Honeywell | THE FUTURE IS WHAT WE MAKE IT | MPA2®

Access Control Unit

MPA2 User Guide

Document 800-25396 - B – December 2019

Revisions

Rev	Date	Revisions
A	03/2019	Document created.
A	03/2019	Added "General Data Protection Regulation" disclosure to the back cover.
B	10/2019	Added "General Data Protection Regulation" and Cyber Security enhancements

Contents

Ordering Information

Please contact your local Honeywell representative or visit us on the web at www.honeywellaccess.com for information about ordering.

Feedback

Honeywell appreciates your comments about this manual. Please visit us on the web at www.honeywellaccess.com to post your comments.

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.

Personal Data Storage

Please be aware that this product can store personal data. Personal data is protected by the General Data Protection Regulation (2016/679) in Europe and therefore the owners of personal data have obtained certain rights thanks to this regulation.

We strongly advise you to be fully aware of these owner ("data subjects") rights as well as which limitations you have to obey regarding the use and distribution of this data. Further details can be found on the GDPR website of the EU:
https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

This page is intentionally left blank

Getting Started

Overview

The MPA2 is a modular 2 Door access control system. An MPA2 access control site is configured with a host system and access control units that exceed existing NETAXS123 specifications and approvals. 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 ports. Each port can support one reader (Wiegand or OSDP). For supported configurations, see *Firmware Compatibility on page 105*.

You can communicate with the MPA2 access control unit either through a host software system or by connecting to the web server through an Ethernet or USB connection. This chapter describes how to connect to 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.

Connecting to the Web Server

The MPA2 embedded web server is intended for supplementary and programming purposes only. It has not been evaluated by UL for use as a monitoring station.

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

- USB
- Ethernet through a direct connection
- Ethernet through a hub/LAN connection

Note 1) The panel that you are connecting to the computer is the Primary panel. DIP switch 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://mywebtech.honeywell.com. Click Download Center > Access Control > MPA > MPA2 Resources and USB Driver Media CD. Click on download link (“Click here to Download” or the Download 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://mywebtech.honeywell.com

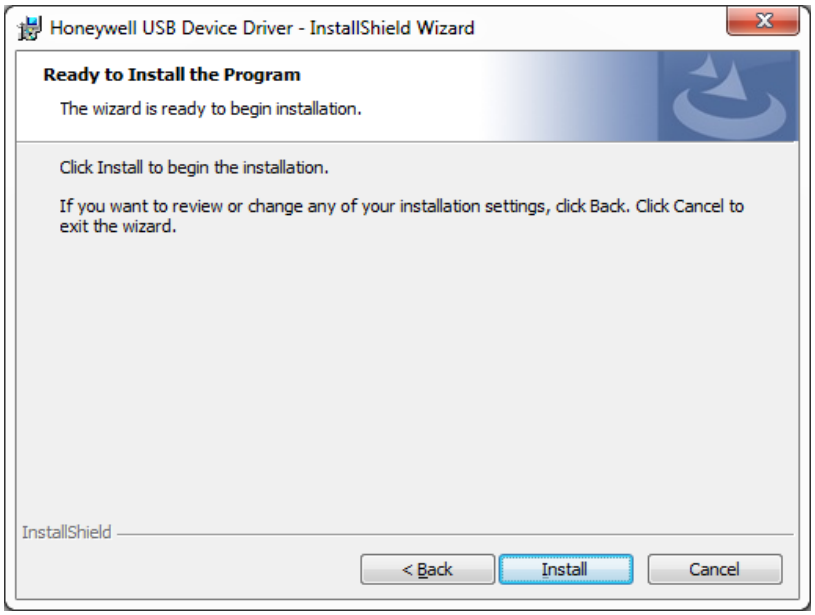
If the file is blocked by the browser then:

- 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"

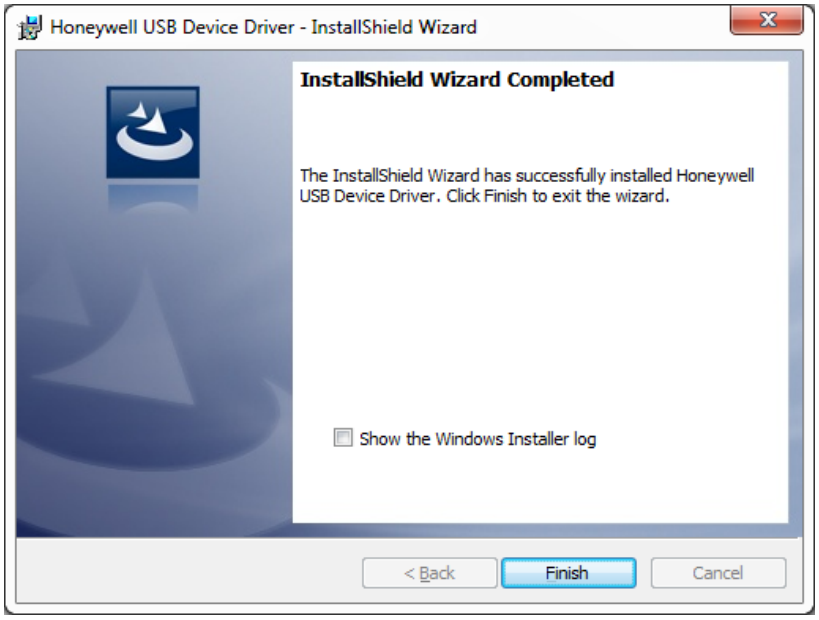
2. Locate and open the compressed ZIP file. Click on the Driver folder. Double-click on **MPA-USB-setup.exe** file to launch. Select **Run** and select **Yes** to allow the USB Driver to be installed.

3. 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.



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



5. Click **Finish**.
6. Connect the computer to the MPA2 controller with a USB-A to Micro USB-B cable.
7. Supply power to the MPA2 controller. Login at https://192.168.2.150.

Setting Up an Ethernet Port

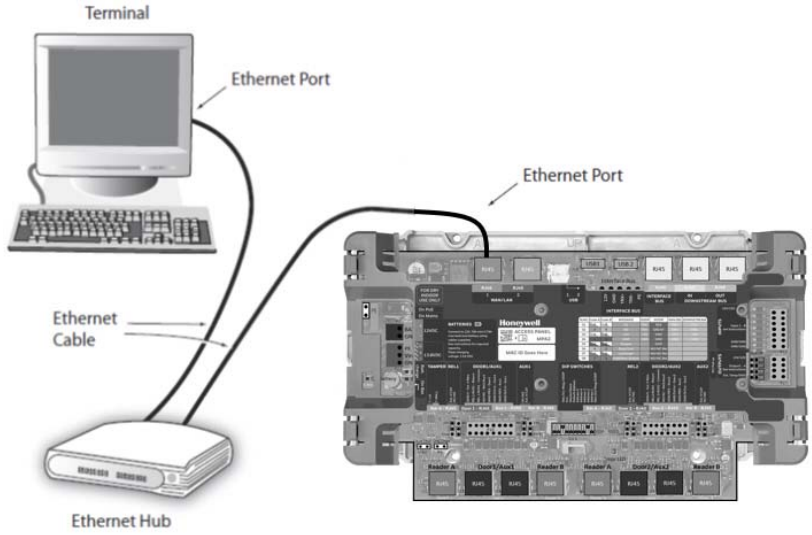
There are two options for connecting the panel to a PC via a web server:

- Using a hub/LAN connection
- Using a direct connection

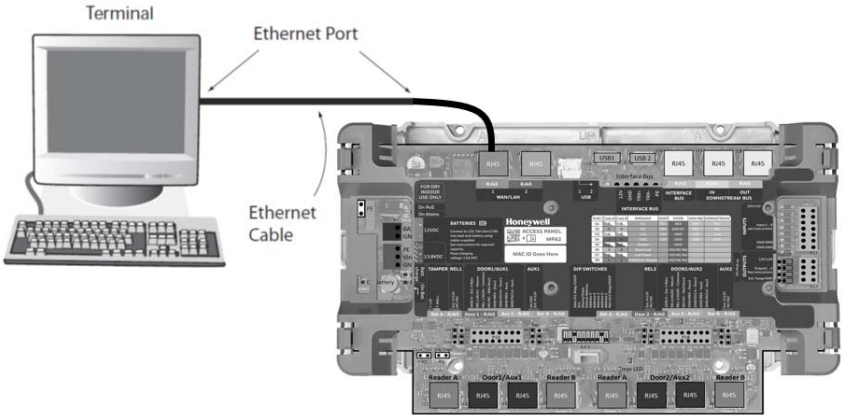
To set up an Ethernet Port

1. Connect your computer's Ethernet port to the panel's Ethernet port using one of the following two methods:

a. Ethernet Hub connection: Connect both the computer's Ethernet port and the panel's Ethernet port to an Ethernet hub with standard Ethernet patch cables.

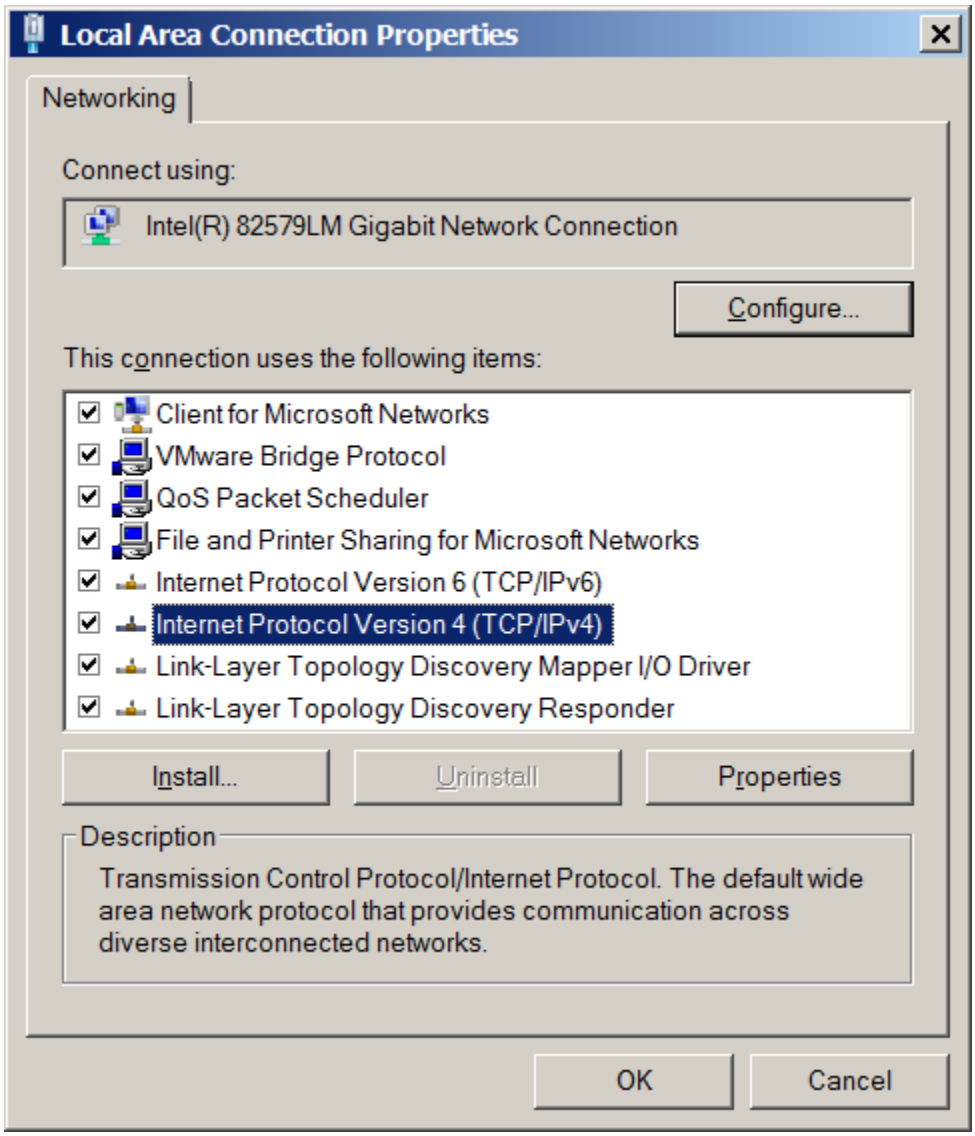


b. Web server direct connection: Connect the computer's Ethernet port directly to the panel's Ethernet port with either a crossover or an Ethernet cable.



2. 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.

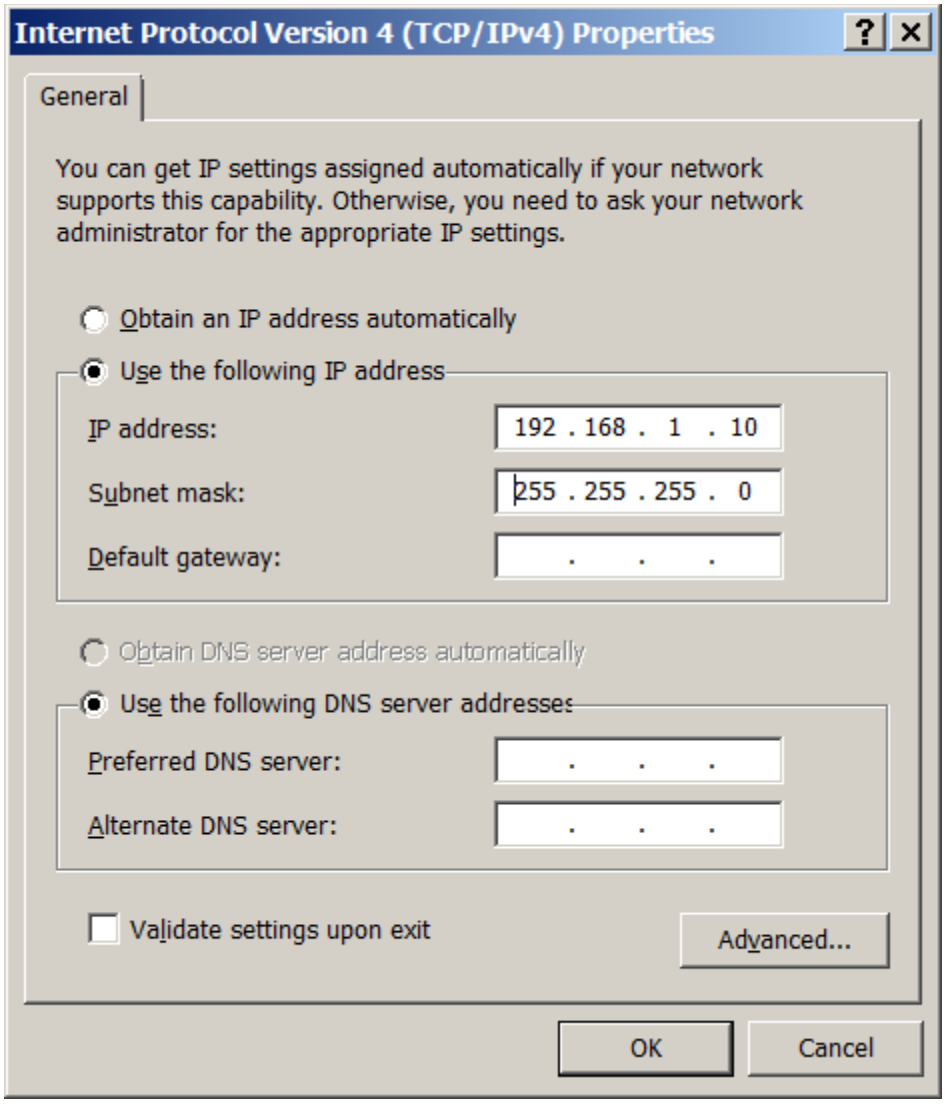
e. Click **Properties** to display your system's current Internet Protocol properties.

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.

f. Select **Use the following IP address**.

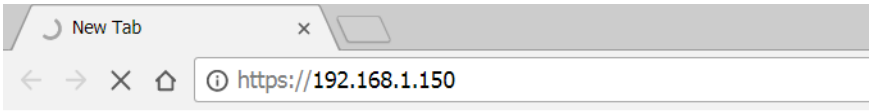
g. Enter **192.168.1.10** in the IP address field.

h. Enter **255.255.255.0** in the Subnet mask field.



i. Click **OK** to accept the entries.

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



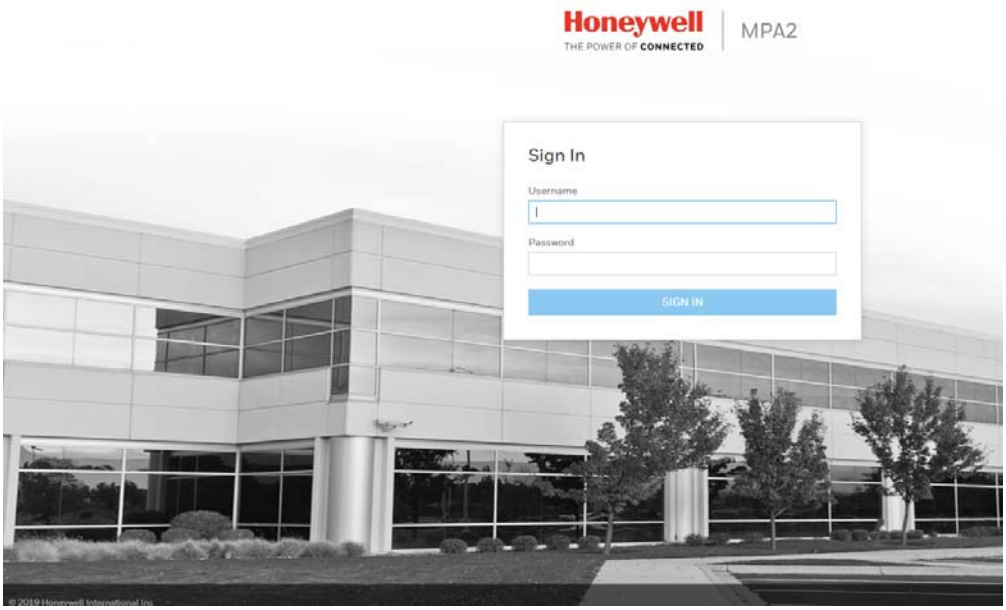
CAUTION **When connecting to the web using a browser, you must use https:// for a secure connection. The standard http:// that is the default in most browsers will not work.**

4. 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*.

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

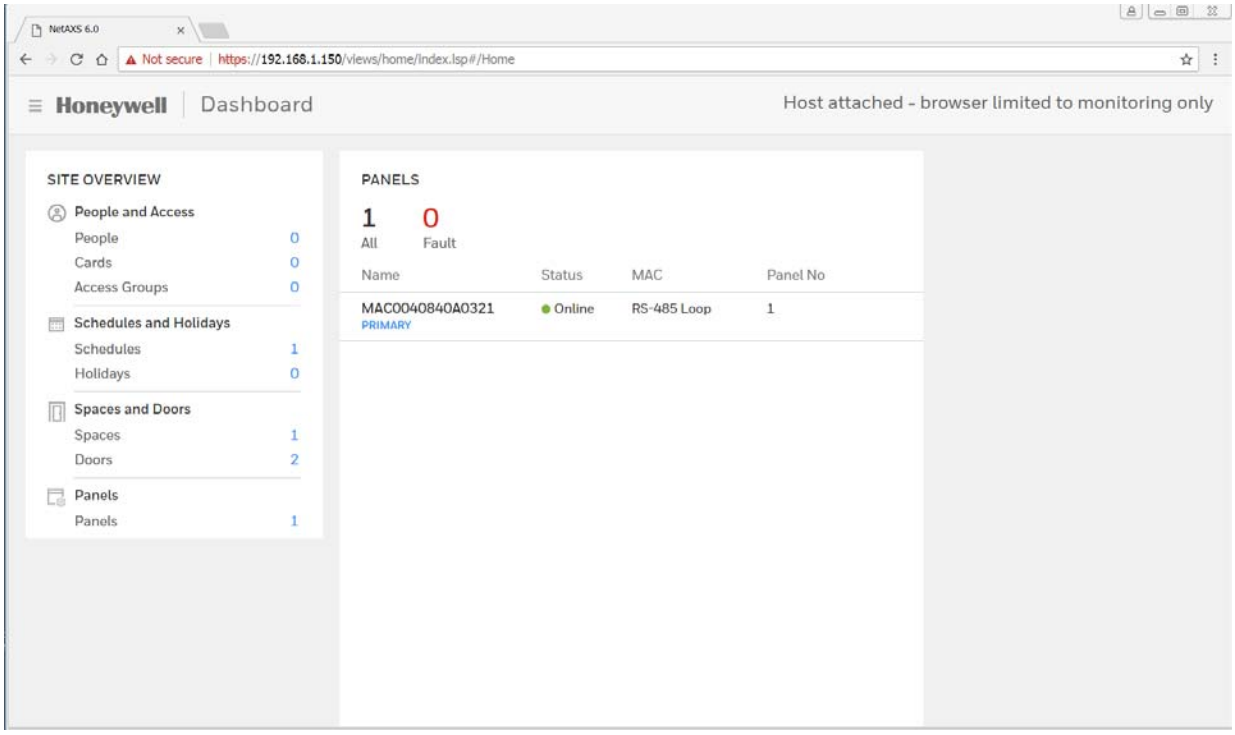
Note If you fail to log in successfully 5 times, the Retry Limit will be exceeded, and the account locks for 30 minutes. Any attempt to log into a locked-out account, within the timeout period, restarts the 30 minute lock-out period.

Note On initial signing in, you will be asked to change your password to a new password. For more information see *Creating MPA2 Accounts on page 119*.

6. 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

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

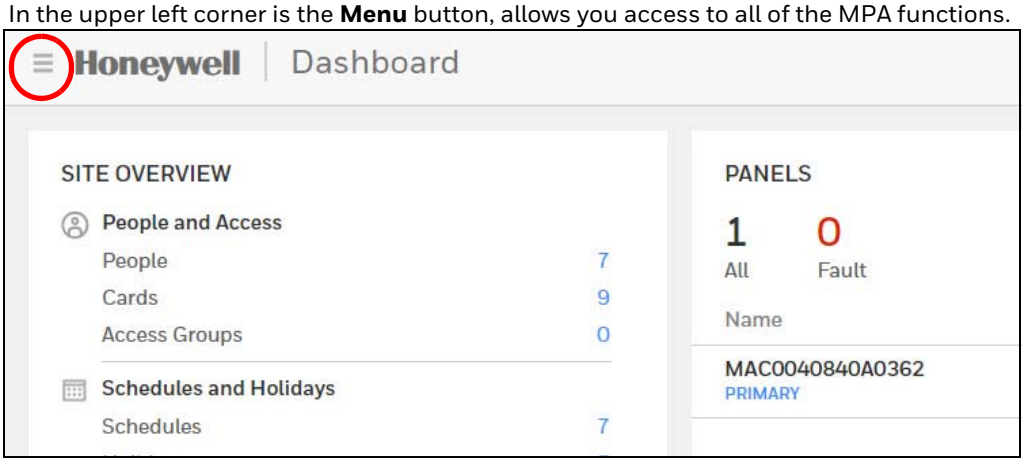


Figure 1-1 Main Menu

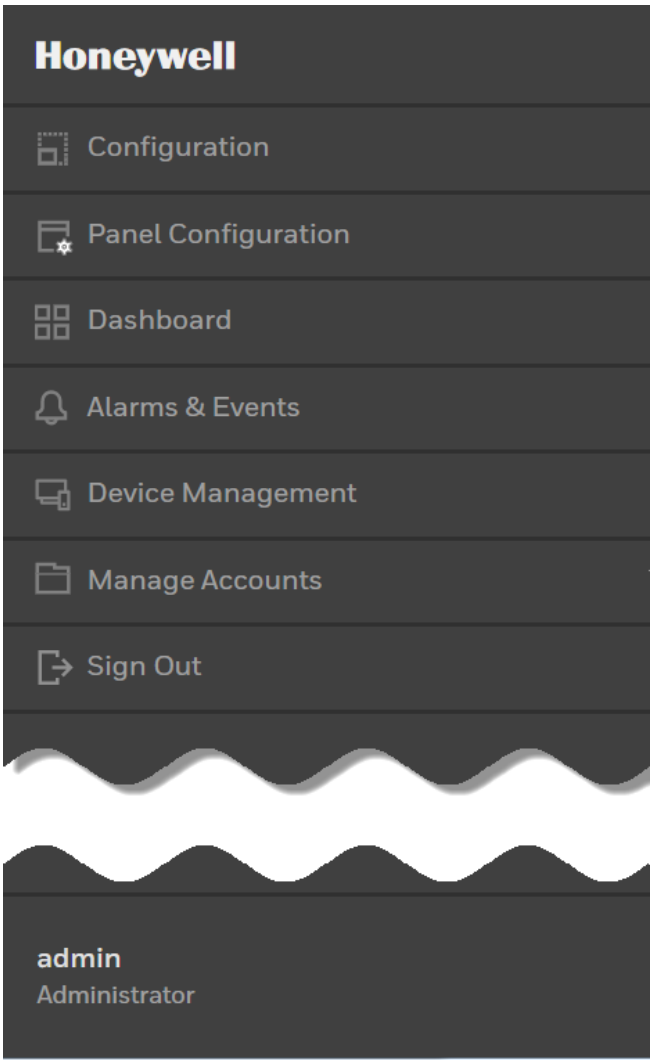
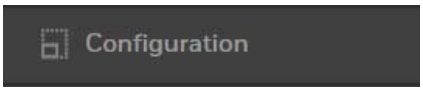
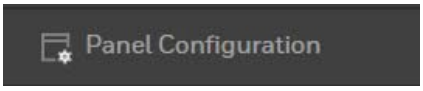
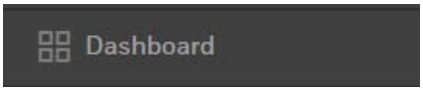
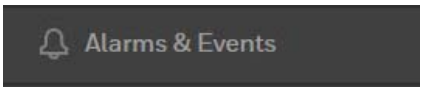
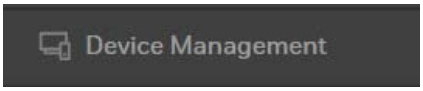
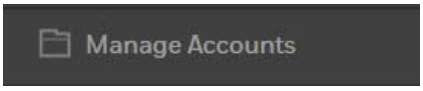
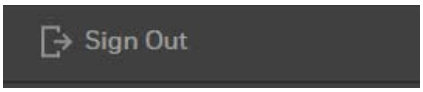


Table 1-1 Main Menu Selections

Icon	Description	For more information, see...
	Access configuration options for Spaces, Schedules, Holiday, People and Cards, and Access.	*Configuring Spaces on page 41*; *Configuring People and Cards on page 67*; *Entering a Panel Name on page 31*
	Access panel configuration options.	*Configuring the EVL (Ethernet Virtual Group) on page 18*; *Configuring the System Via RS-485 Loop on page 22*; *Initial Panel Setup on page 30*
	View the Configuration Summary, and the status of all the panels in the loop.	*Navigating through MPA on page 13*
	View alarms and events	*Monitoring Alarms and Events on page 77*; *Table 3-1*
	Manage Spaces, Doors, and Auxiliary Connections (such as Inputs, Outputs, and Output Groups)	*Configuring Spaces on page 41*; *Configuring Doors on page 45*; *Configuring Panel I/O and Groups on page 53*
	Specify that an account is Administrator, Service, or Operator. Select Language Preference.	*Creating MPA2 Accounts on page 119*
	Sign out	
	The current user	

This page is intentionally left blank

Basic Settings

Overview

This chapter explains the MPA2 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 MPA2 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) on page 18*
OR	
Configure the system via RS485	*Configuring the System Via RS-485 Loop on page 22*
Initial panel setup	*Initial Panel Setup on page 30*
Configuring schedules	*Configuring Schedules on page 37*
Configuring spaces	*Configuring Spaces on page 41*
Configuring people and cards	*Configuring People and Cards on page 67*
Configuring access groups	*Configuring Access Groups on page 74*

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)

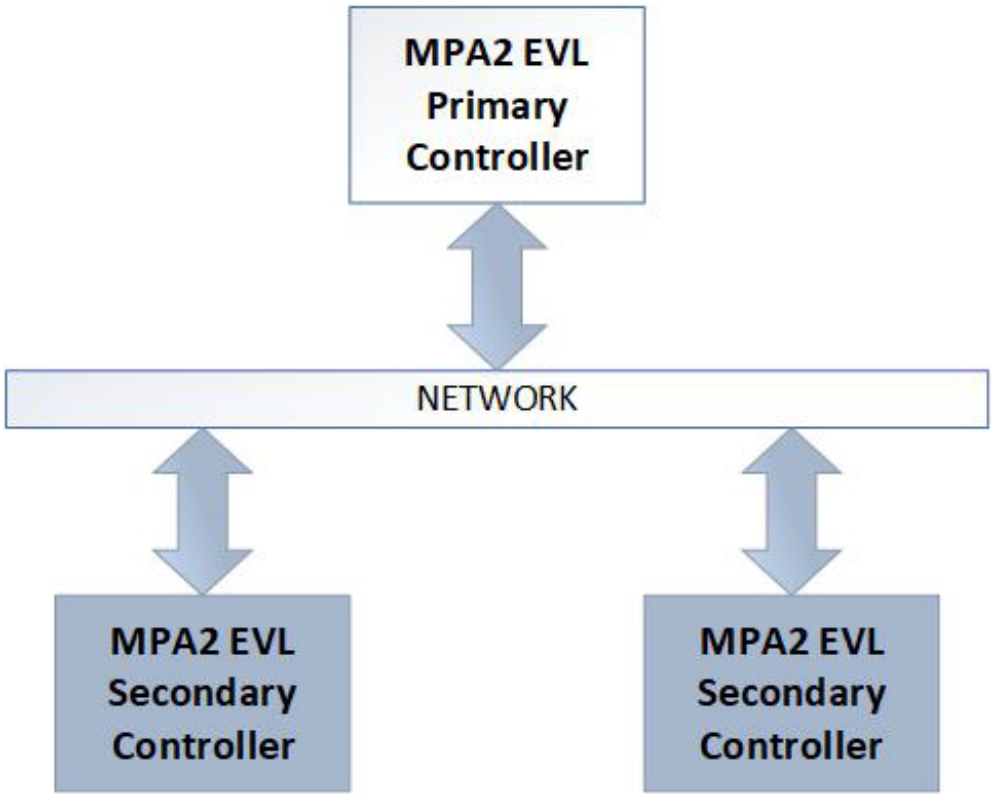
What is an EVL?

An Ethernet Virtual Loop (EVL) allows a group of IP network connected MPA2 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 MPA2 panel is used in EVL mode, DIP (dual in-line package) switches 5-9 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.

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.

Configure other controllers as Secondary controllers by setting DIP switch 3 to OFF.

Table 2-2 Primary DIP Switch Settings (EVL Mode)

DIP Switch (SW1)	Setting
9	On
8	Off
7	Off
6	Off
5	Off
3	On

Table 2-3 Secondary DIP Switch Settings (EVL Mode)

DIP Switch (SW1)	Setting
9	On
8	Off
7	Off
6	Off
5	Off
3	Off

Creating an EVL

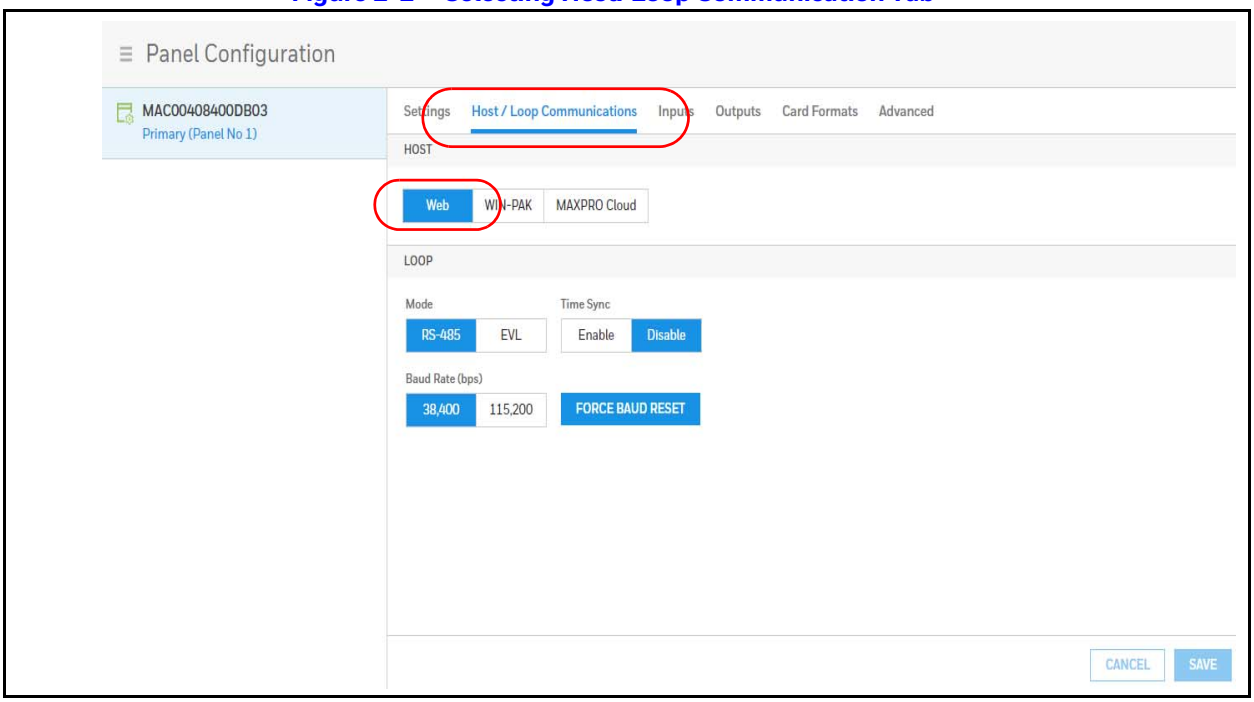
Connect all Controllers to a common IP network. The Secondary IP controllers must have DIP switch 3 set to OFF, and will be configured using the Primary controller.

1. Log into MPA2 Primary panel from a browser through the USB (https://192.168.2.150) or Ethernet connection (https://192.168.1.150).

   See *Setting Up the USB Connection 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



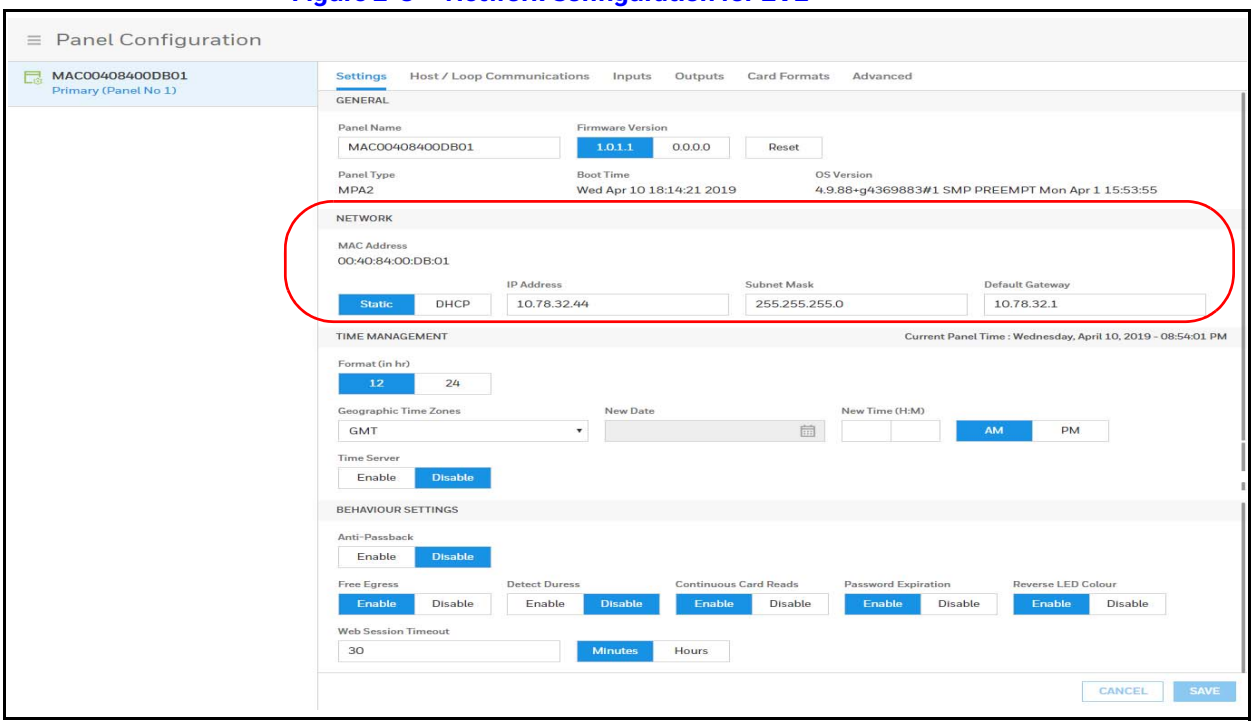
3. Set up Communication attributes (see *Figure 2-2*):
   a. Select **Web** as Host Connection Type.
   b. Select **Ethernet Virtual Loop** as Mode.
   c. Click **Save**. The panel automatically reboots.
4. Log into the MPA2 panel.

   See *Setting Up an Ethernet Port on page 8*.
5. Set up Network Configuration (see *Figure 2-3*):
   a. Navigate to the **Network** field on the **Settings** tab.
   b. Select **DHCP** or enter **Static IP** address assigned to Primary panel.
   c. 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



6. Log into the Primary controller from a browser.

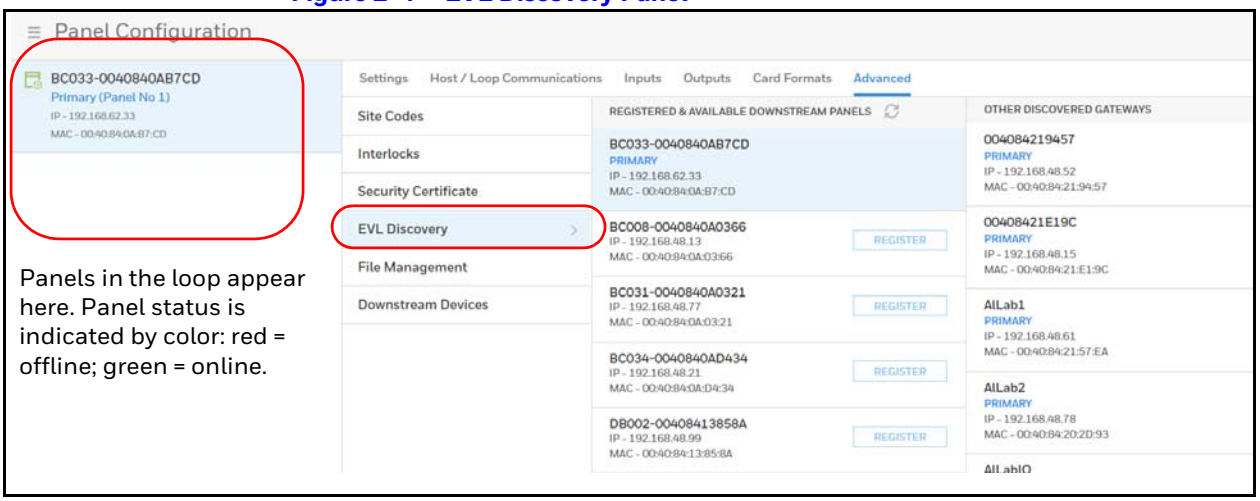
   See *Setting Up an Ethernet Port on page 8*.

7. Register Secondary EVL controllers (see *Figure 2-4*):

Note Only secondary panels can be Registered and Unregistered.

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

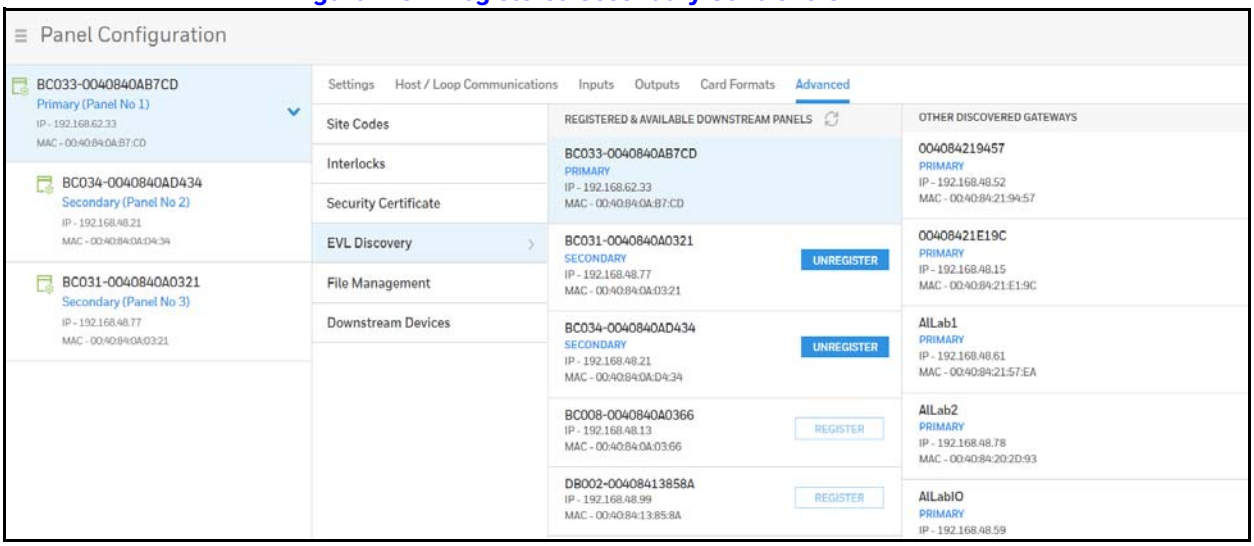
Figure 2-4 EVL Discovery Panel



Discovered panels appear automatically.

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

Figure 2-5 Registered Secondary Controllers



You have now finished creating an Ethernet Virtual Loop.

Configuring the System Via RS-485 Loop

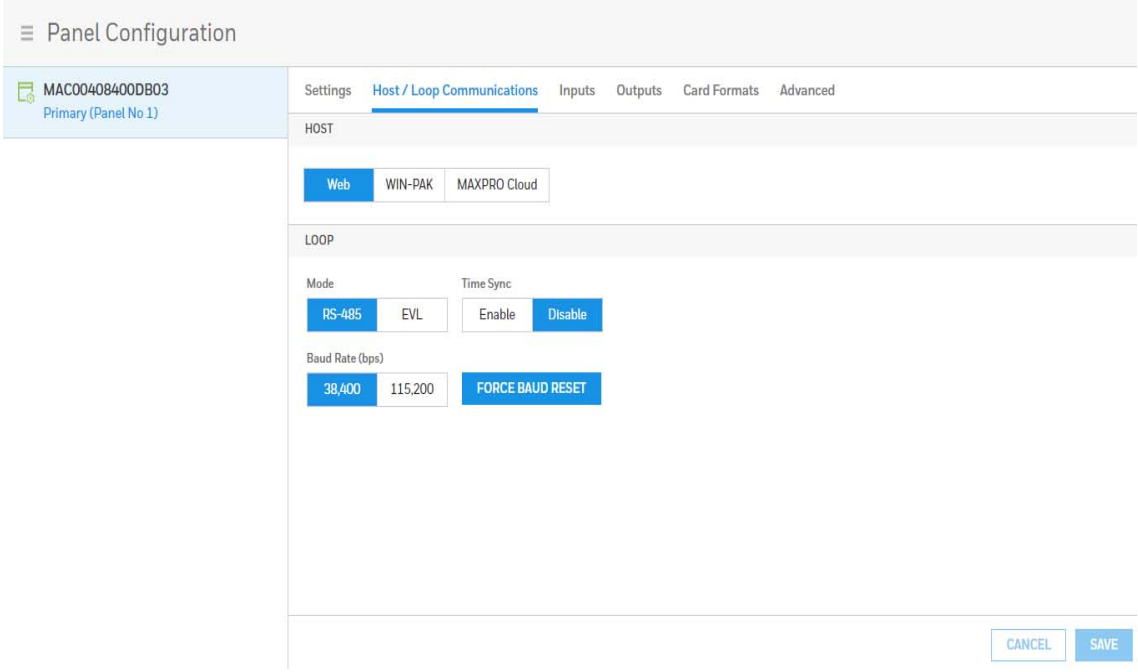
By default, the Loop Mode is set to RS-485. If it was set EVL and the user set it back to RS-485, the panel will automatically reboot. Panels in a RS-485 loop are wired together in daisy chain fashion Up to 31 controllers may be wired together in a RS-485 loop; that is one primary and up to 30 secondary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

IMPORTANT: Only 1 Primary controller may be in a RS-485 loop. All of the Secondary controllers must have DIP switch 3 set to the OFF position.

1. Log into MPA2 Primary panel from a browser through Ethernet (default 192.168.1.150), or USB (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.



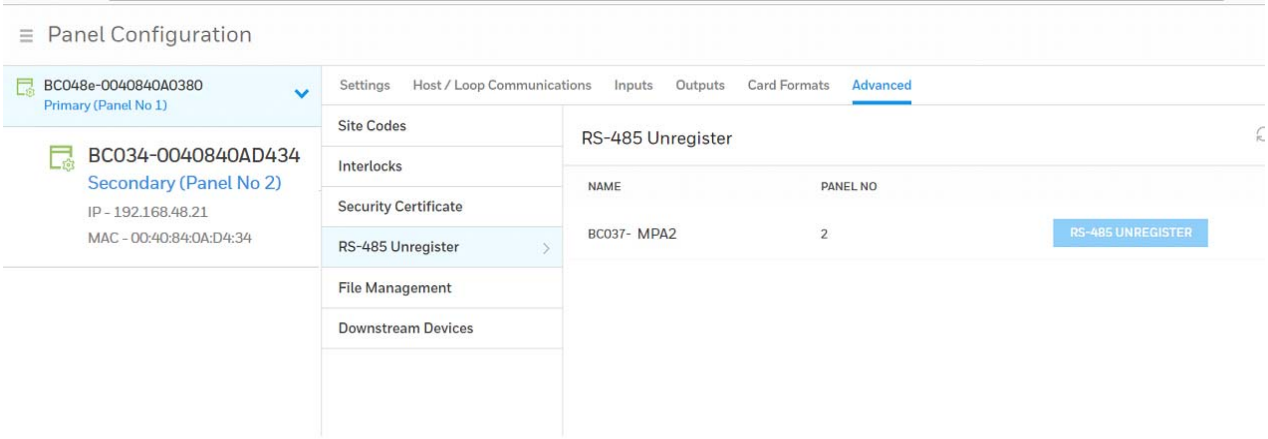
3. Set up Communication attributes
   a. Select Web as Host Connection Type.
   b. Select RS-485 as Mode.
   c. Click Save. The panel automatically reboots.
4. Log into the MPA2 panel.

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)
- Web Users (applies only to primary panel)

Configuring Host/Loop Communications

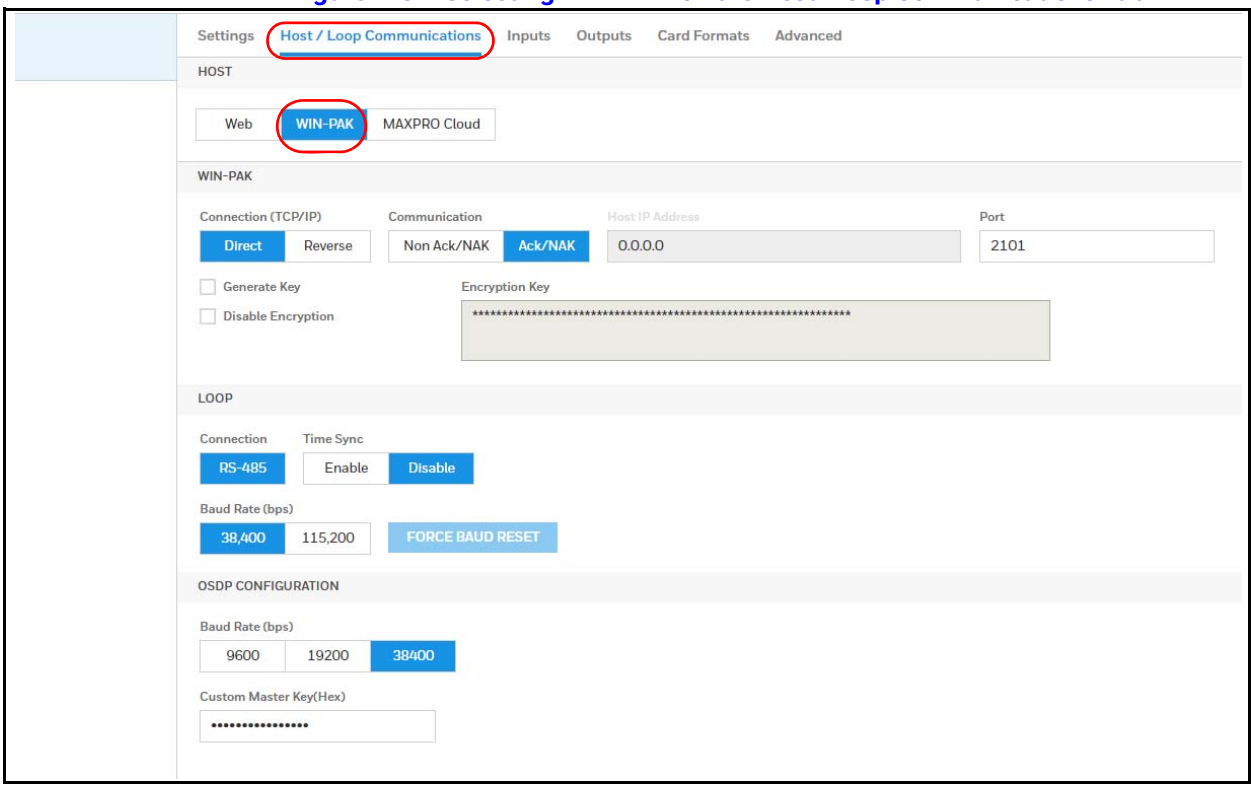
To maintain your MPA2 system configuration or to monitor its status, you must connect to the panel using one of three modes:

- **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 Host Mode

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 2-4 WIN-PAK Host/Loop Communications Mode Settings

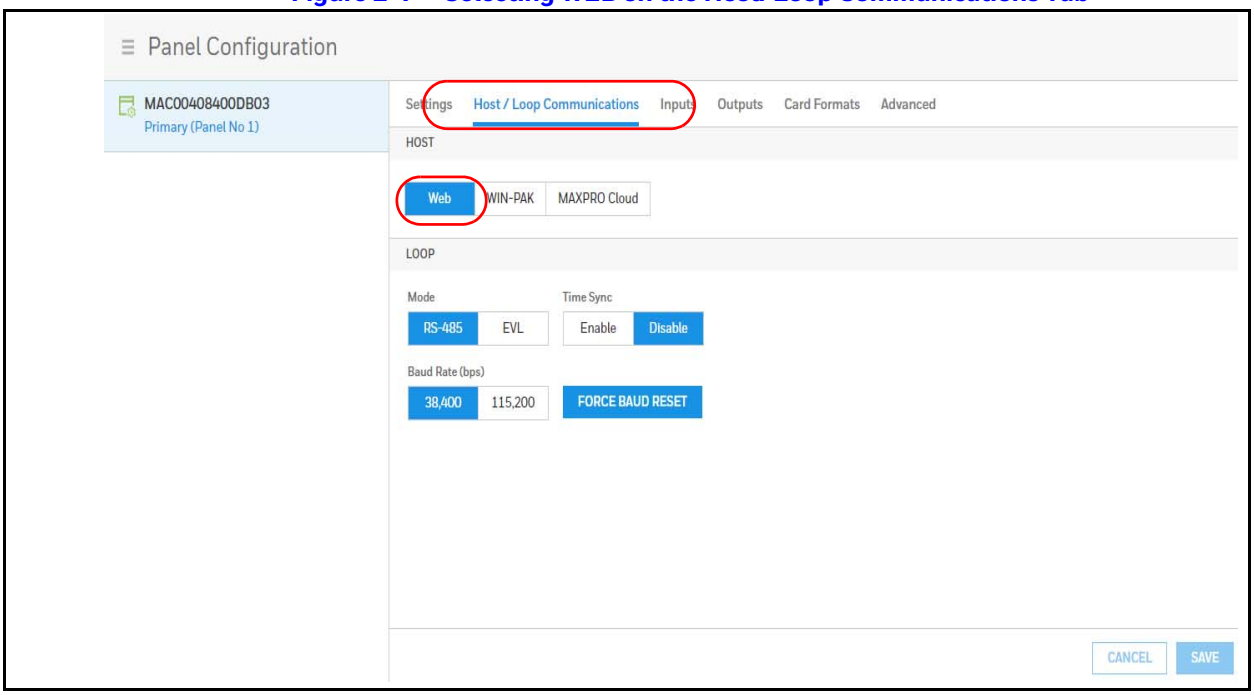
Host/Loop	Setting	Description
Host	**Connection Type**	Specifies the type of physical connection between the host and the Primary panel. If you are connecting from a host software system such as WIN-PAK, select one of the following two connection options: **Direct via TCP/IP** – Host initiates connection to panel. **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.
	Communication Type	Specifies the type of communications. **Ack/NAK** – Provides a response (either an acknowledgment or a non-acknowledgment) in a transmission between the host and panel(s). This is the recommended communications type. **Non Ack/NAK** – Does not provide a response (either an acknowledgment or a non-acknowledgment) in a transmission between the host and panel(s). Normally used in troubleshooting only.
	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. Port 5001 is Reverse TCP/IP.
	Generate Key	Click to create and display a new encryption key. **Note** Whenever this box is checked and the page is saved, the new key must be entered in WIN-PAK.
	Disable Encryption	Select to disable encrypted communication between MPA2 Primary and WIN-PAK Host. Disabling encryption creates an insecure system and is not recommended.
	Encryption Key	This is the password/key used to encrypt communications between Primary and WIN-PAK Host. You must enter this password on WIN-PAK Host.
Loop	**Connection Type**	**RS-485** - If Primary provides access to RS-485 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**.

Setting the Communication Mode to Web

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

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



3. Configure the host settings.

Table 2-5 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.

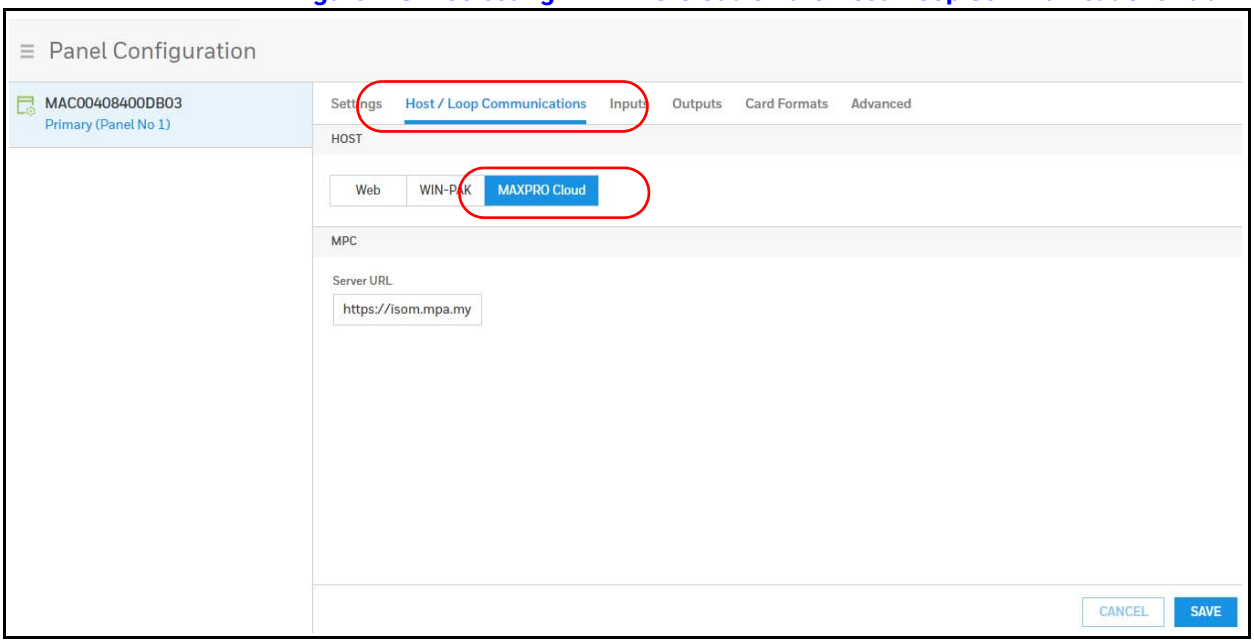
Note When switching from EVL to RS-485 mode, if the EVL primary can not communicate with the DS controller, then the DS controller remains an EVL controller until it is set back to factory defaults.

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



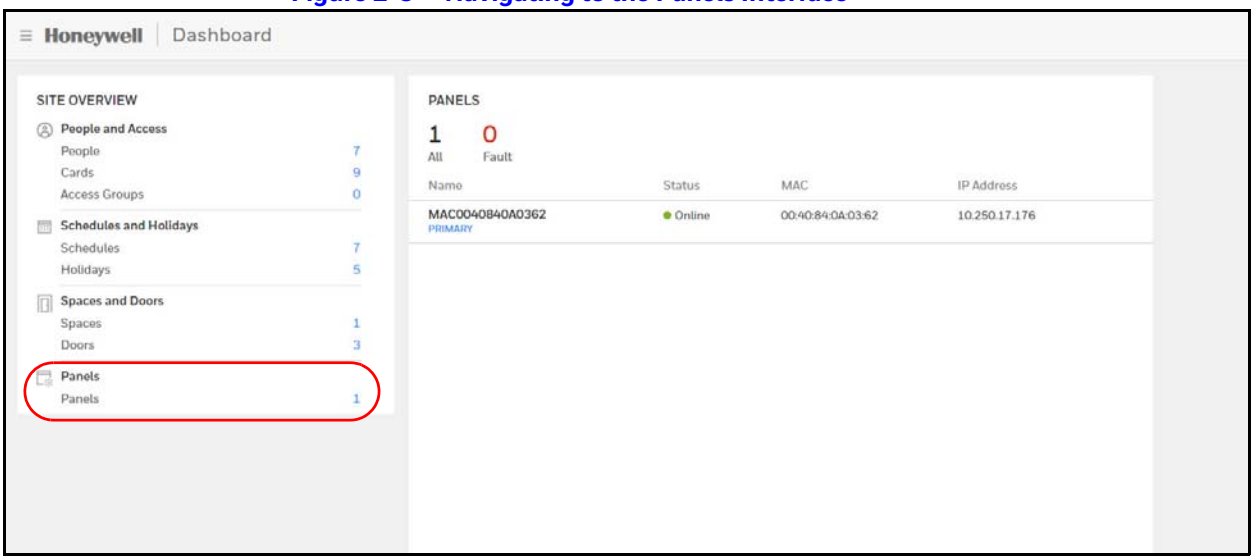
3. Enter the **Server URL**.
4. Click **Save**.

Initial Panel Setup

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

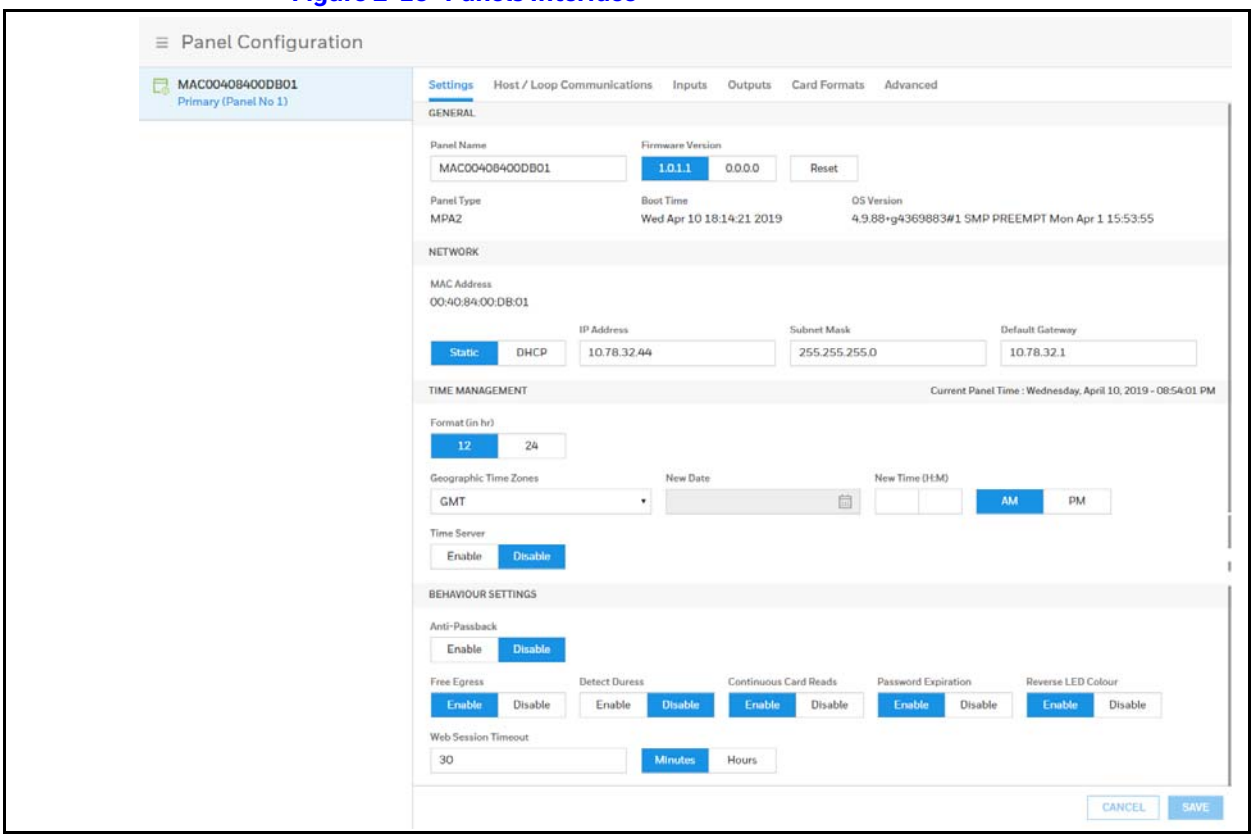
- Click **Panels** in the Dashboard to access the **Panels** interface, or

Figure 2-9 Navigating to the Panels Interface



- Click **Panel Configuration** in the Menu.

Figure 2-10 Panels Interface

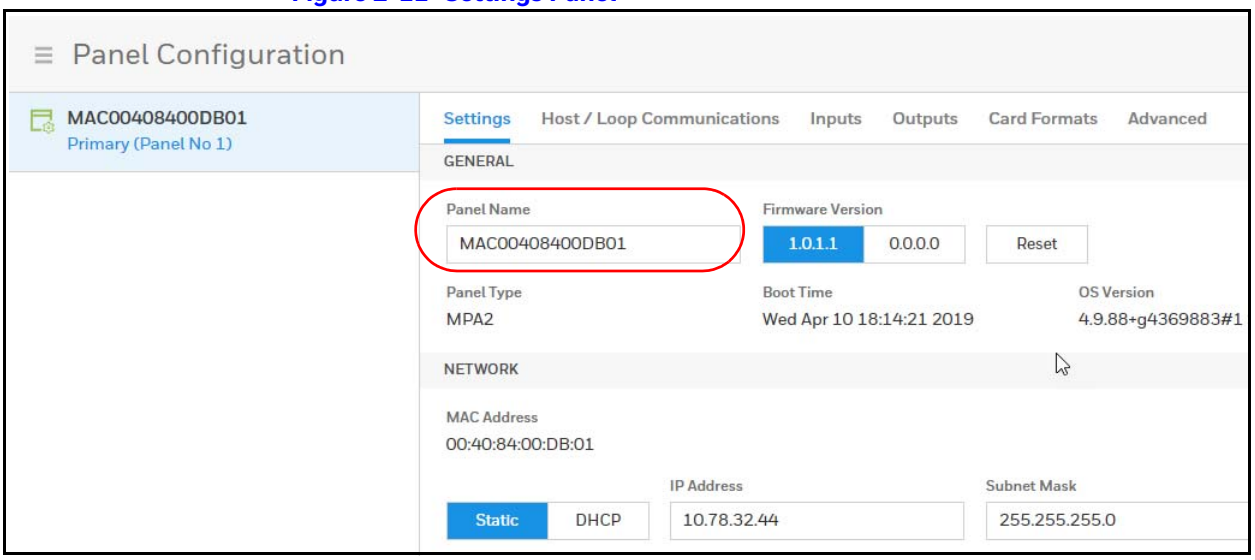


Entering a Panel Name

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



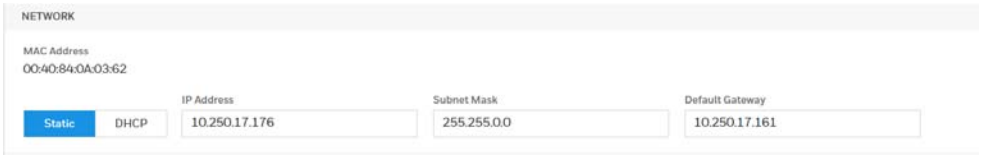
2. Click the **Panel Name** field, and then enter a panel name.
3. Click **Save**.

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 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.

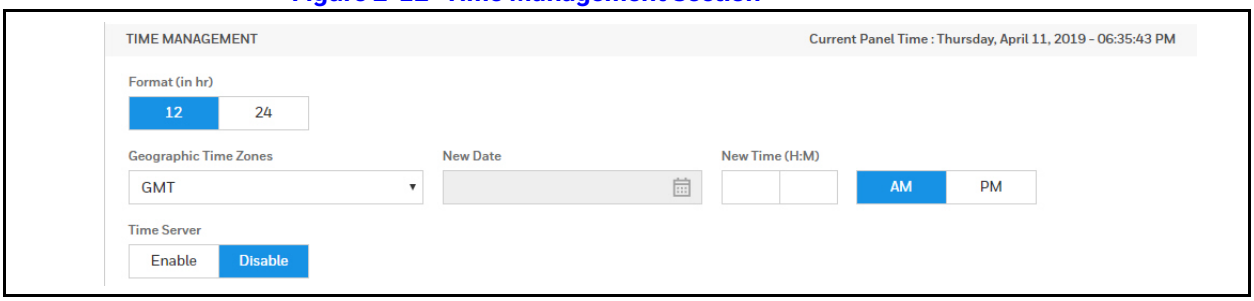
Configuring Time Management

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 2-12 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.

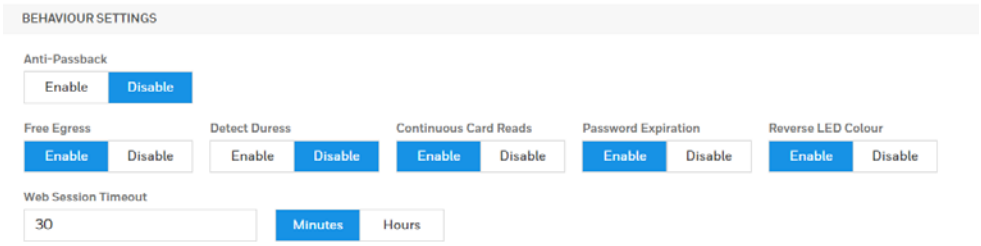
Host/Loop Communications Tab

- Synchronizes the primary panel's time with the secondary panels.

Table 2-6 Time Settings

Tab	Setting	Description
Settings	**Current Panel Time**	Displays by default the current time setting in Day / Month Date / Year - HH:MM:SS AM/PM
	Format	**12 hour** – The 24-hour day is divided into two 12-hour halves, AM and PM; each half is numbered 1-12. **24 hour** – The hours in the 24-hour day are numbered consecutively 0-23. **Note** Format does not affect the format displayed on the Alarms & Events page as they are always reported in 24-hour time format.
	Geographic Time Zone	Select the geographic time zone in which the panel will operate. The time zones are written in the [`continent/city`] format. Find the appropriate continent, and then identify the city with the closest longitude to the panel's location. In the United States, you might find these time zone associations more familiar: **Eastern Time**: America/New York **Central Time**: America/Chicago **Mountain Time**: America/Denver **Pacific Time**: America/Los Angeles
	Date	Specifies a new date to be the current date. Click on the calendar icon to select a year, month, and day.
	Time	Specifies a new time to be the current time. Click to enter the time in Hours: Minutes, then click to select **AM** or **PM (if 12 hour format is selected)**.
	Time Server	Enter the IP address/URL of the Time Server (Time Server is enabled by default) that the Primary will poll to update its time. **Enabled** – Select to enable the specified machine to be the active time server. **URL** – Enter the URL of the time server. Default URL is time.honeywell.com pool.ntp.org **Update Interval** – Specifies the interval of time between each automated synchronization. Recommended value is once per day. Default interval time is 32 minutes. The panel starts to update time as soon as it is enabled and successfully connects to the Time Server; it continues to update according to the interval selected from that start point. Select the update interval, in Minutes or Days. The Days range is 1 to 256 days. The minutes range is 15 to 999 minutes.
Host/Loop Communications	**Time Sync**	**Enable/Disable Time Sync**. Enabling Time Sync synchronizes the secondary panels with the main panel.
	Time (in mins)	Enter a value for how often the MPA2 panels checks and synchronizes the panel times. Enter between **60** and **32,767** minutes.

Configuring Behavior Settings



In the Behavior Settings section of Panel Configuration, you can enable/disable the following:

- 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.
- Free Egress–Configures the panel for free egress. When enabled (Default), the panel automatically configures inputs 1and 9 to act as egress inputs for Doors 1 and 2, respectively. If disabled, those inputs 1 and 9 can be used as general inputs.
- Detect Duress–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.

- Continuous Card Reads – Enables continuous card reading while the output is being energized. When this option is not enabled, a reader will not be able to read a second card during the pulsing of the output 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.
- 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 MPA2 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.

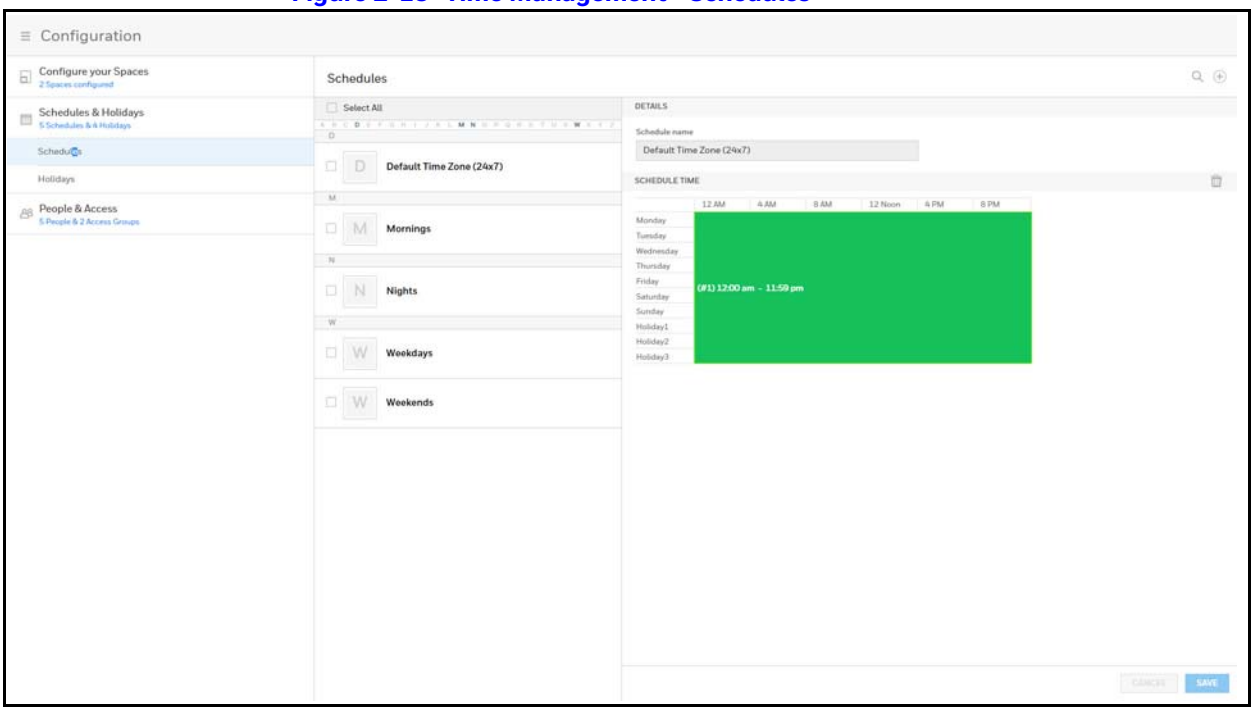
For example, you might assign a group of outputs to be energized from 12:00 AM to 6:00 AM. every day. The 12:00 AM to 6:00 AM, Sunday through Saturday, time period is called a schedule.

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 2-13 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  .
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 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).

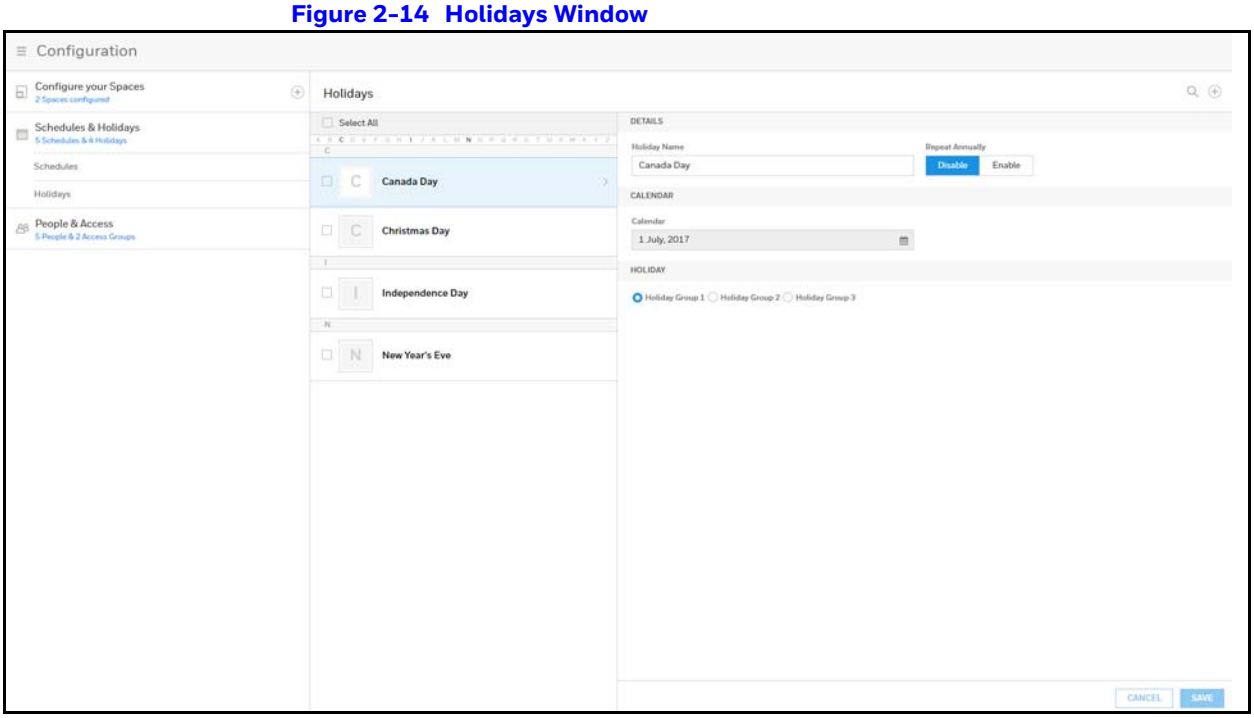
During this Holiday, only Schedules that contain that specific Holiday type work. The Holidays window enables you to further customize how the panel works. For example, you can block access to a building on that day, or grant special access during that day.

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 2-14 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.

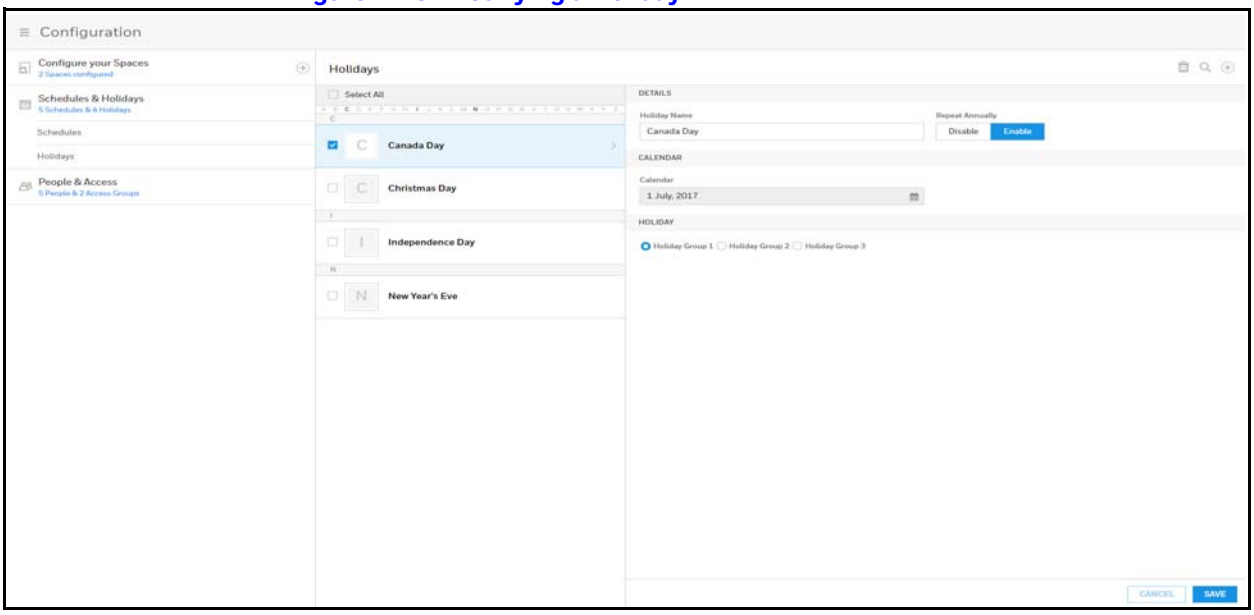
   Assigning a holiday to a Holiday Group maps that holiday to a schedule configuration. The holiday then follows the rules of that schedule. (See *Configuring Schedules on page 37*).
6. Click **Save**. A message appears to confirm that the new holiday was saved.

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 2-15 Modifying a Holiday

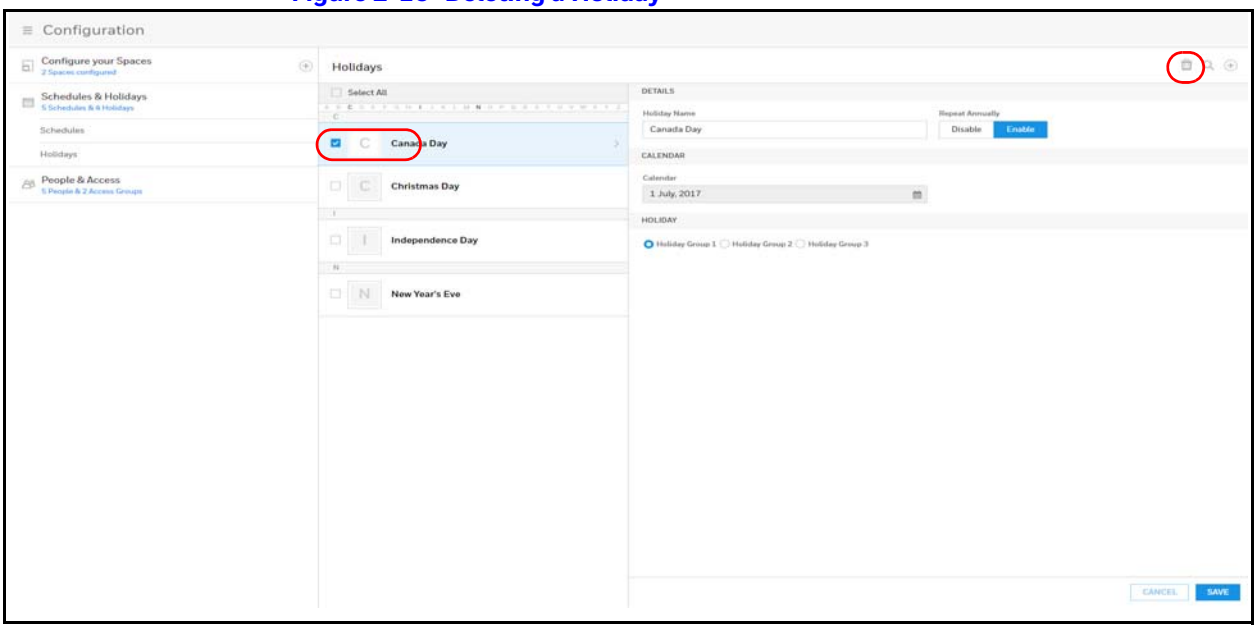


2. Modify the holiday.
3. Click **Save**. A message appears to confirm that the charges were saved.

Deleting a Holiday

1. Click to select the holiday.

Figure 2-16 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.

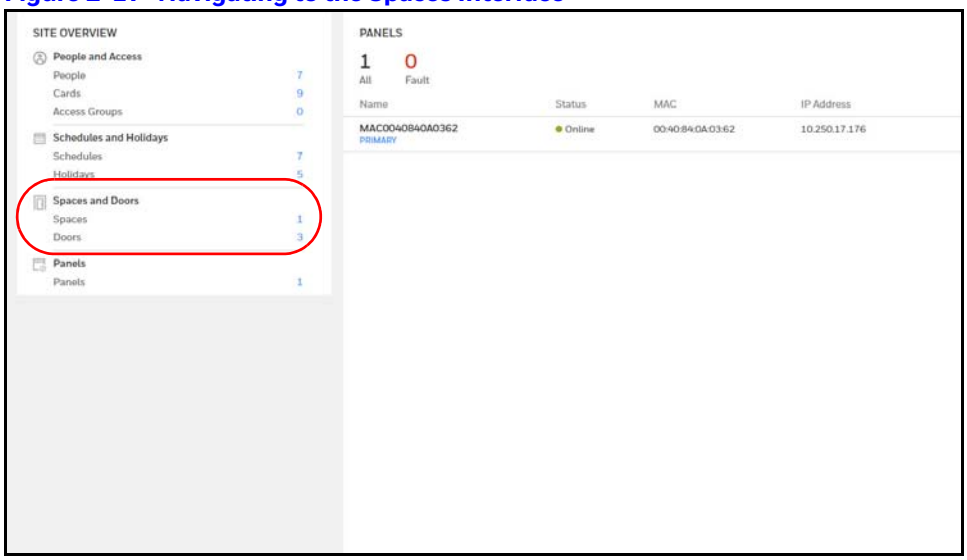
Configuring Spaces

Configuring Spaces

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

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

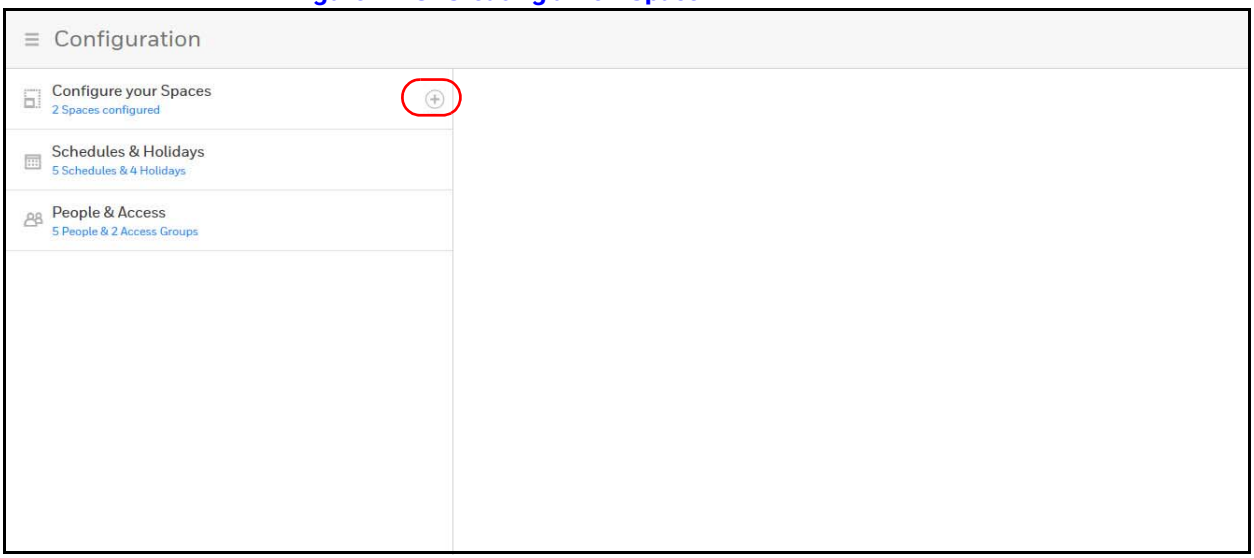
Figure 2-17 Navigating to the Spaces Interface



- Or click **Configuration** in the **Menu**.

2. Click ⊕ to create a new space.

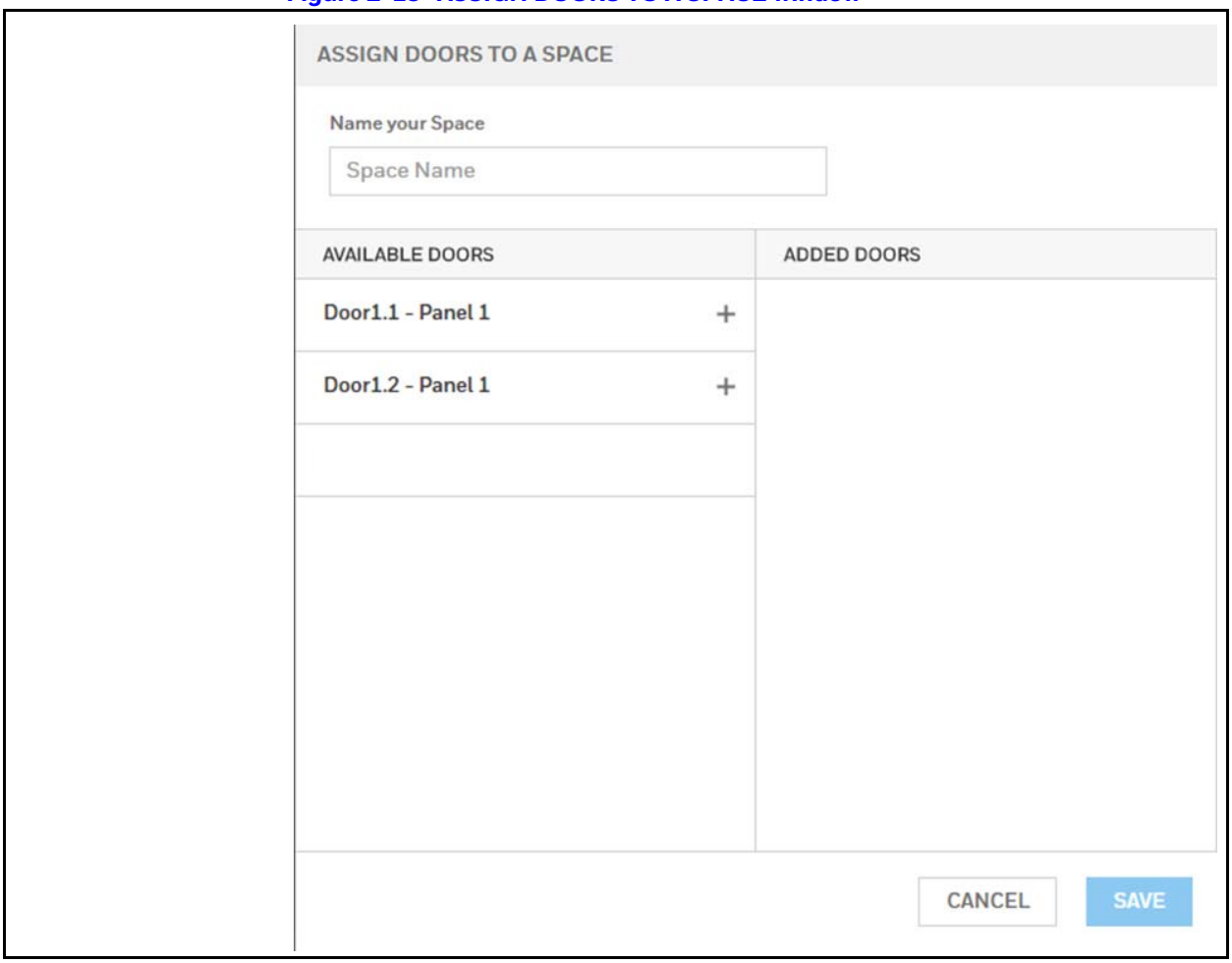
Figure 2-18 Creating a New Space



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.

Figure 2-19 ASSIGN DOORS TO A SPACE window



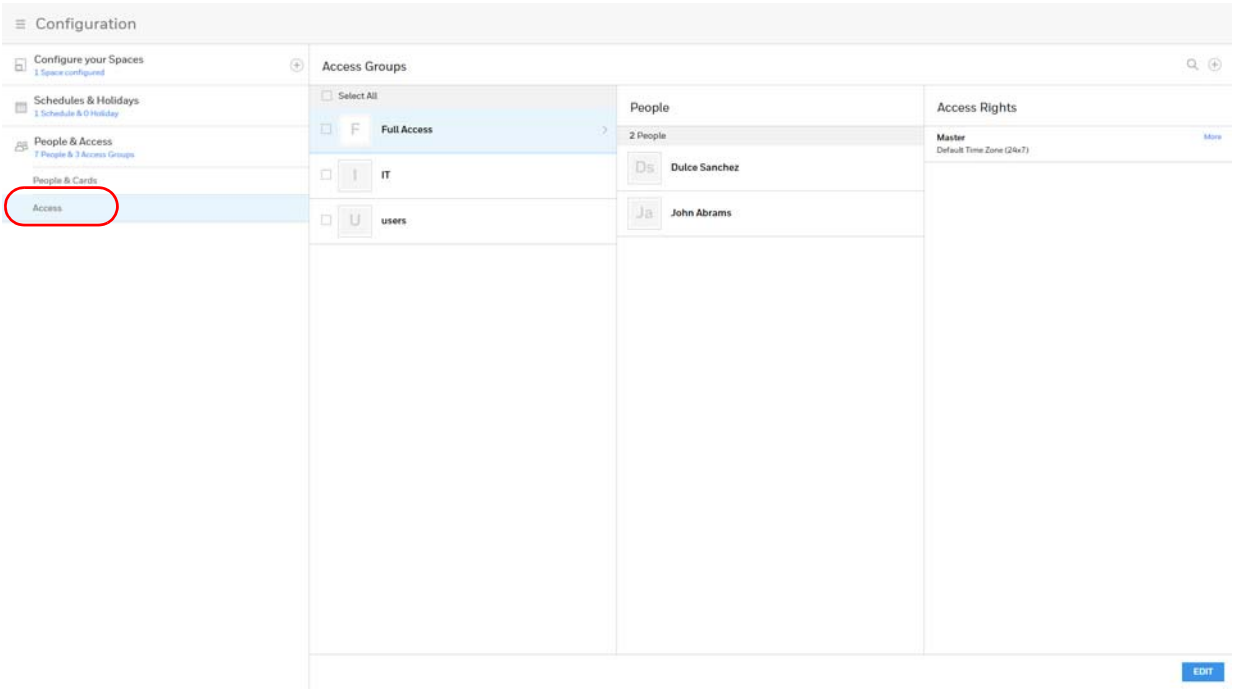
3. Enter a space name in the **Name your Space** field.
4. Click + in the **AVAILABLE DOORS** pane to select the door. The door appears in the **ADDED DOORS** pane.
5. Click **Save**. A message appears confirming the new Space.

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

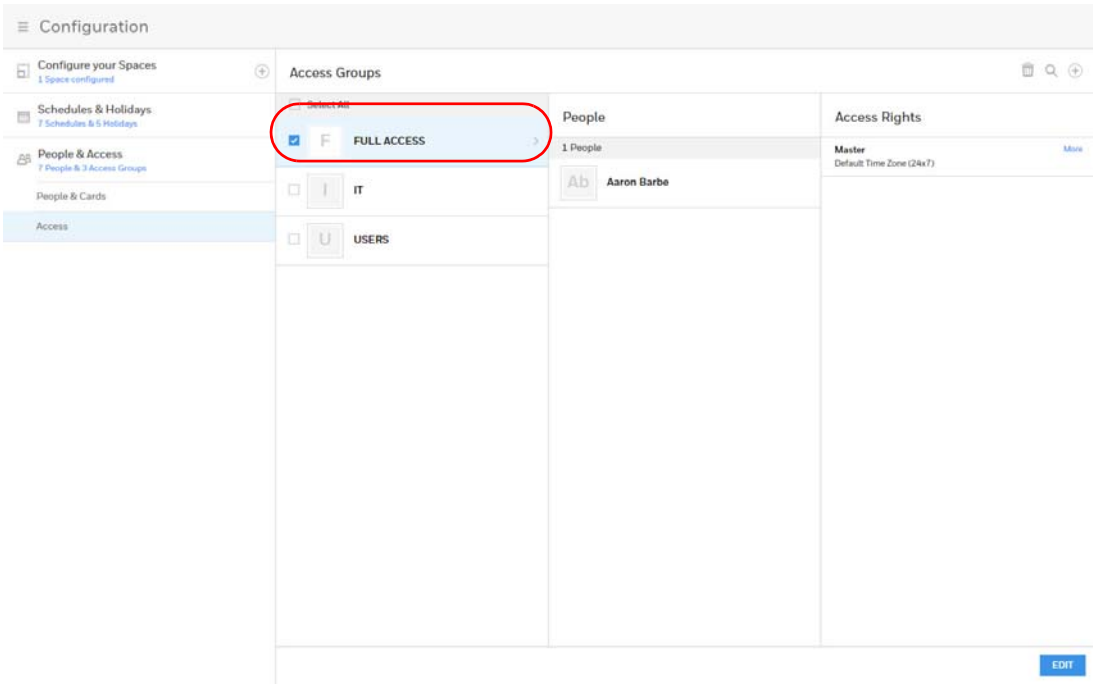
1. Click **People & Access** > **Access Group** > **Access**.

Figure 2-20 Access Groups Interface



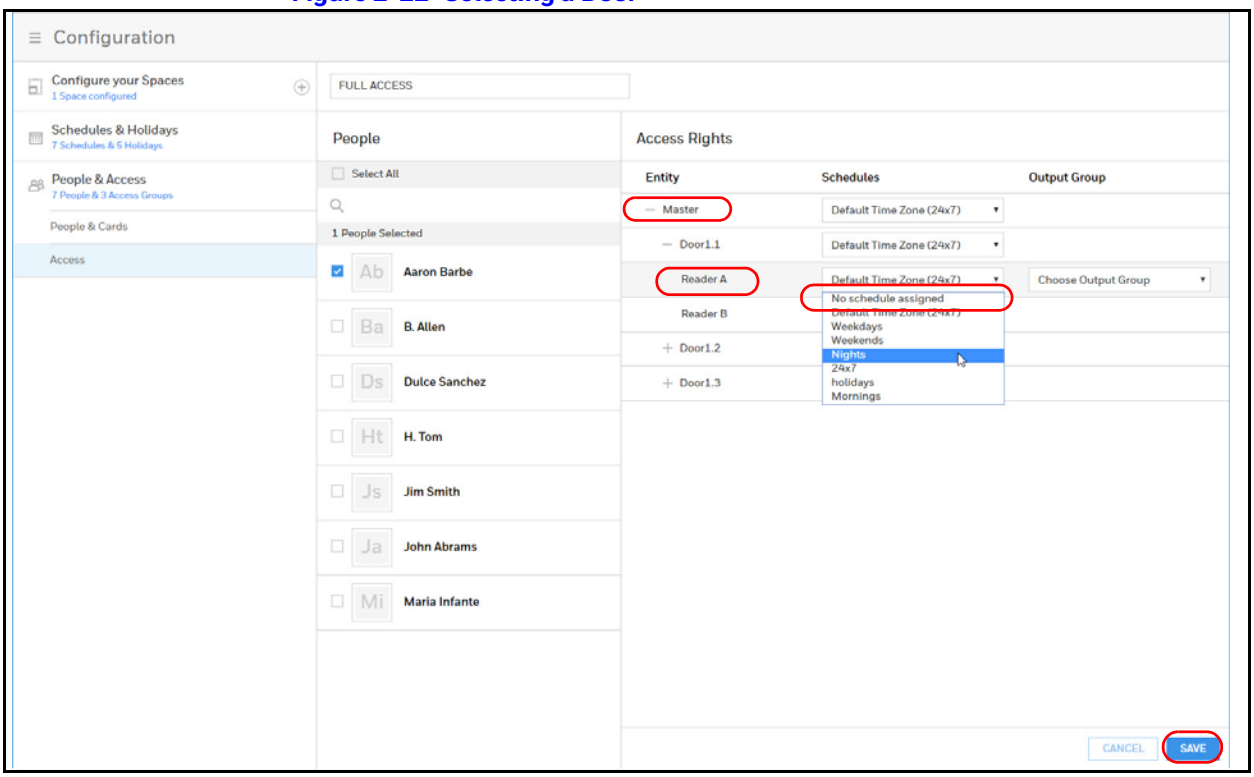
2. Click to select an **Access Group**, then click **EDIT**.

Figure 2-21 Selecting 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** drop-down menu.

Figure 2-22 Selecting a Door



5. Click **Save**.

Configuring Doors

Each panel supports from 1-9 doors. For each door, you must configure the readers, inputs, and outputs.

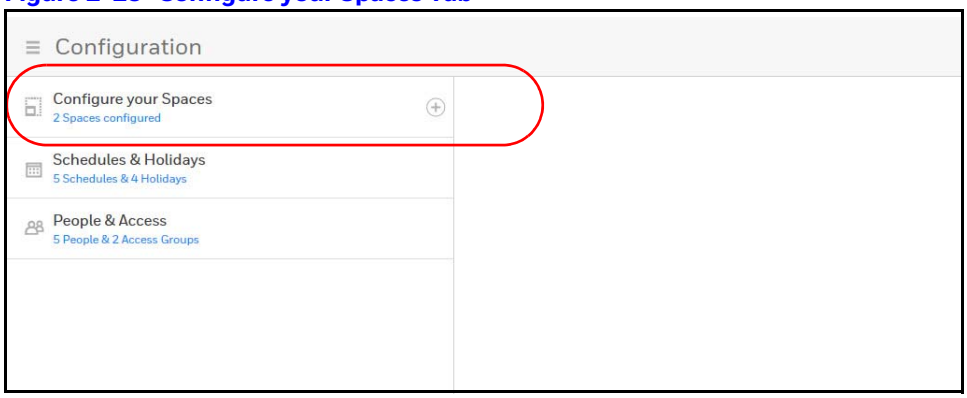
> **Note** You must assign doors to a Space before you can configure the doors. See *Configuring Spaces on page 41*.

Accessing the Doors Configurations

1. Navigate to the **Configure your Spaces** tab by doing one of the following:

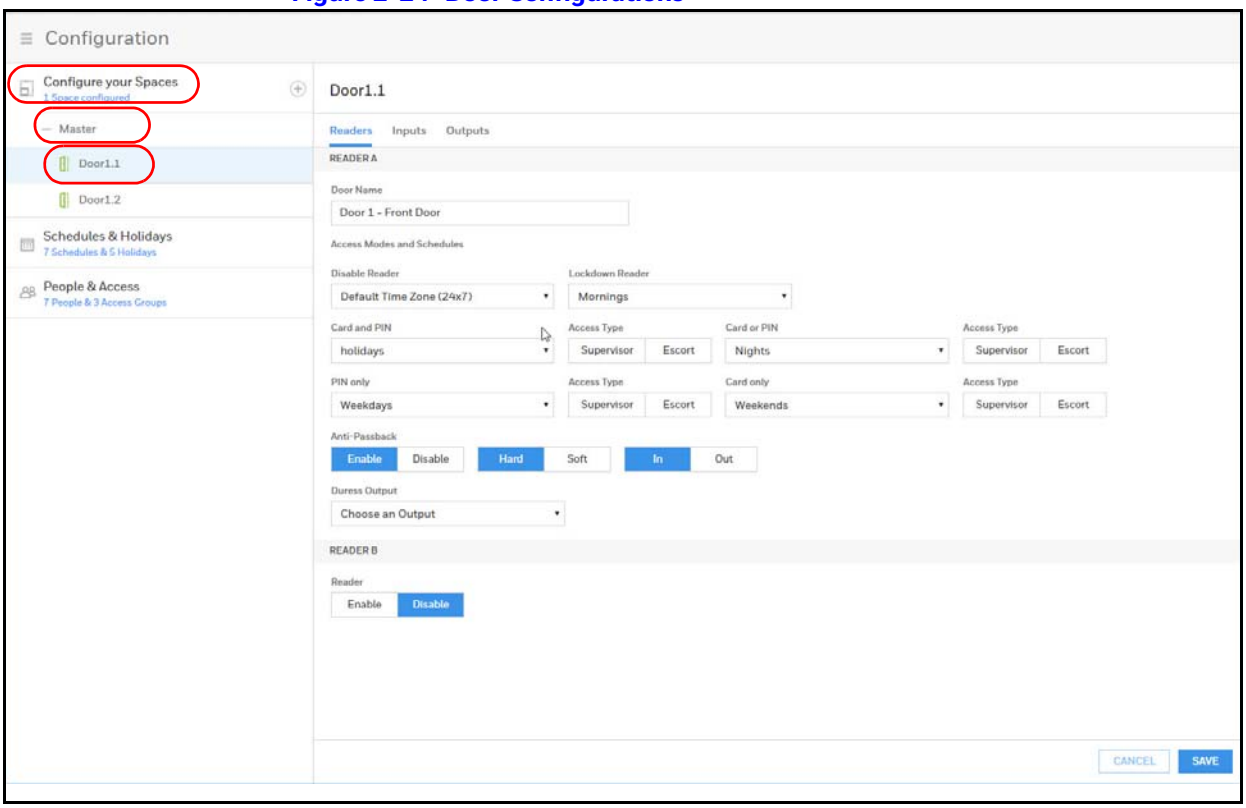
- Click **Menu** > **Configuration**, or
- Click **Spaces** in the **Dashboard**.

Figure 2-23 Configure your Spaces Tab



2. 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 2-24 Door Configurations

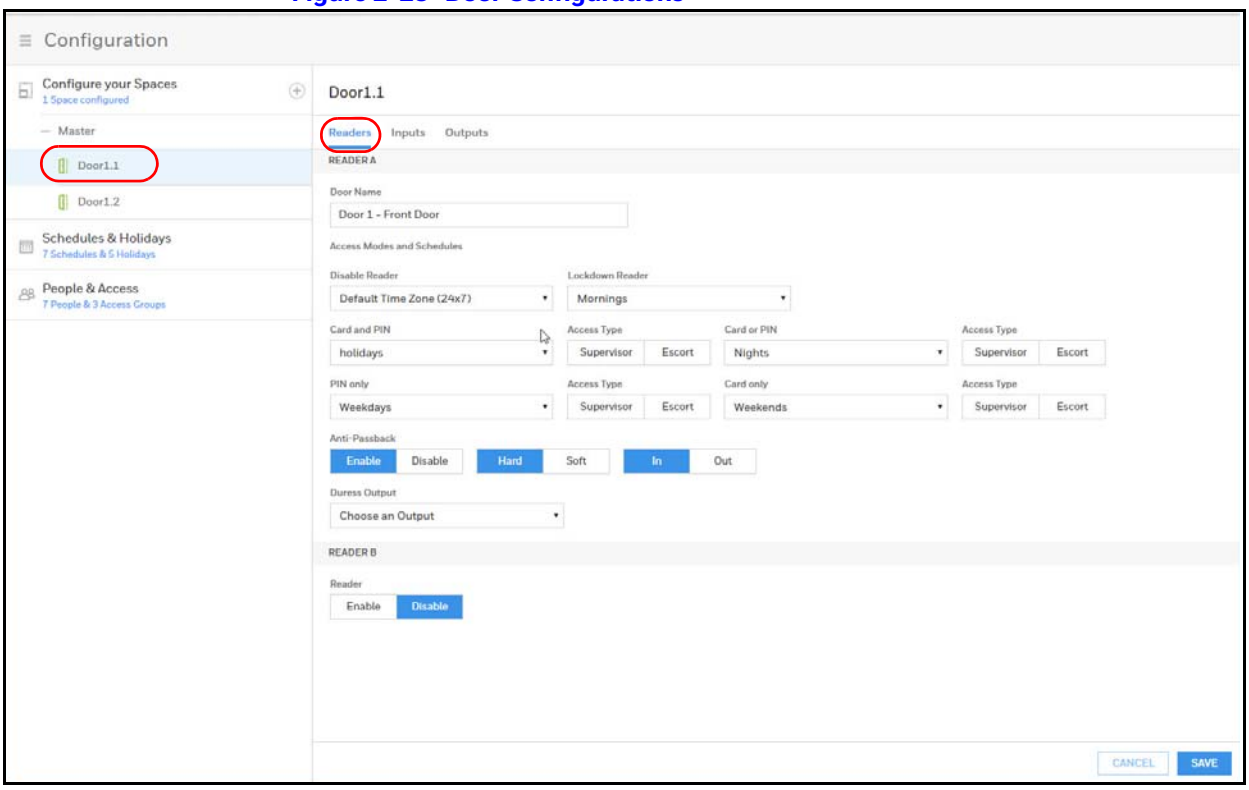


Configuring Door Reader Settings

The Reader settings tab allows you to configure the following settings for both Readers A and B for each door:

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

Figure 2-25 Door Configurations



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).

Table 2-7 Supervisor Mode LED Color Cycle

Action	LED Cycle	Reaction
Supervisor swipes card	N/A	Supervisor gains access but does not enable general access.
Supervisor swipes card again within 10 seconds of initial card swipe	LED turns a steady red	Enables General access.
Supervisor swipes card again twice consecutively	LED alternates red and green	Disables General access for the time zone

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 2-8 Escort Mode LED Color Cycle

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 alternates red and green	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 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 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 to **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 67* 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 MPA2 panel:

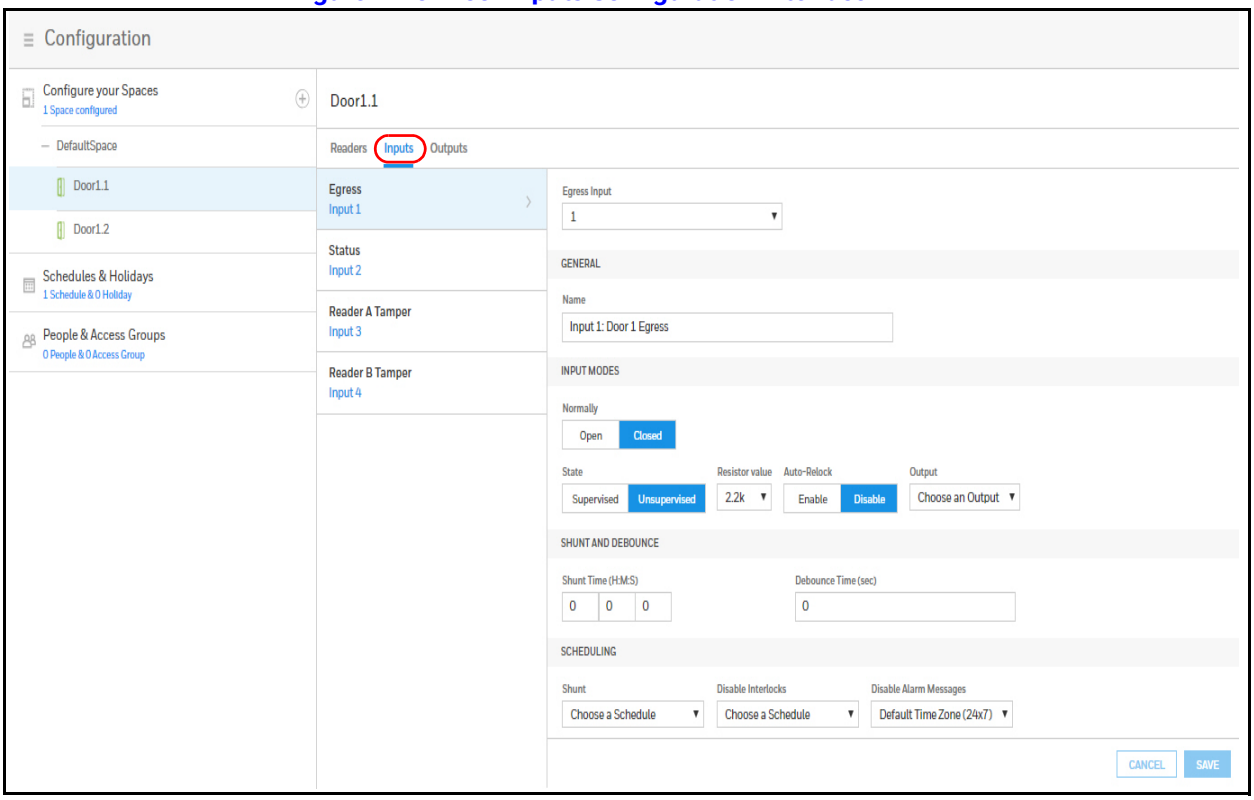
- **Status** – Provides door status information (Doorcnt).
- **Egress** – Allows the door to open or close normally without generating an alarm (REX).
- **Tamper A** – Reports abnormal handling of the reader device or wiring for Reader A.
- **Tamper B** – Reports abnormal handling of the reader device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

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

Figure 2-26 Door Inputs Configuration Interface



2. Enter an **Input Name**.

3. Select **Input Modes**.

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.
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. If you select Supervised, then you must select a Resistor value.
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.
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,

4. Configure Shunt and Debounce times.

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.

5. Configure Scheduling.

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 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.

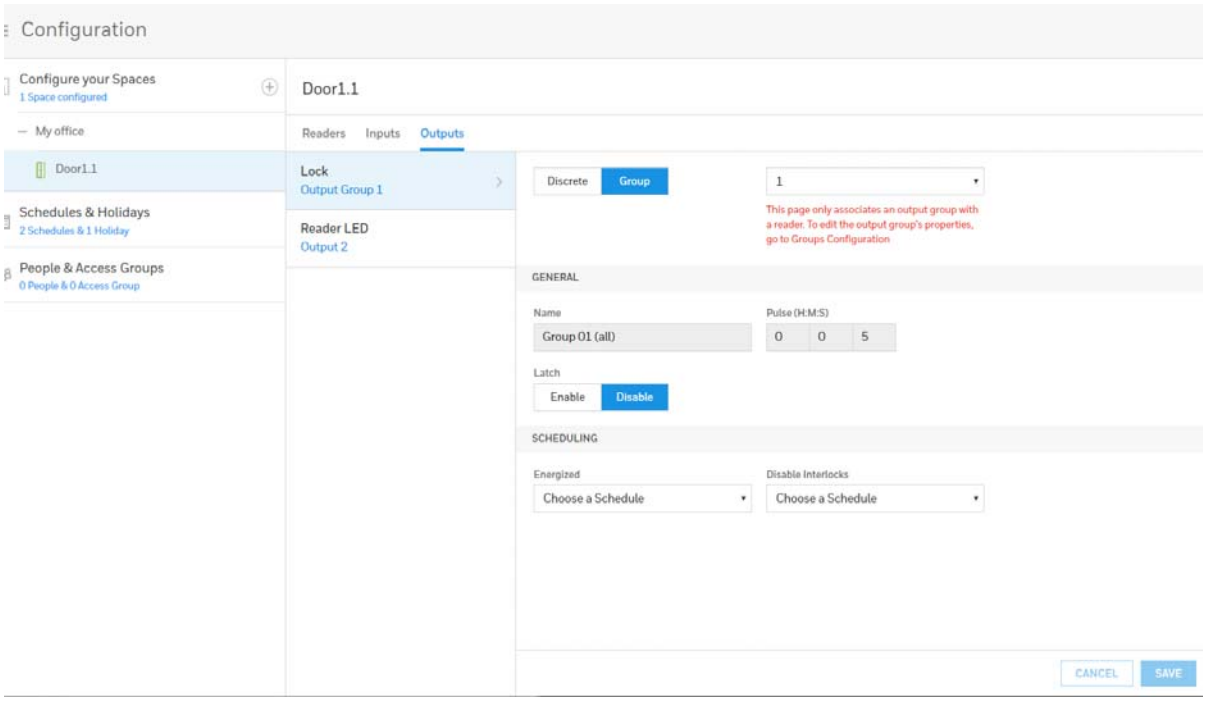
6. Click **Save**.

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.

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

Figure 2-27 Door Output Group



Configuring Inputs

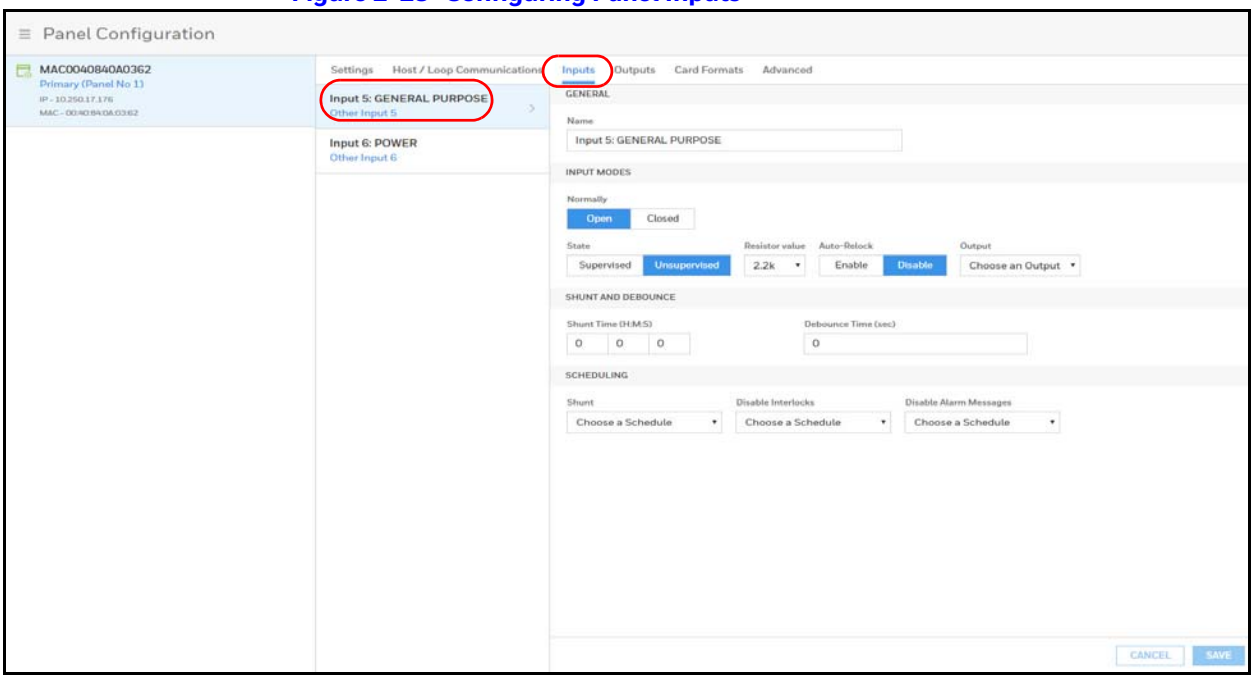
The Inputs tab enables you to:

- 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 2-28 Configuring Panel Inputs



2. Click to select an input.
3. Select **Input Modes**.

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.
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.
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,

4. Configure **Shunt** and **Debounce** times.

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.

5. Configure **Scheduling**.

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.
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.

6. Click **Save**.

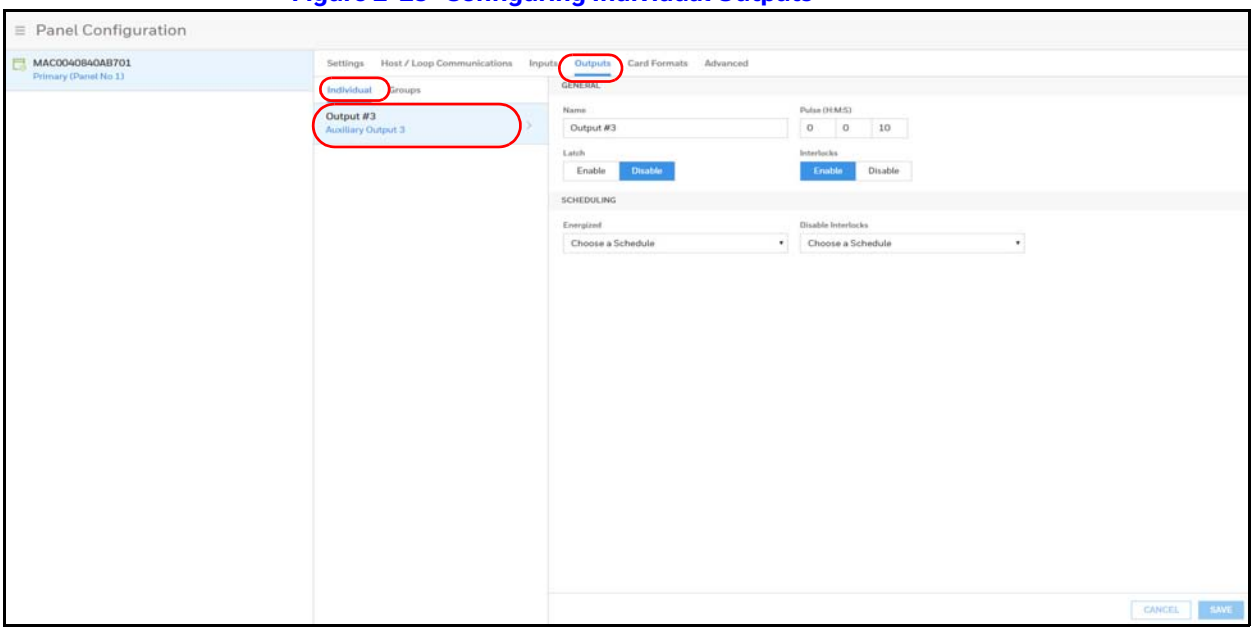
Configuring Outputs

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 2-29 Configuring Individual Outputs



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

Setting	Description
Name	Enter a unique name for the output
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 *Configuring Interlocks on page 63* 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 on page 31*) 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 on page 31*) from the drop-down list.

4. 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:

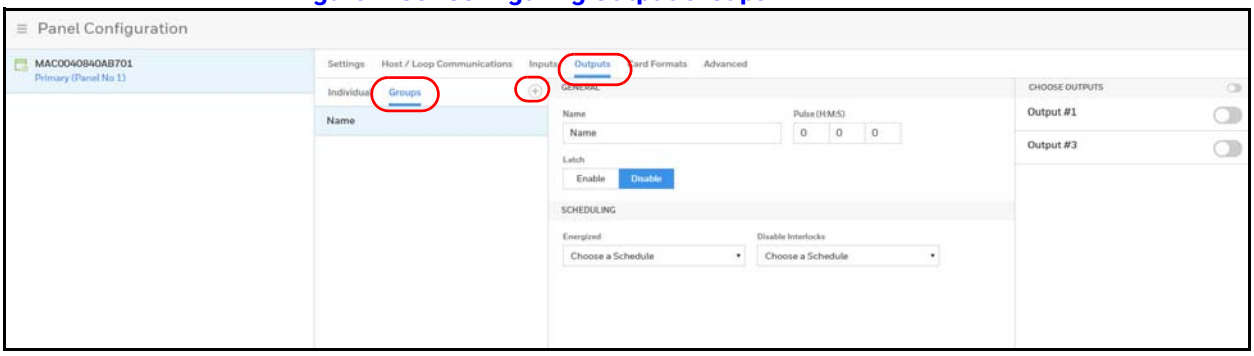
- A group of horns to sound for a set time during a set period
- Energize or de-energize a group of doors during a set period

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 2-30 Configuring Output Groups



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

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).

Setting	Description
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 on page 31*) 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 on page 31*) 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

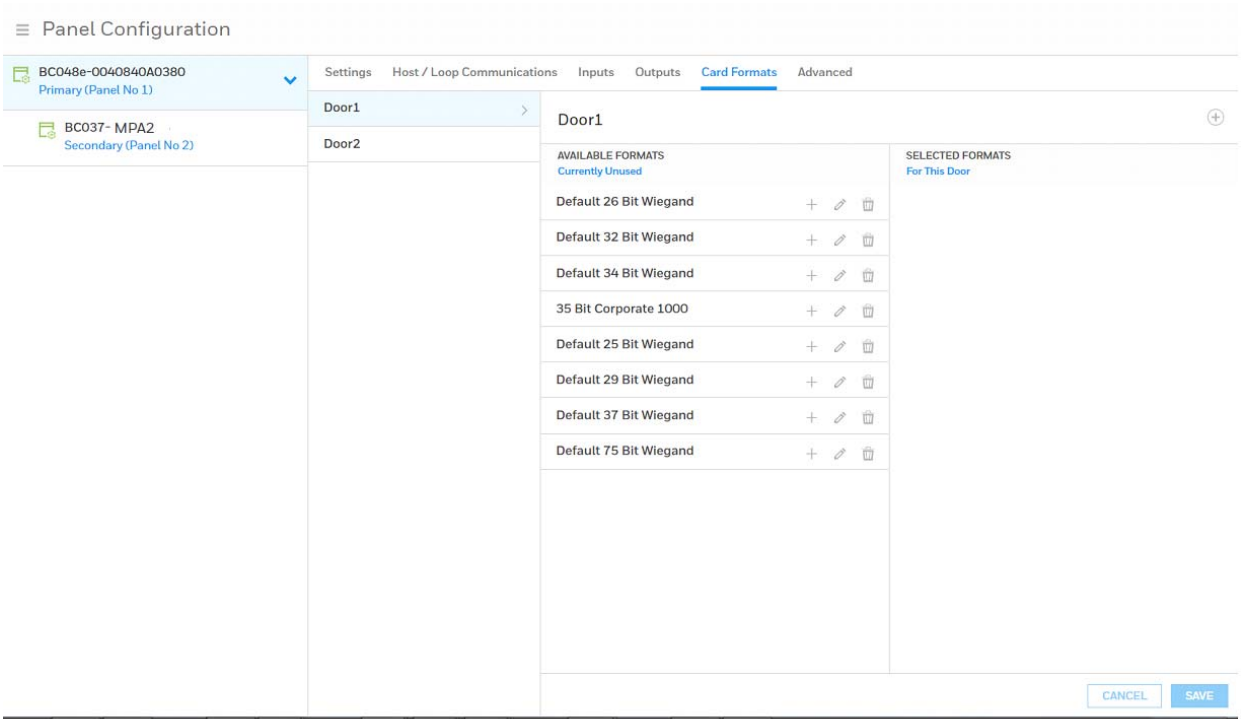


Table 2-9 Card Format Settings

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.

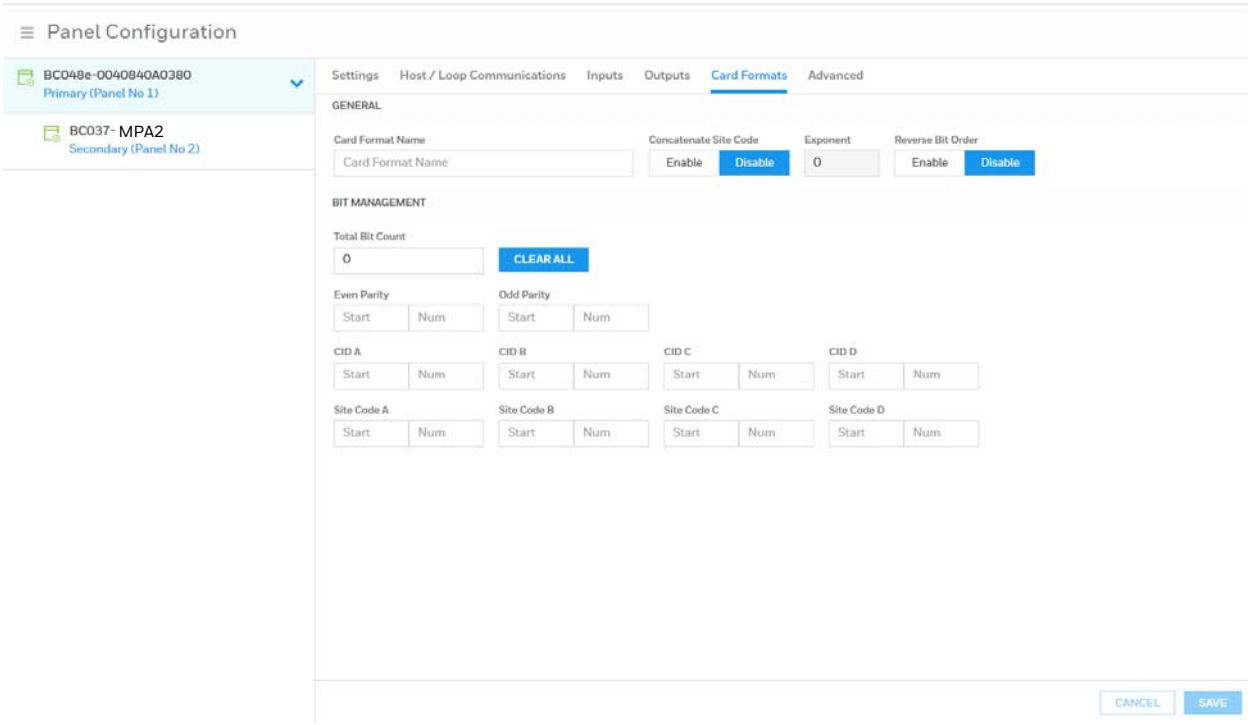
1. Click the Add icon (+) of each desired card format under the Available Formats list, and to move the format(s) into the Selected Formats list.

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 2-9* 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 2-9*.

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.

:



Use the field descriptions in *Table 2-10* to define the layout and click Save.

Table 2-10 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.

Table 2-10 Panel Configuration > Card Formats (continued)

Settings	Description
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.
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.

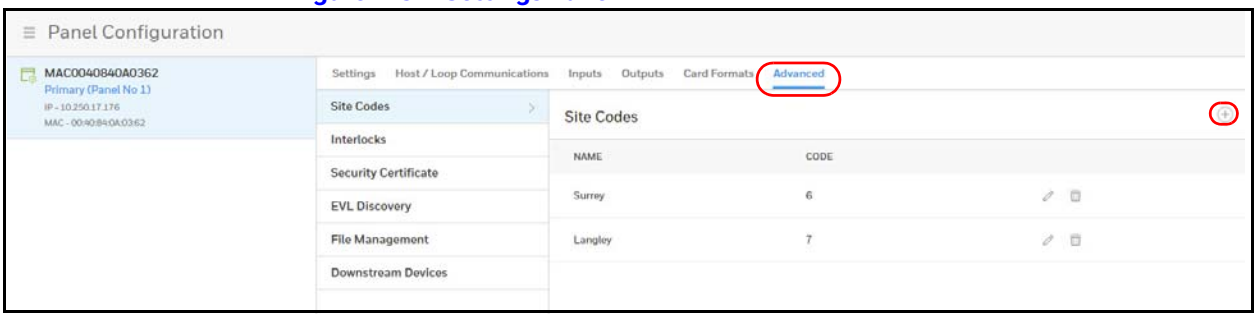
The Site Codes panel enables you to:

- 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 2-31 Settings Panel



Creating a Site Code

1. Click ⊕ to enter a new site name.

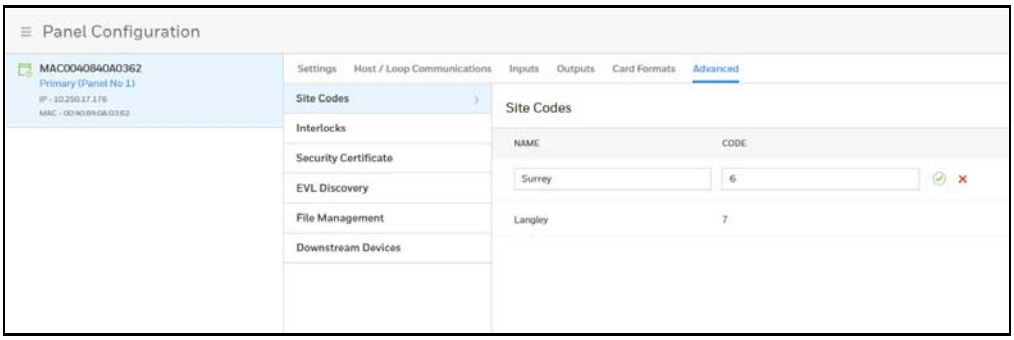
   Editable fields appear in the **Name** and **Code** columns.

2. Enter a unique name for the site code in the **Site code name** field. You can used letters, numbers, and some special characters.
3. 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.
4. Click on the check mark to the creation of the site code.

   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.

Configuring Interlocks

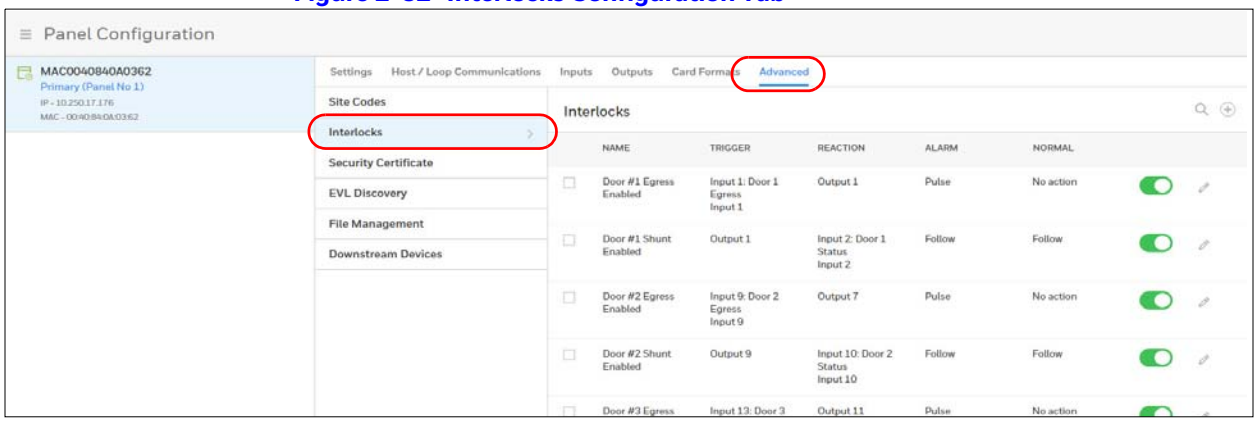
An interlock is a programmed connection between two points. The interlock causes an input point, output point, or group of output points to act in a specified manner when another input point, output point, or group of output points changes its state. An action on the trigger point causes a reaction on 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.**

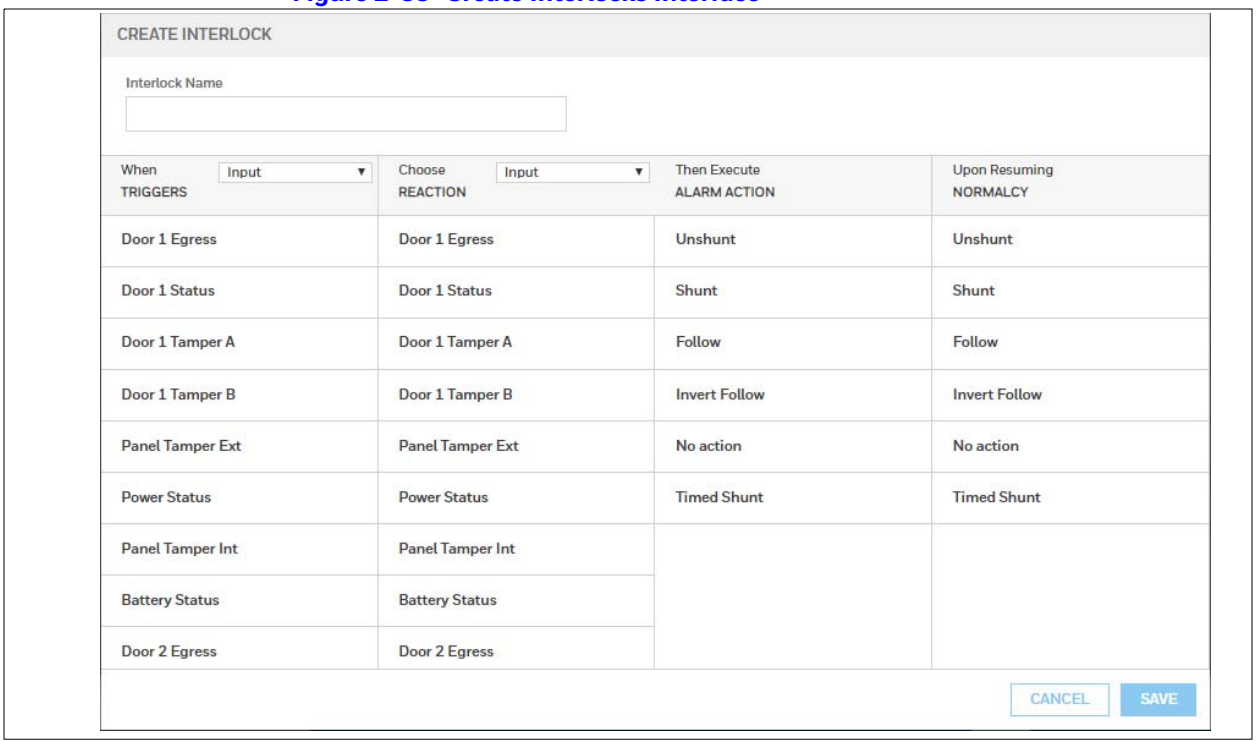
Figure 2-32 Interlocks Configuration Tab



Creating Interlocks

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

Figure 2-33 Create Interlocks Interface



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).

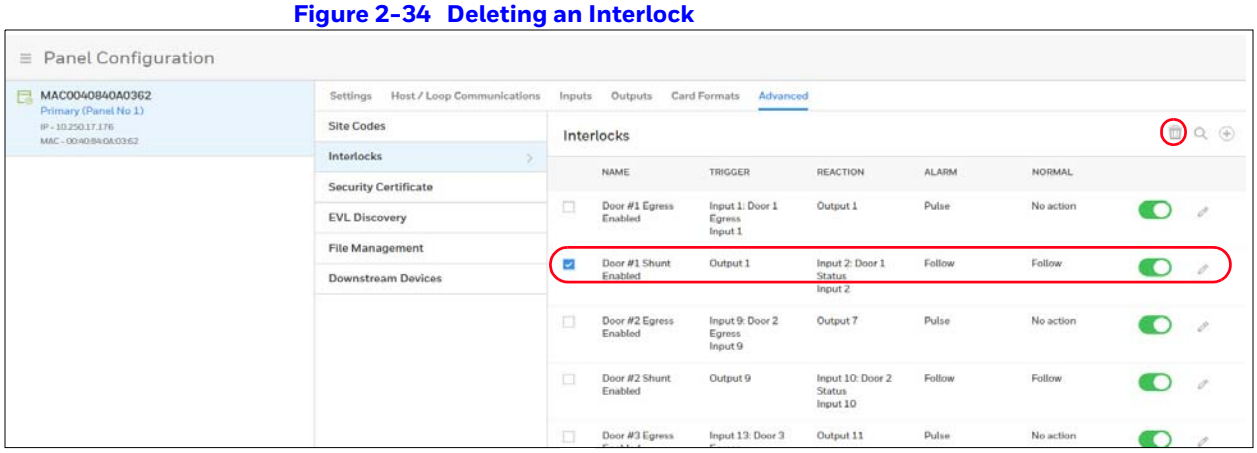
Configuration	Description
Triggers	Specifies the input, output, or output group for which a change of state will cause a reaction from another input, output, or group. If **Trigger** = **Inputs**, then triggers 1-88* will have an interlock link (Int Lnk) number from 1-96. If **Trigger** = **Outputs**,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

Configuration	Description
Interlock Actions	**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. **Upon Resuming (Normalcy)** – Specifies the reacting component's action when the trigger returns to the normal state. Select the action from the available options. Following are the available Input Reactor actions in the drop-down lists: **Unshunt** – Reactivates the input point. **Shunt** – Ignores alarms from the input point. **Follow** – The reacting point (second point) takes on the same state as the triggering point (first point). **Invert Follow** – The reacting point (second point) takes on the opposite state as the triggering point (first point). **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. **Timed Shunt** – Ignores alarms from the input point for a specified amount of time. Following are the available **Output Reactor** actions in the drop-down lists: **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". **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. **Follow** – The reacting point (second point) takes on the same state as the triggering point (first point). **Invert Follow** – The reacting point (second point) takes on the opposite state as the triggering point (first point). **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. **Pulse** – Energizes the output point or group for a specific amount of time. **Pulse Off–** Becomes unshunted for the programmed shunt time, followed by a return to the shunted state.

Deleting Interlocks

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

Figure 2-34 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

> **Note** Downstream I/O is not supported. Please contact Technical support for more details.

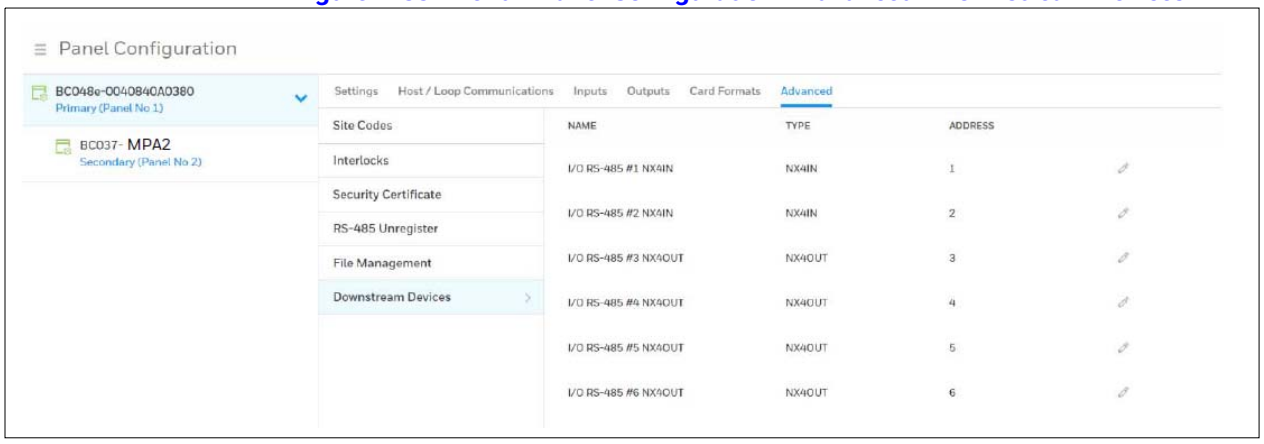
The NETAXS® I/O devices provide the MPA2 panels with additional inputs and outputs. The MPA2 panels supports two Interface types:

- 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 MPA2 panel supports a maximum of six daisy-chained Interface boards - two NX4IN and four NX4OUT boards. The boards connect to the MPA2 panel's RS-485 Interface Bus (J16).

Figure 2-35 Menu > Panel Configuration > Advanced > Downstream Devices



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:

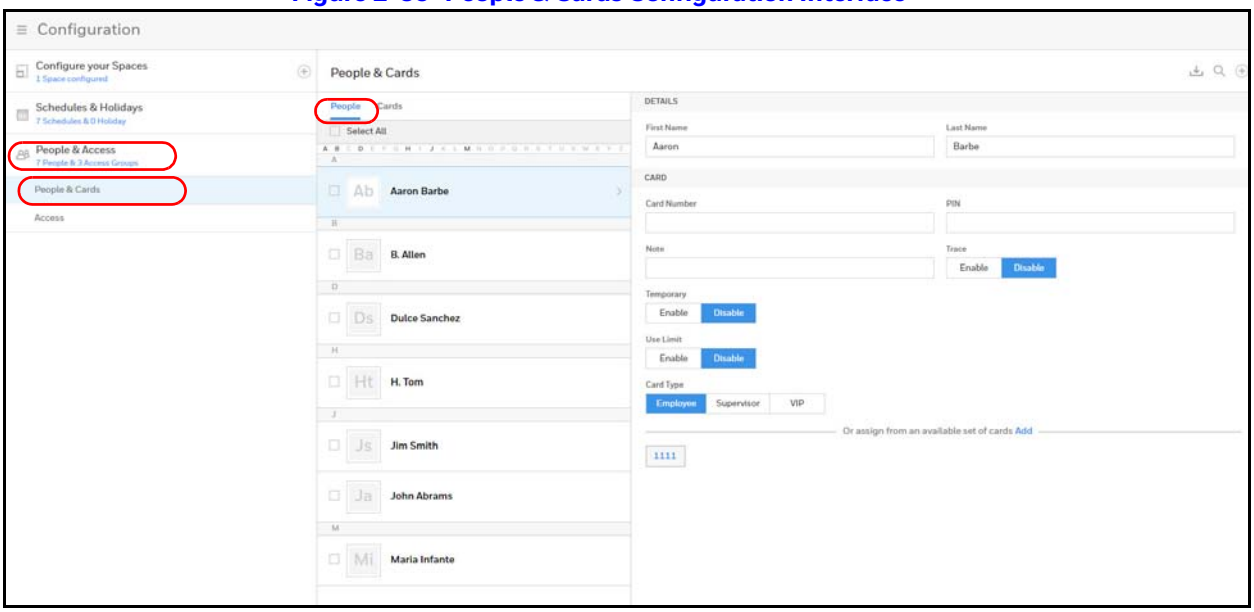
- Create a person, including assigning/adding a card.
- Modify a person.
- Delete a person.

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**.

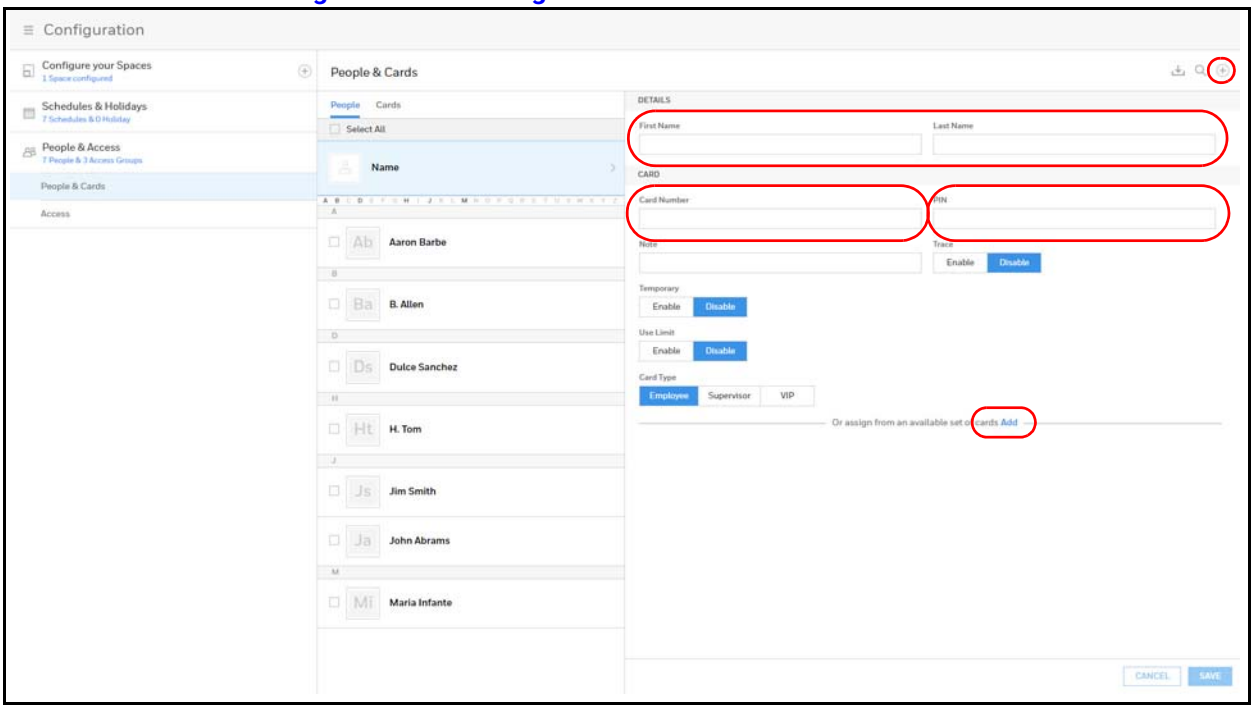
Figure 2-36 People & Cards Configuration Interface



Creating a Person

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

Figure 2-37 Creating a New Person



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

   Or click **Add** near the bottom of the window to assign a card from an available set of cards.
4. Enter a **PIN** (numbers only).

5. Optional: Enter a note, such as Department number, phone extension, or a birthday, for example. Notes can be up to 20 characters.
6. Turn **Trace** on or off.

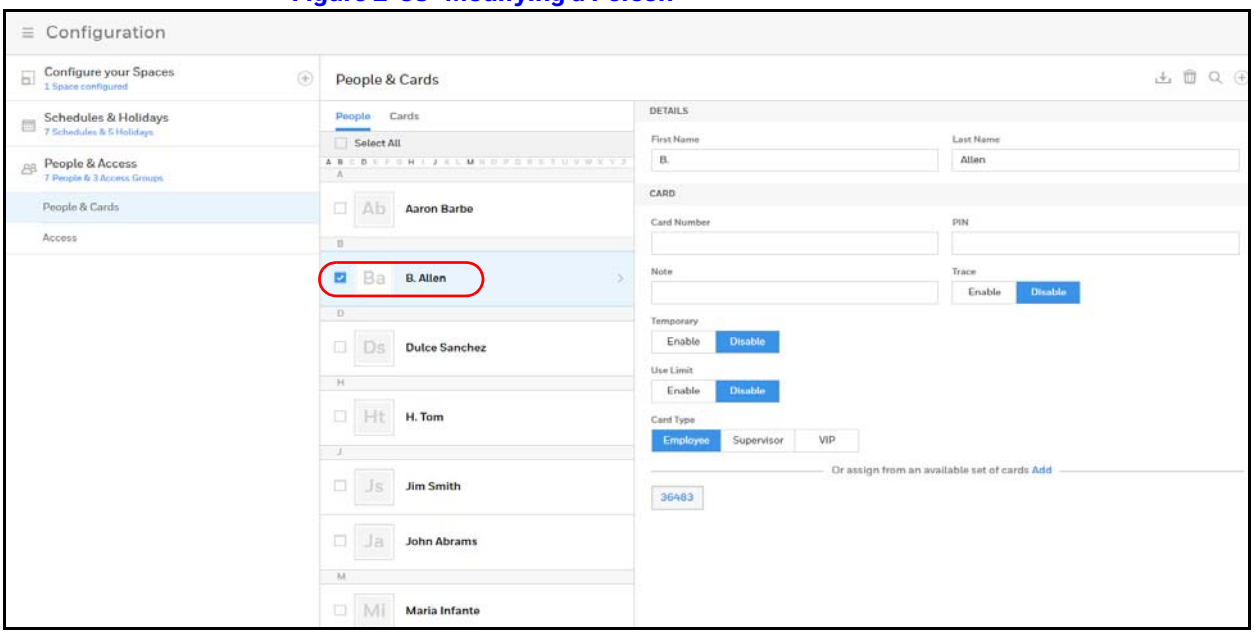
   Trace provides a record of the card holder's path through the facility by sending an alarm message to the alarm monitor whenever a card with trace enabled is presented at a reader.
7. Select a type of **Usage**.
   - If you select **Temporary**, then you must select an end date on the calendar.
   - If you select **Limited**, then you must select the maximum number of times the card can be presented.
8. Select an **Access Type**: Employee, Supervisor, or VIP. See *User Access Types and Functionality on page 119* for more about Access Types.
9. 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 2-38 Modifying a Person

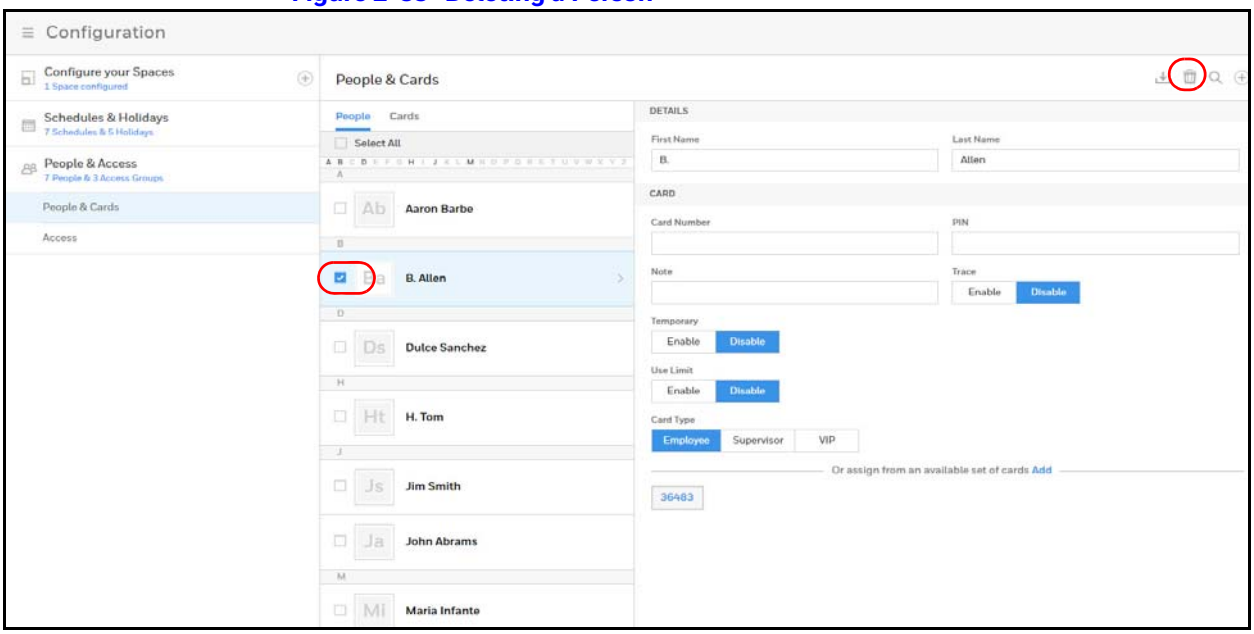


2. Make changes to the person, then click **Save**.

Deleting a Person

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

Figure 2-39 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:

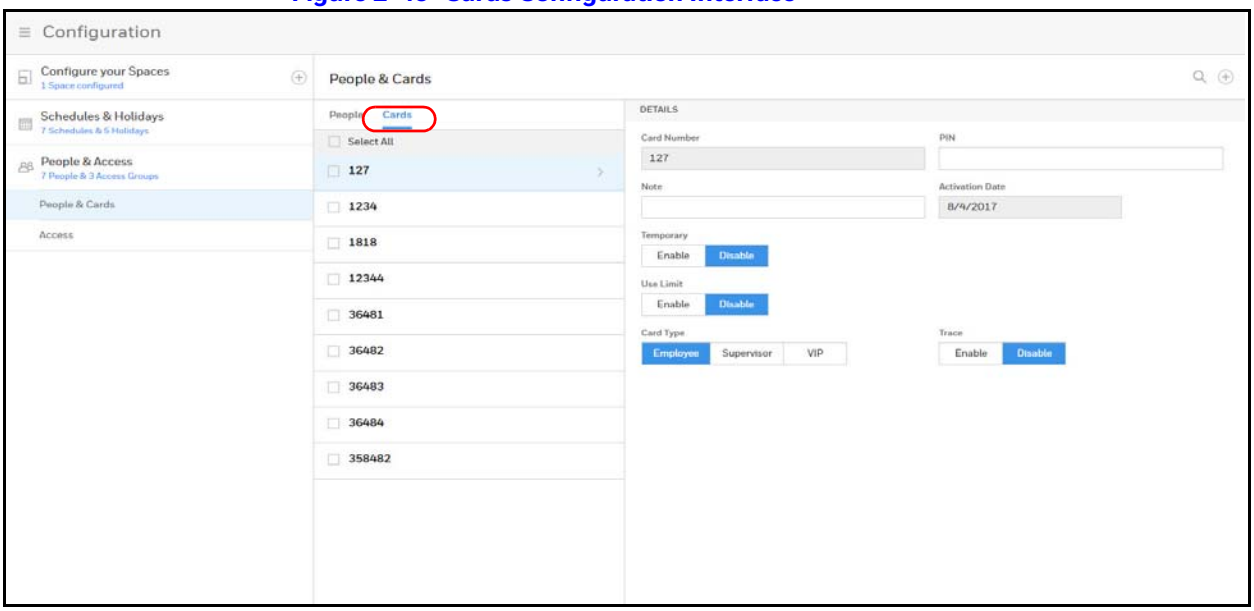
- Create cards encoded with the following information:
- Card Number(s)
- Card Type
- Personal Identification Number (PIN)
- Trace
- Expiration Date
- Use Limit
- Note

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**.

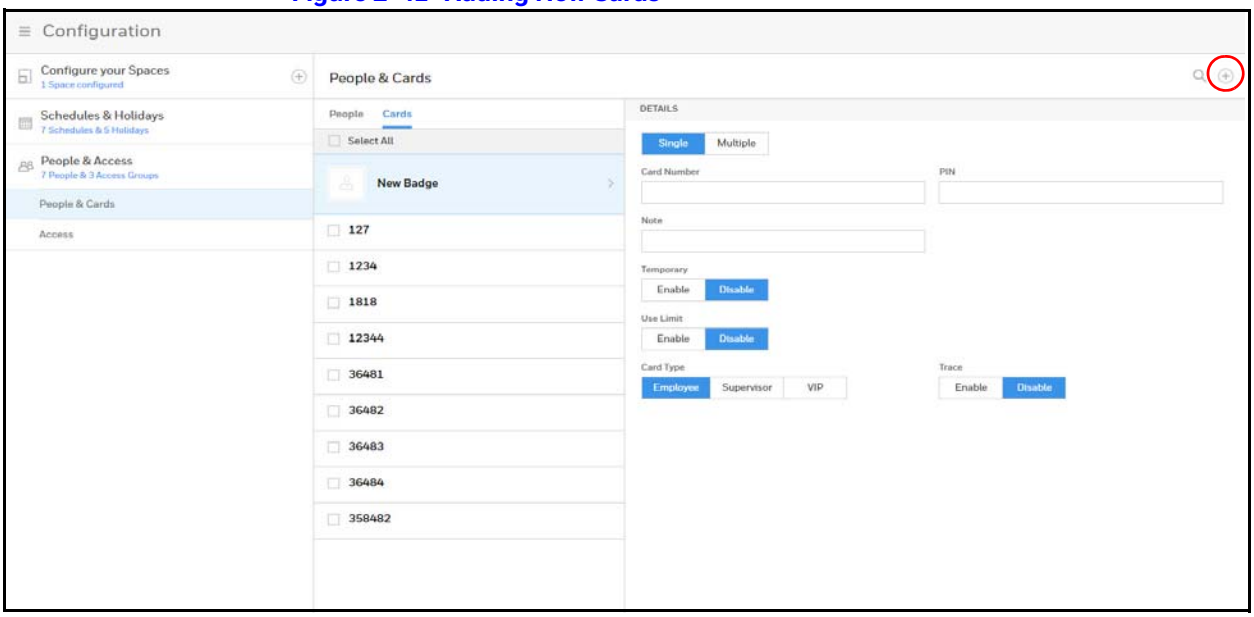
Figure 2-40 Cards Configuration Interface



Adding a New Card

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

Figure 2-41 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 68* 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 46*), 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.

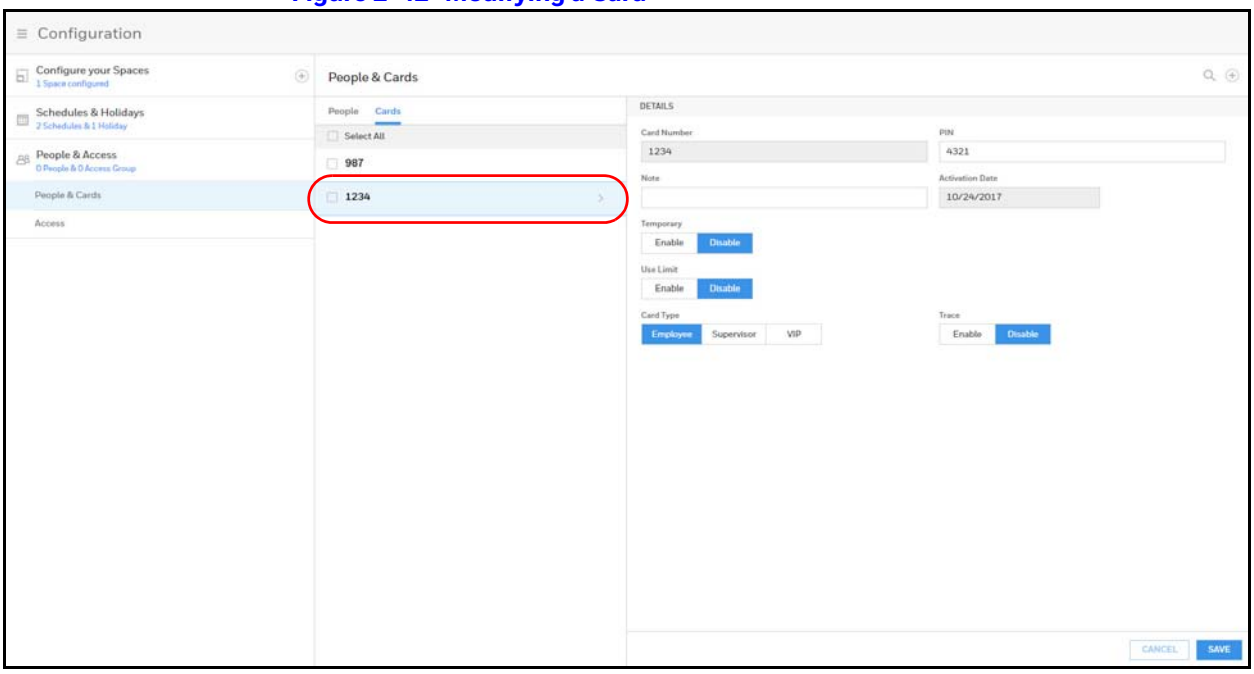
Note Once a VIP card is added to the database, it can gain access to any door regardless of the access level. VIP card can also bypass Duress, Anti-Passback, Disabled Reader Mode, Duress, Limited Use, Lockdown Reader Mode, Site Code, and Temporary Use.

7. Click **Save**.

Modifying Cards

1. Click to select a card.

Figure 2-42 Modifying a Card

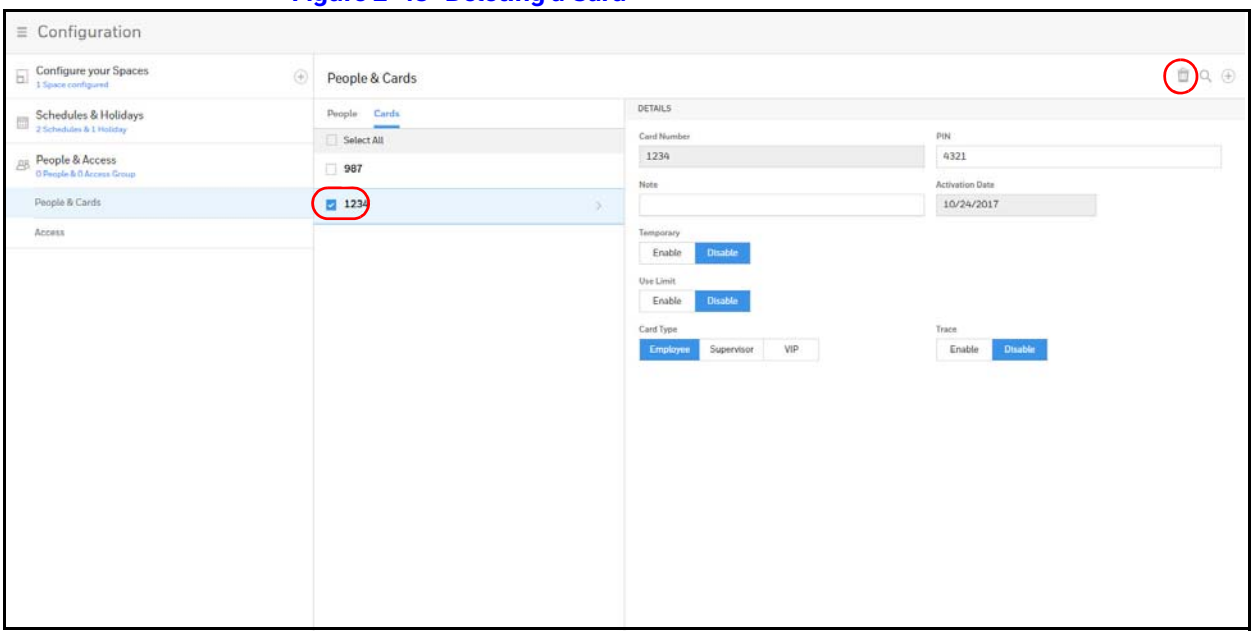


2. Make the changes to the card, then click **Save**.

Deleting Cards

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

Figure 2-43 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:

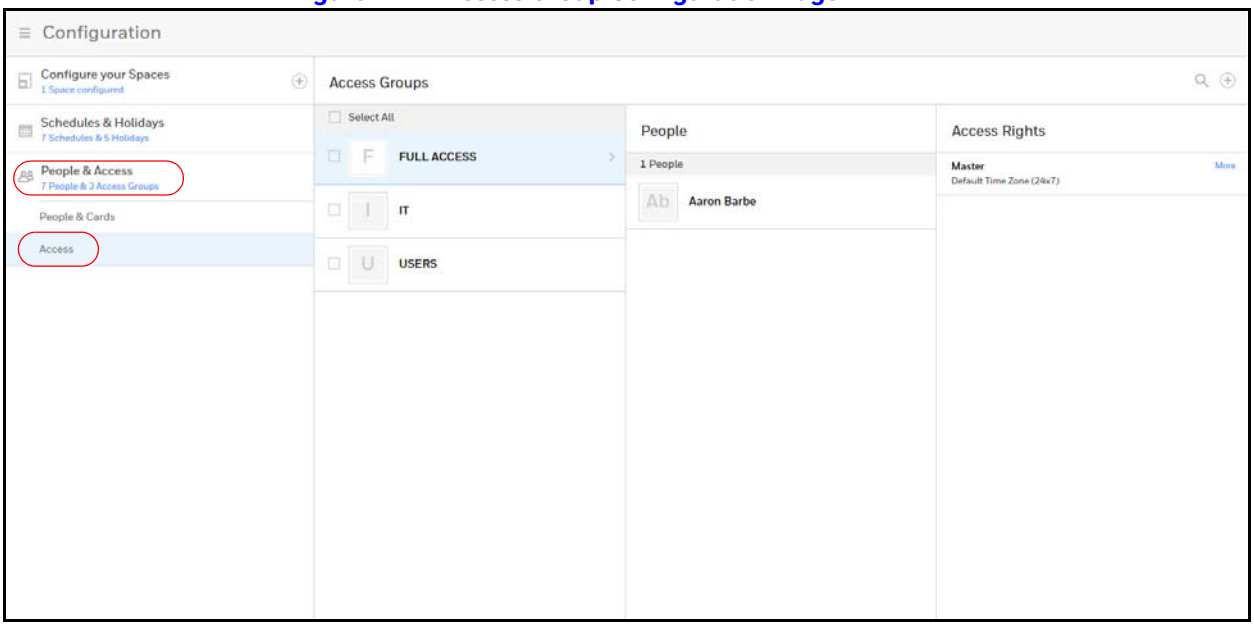
- Select Reader A and/or Reader B for each door. Note that if a reader is disabled, then the schedule drop down list for that reader will not be accessible.
- Create an access group.
- Modify an access group.
- Delete an access group.
- Set a Schedule for each door.
- View other panels with readers in 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 45*), people (see *Configuring People on page 67*), and the schedule (see *Entering a Panel Name on page 31*) 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.**

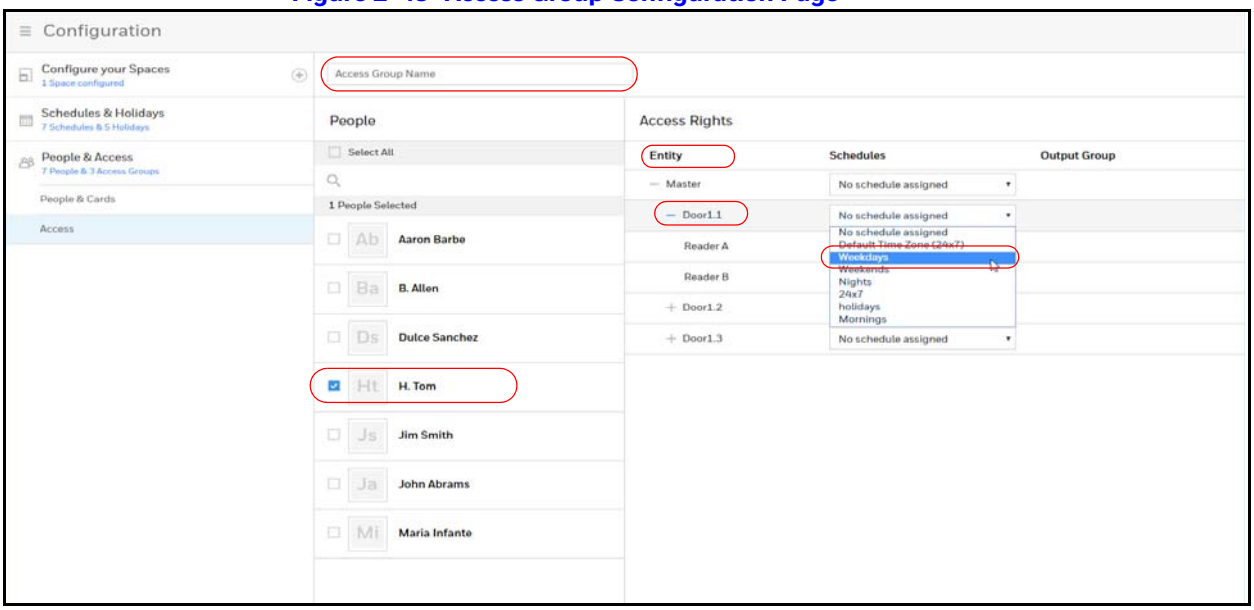
Figure 2-44 Access Group Configuration Page



Creating a New Access Group

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

Figure 2-45 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.

This page is intentionally left blank

Monitoring and Reporting

MPA2 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 an Alarms & (Web) Events Report. Download a Diagnostic Report as a bin file.

Note MPA2 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 MPA2 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 3-1 Alarms & Events Window

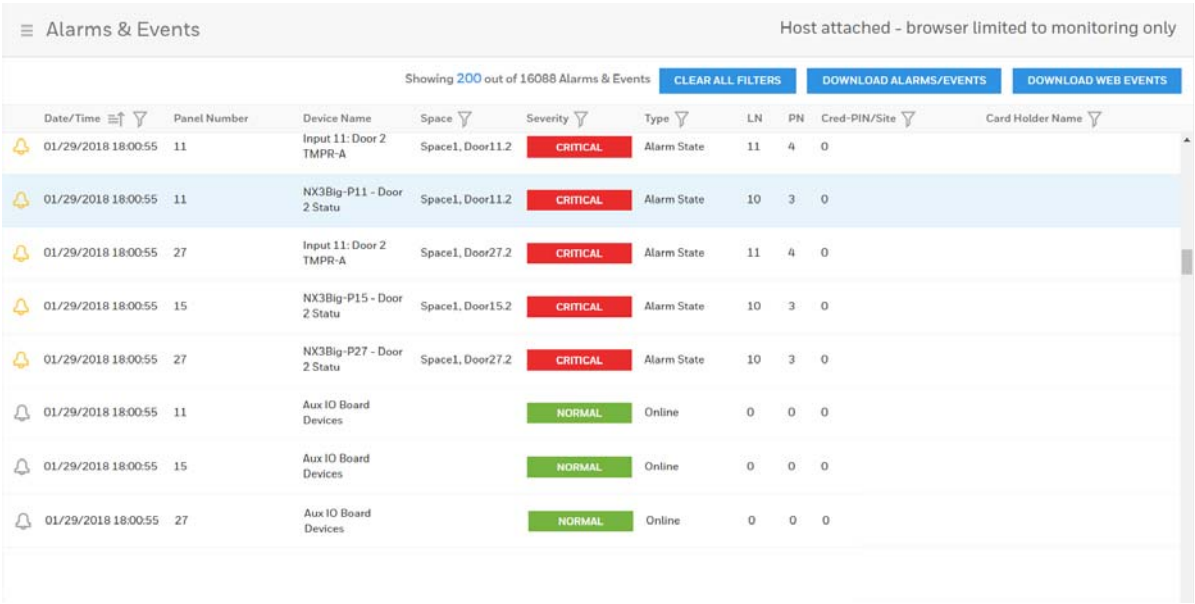


Table 3-1 Alarms & Events Fields

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.

Table 3-1 Alarms & Events Fields

Field	Description
Space	Displays the name of the space where the alarm occurred. **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.
Type	Indicates the type of alarm/event, such as: • Normal State • Alarm State • Ajar State • Card Found • Card Not Found • Input Alarm • Panel Offline **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.
LN (Logical Device Number)	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.
PN (Physical Device Number)	A number at the board level that is assigned to a specific alarm generating point. MPA2 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.

Table 3-1 Alarms & Events Fields

Field	Description
Cred-PIN/Site	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. **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.
Card Holder Name	Reports a Card Holder name on events where the Card Number is an actual card in the system. **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.
Clear All Filters	Click to clear all display filters (Date/Time; Space; Severity; Type; Cred-PIN/Site; Card Holder Name).
Download Alarms/Events	For generating reports. See *Reporting on page 86*.
Download Web Events	For generating reports. See *Reporting on page 86*. Web Events include logins with invalid passwords and logging in/out, for example.

Monitoring/Managing Doors

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

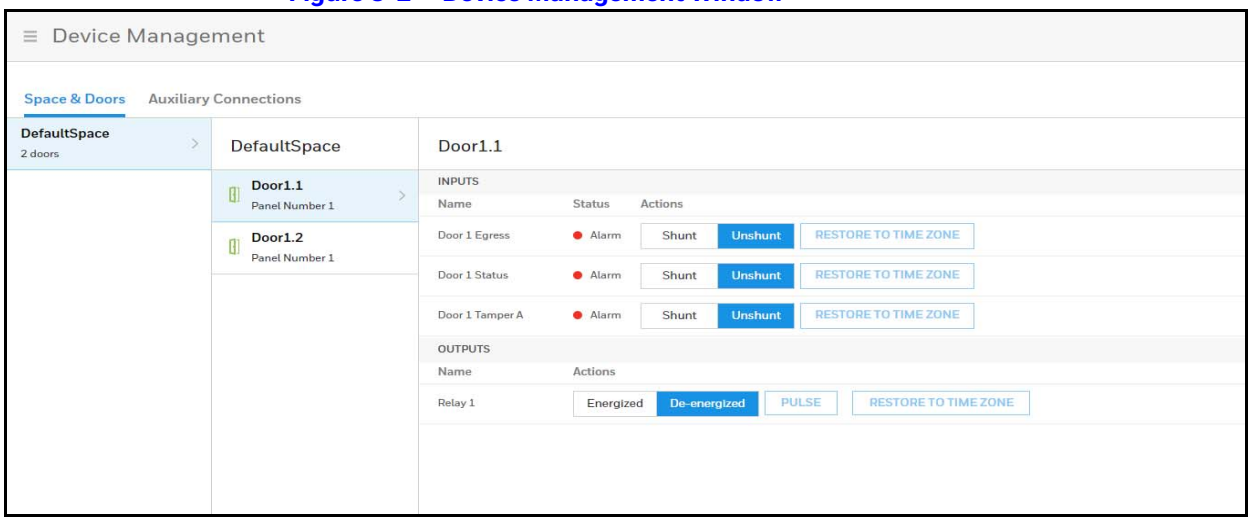
The Door Status screen enables you to:

- 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 on page 33*).
- View the current status of each output (Engergized, De-energized).
- Pulse, energize, or de-energize the Door Lock relay.
- Restore the Door Lock to its schedule.

Navigating to the Spaces & Doors tab:

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

Figure 3-2 Device Management Window



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.

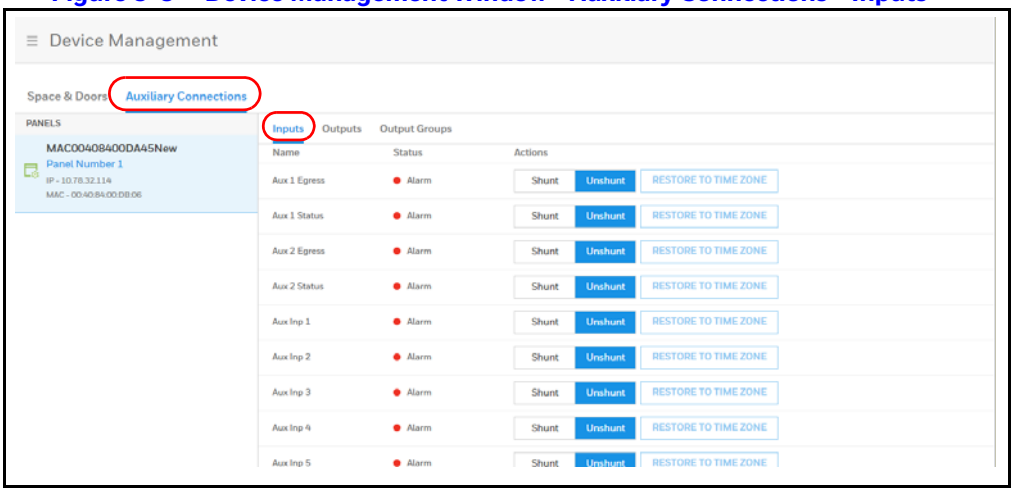
The Input Status screen enables you to:

- 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 (see *Entering a Panel Name on page 31*).

Navigating to the Auxiliary Connections-Inputs tab:

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

Figure 3-3 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 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 three doors. The panel also supports up to three additional auxiliary outputs. For example:

- 1 Door System = 1 Door Output and 1 Aux Output
- 2 Door System = 2 Door Outputs and 2 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 on page 53*) 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.

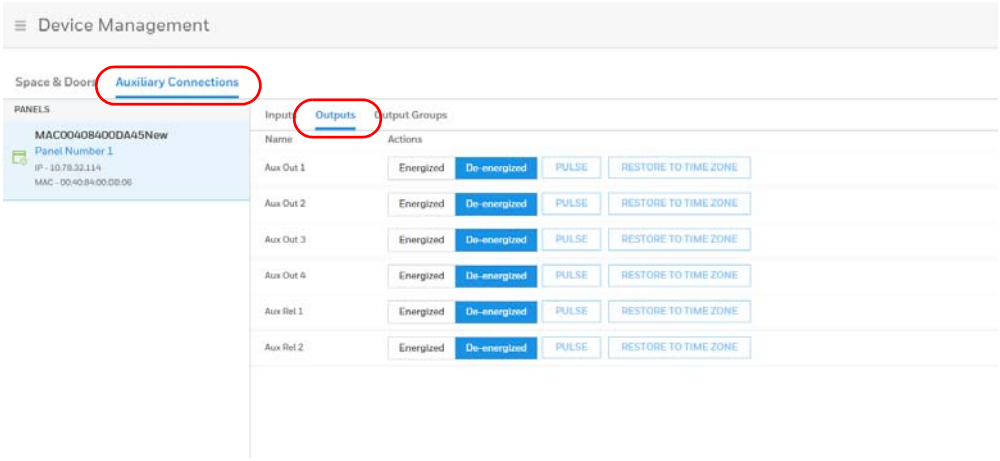
On the Outputs tab, you can do the following:

- 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 Outputs on page 82*).
- 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 on page 31*).

Navigating to the Auxiliary Connections-Outputs tab:

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

Figure 3-4 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
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 Output Group

Configuring Output Groups

Before you can monitor output groups, they must first be configured. See *Configuring Panel I/O and Groups on page 53*), 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 3-5 Device Management - Auxiliary Connections - Output Groups

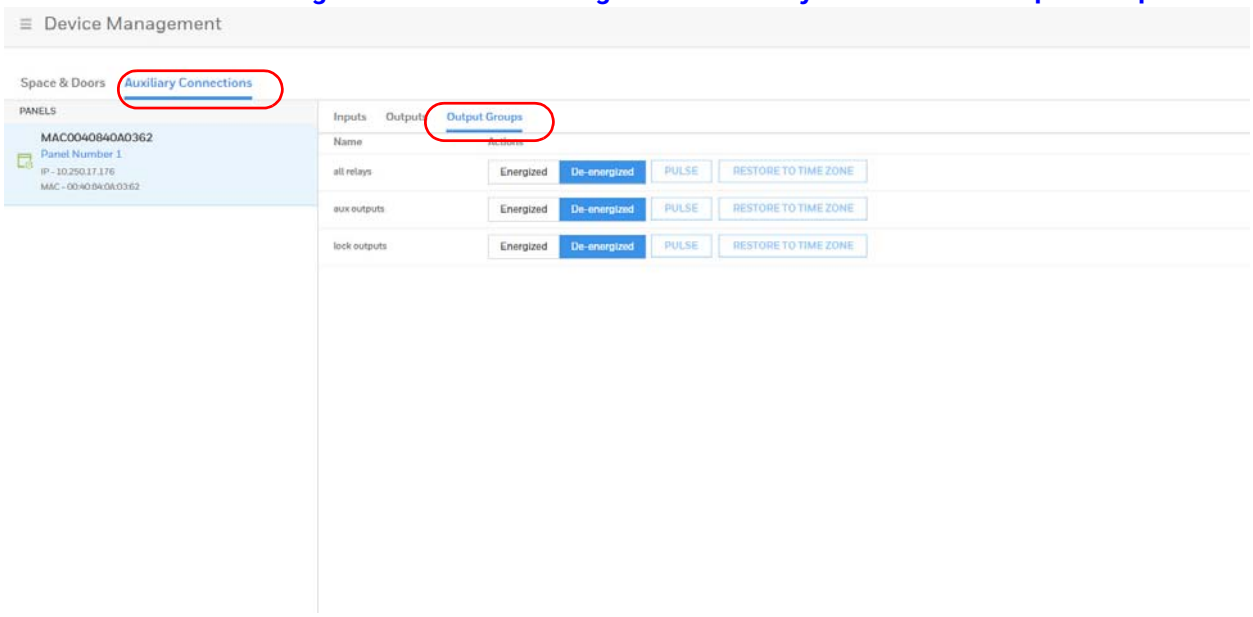


Table 3-3 Output Groups Management Settings

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
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.

Configuring Door Outputs

An output, or output relay, acts like a switch on the panel that either energizes or de-energizes or pulses an output device, such as a door lock or an LED.

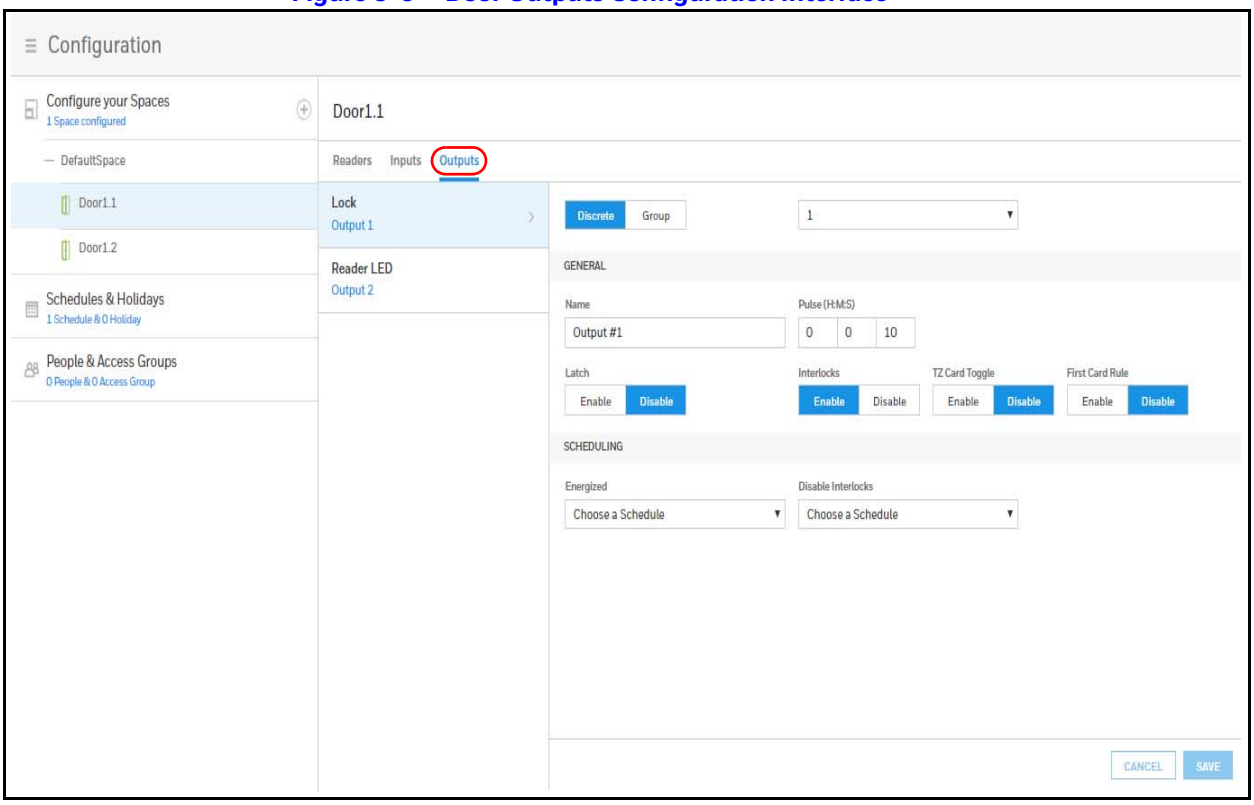
For example, a successful card read at a reader (input device) causes the output relay switch on the panel board to change the normal state of a door lock (output device), so that the normally locked door strike releases and permits entry. This tab configures the lock output relays and reader LED.

The Outputs tab allows you to configure the following settings:

- Output Name
- Pulse time
- Latch and Interlock (enable/disable)
- Scheduling
- TZ Card Toggle
- First Card Rule

1. Click Outputs on the Doors configuration window to open the Outputs configuration pane.

Figure 3-6 Door Outputs Configuration Interface



2. Enter an **Output Name**.
3. Configure the following general settings.

Configuration	Description
Pulse	Specifies the duration for which the device will assume abnormal status. For example, it specifies how long a horn will sound or a door strike will remain released. The maximum length of time is 1 hour, 45 minutes, 59 seconds. You can express seconds in tenths of a second.
Latch	Toggles the state of the outputs between energized and de-energized status upon every activation (code use, interlock, or manual pulse).

Configuration	Description
Interlocks	Enables you to disable the interlock, or programmed interaction between two points. When enabled, this point ignores all interlock actions to it, effectively disabling it from being a Reacting Component.
TZ Card Toggle	Requires, like the First Card Rule, a valid card read within the schedule to enable the schedule (period in which 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 state. **Note** Both TZ Card Toggle and First Card Rule cannot be enabled at the same time. Appears only on door lock outputs.
First Card Rule	Requires a valid card read within the schedule to enable the schedule (period in which doors are unlocked) to take effect. **Note** Both TZ Card Toggle and First Card Rule cannot be enabled at the same time. Appears only on door lock outputs.

4. Configure the following schedule settings.

Configuration	Description
Energized	Sets the period during which the output is automatically energized.
Disable Interlocks	Sets the period during which the interlock, a programmed interaction between selected inputs, outputs, and groups will be disabled. During the selected Schedule, this point ignores all interlock actions to it, effectively disabling it from being a Reacting Component during the Schedule. Outside of the Schedule the point will react to interlocks as expected.

5. Click **Save**.

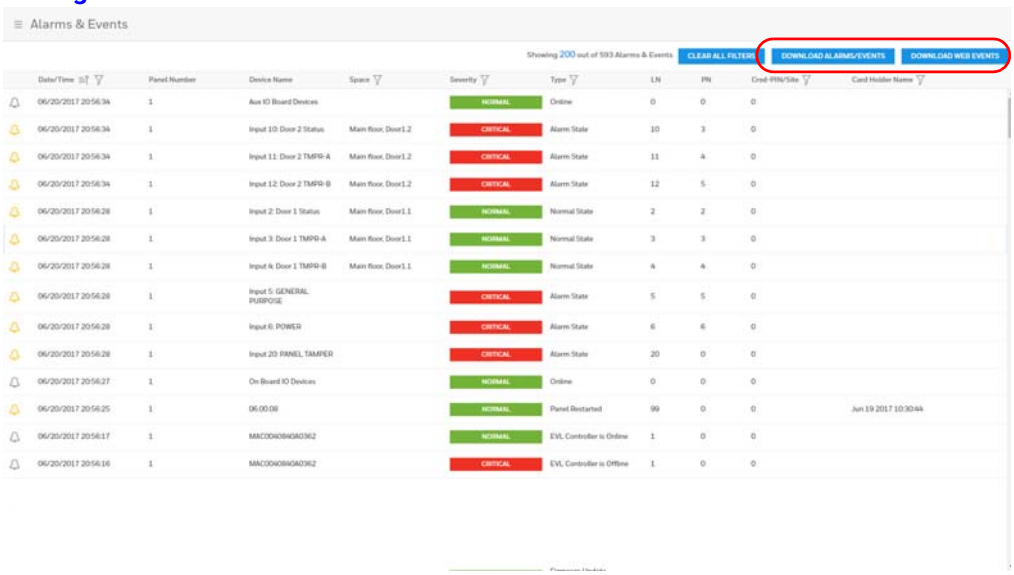
Reporting

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 3-7 Alarms & Events Window



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.

2. Click **OK** to confirm.

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

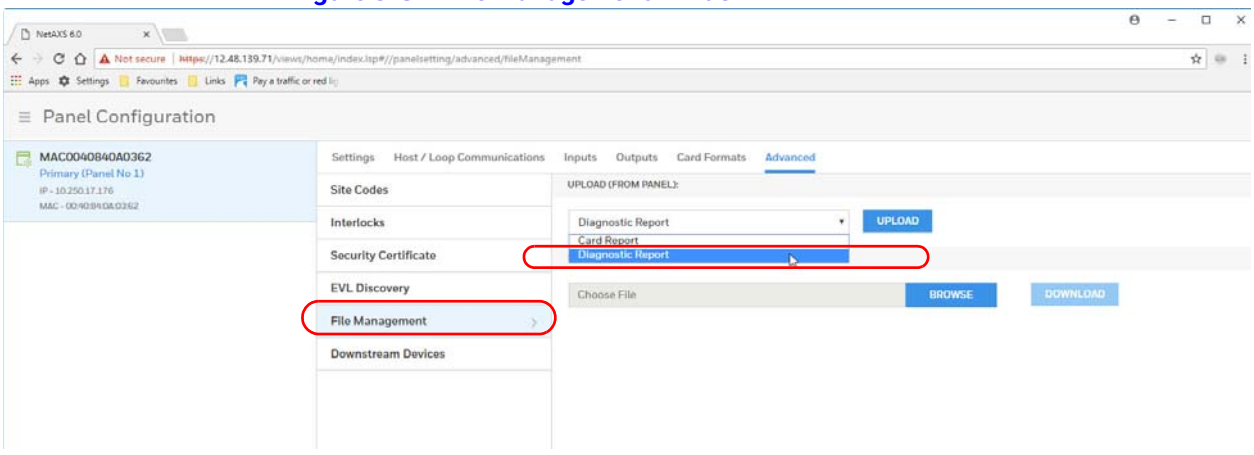
3. Click to open the report in Excel.

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 3-8 File Management Window



2. Select **Diagnostic Report** from the drop-down menu, then click **UPLOAD**.

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.

3. Click **OK** to confirm.

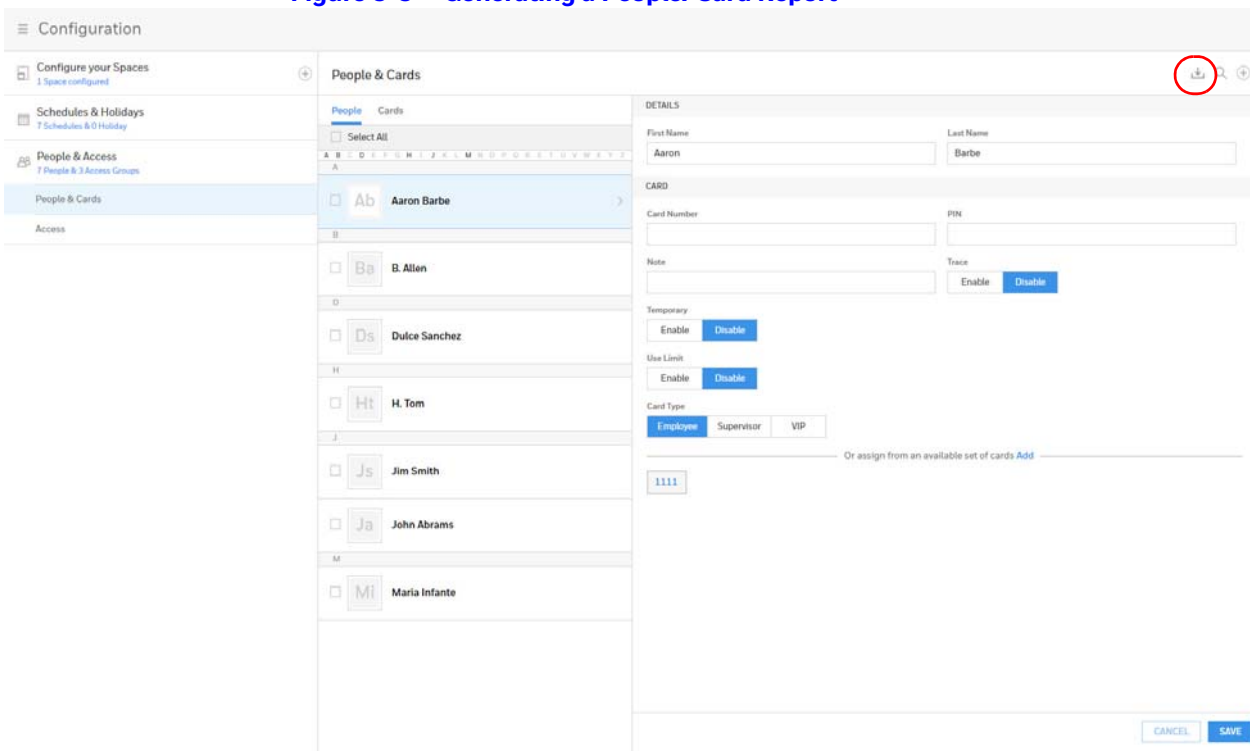
   A .bin file is generated which can be saved and sent to Honeywell technical support for diagnosis.

4. 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 3-9 Generating a People/Card Report



2. Click the download button in the top right corner.

   You see a message confirming that you want to download a People/Cards report.

3. Click **OK**.

   A comma-separated values (.CSV) report is generated and appears in the lower toolbar of your browser.

4. Click to open the report in Excel.

Maintenance

Overview

This chapter contains:

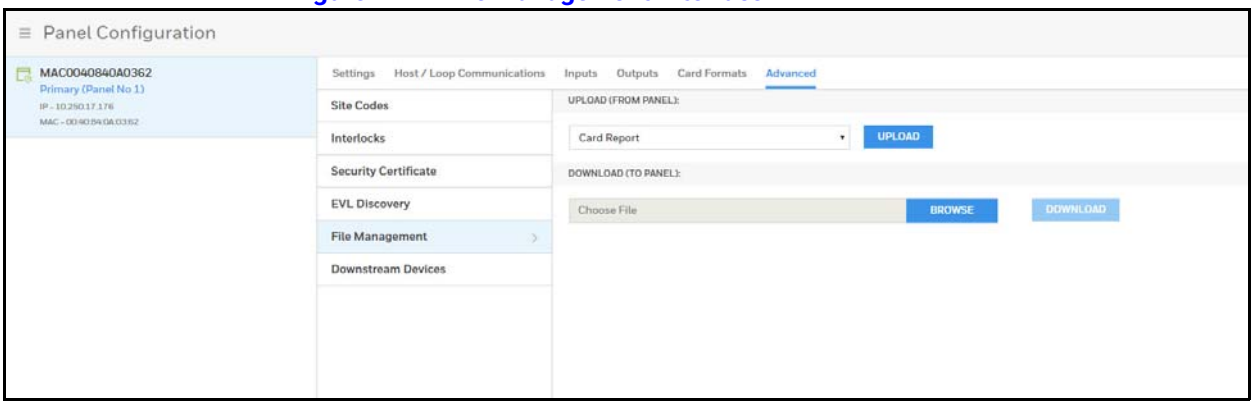
- System-wide backup
- Panel Resets and Restorations
- Firmware Upgrades
- Primary / Secondary Panel Replacement Use Case Scenarios
- Primary / Secondary Panel Hard Default Use Case Scenarios

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 4-1 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

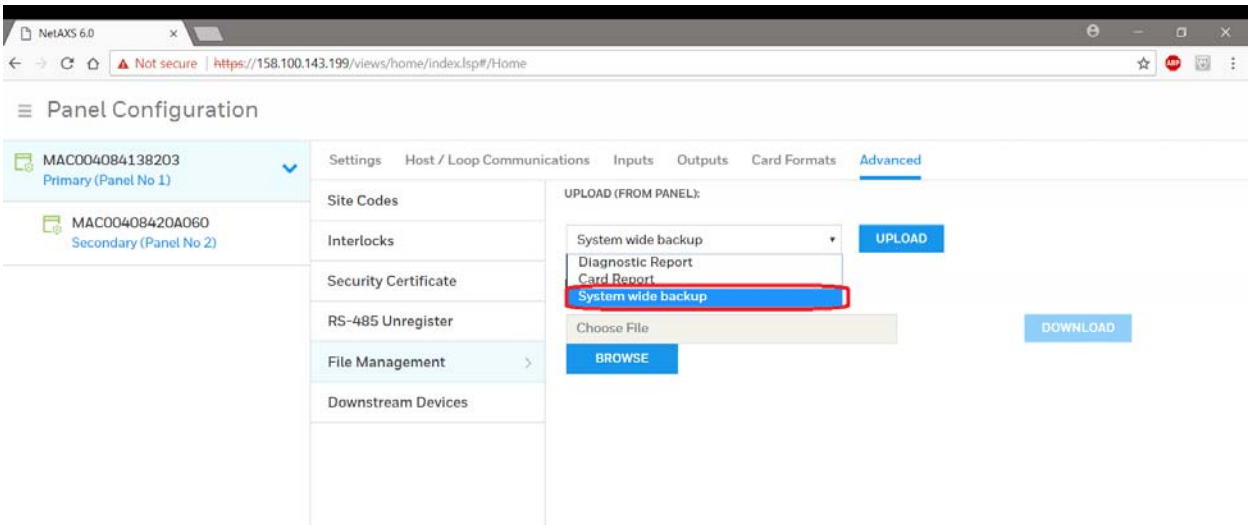
Uploads Card, Common and Panel configuration data in a proprietary internal format.

Common data includes:

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

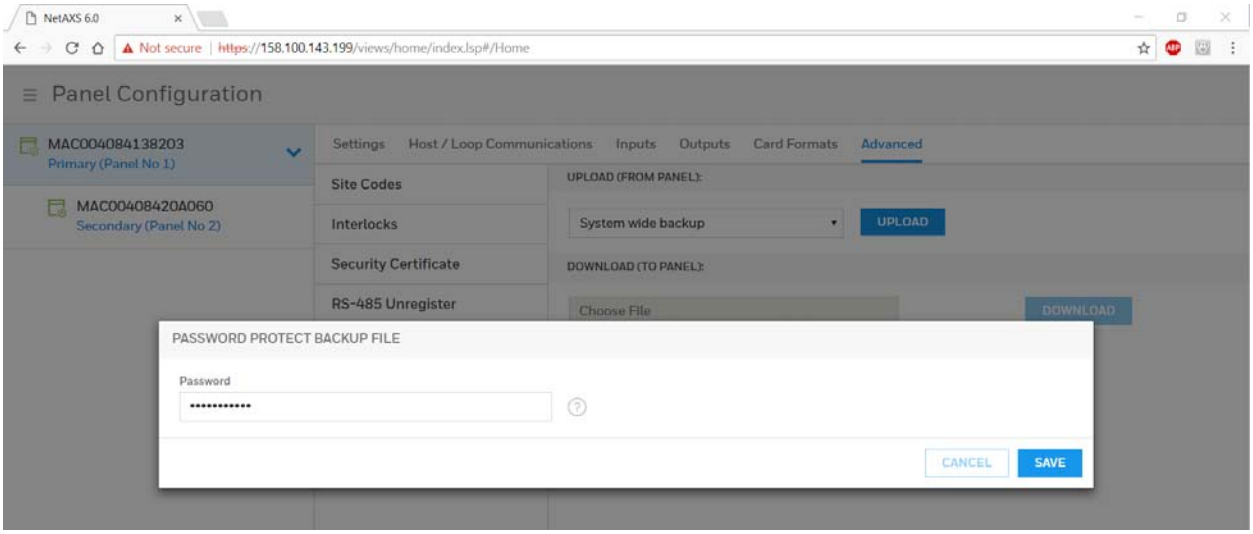
Panel-specific data includes:

- 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 (Also see: *Firmware Upgrades*)

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 (.CVS 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

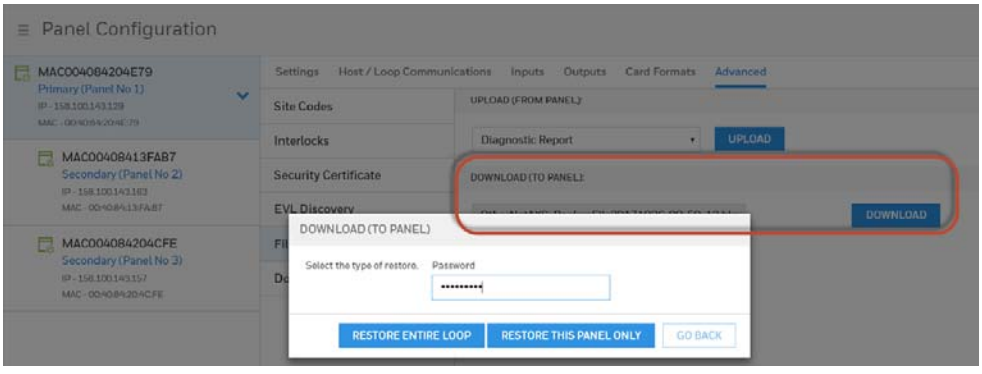
1. Navigate to Primary Panel's Download option, Panel Configuration > Advanced > File Management > Download (To Panel)
2. Click Browse to locate the backup file.
3. Click Download
4. Click "Restore Entire Loop"

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.

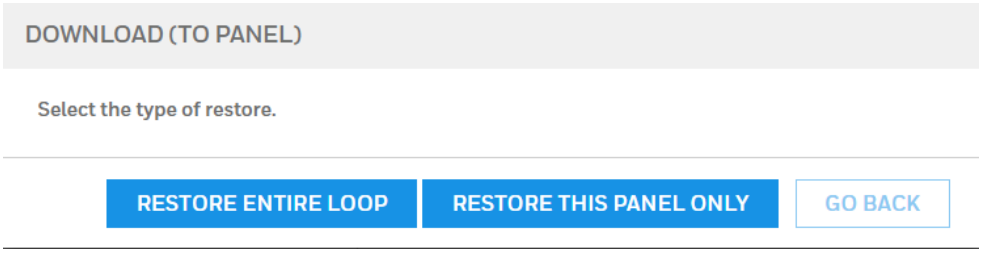
Panel only restore will restore Panel Configuration data for the specific panel and the Restore Entire Loop option will restore Card, Common and Panel Configuration data to each panel in the loop.

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



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 MPA2 "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 MPA2 "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 MPA2 "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 MPA2 "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)

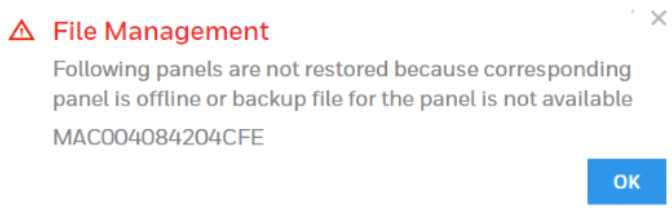
Panel-specific data includes:

- 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

MPA2 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	Factury Settings
OFF										Readers DOOR 1 = Wiegand
ON										Readers DOOR 1 = OSDP
	N.U.									Future Use
		OFF								Downstream/Secondary Panel
		ON								Master/Primary Panel
			OFF							Uses the User Provided Ethernet IP address (Default)
			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

MPA2 SW1 DIP Switch Settings (Continued)

S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	Selection
				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	Readers DOOR 2 = Wiegand
									ON	Readers DOOR 2 = OSDP

1. *DIP Switch 4 (SW1) does NOT require a panel reboot to take effect. This does not affect the USB IP address.*
2. *Both DIP Switch 5 and DIP Switch 6 (SW1) need to be either On or Off to be properly configured.*

MPA2 S1 DIP Switch Settings

S1[a]	S2[a]	S3[a]	S4[a]	S5[a]	S6[a]	S7[a]	S8[a]	Selection
OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	Default Settings
OFF	OFF							OSDP/Reader Port DOOR1 termination (EoL) DISABLED
ON	ON							OSDP/Reader Port DOOR1 termination (EoL) ENABLED
		OFF	OFF					OSDP/Reader Port DOOR2 termination (EoL) DISABLED
		ON	ON					OSDP/Reader Port DOOR2 termination (EoL) ENABLED
				OFF	OFF			RS485-1 (IB2/NX4 Bus) termination (EoL) DISABLED
				ON	ON			RS485-1 (IB2/NX4 Bus) termination (EoL) ENABLED
						OFF	OFF	RS485-2 (Downstream Bus) termination (EoL) DISABLED
						ON	ON	RS485-2 (Downstream Bus) termination (EoL) ENABLED

- *Both DIP Switch 7 and DIP Switch 8 need to be either On or Off to be properly configured.*

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

Note You can also use the ASCII command _I=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.

Restoring the Panel to Factory Default Settings

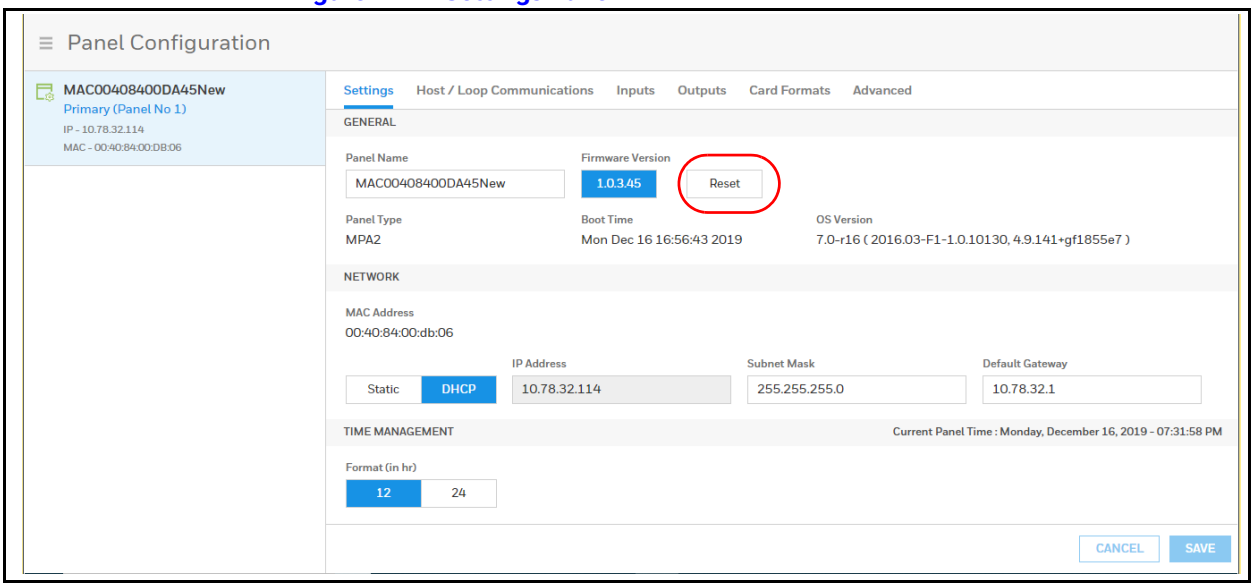
1. Make a note of the existing settings on SW1 DIP switches.
2. While the panel is powered up, turn all of the DIP switches to the OFF position.
3. Power down; then power the panel back up.
4. Wait for the panel to come up. The **RUN LED** should flicker fast.
5. Set the DIP switches back to their original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

   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 4-2 Settings Panel



2. Click **Reset**.

   Click **OK** to reboot the panel.

Firmware Upgrades

Panel Requirements

MPA2 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 MPA2 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 MPA2 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 MPA2 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 MPA2 panel, you must clear your browser's cache. See *Clearing the Cache and Cookies in the Internet Browsers Used by the MPA2 Web Server* for details.

This page is intentionally left blank

Caches and Certificates

Caches

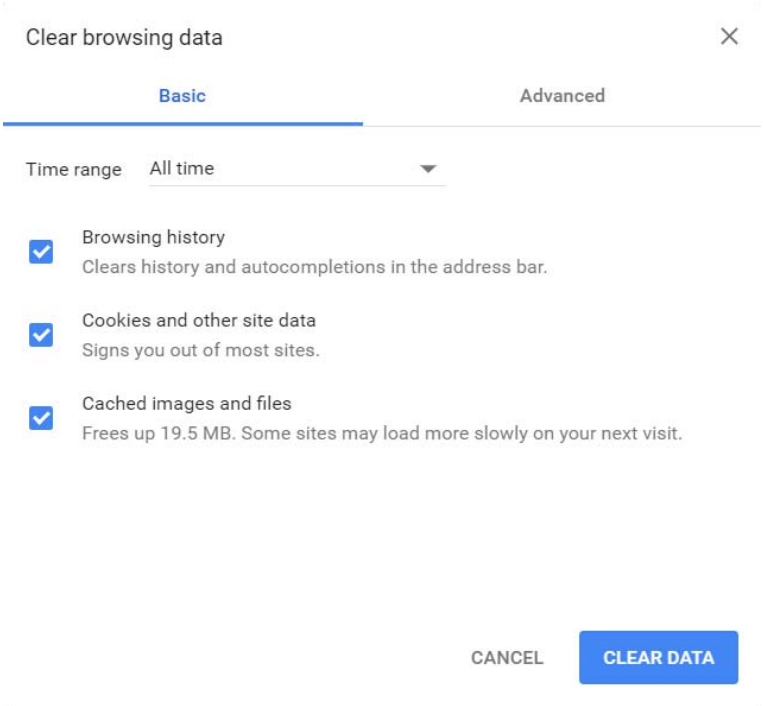
Clearing the Cache and Cookies in the Internet Browsers Used by the MPA2 Web Server

The MPA2 supports Google Chrome. It is recommended that the cache be cleared following a successful upgrade.

Note After upgrading a MPA2 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:



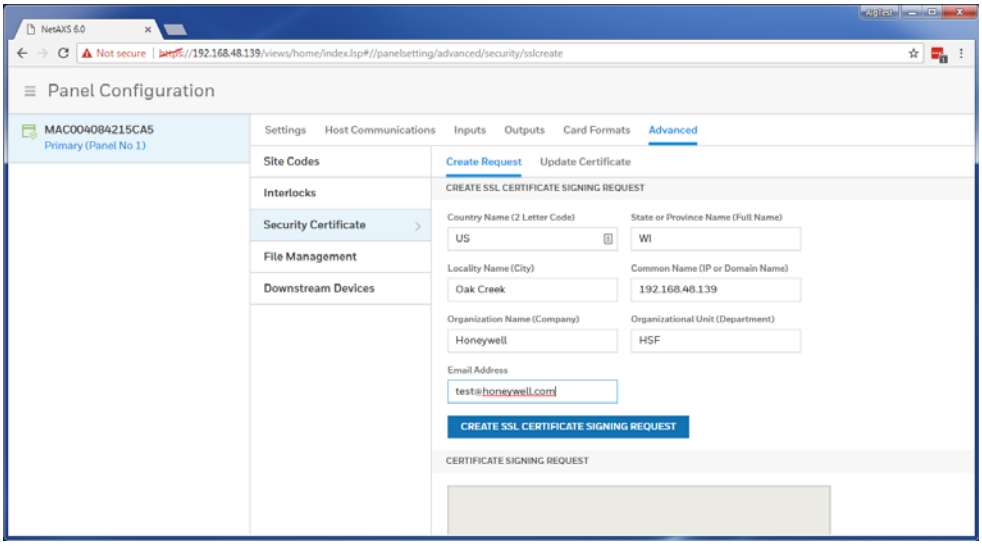
    - Ensure that the selections pictured in the above image are chosen.
3. Click **CLEAR DATA**.

Generating and Installing Certificates

Section 1 – Generating sign-in request and installing certificates

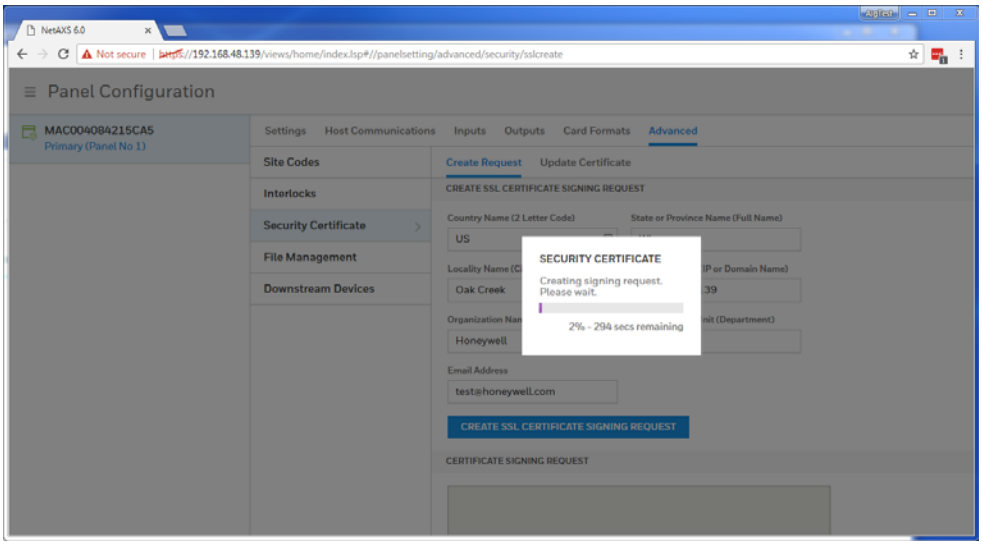
In order to have Google Chrome display the panel as secure, it's necessary to

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.

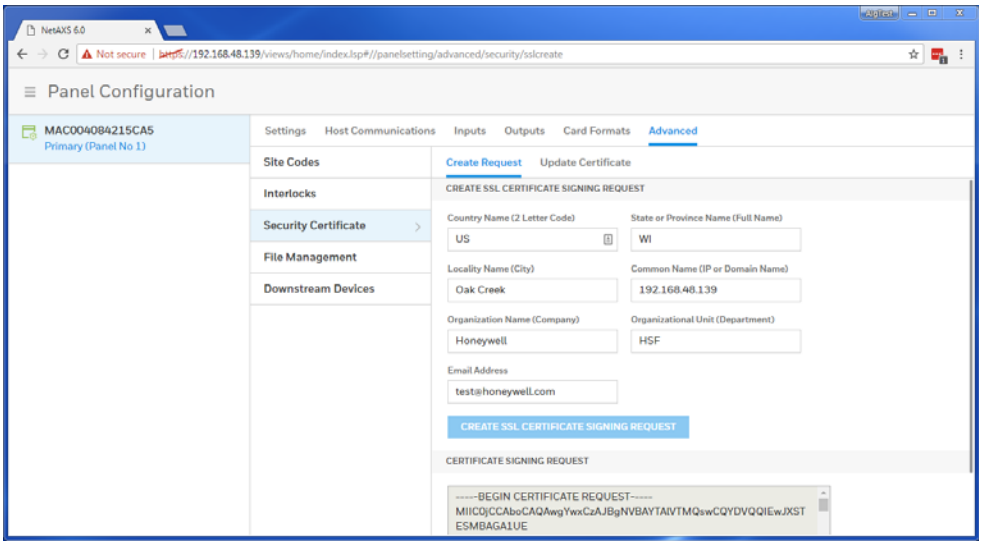


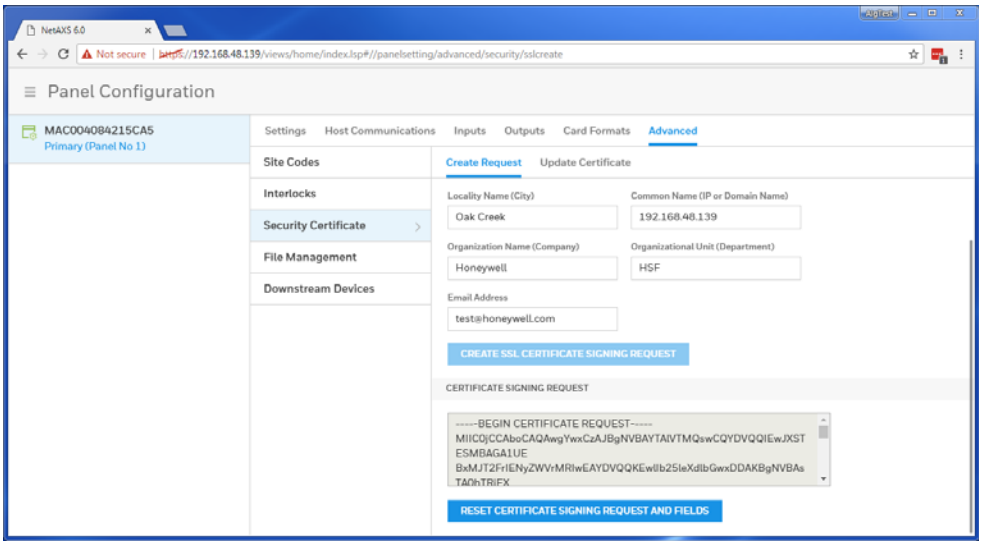
Go to **Advanced Menu > Security Certificate** tab. **Create Request** will be selected at the top of the pane. Fill in the fields as shown above. Make sure that the panel IP address is in the common name field.

Select **Create TLS Certificate Signing Request**.



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

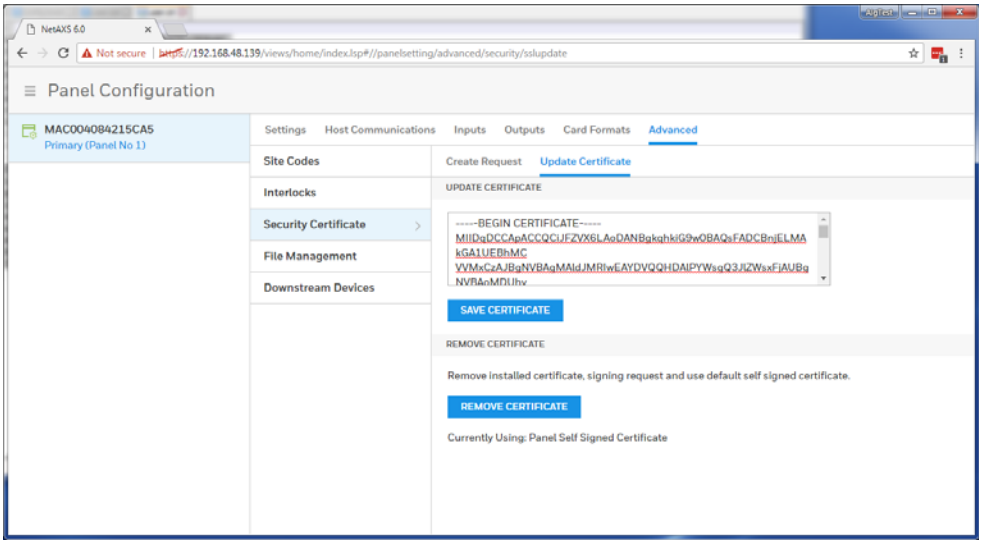


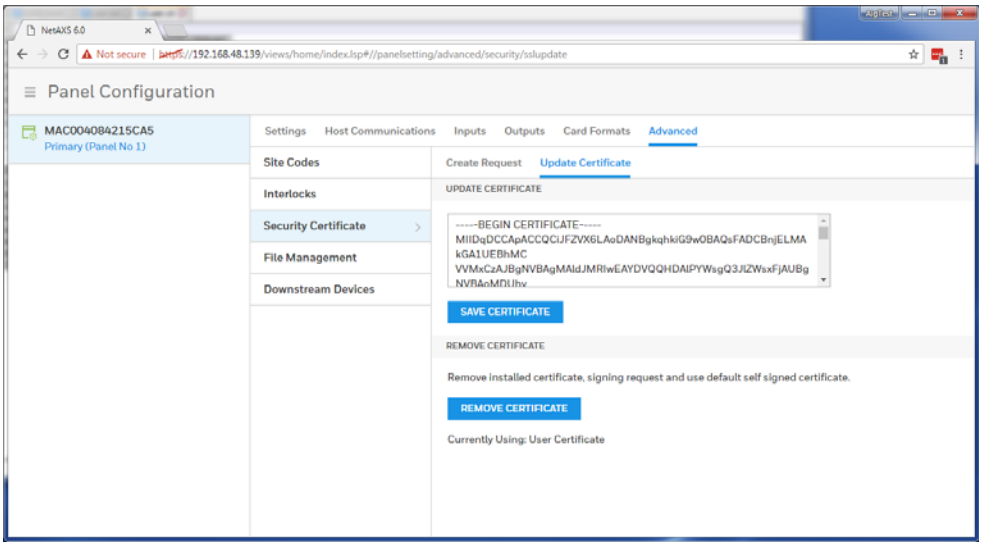


Copy all of the text out of this field and send it to the signing authority of your choice.

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**.



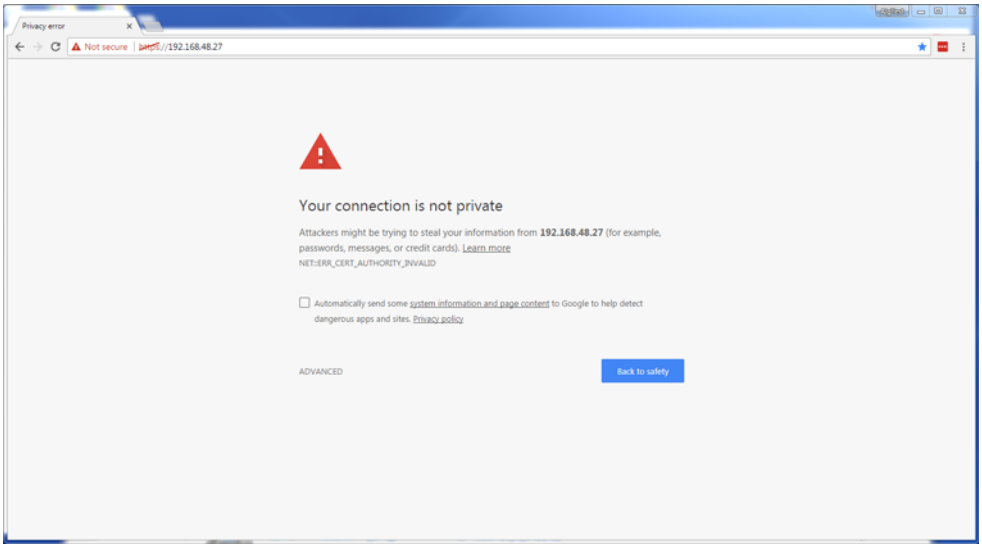


When the save is complete you will notice that the text at the bottom of the page reports "Currently using: User Certificate."

Section 2 - Installing the master certificate into the browser

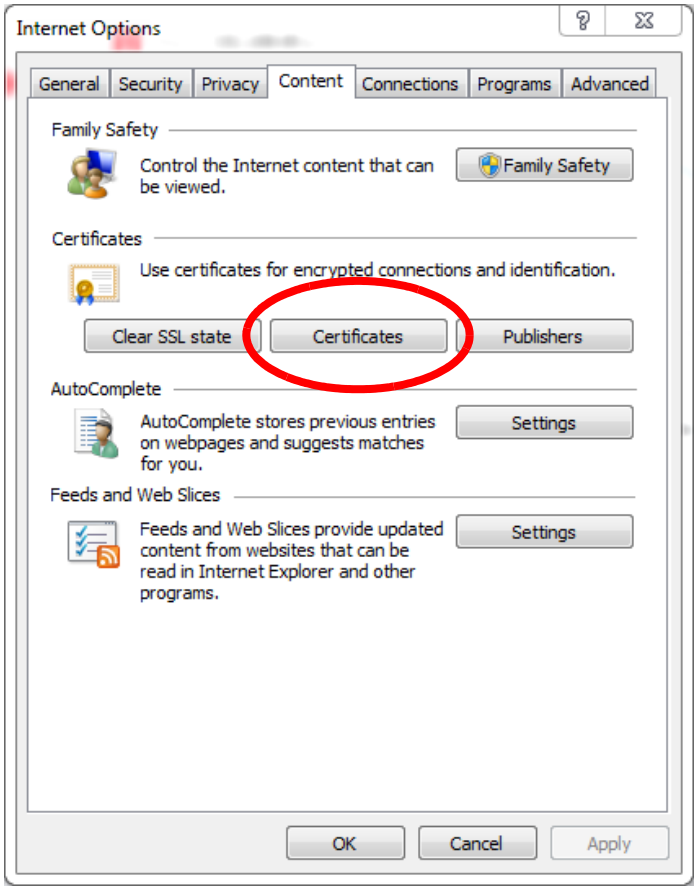
When using a self-signed certificate it is necessary to install the matching master certificate into all computer's browsers that access the MPA panels.

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.

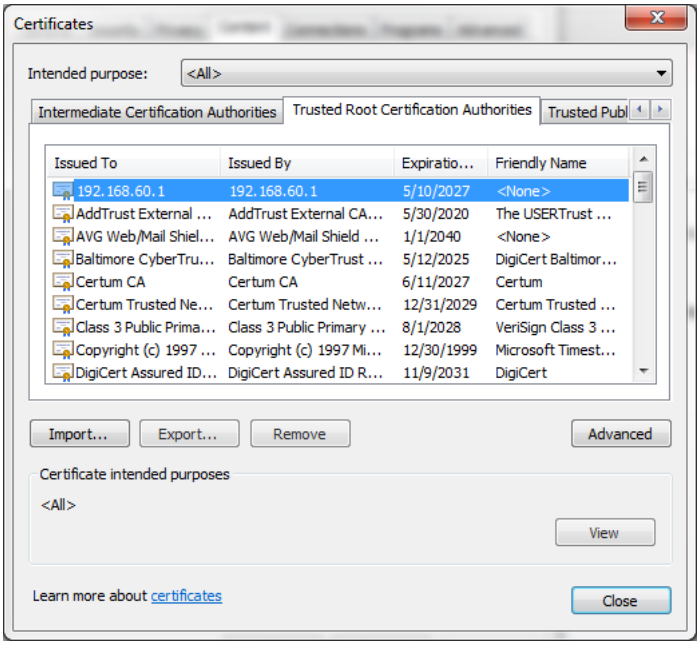


Open **Internet Explorer** and select **Tools (gear icon) > Internet** options.

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

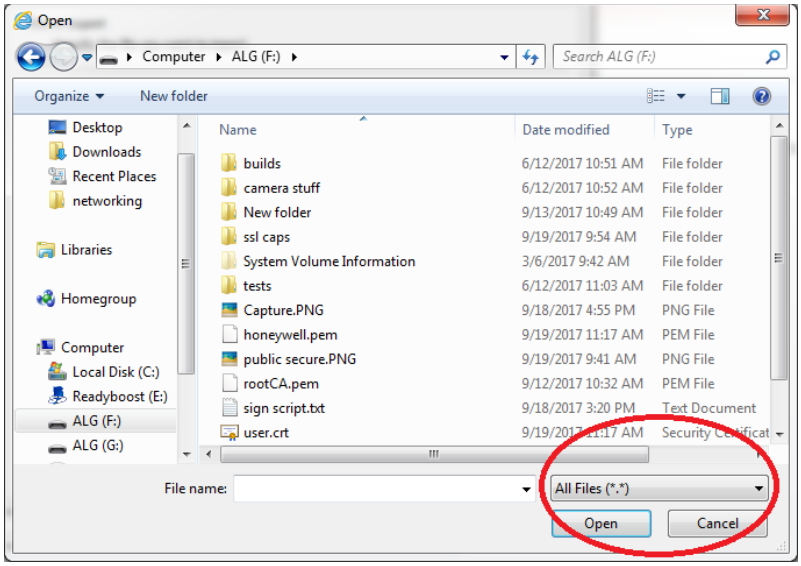


Select the **Trusted Root Certificate Authorities** tab, then select **Import**:

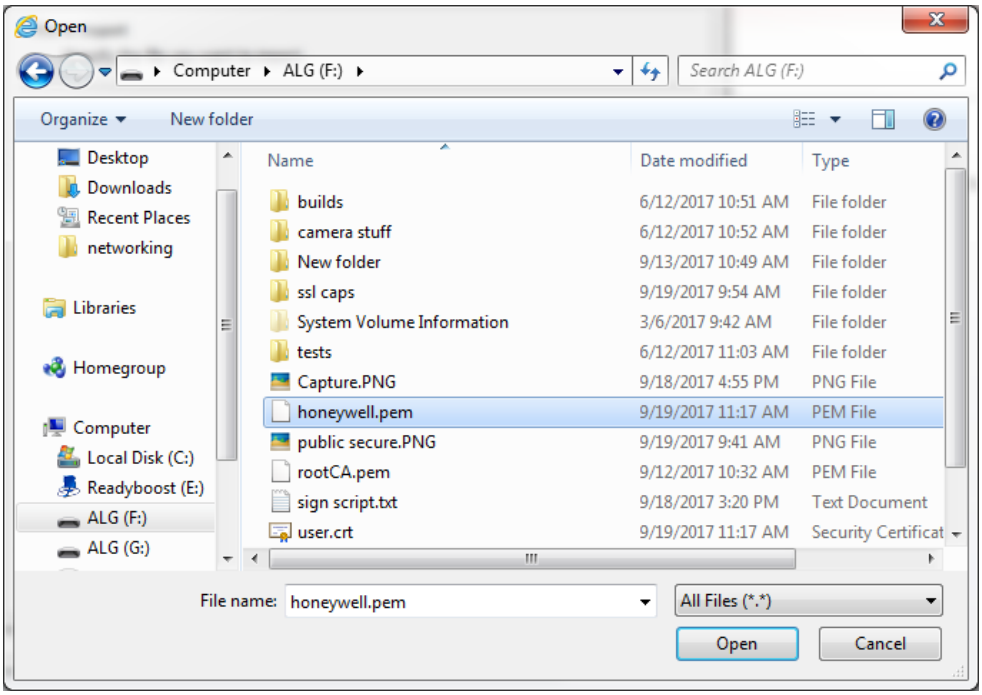


The **Certificate Import Wizard** will appear.

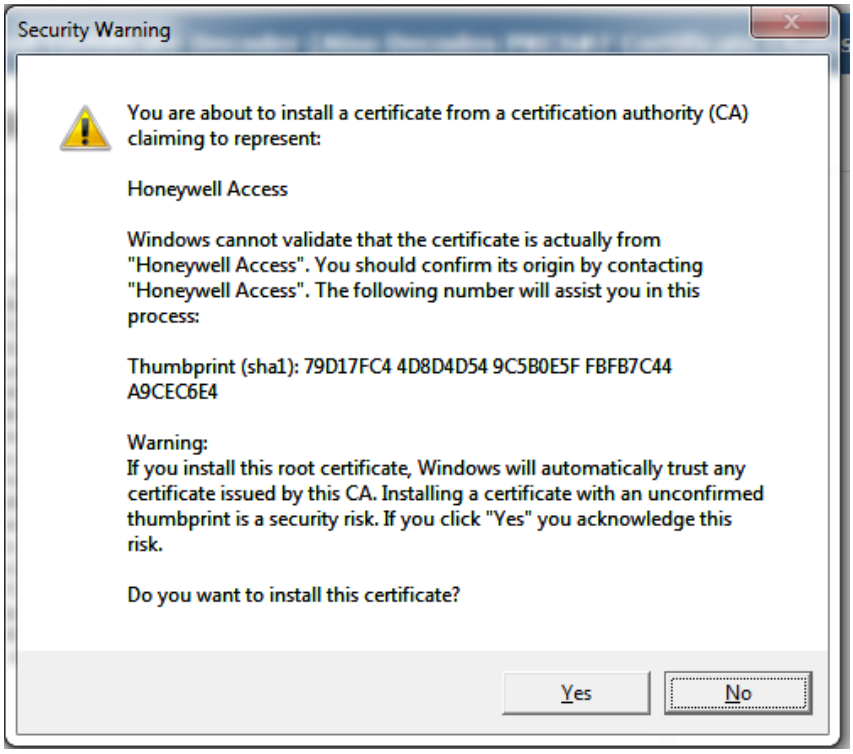
Select **Next** and Browse.



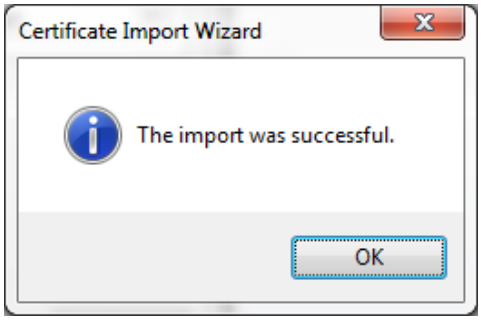
Change the file type to **All Files**. Then select **the master signed certificate** from its location on your machine.



Click **Open** to load the file.

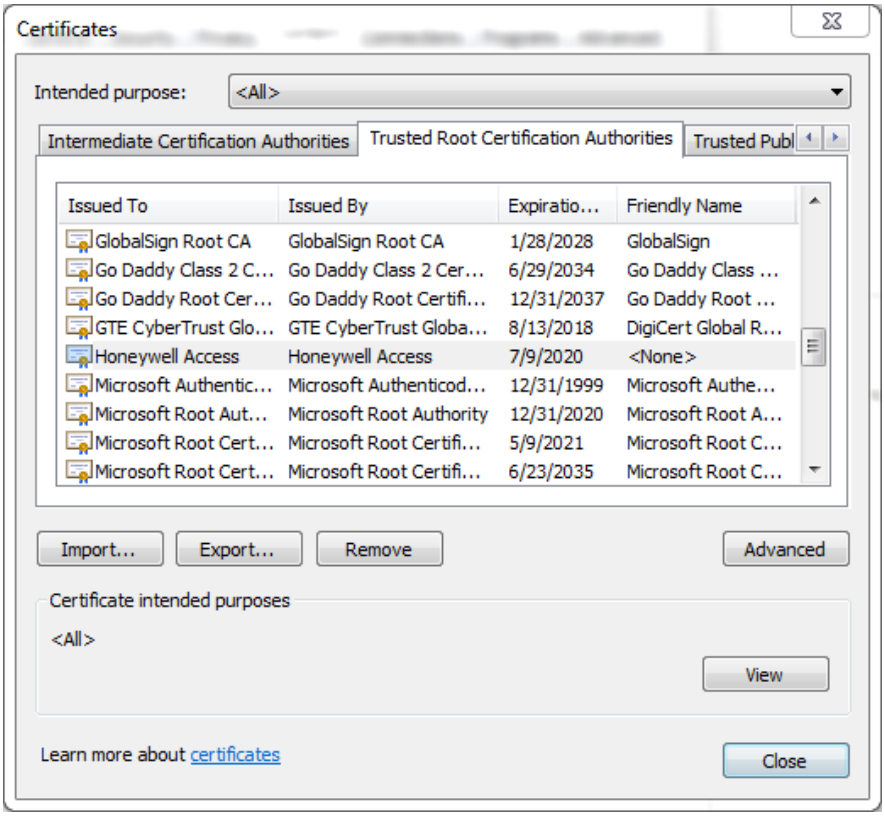


Confirm **Yes** when this warning comes up:



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".

MPA2 Accounts

Creating MPA2 Accounts

A User is someone who will be using the MPA2 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.

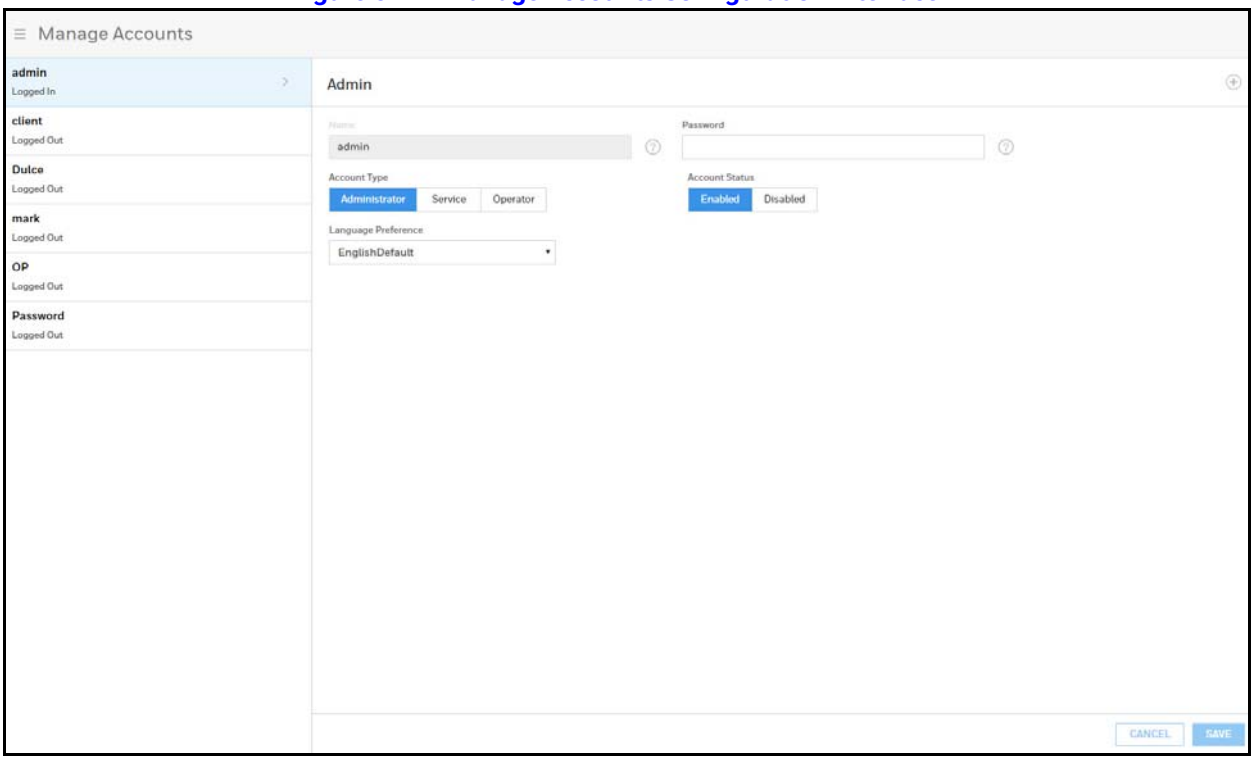
Table 6-1 User Access Types and Functionality

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

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.

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

Figure 6-1 Manage Accounts Configuration Interface

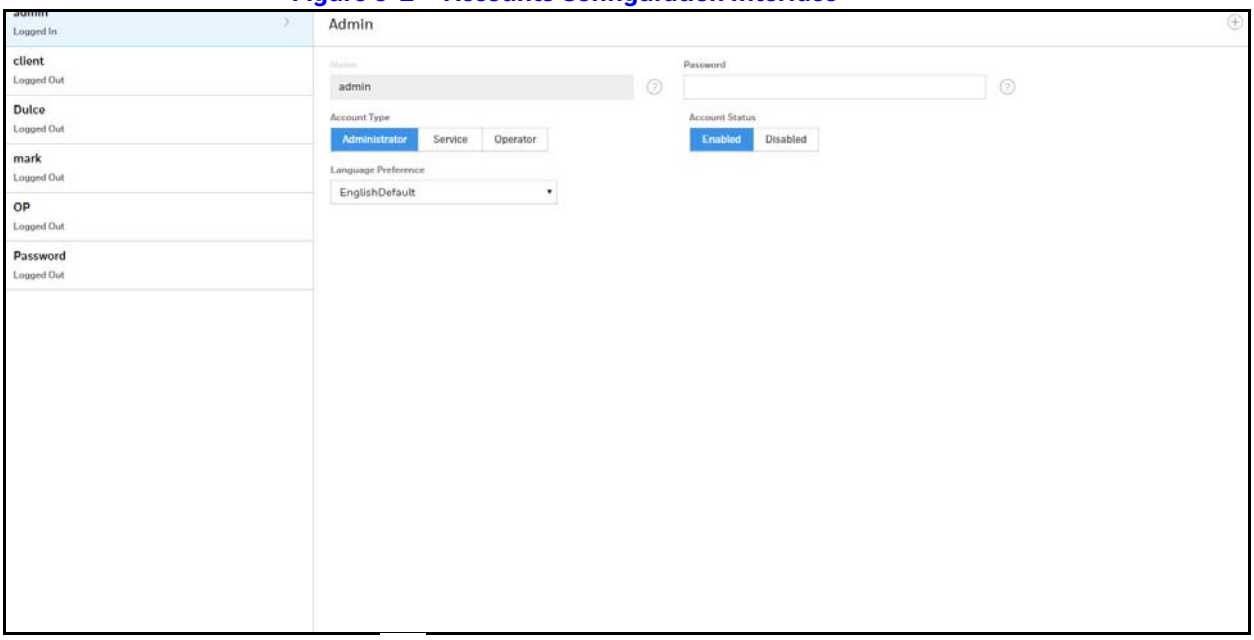


Note When creating passwords, they must meet the following minimum requirements:

- 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 6-2 Accounts Configuration Interface

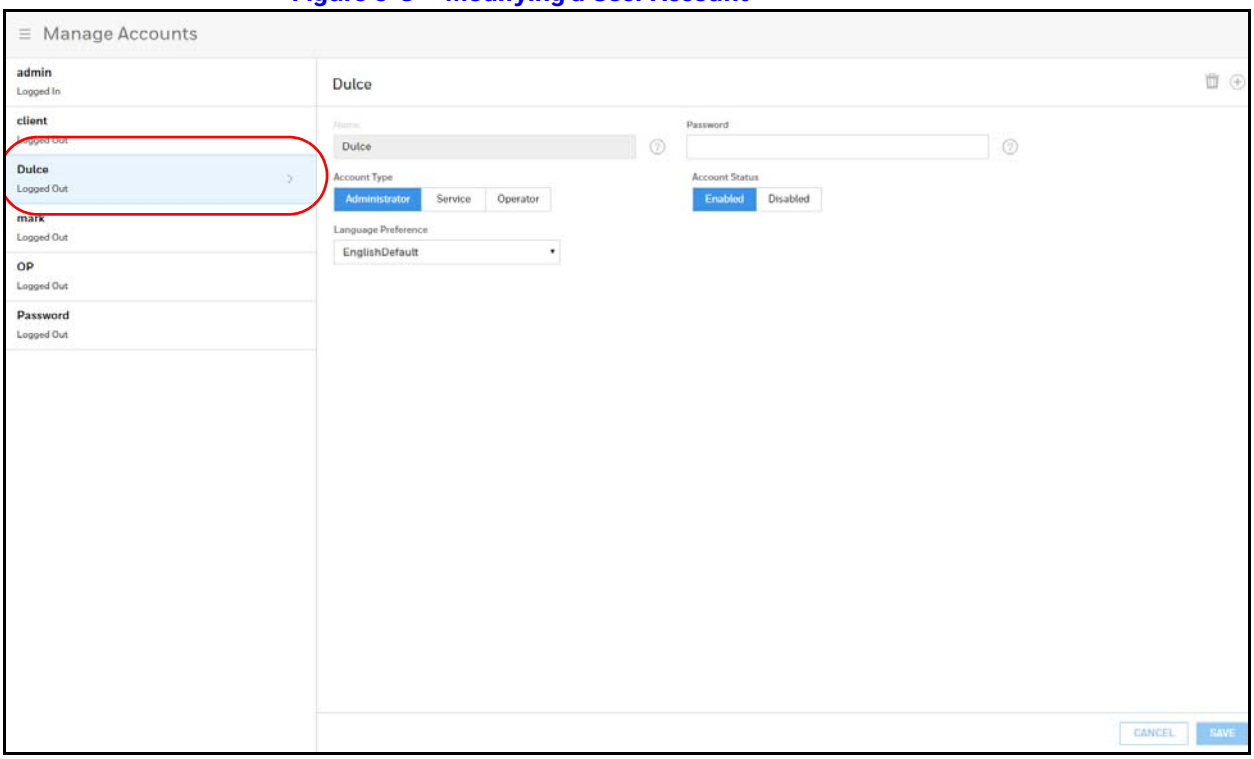


8. Click to ⊕ create a new account.
9. Enter a name.
10. Enter a **Password**.
11. Select an **Account Type**, either **Administrator**, **Service**, or **Operator**. See *Table 6-1* on *page 119* for more about these accounts.
12. Enable/disable the **Account Status**.
13. Select a language.
14. Click **Save**.

Modifying a User Account

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

Figure 6-3 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.

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

For technical assistance please visit https://www.honeywellaccess.com

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://honeywellaccess.com
	MyWebTech Customer Support	https://mywebtech.honeywell.com
	Schedule Support:	https://honeywellsystems.com/ss/schedulesupport/index.html
	Online Training:	https://honeywelldiscovertraining.com

Honeywell Access Systems
135 W. Forest Hill Avenue
Oak Creek, WI 53154
United States
☎ 800-323-4576

www.honeywellaccess.com
+1 800 323 4576, Option 2 (North America only)
https://mywebtech.honeywell.com

Document 800-25396 - B - Dec 2019

Please be aware that this product can store personal data.

Personal data is protected by the **General Data Protection Regulation** (2016/679) in Europe and therefore the owners of personal data have obtained certain rights thanks to this regulation.

We strongly advise you to be fully aware of these owner ("data subjects") rights as well as which limitations you have to obey regarding the use and distribution of this data.

Further details can be found on the GDPR website of the EU:
https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en