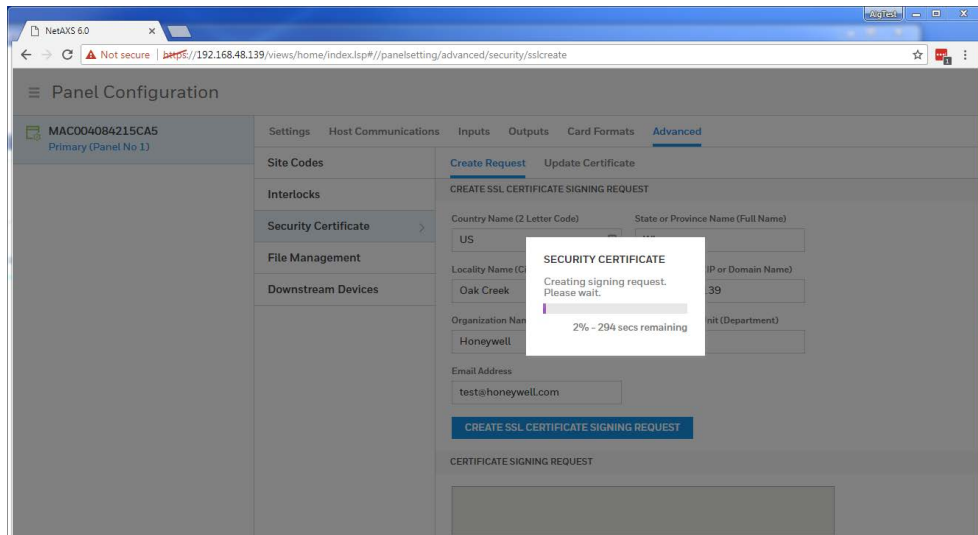
In order to have Google Chrome display the panel as secure, it's necessary to

1. Generate a signing request.
2. The Certificate Authority provides two types of certificates:
3. Certificate to be installed in the panel.
4. Master certificate to be installed in the browser(s).
5. Install the certificate in the panel.
6. Install the master certificate into the browser.



Go to **Advanced Menu > Security Certificate** tab. **Create Request** will be selected at the top of the pane. Fill in the fields as shown above. Make sure that the panel IP address is in the common name field.

Select **Create TLS Certificate Signing Request**.



You will then note that there is text in the **Certificate Signing Request** field.

The screenshot shows the 'Panel Configuration' interface for device MAC004084215CA5. The 'Advanced' tab is selected, and the 'Create Request' button is active. The form contains the following fields:

Country Name (2 Letter Code)	State or Province Name (Full Name)
US	WI
Locality Name (City)	Common Name (IP or Domain Name)
Oak Creek	192.168.48.139
Organization Name (Company)	Organizational Unit (Department)
Honeywell	HSF
Email Address	
test@honeywell.com	

Below the form is a 'CREATE SSL CERTIFICATE SIGNING REQUEST' button and a text area containing the following text:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0jCCAbOCAQAwYwxCzAJBgNVBAYTAiVTMQswCQYDVQQIEwJXST
ESMBAGALUE
```

The screenshot shows the 'Panel Configuration' interface for device MAC004084215CA5. The 'Advanced' tab is selected, and the 'Update Certificate' button is active. The form contains the following fields:

Locality Name (City)	Common Name (IP or Domain Name)
Oak Creek	192.168.48.139
Organization Name (Company)	Organizational Unit (Department)
Honeywell	HSF
Email Address	
test@honeywell.com	

Below the form is a 'CREATE SSL CERTIFICATE SIGNING REQUEST' button and a text area containing the following text:

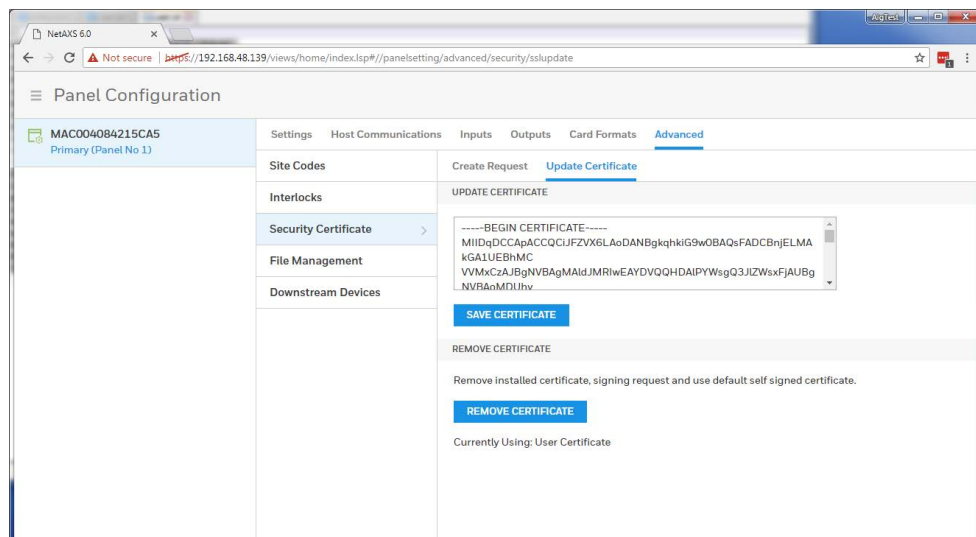
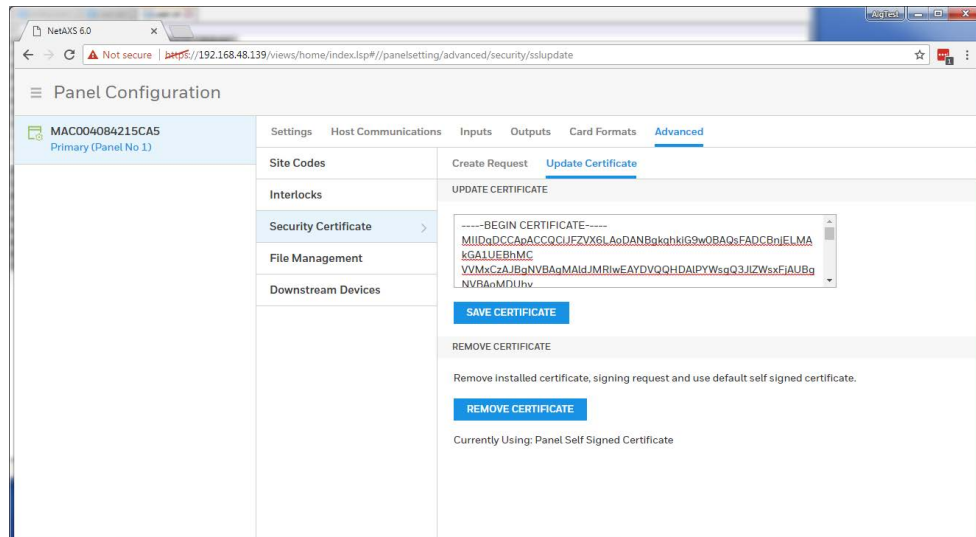
```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0jCCAbOCAQAwYwxCzAJBgNVBAYTAiVTMQswCQYDVQQIEwJXST
ESMBAGALUE
BxMJTzFhEiNyZWVrMRiWEAYDVQKEwllb25leXdlbGwxDCAkBgNVBAs
TA0hTRIFX
```

At the bottom of the text area is a 'RESET CERTIFICATE SIGNING REQUEST AND FIELDS' button.

Copy all of the text out of this field and send it to the signing authority of your choice.

You will receive a signed certificate (also in text format).

Navigate to the **Update Certificate** pane and paste the certificate into the designated field. Select **Save Certificate**.

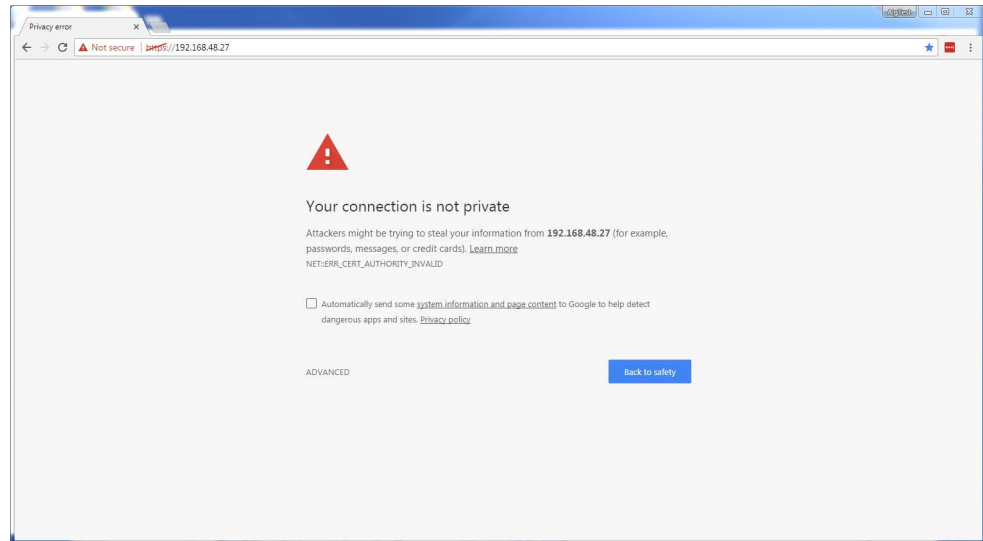


When the save is complete you will notice that the text at the bottom of the page reports "Currently using: User Certificate."

Section 2 - Installing the master certificate into the browser

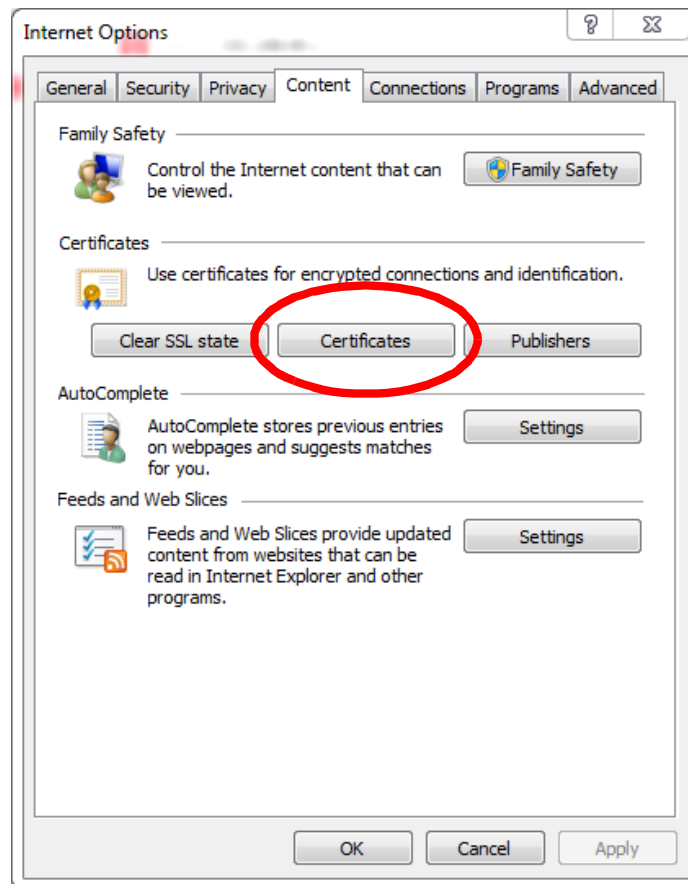
When using a self-signed certificate it is necessary to install the matching master certificate into all computer's browsers that access the MPA panels.

After you have installed the certificate file onto the panel but before you install the master certificate, the browser will still display the broken lock.

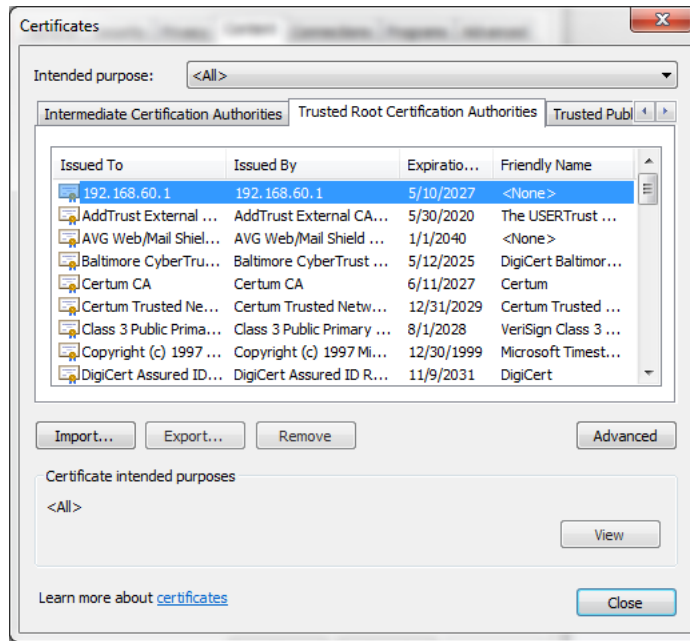


Open **Internet Explorer** and select **Tools (gear icon) > Internet** options.

Select the **Content** tab then select **Certificates** button in center of window.



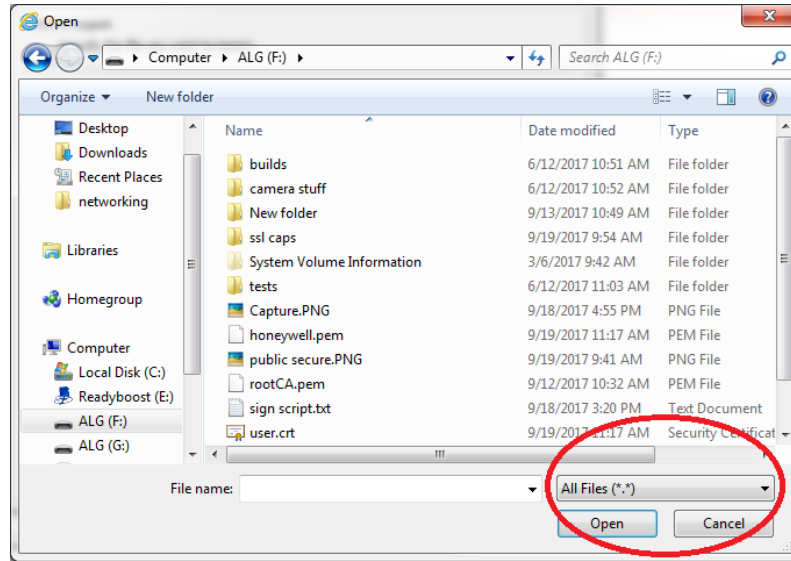
Select the **Trusted Root Certificate Authorities** tab, then select **Import**:



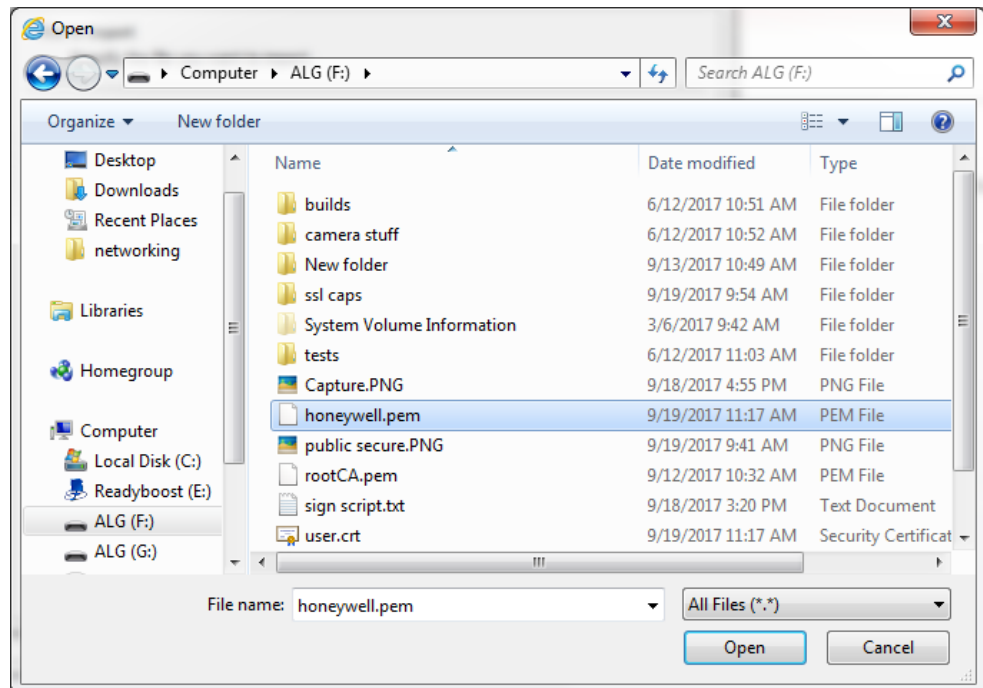
The **Certificate Import Wizard** will appear.



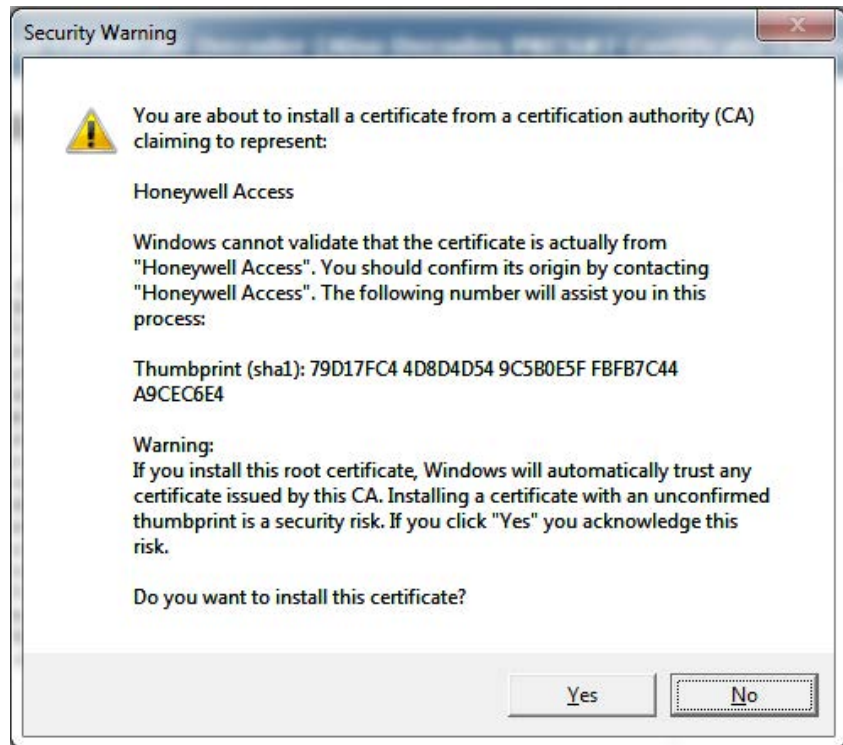
Select **Next** and Browse.



Change the file type to **All Files**. Then select **the master signed certificate** from its location on your machine.



Click **Open** to load the file.

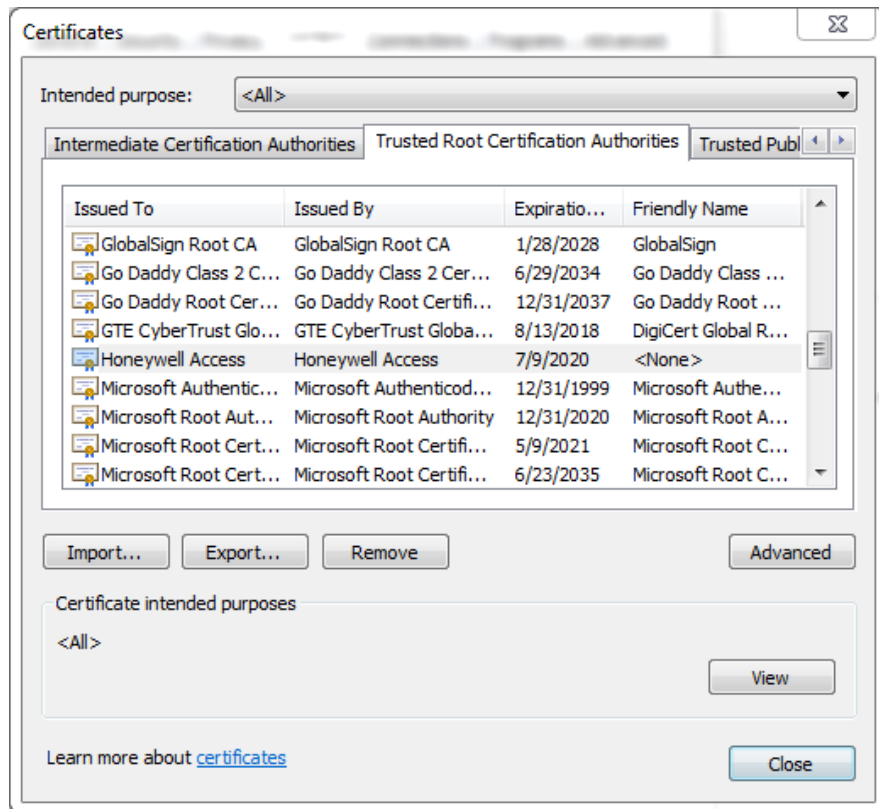


Confirm **Yes** when this warning comes up:



Success!

Now if you scroll down the list of **Trusted Root Certificate Authorities** you should see **the signed certificate** in the list:



Close any Chrome windows that were open. Navigate to the URL MPA Address and the login screen will appear. The address bar will indicate a Lock Icon with "Secure".

Creating MPA2C3 Accounts

A User is someone who will be using the MPA2C3 software in one or more functional roles. The Manage Accounts configuration window allows you to configure the following:

- Add, modify, delete user accounts
- Enable or disable user accounts
- View the user's current login status (logged in or out)

There are three types of user accounts, which all include different abilities and functions.

Table 8-1 User Access Types and Functionality

Function	Operator	Service	Administrator
View alarms/events	3	3	3
Acknowledge alarms	3	3	3
View panel I/O status	3	3	3
Control I/O status	3	3	3
Generate reports	3	3	3
View card database	3	3	3
Create, modify, delete cards		3	3
View all configurations		3	3
Create, modify, delete configurations			3
Perform uploads/downloads			3
Manage own user account	3	3	3
Manage all user accounts			3

Note: *User name is free from text field, if personal identifications details are used for the User name, then it is the responsibility of system administrator to make sure appropriate consent is obtained from the user and maintained to meet GDPR compliance.*

1. Click **Manage Accounts** in the Menu to navigate to the Manage Accounts window.

Figure 1-1 Manage Accounts Configuration Interface

The screenshot displays the 'Manage Accounts' configuration interface. On the left, a sidebar lists several accounts: 'admin' (Logged In), 'client' (Logged Out), 'Dulce' (Logged Out), 'mark' (Logged Out), 'OP' (Logged Out), and 'Password' (Logged Out). The main area shows the configuration for the 'Admin' account. The 'Name' field is set to 'admin'. The 'Password' field is empty. The 'Account Type' is set to 'Administrator', with 'Service' and 'Operator' as alternative options. The 'Account Status' is set to 'Enabled', with 'Disabled' as an alternative. The 'Language Preference' is set to 'EnglishDefault'. At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

Note: When creating passwords, they must meet the following minimum requirements:


- Consist of letters, numbers, and symbols.
- Contain at least one character from each of the following four types: lower-case letters (a–z), UPPER CASE letters (A–Z), numbers (0–9), and symbols [!, @, #, \$, %, ^, &, *, (,)].
- Contain a minimum of 8 and a maximum of 16 characters.
- Not contain the name of the user's account type ("admin", "service", or "operator").
- Not contain a consecutive string of 3 or more repeated characters.

Note: All user passwords will expire after a period of six months; the users will be prompted to change password upon login.

Figure 1-2 Accounts Configuration Interface

The screenshot displays the 'Accounts Configuration Interface' for the 'Admin' account. On the left, a sidebar lists several users: 'admin' (Logged In), 'client' (Logged Out), 'Dulce' (Logged Out), 'mark' (Logged Out), 'OP' (Logged Out), and 'Password' (Logged Out). The main content area is titled 'Admin' and contains the following configuration fields:

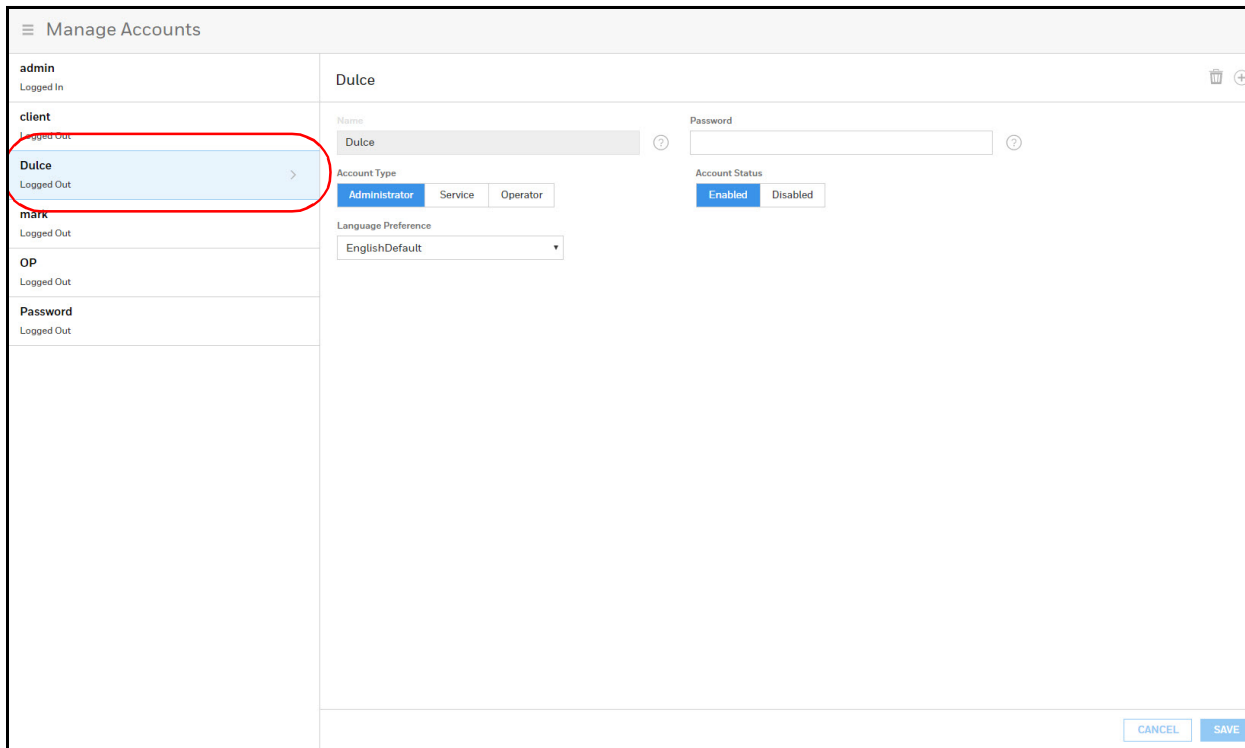
- Name:** A text input field containing 'admin'.
- Password:** An empty text input field.
- Account Type:** Three radio buttons: 'Administrator' (selected), 'Service', and 'Operator'.
- Account Status:** Two radio buttons: 'Enabled' (selected) and 'Disabled'.
- Language Preference:** A dropdown menu currently set to 'EnglishDefault'.

1. Click to  create a new account.
2. Enter a name.
3. Enter a **Password**.
4. Select an **Account Type**, either **Administrator**, **Service**, or **Operator**. See [Table 8-1](#) on [page 156](#) for more about these accounts.
5. Enable/disable the **Account Status**.
6. Select a language.
7. Click **Save**.

Modifying a User Account



1. Click to select an account in the **Manage Accounts** interface.

Figure 1-3 Modifying a User Account



2. Make the changes, and then click **Save**.

Deleting a User Account

1. Click to select an account in the **Manage Accounts** interface. A delete icon  appears.
2. Click , then click **OK** to confirm the deletion.

Admin Password Reset

It is likely that the installer or user forgets the administrator password to access the Web Interface.

To reset the panel's administrator password, the panel must be physically accessed by an authorized person.

The following steps are needed to reset the administrator password

1. Open the panel's cabinet
2. Power OFF the panel.
 - a. Note the current address of the panel reading DIP Switch positions of SW1 bit 5, 6, 7, 8 and 9 (Address 5, Address 4, Address 3, Address 2 and Address 1). *(You need this in step 4a. again)*
 - b. Set DIP Switch positions of SW1 bit 3, 5, 6, 7, 8 and 9 (Primary, Address 5, Address 4, Address 3, Address 2 and Address 1) to ON position. Make DIP switch 3,5,6,7,8, and 9 ON.
3. Power ON the panel.
 - a. Connect to the panel with a computer or laptop via Ethernet ETH1 (HOST) or USB2 (WEB MODE).
 - b. Log in to web login with reset default administrator username and password.
 - i. Follow instructions to create a new administrator password in the Web interface
 - c. Log off
4. Power OFF the panel
 - a. Set DIP Switch positions of SW1 bit 5, 6, 7, 8 and 9 (Address 5, Address 4, Address 3, Address 2 and Address 1) to the original positions noted in step 2a.
5. Power ON the panel
6. Close the panel's cabinet
7. From here use the new administrator password to login the web interface

Note: *Password reset is enabled only for admin account.*

Note: *The password reset only resets the password, however the configuration of the panel will not be reset to factory default.*

Technical Support

Normal Support Hours

USA

USA +1 800 323 4576
Technical Support, Option 2 (Access Control)

Monday through Friday, 7:00 a.m. to 7:00 p.m. Central Standard Time (CST), except company holidays: (800) 323-4576.

Web

<https://buildings.honeywell.com/>

<https://myhoneywellbuildingsuniversity.com/training/support/>

<https://www.security.honeywell.com/>

For technical assistance please click [here](#), scan the below QR code or visit

<https://myhoneywellbuildingsuniversity.com/training/support/>

EMEA

ITALY +390399301301
UK +441344238266
SPAIN +37911238038
FRANCE +33366880142
THE NETHERLANDS +31108080688
Technical Support, Option 2 (Access Control)

Hours of Operation | Monday through Friday, 9:00 am - 7:00 pm EST

Following are the tech support E-mail IDs of different countries.

EMEA	ITALY	hsgittechsupport@honeywell.com
	UK	hsguktechsupport@honeywell.com
	SPAIN	hsgestechsupport@honeywell.com
	FRANCE	hsgfrtechsupport@honeywell.com
	THE NETHERLANDS	hsgnltechsupport@honeywell.com
USA	https://www.honeywellsystems.com/ss/techsupp/index.html	
Web Support	Technical Assistance:	https://buildings.honeywell.com/
	MyWebTech Customer Support	https://myhoneywellbuildingsuniversity.com/training/support/
	Schedule Support:	https://myhoneywellbuildingsuniversity.com/training/support/
	Online Training:	https://honeywelldiscovertraining.com

Table 8-2 Troubleshooting Problems and Solutions

Problem	Solution
The panel powers up, but it does not respond to any communication, cards reads, or input activation.	Ensure that the Address DIP switches are set the correct values. Turn off the power (including battery), change the settings, and re-apply the power.
No communications exist with the Ethernet port.	Check the IP address from the ACS4 setup tool.



Document: 800-27037 User Manual 07/2022

Honeywell Building
Technologies
715 Peachtree St. NE
Atlanta, GA 30308

Honeywell Commercial Security
Carlton Park, Building 5
King Edward Avenue
Narborough, Leicester
LE19 3EQ

<https://buildings.honeywell.com/>



800-27037

© 2022 Honeywell International Inc. All rights reserved. No part of this publication may be reproduced by any means without written permission from Honeywell. The information in this publication is believed to be accurate in all respects. However, Honeywell cannot assume responsibility for any consequences resulting from the use thereof. The information contained herein is subject to change without notice. Revisions or new editions to this publication may be issued to incorporate such changes. For patent information, see www.honeywell.com/patents.