HIGHPOWER
SECURITY PRODUCTS

TEL: (203)-634-3900   FAX: (203)-886-0078
EMAIL: SALES@HIGHPOWERSECURITY.COM
WEB: WWW.HIGHPOWERSECURITY.COM

HighpowerOne Access Control System

8 DOOR CONTROLLER WITH TOUCHSCREEN

OPERATIONS MANUAL

FIRMWARE VERSION 1.0

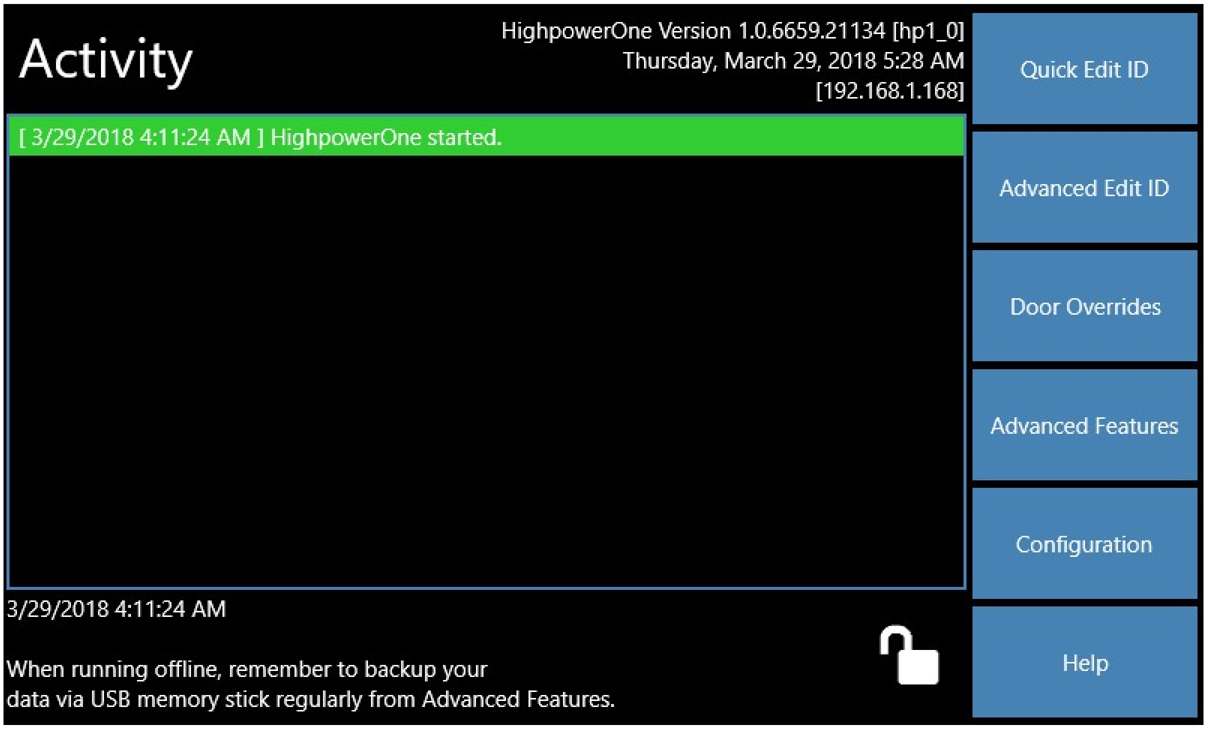
DOCUMENT NUMBER: 980-5000-1.1.0

Monday, May 21, 2018 5/21/2018 10:32:05 AM

Description

The HighpowerOne Access Control System is an eight-door access control panel that interfaces to both Wiegand and ABA type card readers. The unit incorporates an advanced single board computer running on Windows 10 that provides a touch-screen interface for programming. It features the latest SD storage technology providing an incredible amount of storage holding of millions of card numbers, holidays, schedules and activity records. The controller also has an integrated 100Mb ethernet controller and integrated Wi-Fi for remote control using the Highpower Management System software and third-party applications. Highpower provides a published software interface to the controller for software integration by third party manufacturers.

Main Activity Screen



Activity

HighpowerOne Version 1.0.6659.21134 [hp1_0]
Thursday, March 29, 2018 5:28 AM
[192.168.1.168]

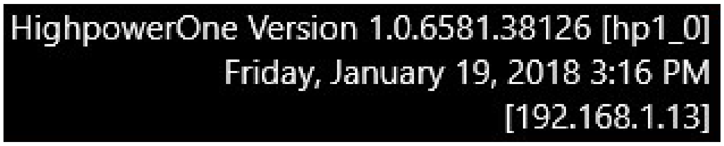
[3/29/2018 4:11:24 AM] HighpowerOne started.

3/29/2018 4:11:24 AM

When running offline, remember to backup your
data via USB memory stick regularly from Advanced Features.

System Information

The system information section of the screen is at the top and shows important data about your particular controller:



HighpowerOne Version 1.0.6581.38126 [hp1_0]
Friday, January 19, 2018 3:16 PM
[192.168.1.13]

System Information Line 1 (Version and WINS)

The name of the product along with its current firmware version. The firmware version includes the major and minor version, followed by the software build number information. In addition to this information, the WINS (IPV6 based) name of the controller. Typically, by default, the name of the device is HP1_<serial number> where the serial number is the name of the device. On a Windows network, you should be able to ping and address the device by this name.

System Information Line 2 (Current Time and Date)

This line shows the current date and time that is set on the controller. This time is used to log all of the transactions that occur in the controller with a time stamp. The controller has two sources for time; this is Internet Time Server time and the onboard Real Time Clock.

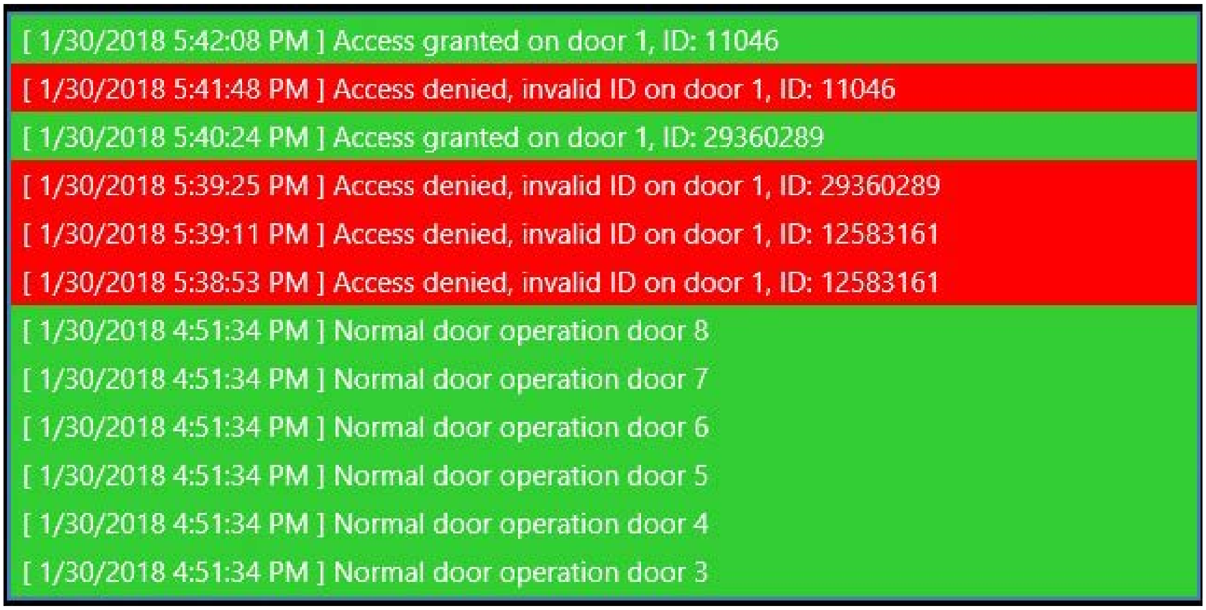
If you are using the controller with the Time Server setting enabled, then the controller will get the time off of a time server via the Internet. To use the Time Server setting properly, the controller would have to be connected to the internet via either the wired Ethernet connection or the Wi-Fi and have access to an internet gateway. Using the time server setting of the controller requires that you set the current time zone in the controller. Setting the time zone is described in a following section. If you are connected to the internet and use this setting, then the controller will always maintain the correct time and date including leap year and automatic daylight savings time compensation. This setting also prevents power outages from disrupting the time settings as the time is checked during power up on boot.

If the controller is not connected to a network and being used in a stand-alone mode via the touch screen, you must change the time setting to use the onboard Real Time Clock. This controller has a second clock source and you can use this Real Time Clock when the internet is not available. With the real-time clock, you set the time using the touch screen in the device and this time is backed up during power outages using an onboard supercapacitor. The time on the device should remain set for a period of approximately two weeks of power outage before having to be set again. In using the real-time clock, you do not have daylight saving time compensation, so you will have to use the touch screen to adjust for future daylight savings time intervals.

System Information Line 3 (Current IPV4 Addresses)

Line three lists all the current IPV4 addresses present in the controller. By default, the controller has IPV4 DNS functions turned on, so the controller will access DNS to assign an address to each of its network interfaces. There are usually at least one IP listed, but more can commonly become available. Usually the first address listed is present when the controller is plugged into a wired Ethernet connection. This is the IPV4 LAN address of the wired connection. The second address is typically the Wi-Fi LAN address. You can use these IPV4 addresses to connect to the controller through many interfaces, but using the WINS address is preferred. These interfaces include a multi-connection TCP/IP server that supports the Highpower command set at port 3000, a HTTP based hardware setup application at port 8080 and a perhaps a web server (implemented in a future release) at Port 80.

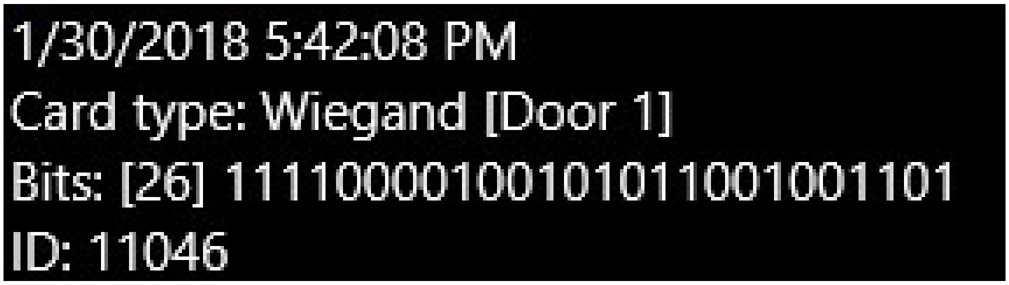
Activity Listing



```
[ 1/30/2018 5:42:08 PM ] Access granted on door 1, ID: 11046
[ 1/30/2018 5:41:48 PM ] Access denied, invalid ID on door 1, ID: 11046
[ 1/30/2018 5:40:24 PM ] Access granted on door 1, ID: 29360289
[ 1/30/2018 5:39:25 PM ] Access denied, invalid ID on door 1, ID: 29360289
[ 1/30/2018 5:39:11 PM ] Access denied, invalid ID on door 1, ID: 12583161
[ 1/30/2018 5:38:53 PM ] Access denied, invalid ID on door 1, ID: 12583161
[ 1/30/2018 4:51:34 PM ] Normal door operation door 8
[ 1/30/2018 4:51:34 PM ] Normal door operation door 7
[ 1/30/2018 4:51:34 PM ] Normal door operation door 6
[ 1/30/2018 4:51:34 PM ] Normal door operation door 5
[ 1/30/2018 4:51:34 PM ] Normal door operation door 4
[ 1/30/2018 4:51:34 PM ] Normal door operation door 3
```

The main activity screen has a scrolling audit trail window that shows system activity. This includes valid and invalid card access requests, requests to exit, output changes due to schedule activity and door override commands. All activity listed in this screen is simultaneously logged into onboard transaction records. These activity records are typically downloaded remotely via Ethernet or Wi-Fi or can also be used to generate an audit trail report onto a USB memory stick.

Card Reader Data Listing



```
1/30/2018 5:42:08 PM
Card type: Wiegand [Door 1]
Bits: [26] 11110000100101011001001101
ID: 11046
```

When a card is presented to a connected card reader, the controller will analyze the card reader output to determine if the data is of Wiegand or ABA type (ABA type is magnetic stripe data, also known as Clock and Data).

Card Reader Listing Line 1 (Date and time of card use)

This is date and time that the card was used on the reader.

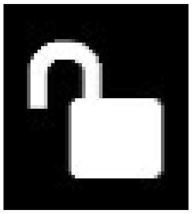
Card Reader Listing Line 2 (Card type)

This is the type of signal that is coming off of the reader. The signal will either be electrically Wiegand or ABA types. The ABA is magstripe output (also known as Clock and Data). The reader will analyze the data to determine what type of decoding is necessary to decode the bit data.

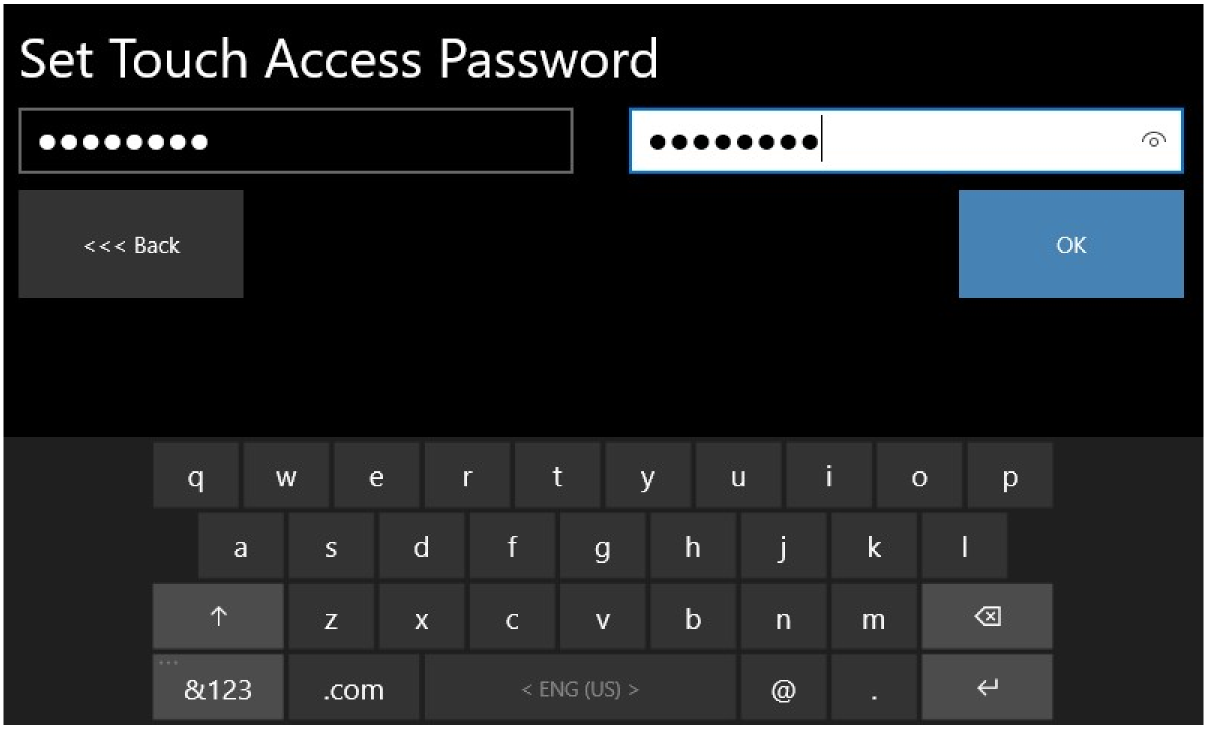
Card reader Listing Line 3 (Bit count and actual bit listing)

This line will show the bits that are coming off the reader and the number of bits. The number of bits is especially useful when handling different Wiegand card format types. The controller can be programmed to accept any Wiegand configuration up to 255 bits. There is a section further down the manual that explains how to program alternative Wiegand formats into the controller.

Screen Lock Feature



Pressing on this icon located at the bottom right of the main screen allows the operator or service person to lock the touch screen to prevent the tampering of settings by unauthorized people. Once you press this icon, you will be brought to a screen where you will have to enter the password twice.

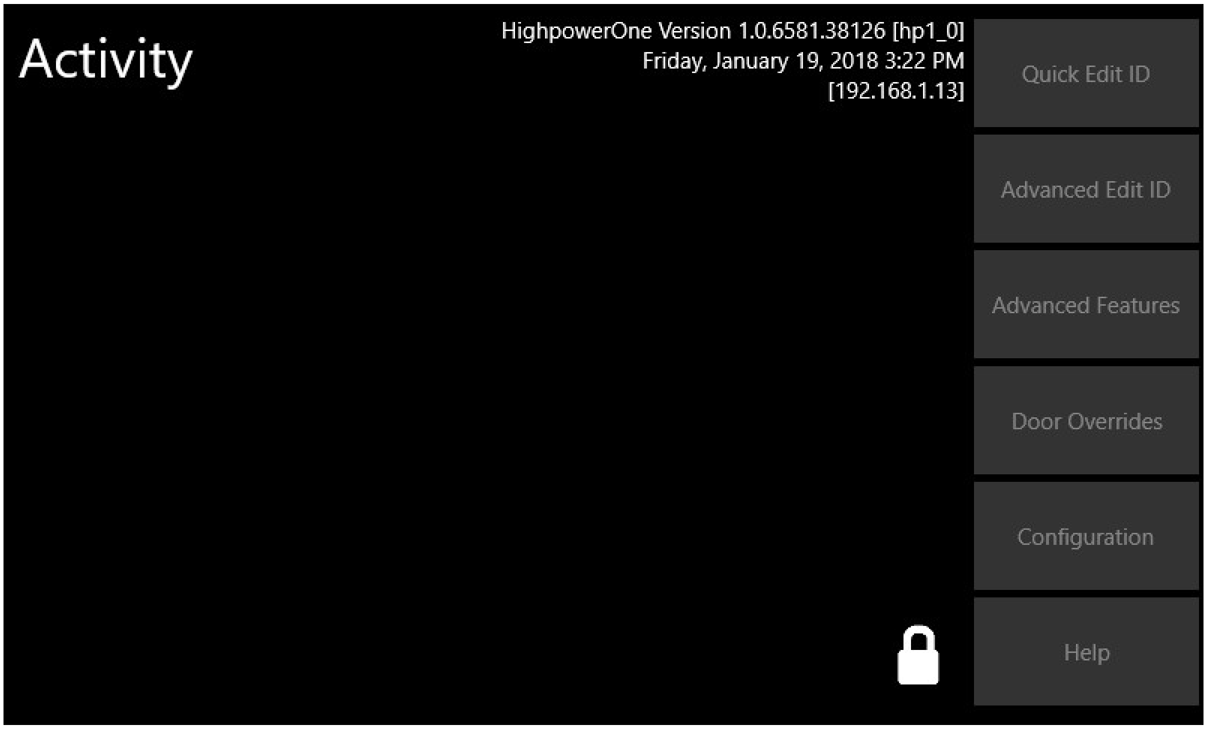


Set Touch Access Password

●●●●●●●●

●●●●●●●●

If the two entries of the password match, clicking OK on the password screen will lock the controller. Once the controller is locked, the padlock will show a locked state and the buttons on the main screen will be greyed out and inoperable. The activity window is hidden in this locked state.

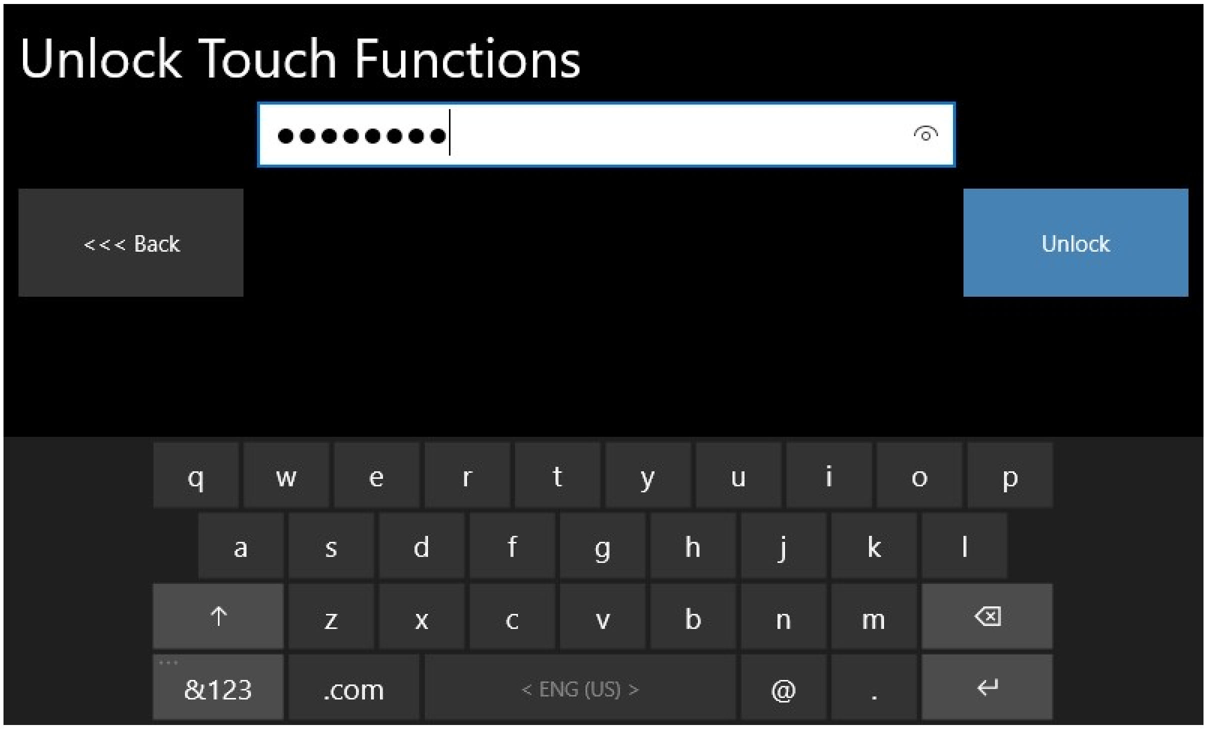


Activity

HighpowerOne Version 1.0.6581.38126 [hp1_0]
Friday, January 19, 2018 3:22 PM
[192.168.1.13]

Do not forget the set password! If this password is forgotten, there is no easy way to get back into the controller without contacting technical support.

To unlock the screen, touch the locked padlock icon again and enter the password.



Unlock Touch Functions

Clearing the activity window

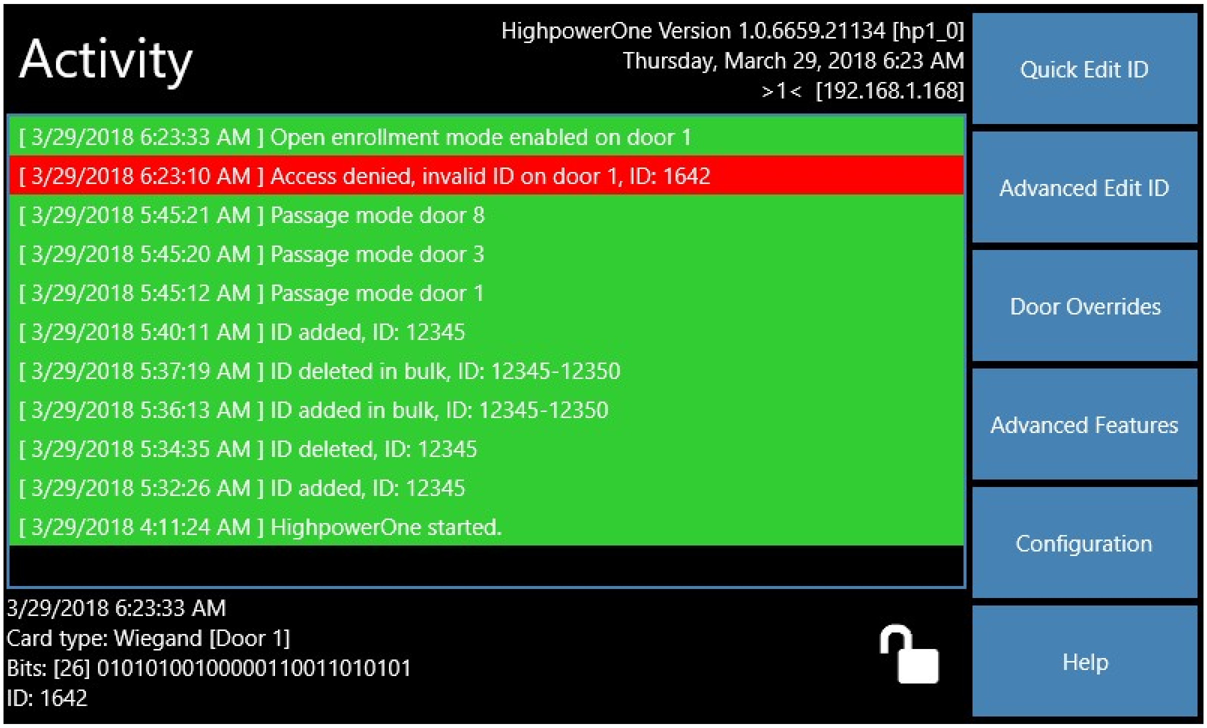
You can hold your finger on the activity window for a few seconds. This will prompt the controller to ask you if you want to clear all activity. The activity will still be present in the controller's memory log, but the activity window is cleared. This is useful when you are doing reader and request to exit switch debugging during the installation of the controller.

Open Enrollment Mode

Open enrollment mode is a mode that allows you to add cards to a certain reader at the reader without interaction with the touchscreen or software. To use this feature, you need to tell the controller that a certain card ID is to be the “open enrollment” card. You specify this card ID using the “Programming Card Configuration” feature under the “Advanced Settings” screen.

Once the open enrollment card is swiped on a reader, the reader will accumulate all the cards that are swiped after it. It will store each card in memory in an “all times” access level. After swiping multiple cards, you can exit this enrollment mode by swiping another programming card. Once you exit the mode, the accumulated cards will operate the door on that reader during all times. This is basically a quick add card feature using just the reader as a programming device.

During the open enrollment mode, the main screen will show an icon to indicate that a certain reader is in this mode:



Activity

HighpowerOne Version 1.0.6659.21134 [hp1_0]
Thursday, March 29, 2018 6:23 AM
>1< [192.168.1.168]

```
[ 3/29/2018 6:23:33 AM ] Open enrollment mode enabled on door 1
[ 3/29/2018 6:23:10 AM ] Access denied, invalid ID on door 1, ID: 1642
[ 3/29/2018 5:45:21 AM ] Passage mode door 8
[ 3/29/2018 5:45:20 AM ] Passage mode door 3
[ 3/29/2018 5:45:12 AM ] Passage mode door 1
[ 3/29/2018 5:40:11 AM ] ID added, ID: 12345
[ 3/29/2018 5:37:19 AM ] ID deleted in bulk, ID: 12345-12350
[ 3/29/2018 5:36:13 AM ] ID added in bulk, ID: 12345-12350
[ 3/29/2018 5:34:35 AM ] ID deleted, ID: 12345
[ 3/29/2018 5:32:26 AM ] ID added, ID: 12345
[ 3/29/2018 4:11:24 AM ] HighpowerOne started.
```

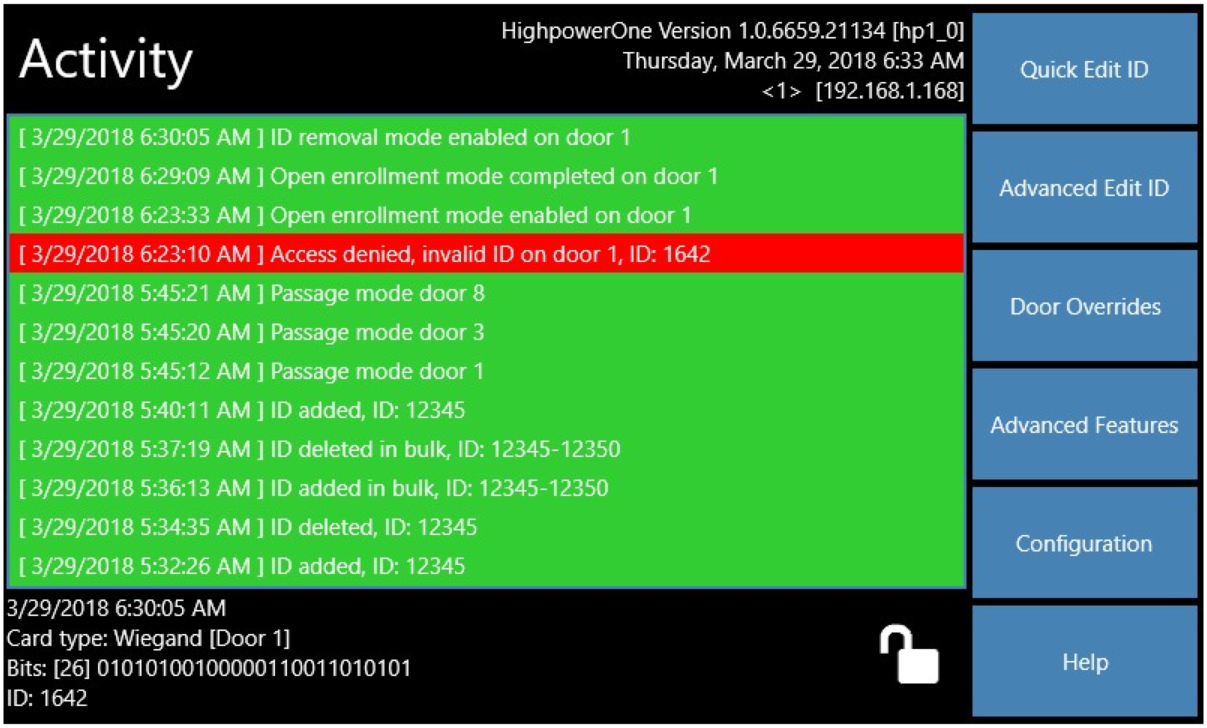
3/29/2018 6:23:33 AM
Card type: Wiegand [Door 1]
Bits: [26] 01010100100000110011010101
ID: 1642

In our example, we can see that reader 1 is in open enrollment mode because there is a “>1<” icon showing next to the IPV4 address in the main screen. Also, there is a log entry at the top of the log that says, “Open enrollment mode enabled on door 1”. As long as the “>1<” icon is showing, the reader is in the enrollment mode, adding cards to memory as they are being swiped.

There is an option in the open enrollment programming card setup screen to activate the relay during a card enrollment. If you turn this option on, the door will open for every card that is enrolled during the enrollment mode, simulating a valid swipe during enrollment. This allows the door to operate normally during an enrollment period simulating normal door operation to users. Once the enrollment period has ended, you turn off the open enrollment with a programming card and only cards that were enrolled then operate the door. You can use this feature to automatically collect card numbers in the case that card numbers are unknown for low security applications.

ID Removal Mode

ID removal mode removes IDs as they are swiped on the reader. This mode works in conjunction with the Open Enrollment mode. After a “programming removeable” card is swiped on a reader, all cards swiped subsequently are removed from memory. You specify this card ID using the “Programming Card Configuration” feature under the “Advanced Settings” screen.



```
HighpowerOne Version 1.0.6659.21134 [hp1_0]
Thursday, March 29, 2018 6:33 AM
<1>  [192.168.1.168]
[ 3/29/2018 6:30:05 AM ] ID removal mode enabled on door 1
[ 3/29/2018 6:29:09 AM ] Open enrollment mode completed on door 1
[ 3/29/2018 6:23:33 AM ] Open enrollment mode enabled on door 1
[ 3/29/2018 6:23:10 AM ] Access denied, invalid ID on door 1, ID: 1642
[ 3/29/2018 5:45:21 AM ] Passage mode door 8
[ 3/29/2018 5:45:20 AM ] Passage mode door 3
[ 3/29/2018 5:45:12 AM ] Passage mode door 1
[ 3/29/2018 5:40:11 AM ] ID added, ID: 12345
[ 3/29/2018 5:37:19 AM ] ID deleted in bulk, ID: 12345-12350
[ 3/29/2018 5:36:13 AM ] ID added in bulk, ID: 12345-12350
[ 3/29/2018 5:34:35 AM ] ID deleted, ID: 12345
[ 3/29/2018 5:32:26 AM ] ID added, ID: 12345
3/29/2018 6:30:05 AM
Card type: Wiegand [Door 1]
Bits: [26] 01010100100000110011010101
ID: 1642
```

In our example, we can see that reader 1 is in card removal mode because there is a “<1>” icon showing next to the IPV4 address in the main screen. Also, there is a log entry at the top of the log that says, “ID removal mode enabled on door 1”. As long as the “<1>” icon is showing, the reader is in removal mode, removing cards from memory as they are being swiped. To exit the mode, swipe any programming card.

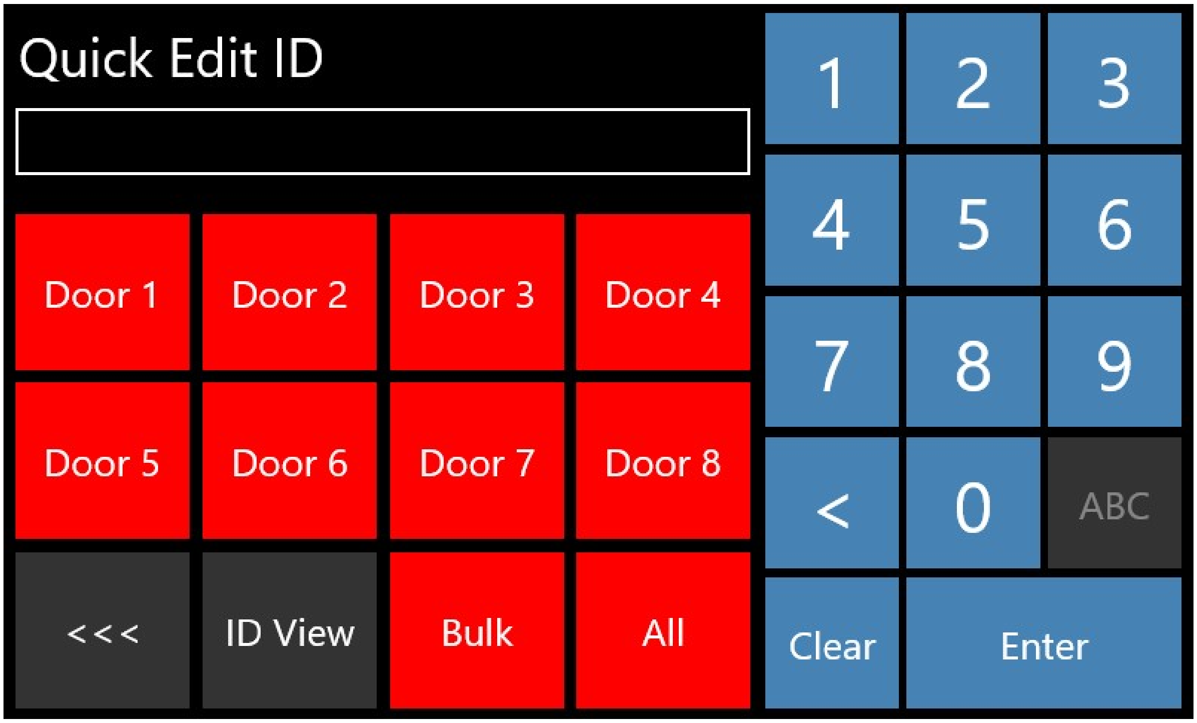
Main Function Buttons

The function buttons at the right on the main screen are used to perform all of the programming functions of the controller. These functions are outlined in the next section (Touch Screen Programming).

Touch Screen Programming

Quick Edit ID

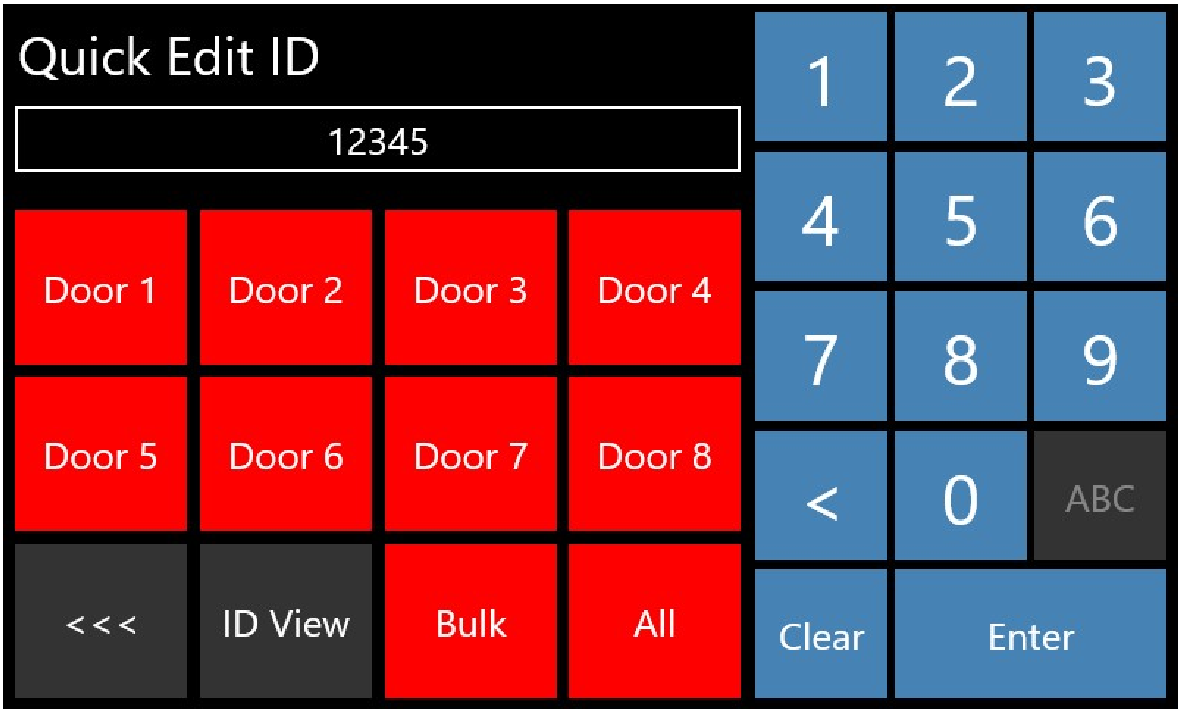
The Quick Edit ID screen of the controller is used to quickly add, delete, bulk enroll, or bulk delete card ID numbers. Card IDs on the controller can be numeric or alphanumeric. Wiegand cards are typically numeric only. ABA type cards using magstripe Track I character set can be alphanumeric. Version 1.0 of the controller only supports the Track II character set, but by allowing alphanumeric entry, future support for Track I character set can be added. Entering cards using the Quick Edit ID feature means that the card will work **a door or doors at all times**. To enter a card that only operates on doors between scheduled times, you need to use the Advanced Edit ID feature described in a following section.



Adding a single card ID

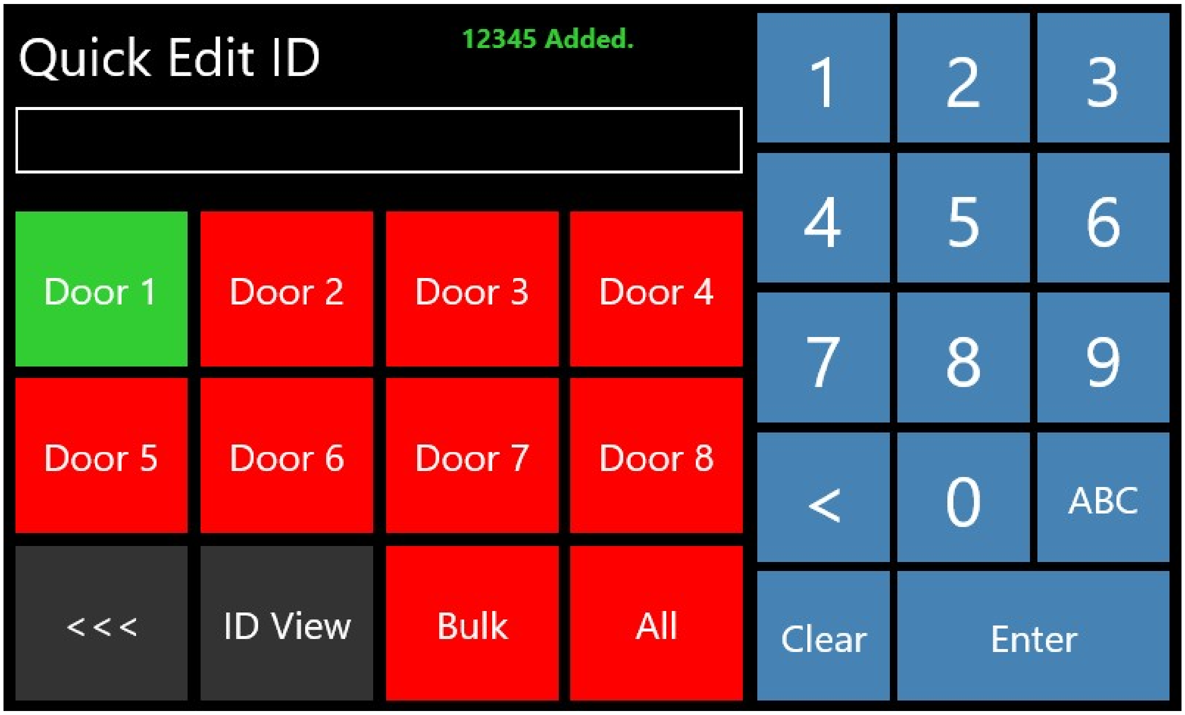
To add a single numeric card, just enter the card number using the blue keypad on the right side of the screen. As you type the numbers, the text box at the top of the screen (outlined in blue) will populate with the digits as you type them. If you make a mistake and enter an incorrect digit, use the "<" button to delete the last digit. If you want to clear all the digits at once, use the "Clear" key on the keypad.

Once you have entered the card number, select the door or doors that the card should operate on (at all times) by pressing the "Door 1" - "Door 8" buttons. When you press on a door button and the door is selected, the button will change in color from Red to Green. See example below of entering card "12345" to Door 1:



If you want to quickly select all of the doors, or deselect all of the doors, you can alternatively press the "All" button at the bottom and the selection of the doors will toggle between all selected and none selected for each press of the "All" button. You will see all of the buttons toggle between the red and the green states. Green means that the card is to be added to that door's memory.

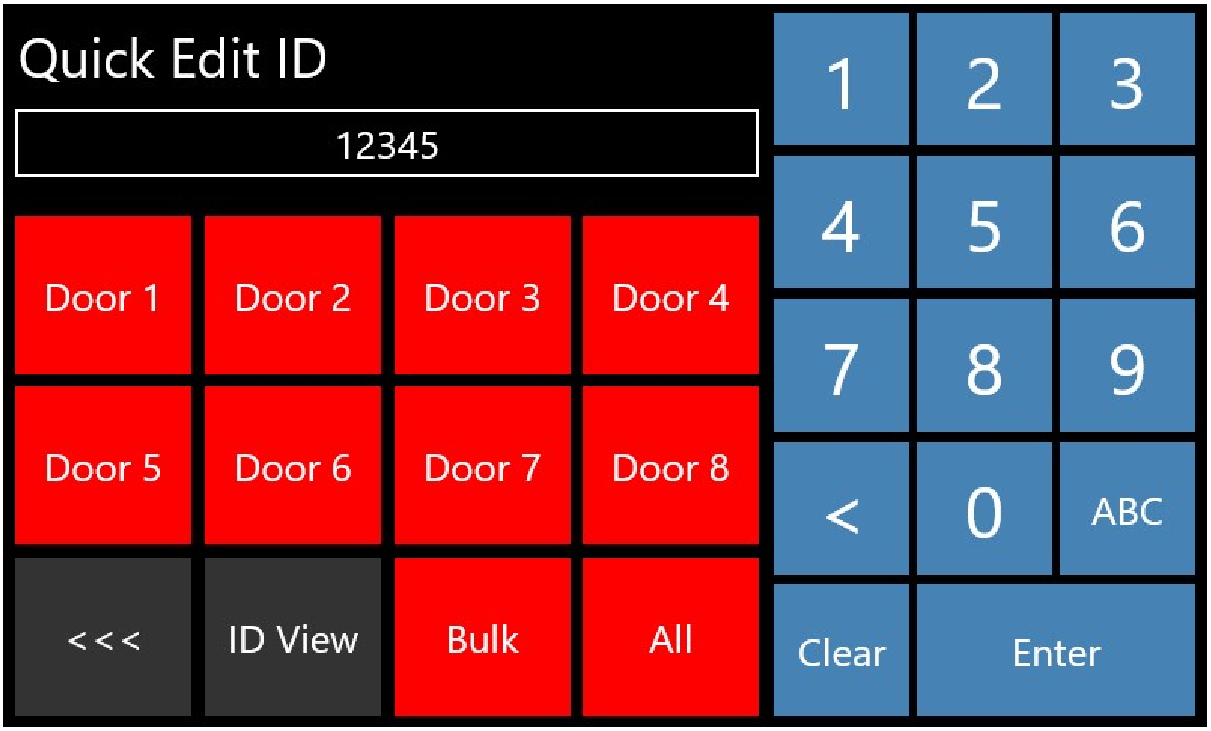
To perform the add, press the "Enter" button on the keypad and the card is added to memory. A green message at the top of the screen will confirm the entry and the card ID box is cleared. The automatic clearing of the card entry box allows for quick entry of the next card ID.


Quick Edit ID

12345 Added.

Deleting a single card ID

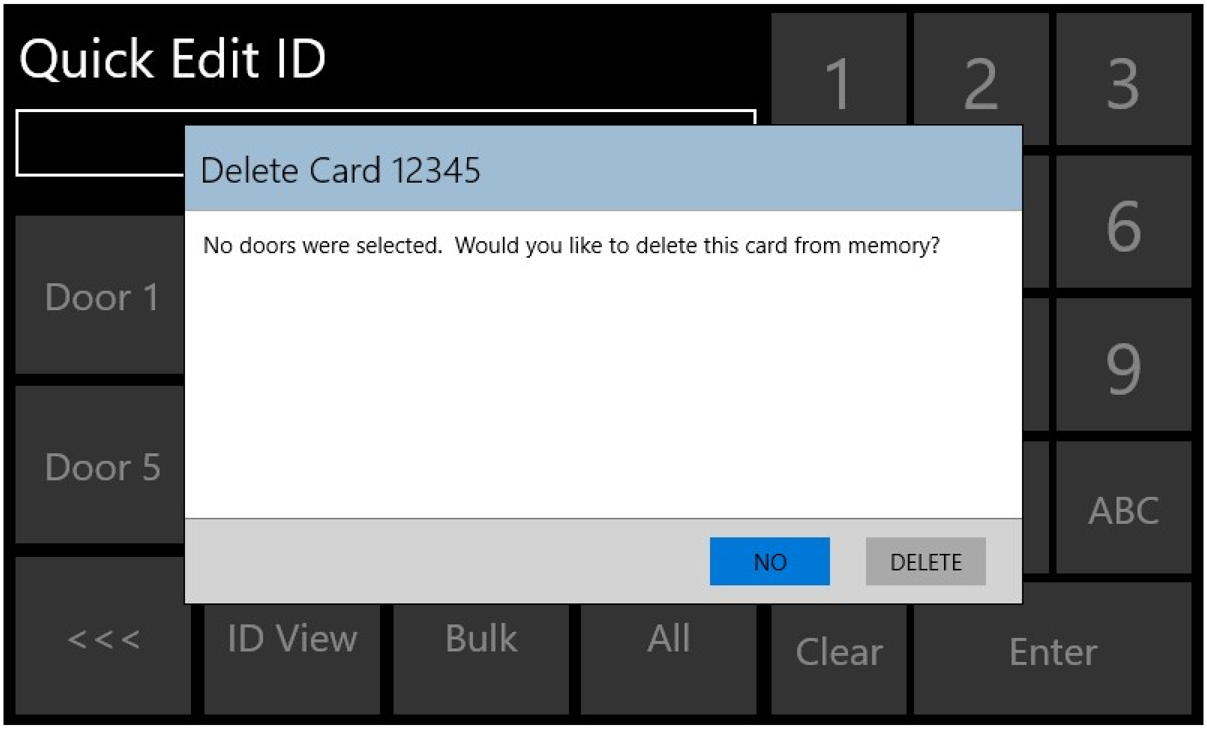
Deleting a single card from memory is like the add process. You enter the card number that is to be deleted on the blue keypad. To start the delete process, you simply make sure that all of the door keys "Door 1" - "Door 8" are unselected (red in color).



Quick Edit ID

12345

After entering the card number and making sure that none of the door buttons are selected, press the “Enter” key. The controller will look up in its memory to see if the card is in memory for any of the doors. If the card is not in memory, the controller will show a red message at the top of the screen telling you that the card was not found and does not need to be deleted. If the card is found, the controller prompt you to make sure that you actually want to delete the card ID.

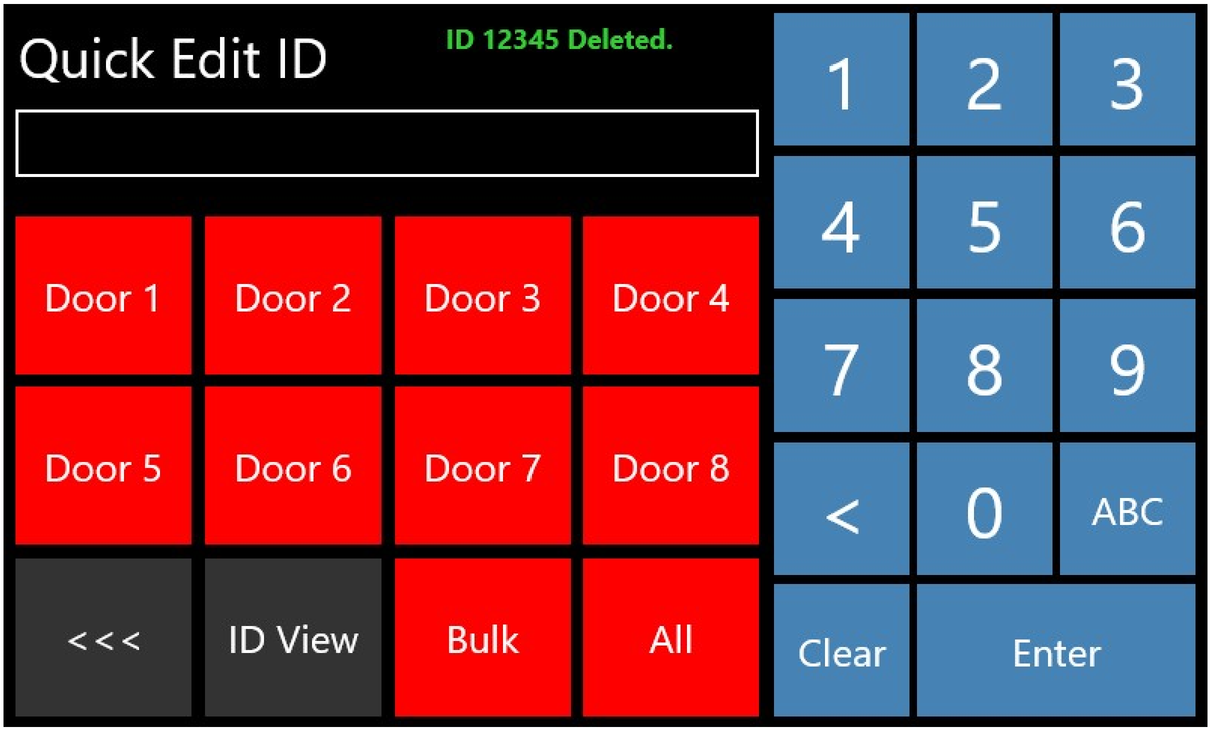


Quick Edit ID

Delete Card 12345

No doors were selected. Would you like to delete this card from memory?

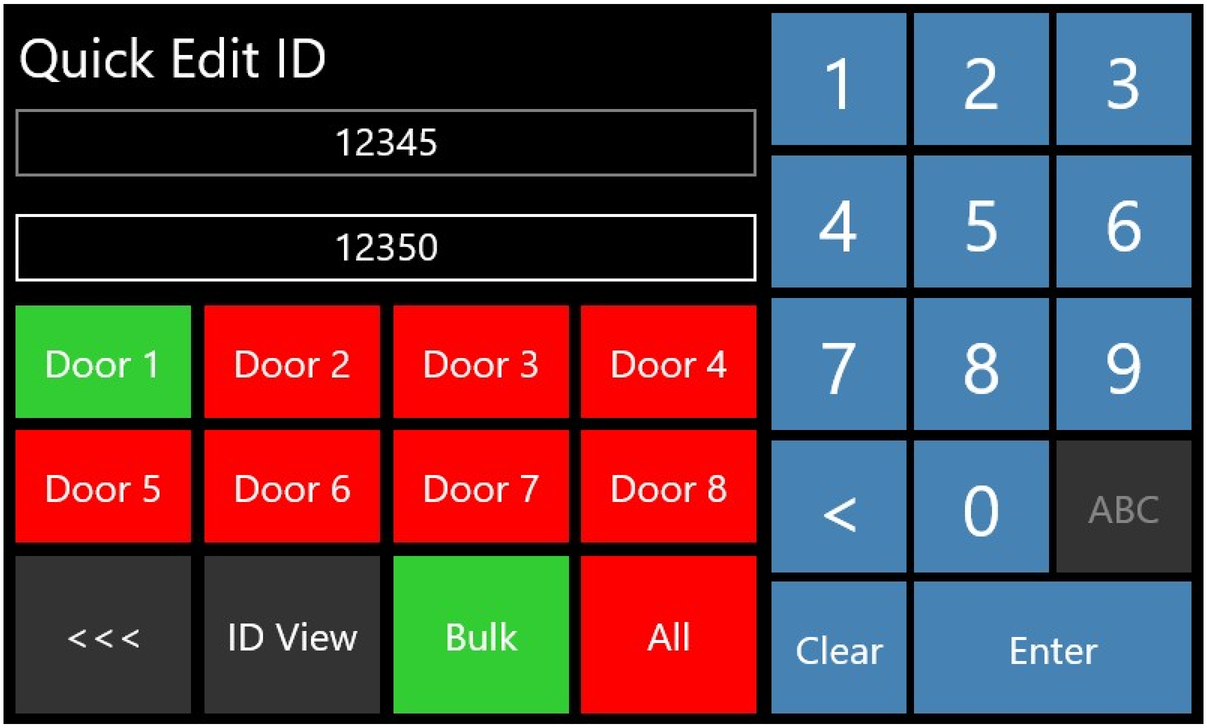
After selecting “Delete” the controller will delete the card ID from all of the doors and provide a message at the top of the screen that the card was deleted.



Bulk Enrolling a range of card IDs

The Quick Edit ID screen is not limited to just entering a single card. If you have a sequence of cards, you can enroll the entire sequence in one action. The screen can be used to enter a range of numeric IDs. Bulk enrolling is limited to numeric cards. To bulk enroll, press the “Bulk” button. This button will turn green and a second card number box will be shown at the top of the screen. To bulk enroll, you need to provide a start ID number and inclusive end ID number.

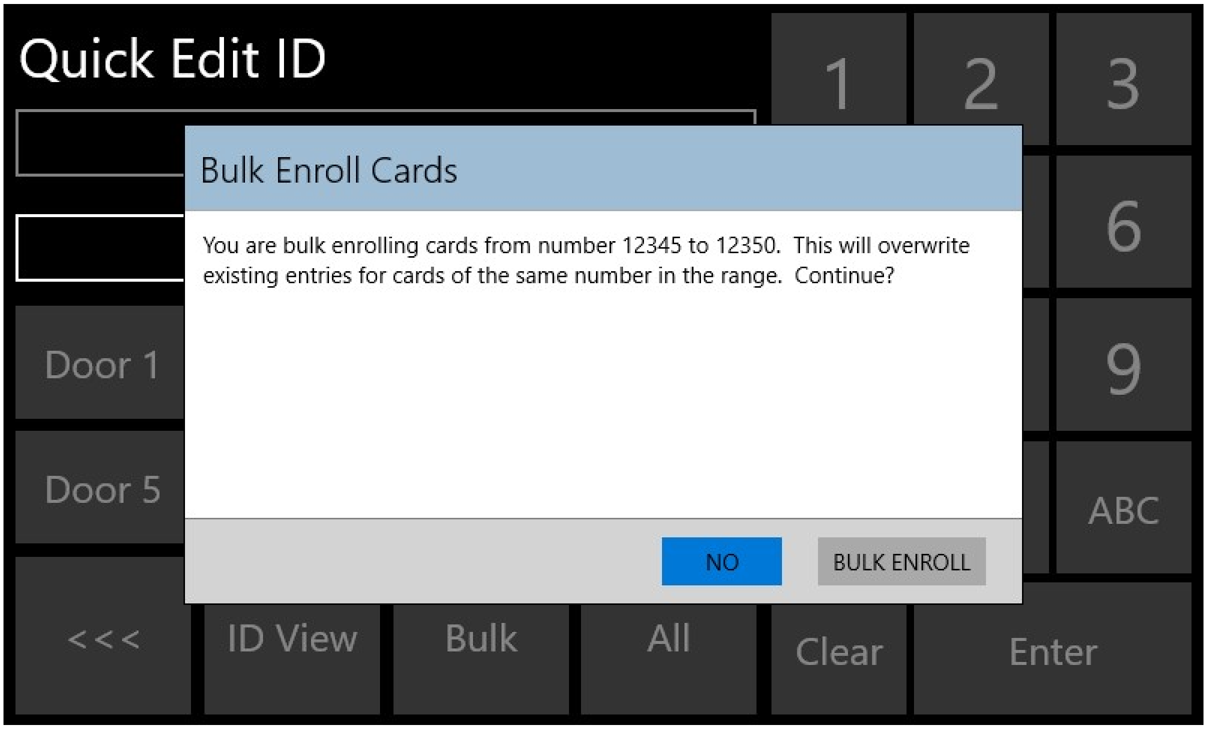
To enter the starting number, touch the top entry box (outlined in blue) and then use the keypad to enter the card ID. Then touch the second entry box below the first and enter the end card number.



12345

12350

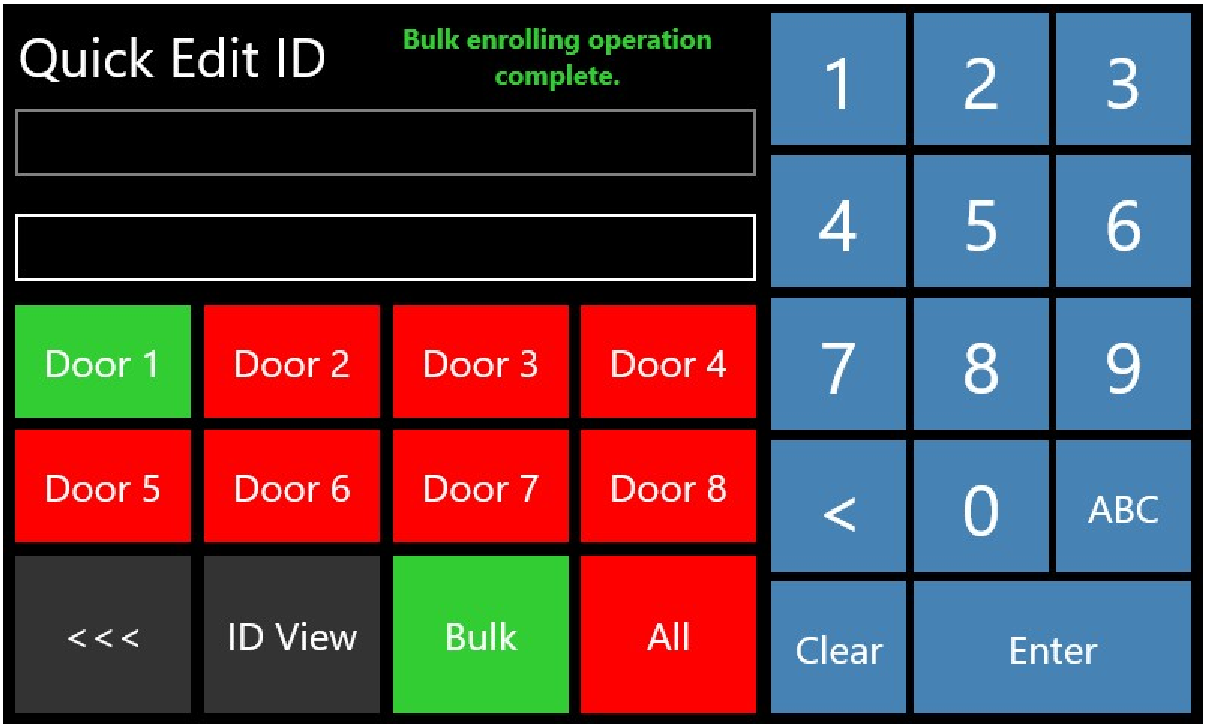
Select the doors that this block of codes should operate on at all times. Once you have selected the appropriate doors, press the “Enter” key and the controller will prompt you with an “Are you sure…” message.



Bulk Enroll Cards

You are bulk enrolling cards from number 12345 to 12350. This will overwrite existing entries for cards of the same number in the range. Continue?

If you are sure, click “Bulk Enroll” on this prompt and the bulk enroll process quickly adds all of the cards.



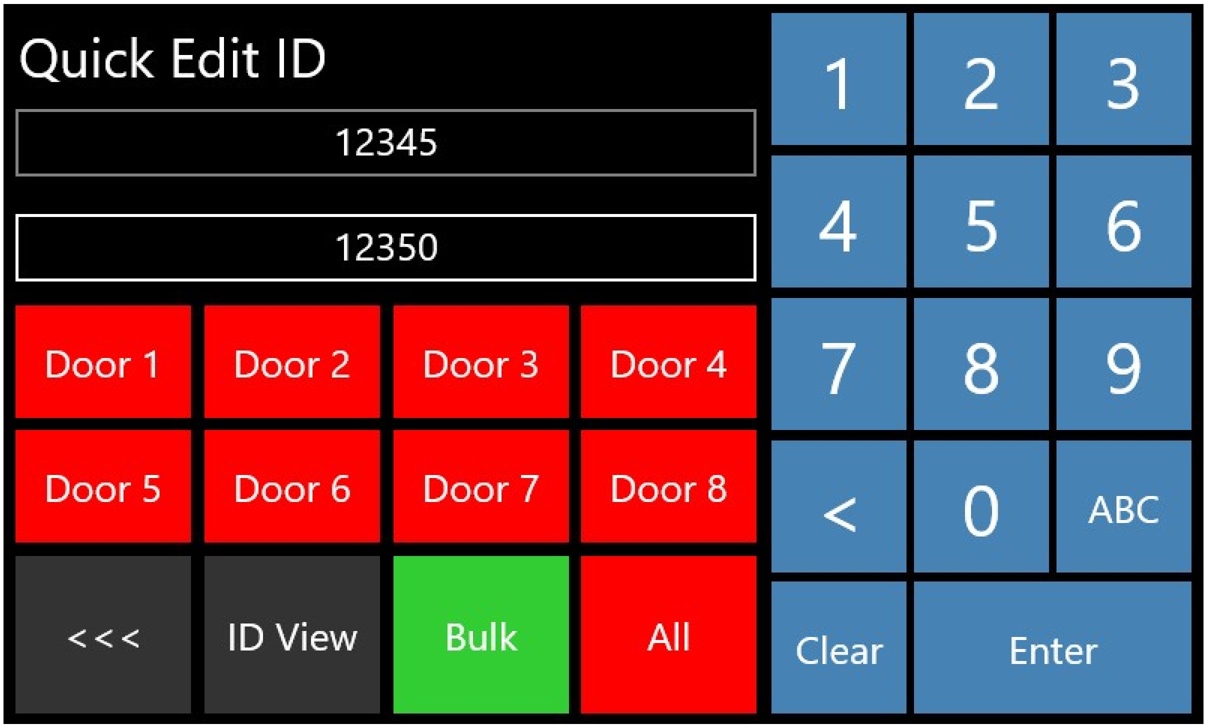
Quick Edit ID

Bulk enrolling operation complete.

Note: If you add a leading zero to the card ID in the first entry box, the controller will add leading zeros to all IDs that are enrolled. The card ID with leading zeros is a different ID than one without. For example, card ID “001” is different than card ID “1”.

Bulk Deleting a range of card IDs

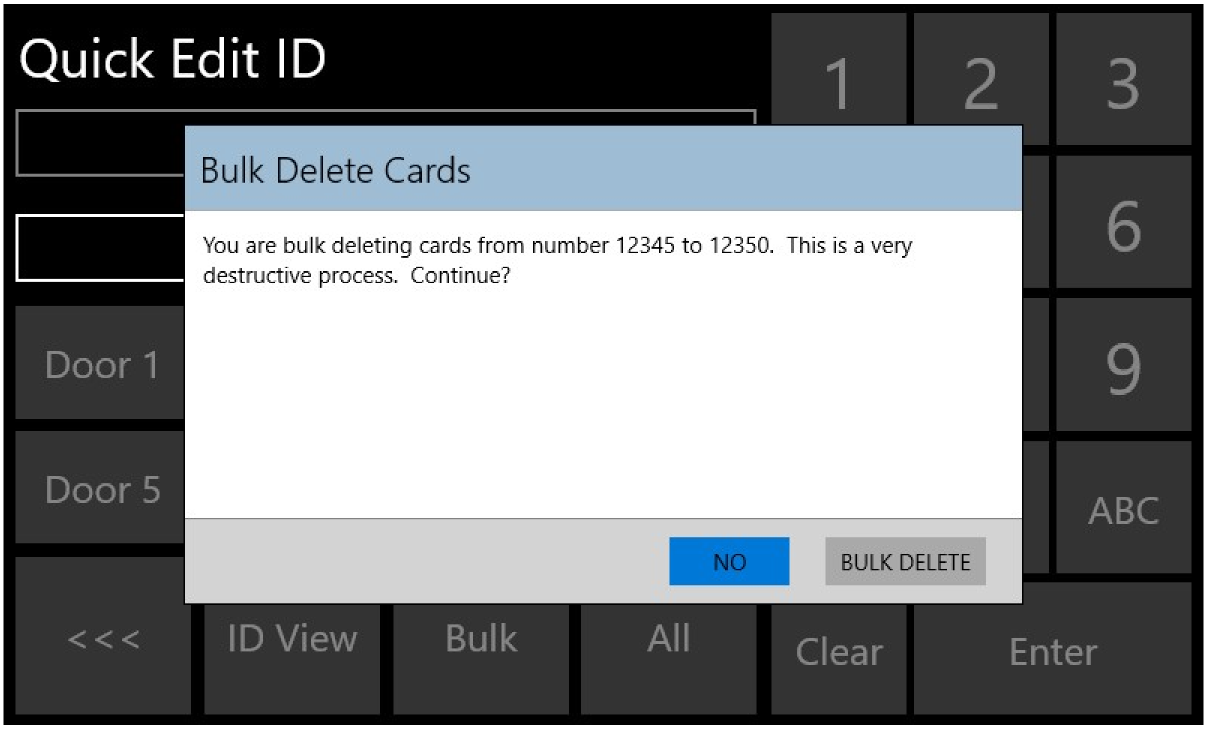
The bulk deleting process is like the bulk enroll process. After pressing the “Bulk” button at the bottom of the screen, two text entry boxes are presented at the top. Enter the starting card ID number in the top field and the ending card ID number in the field underneath the first. Once you have the card ranges to delete established, make sure all of the door buttons “Door 1” - “Door 8” are unselected (red in color). By unselecting all of the doors the controller knows that you are deleting a range of cards.



12345

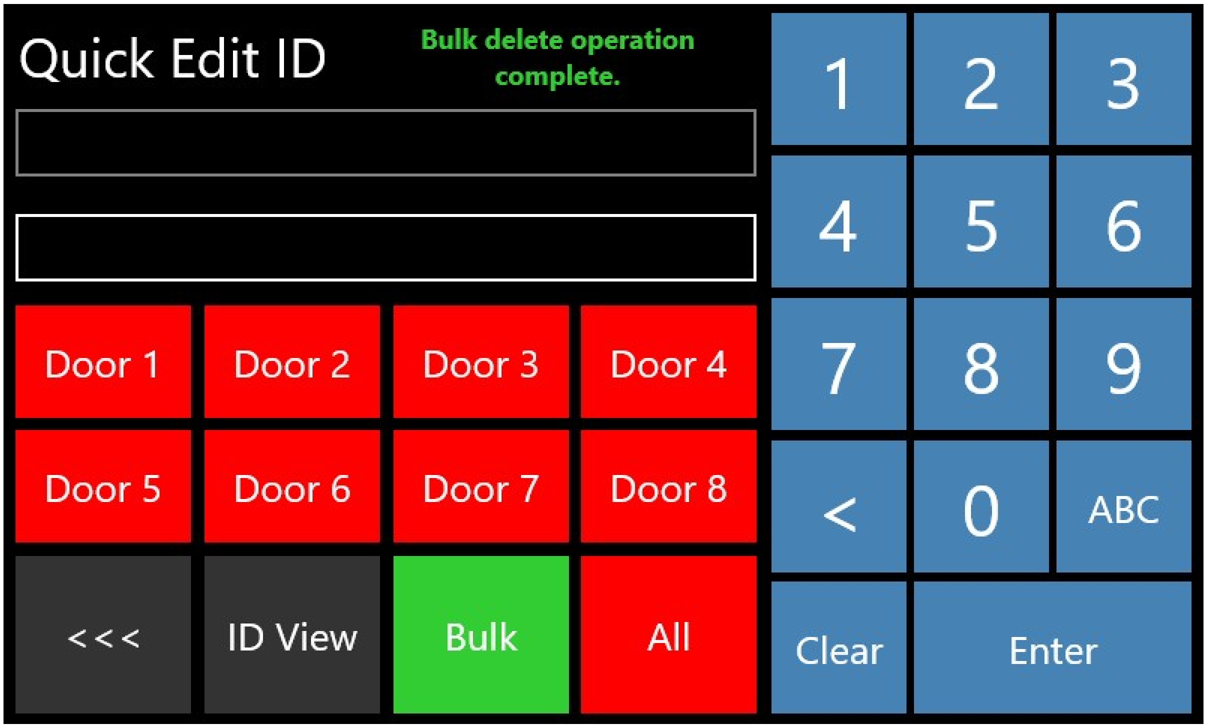
12350

To perform the delete, press the “Enter” key on the keypad. The controller will prompt you with an “Are you sure…” message.



You are bulk deleting cards from number 12345 to 12350. This is a very destructive process. Continue?

If you are sure that you want to perform the delete, click “Bulk Delete” on this prompt and the bulk delete process quickly deletes the range of cards from all the doors.

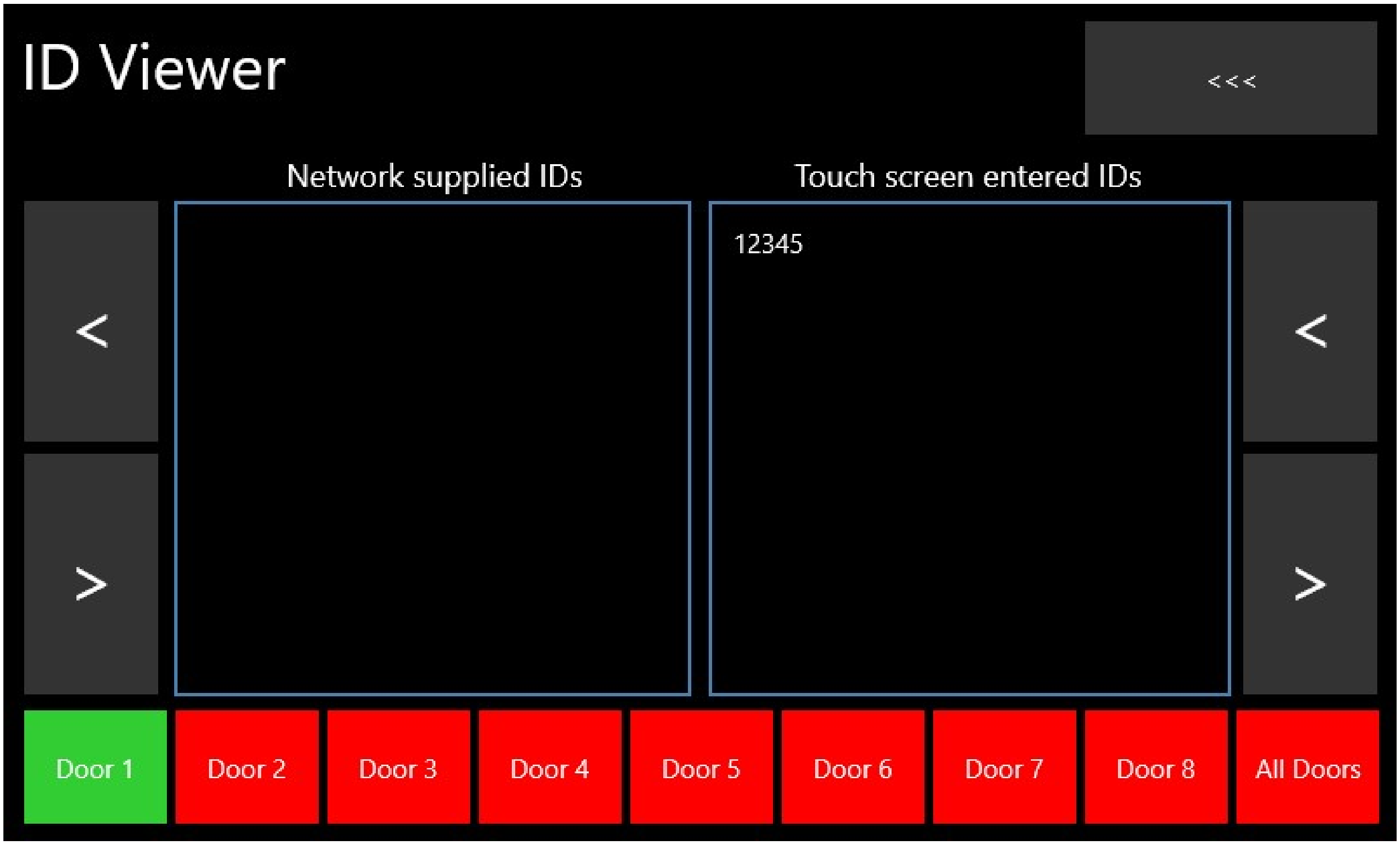


Quick Edit ID

Bulk delete operation complete.

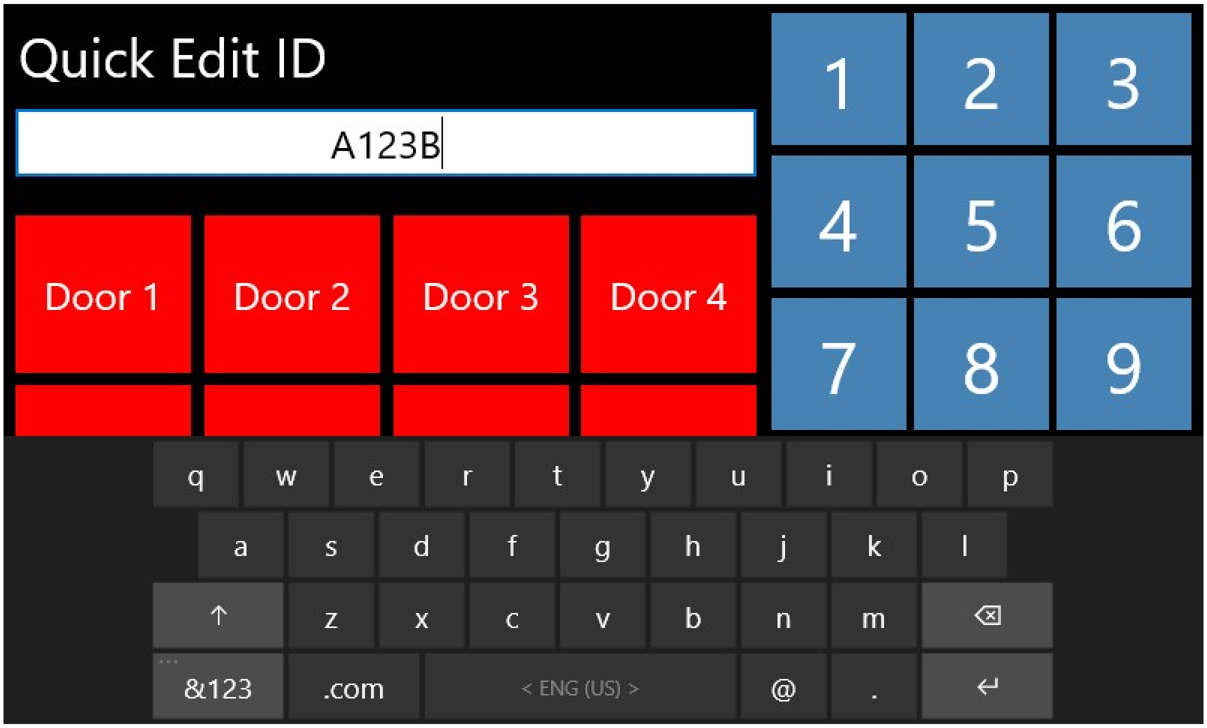
ID Viewer

The ID View button activates the ID Viewer facility that allows you to view all of the current IDs that are in memory for a certain reader or for multiple readers. See further information on this facility in the Advanced Features section of this manual.



Alphanumeric code entry

Alphanumeric code entry has been disabled in this current version of the firmware. Read below about the implementation for future support.



Quick Edit ID

A123B

Alphanumeric code entry is available on the Quick Edit ID screen for future use. Version 1.0 of the controller does not have a reader interface that can support alphanumeric cards but future support for magstripe Track I character set is planned as well as other types of reader interfaces. As a result, you can enter cards that are alphanumeric...there is just no way at this time to connect a reader to the controller that can send the alphanumeric information.

In the single card enroll or delete modes, you can click on the card ID text box at the top of the screen; a full keyboard will come up allowing you to add alphanumeric data. Alternatively, you can press the “ABC” button on the blue keypad to enter this alpha mode. To dismiss the keyboard, tap on some other part of the screen that has free space.

During bulk operations, the alphanumeric entry mode is not available.

Advanced Edit ID

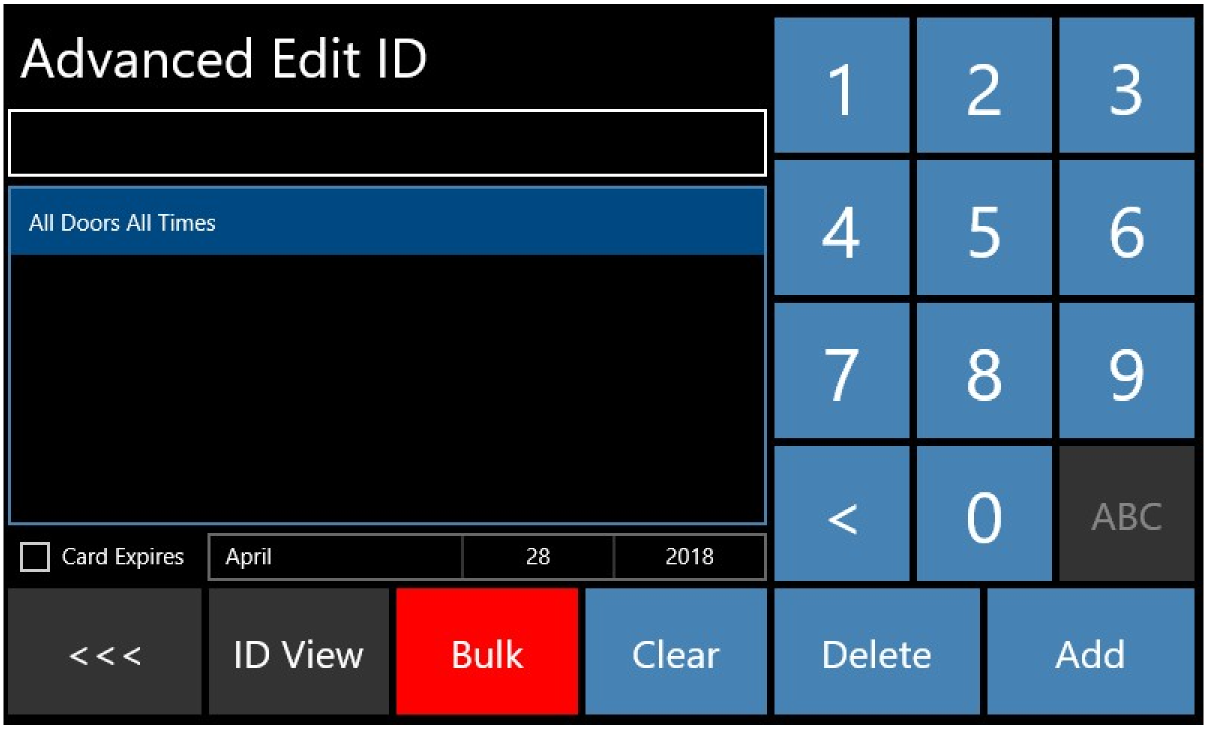
The Advanced Edit screen of the controller is used to add, delete, bulk enroll, or bulk delete card ID numbers by placing the cards into memory based on access levels. **The access levels in the controller are defined by the user before using the advanced edit features**. An access level defines what card should be running on what door, using schedules to control access times.

There is one access level on the controller that is pre-defined, called “All Doors All Times” Using this level, the advanced edit feature works in a similar manner to the Quick Edit ID screen. As you add levels to the controller, they will be available in this screen for use. The advanced edit screen will not only allow you to apply an access level to a card but will also allow you to set up card expiration dates. Card expiration dates prevent the card from working after a particular date if you choose to apply this property to the card ID.

The schedules and access levels are added to the controller using the “Advanced Features” function of the controller. Advanced Features functions are defined later in this manual.

Adding a single card ID

To use the Advanced Edit ID screen, **access levels must be configured beforehand**. Access levels are collections of schedules over doors that tells the system what times it should accept a particular card. There is a default access level defined in the system called “All Doors All Times” that cannot be deleted, but it can be used in the same manner as a user defined access level. If you decide to put the card on the All Doors All Times level, the card will be added to memory with the same result as using the Quick Edit ID screen.



Advanced Edit ID

All Doors All Times

□ Card Expires April 28 2018

The advantage to using the Advanced edit screen is to use access levels to specify easily what doors the card runs on by schedule and that you can also set the card expiration date with Advanced Edit ID.

The Card Expiration date feature can be used with the All Doors All Times feature or any user defined access level. With the Card Expiration feature, you can check a box that makes the card completely stop operating after a particular calendar date. Before that date, the card runs on its selected schedule. The Card Expiration date feature is optional, and it will only be applied to a particular card number if the “Card Expires” checkbox is selected.

To add a card with this screen, use the blue keypad at the right of the screen to enter the card number info the Advanced Edit ID text box. If you make a mistake, use the “<” key to delete the last digit.

Once the card number has been entered, underneath the card number, scroll through the available access levels that you want to place the card on. The access level must be predefined using the Advanced Features screen. The access level will tell the system when the card is expected to work on a particular door at a particular day of the week and time of the day.

Once you select the access level, choose if the card is to expire. If the card is to stop working after a certain date, select the “Card Expires” checkbox and then tap on the date next to the checkbox to set the expiration date.

Once you have all parameters configured, select the “Add” button and the card is added to memory based on the settings in the access level. The expiration date if used is also recorded in the card record. You should get a confirmation message at the top of the screen that the card was added to memory.

If after adding the card using the Advanced Edit screen, the card does not work on the reader, check the main screen records to make sure that the schedule and holiday considerations are met according to the time when the card was presented.

Deleting a single card ID

You can delete a single card ID in the Advanced Edit ID screen without selecting Access Levels or expiration dates. To delete a card, simply enter the card number using the blue keyboard at the right and then tap the “Delete” button found at the bottom of the keypad. The controller will ask you to confirm that the card is to be deleted from memory. You can also delete a card using the Quick Edit ID screen in a similar way. Deleting a card from either screen is the same action in the controller.

Alphanumeric code entry

Alphanumeric code entry is available on the Advanced Edit ID screen for future use. Version 1.0 of the controller does not have a reader interface that can support alphanumeric cards but future support for magstripe Track I character set is planned as well as other types of reader interfaces. As a result, you can enter cards that are alphanumeric...there is just no way at this time to connect a reader to the controller that can send the alphanumeric information.

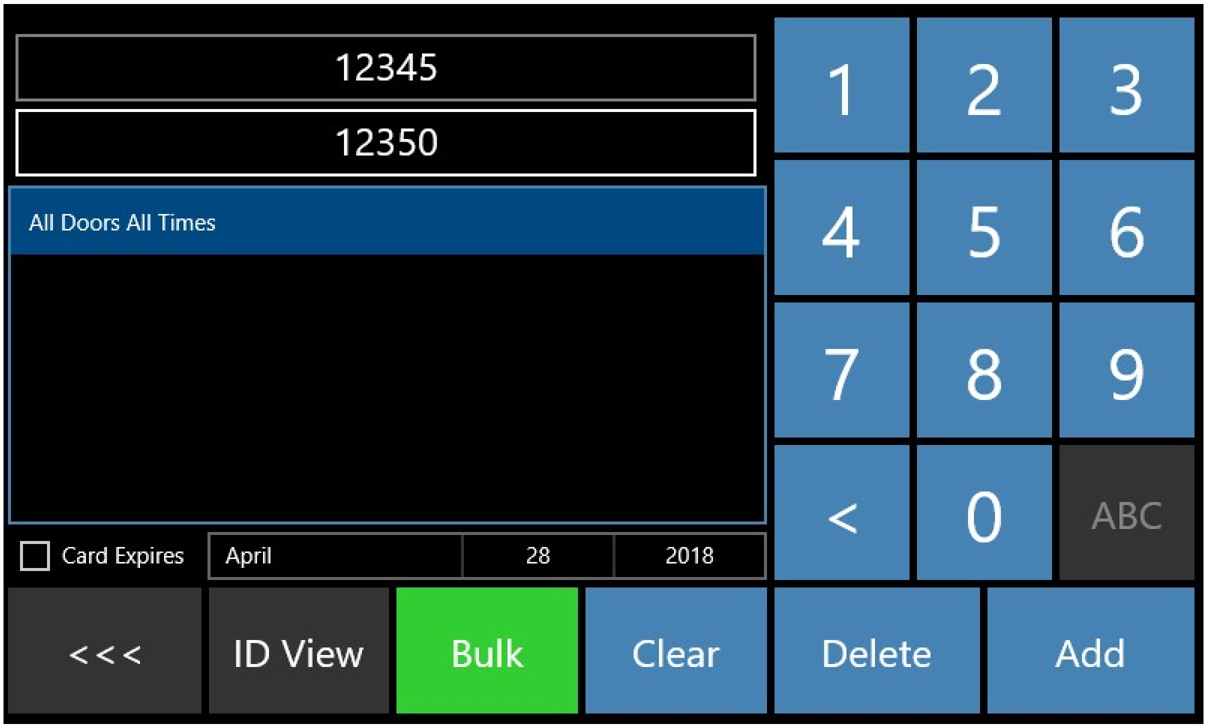
In the single card enroll or delete modes, you can click on the card ID text box at the top of the screen; a full keyboard will come up allowing you to add alphanumeric data. Alternatively, you can press the “ABC” button on the blue keypad to enter this alpha mode. To dismiss the keyboard, tap on some other part of the screen that has free space.

If the on-screen keyboard is too small or a problem to use you can also use a physical USB keyboard plugged the keyboard into one of the controller's USB ports in place of the on-screen keyboard. This is also true using a USB mouse, as plugging in a mouse will create a pointer to do the same functions as tapping on screen.

During bulk operations, the alphanumeric entry mode is not available.

Bulk enrolling a range of card IDs

If you have a set of cards that are in sequence, you can bulk enroll all of them in one action. Press on the “Bulk” button at the bottom of the screen and it will turn from red from green indicating the Bulk mode is enabled. The heading at the top of the screen will also be replaced by a second card entry field. If you tap on the first field, you can then use the keyboard to enter the starting number in the sequence. After entering this number, tap on the second card field just below the first. Then enter the ending card number in the second text box using the keypad. The text box that is active for input at a particular time will be outlined with a white border while the inactive text box border will be grey in color.



12345

12350

All Doors All Times

□ Card Expires April 28 2018

Once the card range is entered, select what access level the cards are to run on and if all of the cards in the range should expire using the “Card Expires” feature in a similar way to enrolling a single card. Once all of these options are set, press the “Add” button and you will be prompted to make sure that you meant to do the bulk enroll. If everything is OK, select “Bulk Enroll” at the prompt and all cards in the sequence are added to memory on the specified access level. If the card expiration feature was used, all cards enrolled will also have an expiration date.

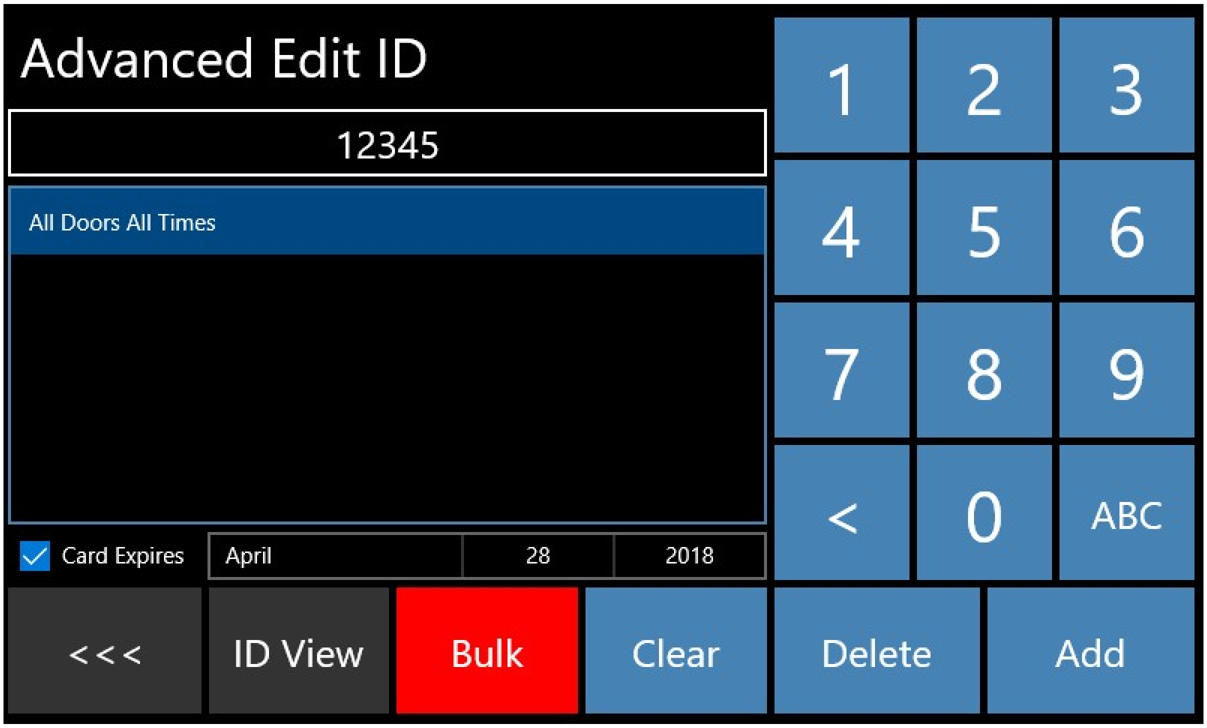
Note: If you add a leading zero to the card ID in the first entry box, the controller will add leading zeros to all IDs that are enrolled. The card ID with leading zeros is a different ID than one without. For example, card ID “001” is different than card ID “1”.

Bulk deleting a range of card IDs

Bulk deleting a range of card IDs happens in a similar manner as deleting a single card. Tap on the “Bulk” button and supply the starting and ending numbers in the range to be deleted. You do not have to be concerned with the access levels or expiration date settings during a deletion. One you supply the card ID number range, press the “Delete” key at the bottom of the blue keyboard. You will be presented with an “Are you sure…” message. If you are sure, select “Bulk Delete” at the prompt and the range of cards is deleted from memory. This is the same action that occurs when you bulk delete from the Quick Edit ID screen.

Card Expiration Dates

While adding a single card or bulk enrolling a range of card IDs, if you select the checkbox for “Card Expires” the card will no longer function in the system after a particular date.



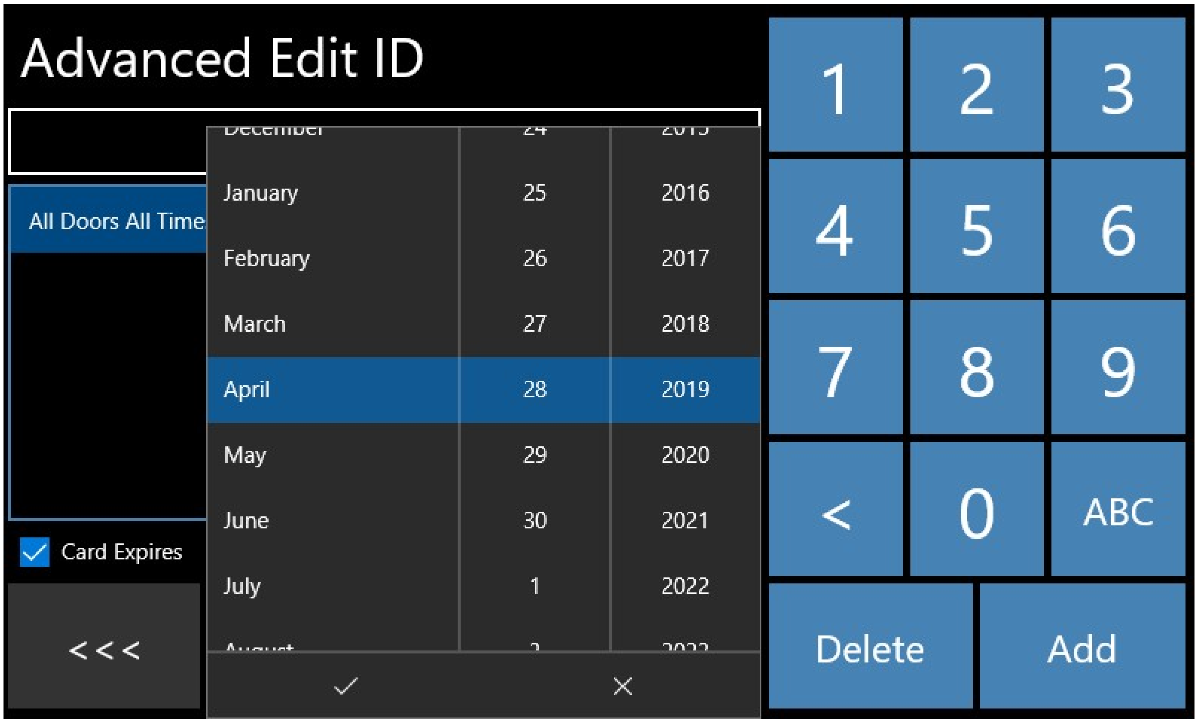
Advanced Edit ID

12345

All Doors All Times

☑ Card Expires April 28 2018

When you use this feature, you will have to supply the date of expiration. Tapping on the field to the right of the “Card Expires” checkbox brings up a date selection window. Use this window to specify the date of expiration.



Advanced Edit ID

All Doors All Time

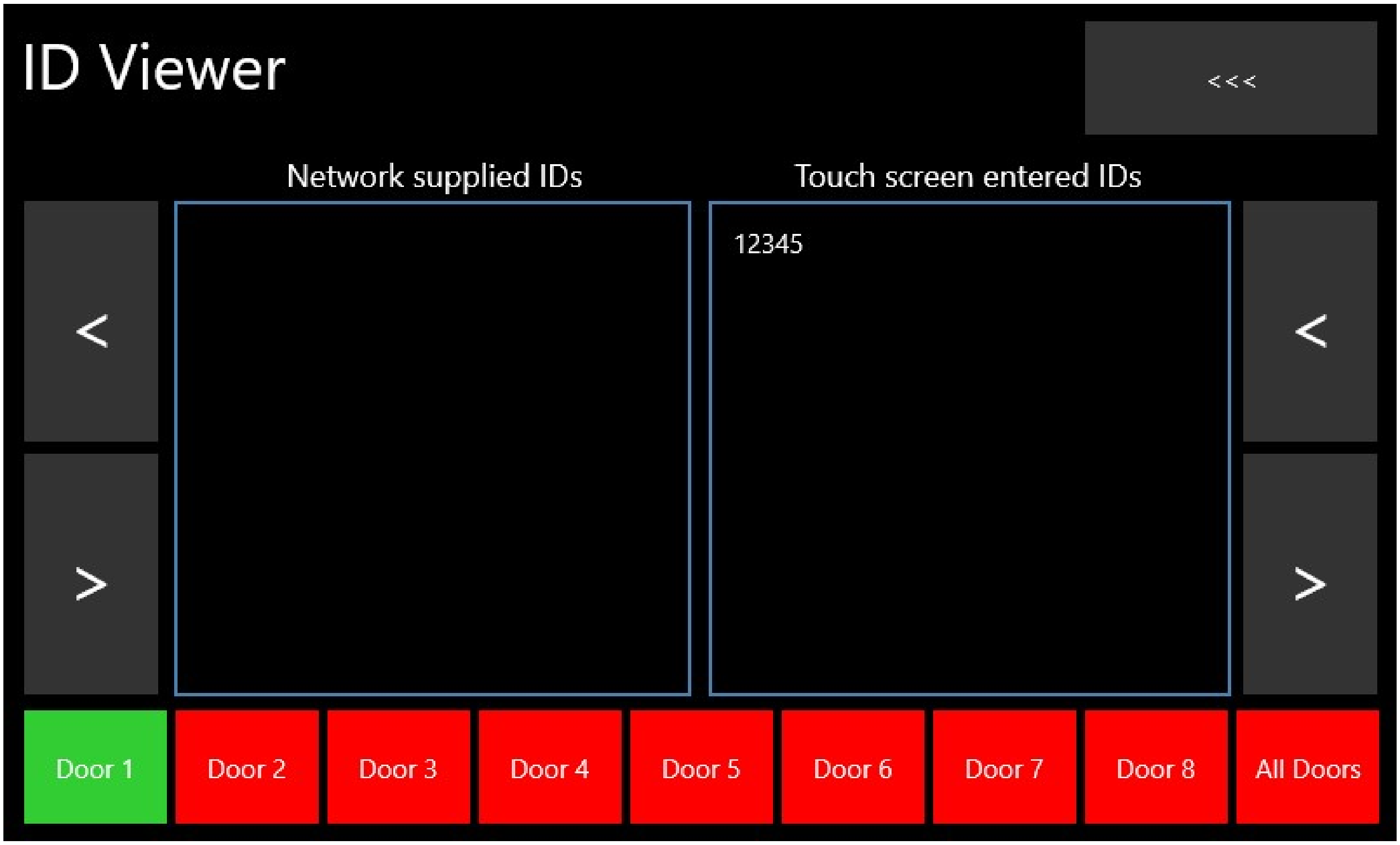
☑ Card Expires

April 28 2019

Once the card ID or range of IDs are enrolled, the card expiration date becomes part of their stored records. Once this date is reached, the card will not function. If you wish to get it functioning again, you need to delete and then re-enroll the card at a later date. Future updates to the controller have plans for editing the expiration date of a card record, but this is not included in Version 1.0 of the firmware at the time of writing this manual.

ID Viewer

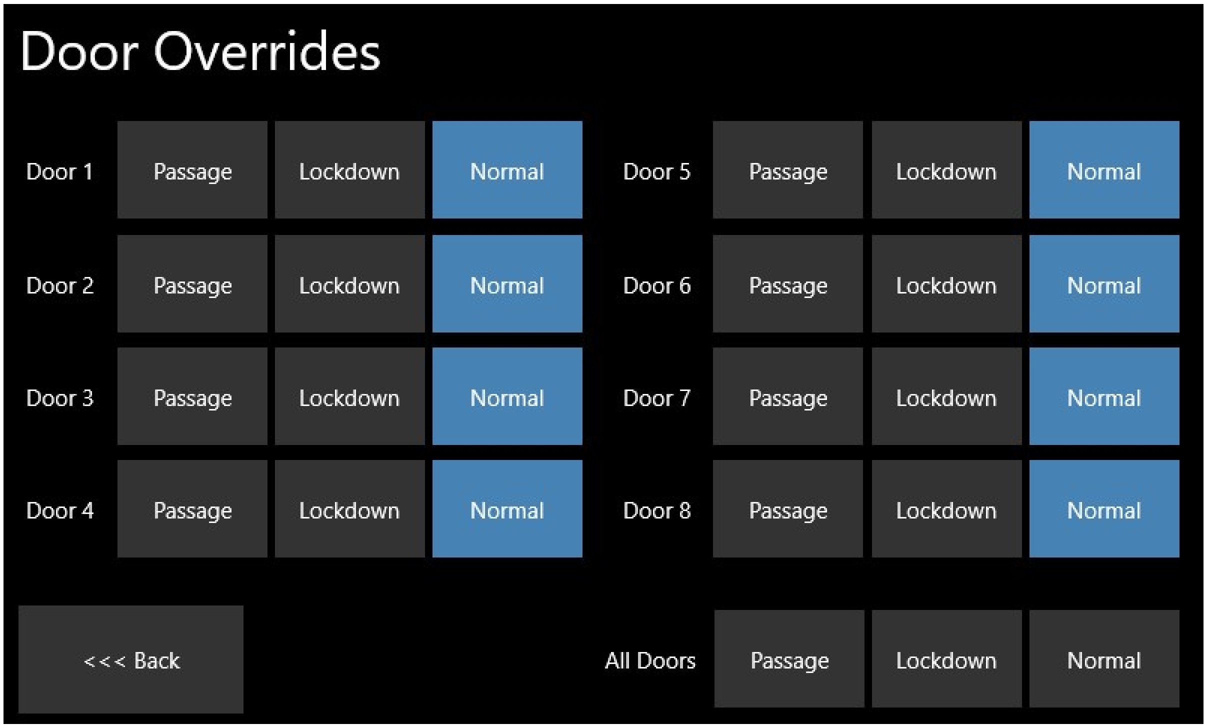
The ID View button activates the ID Viewer facility that allows you to view all of the current IDs that are in memory for a certain reader or for multiple readers. See further information on this facility in the Advanced Features section of this manual.



12345

Door Overrides

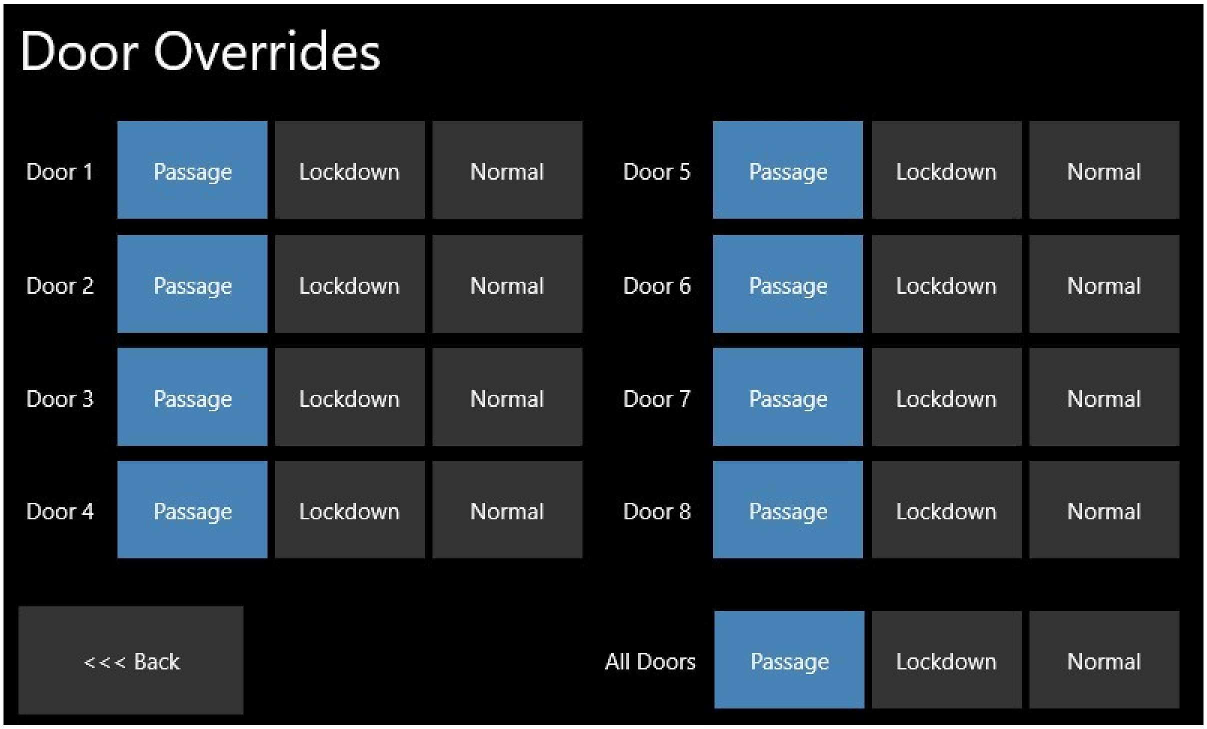
The door overrides screen is used during both diagnostics and emergency situations. With this screen you can quickly place the doors into passage mode, lockdown mode and normal operation mode.



Passage mode forces a door to be unlocked during all times. Lockdown forces a door to be locked during all times and conditions. Normal door operation modes allow the door to lock and unlock on schedule and allows for card access during times when the door is locked, if the card access schedule allows.

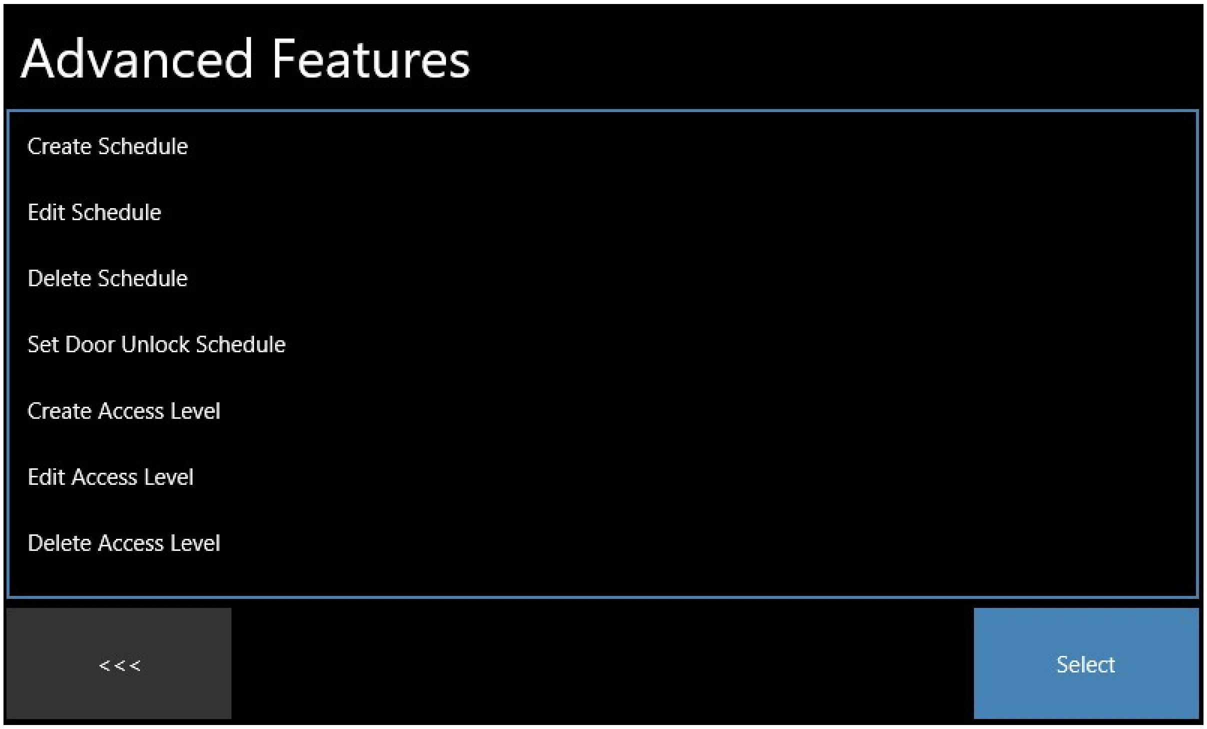
During initial setup the installer can use this screen to test the locking hardware without presenting a valid card. In an emergency, you can force the doors locked or unlocked based on the situation.

In addition to controlling doors individually, there is a set of buttons in this screen that can control all doors simultaneously. These buttons are labelled with the “All Doors” label and are found at the bottom right of the screen. Pressing one of the modes in All Doors will cause a simultaneous state change of all of the doors.



Advanced Features

The advanced features screen allows the programmer to access more sophisticated features if needed.



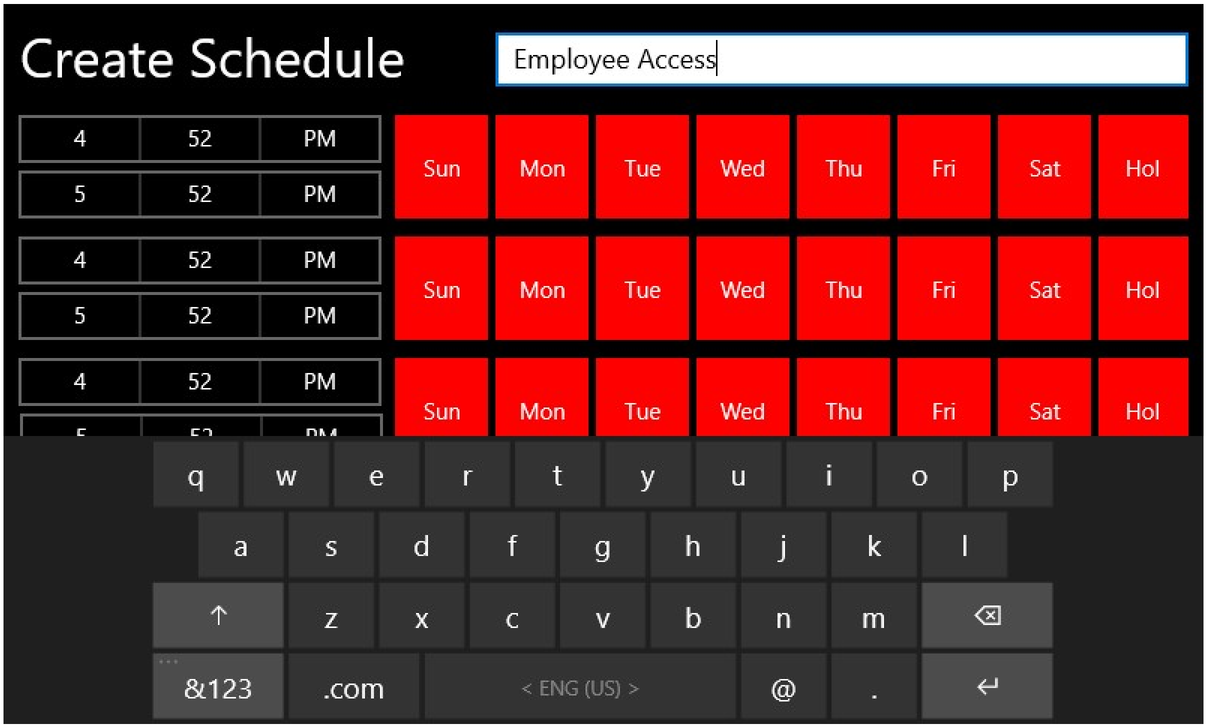
These include creating and deleting schedules, creating and deleting access levels, creating and deleting holidays, accessing detailed controller card format functions, setting up automatic door unlocking on schedule and accessing features that work with a USB memory stick. In the Advanced Features screen, you scroll through the features list with your finger and then select the feature that you are interested in by tapping the feature name. Once you select the appropriate feature in the list, hit the “Select” button at the bottom right of the screen to move to that features specific screen.

Create Schedule

Schedules have a dual use. They can be used both for setting up automatic door unlocking and can also be used in access levels to control when a card has access to a certain door. You can make as many schedules as you need, using them for either function.

To create a schedule, first name the schedule by clicking on the top text box. This is an unlabeled box at the upper right of the screen. Once you click this box, the on-screen keyboard will pop up from the bottom and allow you to enter the name of the schedule. It’s recommended that you name schedules things like “Front Door Unlocking” or “Employee Access Times” ...etc. Name the schedule something descriptive that is appropriate for the application.

If the on-screen keyboard is too small or a problem to use you can alternatively use a physical USB keyboard plugged into one of the controller's USB ports, in place of the on-screen keyboard. This is also true using a USB mouse, as plugging in a mouse will create a pointer to do the same functions as tapping on screen.


Create Schedule

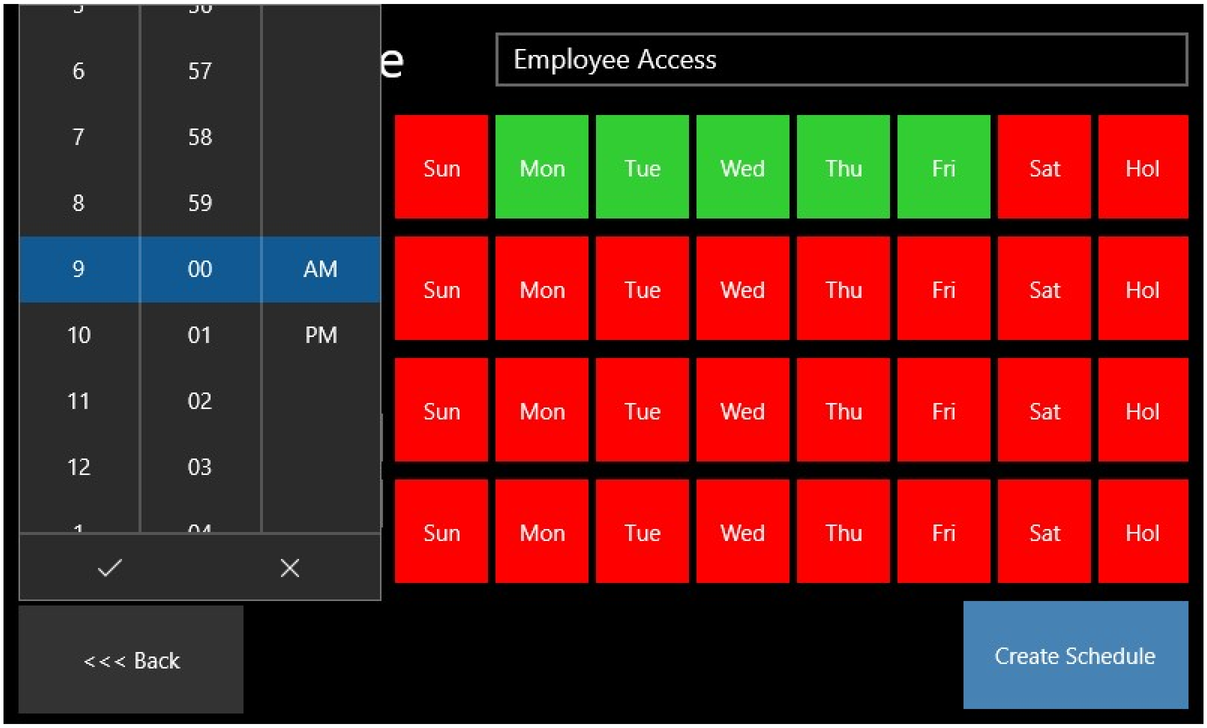
Employee Access

4	52	PM	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol
5	52	PM								
4	52	PM	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol
5	52	PM								
4	52	PM	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol
5	52	PM								

Once you name the schedule, tap somewhere on the screen where there is free space to retract the keyboard. Tapping on the “Create Schedule” screen title up top is a good spot.

In each horizontal row, there are two times, days of the week buttons and a holiday button. Each horizontal row is a separate period in a schedule. When programming the controller with the touch screen there are four periods per schedule available. When adding schedules with the Highpower HMS software, there are eight periods per schedule available.

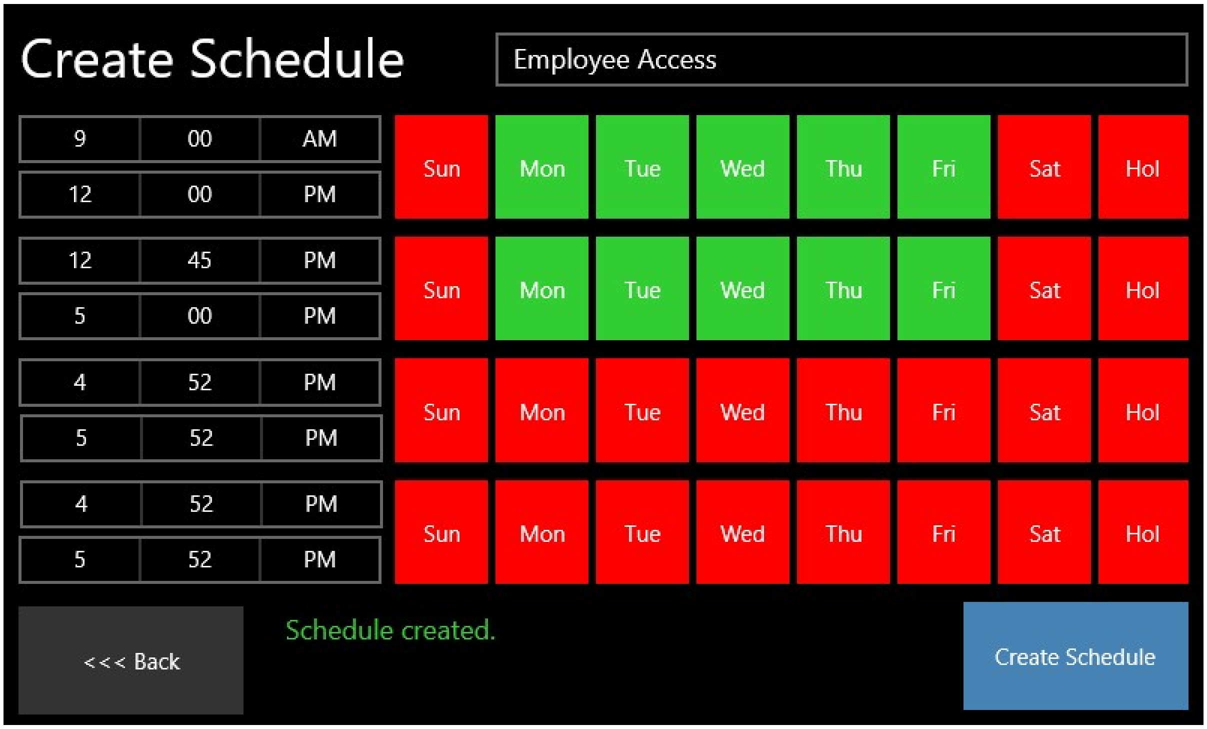
The starting time of a period is the top time entry in each row. The ending time of a period is the lower time entry in each row. The start and end times in each period are set by tapping each time box, which causes a time selection window to show.



	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol
1	🟥	🟩	🟩	🟩	🟩	🟩	🟥	🟥
2	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
3	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
4	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

Set the start and end times so that the start time occurs before the end time for each period. For each period, you select the days of the week that the time intervals are active for. All the day buttons are initially red in color (disabled). By tapping on a specific day, the button toggles to green, which indicates that the day for that period is selected. In addition to the day, the last column of buttons is for holidays. During times when holidays are active, the schedule jumps out of the time zone programmed for a certain day and runs on time zones that are programmed for holidays. You can think of a holiday as an eighth day of the week.

An example of a typical schedule is programmed below:



Create Schedule

Employee Access

	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol
9 00 AM 12 00 PM	🟥	🟩	🟩	🟩	🟩	🟩	🟥	🟥
12 45 PM 5 00 PM	🟥	🟩	🟩	🟩	🟩	🟩	🟥	🟥
4 52 PM 5 52 PM	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
4 52 PM 5 52 PM	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

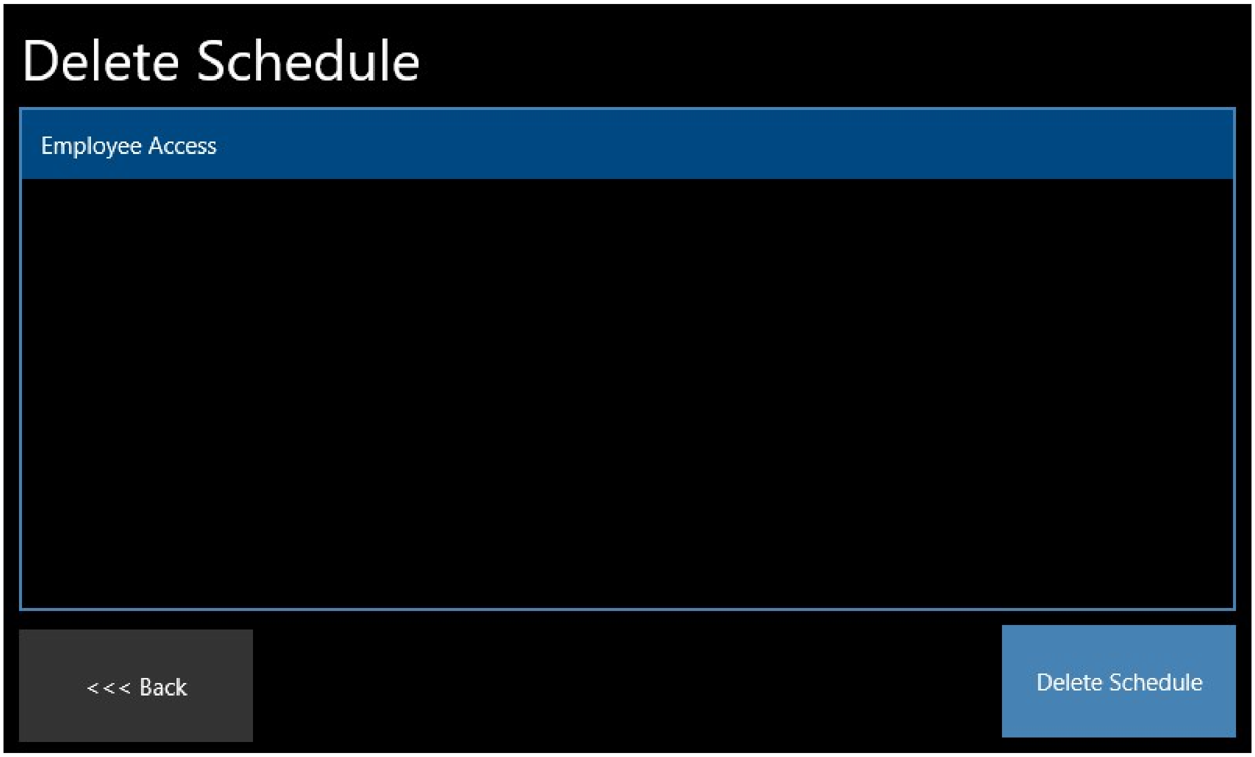
Schedule created.

In this schedule example we are attempting to create a schedule for a simple work day., The start of the first period is 9:00am and ends at 12:00PM to prevent access during lunch hours. These times are valid from Monday-Friday during the workweek. After the first period, we take a 45-minute lunch. After lunch, we need to get back into this area, so we set another period up that runs from the end of lunch (12:45p) to quitting time (5:00p). Since we absolutely don't like working holidays, there are no periods set up for a holiday. If we work different hours during holidays, we would set additional periods up for the holidays. If we work holidays on the same time schedule, we could also include the "Hol" button in a typical period.

Edit Schedule

This feature allows you to recall and edit an existing schedule.

Delete Schedule



Delete Schedule

Employee Access

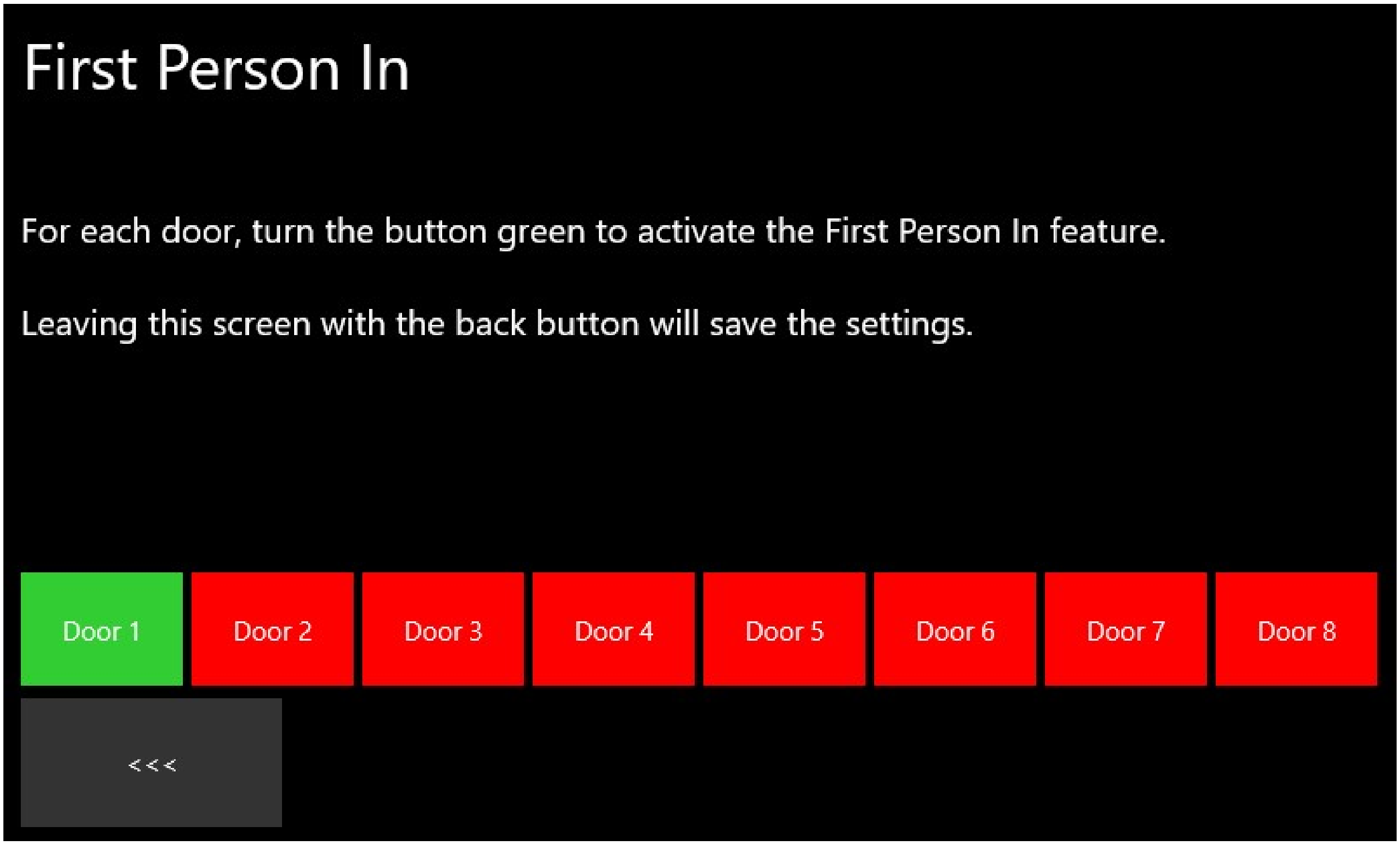
Once a schedule is created, the delete schedule feature allows you to delete it. If the schedule is being used in an access level or as door unlocking schedule, the schedule is deleted and the schedule entry in the access level or door unlocking schedule is changed to "Never".

Set Door Unlock Schedule

Once a schedule is created, you can use the schedule to automatically unlock and relock doors at specific times. After creating the schedules that you need, select one of the schedules for each door. Once selected, the doors will unlock during the scheduled times.

First Person In

The first person in feature is used in conjunction with the automatic door unlocking. With the first person in feature turn on, an unlocking cycle will not start without a valid card swipe.



First Person In

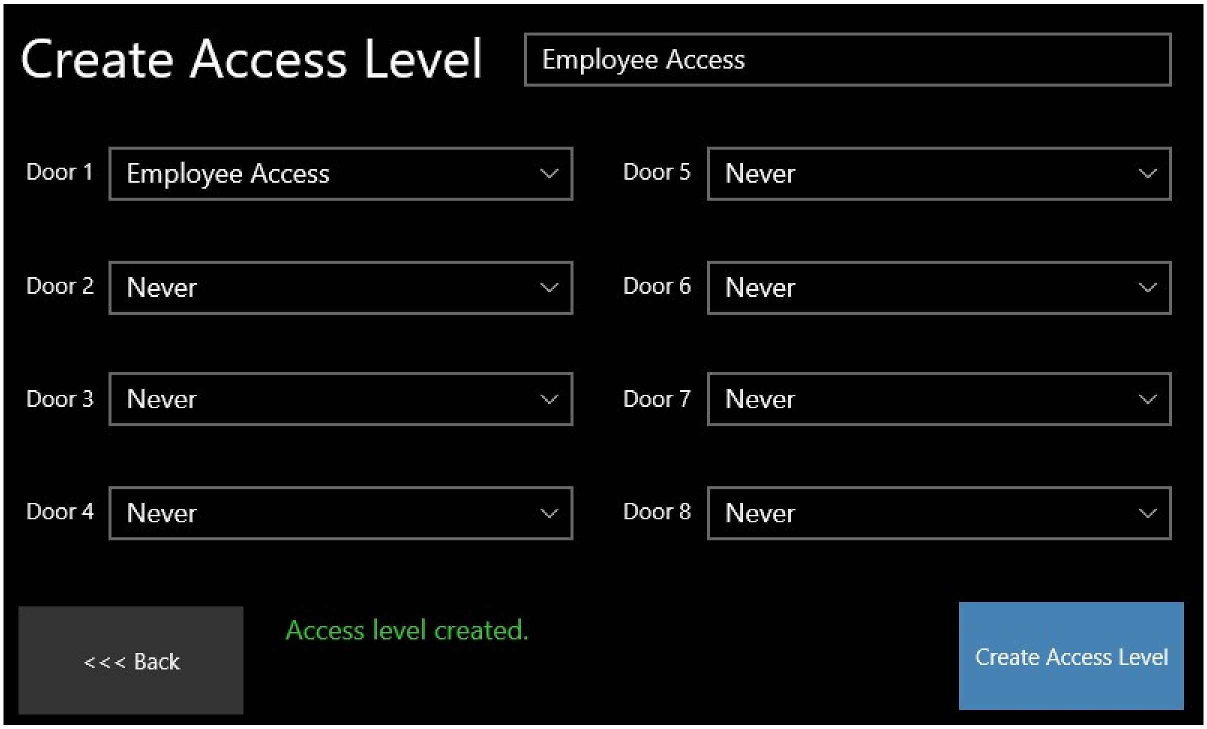
For each door, turn the button green to activate the First Person In feature.

Leaving this screen with the back button will save the settings.

This feature keeps the door locked even though an unlocking interval is occurring, until a valid swipe. It's used to prevent a door from being unlocked at a facility during times when there is no one around and people are delayed for events such as storms, etc. The first person in feature can be turned on or off for each door individually.

Create Access Level

Access levels are used to tell the system when a card has access to a door. Access times of a particular door are controlled by a schedule.



Create Access Level: Employee Access

Door 1: Employee Access

Door 2: Never

Door 3: Never

Door 4: Never

Door 5: Never

Door 6: Never

Door 7: Never

Door 8: Never

Access level created.

In the example above, we are creating an access level to let employees through Door 1. They can only come through Door 1 on the times that are allowed on the “Employee Access” level. The Employee Access level was created before we create the new access level. There are two predefined schedules also available. The “Always” access level means that someone could come through a door at all times. The “Never” access level is the default for each door and means that no one can come through a door.

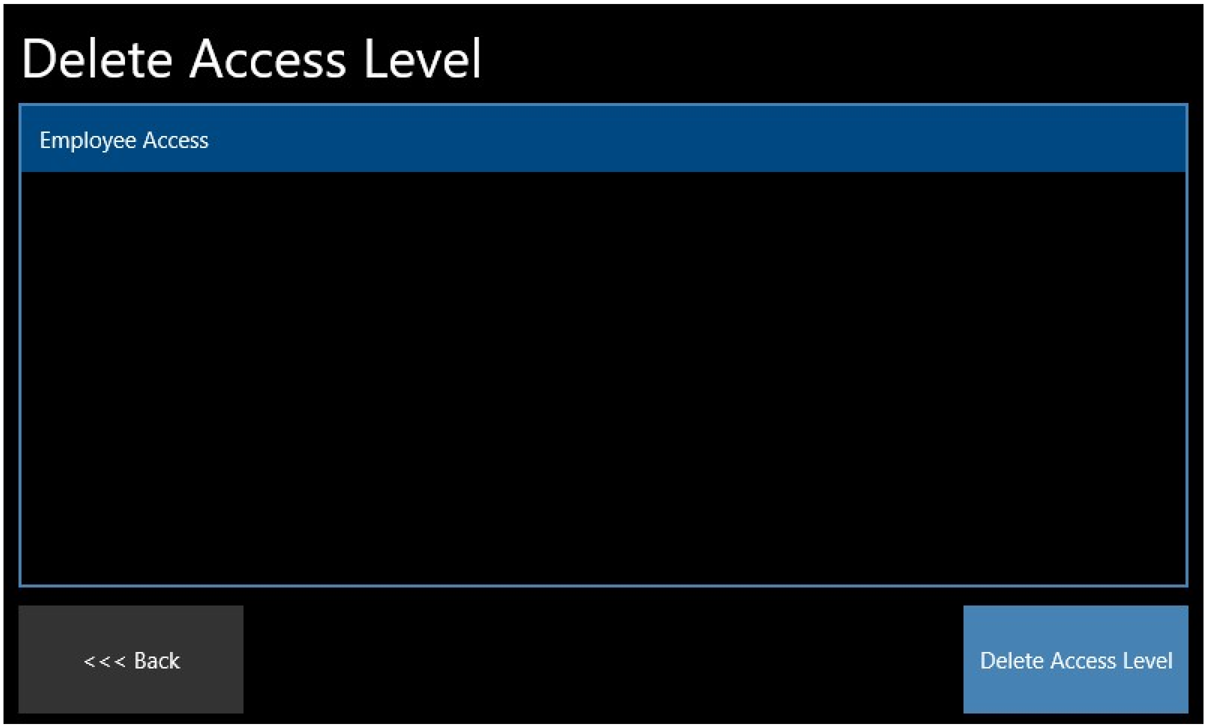
Once you create the access level, you can use the Advanced Edit ID screen to add a card to the system that runs on the access level.

Edit Access Level

This feature allows you to recall and edit an existing access level.

Delete Access Level

Once you create an access level, you may need to later change the system by deleting it. There is a function in the controller that lists all access levels and allows you to select the one that you wish to delete.



Delete Access Level

Employee Access

Holidays

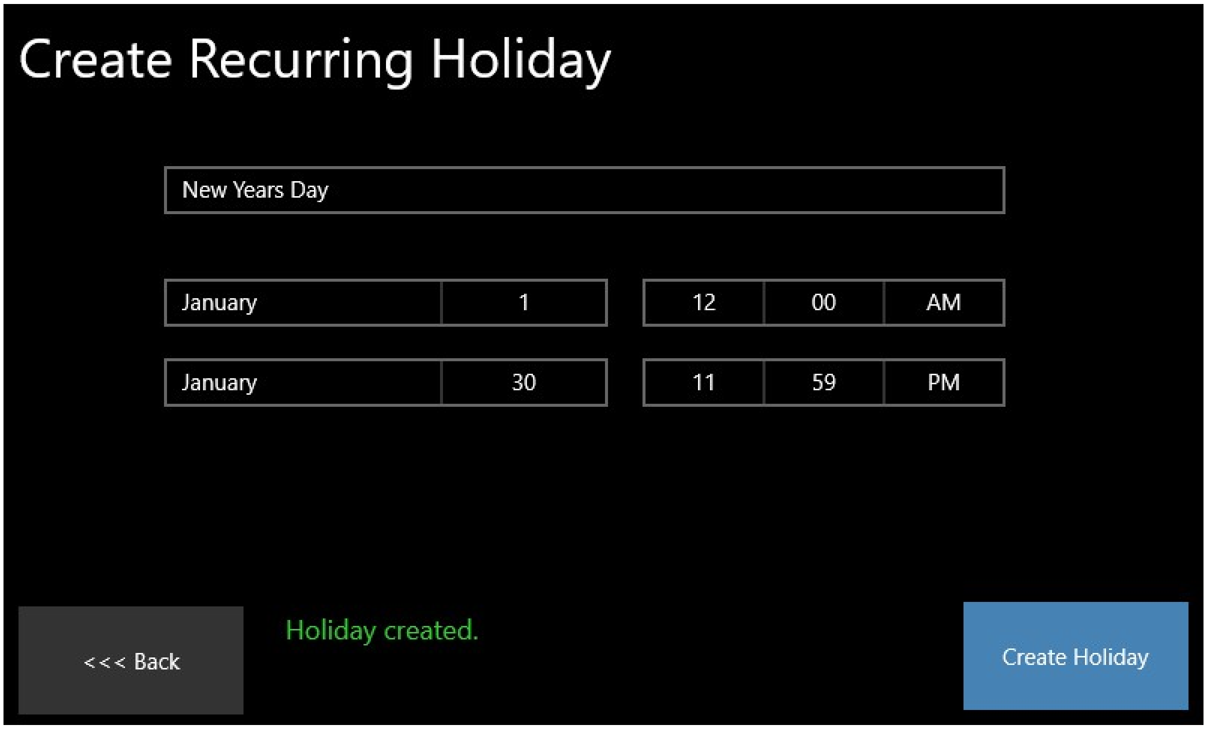
The controller has two types of holidays available. The “recurring holiday” is one that happens on the same calendar date each year. These are holidays like New Year's Day, Christmas, Halloween, etc.

The “non-recurring holiday” is a holiday that is programmed for one date per year and can be things like Labor Day, Easter Sunday or a large business meeting on a certain date.

During a holiday, the controller jumps out of the schedule for a particular day and switches to whatever periods are defined for the “Hol” column in the schedule. This can be thought of as a “day eight” function. If for example, it’s a Tuesday, and we come into a schedule period of either type of schedule, the periods in the schedules defined for Tuesday will no longer run. The periods defined for the “Hol” periods will run. If a period is defined for both a “Tue” and “Hol” columns in this example, then no changes in the Tuesday schedule will occur when a holiday occurs.

Create Recurring Holiday

Recurring holidays are holidays that happen at a certain time, every year.



Create Recurring Holiday

New Years Day

January | 1 | 12 | 00 | AM

January | 30 | 11 | 59 | PM

Holiday created.

Set the name of the holiday by tapping the name field at the top of the recurring holiday screen. This will bring up the on-screen keyboard. You can also use a physical keyboard plugged into a USB port. The holiday name is used just to reference the holiday for deletion in the future. Once you name the holiday, select the month and day of the start of the holiday period. Then to the right of the month and day, set the start time during that day when the holiday period begins.

Just below the first starting time, repeat the process for the ending month, date and time indicating the end of the holiday period. Once you enter this information, select the “Create Holiday” button at the lower left and you should see a confirmation at the bottom of the screen in green saying, “Holiday created.”

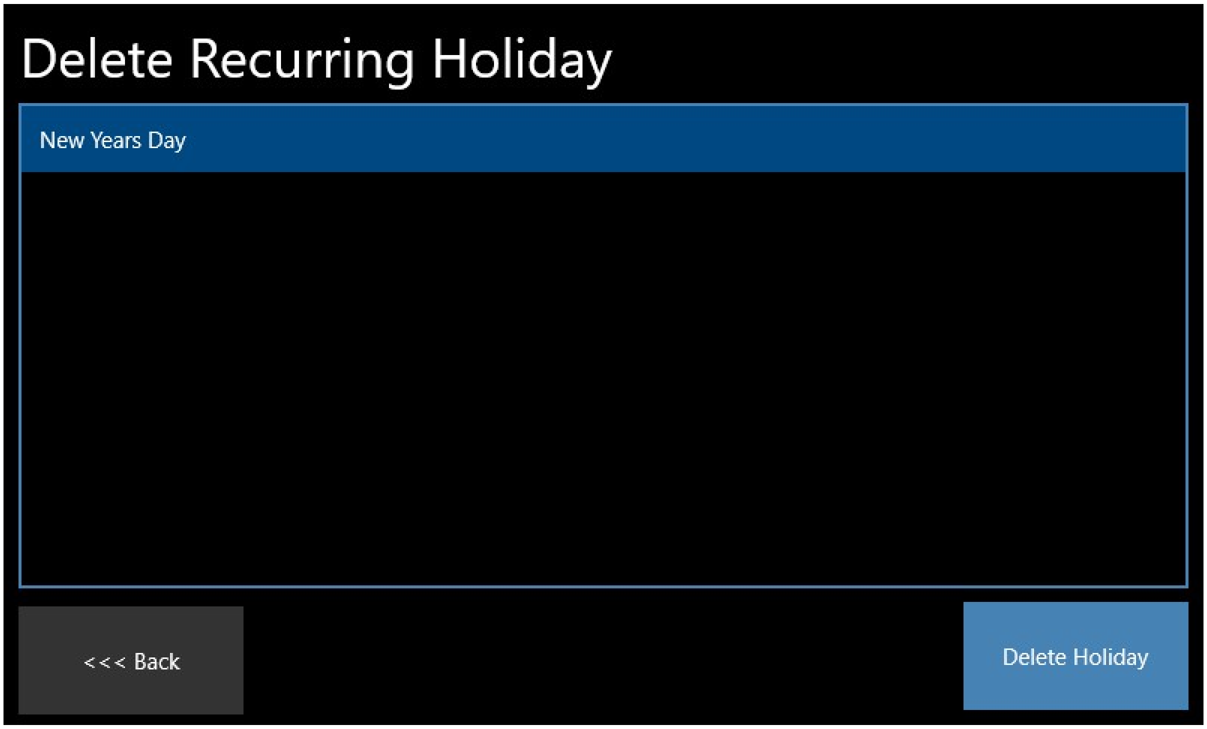
The information for the holiday is maintained so that you can enter a second holiday based on the information from the one that was already created. If you are completed entering all the holidays use the “<<< Back” button to return to the Advanced Features screen.

Because this type of holiday is recurring each year on the same date, the year of the holiday does not have to be provided. During a holiday, the periods in all schedules will shift from the current day to any periods that are defined for the holiday “Hol” column in the schedule.

Edit Recurring Holiday

This feature allows you to recall and edit an existing recurring holiday.

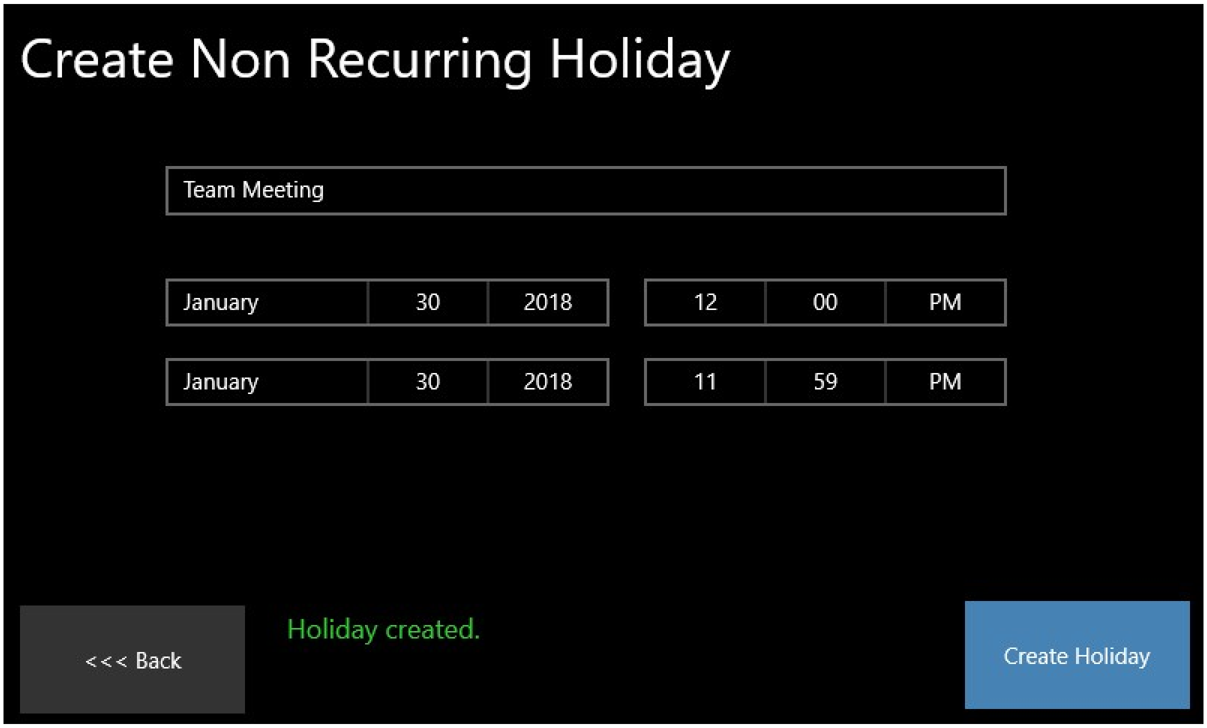
Delete Recurring Holiday



This facility allows you to delete a created holiday in the case where the holiday is no longer used. Select the holiday from the list of all recurring holidays and select “Delete Holiday” key at the bottom of the screen. You should get an “Are you sure…” prompt to make sure that you are deleting the correct holiday. If you are sure, then confirm to complete the deletion.

Create Non-Recurring Holiday

Non-recurring holidays are holidays that do not occur every year, but only happen at a particular date and time each year.



Create Non Recurring Holiday

Team Meeting

January	30	2018	12	00	PM
January	30	2018	11	59	PM

Holiday created.

Set the name of the holiday by tapping the name field at the top of the recurring holiday screen. This will bring up the on-screen keyboard. You can also use a physical keyboard plugged into a USB port. The holiday name is used just to reference the holiday for deletion in the future. Once you name the holiday, select the month, day and year of the start of the holiday period. Then to the right of the month, day and year, set the start time during that day when the holiday period begins.

Just below the first starting time, repeat the process for the ending month, date, year and time indicating the end of the holiday period. Once you enter this information, select the “Create Holiday” button at the lower left and you should see a confirmation at the bottom of the screen in green saying, “Holiday created.”

The information for the holiday is maintained so that you can enter a second holiday based on the information from the one that was already created. If you are completed entering all of the holidays use the “<<< Back” button to return to the Advanced Features screen.

Because this type of holiday is recurring each year on the same date, the year of the holiday does not have to be provided. During a holiday, the periods in all schedules will shift from the current day to any periods that are defined for the holiday “Hol” column in the schedule.

Edit Non-recurring Holiday

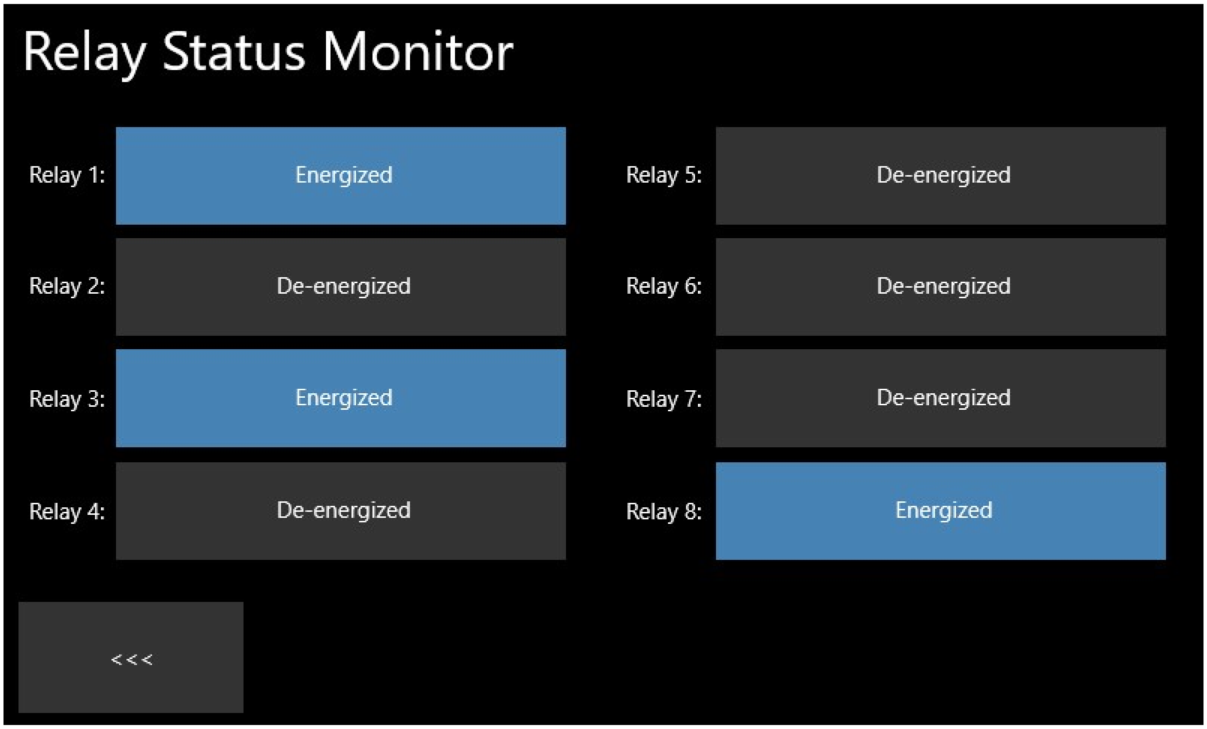
This feature allows you to recall and edit an existing non-recurring holiday.

Delete Non-Recurring Holiday

This facility allows you to delete a created holiday in the case where the holiday is no longer used. Select the holiday from the list of all non-recurring holidays and select “Delete Holiday” key at the bottom of the screen. You should get an “Are you sure…” prompt to make sure that you are deleting the correct holiday. If you are sure, then confirm to complete the deletion.

Relay Status Monitor

This facility allows you to monitor the status of each relay. Each relay state is marked as either “Energized” or “De-energized” based on its current state. The state of the relay changes during card actions, unlocking schedule occurrences, and manual door overrides.



Relay Status Monitor

Relay 1: Energized

Relay 2: De-energized

Relay 3: Energized

Relay 4: De-energized

Relay 5: De-energized

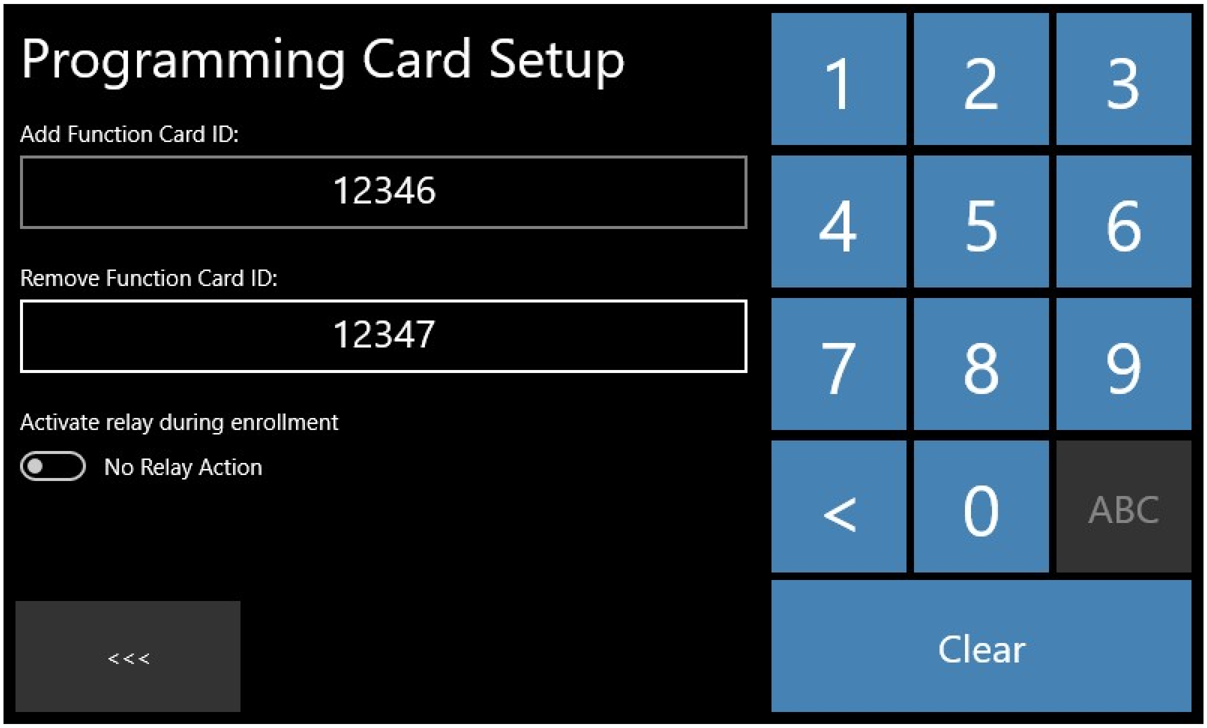
Relay 6: De-energized

Relay 7: De-energized

Relay 8: Energized

Programming Card Configuration

The One can add and remove cards via the reader without interaction with the touchscreen or software. This facility allows you to specify two cards that can be used to trigger open enrollment and card removal functions. After an “open enrollment” card is swiped on a reader, the reader goes into open enrollment mode. The open enrollment mode adds every other card swiped subsequently to be added to memory on the All Times schedule until a programming card is again swiped. If you swipe the specified “Remove Function” card, subsequent cards swiped in that mode get removed from memory until a programming card is swiped.



Programming Card Setup

Add Function Card ID: 12346

Remove Function Card ID: 12347

Activate relay during enrollment

○ No Relay Action

During open enrollment mode, you can tell the controller to activate the relay every time a card is added. This simulates a valid card swipe situation and allows the door to operate normally during the card collection process. To turn this feature on, change the state of the “Activate relay during enrollment” switch “RTE with Enrollment”.

Copy Data Files to USB

If you wish to make a backup of all your settings and access control data, you can back up the controller using a USB memory stick. Place the USB memory stick into a USB slot at the bottom of the controller. Selecting this feature will prompt you with a “Are you sure…” message. You want to make sure that there are no previous files on the card that contain settings you might need as the files will be overwritten. Once you confirm that it’s OK to write files, the controller will copy all its system setting files to the USB memory stick. You can put the USB stick into any of the available USB lots. If you put two USB sticks into the controller, the controller will select only one of the sticks based on USB slot priority so please make sure that you only present one memory stick at a time for this function. You can also use this feature to duplicate a system setup on multiple controllers.

Copy Data Files from USB

If you have made a backup of your system files to a USB stick, you can restore your settings from the stick back to the on-board memory of the controller. Be careful using this feature as it will overwrite all of the settings on the controller with the settings from the USB memory stick. Insert a single USB memory stick into any of the available USB slots. When you select this feature, you will be presented with an “Are you sure…” message prompting you to overwrite the existing setup. If you select “Overwrite” at the prompt the restore operation to the controller is completed.

Clear USB Device

This small feature clears all of the files off of your USB device on the main directory of the device. Use this feature carefully as data loss can occur.

Audit Trail Report to USB Device

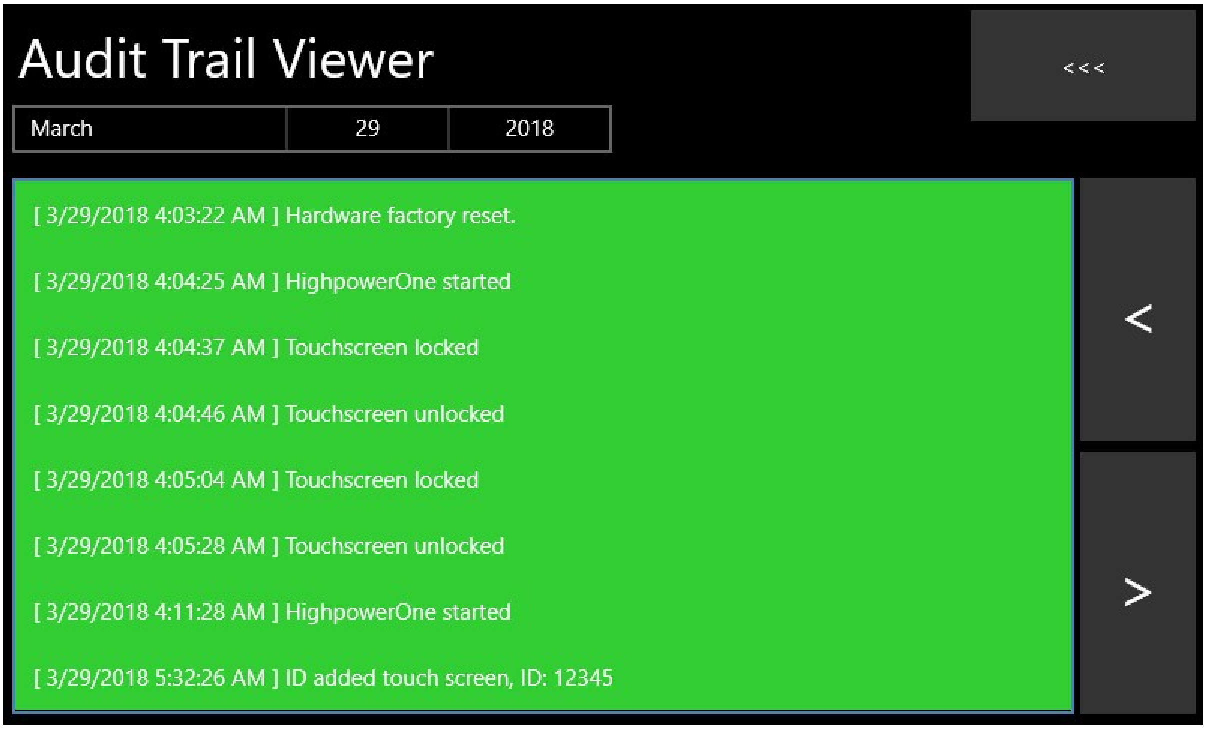
This feature will generate a comma separated value file (CSV) that can be opened in a spreadsheet like Excel, OpenOffice or Google Sheets. This file will contain the audit trail information that is present on the controller. This information is everything that is currently stored in the log including card swipes, schedule changes and other actions. To generate the file, plug in a memory stick to one of the USB connections. Once you trigger this feature, the file will be generated. The file will be on the root folder of the memory stick and will be called *AUDIT.CSV*. Creating this file is not destructive to the log entries, it simply copies the available entries to the CSV file.

If you are using the controller with the Highpower HMS software, the log entries are collected in real time. When the software collects the log entries in real time, the entries are deleted from the hardware as they are collected. The USB log file generation should only be used when the controller is being used in an offline condition as there will be no log entries if the software is collecting them.

When using the controller in an offline condition, the log is programmatically limited to 10,000 entries. Contact the factory if 10,000 entries are not sufficient for your application.

Audit Trail Viewer

The audit trail viewer allows you to review audit trail entries on the screen for a certain day. You can alternatively download the audit trail using a USB memory stick (using the procedure in the previous section) or via software using the HMS software package.



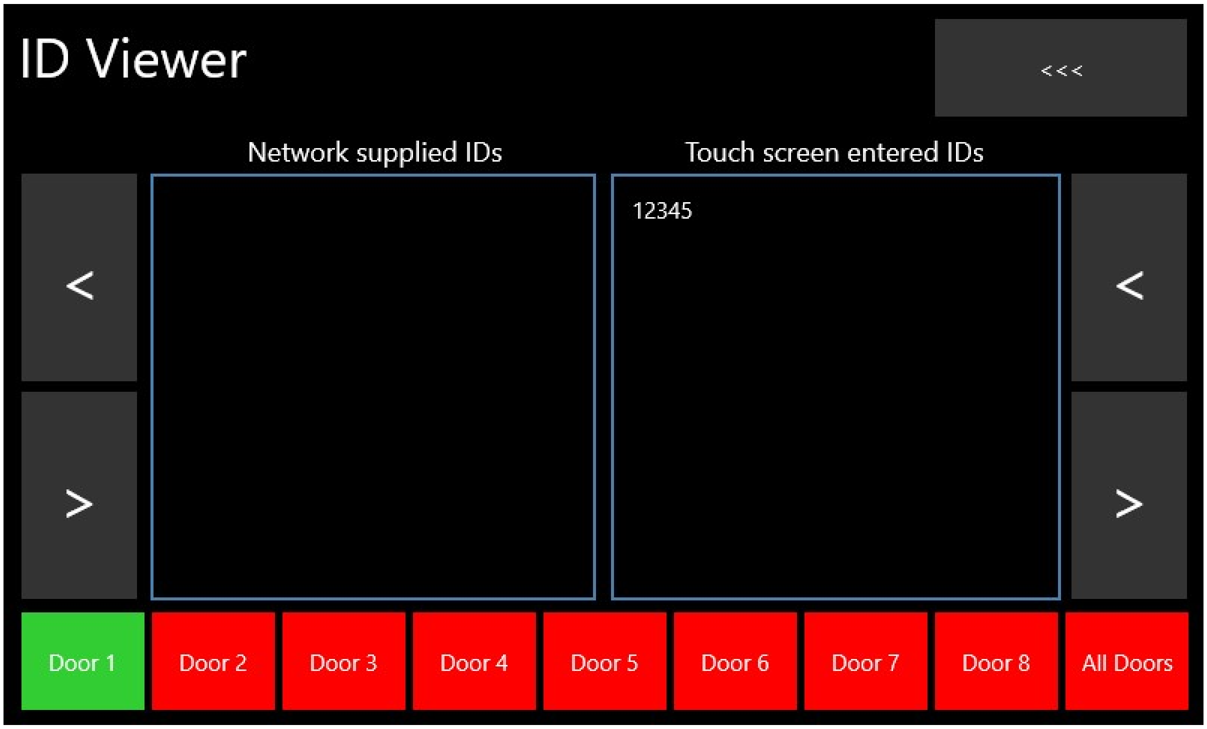
Audit Trail Viewer

```
[ 3/29/2018 4:03:22 AM ] Hardware factory reset.
[ 3/29/2018 4:04:25 AM ] HighpowerOne started
[ 3/29/2018 4:04:37 AM ] Touchscreen locked
[ 3/29/2018 4:04:46 AM ] Touchscreen unlocked
[ 3/29/2018 4:05:04 AM ] Touchscreen locked
[ 3/29/2018 4:05:28 AM ] Touchscreen unlocked
[ 3/29/2018 4:11:28 AM ] HighpowerOne started
[ 3/29/2018 5:32:26 AM ] ID added touch screen, ID: 12345
```

Choose a day of interest from the pulldown menu at the top. Once, the day is selected the entries for that day are listed below. Use the “<” and “>” buttons to scroll through the entry list.

ID Viewer

The system view is a facility that allows you to view all of the card IDs that are programmed into the controller in a basic manner. This feature is useful especially to people that use the Quick Edit ID features and lost track of what cards have already been programmed.

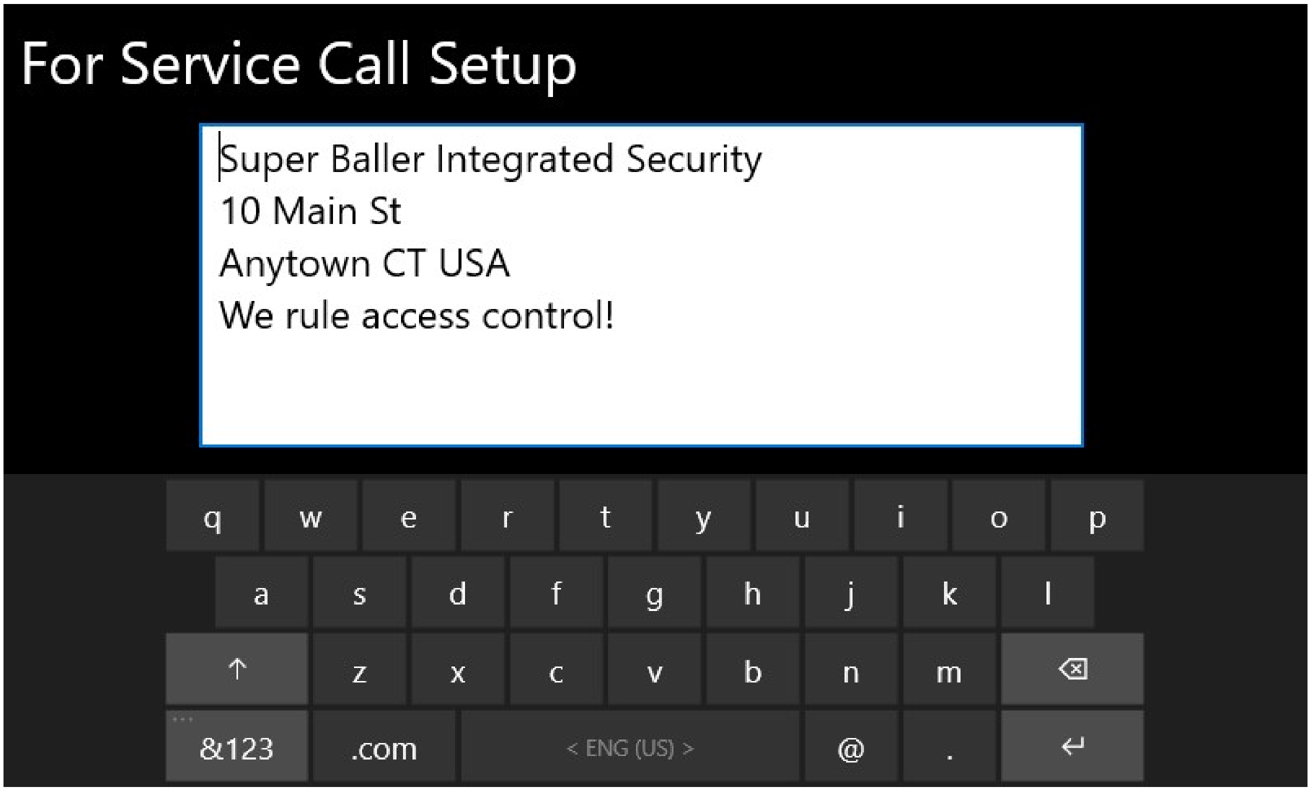


There are two windows on the system viewer. These windows show the cards that have been added to the controller via software and cards that have been added using the touchscreen. Because there are two separate databases for cards based on how they are presented to the controller, we can separate the card IDs between the two windows.

By pressing on the buttons at the bottom of the screen we can show all the cards that are available on a certain door. If you want to see all cards on the controller from any door, select the “All Doors” button. Selecting multiple door buttons will combine the card ID’s from multiple doors into one list and will exclude card IDs that are duplicates over the multiple doors.

Use the “<” and “>” buttons for each window to scroll through the card entry list.

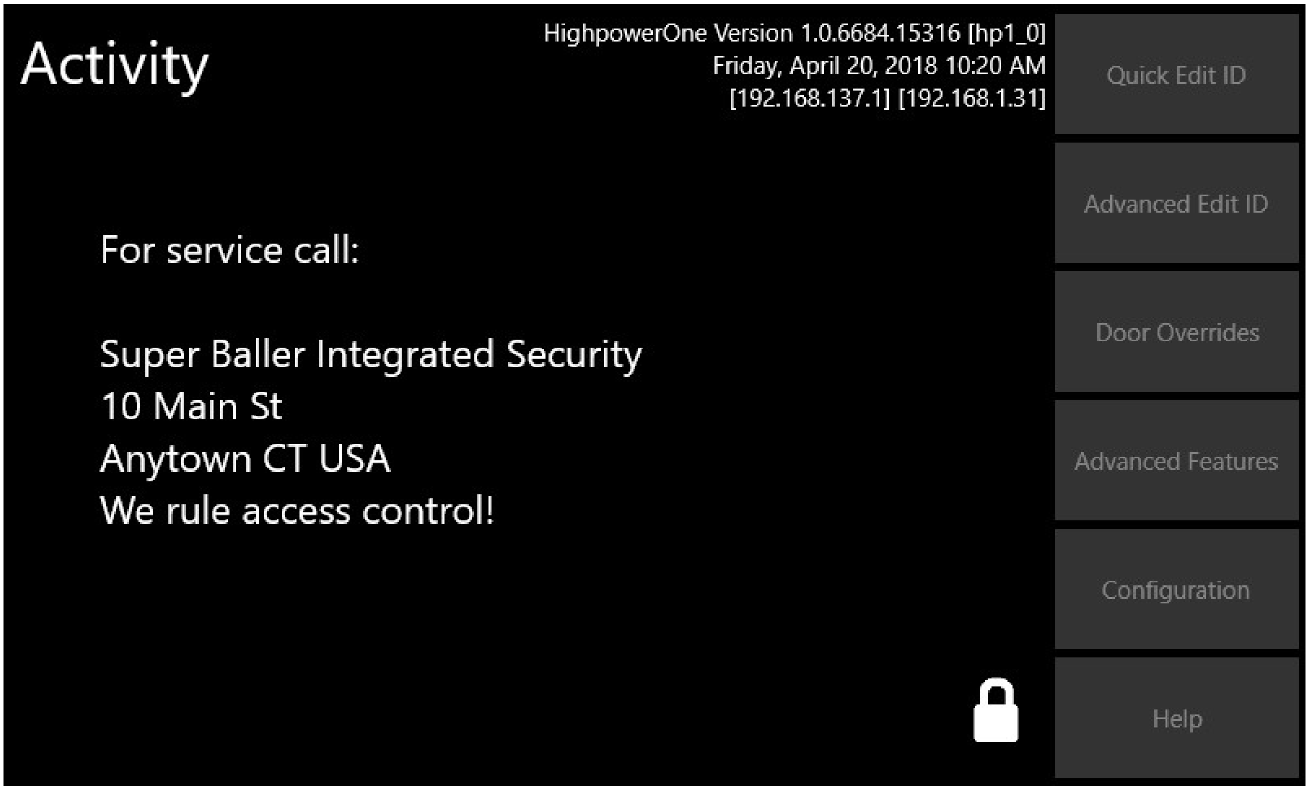
“For Service Call” Setup



For Service Call Setup

Super Baller Integrated Security
10 Main St
Anytown CT USA
We rule access control!

This feature allows an integrator to enter their information into the controller to that users know who is to be called for service. This information is presented on the main screen when it is locked.



Activity

HighpowerOne Version 1.0.6684.15316 [hp1_0]
Friday, April 20, 2018 10:20 AM
[192.168.137.1] [192.168.1.31]

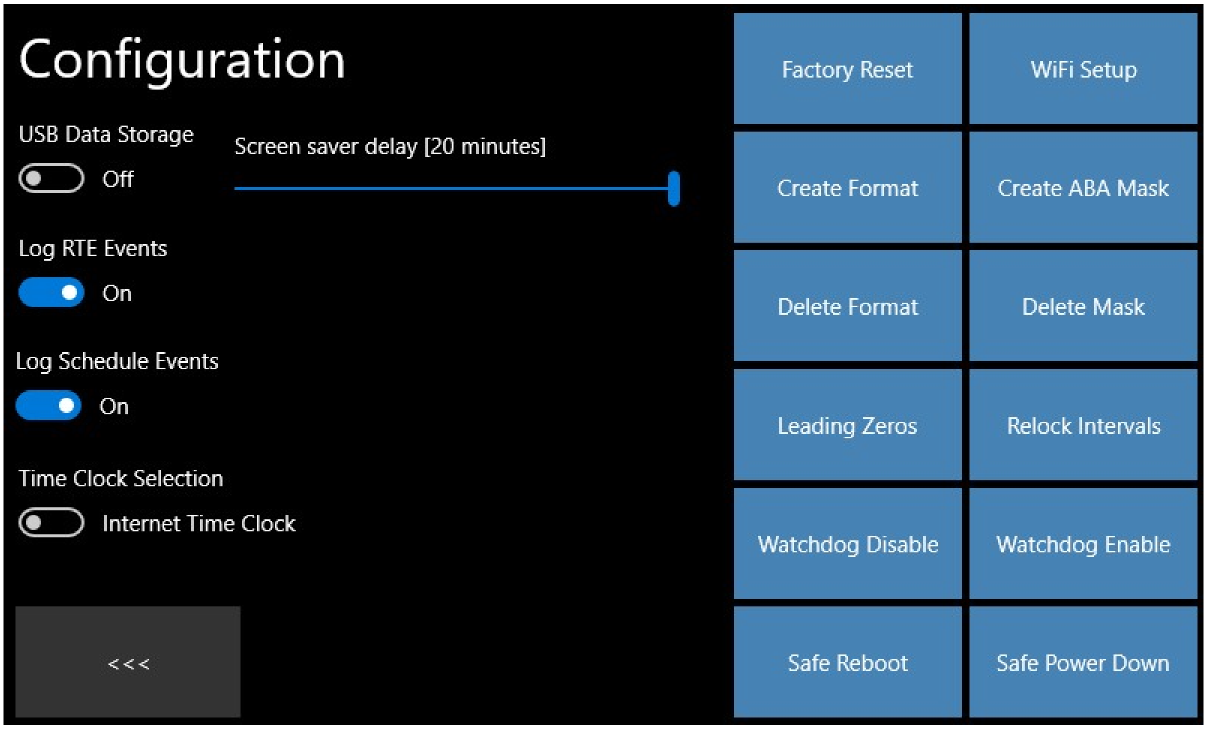
For service call:

Super Baller Integrated Security
10 Main St
Anytown CT USA
We rule access control!

To remove the service message, just clear out all of the characters in the text field of the configuration screen.

Configuration

The configuration screen is used to set up some key hardware settings on the controller. These settings are described below.



Configuration

USB Data Storage
Off

Screen saver delay [20 minutes]

Log RTE Events
On

Log Schedule Events
On

Time Clock Selection
Internet Time Clock

USB Data Storage

The system information stored on the controller is stored in data files. By default, the data files are stored on the onboard SD card. This card also has the operating system on it and provides adequate storage space for large systems. Optionally, for special applications or very large systems, you can choose to keep the data files on a USB memory stick. In doing this, you need to leave the memory plugged into a USB port on the controller at all times. Using this option provides larger memory space and the ability to hot plug configured USB sticks to change the system data on the fly without additional configuration. This is a special option that won't be applicable to most user's application. There is a speed performance hit that occurs when saving codes in bulk enrollment modes with this option, but it provides larger space for special applications.

Log RTE Events

Request to Exit (RTE) Events are logged events that occur when the request to exit input is used on the controller. The request to exit signal is a button push, a normally open contact closure that tells the controller that it should open the door. When this is input is used, it can generate a log entry indicating at what time the door was released. If you use this feature frequently, many log entries will be generated. You might not want to include these entries in the log as the event log will fill quickly. Turning off this feature will prevent the controller from generating a log entry for the request to exit signal.

Log Schedule Events

The controller can generate a log entry for events that are scheduled, mainly automatic door locking and unlocking events. If you want to reduce the size of the log, you can turn these logging events off with this switch.

Time Clock Selection

The controller has two timeclocks and you can select the one that is appropriate for your application. If the controller is connected to the internet you should select the Internet Time Server option. This option will keep the clock synchronized to an accurate internet time server and will have automatic compensation for daylight savings time. For this option to work properly, you need to set the time zone that the controller is operating in. The procedure for setting the time zone is described in a following section.

If the controller is running as a standalone device (not connected to the internet) you will need to use the onboard clock. The onboard real-time clock is a chip that tracks the current date and time. When you turn on this feature, a button will be visible in the configuration screen to set the clock values. Once you set the values, the onboard clock chip maintains the values. The controller has an onboard supercapacitor that holds charge in the case that there is a power outage. This capacitor holds enough power to maintain the time in the time clock chip for approximately two to three weeks.

Screen Saver Delay

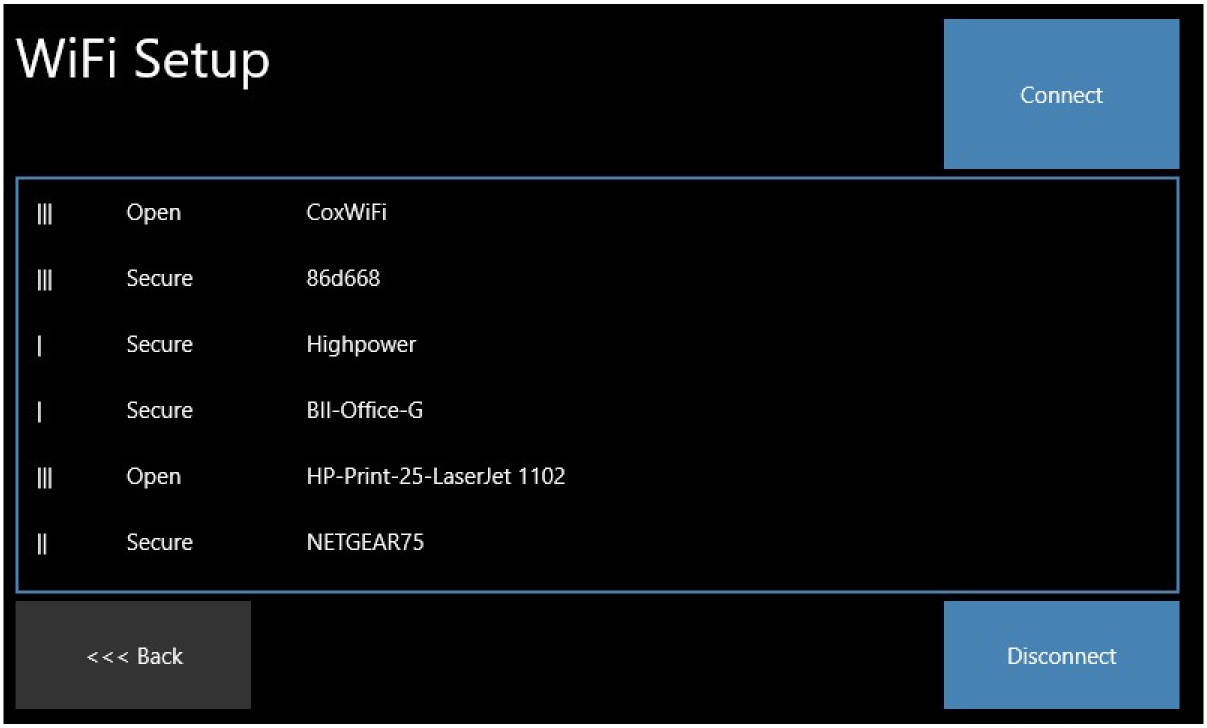
The screen saver delay is a slider that allows you to set the delay of screen blanking between 1 and 20 minutes. After the set time the display will blank to prevent long term burning of the display.

Factory Reset

The factory reset button resets the controller back to default settings. Be careful using this option as it’s very destructive as it clears all settings and data in the controller including wiping all card and audit trail entries.

Wi-Fi Setup

The Wi-Fi setup screen is used to connect the controller to a Wi-Fi router. The controller can be connected to a LAN by Wi-Fi for connection to the Highpower HMS software or to access the controller via PowerShell or web interfaces. This menu allows you to tell the controller what Wi-Fi network should be used and to supply the password to establish a connection to the router.



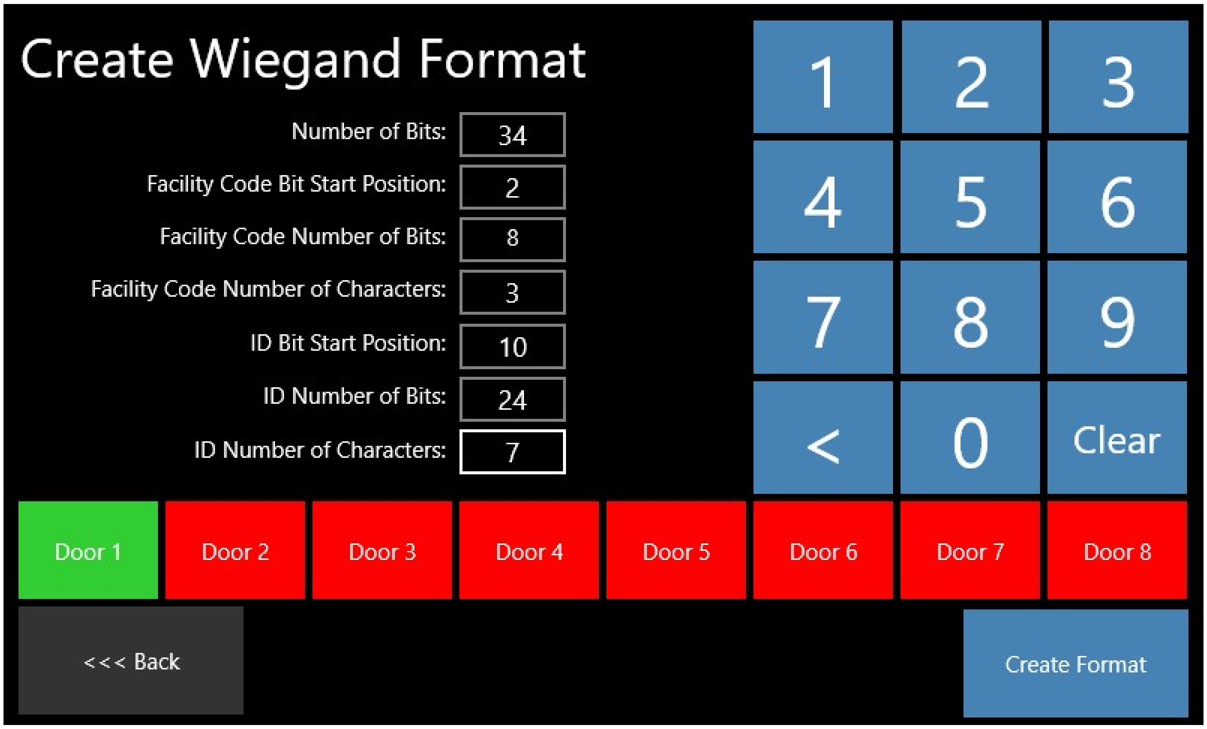
|||	Open	CoxWiFi
|||	Secure	86d668
|	Secure	Highpower
|	Secure	BII-Office-G
|||	Open	HP-Print-25-LaserJet 1102
||	Secure	NETGEAR75

The Wi-Fi setup screen shows all the available networks, a bar graph showing signal strength and the security type of the network along with the network identifier. If the network is listed as ‘Secure’ the controller will prompt you to supply the password required for the connection. Once you select a network and a password if the network is secure, hit the connect button at the top of the screen and the controller will connect.

Because of the potential for disconnects and other potential wireless transmission issues, Highpower recommends that the controller be connected to a wired network for reliability. With skill, the Wi-Fi connection can be made reliable and although we don’t endorse this connection type as the best, we make it available to the user as the hardware was present on the controllers integrated hardware.

Create Wiegand Format

The Create Wiegand Format facility allows you to define custom card formats into the controller. These formats can also be defined using the command set supported on Port 3000 via Ethernet.



Create Wiegand Format

Number of Bits: 34

Facility Code Bit Start Position: 2

Facility Code Number of Bits: 8

Facility Code Number of Characters: 3

ID Bit Start Position: 10

ID Number of Bits: 24

ID Number of Characters: 7

Each reader port has its own set of defined formats. Because the controller supports multiple formats simultaneously, it uses the number of bits in the card transmission to determine which format to use. As a result, you can only define one format for a number of bits. For example, you could not have two 26-bit formats, because the controller would not know which 26-bit format to use for decoding. By supporting multiple bit formats at each controller, you can more easily support legacy cards along with newer issued cards in the same system.

To define the format, click on each of the fields to enter the required parameters. Use the blue keyboard at the right side of the screen to enter each of the fields.

Number of Bits

This is the overall number of bits in the card format that you are defining. This is how the controller determines what format to use for a card format bit length.

Facility Code Bit Start Position

If your card format has a facility code field to be decoded, this parameter determines the start position of the field in the format. Counting the most significant bit in a card format (the leftmost bit) starts at bit 1. In our example above, our format has a parity bit at 1 that we want to ignore in the facility code, so we are skipping over bit 1 and looking for the facility code at bit 2, the second most significant bit.

Facility Code Number of Bits

This is the number of bits in the facility code field. In our example, the facility code is eight bits long.

Facility Code Number of Characters

The number of bits in the facility code represent a numeric value. The controller takes this value and converts the value into a decimal number. For example, if the facility code had all eight bits set as ones, ‘11111111’ converting the number to a decimal would be decimal ‘255’. This field determines how many decimal positions the field should report. In our example, we want to report 3 decimal positions to accommodate ‘255’. If you wanted leading zeros reported, you could for example, choose 6 decimal positions, where the controller would report ‘000255’ as a facility code. Choosing a value less than three digits would truncate the output of the facility code in a weird way so be cautious to leave enough decimal digits in this setting to accommodate the largest number in the field. If you put a zero into this field, the facility code will not be reported.

To calculate the number of decimals required to accommodate the field, calculate the largest number that a particular field length could possibly generate using the following:

LARGEST NUMBER = 2 ^ (FIELD LENGTH) - 1

In our example, we have 8 bits in the facility code. 2 raised to the power of 8 = 256. 256 -1 = 255, which is the largest possible number that we need to accommodate.

In the controller, the facility code is reported as part of the overall card ID. This is described further in a following section.

ID Bit Start Position

This is the location in the bits of the card format that is the start of the card ID field. Counting the most significant bit in a card format (the leftmost bit) starts at bit 1. In our example above, our particular format has a parity bit and a facility code, so we are skipping over these bits and starting at bit 10 to decode our ID.

ID Number of Bits

This is the number of bits in the ID field. In our example, the number of bits in the ID field is 24 bits long.

ID Number of Characters

The number of bits in the ID code represent a numeric value. The controller takes this value and converts the value into a decimal number. For example, if the facility code had all bits set as ones, ‘111111111111111111111111’’ converting the number to a decimal would be decimal ‘16777214’’. This field determines how many decimal positions the field should report. In our example, we want to report 8 decimal positions to accommodate ‘16777214’. If you wanted leading zeros reported, you could for example, choose 10 decimal positions, where the controller would report ‘0016777214’ as an ID code. Choosing a value less than eight digits would truncate the output of the facility code in a weird way so be cautious to leave enough decimal digits in this setting to accommodate the largest number in the field. If you put a zero into this field, the ID code will not be reported. This might be good for limited applications where you are just looking for any card of a certain facility code.

To calculate the number of decimals required to accommodate the field, calculate the largest number that a certain field length could possibly generate using the following:

LARGEST NUMBER = 2 ^ (FIELD LENGTH) - 1

In our example, we have 24 bits in the facility code. 2 raised to the power of 24 = 16777215. 16777215 - 1 = 16777214, which is the largest possible number that we need to accommodate.

In the controller, the ID code is reported as part of the overall card ID. This is described further in a following section.

Format Door Selection

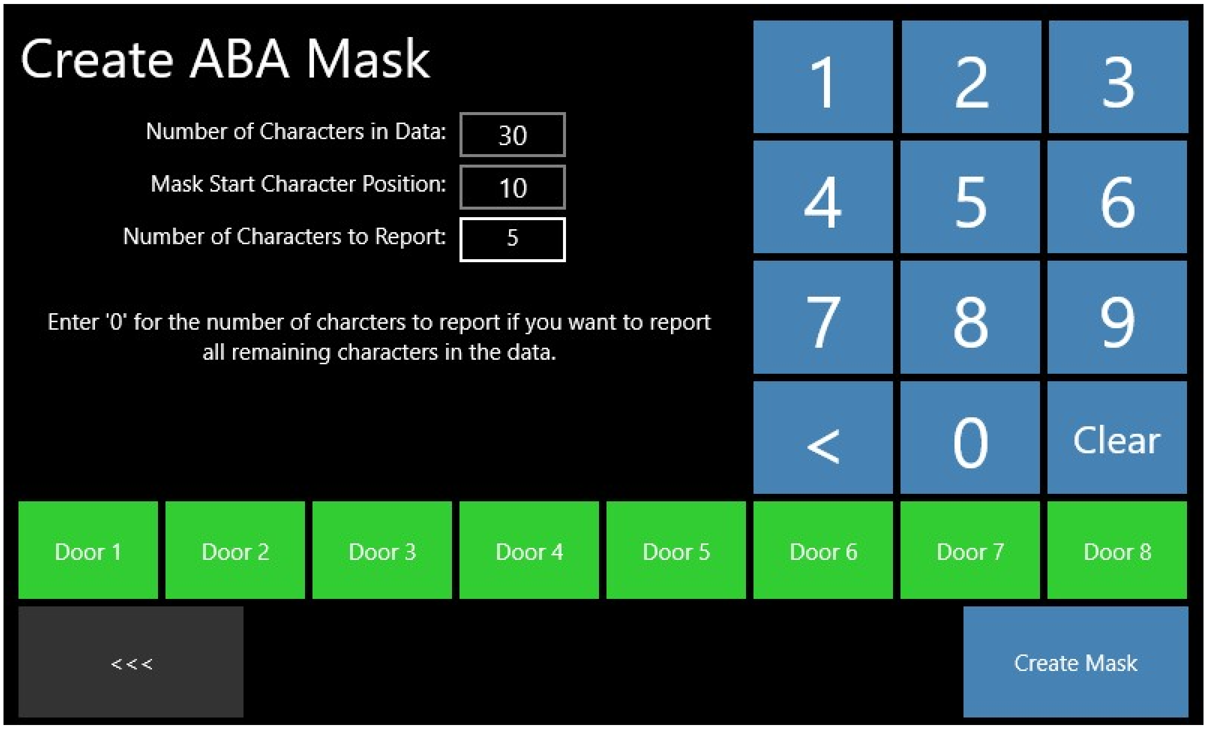
Once your format is defined, you will want to apply the format to a reader or readers. Most likely all of the readers will apply. Selecting the door buttons at the bottom of the screen saves the defined format to the selected doors that are highlighted in green. Pressing the door buttons at the bottom of the screen toggles the buttons from green to red. Change the buttons to red if you don’t want the custom format applied to a reader. Because most custom formats are used over all doors in a system, you will want to make sure in this case that all the buttons are highlighted green before pressing the “Create Format” button. This is the default state of the buttons.

Composite Card IDs

When you program both facility code parameters and card ID parameters into the controller, the controller will combine both fields digits to form one card ID. For example, if your card has a facility code of 125 and a card ID of 5432, the controller will report the combined card ID number of 12505432. To prevent the facility code acting as a prefix to the card ID, enter 0 into the facility code number of decimal characters field.

Create ABA Mask

ABA Masking is a feature that tells the controller how to extract certain characters out of the Track II data coming off of a magstripe or proximity card. Out of a long string of magstripe data, you can pull out a subset of characters to be the card ID. This facility sets up the parameters of the character extraction.



Create ABA Mask

Number of Characters in Data: 30

Mask Start Character Position: 10

Number of Characters to Report: 5

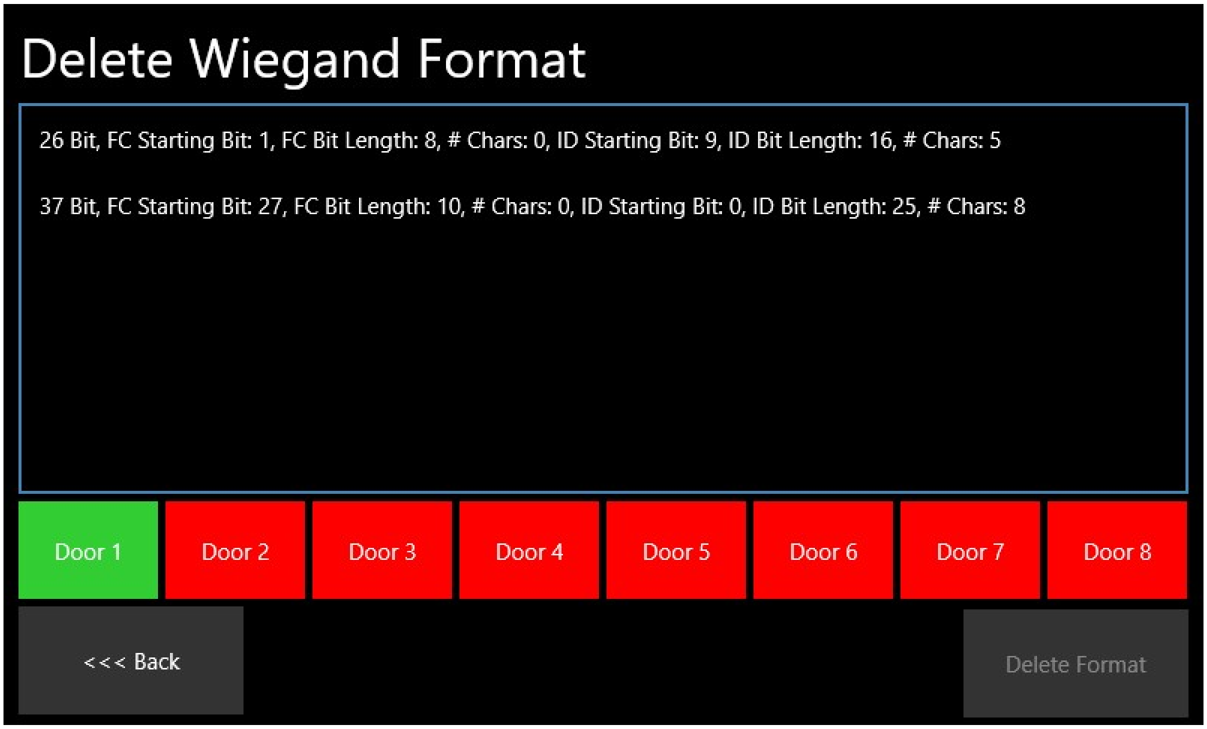
Enter '0' for the number of charcters to report if you want to report all remaining characters in the data.

In the example above, we are adding a mask to all readers, since all readers are marked with the lower buttons in a green color. To only apply a mask to particular readers, toggle the colors of the reader buttons to red in order to exclude certain readers. Our mask looks for magstripe data that is 30 characters long. If a 30 character magstripe card is swiped on the reader with this mask, then only five of the characters in the magstripe will be reported. The extraction of these five characters starts at position 10 in the data stream.

Please note, if no masks are supplied to a reader, the reader output will be un-masked and all data is reported as the card ID. As soon as a mask is supplied, all data that is not masked will not be reported. By default the controller has no masks as default.

Delete Wiegand Format

If you have added a custom Wiegand Card Format to a reader, you can later remove the format if changes in the card formats used by the system occur. By pressing the button at the bottom of the screen for a door, all of the formats active on that door are displayed. From the display, you select which format should be deleted. Because the formats do not have names, the controller provides you with the information for each format.



Delete Wiegand Format

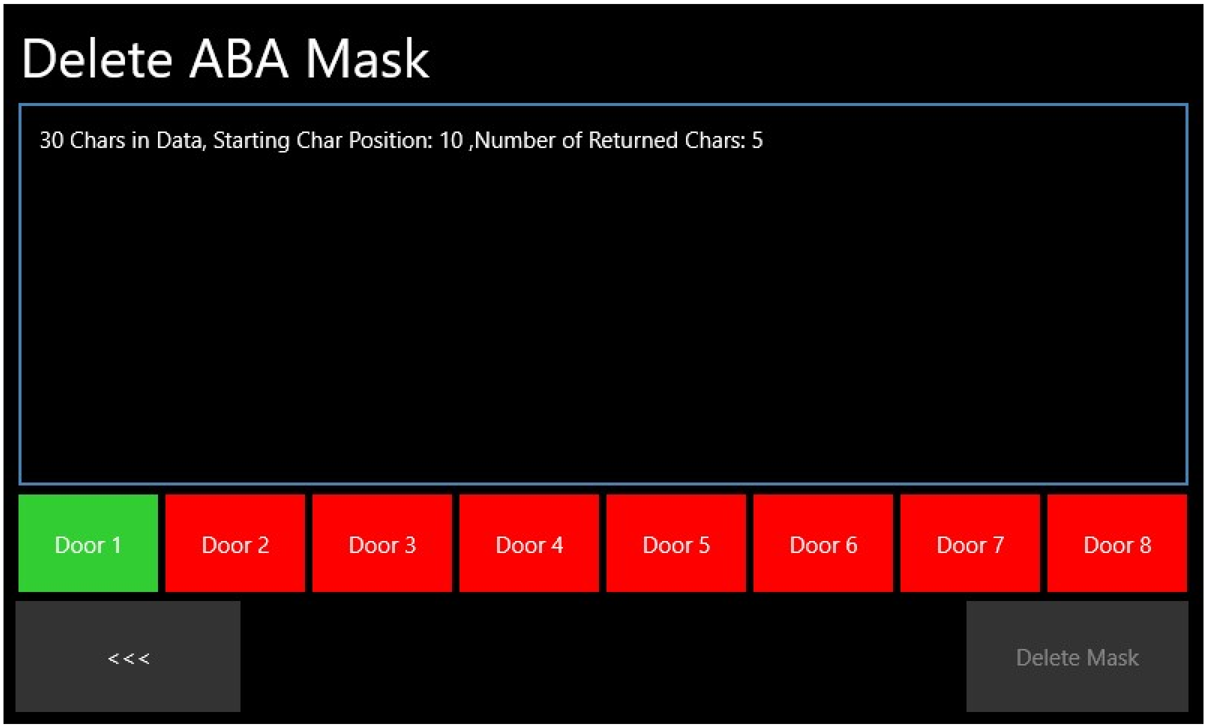
26 Bit, FC Starting Bit: 1, FC Bit Length: 8, # Chars: 0, ID Starting Bit: 9, ID Bit Length: 16, # Chars: 5

37 Bit, FC Starting Bit: 27, FC Bit Length: 10, # Chars: 0, ID Starting Bit: 0, ID Bit Length: 25, # Chars: 8

If the format is present on multiple doors, you will need to delete the entry on each of the doors independently.

Delete ABA Mask

This facility allows you to remove an ABA mask from certain readers.



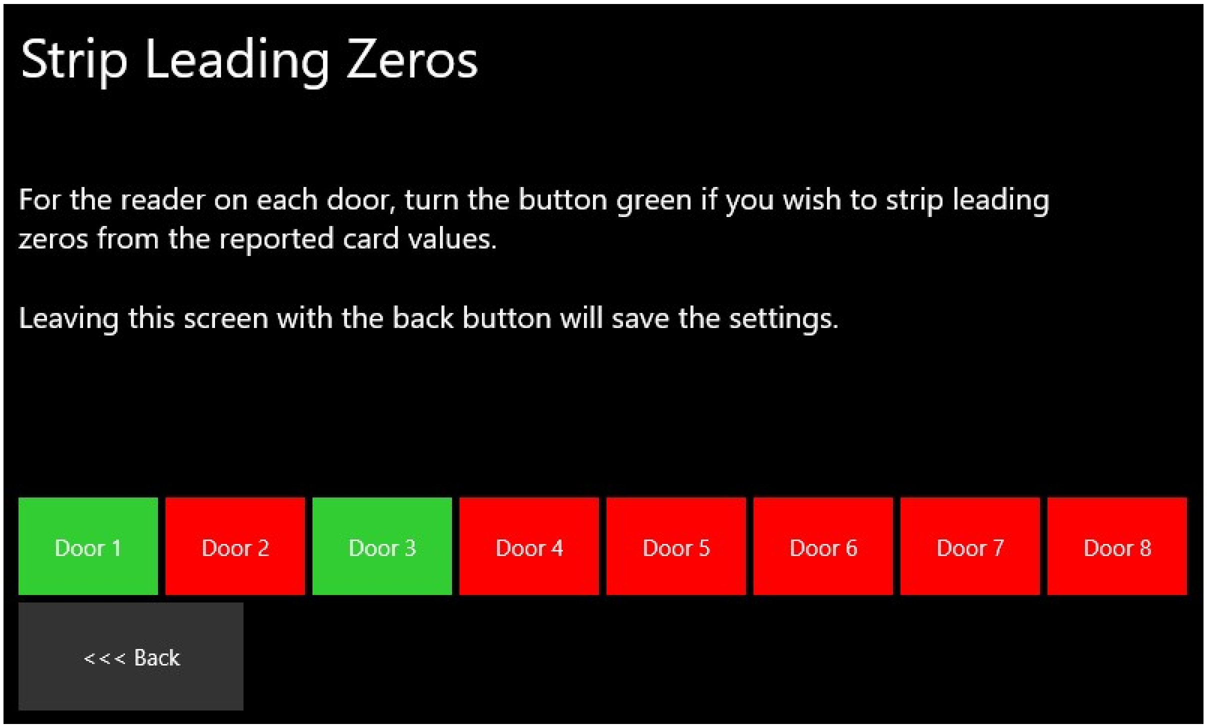
Delete ABA Mask

30 Chars in Data, Starting Char Position: 10 ,Number of Returned Chars: 5

To delete a mask, first use the buttons below to select the reader that is being considered. Then in the list above, select the mask to be deleted. Once selected, hit the “Delete Mask” to remove the mask from the reader.

Reader Strip Leading Zero Settings

If the defined format for the card is set to convert the ID field into a specific number of digits, there are times when cards that have small values can produce leading zeros in the output. For example, if you use a 26 bit card, which normally reports a 5 digit number but the card value swiped is under 10,000 you would get a card swipe that has leading zeros. Card 1234 for example would be reported as card 01234. If you do not want to report the leading zero, you can turn on the Leading Zero Stripping feature.



Strip Leading Zeros

For the reader on each door, turn the button green if you wish to strip leading zeros from the reported card values.

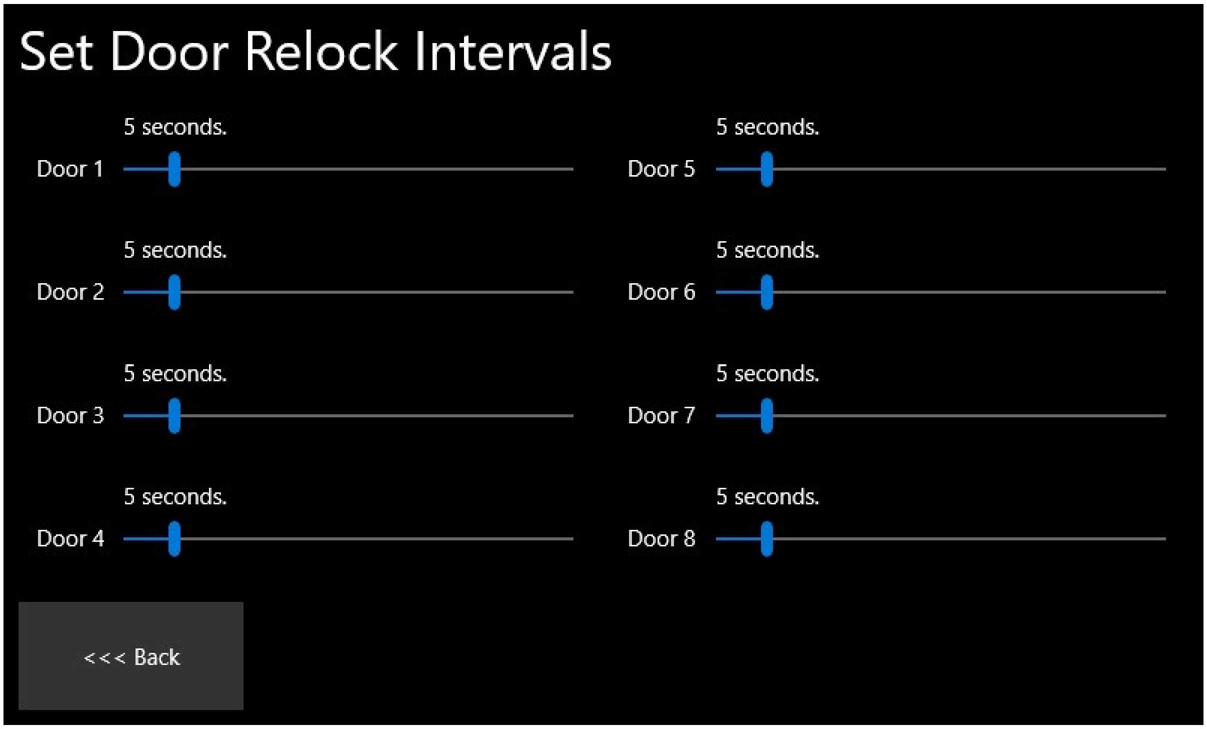
Leaving this screen with the back button will save the settings.

🟩 Door 1 | 🟥 Door 2 | 🟩 Door 3 | 🟥 Door 4 | 🟥 Door 5 | 🟥 Door 6 | 🟥 Door 7 | 🟥 Door 8

To turn on the feature for a reader, just select the reader that the feature is turned on for at the bottom of the screen. Any reader that is marked in green has the feature turned on. You toggle the feature state just by tapping the buttons. After selecting the readers that has the feature turned on, hit the “<<< Back” key to save your selections and return to the Advanced Features menu.

Relock Intervals

This screen allows you to set the automatic relock delay of each of the eight doors in the system. Adjust each slider to set the delay of every door from 1 to 99 seconds.



Set Door Relock Intervals

Door 1 5 seconds.

Door 2 5 seconds.

Door 3 5 seconds.

Door 4 5 seconds.

Door 5 5 seconds.

Door 6 5 seconds.

Door 7 5 seconds.

Door 8 5 seconds.

Once you leave the screen with the << Back button the settings are saved.

Watchdog Controls

There are two function buttons to control the watchdog feature. The watchdog feature resets the main computer on the controller if the application hangs due to unusual hardware situations. The watchdog feature is described further in a following section. The functions to enable and disable the watchdog are mainly used when the firmware of the controller is being updated remotely. Only use these features if directed by the factory.

Safe Reboot

If you want to reboot your controller in a controlled way, you can use the Safe Reboot function. This function will make sure that all the settings that you made to the controller are saved properly and will cause a reboot. Often, many settings in the controller are queued to be saved several minutes later due to the way the Windows 10 operating system functions. The safe reboot feature stores these settings and reboots the controller.

Safe Power Down

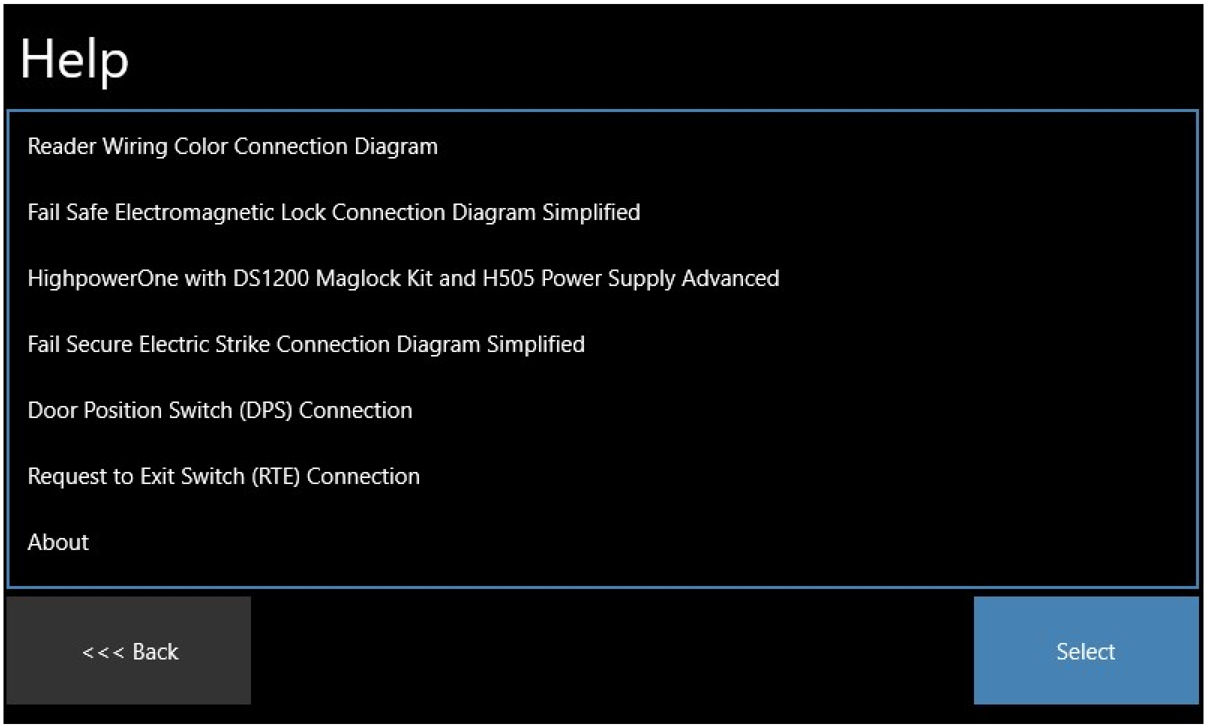
If you want to power down the controller in a controlled way, you can use the Safe Power Down function. This function will make sure that all the settings that you made to the controller are saved properly and will cause a proper operating system shutdown before pulling power. This function is useful in preserving the valid state of the SD card storage system.

Often, many settings in the controller are queued to be saved several minutes later due to the way the Windows 10 operating system functions. The safe shutdown feature stores these settings and shutdown the controller.

Due to limitations of the hardware design, the controller does not actually power down. This is a mechanism to provide an orderly software shutdown. The software will perform a software shutdown and you will see a brief “whitening” on the screen and the LAN LEDs will go out. Once you see the screen react to the shutdown, it’s safe to pull the power. If you do not pull the power, the watchdog activation system will eventually kick in and cause the controller to reboot.

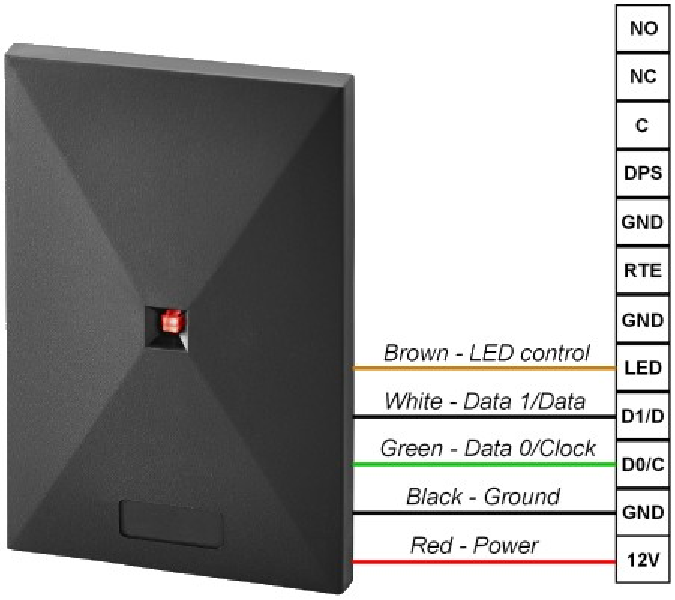
Help

The help system in the controller is a series of wiring diagrams and other information that installers can use during initial installation.


Help
Reader Wiring Color Connection Diagram
Fail Safe Electromagnetic Lock Connection Diagram Simplified
HighpowerOne with DS1200 Maglock Kit and H505 Power Supply Advanced
Fail Secure Electric Strike Connection Diagram Simplified
Door Position Switch (DPS) Connection
Request to Exit Switch (RTE) Connection
About
<<< Back
Select

You can select a particular diagram from the help system selection menu. See an example below:

Wiegand or Magstripe Reader Connection



Don't connect the reader while the controller is powered.
Remove the terminal block when connecting the reader wires.

Please do not connect the readers and other accessories to the controller while it is powered in order to prevent shorts and other types of power issues. Best practice is to use the diagrams as notes for paper sketches or to take a picture of the diagrams with your cell phone to make connections while the controller is depowered. Once you select a diagram to view in the help system, it remains displayed until you click on the screen once again. Clicking on the diagram dismisses it and brings you back to the help selection menu.

Non-volatile settings considerations

Generally, when making settings changes to the controller, the settings changes normally become active immediately. After being adjusted, these settings are queued in memory to later be saved on the SD memory for non-volatile storage. **This process can take a few minutes. You want to make sure that once a settings change is made to the controller, that power is not removed immediately to make these changes permanent.** Allow up to 5 minutes before de-powering the controller after changing a setting.

Software Integration

The HighpowerOne has a TCP/IP server located at Ethernet Port 3000 that can be used to send commands to the controller. This port can be access over both a wired and Wi-Fi connection of the controller to a LAN. The command set is defined in this section. All commands are completed with a carriage return character ASCII 13 (hex 0D). The responses from the controller are also all suffixed with an ASCII 13 character (hex 0D). You can open a connection to the controller with a terminal such as ‘PuTTY’ (http://www.putty.org/) or from your own application code.

Command Set via Port 3000

V -Version

Sends the version of the controller.

F000 -Version

Sends the version of the controller.

F010rxx -Forced relay activation

Triggers relay number r for xx seconds. r = 0 to 7 (Door 1 - Door 8), xx = 00 - 99 seconds

F020rdd -Set relay delay time

Set relay delay time of a relay for auto relocking cycle.
r = 0 to 7 (Door 1 - Door 8), xx = 00 - 99

F030x -Log request to exit events setting

Turns on or off logging of RTE events.
x=0 logging off, x=1 logging on

F031x -Log door schedule events setting

Turns on or off logging of door schedule events.
x=0 logging off, x=1 logging on

F07d -Door position switch (DPS) status check

Check the door position switch status on door number d. d = 0 to 7 (Door 1 - Door 8)
Response string: *OPEN* or *CLOSED* or *UNDEFINED INPUT*

F08d -Relay state check

Check the relay status on door d. d = 0 to 7 (Door 1 - Door 8)
Response string: *DEENERGIZED* or *ENERGIZED* or *UNDEFINED OUTPUT*

F11d -Set door to normal operation

Door d set to normal door operation. d = 0 to 7 (Door 1 - Door 8)
Response string if input valid: *OK*

F12d -Set door to lockdown mode

Door d set to lockdown mode. d = 0 to 7 (Door 1 - Door 8)
Response string if input valid: *OK*

F13d -Set door to passage mode

Door d set to passage mode. d = 0 to 7 (Door 1 - Door 8)
Response string if input valid: *OK*

F14d -Report the mode of door

Report the door mode of door d. d = 0 to 7 (Door 1 - Door 8)
Response string if input valid: *NORMAL DOOR d* or *LOCKDOWN DOOR d* or *PASSAGE DOOR d*

F100rsssmmddyyyyi… -Add a card schedule to active memory bank

Add a card ID i to reader r on schedule ss to active memory bank.
mmddyyyy = expiration date. if 000000000=no expiration

F105rsssmmddyyyyi… -Add a card schedule to inactive memory bank

Add a card ID i to reader r on schedule ss to inactive memory bank.
mmddyyyy = expiration date. if 0=no expiration

F110ri… -Delete a card from active memory bank

Delete a card ID from reader r on the active memory bank.
r = 0 to 7 (Door 1 - Door 8), i = card ID

F115ri… -Delete a card from inactive memory bank

Delete a card ID from reader r on the inactive memory bank.
r = 0 to 7 (Door 1 - Door 8), i = card ID

F120r -Delete all cards from a reader active bank

Delete all cards from reader r on active bank. r = 0 to 7 (Door 1 - Door 8)

F125r -Delete all cards from a reader inactive bank

Delete all cards from reader r on inactive bank. r = 0 to 7 (Door 1 - Door 8)

F130r -List all cards on a reader active bank

List all cards on reader r from active bank. r = 0 to 7 (Door 1 - Door 8)

F135r -List all cards on a reader inactive bank

List all cards on reader r from inactive bank. r = 0 to 7 (Door 1 - Door 8)

F140ri… -Return the schedule number of a card active bank

Return the schedule number of a card ID i on the active memory bank for reader r.
r = 0 to 7 (Door 1 - Door 8), i = card ID

F145ri… -Return the schedule number of a card inactive bank

Return the schedule number of a card ID I on the inactive memory bank for reader r.
r = 0 to 7 (Door 1 - Door 8), i = card ID

F160r -Deactivate strip leading zeros from card IDs

Do not strip out leading zeros from card id.
r = 0 to 7 (Door 1 - Door 8)

F161r -Activate strip leading zeros from card IDs

Strip out leading zeros from card id.
r = 0 to 7 (Door 1 - Door 8)

F170r -Return the number of card IDs on a reader active bank

Return the number of card IDs on reader r on the active memory bank.
r = 0 to 7 (Door 1 - Door 8)

F175r -Return the number of card IDs on a reader inactive bank

Return the number of card IDs on reader r on the inactive memory bank.
r = 0 to 7 (Door 1 - Door 8)

F200 -Swap memory bank inactive to active

Swap system memory banks and delete old inactive bank data.

F210aabbccddeeffgghh -Set relay delay times for all relays

Set relay delay time for automatic relock cycle of all relays with one command.
aa = 00 - 99 seconds (relay 0 - Door 1)
bb = 00 - 99 seconds (relay 1 - Door 2)
cc = 00 - 99 seconds (relay 2 - Door 3)
dd = 00 - 99 seconds (relay 3 - Door 4)
ee = 00 - 99 seconds (relay 4 - Door 5)
ff = 00 - 99 seconds (relay 5 - Door 6)
gg = 00 - 99 seconds (relay 6 - Door 7)
hh = 00 - 99 seconds (relay 7 - Door 8)

F240rbbSSLLDDiillldd -Add a Wiegand format to reader

Add a Wiegand format to reader r.

r=reader number
bb=number of total bits in card format
SS=site code start bit location from 1
LL=site code number of bits
DD=number of digits to translate site code into
ii=id code start bit location from 1
ll=id code number of bits
dd=number of digits to translate id code into

F245rbb -Delete a Wiegand format from a reader

Delete a Wiegand format from reader r.
r=reader number, bb=number of bits in the format.

F250r -Add an ABA mask to reader

Add a magstripe mask to reader r
r=reader number
Non-functional stub in firmware V1.0

F260r -Delete an ABA mask on reader

Delete a magstripe mask to reader r.
r=reader number
Non-functional stub in firmware V1.0

F400rsssdhhmmhhmm -Add a schedule to a reader active bank

Add a schedule to a reader where sss is schedule number on the active bank.
r=reader numberf
Sss=schedule number
d = day of week
hhmm = start hours/minute
hhmm = end hours/minute

F405rsssdhhmmhhmm -Add a schedule to a reader inactive bank

Add a schedule to a reader where sss is schedule number on the inactive bank.
r=reader number
Sss=schedule number
d = day of week
hhmm = start hours/minute
hhmm = end hours/minute

F410rsssd -Clear a schedule from a reader active bank by day

Clear a schedule sss on the active bank from reader r on day d.

F415rsssd -Clear a schedule from a reader inactive bank by day

Clear a schedule sss on the inactive bank from reader r on day d.

F420rsss -Clear a schedule from a reader active bank all days

Clear a schedule sss from reader r on the active bank, for every day.

F425rsss -Clear a schedule from a reader inactive bank all days

Clear a schedule sss from reader r on the inactive bank, for every day.

F430r -Clear all schedules from a reader active bank

Clear all schedules from reader r on the active bank.

F435r -Clear all schedules from a reader inactive bank

Clear all schedules from reader r on the inactive bank.

F450rxxxyyy -Link a schedule on a reader active bank

Link a schedule on the active bank. Connect schedule xxx to schedule yyy on reader r.

F455rxxxyyy -Link a schedule on a reader inactive bank

Link a schedule on the inactive bank. Connect schedule xxx to schedule yyy on reader r.

F460r -Delete all schedule links on a reader active bank

Delete all schedule links on reader r on the active bank.

F465r -Delete all schedule links on a reader inactive bank.

Delete all schedule links on reader r on the inactive bank.

F470dsss -Set the unlock schedule of a door

Set the unlock schedule sss of door d.

F48xd -First person in feature on/off

First person in toggle on door d where
x = 0: turn off
x = 1: turn on

F500 -Return log entries

Return a log entry or multiple log entries.
Log entries are individually cleared in hardware as they are retrieved with F500.

Returned string: xxxxxxxxyyyyyyyyiiiiiiii…..|r|MMDDYYHHMMSS|T

Where
xxxxxxxx is the state of each of the relay from relay 1 to 8 at the time of log retrieval.
If x = 0 the relay is de-energized. If x=1 the relay is energized.

yyyyyyyy is the state of each of the door position switches at the time of log retrieval.
If x = 0 the DPS is open. If x = 1 the DPS is closed. DPS is a normally open, held closed signal.

r is the reader number or door number that the log was generated from.

MMDDYYHHMMSS is the timestamp of when the log occurred.

T is the type of log entry

Where:
T = 0   Access Granted
T = 1   Access Denied
T = 2   Access Denied by Schedule
T = 3   Access Denied, Card Expired
T = 4   Request to Exit
T = 5   Door Unlocked by Schedule
T = 6   Door Locked by Schedule
T = 7   Door set to Normal Operation
T = 8   Door set to Lockdown Mode
T = 9   Door set to Passage Mode
T = 10   Touch screen Locked
T = 11   Touch screen Unlocked
T = 12   HighpowerOne started
T = 13   Open enrollment mode started
T = 14   Open enrollment mode completed
T = 15   ID removal mode started
T = 16   ID removal mode completed
T = 17   ID added by open enrollment
T = 18   ID removed by open enrollment
T = 19   ID added by touchscreen
T = 20   ID removed by touchscreen
T = 21   ID added by touchscreen bulk operation
T = 22   ID deleted by touchscreen bulk operation
T = 23   HighpowerOne factory reset

Log entries are separated by a } character if more than one log is available.
Command returns xxxxxxxxyyyyyyyyEND if no more log entries are available.

F510   -Clear all log entries

Clear all log entries. (Very destructive)
Use F500 to both retrieve and clear individual log entries. F510 is just for factory use.

F565rriiiiiiii…|sss|MMDDYYHHMMSS}iiiiiii….|sss|MMDDYYHHMMSS}... -Power transfer

Fast power transfer multiple IDs to reader r on the inactive bank. Fields are separated by the pipe symbol “|” The purpose of power transfer is to quickly send a block of codes to the controller’s inactive memory bank. Once the bank is filled with card entries and updates of other information like schedules, then you do a bank swap using command F200 and the changes become active on the controller. F200 command changes the memory banks in the controller to move the new data to an active state and also deletes all of the old data that was present in the foreground bank before the swap. The bank change command does not affect log data in any way.

rr = reader number
Iiiiiii... = a card ID
sss = schedule for card ID
MMMDDDYYYHHMMSS = expiration date of card ID, if 00000000 then no expiration date
} allows the separation of multiple card ID information.
The overall length of the entire command is recommended to be under 1450 characters total.

F600eeeMMDDHHIImmddhhmm -Add recurring holiday active bank

Add a recurring holiday on the active bank.
eee=entry number
MM= start month
DD=start day
HH=start hour
II=start min
mm=end month
dd=end day
hh=end hour
mm=end hour

F605eeeMMDDHHIImmddhhmm -Add a recurring holiday inactive bank

Add a recurring holiday on the inactive bank.
eee=entry number
MM= start month
DD=start day
HH=start hour
II=start min
mm=end month
dd=end day
hh=end hour
mm=end hour

F610eeeMMDDYYYYHHIImmddyyyyhhmm -Add a non-recurring holiday active bank

Add a non-recurring holiday on the active bank.
eee=entry number
MM= start month
DD=start day

YY=start year
HH=start hour
II=start min
mm=end month
dd=end day
yy=start year
hh=end hour
mm=end hour

F615eeeMMDDYYYYHHIImmddyyyyhhmm -Add a non-recurring holiday inactive bank

Add a non-recurring holiday on the inactive bank.
eee=entry number
MM= start month
DD=start day
YY=start year
HH=start hour
II=start min
mm=end month
dd=end day
yy=end year
hh=end hour
mm=end hour

F620eee -Delete a recurring holiday active bank

Delete a recurring holiday on the active bank.
eee=entry number

F625eee -Delete a recurring holiday inactive bank

Delete a recurring holiday on the inactive bank.
eee=entry number

F630eee -Delete a non-recurring holiday active bank

Delete a non-recurring holiday on the active bank.
eee=entry number

F635eee -Delete a non-recurring holiday active bank

Delete a non-recurring holiday on the inactive bank.
eee=entry number

F640 -Delete all recurring holidays active bank

Delete all recurring holidays on the active bank.

F645 -Delete all recurring holidays active bank

Delete all recurring holidays on the inactive bank.

F650 -Delete all non-recurring holidays active bank

Delete all non-recurring holidays on the active bank.

F655 -Delete all non-recurring holidays inactive bank

Delete all non-recurring holidays on the inactive bank.

F800 -Setting listing of the controller

Prints a rundown of all settings in the controller. The output uses both carriage returns and linefeeds so that the output report formats properly in a telnet session. Mainly for factory diagnostics.

Report format:

```
Current active memory bank: 0
Relay 0 delay: 5
Relay 1 delay: 5
Relay 2 delay: 5
Relay 3 delay: 5
Relay 4 delay: 5
Relay 5 delay: 5
Relay 6 delay: 5
Relay 7 delay: 5
Door 0 unlock schedule: 0
Door 1 unlock schedule: 0
Door 2 unlock schedule: 0
Door 3 unlock schedule: 0
Door 4 unlock schedule: 0
Door 5 unlock schedule: 0
Door 6 unlock schedule: 0
Door 7 unlock schedule: 0
Door 0 strip leading zeros: 0
Door 1 strip leading zeros: 0
Door 2 strip leading zeros: 0
Door 3 strip leading zeros: 0
Door 4 strip leading zeros: 0
Door 5 strip leading zeros: 0
Door 6 strip leading zeros: 0
Door 7 strip leading zeros: 0
Door 0 first person-in active: 0
Door 1 first person-in active: 0
Door 2 first person-in active: 0
Door 3 first person-in active: 0
Door 4 first person-in active: 0
Door 5 first person-in active: 0
Door 6 first person-in active: 0
```

Door 7 first person-in active: 0

F810r -Show all card IDs of a reader active bank

Print out all card ID data on reader r on the active bank. For diagnostic use only.

F815r -Show all card IDs of a reader inactive bank

Print out all card ID data on reader r on the inactive bank. For diagnostic use only.

F820rd -Show all schedules of a reader active bank

Show all schedules on the active bank for reader r, where d=day of week

F825rd -Show all schedules of a reader inactive bank

Show all schedules on the inactive bank for reader r, where d= day of week

F830 -Show recurring holidays on the active bank

Audit recurring holidays on the active bank.

F835 -Show recurring holidays on the inactive bank

Audit recurring holidays on the inactive bank.

F840 -Show non-recurring holidays on the active bank

Audit non-recurring holidays on reader r on the active bank.

F845 -Show non-recurring holidays on the inactive bank

Audit non-recurring holidays on the inactive bank.

F850r -Show the Wiegand card formats on a reader

Audit Wiegand card formats on reader r.

F870 -Show the current controller time

Get current controller time.

F875DDMMYYYYHHMMSS -Set the onboard clock time

Set onboard real time clock value.

Where:
DD = day
MM = month
YYYY = year
HH = hour
MM = minutes
SS = seconds

Please note that this command has a slightly different order than the date time format on other commands. The result of a successful clock set will return the date and time that was set. If the information passed to the controller with this command is invalid, then the controller will return the word “BAD”

F876 -Use the onboard clock as the clock source

Set the onboard real-time clock as the time source.

F877 -Use the internet clock as the clock source

Set the internet time server as the time source.

F880 -Use the SD card for system database storage

Switch the active storage media to the onboard SD card.

F881 -Use a USB stick for system database storage

Switch the active storage media to USB memory stick.

F900 -Clear all data on the active bank

Clear all data on active bank.

F905 -Clear all data on the inactive bank

Clear all data on inactive bank.

F950 -Turn off the PI watchdog timer

Turns off the Pi watchdog timer. Factory use only.

F960 -Turn on the PI watchdog timer

Turns on the Pi watchdog timer. Factory use only.

F975 -Forced watchdog hardware reboot

Hard hardware reboot. Factory use only.

F999 -Factory reset

Factory reset. (Very destructive)

Deletes all codes, schedules, holidays and other added information in the controller.
Re-establishes the following parameters in the controller:

Current active memory bank is 0
Screen saver delay set to 5 seconds
Door automatic re-lock relay time on all doors set to 5 seconds
Log RTE events = on
Log door schedule events = on

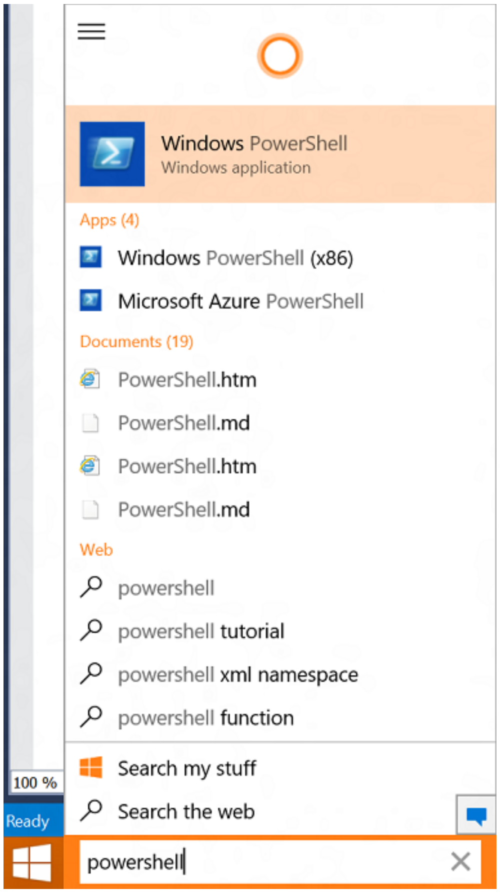
Anti-tailgating, doors 1 - 8 = on
Strip leading zeros, readers 1 - 8 = on
Door unlock schedules all set to None
First person in feature on all doors set to Off
Touch screen password set to nothing, touch screen lock turned off
Sets up 26-bit and Highpower 37 bit card formats on all controllers and deletes all other formats.

Powershell Remoting

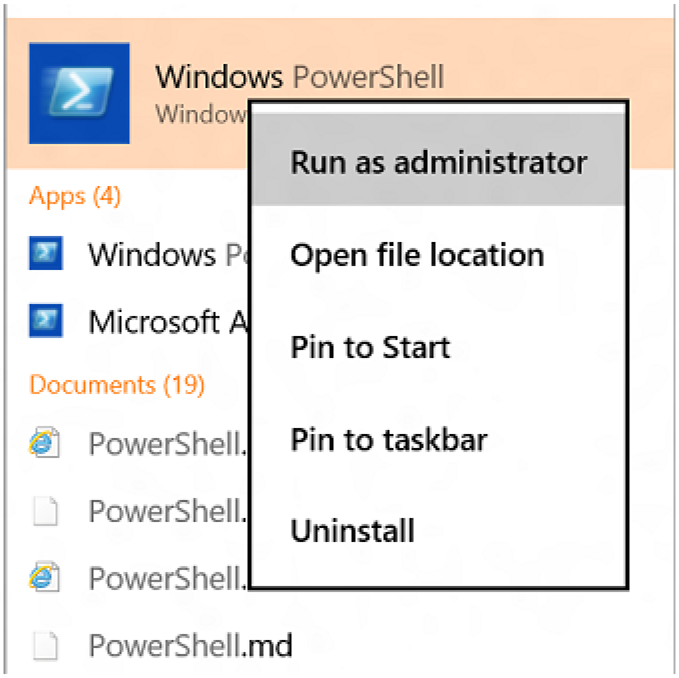
The controller allows an administrator to connect to it remotely over the LAN using Powershell. Powershell remoting allows an administrator to perform low level administration of the device in a similar way to a Windows 10 PC. The Powershell remoting function will provide a low-level command shell that can be helpful during upgrades and other low-level functions including advanced network settings. **Please use this feature cautiously and under factory advisement as bad commands can mess up the controller's software configuration.**

Connecting with Powershell

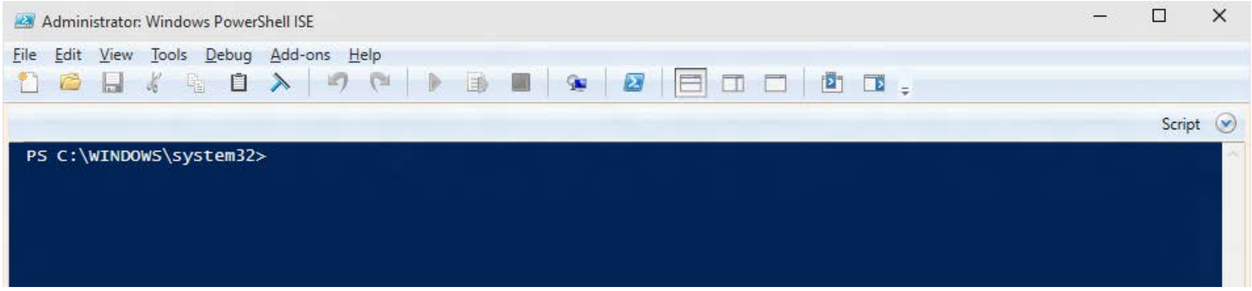
Start Powershell from Windows 10 as Administrator:



Right click on the PowerShell entry and select “Run as Administrator”



The Powershell console should come up:


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script

```
PS C:\WINDOWS\system32>
```

Enter the following commands:

```
net start WinRM
```

(starts the Windows remote management service if not running)

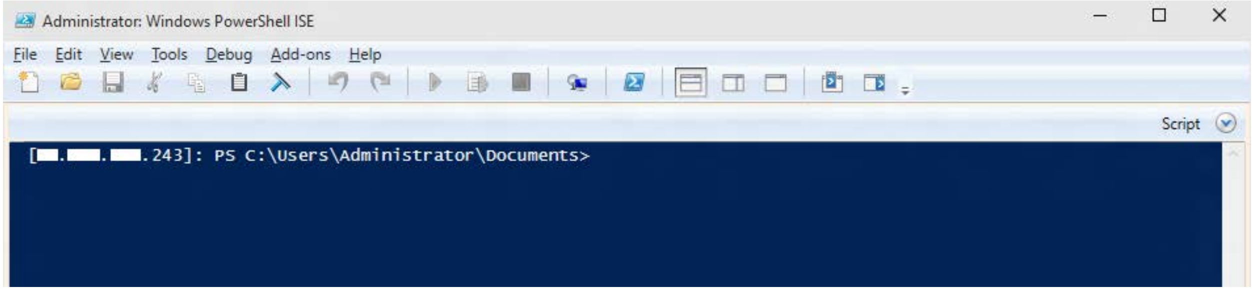
```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value <machine-name or IP Address>
```

(replace the machine-name or IP Address with the name of your controller similar to hp1_xxxxx)

```
Enter-PSSession -ComputerName <machine-name or IP Address> -Credential <machine-name or IP Address or localhost>\Administrator
```

(replace the machine-name or IP Address with the name of your controller similar to hp1_xxxxx)
(this connection step could take up to 30 seconds)

If the connection is successful to the controller, you should see the IP address of your device before the prompt.


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script

```
[[redacted].[redacted].[redacted].243]: PS C:\Users\Administrator\Documents>
```

Unified Write Filter

The Unified Write Filter is a Windows mechanism that protects the system data on your SD card. You can think of this system almost as a write-protection mechanism for changes that may have been done. These changes included major system settings like force setting IP addresses and other system level settings. In order to make system level settings to the controller, you first will need to temporarily deactivate the Unified Write Filter feature. You do this from the Powershell command line with the following command:

uwfmgr.exe filter disable

You must then reboot the controller before continuing with the following command:

restart /r /t 0

Once this feature is disabled, you can then make system changes including changing time zone settings, login settings, forced network settings and other system level settings. If you do not turn off the filter before making the changes, the system changes will only be temporary. Not turning off the filter will cause the system to default back to the last configuration on the next power cycle.

After making these changes, you should turn on the Unified Write Filter, as it protects the boot environment of the controller as the controller boots off of an SD card. This software feature prevents damage to data on the SD card if there is an un-intended power-down situation. This software feature is used to harden Windows based hardware devices that run on SD cards, such as this controller. After making your system level changes, turn the Unified Write Filter back on with the following command:

uwfmgr.exe filter enable

After issuing this command, you need to reboot the controller for the filter to take effect:

restart /r /t 0

Changing the Administrative Password via Powershell

First follow the procedure above to disable the Unified Write Filter (software write-protect).

Once remoted with Powershell, to change the Administrative password of the controller:

```
net user Administrator [new password]
```

(fill in the field for [new password] with your new password)

After making the changes, turn the Unified Write Filter back on.

Changing the Machine Name via Powershell

The factory recommends that you don’t change the machine name unless necessary because it could make remote technical support from the factory more difficult. Despite this you can use PowerShell to change the network name of the controller.

First follow the procedure above to disable the Unified Write Filter (software write-protect).

Using the following command to change the computer name:

```
setcomputername <new-name>
```

(where new-name is the new name for the controller)

After renaming the device you will need to restart the controller for the change to take effect:

```
shutdown /r /t 0
```

After making the changes, turn the Unified Write Filter back on.

Changing the Time zone via Powershell

You must set the time zone in the controller if you are using the controller with the Internet Time setting enabled.

First follow the procedure above to disable the Unified Write Filter (software write-protect).

Secondly, to set the time zone:

```
Set-TimeZone "Eastern Standard Time"
```

(Replace ‘Eastern Standard Time’ with the Windows name of your time zone)

Available time zone names (omit any notes in parentheses from the name):

Australian Central Daylight Savings Time	UTC+10:30
Australian Central Standard Time	UTC+09:30
Acre Time	UTC−05
ASEAN Common Time	UTC+06:30 – UTC+09
Australian Central Western Standard Time (unofficial)	UTC+08:45
Atlantic Daylight Time	UTC−03
Australian Eastern Daylight Savings Time	UTC+11
Australian Eastern Standard Time	UTC+10

Afghanistan Time	UTC+04:30
Alaska Daylight Time	UTC−08
Alaska Standard Time	UTC−09
Amazon Summer Time (Brazil)[1]	UTC−03
Amazon Time (Brazil)[2]	UTC−04
Armenia Time	UTC+04
Argentina Time	UTC−03
Arabia Standard Time	UTC+03
Atlantic Standard Time	UTC−04
Australian Western Standard Time	UTC+08
Azores Summer Time	UTC±00
Azores Standard Time	UTC−01
Azerbaijan Time	UTC+04
Brunei Time	UTC+08
British Indian Ocean Time	UTC+06
Baker Island Time	UTC−12
Bolivia Time	UTC−04
Brasília Summer Time	UTC−02
Brasilia Time	UTC−03
Bangladesh Standard Time	UTC+06
Bougainville Standard Time[3]	UTC+11
British Summer Time (British Standard Time from Feb 1968 to Oct 1971)	UTC+01
Bhutan Time	UTC+06
Central Africa Time	UTC+02
Cocos Islands Time	UTC+06:30
Central Daylight Time (North America)	UTC−05
Cuba Daylight Time[4]	UTC−04
Central European Summer Time (Cf. HAEC)	UTC+02
Central European Time	UTC+01
Chatham Daylight Time	UTC+13:45
Chatham Standard Time	UTC+12:45
Choibalsan Standard Time	UTC+08

Choibalsan Summer Time	UTC+09
Chamorro Standard Time	UTC+10
Chuuk Time	UTC+10
Clipperton Island Standard Time	UTC−08
Central Indonesia Time	UTC+08
Cook Island Time	UTC−10
Chile Summer Time	UTC−03
Chile Standard Time	UTC−04
Colombia Summer Time	UTC−04
Colombia Time	UTC−05
Central Standard Time (North America)	UTC−06
China Standard Time	UTC+08
Australian Central Standard Time	UTC+09:30
Australian Central Daylight Time	UTC+10:30
Cuba Standard Time	UTC−05
China time	UTC+08
Cape Verde Time	UTC−01
Central Western Standard Time (Australia) unofficial	UTC+08:45
Christmas Island Time	UTC+07
Davis Time	UTC+07
Dumont d'Urville Time	UTC+10
AIX-specific equivalent of Central European Time[5]	UTC+01
Easter Island Summer Time	UTC−05
Easter Island Standard Time	UTC−06
East Africa Time	UTC+03
Eastern Caribbean Time (does not recognize DST)	UTC−04
Ecuador Time	UTC−05
Eastern Daylight Time (North America)	UTC−04
Australian Eastern Summer Time	UTC+11
Eastern European Summer Time	UTC+03
Eastern European Time	UTC+02
Eastern Greenland Summer Time	UTC±00
Eastern Greenland Time	UTC−01

Eastern Indonesian Time	UTC+09
Eastern Standard Time (North America)	UTC−05
Australian Eastern Standard Time	UTC+10
Further-eastern European Time	UTC+03
Fiji Time	UTC+12
Falkland Islands Summer Time	UTC−03
Falkland Islands Time	UTC−04
Fernando de Noronha Time	UTC−02
Galápagos Time	UTC−06
Gambier Islands Time	UTC−09
Georgia Standard Time	UTC+04
French Guiana Time	UTC−03
Gilbert Island Time	UTC+12
Gambier Island Time	UTC−09
Greenwich Mean Time	UTC±00
South Georgia and the South Sandwich Islands Time	UTC−02
Gulf Standard Time	UTC+04
Guyana Time	UTC−04
Hawaii–Aleutian Daylight Time	UTC−09
Heure Avancée d'Europe Centrale French-language name for CEST	UTC+02
Hawaii–Aleutian Standard Time	UTC−10
Hong Kong Time	UTC+08
Heard and McDonald Islands Time	UTC+05
Khovd Summer Time	UTC+08
Khovd Standard Time	UTC+07
Indochina Time	UTC+07
Israel Daylight Time	UTC+03
Indian Ocean Time	UTC+03
Iran Daylight Time	UTC+04:30
Irkutsk Time	UTC+08
Iran Standard Time	UTC+03:30
Indian Standard Time	UTC+05:30

Irish Standard Time[6]	UTC+01
Israel Standard Time	UTC+02
Japan Standard Time	UTC+09
Kyrgyzstan Time	UTC+06
Kosrae Time	UTC+11
Krasnoyarsk Time	UTC+07
Korea Standard Time	UTC+09
Lord Howe Standard Time	UTC+10:30
Lord Howe Summer Time	UTC+11
Line Islands Time	UTC+14
Magadan Time	UTC+12
Marquesas Islands Time	UTC−09:30
Mawson Station Time	UTC+05
Mountain Daylight Time (North America)	UTC−06
Middle European Time Same zone as CET	UTC+01
Middle European Summer Time Same zone as CEST	UTC+02
Marshall Islands Time	UTC+12
Macquarie Island Station Time	UTC+11
Marquesas Islands Time	UTC−09:30
Myanmar Standard Time	UTC+06:30
Moscow Time	UTC+03
Malaysia Standard Time	UTC+08
Mountain Standard Time (North America)	UTC−07
Mauritius Time	UTC+04
Maldives Time	UTC+05
Malaysia Time	UTC+08
New Caledonia Time	UTC+11
Newfoundland Daylight Time	UTC−02:30
Norfolk Island Time	UTC+11
Nepal Time	UTC+05:45
Newfoundland Standard Time	UTC−03:30
Newfoundland Time	UTC−03:30
Niue Time	UTC−11

New Zealand Daylight Time	UTC+13
New Zealand Standard Time	UTC+12
Omsk Time	UTC+06
Oral Time	UTC+05
Pacific Daylight Time (North America)	UTC−07
Peru Time	UTC−05
Kamchatka Time	UTC+12
Papua New Guinea Time	UTC+10
Phoenix Island Time	UTC+13
Philippine Time	UTC+08
Pakistan Standard Time	UTC+05
Saint Pierre and Miquelon Daylight Time	UTC−02
Saint Pierre and Miquelon Standard Time	UTC−03
Pohnpei Standard Time	UTC+11
Pacific Standard Time (North America)	UTC−08
Philippine Standard Time	UTC+08
Paraguay Summer Time[7]	UTC−03
Paraguay Time[8]	UTC−04
Réunion Time	UTC+04
Rothera Research Station Time	UTC−03
Sakhalin Island Time	UTC+11
Samara Time	UTC+04
South African Standard Time	UTC+02
Solomon Islands Time	UTC+11
Seychelles Time	UTC+04
Samoa Daylight Time	UTC−10
Singapore Time	UTC+08
Sri Lanka Standard Time	UTC+05:30
Srednekolymsk Time	UTC+11
Suriname Time	UTC−03
Samoa Standard Time	UTC−11
Singapore Standard Time	UTC+08
Showa Station Time	UTC+03

Tahiti Time	UTC−10
Thailand Standard Time	UTC+07
Indian/Kerguelen	UTC+05
Tajikistan Time	UTC+05
Tokelau Time	UTC+13
Timor Leste Time	UTC+09
Turkmenistan Time	UTC+05
Turkey Time	UTC+03
Tonga Time	UTC+13
Tuvalu Time	UTC+12
Ulaanbaatar Summer Time	UTC+09
Ulaanbaatar Standard Time	UTC+08
Kaliningrad Time	UTC+02
Coordinated Universal Time	UTC±00
Uruguay Summer Time	UTC−02
Uruguay Standard Time	UTC−03
Uzbekistan Time	UTC+05
Venezuelan Standard Time	UTC−04
Vladivostok Time	UTC+10
Volgograd Time	UTC+04
Vostok Station Time	UTC+06
Vanuatu Time	UTC+11
Wake Island Time	UTC+12
West Africa Summer Time	UTC+02
West Africa Time	UTC+01
Western European Summer Time	UTC+01
Western European Time	UTC±00
Western Indonesian Time	UTC+07
Western Standard Time	UTC+08
Yakutsk Time	UTC+09
Yekaterinburg Time	UTC+05

After setting the time zone, turn the Unified Write Filter back on.

Managing Known Networks

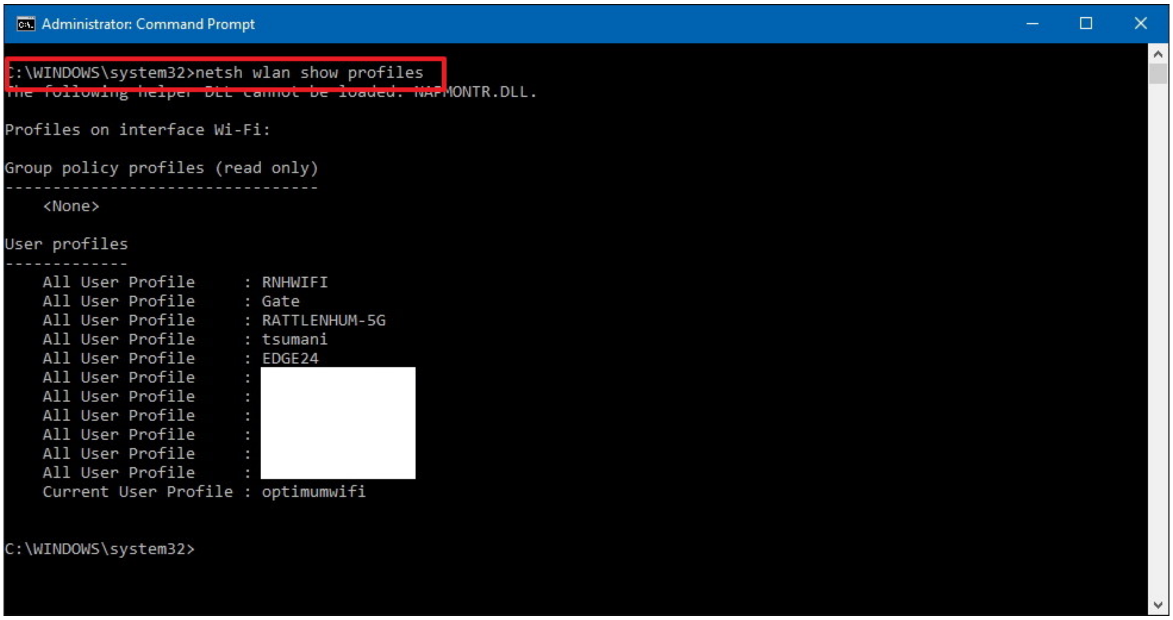
The Windows 10 operating system on the One keeps a list of Wi-Fi networks that it has connected to in the past with the network credentials so that it can automatically reconnect to the networks after a restart. Each entry in this list is called a “profile”. If you need to remove or manage profiles, you can do this via powershell via the NETSH command. The following information is provided from https://www.windowscentral.com/how-manage-wireless-networks-using-command-prompt-windows-10:

View wireless network profiles saved on your PC

Every time you connect to a wireless access point, the operating system creates a "wireless network profile", and it's stored on your computer, you can view all these profiles using the following command line on the Command Prompt:

```
Netsh WLAN show profiles
```

On the list, which you can see in the screenshot, shows all the profiles stored on your computer for every wireless adapter and which users have the right to connect using those profiles.

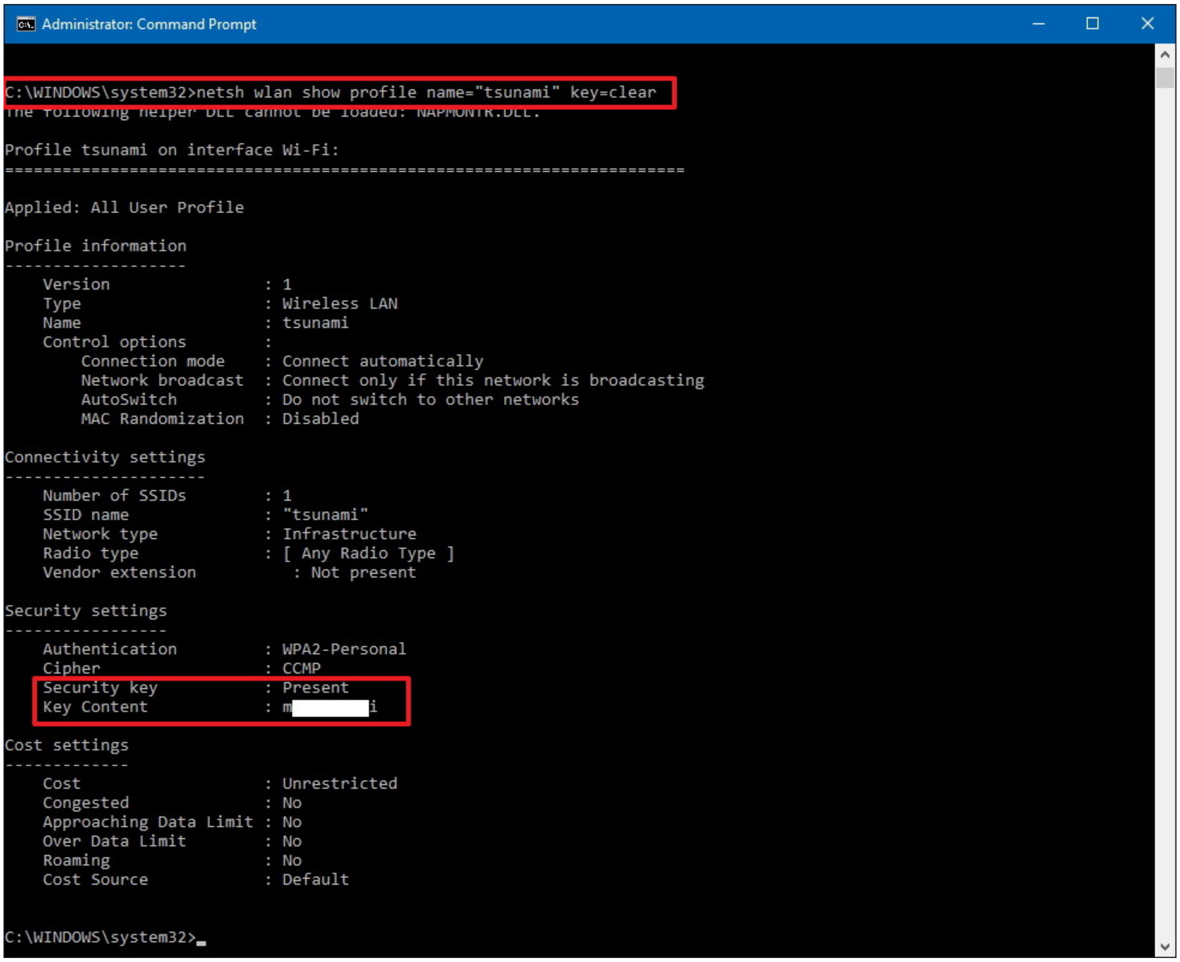


```
C:\WINDOWS\system32>netsh wlan show profiles
The following helper DLL cannot be loaded: NAPMONTR.DLL.

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : RNHWIFI
    All User Profile     : Gate
    All User Profile     : RATTLENHUM-5G
    All User Profile     : tsumani
    All User Profile     : EDGE24
    All User Profile     : [redacted]
    All User Profile     :
    All User Profile     :
    All User Profile     :
    All User Profile     :
    All User Profile     :
    Current User Profile : optimumwifi


C:\WINDOWS\system32>
```

Recover network security key from any wireless profile stored

If you lost and cannot remember your network security key to connect another device to a particular Wi-Fi access point, you can use the following command to view your network security key:

```
Netsh WLAN show profile name="Profile_Name" key=clear
```



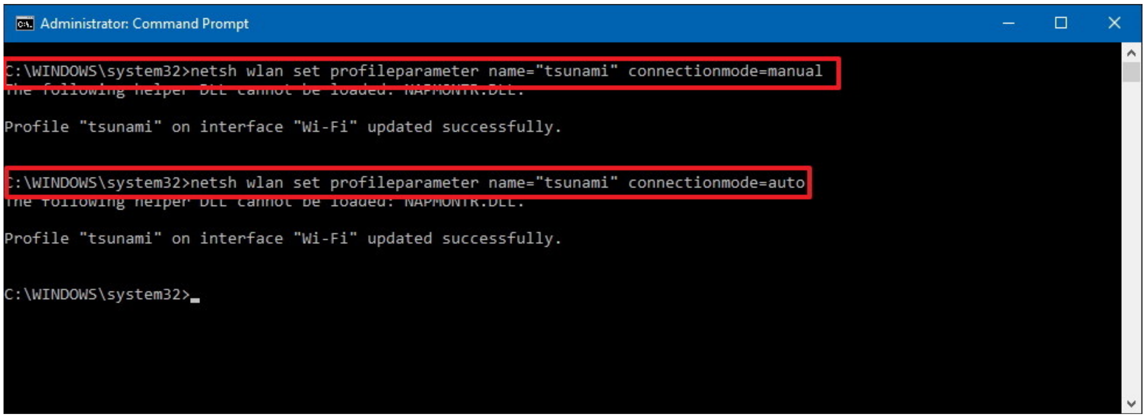
```
C:\WINDOWS\system32>netsh wlan show profile name="tsunami" key=clear
The following helper DLL cannot be loaded: NAPMONTR.DLL.

Profile tsunami on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : tsunami
    Control options        :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "tsunami"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Security key           : Present
    Key Content            : [redacted]

Cost settings
-------------
    Cost                   : Unrestricted
    Congested              : No
    Approaching Data Limit : No
    Over Data Limit        : No
    Roaming                : No
    Cost Source            : Default


C:\WINDOWS\system32>_
```

Keep in mind that you can view your current network security key through the wireless adapter properties in Control Panel. However, you can use this command to recover any network security key of any profile stored on your computer.

Stop connecting automatically to a wireless network out of range

Sometimes, you have your Windows 10 PC configured to connect to different wireless networks automatically, but then you realize that your device always connects to the access point that offers poor connectivity, or your device tries to connect to a network that is out of range. For those cases, you can use the following command to prevent your computer from connecting to different networks automatically:

```
Netsh WLAN set profileparameter name="Profile_Name"
connectionmode=manual
```



```
C:\WINDOWS\system32>netsh wlan set profileparameter name="tsunami" connectionmode=manual
The following helper DLL cannot be loaded: NAPMONTR.DLL.

Profile "tsunami" on interface "Wi-Fi" updated successfully.

C:\WINDOWS\system32>netsh wlan set profileparameter name="tsunami" connectionmode=auto
The following helper DLL cannot be loaded: NAPMONTR.DLL.

Profile "tsunami" on interface "Wi-Fi" updated successfully.


C:\WINDOWS\system32>_
```

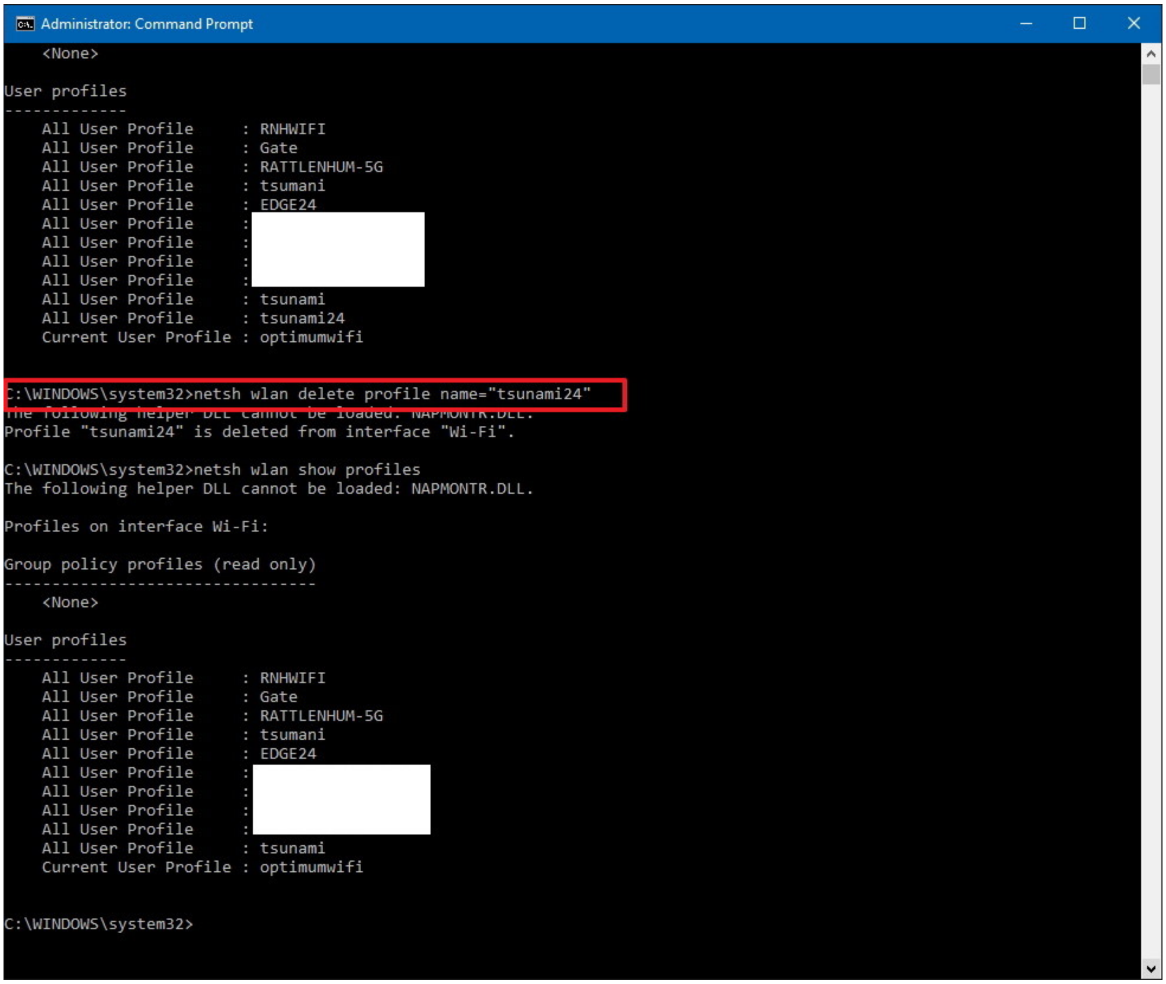
It's important to note that Windows 10 will always make a priority those networks you choose to connect automatically. If you want to move up a network in the list of precedence, you can use the following command:

```
Netsh WLAN set profileparameter name=" Profile_Name"
connectionmode=auto
```

Delete wireless network profiles stored on your PC

When you no longer need to connect to a certain wireless network, the access point is no longer available, or you need to reset the network profile settings, you can also use Netsh WLAN to delete any profile stored on your computer using the following command:

```
Netsh WLAN delete profile name="Profile_Name"
```



```
Administrator: Command Prompt
    <None>

User profiles
-------------
    All User Profile     : RNHWIFI
    All User Profile     : Gate
    All User Profile     : RATTLENHUM-5G
    All User Profile     : tsumani
    All User Profile     : EDGE24
    All User Profile     : [redacted]
    All User Profile     :
    All User Profile     :
    All User Profile     :
    All User Profile     : tsunami
    All User Profile     : tsunami24
    Current User Profile : optimumwifi


C:\WINDOWS\system32>netsh wlan delete profile name="tsunami24"
The following helper DLL cannot be loaded: NAPMONTR.DLL.
Profile "tsunami24" is deleted from interface "Wi-Fi".

C:\WINDOWS\system32>netsh wlan show profiles
The following helper DLL cannot be loaded: NAPMONTR.DLL.

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : RNHWIFI
    All User Profile     : Gate
    All User Profile     : RATTLENHUM-5G
    All User Profile     : tsumani
    All User Profile     : EDGE24
    All User Profile     : [redacted]
    All User Profile     :
    All User Profile     :
    All User Profile     :
    All User Profile     : tsunami
    Current User Profile : optimumwifi


C:\WINDOWS\system32>
```

If you can't remember the name of the network profile, you can use the `Netsh WLAN show profiles` command to list all the available profiles.

Additional Hardware Configuration

Hardware Setup via Web Interface

The controller has a convenient web interface for configuring hardware details located at Ethernet port 8080.

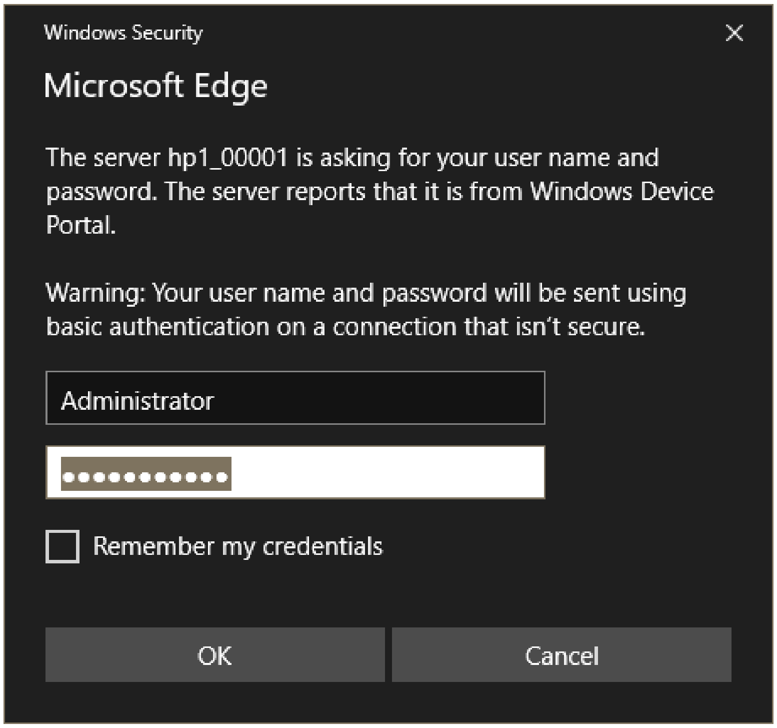
Before making any changes with the web interface, you need to turn off the Unified Write Filter (software-based write-protection) feature using the procedure in the Powershell remoting section).

Once the controller is connected to your LAN, to access this interface, open any web browser on a computer on the LAN and enter the address:

Hp1_xxxxx:8080 where xxxxx is the serial number of your controller

After entering this address in the address line of the browser press enter. The browser should prompt you for connection to the controller asking for a username and password.

In Edge browser:



Windows Security

Microsoft Edge

The server hp1_00001 is asking for your user name and password. The server reports that it is from Windows Device Portal.

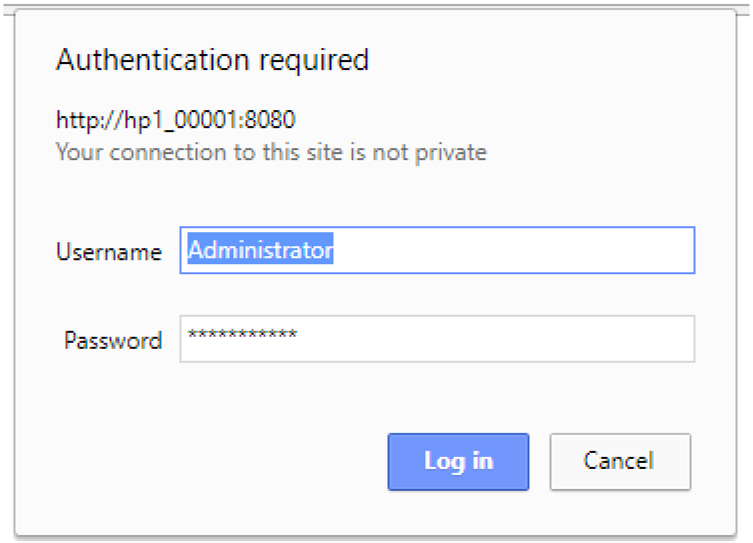
Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

Administrator

●●●●●●●●●●●

□ Remember my credentials

In the Chrome browser:



Authentication required

http://hp1_00001:8080
Your connection to this site is not private

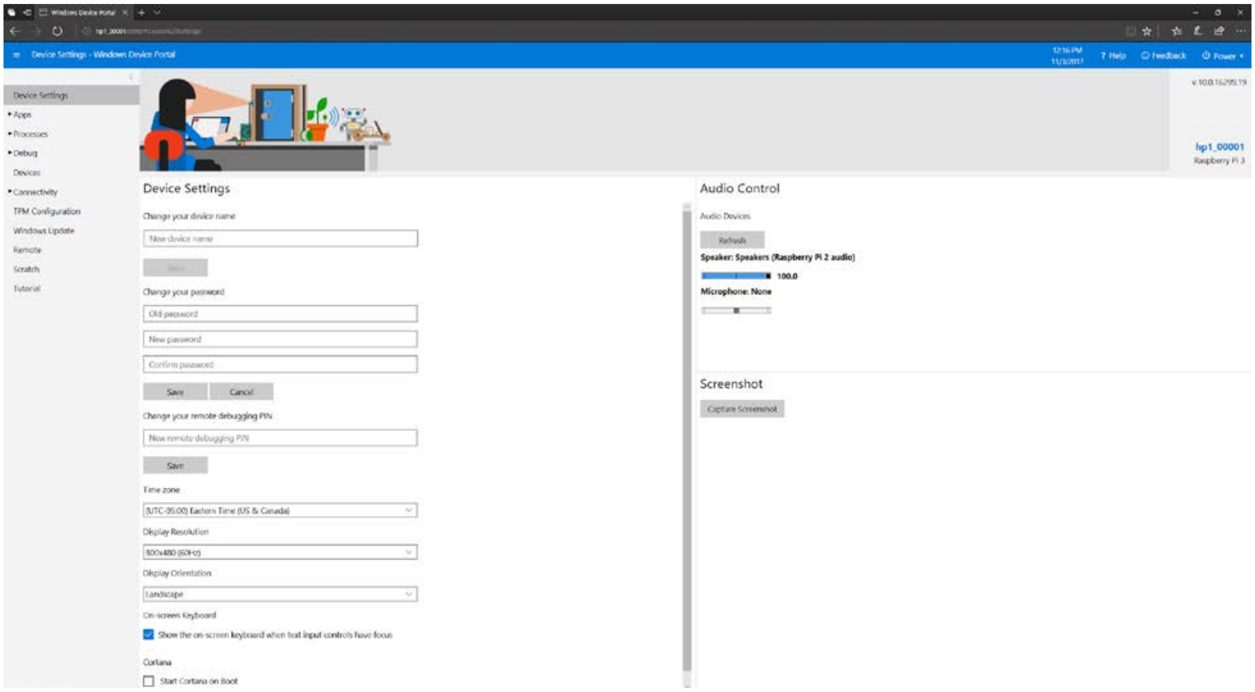
Username: Administrator

Password: ***********

By default, the factory login is the following:
User name = Administrator
Password = password12!

YOU WILL NEED TO CHANGE THIS LOGIN AND PASSWORD to secure the controller. This controller has Windows 10 running on it and all the standard Windows security models should be observed.

Once you enter this credential information, you will be presented with tools to manage the controller. These tools are called the Windows Device Portal:



Device Settings

Change your device name

New device name

Change your password

Old password

New password

Confirm password

Change your remote debugging PIN

New remote debugging PIN

Time zone: (UTC-05:00) Eastern Time (US & Canada)

Display Resolution: 800x480 (60Hz)

Display Orientation: Landscape

On-screen Keyboard

☑ Show the on-screen keyboard when text input controls have focus

Cortana

☐ Start Cortana on Boot

Audio Control

Audio Devices

Speaker: Speakers (Raspberry Pi 2 audio)

100.0

Microphone: None

Screenshot

There are only a few controls that you will want to change as other control settings are critical to the proper operation of the controller. The first selection on the left menu is called “Device Settings” This entry will allow you to quickly change the device password and set the time zone of the device if you are using the internet clock.

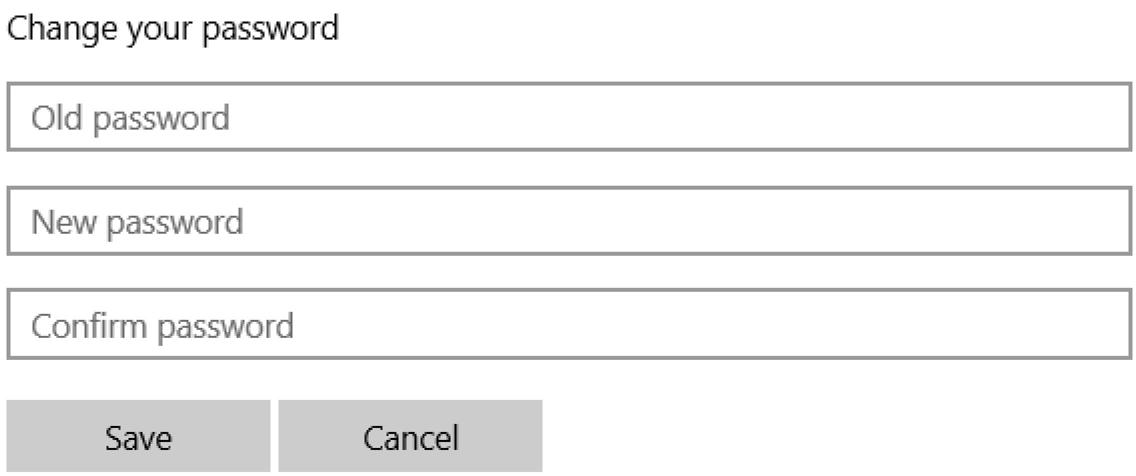
Once these settings are adjusted, turn back on the Unified Write Filter, using the procedure in the Powershell remoting section above.

Changing the Administrative Password

If you are running the controller on a LAN using the Highpower HMS software, you will want to change the default login password for the device. The Device Settings screen has a facility to do this.

Before making any changes with the web interface, you need to turn off the Unified Write Filter (software-based write-protection) feature using the procedure in the Powershell remoting section).

There is a section on the Device Settings screen that looks like the following:



Complete the fields and then click Save to update your new password.

Once these settings are adjusted, turn back on the Unified Write Filter, using the procedure in the Powershell remoting section above.

Changing the Time Zone

In the Device Setting screen, you can configure the time zone settings of the controller. The time zone is used to calculate the correct time if you are using the device with the Internet Time Clock selected. Pull down the selection box and select the appropriate time zone.

Watchdog Timer

Description

The controller has a hardware watchdog circuit that is designed to monitor and reset the controller's main software system if the system locks up. After two minutes, if the software suite not refresh the timer, the controller will reboot itself. This watchdog timer is useful if the system experiences some sort of unusual hardware condition such as a brown out condition in the power supply. This monitoring feature helps the controller come back online on its own especially in situations where the controller is remote.

This watchdog system needs to be temporarily disabled in the case where the factory is doing a remote software upgrade. There are three ways to temporarily disable the watchdog for remote upgrades.

Temporarily disabling the watchdog feature

Disabling the watchdog feature should only be done under factory advisement. There are three ways to disable the hardware watchdog. The watchdog must be disabled during remote software upgrades as the running Highpower application on the controller is what prevents the timer from triggering a reset.

The easiest method is to go into the configuration screen in the controller. In this screen there is a button that can temporarily disable the watchdog timer and then enable it. This feature can obviously only be used when the main controller application is running.

The watchdog timer can also be disabled and enabled remotely for remote software updates. There is a command in the command set to accomplish this. Using a terminal program, connecting to port 3000 and offering the appropriate command will control the watchdog state.

Lastly, if the controller’s application is damaged and can't run (caused for example by loss of power during a previous software upgrade) you can disable the watchdog mechanically without using the onboard software application. Shunting the Request to Exit (RTE) terminal on reader port 8 during power up will disable the watchdog timer.

The watchdog will automatically be turned back on when the power in the controller is cycled. The controller does not store the state of the watchdog timer in a non-volatile way.

Watchdog timer led response

There are two LEDs in the upper left corner of the controller that indicates the status of the watchdog.

A green LED illuminated at the upper left corner of the controller's circuit board along with an extinguished red LED indicates that the controller is in a normal running state. The watchdog is checking the system and an automatic reboot will occur if the application freezes.

An extinguished green led with an illuminated red LED indicated that the controller is in a reset state. In this state, the controller will keep getting reset automatically every two minutes unless the application comes up and starts refreshing the watchdog. Once the application comes back online, it will start refreshing the watchdog timer and the controller will return to a ready state.

When both green and red LEDs are illuminated, the controller is indicating that the watchdog feature has been temporarily disabled. The watchdog will stay disabled until either the user re-enables the watchdog via the screen or by command, or if the controller is power cycled.

USB Ports

The controller has four USB ports available. These ports can accept standard USB accessories like keyboard, mice, memory sticks and certain additional types of network adapters. The memory stick is especially useful as you can use the memory stick for system backups, audit trail retrieval and additional system storage space.

If you install a keyboard one of these ports, a mechanical keyboard can be used in place of the smaller on-screen keyboard.

Plugging a mouse into one of these ports causes a mouse pointer to appear on screen that can be used in place of tapping on touch screen controls.

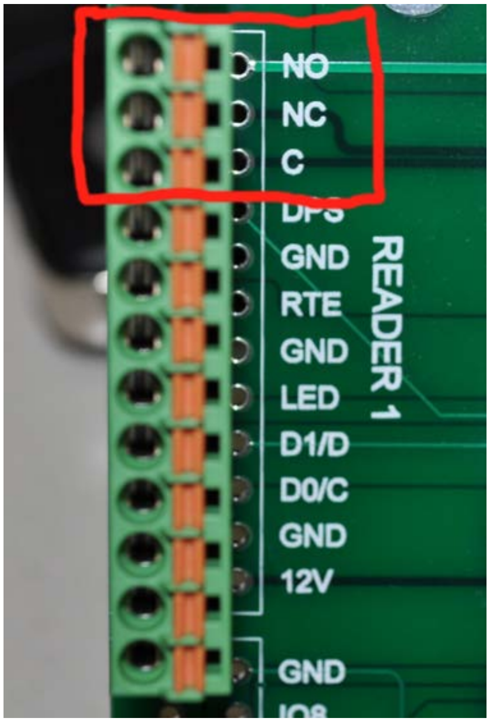
Properly powering the controller

Powering the controller properly is very important. This controller has powerful but very sensitive electronics packaged into it including touch screen controllers and single board computers with SD cards. When powering the controller, **it is critical that you do not use a common power supply for both the controller and the locking hardware.** It’s tempting in some installations to use one 12-volt power supply to power both the controller and locks such as electric strikes and electromagnetic locks based on the availability of high voltage power. **Don't do it.** Electromagnetic locks and electric strikes have solenoids that produce large inductive reverse electrical surges when they are depowered. Most manufactures include surge suppressors in these devices in order to reduce this reverse kickback. **Initially, you may find that using a common supply does not affect the operation of the controller. As the surge suppressors in the locks start to experience repeated discharge cycles with every card swipe, they will over time either become less effective or will stop working completely, long before the lock fails.** This electrical condition, when the power supply is also connected in common with the controller's input voltage, will cause damage to the controller's electronics due to the large reverse negative polarity kickbacks. We have added some surge suppressors and noise suppressors to the power supply input of the controller, but we cannot guaranty that these filters will be effective in untested conditions. **Using a common power supply to both the controller and the lock hardware voids the factory warranty.** We recommend using the power supply that is furnished with the controller for proper operation. This is a tested plug in wall transformer with a filtered 12V DC output which connects to the barrel connector on the controller board. In cases where you can't use the supplied plug in transformer or you don't want to take our recommendations and think we are full of it and that you know more than we do on this issue, we have provided an additional power supply terminal block for connection of an external 12V DC supply. If you decide to use your own supply, make sure that it's filtered and free from electrical noise and provides at least 2000mA of regulated 12V power. This excludes many cheaply made commonly available switching supplies from many popular manufacturers in the security industry that you probably have readily available. **The factory cannot guaranty the performance of the controller when you use your own power supply.**

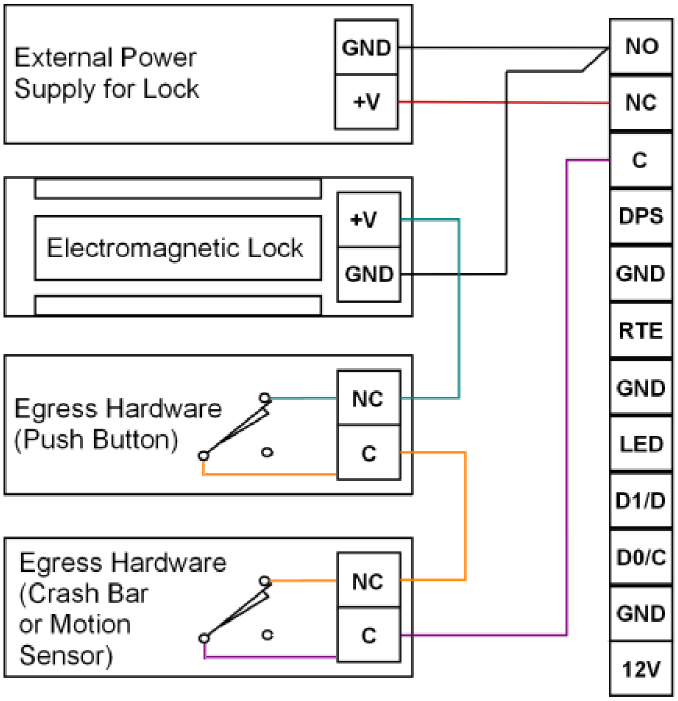
Electrical Connections

Relay outputs

The relay outputs on the controller are rated for a maximum 5 Amps 24V DC power. They can be used to switch lock power directly. There is one relay for each door, eight in total. The COMMON, NORMALLY OPEN, and NORMALLY CLOSED relay connections are located at the top of each door terminal block and are labelled C, NO and NC. The relay output contacts have MOV surge suppressors across the contact which limit the controlled voltage on each contact to 24V. Despite the presence of these surge suppressors, additional MOVs should be installed on devices that have inductive loads like electric strikes and electromagnetic locks at these devices.

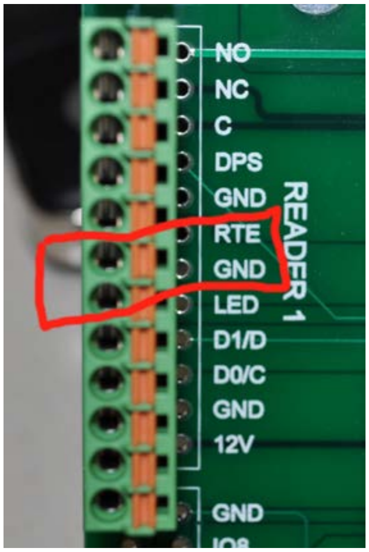


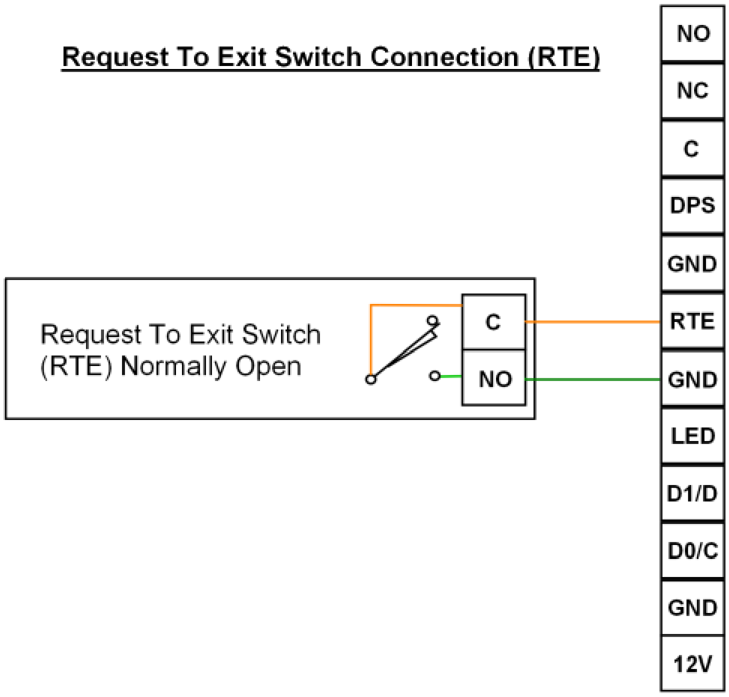
Simple Fail Safe Lock Configuration


External Power Supply for Lock
GND
+V
Electromagnetic Lock
+V
GND
Egress Hardware (Push Button)
NC
C
Egress Hardware (Crash Bar or Motion Sensor)
NC
C
NO
NC
C
DPS
GND
RTE
GND
LED
D1/D
D0/C
GND
12V

Request to Exit Inputs

There is a request to exit input for each door. The request to exit input causes the controller to trigger the door unlock cycle. The door unlock cycle time starts when the request to exit signal is release. Typically this signal is a normally open contact connected between the RTE input and the adjacent ground terminal.

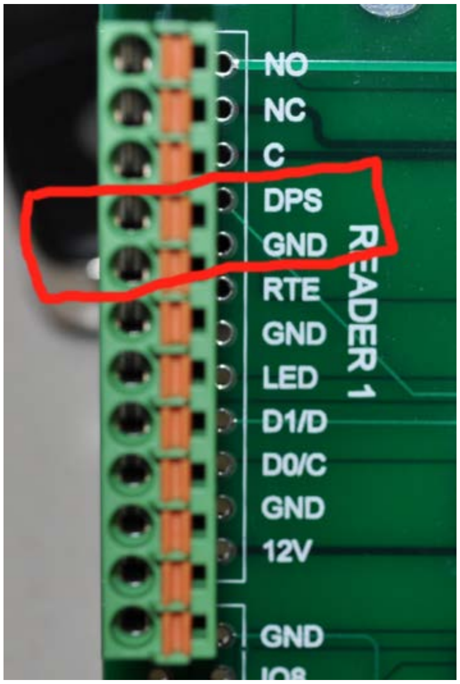




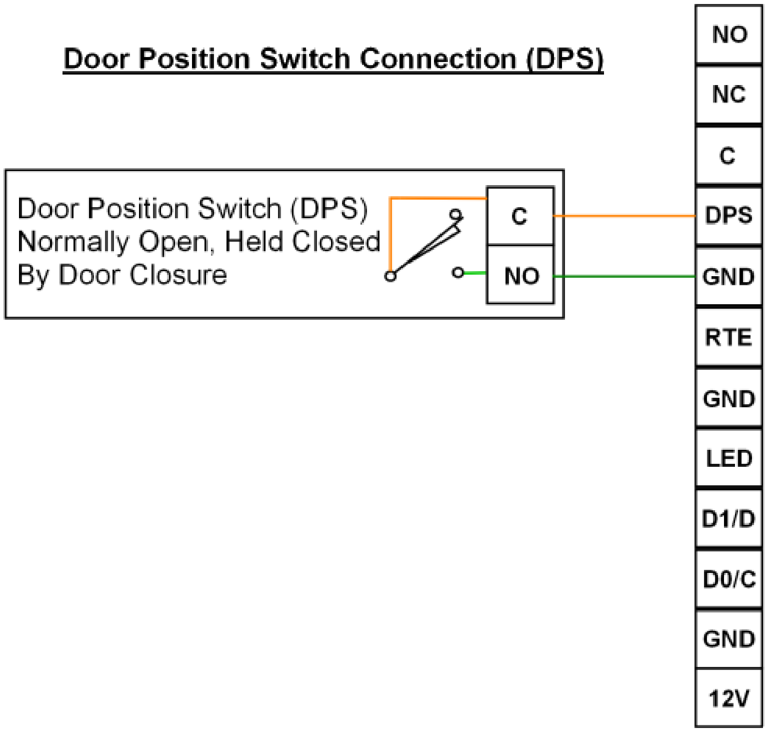
Door Position Switch Inputs

There is a Door Position Switch input for each door. This input is used to implement an anti-tailgating feature on the door. When a door is opened after a valid card entry, as soon as the door closes, the controller will lock the door immediately, overriding the existing unlock time. The door position switch input is also used to monitor the state of the door, open or closed, in the Highpower HMS software.

To use this input, connect a normally open-door position switch between the input and the adjacent ground terminal. The door when closed, will hold this contact closed.



Door Position Switch Connection (DPS)

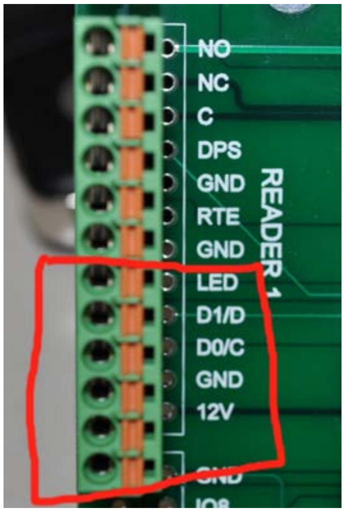


Door Position Switch (DPS)
Normally Open, Held Closed
By Door Closure

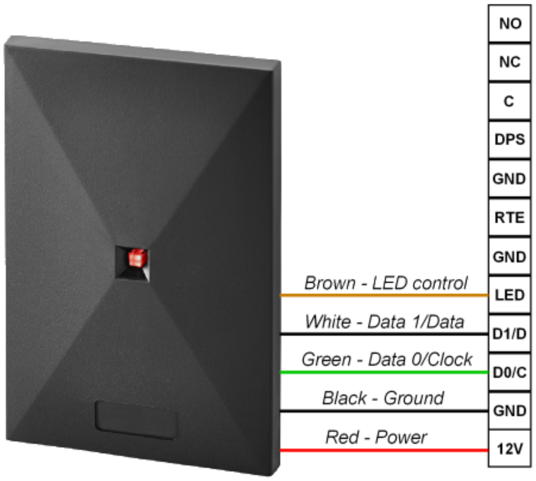
Reader inputs

There are eight independent reader inputs on the controller. These inputs can handle both Wiegand and ABA (magstripe emulation also known as clock & data) reader types. The controller will automatically discriminate between the two types of data and do the appropriate translation. In this initial version of the controller firmware you can use the Wiegand formats that are default from the factory or define your own formats. These formats include standard 26 Bit Wiegand and Highpower 37 bit.

The controller will also decode a full ABA input stream, but on the initial version there is no masking features yet available on the ABA interface which would allow you to restrict the card output to a specific number of characters. This is a feature that is planned for a future release of the firmware.

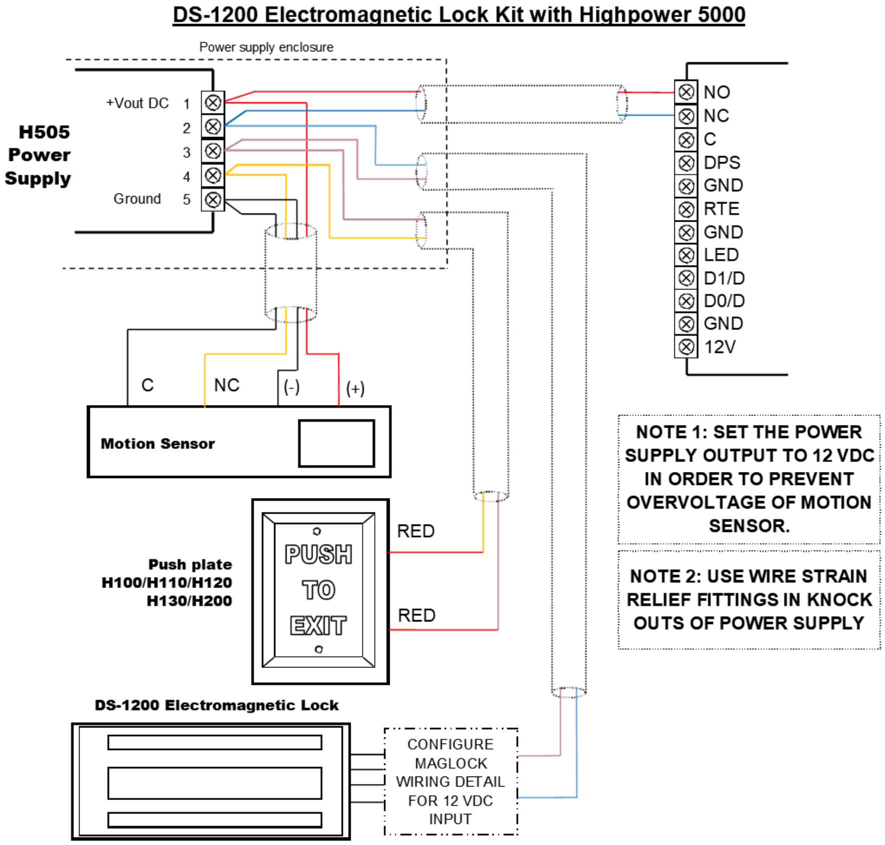


Wiegand or Magstripe Reader Connection



Don't connect the reader while the controller is powered.
Remove the terminal block when connecting the reader wires.

Typical Maglock System Connection Diagram


DS-1200 Electromagnetic Lock Kit with Highpower 5000
Power supply enclosure
H505 Power Supply
+Vout DC
Ground
1
2
3
4
5
NO
NC
C
DPS
GND
RTE
GND
LED
D1/D
D0/D
GND
12V
C
NC
(-)
(+)
Motion Sensor
Push plate H100/H110/H120 H130/H200
PUSH TO EXIT
RED
RED
DS-1200 Electromagnetic Lock
CONFIGURE MAGLOCK WIRING DETAIL FOR 12 VDC INPUT
NOTE 1: SET THE POWER SUPPLY OUTPUT TO 12 VDC IN ORDER TO PREVENT OVERVOLTAGE OF MOTION SENSOR.
NOTE 2: USE WIRE STRAIN RELIEF FITTINGS IN KNOCK OUTS OF POWER SUPPLY

Electrical Enclosure Notes

The electrical enclosure that houses the HighpowerOne main board and display has hinged door and the door is shipped from the factory on the left side. If you wish to change the location of the hinge or in order to accommodate different conduit entrance locations, you can re-orient the entire controller assembly inside the enclosure. This can be done before or after mounting. To do this remove four #8 sheet metal screws at the corners of the two mounting brackets. Rotate the controller board with display in 90 or 180-degree orientations. The holes in these brackets will line up with alternative fastening locations in the box at 90 and 180 degrees. Putting the hinged side of the controller on the top adds minor additional weather resistance. The box is purposely non-metallic, made from a UV rated material, so that the enclosure does not interfere with the wireless Wi-Fi feature on the controller.

Known Software Issues

There are no known issues at the time of release. There are enhancements planned to the firmware for the next release. To report any bug incidences detected, contact Highpower technical support at 203-634-3900.

Planned enhancements

Add the ability to control the first person in mode via touchscreen.

Warranty

Highpower products are warranted to the original buyer to be free from defects in materials and workmanship under normal use and service with proper maintenance for one year from the date of factory shipment. Highpower assumes no responsibility for products damaged by improper handling, misuse, neglect, modification, improper installation, improper voltage application, repair, alteration, electrical shorts or accident. This warranty is limited to the repair or replacement of the defective unit.

Using a common power supply to both the controller and the lock hardware voids the factory warranty. The factory cannot guaranty the performance of the controller when you use your own power supply. Using an unapproved power supply with the controller also voids the warranty.
ALWAYS use a separate power supply to power the controller from the one that is being used to power the locking hardware.

There are no expressed warranties other than those set forth herein. Warranty expressly excludes third party additions, deletions and or upgrades to this product. Highpower' s maximum liability under any circumstance shall be limited to the actual price paid for the product.

Firmware Revision History

V1.0.6659.21134 – 3/32/2018 Initial Release

General Specifications

· Eight-door Wiegand reader controller with eight Door Position Switch (DPS) inputs and eight Request-To-Exit (RTS) signal inputs.
· 7" capacitive touch screen for programming and diagnostics. Touchscreen can perform all functions that can be accomplished in software.
· Fast operation with ARM Cortex A53 processor running at 1.2 GHz.
· Replaceable SD Card storage for operating system and user data storage.
· Base memory configuration of over 25 million card storage entries and 10,000 entry audit trail.
· Virtually unlimited access levels, schedules and holidays.
· 100 Mb Ethernet with IPV6 for modern networks preventing IPV4 management issues.
· Onboard WIFI adapter for communicating with wireless networks.
· Expansion port and optional 16 signal I/O port for future capabilities including automation.
· Windows Powershell access for Windows PC type management.
· Four USB ports for connection of USB memory sticks, mouse, keyboard and high performance wireless networking adapters.
· Highpower HMS V5 networking software license included with hardware purchase.
· TCP/IP command port located at Port 3000 for access to the Highpower command set allowing integration into OEM software.