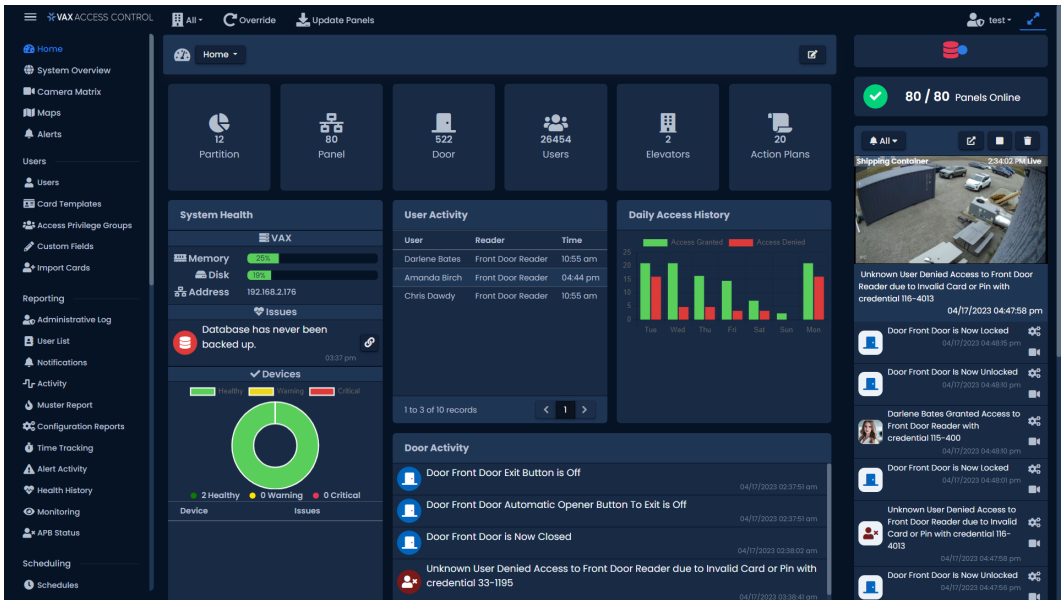
Quick Guide

VICON

VAX

Vicon Access Control System

XX274-10-00



Be sure to check Vicon's website to be see if you have the most [up-to-date software]

Document Number: 8009-8274-10-00 Rev: 10/23
Product specifications subject to change without notice

Vicon Industries Inc.
Tel: 631-952-2288) Fax: 631-951-2288
Toll Free: 800-645-9116
24-Hour Technical Support: 800-34-VICON
(800-348-4266)
UK: 44/(0) 1489-566300

Table of Contents

This is an abbreviated programming manual addressing basic program settings for a Vicon Access Control System (VAX). A complete User Guide can be found on Vicon website.

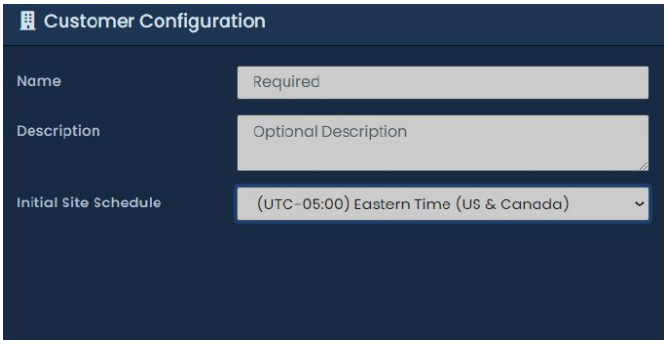
General

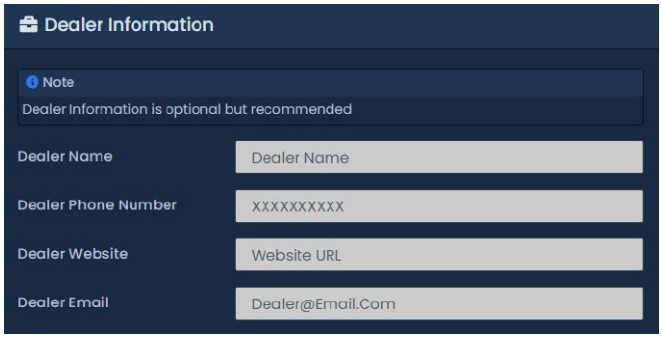
Vicon Access Control (VAX) is a modern HTML5 web-based client/server access control system. The server application is designed to be installed on a standalone PC and can be accessed using one or more clients via a web browser. The software can be used for system partitioning, to create different sites for buildings or areas, to create schedules for access times, to add multiple panels or door modules to the system and to create access privilege groups.

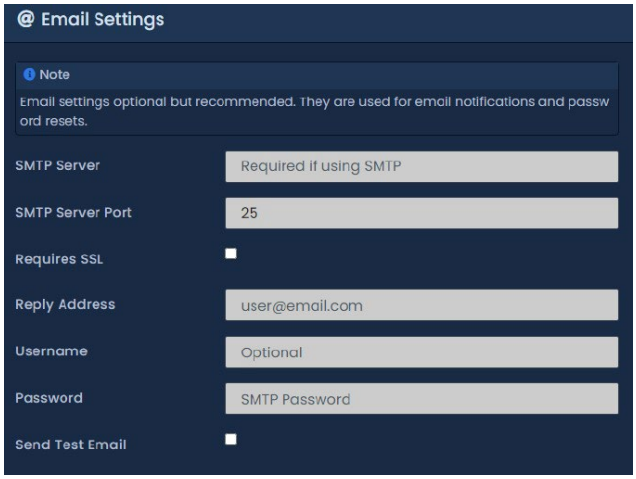
Initial Setup

Access the VAX server through the chosen browser and enter "https://VAX Server IP address:11001" in the URL bar. Proceed through any browser warnings; a splash screen will display, followed by the Initial Configuration wizard. This is broken up into four steps: EULA, Customer Configuration, Server Address and Initial Administrator.

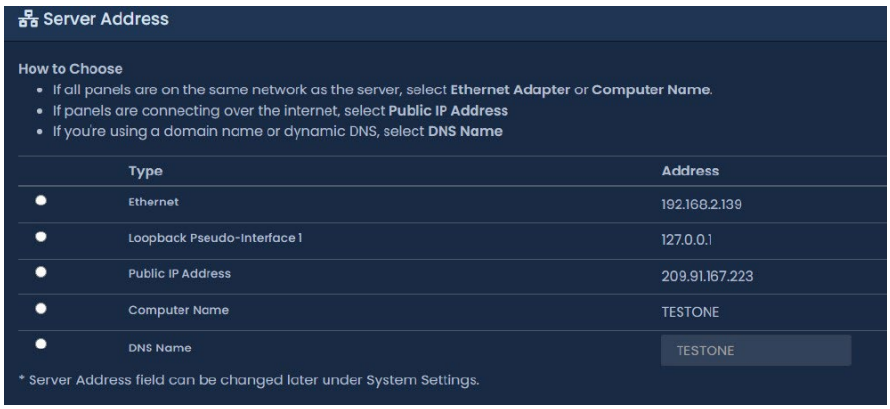
After accepting the EULA, fill out the customer and dealer information on the next pages. It is also recommended to set up an email for the purpose of password recovery.



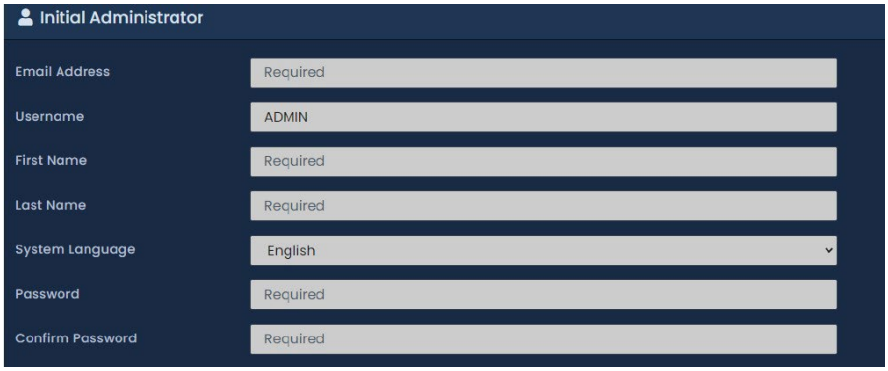




In the server address section, select the network interface the software will connect to. This interface requires a static address or a DHCP address.



At least one administrator account must be created for programming and managing the system. Additional administrator accounts can be added later. Permissions can be assigned to each administrator to delegate system management. Complete the initial administrator form and click Create Customer when finished. Login with the initial administrator's username and password on the login page.



Create Partitions (Optional)

Partitioning, a method of logically separating the access control system into distinct sections (e.g., buildings or areas in a system) and defining specific permissions for Administrators to specific Partition(s), is the foundation of any configuration. On the Side Bar, scroll down to System; select Partitions. On the Partitions screen, the default partition displays. Click the Add button to create your custom Partition.

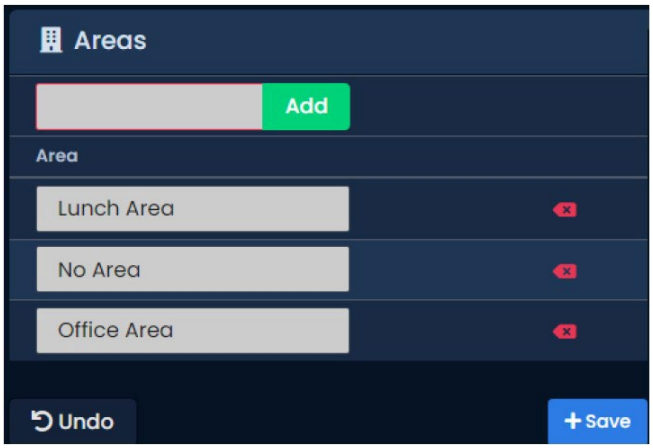
Fill in the Name and Description text fields. If Auto Panel Update is checked, any panel that is added to the Partition will automatically be updated 15 minutes after changes are made. Click +Create to finish adding the partition.

Create Sites

Sites are the method Panels are associated with Partitions. A Panel cannot be assigned directly to a Partition. A Site must be created in the Partition first and then the Panel is assigned to the Site; if a new Partition was created, then a Site must be added. On the Side Bar, scroll down to System and select Sites and Areas. On the Sites and Areas screen, the default site displays. Click the Add button to create your custom Site. Fill in the Name, Description, Time Zone and Partition text fields and click +Create.

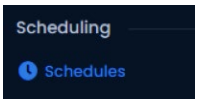
Create Areas (Optional; Required for Anti-Passback/User Tracking)

After a Site is created, Areas can be created and assigned to Doors, so the system can know which Readers grant access to which Areas. Areas are primarily used for anti-passback and user tracking via a Muster Report. To add an Area, click on the **Sites and Areas** menu. Choose a Site by clicking on the cogwheel icon and then click on the Areas tab. On the **Areas** tab, enter a name for the new area and click the Add button. For the first area, rename the field labeled No Area.



Create Schedules

Schedules are created for **Doors, Floors, Inputs, Outputs** and **Users**. A user can be denied access if any if these schedules are set to deny access for the current time. To create a schedule, from the Side Bar scroll to the Scheduling section and click on the Schedules icon.



Door Schedule: Grant or restrict access to a door based on the set time.

Floor Schedule: Grant or restrict access to a floor based on the set time.

Input Schedule: Dictates when an input will be monitored and when it will be ignored.

Output Schedule: Dictates when an output will be Open or Closed (On or Off).

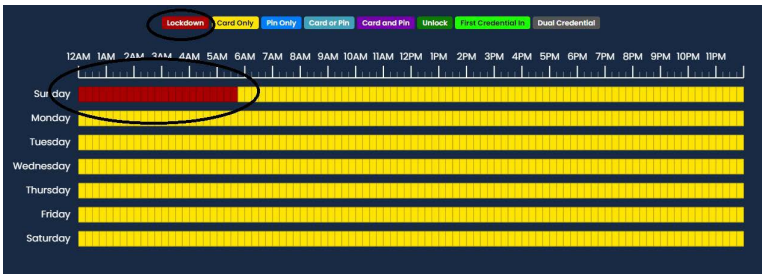
User Schedule: Applied to Users through Access Privilege Groups, these only have two possible states, Allowed and Not Allowed. They support up to 8 time spans in a day.

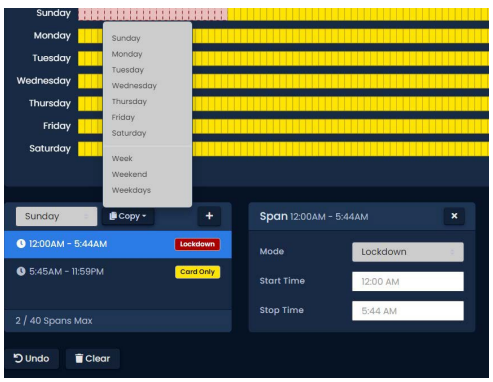
Go to the tab for Doors, Floors, Inputs, Outputs or Users. Default schedules are available; if additional schedules are needed, click the Add button.

Give the Schedule a Name and Description. Select the Partitions for which this schedule will be used.

Select the desired door state from the options at the top (e.g., Lockdown). Click and drag the mouse over the date and time the door state is being set for.

After the Door Schedule has been created, the Span editor menu displays as below. Click to edit a certain door state time span. Additionally, click the Copy button and select a specific day to copy it to an existing door schedule.





Configure Panels

Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds; Setup Password displays on the LCD screen. The default PIN is 0000, which can be changed in the VAX software Panel menu. Press the ESC button; Access Granted should display. Use the white up and down buttons on the Panel to locate and set the arrow on the LCD screen. The first menu that displays is Server IP Addr. Press the Enter button to enter and edit the VAX server IP address. To edit the address, click on the white left and right buttons to select the digit position. Click on the Enter button to select and click on the white up and down buttons to change the number. To save, click on the black ESC button followed by the black Enter button. The next important menu is "Server Conn Mode" which can be entered and changed between Server IP and Server Name (DNS); by default, it's Server IP. Finally, go to Panel IP Addr menu to assign the Panel and IP address. If needed, also set the Panel subnet address in the Panel SubnetMsk menu and Gateway IP address in the Panel Gateway menu. For details on the other Panel menus, refer to the VAX 3.1 User Guide. The next menu to go to is Panel Comm Mode. On this menu, the DHCP Client is the default. Keep this if the server is on a DHCP network and it is desirable for the Panel to be automatically assigned an IP address; if not, click on the white down button to select Static IP.

A message displays stating Change Confirm? There are two options, Yes, by pressing ENTER, or No, by pressing ESC.

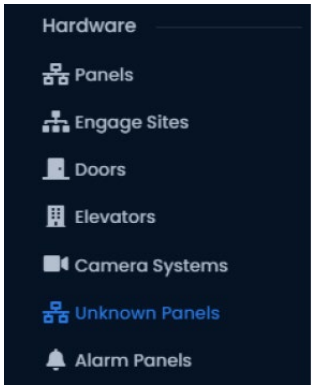
When the process is complete, save the setup.

Add Panels to VAX

There are two methods to add a Panel to VAX, adding a panel from the Unknown Panels screen or adding a panel manually with MAC address.

Method 1

From the Navigation menu, click Unknown Panels under the Hardware section.

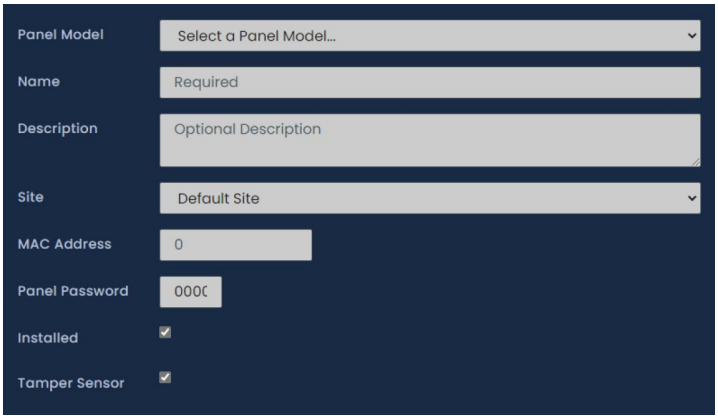


On the Unknown Panels screen, any Panels that communicate successfully to the server that have not been added yet appear in the list. Identify the Panel to be added and click the + button to go to the Add Panel screen.

Method 2

The following information is required to add a Panel manually: Panel model; MAC address of Panel; DHCP or Static IP address; Location of Panel; If a Door Panel, is it using a door contact.

After the method is decided upon, the Panel is added. From the Navigation menu, under Hardware, click Panels. Click the Add button. On the Add Panel screen, there are several dropdown menus, text fields and check boxes to populate. If the Unknown Panels method was used, most information auto fills.



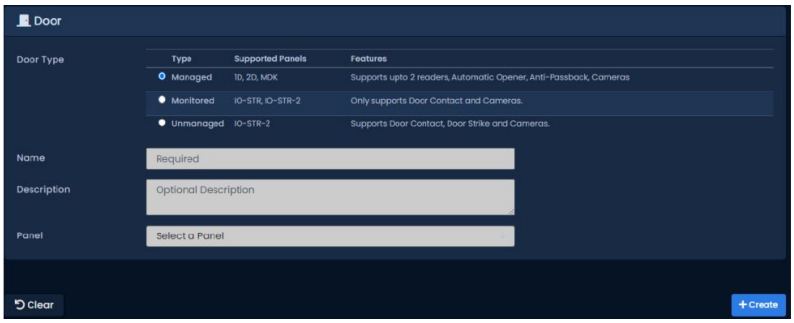
Complete any missing information and then click Save.

Note that there is a Tamper Sensor checkbox. When this is checked and the Panel cover is open, an audible alarm will sound. While installing the Panel, it is recommended to uncheck this option to avoid constant alarming.

Add Doors and Elevators

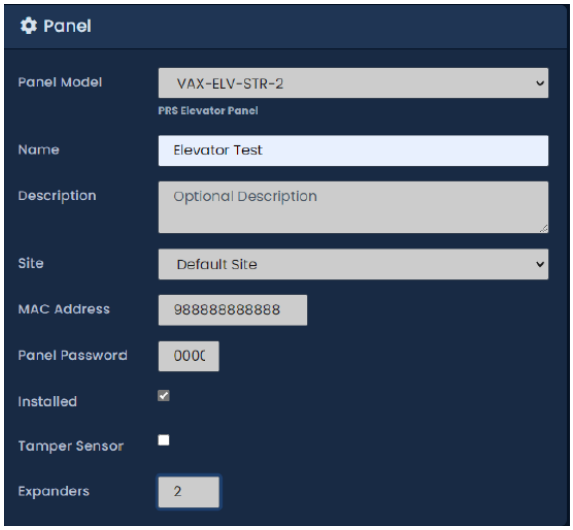
On the Side Bar, scroll to Hardware and click the Doors icon. 

On the Doors screen, click the Add button. On the Add Door screen, fill in the fields required; for Door type, select Managed for doors with locks or readers. When finished, click Save.



Adding an Elevator Panel is very similar to adding a Door Panel. From the Side Bar, click the Panels icon. 

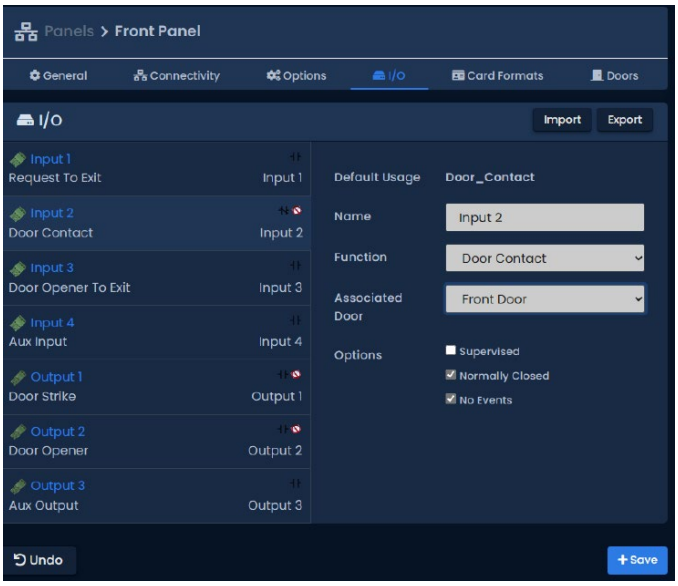
On the View Panels screen, click the Add button. On the Add Panel screen, there are several dropdown menus, text fields and check boxes to populate. Be sure the Panel Model is set to VAX-ELV-STR-2. After all the fields are filled, click Create; if successful, the message Panel added successfully displays.



Inputs and Outputs

Once a Door is configured, inputs and outputs for the door must be programmed. The options for configuration depend on the Panel model.

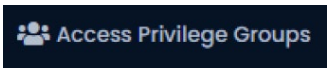
From the Panels screen, select the I/O tab. On the I/O tab, the left column shows each Input and Output with the current function under it. The currently selected Input/Output will have its information shown on the right side.



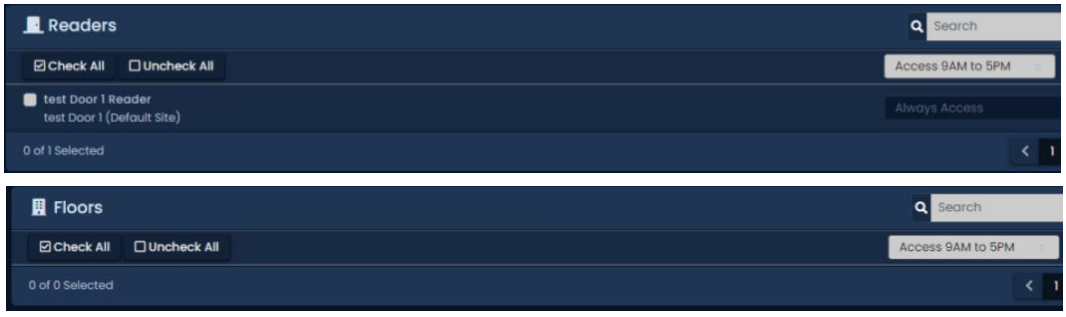
There are 10 Input functions and 8 Output functions. A list of these is provided at the end of this document.

Creating Access Privilege Groups

Access Privilege Groups are a way to manage and delegate access to an entire group. They are the link that permits a User's access at a Reader or Floor based on the User Schedule and the Door/Floor Schedule. Users can be part of more than one Access Group.

On the Side Bar, scroll down to Users and click on Access Privilege Groups. 

On the Access Privilege Groups screen, click the Add button. On the Access Privilege Group screen, there are a few fields to populate. Once a Partition is selected, that Partition will appear on the page and Users (and User Schedule), Readers and Floors can be assigned. Once all the settings are complete, click Create.



Updating Panels

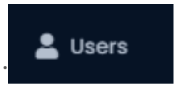
Updating Panels pushes relevant information into the Panel's flash memory and must be done for changes in the software to be applied to the Panels. Panels can be updated from any page in the VAX software by clicking the Update Panels button on the top right of the page. 

The browser will prompt with a message asking if you are sure you want to do this action; click Yes/Continue/OK. A window displays that shows the status of the updates being sent to the Panel. After the Panel receives all the information, it will disconnect from VAX for a few moments and then will attempt to reconnect.

Add Users/Credentials

Users can be added in several ways, including one at a time, importing multiple users from a .csv import, using Unknown User Denied Access Notification or using an Active Directory. The One at a Time and Unknown User Notification are described below. Refer to the VAX User Guide for the other methods.

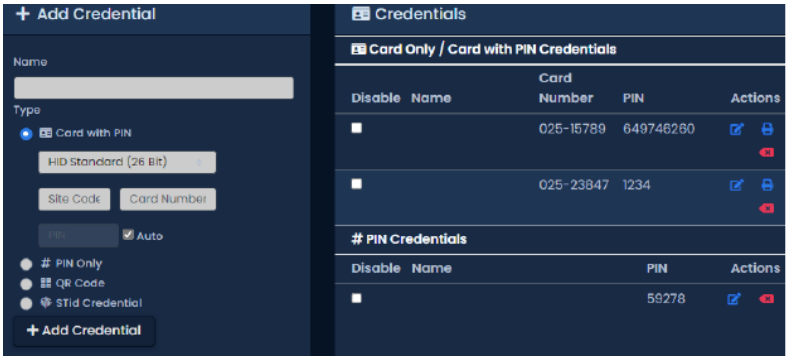
Adding Users One at a Time

On the Side Bar, scroll to Users and click on the Users icon. 

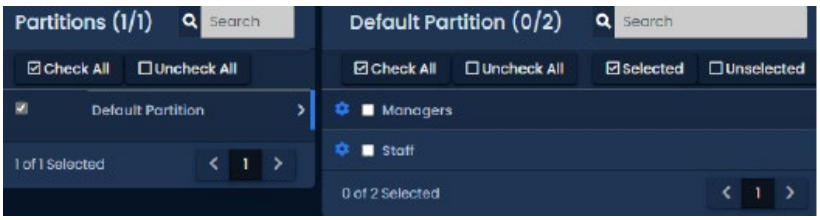
On the Users screen, click the Add button. On the Add Users page, there are several text boxes and check boxes to fill, including Special User Privileges. In the General section, all settings are optional except First and Last Name. Fill in any information in the Images and Custom fields as needed.

Under the Credentials section, a variety of credentials such as cards, fobs, PINs can be added.

Enter the site code (facility code) and card number into the Site Code and Card Number text boxes. A PIN associated with the Credential is auto generated. Click the Add Credential button; the Credential moves to the right side, indicating success. Now any additional Credentials associated with the User can be entered.

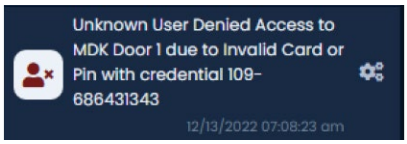


The last section is to assign the User to Access Privilege Groups. Select the Access Groups or Partition the User should belong to. Click Create.



Adding Users from a Notification

Users can be added by simply presenting their Credential at a reader. The Credential will be denied, and a notification will appear. Click on the notification Unknown User Denied Access to <Reader Name> due to Invalid Card or PIN with credential <site code>-<card number>.



This will go to the Add User screen with the credential pre-populated based on credential corresponding to the notification. Fill in any additional fields as noted in the procedure above.

Backup Programming

Access the System Manager UI and click Backup. Select the items to backup (default settings are recommended):

- Database: VAX database (recommended)
- Profile Pictures: Images associated with Users (cardholders) (recommended)
- Maps: Images associated with any graphical maps

Select the backup options (default settings are recommended):

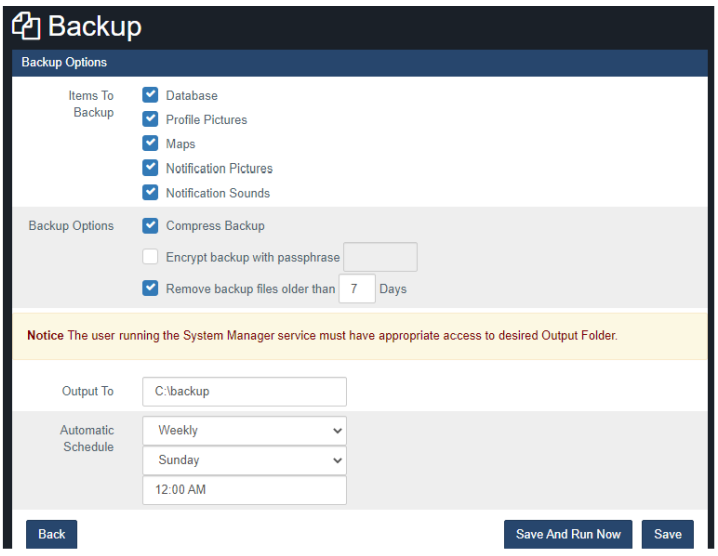
- Compress Backup: Determines whether the backup file is compressed upon successful backup (recommended)
- Remove Files Older than X Days: Automatically removes .prbak files from the backup location if the age exceeds
  the number of days specified
- Encrypt Backup with Password: Check if a password should be required to restore the backup

Determine where the backup will be saved to, local drive, USB drive or network share (e.g., C:\Backup) into the Output To field.

Select a Backup Schedule:

- Disabled: No automatic schedule
- Daily: Backup occurs once a day at the specified time
- Weekly: Backup occurs once a week on the day and time specified

A Backup can be run at any time by selecting the Save and Run Now button. Alternatively, click Save to save the backup settings and run on the next scheduled time (if a backup schedule has been set). If a folder or network permissions prevented the backup from being written, an error will display. When performing the first backup, browse to the output and verify that the backup has been written. This may take several minutes for large databases.



Input and Output Functions

Function	Description
Input Functions	
Disabled	The Input is disabled and will not react to any Input state changes on the selected Input.
Request To Exit	Allows the Input to be used as a REX. This will allow a push button or other dry contact input to unlock the associated door.
Door Contact	This Input function is used for Inputs that track if the Door is open or closed. Also referred as a door position switch. Should be disabled if not in use.
Door Opener To Exit	This type of Input is generally used for handicapped operators for activating auto-door openers. Automatic Opener must be enabled in Door Configuration Options.
Motion Sensor	This Input function is used for external motion sensors. Unlock By Motion must be unchecked in Door Configuration Options for the motion sensor to unlock the door. By default the motion sensor will prevent forced open alarm. Integrated Motion must be disabled in Panel Configuration Options tab.
Aux Input	This Input function has the most configurable options, including Input actions such as pulsing Outputs, overriding Doors, activating alarms. Aux Input actions are covered in more detail in the section called "Aux Input Actions".
Emergency Alarm	This Input function is used to receive commands from Emergency Alarm Systems. For example, you can set this Input to unlock the Door and play a buzzer when a fire alarm is triggered.
External Alarm Status	This Input function is used to monitor an alarm system status. When the alarm is considered "Armed", Readers will not accept Credentials unless the User associated with that Credential has the "Disengage Alarm" User privilege set to on.
Door Opener To Enter	This type of Input is generally used for handicapped operators for activating auto-door openers. Automatic Opener must be enabled in Door Configuration Options.
Door Unlocked or Open/Prevent Unlock	Used in Mantrap configurations. When the door is open or unlocked, this output will activate, is usually connected to an input on another panel controlling access to the same area. Connect to an input with the function "Door Prevent Unlock".
Output Functions	
Disabled	The Output is disabled and will not fire, even if instructed to by override.
Door Strike	Used to define an Output as being connected to a Door strike/Mag lock. Note: Output 1 is the only wet-contact, therefore Door strikes on Output 2 and 3 would require an external lock power supply.
Door Opener	Used to define an Output that is connected to the trigger Input on an auto-Door opener device.
External Buzzer	Used for external speakers. Will activate relay when the door is forced or held open. Global buzzer option will allow all doors connected on the same panel to activate the same output.
Alarm Interface	This Output is connected to an Input on the alarm panel capable of arming the alarm system; the alarm can now be armed using a triple swipe command. For more information on triple swipe scenarios please see Chapter 17, *Triple Swipe Features*.
Aux Output	An Output that can be triggered from Input changes or through triple swipe commands.
Secondary Door Strike	Setting an Output to this function will result in the Output being fired whenever the primary Door strike is fired. If the Door is in the state unlocked, the Output will remain on until the state of the Door changes.
Door Prevent Unlock	Used in Mantrap configurations to prevent access to an area if the input is activated by an external source (usually another panel controlling access to the same area). Can be used in other applications such as ground loops for parking gates.


VICON