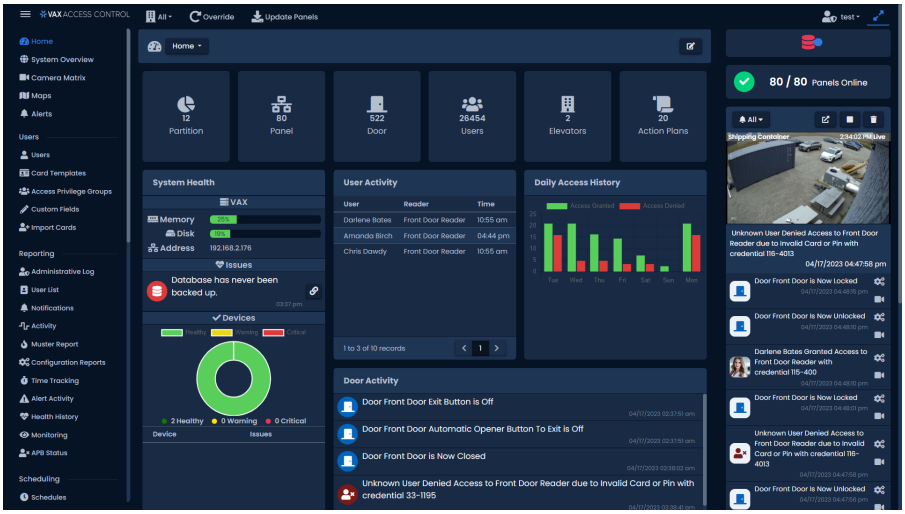
User Guide

VICON

VAX

Access Control System ver. 3.1

XX274-30-09



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
www.vicon-security.com

Vicon Access Control (VAX) Tech Guide

Vicon Access Control (VAX) Tech Guide

Table of Contents

Introduction

Vicon is proud to present Vicon Access Control (VAX). This guide is designed to assist you in planning, installing and configuring your new access control system. Although we have gone to great lengths to ensure the installation process is intuitive and straight forward, we do recommend reading this guide in its entirety before installing a Vicon Access Control access system. Thank you for your business.

Vicon Software - End User License Agreement

IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single legal entity) and Vicon with which you acquired the Vicon software product(s) identified above ("SOFTWARE"). The SOFTWARE includes Vicon software, and may include associated media, printed materials, "online", or electronic documentation and internet based services. Note: Any software, documentation, or web services that are included in the SOFTWARE, or accessible via the SOFTWARE, and are accompanied by their own license agreements or terms of use are governed by such agreements rather than this EULA. This EULA is valid and grants the end-user rights ONLY if the SOFTWARE is genuine. By installing, copying, downloading, accessing or otherwise using the SOFTWARE, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, you may not use or copy the SOFTWARE, and you should promptly contact Vicon for instructions on return of the unused product(s) in accordance with Vicon return policies.

1. SOFTWARE PRODUCT LICENSE

   The term "COMPUTER" as used herein shall mean the HARDWARE, if the HARDWARE is a single computer system, or shall mean the computer system with which the HARDWARE operates, if the HARDWARE is a computer system component.

2. GRANT OF LICENSE

   Vicon grants you the following rights, provided you comply with all of the terms and conditions of this EULA:

   Installation and Use: Except as otherwise expressly provided in this EULA, you may install, use, access, display and run only one (1) copy of the SOFTWARE on the COMPUTER. The SOFTWARE may not be used by more than the number of genuine licensed copies registered with Vicon.

   Mandatory Activation: THIS SOFTWARE CONTAINS TECHNOLOGICAL MEASURES THAT ARE DESIGNED TO PREVENT UNLICENSED OR ILLEGAL USE OF THE SOFTWARE. The license rights granted under this EULA are limited to the first year (1 year) after you first run the SOFTWARE unless you supply information required to activate your licensed copy in the manner described during the setup sequence (unless Vicon has activated for you). You can activate the SOFTWARE through the use of telephone; toll charges may apply. You may also need to reactivate the SOFTWARE if you modify your HARDWARE or alter the SOFTWARE.

   Back-up Copy: YOU MAY MAKE A SINGLE BACK-UP COPY OF THE SOFTWARE. You may use the back-up copy solely for your archival purposes and to reinstall the SOFTWARE on the COMPUTER. Except as expressly provided in this EULA or by local law, you may not otherwise make copies of the SOFTWARE, including the printed materials accompanying the SOFTWARE. You may not loan, rent, lease, lend or otherwise transfer the DVD or back-up copy to another User.

   Reservation of Rights: Vicon reserves all rights not expressly granted to you in this EULA.

3. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

   Consent to Use of Data: You agree that Vicon may collect and use technical information gathered in any manner as part of the product support services provided to you, if any, related to the SOFTWARE. Vicon may use this information solely to improve their products or to provide customized services or technologies to you. Vicon may disclose this information to others, but not in a form that personally identifies you.

   Database Information: The information stored in the database and/or database backup files can only be accessed via the Vicon licensed SOFTWARE. Any attempts to access the database information

via unlicensed and/or unauthorized access will terminate this license agreement. Vicon provides no direct access to the database information.

Additional Software/Services: The terms of this EULA apply to Vicon updates, supplements, and add-on components of the SOFTWARE that Vicon may provide to you or make available to you after the date you obtain your initial copy of the SOFTWARE, unless other terms are provided along with such Supplemental Components. Limitations on Reverse Engineering, Decompile and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE.

Separation of Components: The SOFTWARE is licensed as a single product. Its component parts may not be separated for use on more than one computer. Single EULA: The package for the SOFTWARE may contain multiple versions of this EULA, such as multiple translations and/or multiple media versions (e.g., in the User documentation and in the software). In this case, you are only licensed to use one (1) copy of the SOFTWARE.

Termination: Without prejudice to any other rights, Vicon may cancel this EULA if you do not abide by the terms and conditions contained herein. In such event, you must destroy all copies of the SOFTWARE and all of its component parts. Trademarks: This EULA does not grant you any rights in connection with any trademarks or service marks of Vicon or its suppliers.

4. UPGRADES

   If the SOFTWARE is labeled as an upgrade, you must be properly licensed to use a product identified by Vicon as being eligible for the upgrade in order to use the SOFTWARE ("Eligible Product"). For the purpose of upgrade(s) only, "HARDWARE" shall mean the computer system or computer system component with which you received the Eligible Product. SOFTWARE labeled as an upgrade replaces and/or supplements (and may disable, if upgrading a Vicon software product) the Eligible Product which came with the HARDWARE. After upgrading, you may no longer use the SOFTWARE that formed the basis for your upgrade eligibility (unless otherwise provided). You may use the resulting upgraded product only in accordance with the terms of this EULA and only with the HARDWARE. If the SOFTWARE is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

5. INTELLECTUAL PROPERTY RIGHTS

   All title and intellectual property rights in and to the SOFTWARE (including but not limited to any images, photographs, animations, video, audio, music, text and incorporated into the SOFTWARE), the accompanying printed materials, and any copies of the SOFTWARE, are owned by Vicon or its suppliers. The SOFTWARE is licensed, not sold. All title and intellectual property rights in and to the content that is not contained in the SOFTWARE, but which may be accessed through use of the SOFTWARE is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. Use of any on-line services which may be accessed through the SOFTWARE may be governed by the respective terms of use relating to such services.

6. EXPORT RESTRICTIONS

   You acknowledge that the SOFTWARE is subject to U.S. and Canadian export jurisdiction. You agree to comply with all applicable international and national laws that apply to the products, including the U.S. & Canadian Export Administration Regulations, as well as end-User, end-use and destination restrictions issued by U.S., Canadian and other governments.

7. ADDITIONAL PROVISIONS

   FOR THE LIMITED WARRANTIES, LIMITATION OF LIABILITY, AND OTHER SPECIAL PROVISIONS, PLEASE REFER TO THE ADDITIONAL PROVISIONS PROVIDED the relevant section within the master tech guide AND/OR OTHERWISE WITH THE SOFTWARE. SUCH LIMITED WARRANTIES, LIMITATION OF LIABILITY AND SPECIAL PROVISIONS ARE AN INTEGRAL PART OF THIS EULA.

Copyright

Vicon Industries Inc.

Phone: 800-645-9116

631-952-2288

Website: www.vicon-security.com

Chapter 1. Getting Started

Overview

VAX is a modern HTML5 web-based client/server access control system. The server application is designed to be installed on a stand-alone PC and may be accessed using one or more clients via a web browser. The VAX server software consists of:

- **VAX Web Server**: The Web Server's responsibility is to host the web application and facilitate client access to managing your access control system.
- **VAX System Manager** System Manager's responsibility is to manage backing up and restoring the database, as well as manage multi tenant configuration, general server configuration.
- **VAX System Monitor**: The System Monitor allows you to view the status and offers limited control over the web server and backup/restore utilities.
- **Database Provider** VAX uses a relational database to store the configuration and notifications from the access control system. It can be configured to use either of the following databases:
  - ***Microsoft SQL Server Database*** The VAX software can be configured to use a local or remote Microsoft SQL Database. You may opt to use the free (included) SQL Express 2019 or your own pre-installed instance of Microsoft SQL. Please Note: A minimum version of 2008 is required.
  - ***Postgres*** The VAX software can be configured to use a local or remote PostgreSQL database. You may opt for the installer to install it, or use your own existing instance. Please Note: A minimum of Postgres v12 is required.

Server Requirements

The VAX application server is designed to run on a modern PC running Microsoft Windows 10 or Windows Server 2016 is recommended for optimal performance.

Note

It is possible to install the VAX software on a shared PC, however where possible, we do recommend a standalone installation for optimal performance and reliability. It is also possible to install VAX on a virtual machine, off-site, or in the cloud. For more information regarding Panels communicating with the Panel through the internet, please see the section called “Configuring Advanced Remote Access Through the Internet”.

- 2GHz or faster 32-bit (x86) or 64-bit (x64) processor. Two or more cores recommended.
- 4GB RAM for 32-bit and 64-bit .
- 10GB Free Hard Drive Space (Additional space required for database).
- Windows 10 Home or Higher (Windows 7 Not Supported). Windows 10/11 Supported.
- Microsoft .Net Framework 4.8.1.
- Microsoft SQL Server 2016 or SQL Server 2016 Express or Higher (SQL Express installation available from the VAX Installer).

Note

The computer specifications are the minimum standards for a basic system. When a system includes a large number of clients (10+), controllers (50+), and/or users (2000+), additional server power is strongly recommended.

Operating Systems Supported

Note

Please note this refers to operating systems able to run the server software. Clients are supported regardless of OS version as long as HTML5 is supported. For more information on supported client web browsers, please see the section called “Supported Browsers”

Table 1.1. Supported Operating Systems

Operating System	Notes
Windows 11 Professional (32 and 64 bit)	
Windows 11 Home (32 and 64 bit)	
Windows 10 Professional (32 and 64 bit)	
Windows 10 Home (32 and 64 bit)	
Windows Server 2016 (Any Version)	
Windows 8 Professional (32 and 64 bit)	
Windows 8 Home (32 and 64 bit)	
Windows Server 2016	

The following operating systems are unsupported. VAX cannot be successfully installed on these operating systems:

Table 1.2. Unsupported Operating Systems

Operating System (Not Supported)	Notes
Windows XP (any version)	Missing hostable web core
Windows Vista (any version)	Missing hostable web core
Windows 8/7 Starter Edition	Missing components
Windows 7 Home Basic	Missing components
Windows Server 2003 (any version)	Missing hostable web core
Windows RT	ARM Specific

Installation Procedures

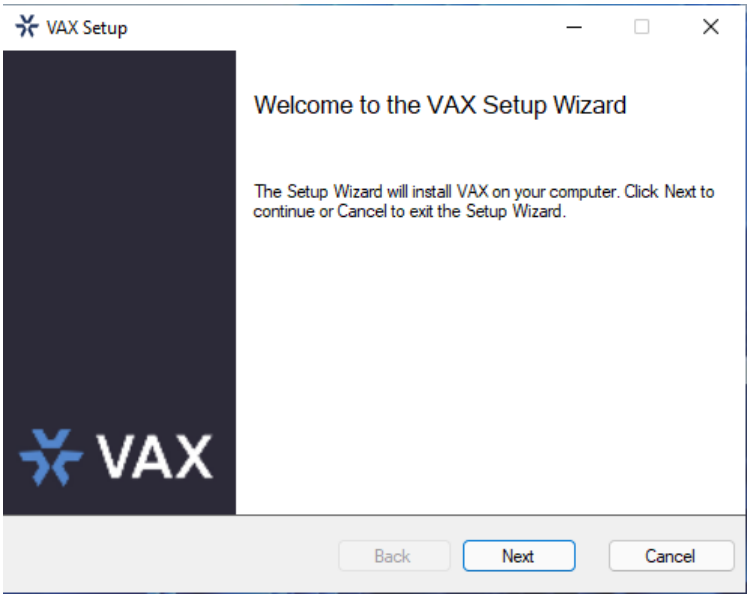
This section covers the installation of VAX and some frequently asked questions.

New Installation VAX

1. Locate and run the file called "VAX.exe" on your installation media or download and run the installer from our website.

2. On older operating systems, the installer may require an installation of .NET Framework 4.5.1. If needed, the installer will execute the bundled .NET framework installer prior to launching the VAX installer. Once the necessary prerequisite installed, the installer will automatically launch the VAX application installer.

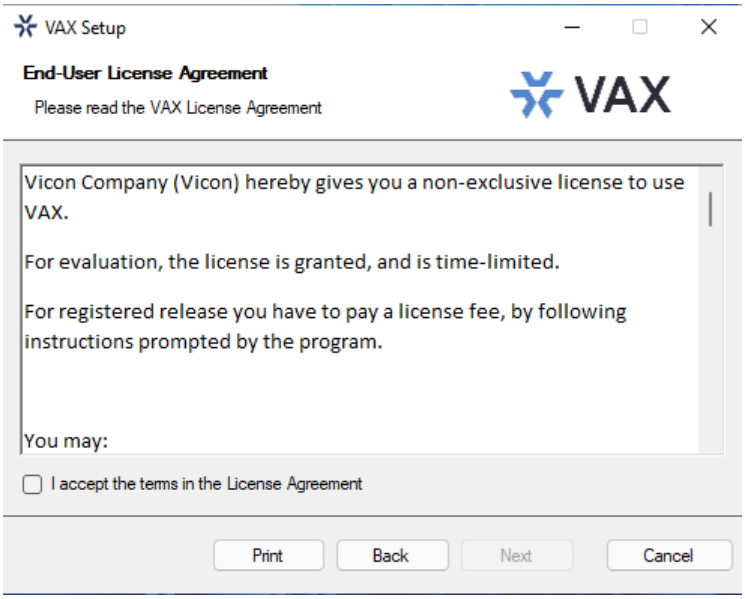
Figure 1.1. VAX Application Installer



After the VAX Installer has loaded, click the **Next** button to continue.

3. On the following screen, please read and accept the License Agreement. This agreement must be accepted in order to proceed with the VAX installation. Click **Next**.

Figure 1.2. VAX License Agreement



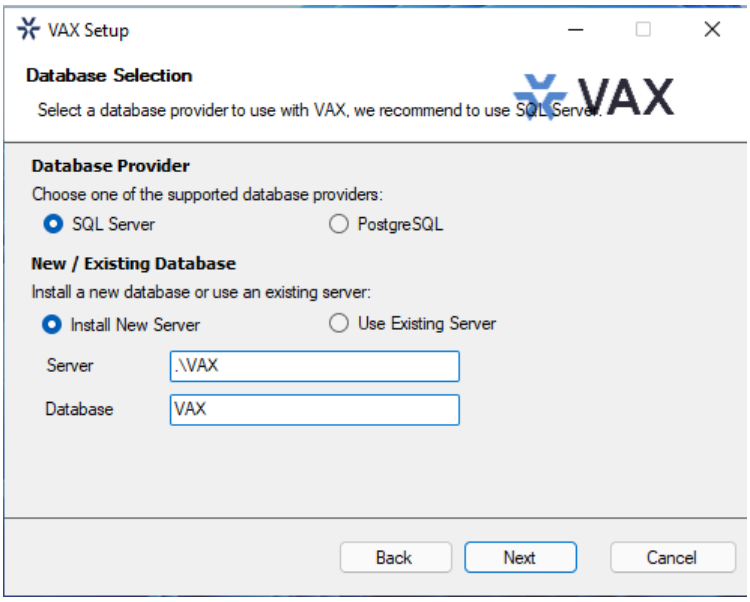
4. The next step is to choose the installation type:

   - ***Typical installation*** is recommended for normal installations. It uses the default settings for the listening ports, uses the local NT SERVICE accounts for the services, creates inbound rules for the listening ports in Windows Firewall and generates a self-signed certificate.

   - ***Advanced Installation*** is recommended for users who wish to use an external SQL Server or may need advanced configuration options for domain environments. You are given far more control over various VAX configuration options.

5. The Database Selection page allows you to select which database provider to install or use and allows you to configure the connection settings VAX will use to access the database.

Figure 1.3. VAX Database Selection



- **Database Provider** Either SQL Server or PostgreSQL can be used as the database. For new installations, we would recommend to use SQL Server. If upgrading an existing installation, these fields should auto populate.

  ### Note

  It is recommended to use SQL Server when hosting the database on the same machine as the VAX software.

- **Install New Server / Use Existing Server** If you have an existing installation of the database provider, you can select it in the **Server** dropdown field. Otherwise you can select **Install New Server** to install the selected database provider and configure it for use with VAX.

- **Server** The Server field allows to you to enter the address of the database server. If SQL Server and Use Existing Server is selected, the Server field dropdown will show a list of detected instances of SQL Server.

  If you are updating an existing installation, the Server field will populate with the existing configured SQL server.

- **Database** The Database Name is the unique name given to the database within the database server. The dropdown will show a list of databases that it detected in the selected server.

- **Username** An optional field for the username to authorize the software to access the database. This field is not required for basic installation and is used for authorizing to your own external database provider.

- **Password** An optional field for the password to authorize the software to access the database. This field is not required for basic installation and is used for authorizing to your own external database provider.

6. **[Advanced Installation Only]** Communication Setup allows you to modify the ports used by the software to host web services and communication servers.

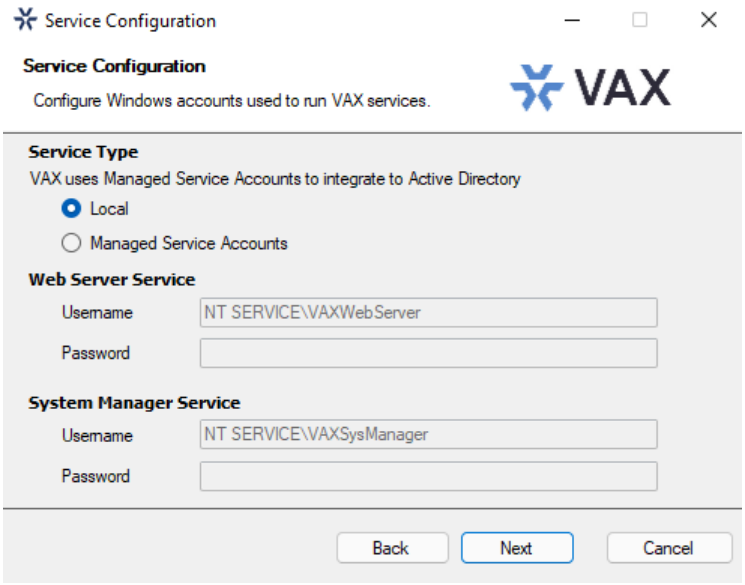
Web Server: The web server service is responsible for providing the web based interface and APIs. The **HTTPS Port** is the port the server will listen on for web communications, by default is **11001**.

Panel Communication: The web server service hosts a server to communicate with our panels. The **TCP/UDP Port** is the port the server will listen on for panel connections, by default is **9876**.

System Manager: The system manager service is responsible for managing database backups and server configuration. The **HTTPS Port** is the port the server will listen on for management communication, by default it is **11002**.

7. **[Advanced Installation Only]** Service Configuration allows you to configure the accounts used to host the Web Server and System Manager services. The **Local** option will use NT SERVICE accounts, which are special virtual Windows accounts used to host services. The **Managed Service Account** option is used for Active Directory integration to permit the services access to query the domain. Creating Managed Service Accounts is outside the scope of this installation manual.

Figure 1.4. VAX Service Configuration

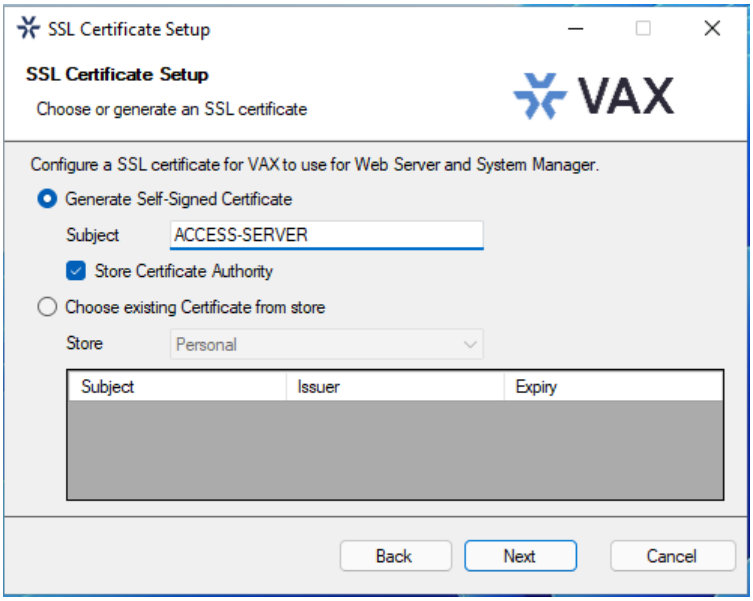


8. **[Advanced Installation Only]** SSL Certificate Setup allows you to generate or select an SSL certificate to use to host the Web Server and System Manager web services. The **Generate Self-Signed Certificate** option will generate a new certificate with the specified subject to use. Self-Signed certificates will generate a warning when browsing to the software as the browser can't validate the issuer of the certificate. Selecting the **Store Certificate Authority** will remove this warning on the installation computer only, by storing the signing certificate as a certificate root.

   The **Choose an existing Certificate from store** option will let you select a certificate from the Windows Certificate Store that has a valid private key. Certificates that have been imported into Windows will show here.

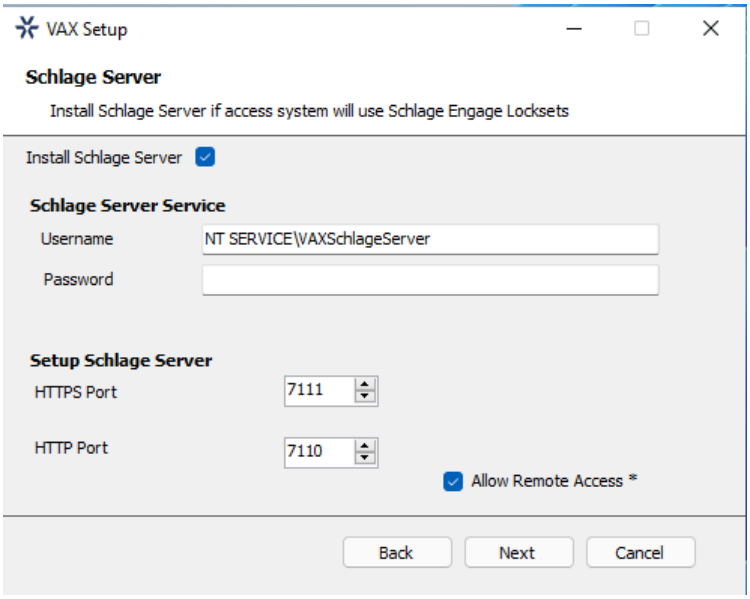
   SSL Certificates can be managed after installation in System Manager under Settings → Certificates.

Figure 1.5. VAX SSL Certificate Setup



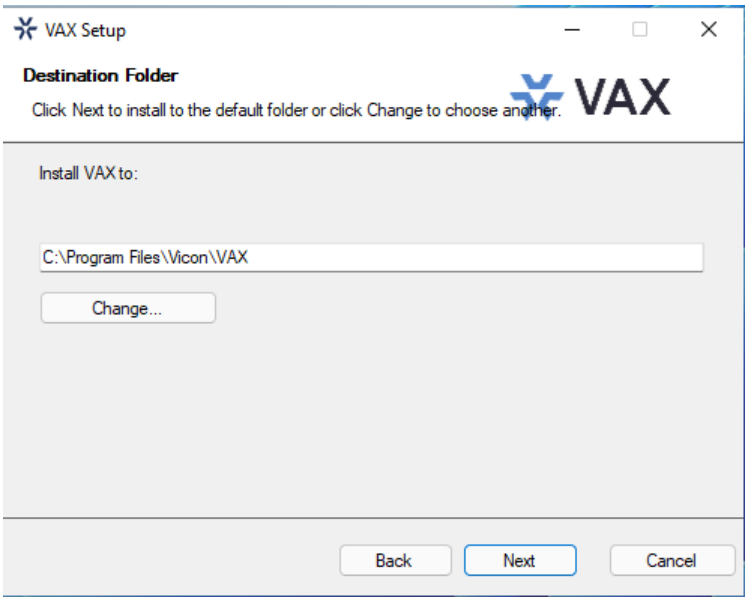
9. **[Advanced Installation Only]** Schlage Server is a seperate service which communicates with Schlage Engage gateways and locksets. If you require the use of the Schlage lockset integration, check the **Install Schlage Server** option and customize the Schlage server ports or service accounts as required.

Figure 1.6. VAX Schlage Server



10. The next step is to select the installation directory where you would like the VAX application to be installed.

Figure 1.7. VAX Destination Folder



11. You have now completed the configuration portion of the installer. Click **Install** to perform VAX installation and **Finish** when the installation completes.

Upgrading VAX

Periodic updates are released to VAX to enhance features, fix bugs or improve compatibility. VAX does not offer separate upgrade packages. Our standalone installer is capable of installing a new software instance or upgrading an existing instance of the VAX software.

Upgrade Installation

Depending on how you've installed VAX, the procedure for upgrading the VAX software may require some steps not covered in this section. Please see Chapter 2, *Upgrading VAX* for more details on these extra steps. We recommend doing a backup of your VAX database prior to upgrading. For more information about backing up your database, please see the section called “Backing up your VAX Database”. We also recommend stopping the VAX service via **System Monitor** prior to installation. Please note, if the installer does not contain a newer version than the currently installed version, you will not be given the option to perform an upgrade.

Updating Firmware

In some cases, in order to utilize the latest version of VAX, a firmware update is also required on the Panels (please, see the section called “Panel Firmware Updates”).

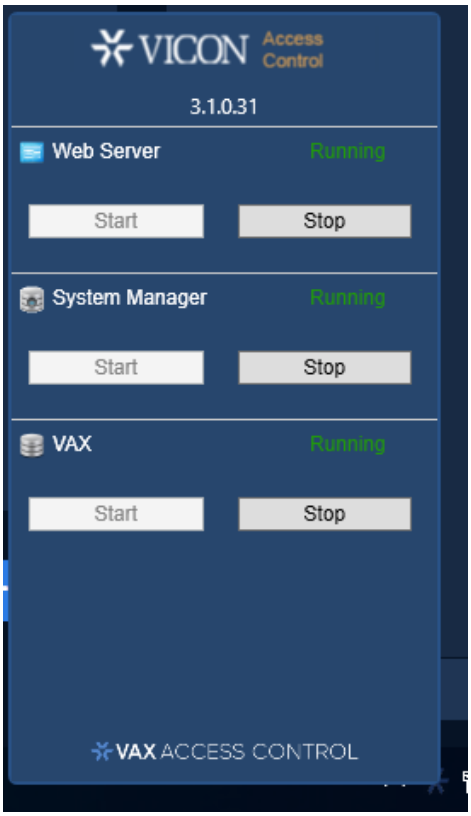
System Monitor

System Monitor is a tray application that shows you the status and offers limited control over the web server process. It can give you several useful shortcuts when the icon is right clicked. It will also show you the current version of your VAX software.

Once VAX is installed on the server, the system monitor icon will sit in the system tray (by the clock, highlighted below). If you do not see this icon, it may be hidden. You can use the arrow icon in the system tray to display hidden icons. You can also launch the System Monitor from the start menu of the computer VAX is installed on.

To view the System Monitor, simply click on the icon and a small window will appear near your system tray (pictured below).

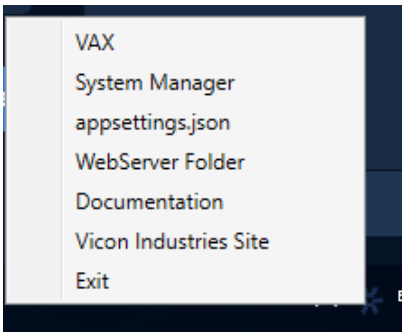
Figure 1.8. System Monitor Window



Once the System Monitor window is open, you can use the **Start** and **Stop** buttons to start and stop the Services used by VAX. This can be useful if the database or web service don't start automatically.

Tip

If you right click on the System Monitor icon, you'll get several useful shortcuts.



Frequently Asked Questions

Q: Do I have to use SQL Express 2019 or can I use my own database software?

A: We support any Microsoft SQL Server from 2016 to present or Postgres v12 or later, however when using our software to install SQL Express, you can be assured it is configured optimally for our system. If you choose to use you own database server instance, you will need to ensure the correct privileges and protocols are available for connection. This is something we generally only recommend for technicians or network Administrators who are well versed in the installation and configuration of SQL Server. Also please note different versions of SQL have different operating system and PC requirements. If you choose to use a different version, please ensure your PC meets the requirements for that version.

Q: Do you support Windows Vista or Windows XP operating systems?

A: At this time there is no plan to support operating systems earlier than Microsoft Windows 10. We are committed to ensuring the software works with future versions of Microsoft Windows.

Q: I received an SQL error during VAX installation. What should I do?

A: As part of the VAX installation, you are required to provide the correct SQL information which the installer uses to configure a number of VAX database and security options. If this information is incorrect, it will need to be corrected before you are able to successfully install the VAX software. If you have chosen to install SQL Express as part of the VAX installation, the settings should automatically be populated. However if you have chosen to use a custom database version and/or instance, you will need to manually populate these settings.

Q: What is the maximum database size supported?

A: If you are using Postgres, there is no maximum database size. If you are using Microsoft SQL Server, the maximum database size is a direct limitation of the version of SQL installed, not the VAX software. If you have used the default SQL Express 2019 installation, the maximum database size is 10GB. Earlier versions of SQL Express prior to 2008 generally had a limitation of 2GB.

Q: Is VAX 32-bit or 64-bit?

A: VAX is a 32-bit application designed to run both in native 32-bit operating systems and on 64-bit operating systems capable of 32-bit emulation (x64). There is no plan to support a native 64-bit installation as the VAX software will not benefit from the increased addressing 64-bit provides.

Client Installation

VAX supports client connectivity via web-based access. As a result, there is no VAX client software to install; rather you use your web browser to access the VAX server.

Supported Browsers

The list of browsers supported is by no means a comprehensive list. These are browsers that receive testing by Vicon Industries. Although other browsers may work, we do not provide technical assistance with them. We are always looking for user feedback in deciding what browsers to provide first class support for and we will expand the list of supported browsers as their market share dictates.

Table 1.3. VAX Browser Support

Browser	Version	Supported	Notes
Google Chrome	24.0+	Yes	Vicon Industries's browser of choice
Mozilla Firefox	20.0+	Yes	
Microsoft Internet Explorer	11	Yes	Note: IE11 is required for certain camera integrations.

Browser	Version	Supported	Notes
Microsoft Internet Explorer	6.0 to 10	No	No modern HTML5 Support
Microsoft Edge	20.0+	Yes	Note: Some issues with browsing to localhost address via DNS name. IP address or remote client work fine.
Apple Safari	6.0+ (Mac/iOS)	Yes	

Accessing the Server

Once you have ensured you have a browser that supports the VAX software, accessing the VAX software is very simple. If you are accessing the server from the PC it has been installed on, a start menu link is provided; otherwise you will need to enter the address manually into your web browser.

Accessing VAX From the PC the Server Software is Installed on:

During installation a shortcut is placed in your start menu for VAX. The link for VAX can be located by clicking Start -> All Programs -> VAX and finally clicking on **"Launch VAX."**

Accessing VAX From a Remote PC:

Open your web browser and within the address bar enter the address of the VAX Server using the format: **https://*NameOfTheComputer*:11001**

Alternatively, you can use the IP address of the server if the server is using a static IP address using the format: **https://192.168.1.100:11001**

Example 1.1. Accessing VAX server remotely

https://*ComputerName*:11001 (default port is 11001)

Once you have entered the address, press Enter to navigate to the VAX software.

Frequently Asked Questions

Q: **Why is browser XXX not supported?**

A: Web browsers although similar in appearance differ greatly in terms of features. We at a minimum require HTML5 support and many standard compliant browsers not listed in our supported list, will work just fine with our software. In order to provide the best possible experience, we do provide a set of recommended browsers. Browsers not mentioned in the recommended list may work fine but should issues occur, we do only provide technical support for browsers listed as supported.

Q: **Do I require Windows 7 or newer on the client?**

A: No. One of the benefits to web-based software is the flexibility it offers for connectivity. The client software is not limited by operating system but rather by the browser installed on the client machine. Windows XP is generally the oldest version of Windows we would recommend and Mac and Mobile platforms are fully supported as long as a supported web browser is used.

Q: **Can I access VAX without using SSL (HTTPS protocol)?**

A: No. For the sake of security, we do not support unencrypted connections.

Q: I'm using an unsupported browser and there are graphical anomalies or issues attempting use the VAX software. How do I resolve?

A: Use a supported browser. We do not provide support for any browser not listed as supported. However if you feel there would be a benefit in supporting a browser not in our supported list, we would love to hear from you. At a very minimum, HTML5 will always be required.

Q: I'm using Internet Explorer 10 which is listed as supported but I am still experiencing graphical anomalies or issues with the VAX software. How do I resolve?

A: Internet Explorer has a feature called Compatibility Mode which is enabled by default for Intranet (not public facing) sites. To achieve the best experience in Internet Explorer browsers, we recommend this feature be disabled for our application.

To disable Compatibility Mode in Internet Explorer 10, refer to the following steps:

1. Open Internet Explorer and press F12 to open the Developer Tools.
2. At the very top of the new Window you will see two drop-down lists, one labelled 'Browser Mode' and one labelled 'Document Mode'. Ensure Browser Mode is IE10 (or higher) and Document Mode is IE10 Standards (or higher).
3. In Internet Explorer 11, click on the gear icon on the top right of the web browser window.
4. Select "Compatibility View Settings".
5. Ensure the checkbox labeled "Display Intranet sites in Compatibility View" is not selected.

Chapter 2. Upgrading VAX

This chapter covers the process of upgrading VAX, the pre-requisites for upgrading, and how to update the firmware on the Panels (the door and elevator control boards).

Software Upgrades

Periodically, updates are released to VAX to enhance features, fix bugs or improve compatibility. VAX does not offer separate upgrade packages. Our standalone installer is capable of installing a new software instance or upgrading an existing instance of the VAX software. All licensed instances of VAX are entitled to software updates as they are released.

Download the Latest Version of VAX

Visit our VAX downloads page at:

https://www.vicon-security.com/software-downloads-library/vax-access-control-software/

You'll be prompted for credentials to download; please contact Vicon Industries for these details.

Prerequisite Installation

In order to upgrade VAX, the following requirements will need to be met.

- Upgrade must be performed from the computer on which VAX is currently installed.
- You must be logged in as the same Windows Login that installed VAX (due to database permissions).
- If the upgrade includes a firmware update for the panels, UDP port 9876 must not be blocked.

Upgrade Installation

The procedure for upgrading the VAX software is identical to that of a fresh install. (Please, see the section called “Installation Procedures”).We recommend doing a backup of your VAX database prior to upgrading. For more information about backing up your database, please see the section called “Backing up your VAX Database”. We also recommend stopping the VAX service via **System Monitor** prior to installation.

Note

During installation, it's advised you click "Advanced" and ensure information such as the database connection looks correct.

Panel Firmware Updates

Periodically when we enhance VAX, firmware upgrades to your Panels will be required with the software updates. Updating a Panel's firmware is a relatively straight forward process.

Warning

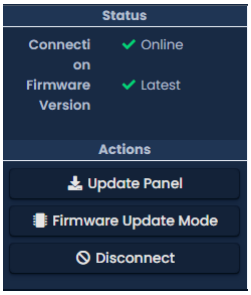
While in firmware update mode Panels are non-functional. They will not respond to card presentations, do not generate notifications and place the Door into a lock-down state. To limit the impact this has on your site, we suggest only placing 1 Panel at a time into Firmware Update Mode.

1. When a Panel attempts to connect to the VAX application and and the firmware is found to be out of date, you will see an indicator at the bottom of the notification panel on the right side of the screen.

2. In order for a Panel to have its firmware updated we must place it into Firmware Update Mode. To do this we will navigate to the System Overview page in the software. Click on the "x/x Panels Online" box above the Notifications area **or** in the left navigation menu, click on **System Overview** .

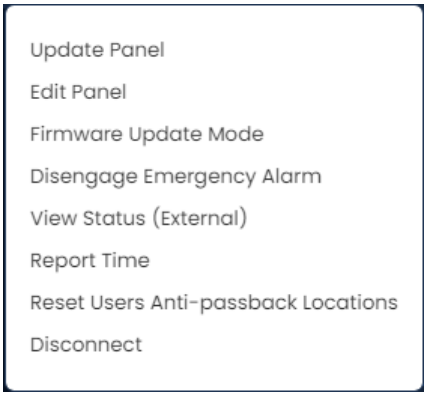
3. On the System Overview you will see a list of all Panels in your system. Any Panels that require a firmware update will show a Critical status and if you expand it, the **Firmware Version** will show Outdated.

Figure 2.1. System Overview Showing Firmware Out of Date Message



4. The next step is to place your Panels into Firmware Update Mode. This can be accomplished on the System Overview page.

   a. On the right side of Panel, click on the blue gear icon, pictured below. A context menu will appear.



   b. Select 'Firmware Update Mode' from the context menu.

   c. The Panel will now disconnect and attempt to update its firmware.

> **Note**
>
> You can perform multiple firmware updates at the same time if needed.

5. The VAX server will accept incoming connections from Panels in firmware update mode on **UDP Port 9876** and automatically apply the latest matching firmware for your Panel. Once complete, the server will instruct the Panel to reboot into normal mode, at which point the Panel will resume normal operation. If the panel does not connect to the server on UDP 9876 within 60 seconds, the panel will reboot.

6. Repeat the above process on all panels that indicate they require a firmware update. After all Panels have had their firmware updated, we recommend doing a update to all your Panels. The 'Update Mode' status icon on the Dashboard under Devices menu will disappear automatically, or you can refresh the page.

Troubleshooting Firmware Update Problems

Panel continues to show firmware out of date after placing it into firmware update mode. If a Panel continues to show it requires a firmware update after placing the panel into firmware update mode and coming back online, ensure there isn't any third party firewall blocking UDP port 9876. Ensure there are no enterprise firewall solutions between the server and the Panel on the network blocking UDP port 9876.

Panel does not come back online after placing into firmware update mode. If a panel does not come back online after several minutes, we recommend physically checking the LCD of the panel.

- If the LCD shows the message "Run Application Timeout", power down the panel by unplugging the Cat5 from the left side of the board. Press and hold the button labeled Enter (SW3) while plugging in the cat5. This will place the panel back into firmware update mode.
- The LCD on the panel will show the current server address it is looking to update its firmware from, if you see this set as 192.168.2.10, it could indicate it had a problem during the update. Try the above suggestion or change the VAX server's IP address temporarily to 192.168.2.10 with a 255.255.255.0 subnet mask.

Frequently Asked Questions

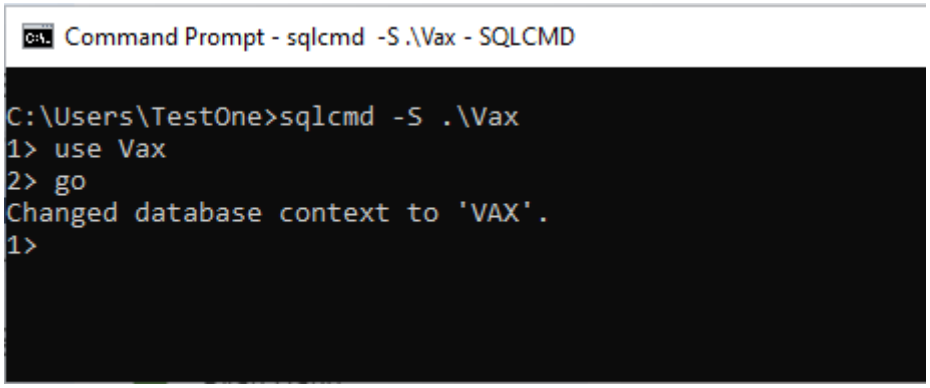
Q: **How can I check if my Windows login can upgrade VAX?**

A: To check if your account has the right permissions, we can simply make a connection to the VAX database and see if we're denied or granted access. This may require the assistance of IT staff or Vicon Industries.

1. Open a command line with administrator privileges (right click cmd.exe, 'Run as Administrator').
2. At the command line, type: 'SQLCMD -S .\VAX' (your instance name may be different). Click 'ENTER'.
3. At the '1>', type 'USE VAX' and press 'ENTER'.
4. At the '2>', type 'GO' and press 'ENTER'.

If you see the message "Changed database context to 'VAX'.", your Windows account has permission to upgrade VAX.

Figure 2.2. Command Prompt: Backup



If you see the message "The server principal "computer/user" is not able to access the database "VAX" under the current security context", your Windows account does not have permission to upgrade VAX.

Q: My Windows login doesn't have permission to upgrade VAX; how do I find out which account does?

A: Due to the manner that SQL database permissions work, when VAX is initially installed, the Windows login installing the software gets implicit permission to access the database. Likely (but not always), we can find this user account name by checking a log file generated by the MS SQL installer.

1. Browse to your installation directory of SQL server (usually located in "C:\Program Files \Microsoft SQL Server").

2. Use the search bar to search all folders for a file called "sql_common_core_Cpu64_1.log" or "sql_common_core_Cpu32_1.log". Open the file in notepad.

3. Once you've opened the file, use the 'find' function and look for the string "appdata". The first result should show the path to the user directory of the correct Windows login.

If the Windows login is unavailable, or does not exist anymore, please contact Vicon Industries.

Chapter 3. Initial Configuration

This chapter will cover the initial configuration of the software and hardware elements of VAX. This includes the initial setup of the software, the initial setup of the Panels and how to associate a Panel with VAX.

Initial Software Configuration

This section will cover the initial configuration of your access control system. This is simply a matter of providing the VAX software with enough information for it to build your initial database.

Access the VAX server through your HTML5 browser of choice. (For more information on accessing the server, please see the section called “Accessing the Server”.) Once your browser reaches the server, you may notice a pop up indicating that the connection to the server is 'Untrusted' or 'Not Private'. Due to the dynamic nature of our software, we are unable to create a Signed Certificate with a Certificate Authority. Communications to the server are encrypted with 128-bit SSL. In Google Chrome, click 'Advanced' and 'proceed to..'. In other browsers, click 'Proceed Anyways' or 'Add Exception' (depending on your browser).

Once you reach the server and proceed past any browser warnings, you'll be presented with the a splash screen, followed by the Initial Configuration wizard. It is broken into four steps: EULA, Customer Configuration, Server Address and Initial Administrator.

EULA

1. Read through the End User License Agreement then check the **I agree to the End User License Agreement** checkbox at the bottom.
2. Click the **Next** button in the bottom right of the page.

Customer Settings

1. Enter a **Name** for the customer and set the **Initial Site Time Zone** of the system.
2. Optionally enter information about the dealer managing the system so that the end user may easily contact for support.
3. Optionally enter email configuration to enable password resets and emailed notifications and system alerts.
4. Click the **Next** button in the bottom right of the page.

Customer Configuration

Figure 3.1. Customer Configuration

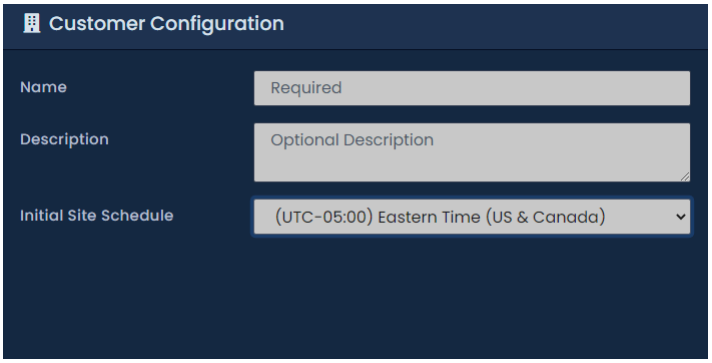
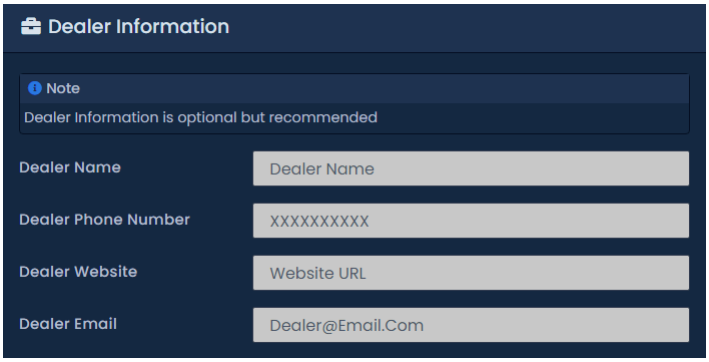


Table 3.1. Customer Configuration Fields

Field	Brief Description
Name	This is the name of the host, customer or company name (not specific site).
Description	An optional description of the host, customer or company.
Initial Site Time Zone	This is the primary time zone your first site operates under. Additional sites may be added afterwards with different time zones.

Dealer Information

Figure 3.2. Dealer Information



Note

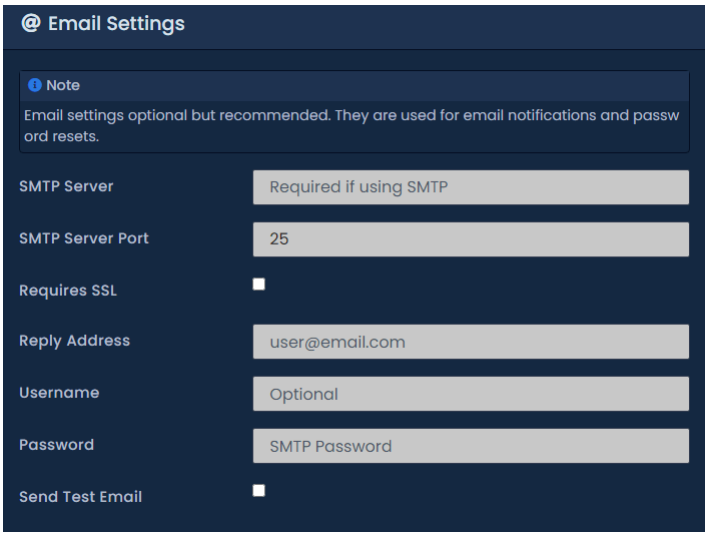
Dealer Information is optional, but recommended.

Table 3.2. Dealer Information

Field	Brief Description
Dealer Name	This is the name of the dealer installing the system and/or responsible for supporting the end user of the system.
Dealer Phone Number	This is the primary contact phone number of the dealer installing the system and/or responsible for supporting the end user of the system. No dashes between sections of number (eg: 800-348-4266)
Dealer Website	This is the website address of the dealer installing the system and/or responsible for supporting the end user of the system. Enter the full URL of the dealer website. Example: https://www.vicon-security.com
Dealer Email	This is the primary contact email address of the dealer installing the system and/or responsible for supporting the end user of the system.

Email Settings

Figure 3.3. Email Settings



Note

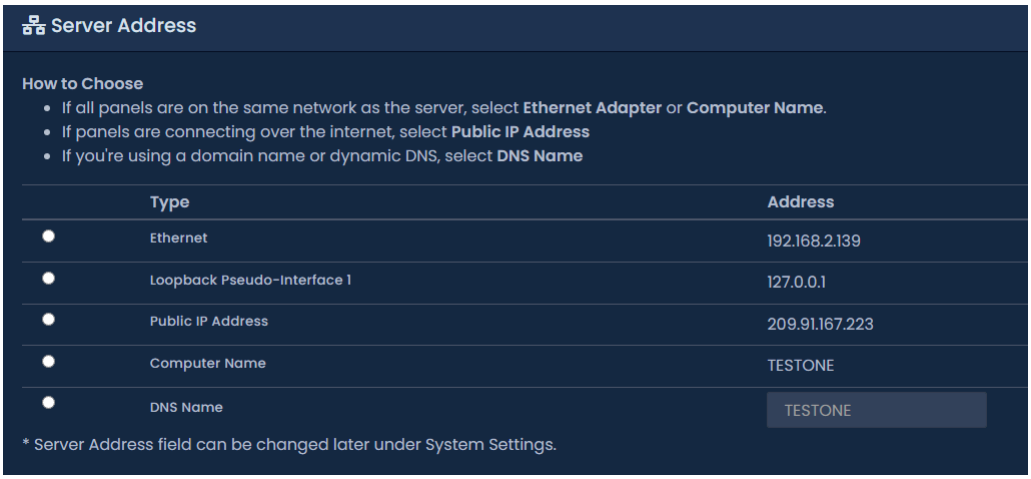
Email Settings are optional, but recommended. These can be used to recover a forgotten password and to receive notification emails.

Table 3.3. Email settings Fields

Field	Brief Description
SMTP Server	This is the name of the SMTP server required for sending emails (eg: mail.ISPdomain.com).
SMTP Server Port	This is the port used for sending emails via SMTP (port 25 is common, however your settings may vary).
Requires SSL	Check the Secure Socket Layer checkbox if your email client requires and uses SSL for encrypting email messages.
Reply Address	This is the email address that notifications and email recovery will be sent from. It can be the same as the sender email address.
Username	This is the username required for authenticating and sending email via SMTP.
Password	This is the password required for authenticating and sending email via SMTP.

Server Address

Figure 3.4. Server Address



The VAX panels initiate the connection to the server and therefore need to be configured with the address to reach the server. When a panel is sent new configuration, or in other words has its tables updated, it is sent this server address. This settings will depend on where on the network the panels are in relation to the server.

1. Review the options shown in the table below and select the option that best describes your network layout.

2. Click the **Next** button in the bottom right of the page.

Table 3.4. Server Address Types

Field	Brief Description
Ethernet Adapter	Each network adapter that has an IPv4 address will be displayed in the table. If the panels are on the same local network as the adapter, select this option. **Note:** It may show a warning that DHCP is enabled when selected, if so, we recommend using the computer name, setting a static IP, or a DHCP reservation to ensure the IP address does not change.
Public IP Address	This is the public facing IP address of the default gateway of the server, if applicable. If the panels are connecting over the internet to the server, select this option. **Note:** Connecting panels over the internet will usually require port forwarding in the router. Additionally, depending on your internet provider, your public IP address may be dynamic and could change. If you've determined your public IP address is dynamic, we recommend using a dynamic DNS service and selecting the Custom option.
Computer Name	By default, the name of the PC VAX was installed. Panels on the same local network as the server can resolve the computer name using DNS or NetBIOS resolution. We recommend this option if the PC is using DHCP to obtain an IP address.
Custom	You may enter a custom IPv4 or DNS address for the panels to use to connect to the server. Select this option if you have your own DNS address that resolves to the server, or are using a dynamic DNS service.

Administrator

Figure 3.5. Initial Administrator

1. Enter an **Email Address**, **First Name**, **Last Name**, and **Password** for the initial system administrator.

2. Once all the fields have been set, click **Create Customer** to continue.

Table 3.5. Initial Administrator Fields

Field	Brief Description
Email Address	This is the email address/Username of the primary VAX Administrator. This email address will be used to login to the site initially.
Username	By default, this field will populate with the email address set above it. However you may change the username to something other than the email. It must be between 5 and 255 characters.
First Name	The first name of the primary VAX Administrator. Accepts 2-64 characters, and may not contain special characters.
Last Name	The last name of the primary VAX Administrator. Accepts 2-64 characters, and may not contain special characters.
Language	The language shown in the UI and of the messages sent to the primary VAX Administrator. This is set on a per-Administrator basis.
Password	Enter and confirm the password to be used by the primary Administrator. Accepts 6-16 characters. This may be changed at a later time.

If everything entered was valid, VAX will automatically create and setup your database for use.

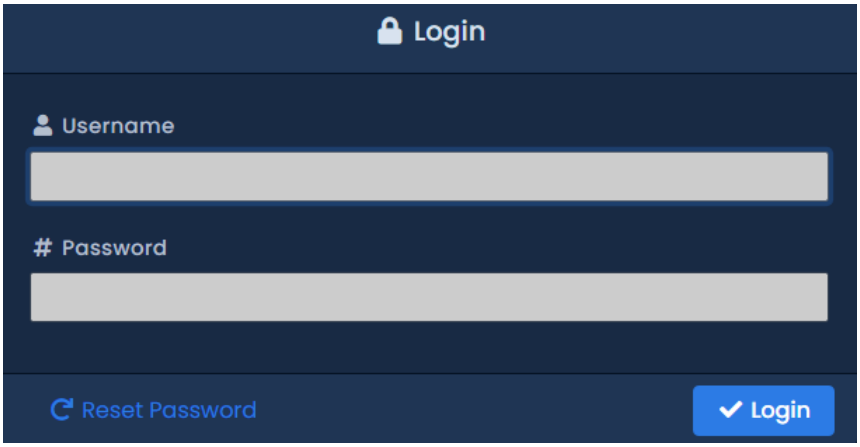
Congratulations! You are now ready to start configuring your access control system. We can now move on to configuring the panels to communicate with the server.

Logging Into VAX Web Interface

Once you've completed the Initial Configuration, or the system has been pre-configured for you, you may now login to VAX web interface.

At the **Login Page**, please enter the email address and password you entered on the Initial Config page or the email and password provided to you by the installer of the system. Click the **Login** button on this screen. You will now be taken to the **Home** page of the VAX web interface.

Figure 3.6. VAX Login Screen



Password Recovery in VAX

In the event that you are unable to remember or misplace your password to login to VAX, you may go through the password recovery process by clicking the blue **Reset Password** button on the bottom of the page.

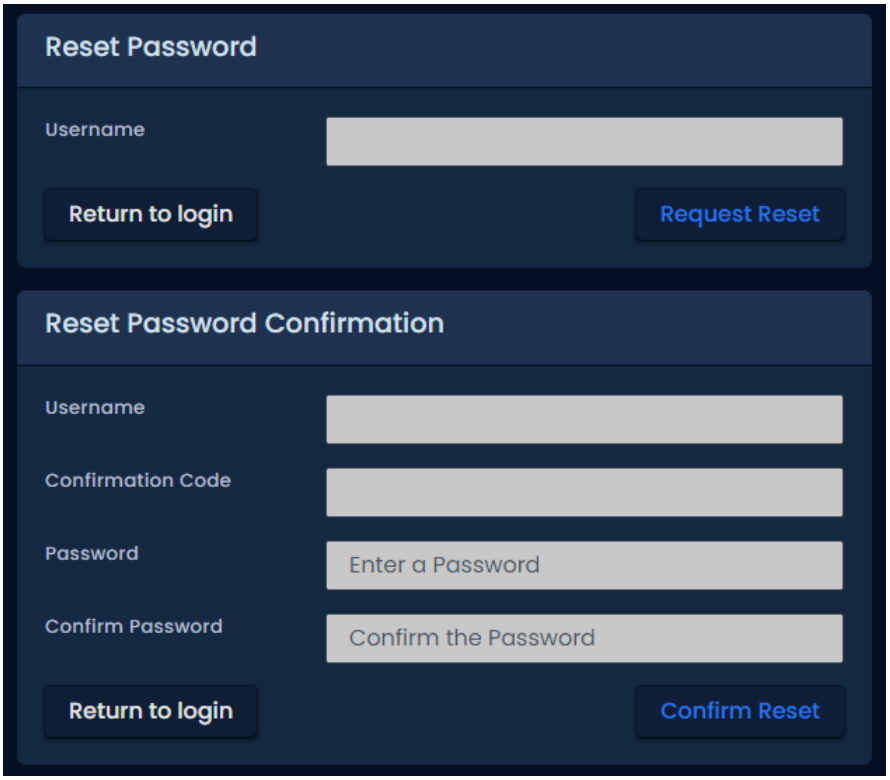
Warning

Due to the high-security nature of this product, passwords may only be reset if Email Configuration has been programmed in the software. If it has not been programmed, please contact Vicon Industries. Chapter 37, *Support*.

For information on Email Configuration for use with email alerts and password recovery, please see the section called “Email Settings”.

On the **Reset Password** page, populate the email of the Administrator account you would like to reset the password for. Click the **Request Reset** button. If email settings are correct, you will receive a Confirmation Code emailed to the supplied Administrator email. Input this code into the Confirmation Code field and enter your new password. Click **Confirm Reset**; you will now be taken back to the Login page.

Figure 3.7. Password Reset Page



Panel Initial Configuration

This section will cover common initial configuration of VAX PoE and 12VDC powered door, elevator and input/output controllers. This section is focused on configuring communication information manually into the Panel so that it can connect to the VAX server software. The software aspect of configuring a panel will go into more detail in Chapter 7, *Setting up Your Panel*.

This aspect of the configuration requires the VAX software installed onto a PC or server with the Initial Configuration completed with an assigned email account name and valid password. We will refer to the PC with VAX installed as the VAX Server. Note the IP address or name of the VAX server; this is required during Panel Configuration.

Built-in diagnostics can still be accessed, even when the server is not available or not installed yet.

From a hardware perspective, the VAX PoE powered panels should either be mounted at its intended location or temporarily accessible physically near the VAX server with a Cat5e/6 cable (non-crossover) connected directly to either a PoE Injector or powered network switch (Note: Maximum cable run from VAX VAX-1D-1to injector or powered switch is 100 meters or 330 feet). In the case of a 12VDC powered controller, such as the VAX-MDK Panels, 12-13.5 VDC power should be plugged in and the Cat5 should be connected to network that can reach the VAX server locally or through the internet.

Warning

If you're about to perform a Panel installation, we recommend you read Chapter 6, *Planning an Access Control Deployment* along with this chapter in its entirety prior to configuration.

Information to Collect Prior to Configuration

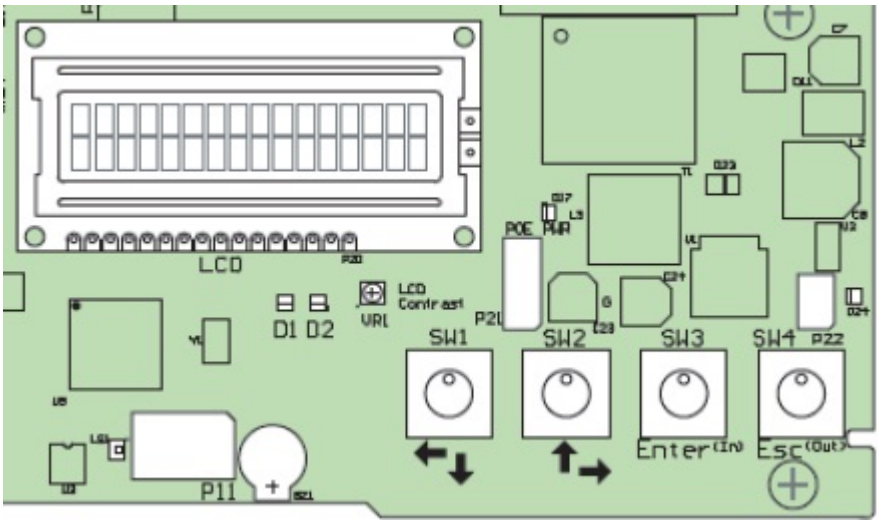
- The **Static IP** or **Server Name** of the VAX server.
- Will this Panel be using **DHCP** or a **Static Address** for the IP address? If static, which IP, subnet, gateway and DNS should be used?

- Is the IT staff at the location aware of the new device(s) being added to the network(if applicable)?

Navigating the Panel Interface

There are 4 buttons located on the lower right corner of a VAX controller for accessing, viewing and configuring a Panel.

Figure 3.8. Panel Buttons (same button layout on PoE and 12VDC powered panels)



The two white buttons (SW1 & SW2) are used for moving up and down through menus when not editing a specific menu item, and for moving left and right over value data when editing a specific menu item. The two black buttons (SW3 = Enter, SW4 = Esc) are used for selecting a menu item, placing a particular value in edit and non-edit mode, saving or cancelling changes and committing changes to memory.

The default state of the panel is a scrolling menu that displays the following:

- Door State(s)
- Door Schedule
- Network Name
- Panel Name and Site association
- Date and Time
- Server Connection Mode
- Panel Communication Mode

Note

You may hit the Enter key (SW3) while in the default menu to pause the scrolling and have it stay on the same item.

To quickly see how the Panel is currently configured (READ ONLY), hold the ESC (SW4) button for 4 seconds or until the Panel beeps twice. You can now use the navigation buttons (SW1 & SW2) to view a current settings.

Table 3.6. Read Only Configuration View

01 Panel Name	02 Area Name

03 Panel Device ID	04 Panel Run Mode
05 Default Panel Address	06 Actual IP Address
07 Panel MAC Address	08 Panel Subnet Mask
09 Panel Gateway	10 Panel DNS
11 Panel Communication Mode	12 Server IP Address
13 Server Name	14 Server Port
15 Server Connection Mode	16 Firmware Version
17 HTTP Server Mode	

Some of the more important/useful fields to note are the following:

07 Panel MAC Address: This is the MAC address of the Panel. Note the address for when you are adding the Panel to VAX or if the IT staff needs it for port security.

06 Actual IP Address: By default, the Panel will try to use DHCP to obtain an IP Address; if successful, this address will be here. You can use this address to access the **Panel Web Configuration Page**, however this address could change depending on the DHCP server settings.

15 Server Connection Mode: This field shows the connection method the Panel is attempting to use to reach the server (IP Address or Server Name).

Communication Mode Configuration: Server IP

This section covers how to configure the Panel to communicate with the **Static Server IP Address** of the VAX server.

Note

Communication between the Panel and server can only happen when both sides have valid IP addresses. By default the Panel will attempt to obtain an address via DHCP. If the Panel needs to have a static IP manually configured, please see the section called “Panel IP Settings: Static IP”.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

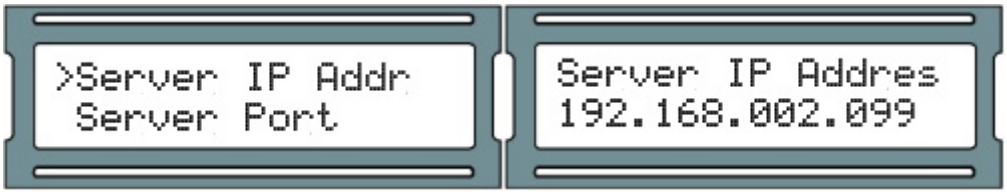
3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'SERVER CONN MODE' and then press the ENTER button. This setting defines the server communcation mode (Spelled Sever Conn Mode due to character space limitations).

4. Now on the 'SERVER CONN MODE' screen, press the white up or down buttons until the arrow on the LCD screen is indicating '1: Server IP' is selected and press the ESC button.

5. You will be presented with a message stating 'CHANGE CONFIRM?' and have two options: YES via pressing the ENTER button or NO via pressing the ESC button. If you wish to commit that setting to the Panel, press the ENTER button. You will now be presented with message indicating 'CHANGED'. Pressing the ESC button will cancel the operation and present a message indicating 'NOT CHANGED'. (Note: If no selection is made within 20 seconds, the change process will time-out and you will have to start it again.)

6. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'SERVER IP ADDR' and then press the ENTER button.

7. Using the white buttons for left and right movement as well as using them for changing numerical values for each position of the IP address of the server and using the ENTER button to switch between EDIT mode (position blinking between value and solid black) and VIEW mode (position blinking between value and blank), enter the full server IP address.



8. With full the IP address completed on the LCD screen, ensure you are in VIEW mode (indicated by positional value blinking between value and blank) and then press the ESC button.

9. You will be presented with a message stating 'CHANGE CONFIRM?' and have two options: YES via pressing the ENTER button or NO via pressing the ESC button. If the IP address for the server is correct and you wish to commit that setting to the Panel, press the ENTER button. You will now be presented with message indicating 'CHANGED'. Pressing the ESC button will cancel the operation and present a message indicating 'NOT CHANGED'. (Note: If no selection is made within 20 seconds, the change process will timeout and you will have to start it again.)

10. Press ESC once more to save the configuration to flash memory. You'll be presented with 'Setup Saved'.

Communication Mode Configuration: Server Name (DNS)

This section covers how to configure the Panel to communicate with the server via DNS name. This is useful when the VAX server is on a laptop or cannot have a static IP. The Panel will use a local DNS server to translate the Server Name to the IP the server it is currently using. We advise that our dealers/clients be aware that home routers can be used as a DNS server, but often under perform or only act as DNS repeaters, which will not function with our Panels.

Note

Communication between the Panel and server can only happen when both sides have valid IP addresses. By default the Panel will attempt to obtain an address via DHCP. If the Panel needs to have a static IP manually configured, please see the section called “Panel IP Settings: Static IP”.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'SERVER CONN MODE' and then press the ENTER button. This setting defines the server communcation mode (Spelled Sever Conn Mode due to character space limitations).

4. Now on the 'SERVER CONN MODE' screen, press the white up or down buttons until the arrow on the LCD screen is indicating '2: Server name' is selected and press the ESC button.

5. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Server name' and then press the ENTER button.

6. Using the white buttons for left and right movement as well as using them for changing alphabetical, numerical, and symbol values for each position of the server name and using the ENTER button to switch between EDIT mode (position blinking between value and solid black) and VIEW mode (position blinking between value and blank), enter the full server name (up to 16 characters).

7. With full server name completed on the LCD screen, ensure you are in VIEW mode (indicated by positional value blinking between value and blank) and then press the ESC button.

8. You will be presented with a message stating 'CHANGE CONFIRM?' and have two options: YES via pressing the ENTER button or NO via pressing the ESC button. If the IP address for the server is correct and you wish to commit that setting to the Panel, press the ENTER button. You will now be presented with message indicating 'CHANGED'. Pressing the ESC button will cancel the operation and present a message indicating 'NOT CHANGED'. (Note: If no selection is made within 20 seconds, the change process will timeout and you will have to start it again.)

9. Press ESC once more to save the configuration to flash memory. You'll be presented with 'Setup Saved'

Note

It is often easier to do the initial connection with Server IP and then change the connection mode to Server Name from the System Settings setting titled Server Address in the VAX web interface.

Panel IP Settings: DHCP

This section covers how to set the Panel to obtain an IP address automatically using DHCP. This is the default setting the Panel comes shipped with.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Panel Comm mode' and then press the ENTER button.

4. Now on the 'Panel Comm mode' screen, press the white up or down buttons until the arrow on the LCD screen is indicating '1: DHCP client' is selected and press the ESC button.

5. You will be presented with a message stating 'CHANGE CONFIRM?' and have two options: YES via pressing the ENTER button or NO via pressing the ESC button. If the IP address for the server

is correct and you wish to commit that setting to the Panel, press the ENTER button. You will now be presented with message indicating 'CHANGED'. Pressing the ESC button will cancel the operation and present a message indicating 'NOT CHANGED'. (Note: If no selection is made within 20 seconds, the change process will timeout and you will have to start it again.)

6. Press ESC once more to save the configuration to flash memory. You'll be presented with 'Setup Saved'.

Panel IP Settings: Static IP

This section covers how to set up the Panel with a static IP. This is used when a DHCP server is not available or the IT staff has already designated an IP for the Panel.

You will need the following information (from IT staff or equivalent) prior to configuring a static address:

- IP Address of the Panel.
- Subnet mask associated with the Panel IP.
- Default gateway (only applicable if traveling across WAN or internet links to server).

Once you have this information, use the following steps to assign a static IP address on the panel.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Panel Comm mode' and then press the ENTER button.

4. Now on the 'Panel Comm mode' screen, press the white up or down buttons until the arrow on the LCD screen is indicating '0: Static IP' is selected and press the ESC button.

5. You will be presented with a message stating 'CHANGE CONFIRM?' and have two options: YES via pressing the ENTER button or NO via pressing the ESC button. If the IP address for the server is correct and you wish to commit that setting to the Panel, press the ENTER button. You will now be presented with message indicating 'CHANGED'. Pressing the ESC button will cancel the operation and present a message indicating 'NOT CHANGED'. (Note: If no selection is made within 20 seconds, the change process will timeout and you will have to start it again.)

6. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Panel IP Addr' and then press the ENTER button.

7. Using the white buttons for left and right movement as well as using them for changing numerical values for each position of the IP address of the Panel and using the ENTER button to switch between EDIT mode (position blinking between value and solid black) and VIEW mode (position blinking between value and blank), enter the full Panel IP address.

8. With full IP address completed on the LCD screen, ensure you are in VIEW mode (indicated by positional value blinking between value and blank) and then press the ESC button.

9. You will be presented with a message stating 'CHANGE CONFIRM?' and have two options: YES via pressing the ENTER button or NO via pressing the ESC button. If the IP address for the server is correct and you wish to commit that setting to the Panel, press the ENTER button. You will now be presented with message indicating 'CHANGED'. Pressing the ESC button will cancel the operation and present a message indicating 'NOT CHANGED'. (Note: If no selection is made within 20 seconds, the change process will timeout and you will have to start it again.)

10. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Panel Subnetmsk' and then press the ENTER button.

11. Using the white buttons for left and right movement as well as using them for changing numerical values for each position of the Subnetmask of the Panel and using the ENTER button to switch between EDIT mode (position blinking between value and solid black) and VIEW mode (position blinking between value and blank), enter the full Panel subnetmask.

12. With the full subnetmask completed on the LCD screen, ensure you are in VIEW mode (indicated by positional value blinking between value and blank) and then press the ESC button.

13. You will be presented with a message stating 'CHANGE CONFIRM?' and have two options: YES via pressing the ENTER button or NO via pressing the ESC button. If the IP address for the server is correct and you wish to commit that setting to the Panel, press the ENTER button. You will now be presented with message indicating 'CHANGED'. Pressing the ESC button will cancel the operation and present a message indicating 'NOT CHANGED'. (Note: If no selection is made within 20 seconds, the change process will timeout and you will have to start it again.)

14. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Panel Gateway' and then press the ENTER button.

15. Using the white buttons for left and right movement as well as using them for changing numerical values for each position of the Panel gateway and using the ENTER button to switch between EDIT mode (position blinking between value and solid black) and VIEW mode (position blinking between value and blank), enter the full Panel gateway.

16. With full Panel gateway completed on the LCD screen, ensure you are in VIEW mode (indicated by positional value blinking between value and blank) and then press the ESC button.

17. You will be presented with a message stating 'CHANGE CONFIRM?' and have two options: YES via pressing the ENTER button or NO via pressing the ESC button. If the IP address for the server is correct and you wish to commit that setting to the Panel, press the ENTER button. You will now be presented with message indicating 'CHANGED'. Pressing the ESC button will cancel the operation and present a message indicating 'NOT CHANGED'. (Note: If no selection is made within 20 seconds, the change process will timeout and you will have to start it again.)

18. Press ESC once more to save the configuration to flash memory. You'll presented with 'Setup Saved'

Resetting a Panel

This section will cover how to reset a Panel to a default state. If at any point you need to reset the Panel to factory default values, refer to these steps:

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Erase Flash Mem' and then press the ENTER button.

4. You will be presented with a message stating 'Erase Flash Mem?' and have two options: YES via pressing the ENTER button or NO via pressing the ESC button.

5. You will be presented briefly with a message indicating 'ERASING FLASH' followed by 'ERASED' and then the LCD screen will revert back to the 'ERASE FLASH MEM' screen. (Note: Erase process will timeout if there is no activity within 60 seconds.)

6. The Panel will now restart and now be in a default state. You can now configure the Panel.

Testing Input/Outputs at the Door

This section covers methods technicians can use to test the Panel once its been mounted at the door.

Table 3.7. Testing at the Door

Test Name	Description/Common Use
Output Test	Used for testing the 3 Output relays, generally used to verify if the Door Strike was properly wired up.
Input Test	Used for testing the 4 Inputs, generally used to verify if the Door contact and/or Exit Button were properly wired up.
Reader Test	Used for testing the 2 Reader ports, generally used to verify if the Reader was wired up correctly and to check the bit format of the cards.

Output Test (PoE Models)

This section includes detailed instructions on performing an Output test on PoE powered door controllers.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Output Test' and then press the ENTER button.

4. Press the white up or down buttons to move the cursor over the Output you'd like to test. Press ENTER and the highlighted zero will change to a 1, and the Output will be triggered. Press ENTER again to disengage the Output. When you are done testing, press the ESC button.

5. After you've pressed ESC you'll see a message saying 'Canceled'. You'll be returned to the option menu. You can now proceed with additional tests.

Output Test (VAX-MDK)

This section includes detailed instructions on performing an Output test on 12VDC powered door, elevator or IO controllers.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Output Test' and then press the ENTER button.

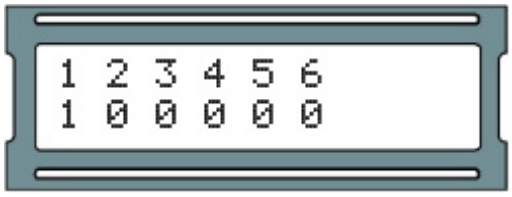
4. On 12VDC powered models you will need to select a board type. Using the white up and down buttons on the Panel, locate the option best suited for what you need and press the Enter button. These options are outlined below:

Table 3.8. Action Categories

Menu Option	Description
1: Use Preset DB	Output test will automatically detect what board type is configured based on the current database configuration.
2: PRS_IO8	Select this option if the connected expander boards are IO expanders (VAX-IO-EXP8-PCB).
3: PRS_TDM	Select this option if the connected expander boards are two door expanders (VAX-EXP-2D).
4: PRS_IO8_All	This option will allow you to test relays on multiple IO expanders at once (VAX-IO-EXP8-PCB).
5: PRS_TDM_All	This option will allow you to test relays on multiple two door expanders (VAX-EXP-2D).

5. After selecting a Board Type, you will now choose a Board Address. Currently supported addreses are 1-4 for VAX-EXP-2D expanders and 1-8 for VAX-IO-EXP8-PCB expanders. Using the white up and down buttons on the Panel, locate the address for the expander you wish to test and press the Enter button.

6. Press the white up or down buttons to move the cursor over the Output you'd like to test. Press ENTER and the highlighted zero will change to a 1, and the Output will be triggered. Press ENTER again to disengage the Output. When you are done testing, press the ESC button.



7. After you've pressed ESC you'll see a message saying 'Canceled'. You'll be returned to the option menu. You can now proceed with additional tests.

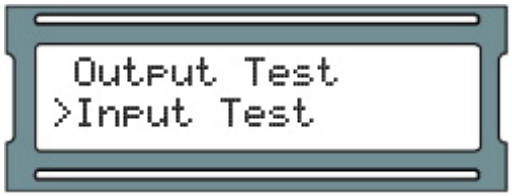
Input Test (PoE Models VAX-1D-1)

This section includes detailed instructions on performing an Input test on PoE powered door controllers.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

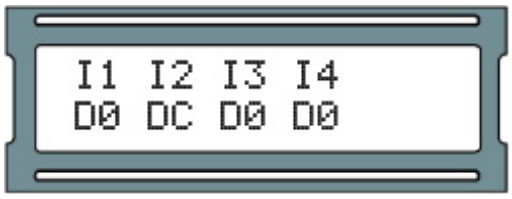
2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Input Test' and then press the ENTER button.



4. You'll be shown briefly a legend regarding the Input states.

5. If you have any Input devices such as door contacts or REX devices, the Panel will beep and show you which Inputs are active. Inactive Inputs are 'DO' and active Inputs are 'DC'. If you're testing a door contact, open and close the door and monitor the Input change. When you are done testing, press the ESC button.



6. After you've pressed ESC you'll see a message saying "Canceled'. You'll be returned to the option menu. You can now proceed with additional tests.

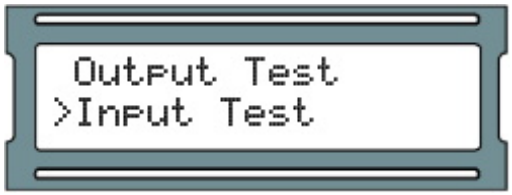
Input Test (VAX-MDKModels)

This section includes detailed instructions on performing an Input test on 12VDC powered door, elevator or IO controllers.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Input Test' and then press the ENTER button.



4. On 12VDC powered controllers you will need to select a board type. Using the white up and down buttons on the Panel, locate the option best suited for what you need and press the Enter button. These options are outlined below:

Table 3.9. Action Categories

Menu Option	Description
1: Use Preset DB	Input test will automatically detect what board type is configured based on the current database configuration.

Menu Option	Description
2: PRS_IO8	Select this option if the connected expander boards are IO expanders (VAX-IO-EXP8-PCB).
3: PRS_TDM	Select this option if the connected expander boards are two door expanders (VAX-EXP-2D).

5. After selecting a Board Type, you will now choose a Board Address. Currently supported addreses are 1-4 for VAX-EXP-2D expanders and 1-8 for VAX-IO-EXP8-PCB expanders. Using the white up and down buttons on the Panel, locate the address for the expander you wish to test and press the Enter button.

6. You'll be shown briefly a legend regarding the Input states.

7. If you have any Input devices such as door contacts or REX devices, the Panel will beep and show you which Inputs are active. Inactive Inputs are 'Do' and active Inputs are 'Dc'. If you're testing a door contact, open and close the door and monitor the Input change. When you are done testing, press the ESC button.

8. After you've pressed ESC you'll see a message saying "Canceled'. You'll be returned to the option menu. You can now proceed with additional tests.

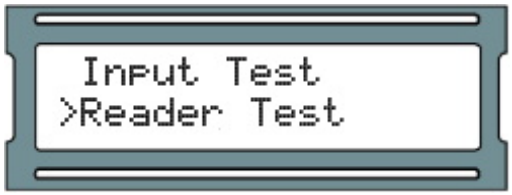
Reader Test (PoE Model VAX-1D-1)

This section includes detailed instructions on performing a Reader test on PoE powered door controllers.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Reader Test' and then press the ENTER button.



4. You'll be shown a screen that says 'No Card Input'. You may now present a proximity card or fob to one of the attached Readers.

5. If the Reader is correctly wired, and a 40 or 26 bit card is presented, you'll see information about the card and the Reader appear on the screen. If you are using a second Reader, you can perform the test on that Reader in the same manner. When you are done testing, press the ESC button.

6. After you've pressed ESC you'll see a message saying "Canceled'. You'll be returned to the option menu. You can now proceed with additional tests.

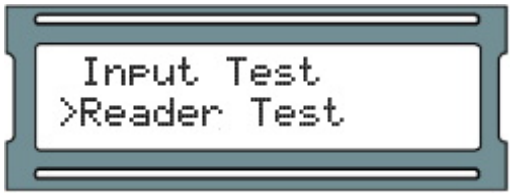
Reader Test (VAX-MDK Models)

This section includes detailed instructions on performing a Reader test on 12VDC powered door and elevator controllers.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout.)

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'Reader Test' and then press the ENTER button.



4. On 12VDC powered controllers you will need to select a board type. Using the white up and down buttons on the Panel, locate the option best suited for what you need and press the Enter button. These options are outlined below:

Table 3.10. Action Categories

Menu Option	Description
1: Use Preset DB	Input test will automatically detect what board type is configured based on the current database configuration.
3: PRS_TDM	Select this option if the connected expander boards are two door expanders (VAX-EXP-2D).
5:PRS_TDM_All	This option will allow you to test readers on multiple two door expanders (VAX-EXP-2D) at the same time.

5. After selecting a Board Type, you will now choose a Board Address. Currently supported addreses are 1-4 for VAX-EXP-2Dexpanders and 1-8 for VAX-IO-EXP8-PCB expanders. Using the white

up and down buttons on the Panel, locate the address for the expander you wish to test and press the Enter button.

6. You'll be shown a screen that says 'No Card Input'. You may now present a proximity card or fob to one of the attached Readers.

7. If the Reader is correctly wired, and a 40 or 26 bit card is presented, you'll see information about the card and the Reader appear on the screen. If you are using a second Reader, you can perform the test on that Reader in the same manner. When you are done testing, press the ESC button.

8. After you've pressed ESC you'll see a message saying "Canceled'. You'll be returned to the option menu. You can now proceed with additional tests.

Panel HTTP Configuration Interface

This section will cover how to access the Panel HTTP configuration web interface and how to make changes in this interface.

Note

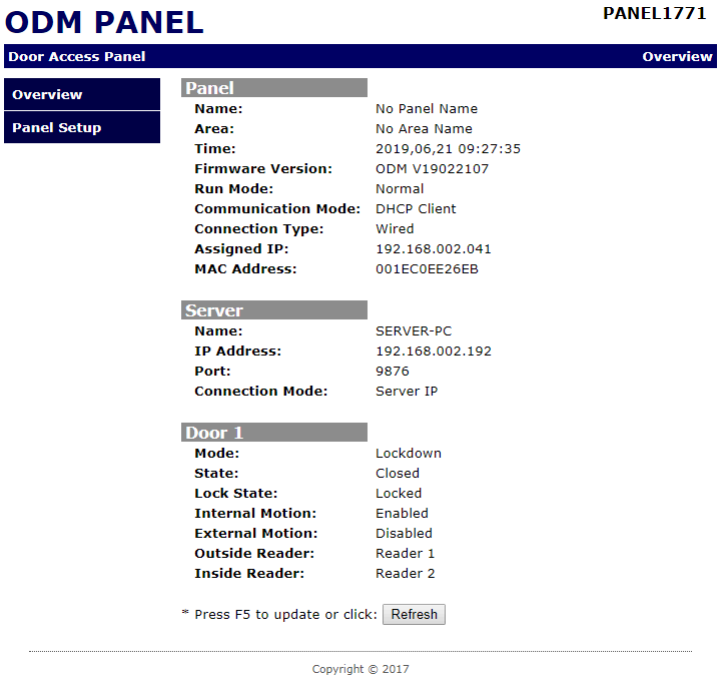
The Panel HTTP Interface is currently unsupported on some models such as PoE elevator panels.

Each Panel has a configuration web interface that can be accessed through a web browser, as long as the client connecting to this interface is on the same network. In this interface you can configure many of the settings we can configure manually. If the Panel has a valid IP address through either DHCP or a manually entered static address, you can use that address through a web browser to access this interface.

1. Obtain the IP address of the Panel by holding SW4 for 4 seconds on the Panel, and using SW1 and SW2 to browse to '06 Actual IP Add'. If you have assigned a static address to the Panel, that will be the address you use. Alternatively, if the Panel has made any communication to the server, you can likely find the address by doing the following: Open a command prompt on the server, type 'arp -a' and press Enter. Once you find the MAC address, look to the adjacent entry in the column left of the MAC address; you will see the IP address associated with that MAC address.

2. Open a web browser and type the IP address of the Panel by itself, no port numbers, 'http' or 'www' required. If the connection is successful you will be prompted for a user name and password. The user name is 'user' and the password is the 4 digit password that is used to access the Panel on board interface, by default is '0000'. Once you login, you'll see the **Door Access Panel Overview**.

Figure 3.9. Panel HTTP Configuration Overview



There are two pages in the web interface which can be accessed with the navigation panel on the left side of the page. **Overview** (the main page) shows read only Panel information. **Panel Setup** is where you can override the Panel communication settings.

Overview: On the overview page you can see Panel status and configuration. Some of the noteworthy sections include: the Panel Name, the Firmware Version, Communication mode (how it obtains its IP address), assigned IP address, MAC address, the Server Name, Server IP and Server Connection Mode (IP or name) the Panel is using to connect to the server. For each Door: the Mode of the Door (which of the 8 Door states the Door is currently in), State (open or closed, if the Door has a Door contact) and the Lock State (locked or unlocked).

Panel Setup: On the Panel setup screen, you'll be able to change communication settings on the Panel: the Panel Com Mode (how the Panel obtains its IP address), Panel IP (will not be set unless Panel com mode is static IP), Server Name (if communicating to the server by name), Server IP (if communicating to the server by IP address), Server Connection Mode (the communication method the Panel will use to find the server), and the HTTP Server Mode (enables the Panel web interface). Once you have entered any changes, you can press **Set Panel Configuration** to save the changes.

Warning

Changes in this interface that are saved will override any manually entered information, or configuration obtained from the VAX software. If changing communication methods in the interface, we advise making those same changes in the VAX software. The **Panel Setup** screen should only be used for initial configuration or when the server information has changed.

Adding a Panel to VAX Access Control

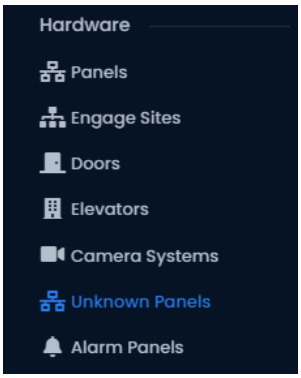
This section will cover the basic process of adding a Panel in VAX Access Control. In most deployments it is a fairly easy process and can be done in two different ways.

Method 1: Adding a Panel Unknown Panels Screen

This section will cover adding a Panel to the software after the Panel has been configured to look for the server.

The Panel is configured to find the server by **Name** or **IP Address**. (Please see the section called “Panel IP Settings: Static IP” and the section called “Communication Mode Configuration: Server Name (DNS)” for details on configuring a Panel to find a VAX Access Control server.)

1. Access your VAX Access Control system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. In the left navigation menu, click on **Unknown Panels** under the Hardware section at the bottom of the navigation menu.



4. On the Unknown Panels screen, any Panels that communicate successfully to the server that have not been added yet will appear in this list. Name, MAC address, IP Address, Panel Type, Firmware Version will be displayed.

Tip

If you're not sure which MAC address belongs to which controller, you can access the Read Only menu on a Panel by pressing and holding the ESC key for 4 seconds. Use the white buttons to find Item 7, Panel MAC Address.

5. When you've identified the Panel you'd like to add, click the + button to the left of the panel name. You'll be taken to the **Add Panel** screen with the MAC Address, Panel Model and IP information fields pre-populated.
6. Please proceed to the section called “Adding a Panel: Basic Configuration” for continued instructions on adding a Panel.

Method 2: Adding a Panel Manually With MAC Address

This section will cover adding a Panel manually in VAX Access Control. You may choose this method for the following reasons:

- You have not yet configured the Panel to communicate with the server.
- You are pre-configuring the software prior to the deployment of the Panels.

The following information should be collected prior to manually adding Panels:

- The Panel model (on the box the Panel came in) for each Panel (for full list of models, please see the relevant section within the master tech guide.
- MAC address of each Panel.
- If the Panels will be using DHCP or static addresses.
- Location of the Panels (generally used for naming the Panels).
- If the Panel is a Door Panel, will it be using a Door contact?

Note

If all this information is not available, you can use placeholder values for the MAC addresses and names.

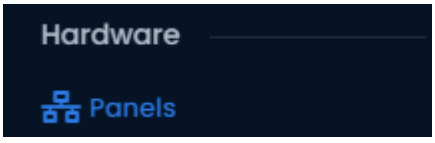
Once you've collected this information, we can now begin adding the Panels. Please proceed to the section called “Adding a Panel: Basic Configuration”.

Adding a Panel: Basic Configuration

This section will cover the various fields that need to be populated in order to add a Panel in VAX Access Control. It is advised to fill them in the order they are shown on the screen, the exception being the MAC address if it is pre-populated.

If you are not already on the **Add Panels** screen:

1. Access your VAX Access Control system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. In the left navigation menu, click on **Panels** under the Hardware section at the bottom of the navigation menu.



4. On the **Panels screen**, click the **Add** button.

On the **Add Panel** screen you'll be presented with several drop-down menus, text fields and check-boxes to populate. If you navigated to this page from the Unknown Panels screen, most information will be auto filled for you.

Figure 3.10. Add Panel Screen

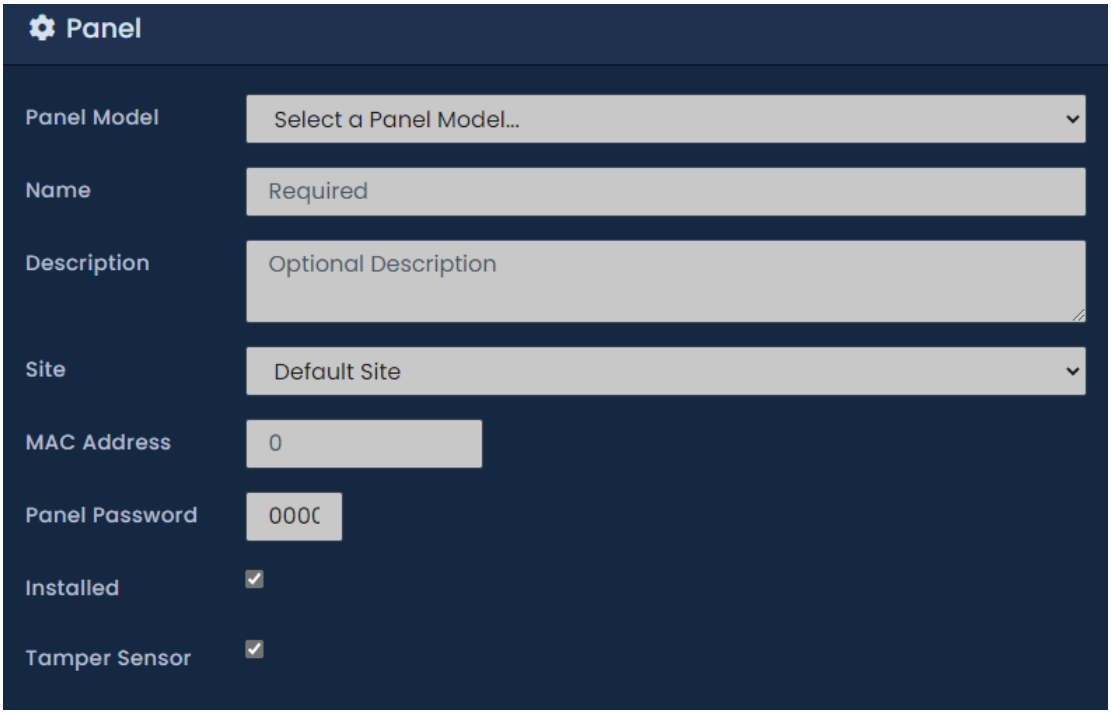
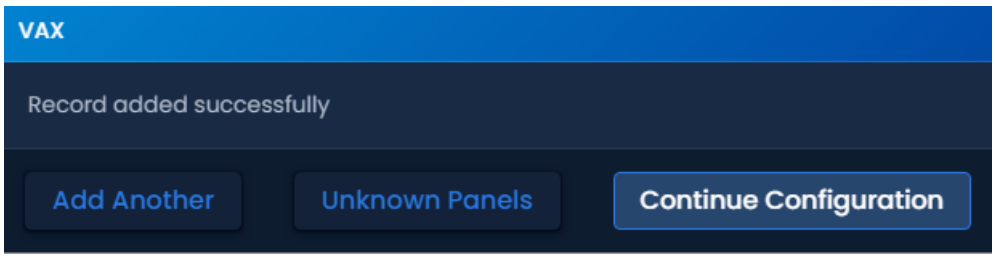


Table 3.11. Add Panel Fields

Drop-down/Text Box/Checkbox	Description
Panel Model	Select the Panel model using this drop-down menu; depending on the model you choose, additional options may be displayed.
Name	The name of the Panel; we recommend naming the Panel based on its location on the site. Accepts 4 to 60 characters.
Description	Optional description of the Panel. Accepts 0 to 255 characters.
Site	Select the site the Panel will reside on. This cannot be changed once the Panel is added.
MAC Address	The unique network address built into every Panel. May be pre-populated if you're adding the Panel through an Unknown Connection From Panel Notification. Must be 12 characters.
Panel Password	The password is required for access to the administration menu built into the Panel. Valid values are 0 to 9999. The default value is '0000'.
Installed	Sets whether the panel and its devices should appear in System Overview or other status pages.
Tamper Sensor	Uncheck to automatically disable the integrated tamper sensor once the Panel is added.
Door Contacts	Uncheck if there are no Door Contacts attached to the Panel.
Auto Add Doors	Check if you want to automatically add Doors to this Panel. They will be named based on the name of the Panel. For example, name "Front Panel" will add a door named "Front Door".
Expanders (select models only)	Number of expander modules. Either IO or door modules. Enter the correct amount (1-8 for IO modules, 1-4 for door modules).

Drop-down/Text Box/Checkbox	Description
Connection Mode	Method in which the Panel will obtain its IPv4 address. If you have manually configured an IP address on the panel, you will need to set this to Static IP and fill in the networking details.

You can now click **Save**; you'll be asked to correct any information that is missing or invalid. Once corrected press **Save** again. A message box will appear that will say **Record added successfully** with the options to **Add Another** (which will take you back to the **Add Panel Screen**), **Continue Configuration** (which will bring you to the **Edit Panel Screen** where you can configure additional options that are covered in the section called “Advanced Panel Configuration”) or **Unknown Panels** which will bring you to the Unknown Panels list.



Warning

Prior to your first update to the Panels, we advise configuring the advanced settings of your Panels. This can be found in the section called “Advanced Panel Configuration”.

Where to Go From Here

You've now completed the two most important chapters in the book.

If you've just completed an installation of the software, we recommend you take a moment to explore and change the default password of the System Manager UI. For more information, please see Chapter 5, *System Manager UI*.

For information on the VAX license and information on licensing your software, please see Chapter 4, *Software Licensing*.

If you're ready to continue configuring a Panel, please see the section called “Advanced Panel Configuration”.

If you're inexperienced with access control, or would like to brush up on terminology specific to VAX, please see Chapter 6, *Planning an Access Control Deployment*. It contains more information for successfully planning a deployment, along with links to many different parts of this guide.

For support contact information, please see Chapter 37, *Support*.

Chapter 4. Software Licensing

This chapter will cover the software licensing aspect of VAX, information about the licensing process, how card formats work with our product license, and frequently asked questions about licensing your software.

VAX is a licensed product. Licensing helps us continue to develop and add new features to VAX. It also helps integrators maintain good end user relations, perform door hardware maintenance and can facilitate reoccurring revenue for the installer. Licensed software gives dealers and end users the benefit of low upfront costs. With a valid VAX license, your system is also entitled to free core software updates.

Note

VAX includes a 15 day trial license upon initial installation.

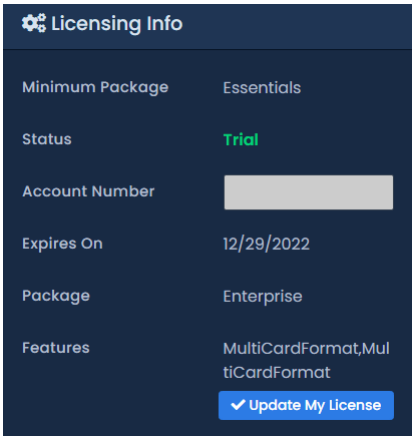
Licensing Your Software

Activating the software license on your VAX is simple by design. The License Options section is included as well in order to facilitate your choice of licensing tier as it will provide you with the necessary package to retain the features of your current configuration.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. In the left navigation menu, click on **Licensing** under the Administration section at the bottom of the navigation menu.

4. Ensure you have a valid account number in the **'Account Number'** field. If not, this can be obtained by contacting your dealer or installer.

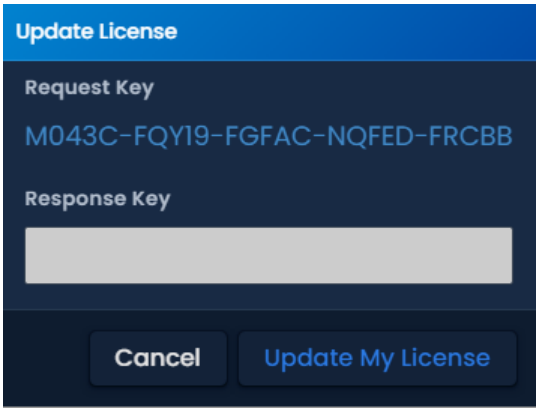
Figure 4.1. VAX Licensing Screen



5. The next step is to take note of your **'Expires On'** to determine if licensing is required at this time and make note of your software package.
6. Unless you are either within the last 30 days of your software license or you wish to change your software package there is no need to update your license. If you determine the license needs to be updated, continue on to the next step.

7. To generate a new license click the **'Update My License'** button at the bottom of the screen.

8. You will be presented with your new **Request Key**. Contact your dealer, installer or Vicon Industries (please see Chapter 37, *Support*) with this request key (only valid on the day it was generated). Your license options will be reviewed to determine the best license duration and software package for your needs and you will then be provided with a response key that will activate your software.



9. Once you have entered the **Response Key** provided by Vicon Industries, click **'Update'** to activate your license.

Note

The **Response Key** should be entered in all capital letters with the dashes between every 5 characters.

Supported Card Formats

Note

VAX supports a variety of card bit formats, however for simplicity and added security, we recommend using our 40 bit high-security credentials when possible. As part of your VAX license, you can have third party card formats locked out. This can add additional security to your systems by restricting the use of lower security credentials. For more information about other card formats and enabling them in your software license (free of charge) please contact Vicon Industries. See Chapter 37, *Support*.

FAQ for Software Licensing

Q: Will I receive notice before my license will expire?

A: Absolutely. Within the last 30 days of your license period, the VAX software will advise the software is about to expire and provide the exact expiry date.

Note

If email settings are configured, VAX will attempt to email any system administrators and the dealer that the license will be expiring soon.

Q: What happens when my software expires?

A: On the first login after a license has expired, a 10 day grace period will start. During this grace period all features will be available. All critical functions and existing configurations will continue to run after the software expires and the 10 day grace period is over - see the questions below for what will be available and what will not be available when the software expires

Q: What features will be available after my license has expired and my 10 day grace period is over?

A: After the license has expired and the 10 day grace period is over; a very small subset of features are available:

- Most screens are available in read only mode, including viewing users, holidays, access groups etc.
- Personal safety affecting features are maintained for your security. This includes
  - Pulsing Doors
  - Removing Users/Credentials
  - Overriding Doors, Floors, Inputs and Outputs
  - Override to Crisis Level
  - Removing Administrators, Changing Passwords and Modifying Permissions
  - Panel Commands (inc Update Panels, Reset Anti-Passback, Get Time, Disconnect Panel, Place Panel into Firmware Update Mode)
  - System Status
  - Updating License Information

Q: What features will not be available after my license has expired and my 10 day grace period is over?

A: The majority of changes to your system are disabled. This includes (but is not limited to):

- Adding Users/Credentials
- Adding/Modifying Holidays
- Changing Scheduless
- Viewing Cameras
- Viewing Reports

Q: Why does VAX require a license?

A: Early on in development we decided to go with a licensed approach for a few reasons.

- To provide a significantly lower upfront software cost in comparison to our competitors.
- To offer end-users the ability to pay for the features they need, ensuring that smaller sites that may not take advantage of the full VAX feature set are offered a price inline with what they need.
- To allow us to continue to upgrade and enhance the base VAX feature set and offer these updates at no additional charge to the end-user.
- To reduce software piracy.

Q: What license terms are available?

A: There are various levels of software licenses that are valid for 1 year or 5 years term license. Each tier increases certain aspects such as door/camera count. Please contact Vicon Industries for more information on these packages. (Please, see Chapter 37, *Support*).

Q: What does a VAX license entitle me to?

A: An active VAX license is always required to use the VAX software and this license will entitle you to all software updates for the term of the license. This includes any additional features and enhancements added within your software package.

Q: Is my software license still valid if I change the computer that hosts the VAX software?

A: Upon restoring a VAX database to a different computer it will automatically invalidate your license. However, you are not charged a fee to license the new computer. Contact Vicon Industries to have your license re-armed, which will provide you a valid software license for your new PC carrying over the remaining time of your previous license and your licensed software package.

Chapter 5. System Manager UI

The System Manager UI is a separate web interface used for management purposes such as running database backups, starting or stopping the main application web service, changing network settings, etc.

Accessing the System Manager UI

Accessing the System Manager UI is a very similar procedure to accessing the VAX web interface; the primary difference is that it is hosted on a different port (11002).

1. **Accessing System Manager UI from the PC the Server is Installed on**

   During installation, a shortcut is placed in your Start menu for **System Manager UI**. The link for **System Manager UI** can be located by clicking Start -> All Programs -> VAX and finally clicking on **"Launch VAX System Manager"**.

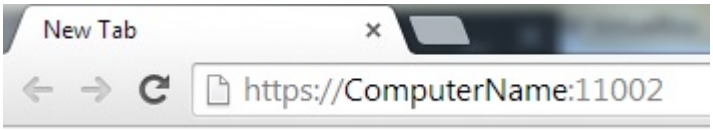
   Accessing System Manager UI from a Remote PC

   Open your web browser and within the address bar enter the address to the **System Manager UI** software using the format: **https://*NameOfTheComputer*:PortNumber** .

   Alternatively, you can also access the **System Management UI** through IP address using the format: **https://*192.168.0.100*:PortNumber** .

   ### Example 5.1. Accessing System Manager UI Remotely

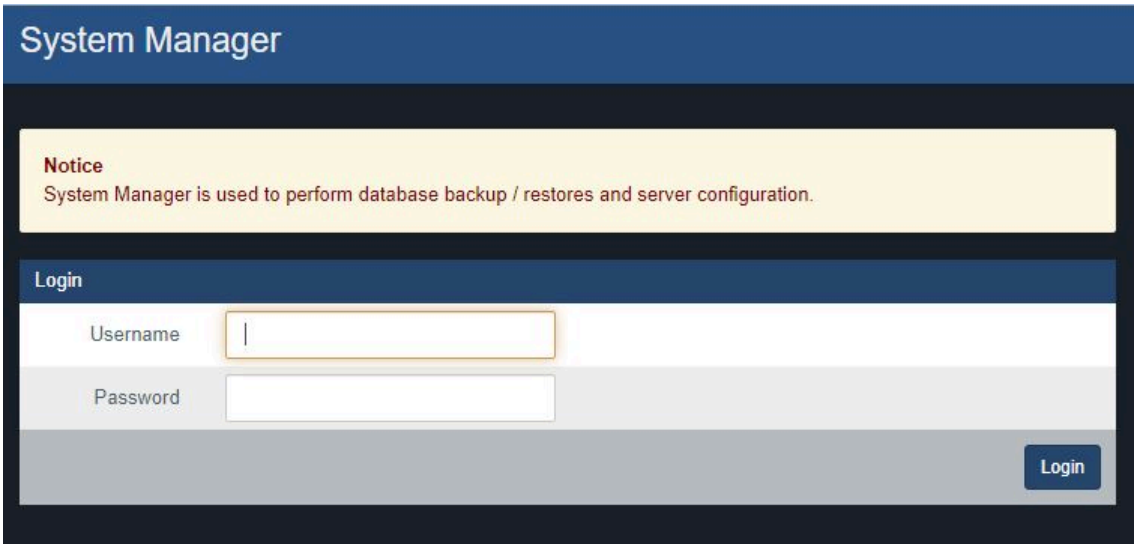
   https://*ComputerName*:11002 (default port is 11002)

   Once you have entered the address, press enter to navigate to the VAX **System Manager UI**.

2. You will see a temporary splash screen and then you should be presented with the login window.

   ### Figure 5.1. System Manager UI Login Window

Default Username and Password for System Manager UI

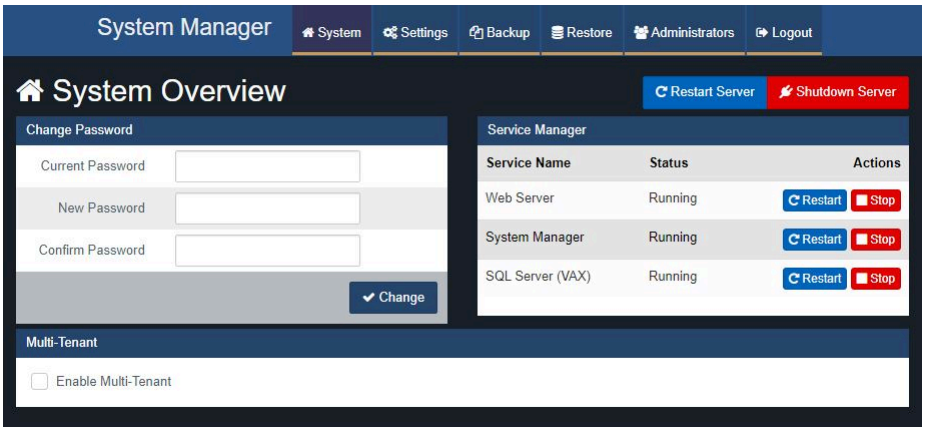
The default Username is 'vicon' and the default password is 'viconaccess' (case sensitive and without the quotes).

Caution

We recommend changing the default **System Manager UI** password as soon as possible.

3. Upon logging in you will be presented with the **System Screen.**

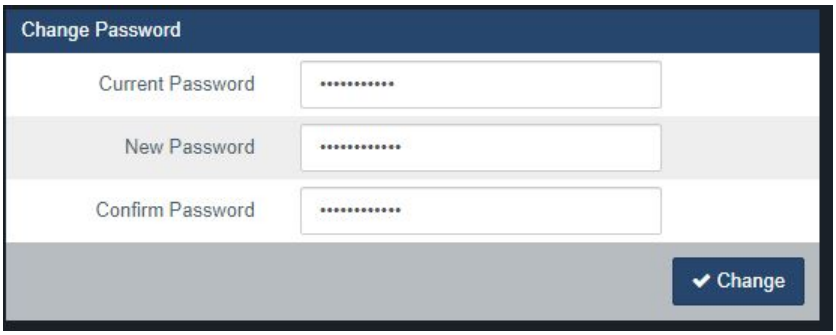
Figure 5.2. System Manager UI System Screen



Changing System Manager UI Password

1. Click on **'System'** in the top menu when logged into the system manager UI.
2. On the **System Screen**, there will be a Change Password section on the left side of the screen.

Figure 5.3. Change Password Section



3. Enter your current password (default is 'vaxaccess') followed by the new password twice.
4. Click **'Change'** to complete the password change procedure.

Backing up your VAX Database

1. Access the System Manager UI. (Please, see the section called “Accessing the System Manager UI”.)
2. Click on **'Backup'** in the top menu.

3. Select the Items you wish to backup (default settings are recommended).

   - **Database**

     The VAX database (recommended).

   - **Profile Pictures**

     Images associated with your Users (cardholders) (recommended).

   - **Maps**

     Images associated with any graphical maps.

4. Select your backup options (default settings are recommended).

   - **Compress Backup**

     Determines whether the backup file is compressed upon successful backup (recommended).

   - **Remove Files Older then X Days**

     Automatically removes .prbak files from the backup location if the age exceeds the number of days specified. Adjust to keep more backups or uncheck to keep all backups until they are manually deleted.

   - **Encrypt Backup with password**

     Check if you would like a password to be required to restore the backup.

5. Determine where your backup will saved to. We offer support for either a local drive, USB drive or a network share.

Caution

The Windows user running the System Manager service must have appropriate access to desired output folder. The default Windows service account is "NT SERVICE\VAXSysManager". In the case of backing up to a network drive, it may not be possible to give read and write access to the default service account the System Manager service runs as. In this case you will need to reinstall the software and specify a different Windows account that does have access to that network drive. Please see the relevant section within the master tech guide for more information.

Backup to Local or USB Drive

- The text box below can now be filled with a path to a backup location, including a local drive or USB. The format of the path looks like: **"C:\Backup"**

Note

If the folder you entered in the 'Output to' text field does not exist, it will be created.

Backup to Network Share

- Enter the path of your network share.

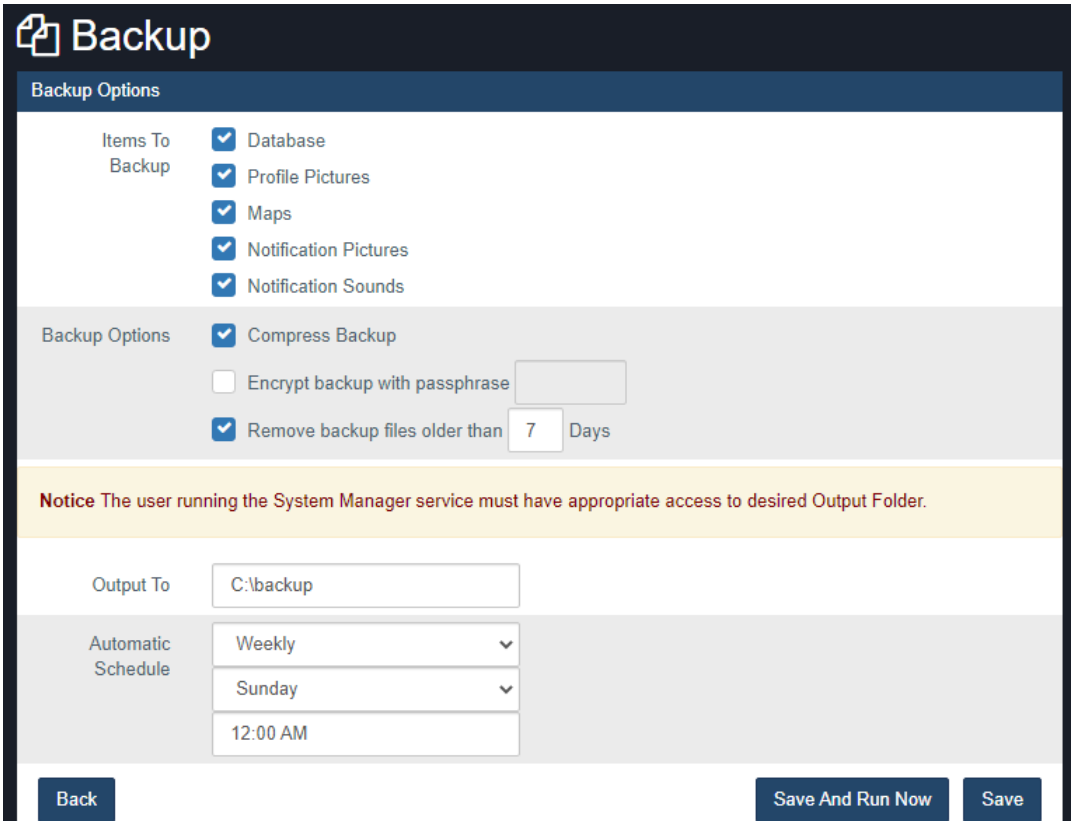
Example 5.2. Network Share Example

\\Servername\PathToMyBackupShare

6. Select a Backup Schedule.
   - **Disabled:** No automatic schedule. Backup is initiated by hitting the **'Save and Run Now'** button.
   - **Daily:** Backup occurs once a day at the time specified.
   - **Weekly:** Backup occurs once a week on the day of week and time specified.
7. If you wish to run the backup immediately, click the **'Save and Run Now'** button. Alternatively click the **'Save'** button to save your backup settings and run on the next scheduled time (if a schedule is defined).

   If folder or network permissions prevented the backup from being written you will see an error. When performing your first backup you should browse to the output and verify the backup has been written. This may take several minutes for larger databases.

Figure 5.4. System Manager Backup Screen



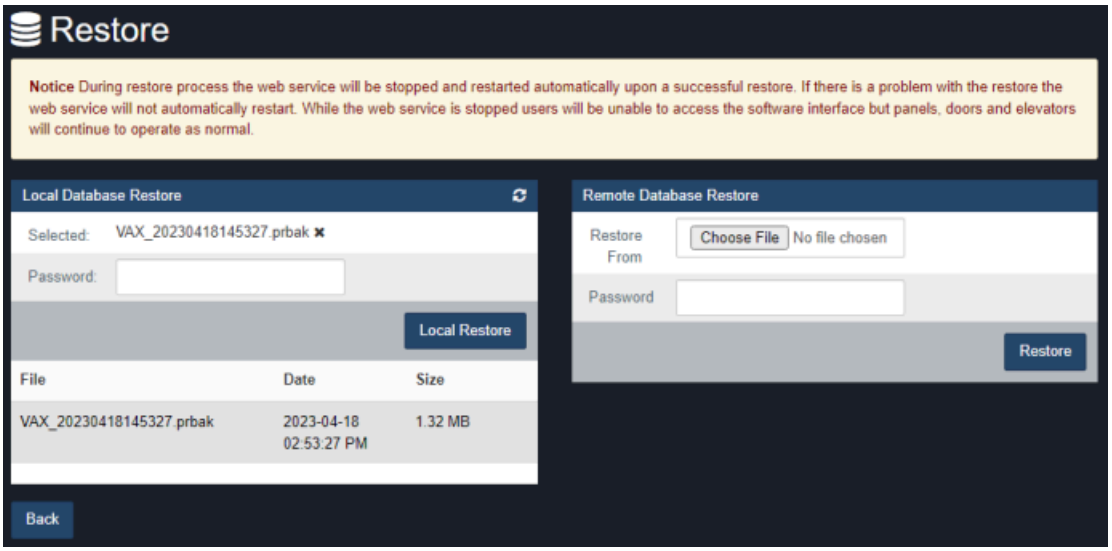
Note

If you are having trouble performing a backup of your database using the **System Manager UI**, there is a manual method to perform backups that is detailed in the section called “Performing Manual Back-up and Restore with MSSQL Command-Line”.

Restoring Your VAX Database

1. Access the System Manager UI (see the section called “Accessing the System Manager UI”).
2. Click on **'Restore'** in the top menu.

Figure 5.5. Restore Database



3. On the left side of the screen will you will see any existing backup files found in the configured backup folder.

4. You may restore by directly selecting a database backup from the list or use the Choose File button to manually select a database backup file. A backup that was performed on March 25th 2022 would be called "VAXfullbackup_20220325010349.prbak".

Restoring from Backup File

- Optionally enter the password if a password was used during backup.
- Click the **'Restore'** button or **Local Restore** button.

5. The database will now be restored**. If the restore process fails**, we recommend trying it again. If it continues to fail there is a manual method to perform the database restore detailed in the section called “Performing Manual Back-up and Restore with MSSQL Command-Line”.

Warning

During restore process the web service will be stopped and restarted automatically upon a successful restore. If there is a problem with the restore the web service will not automatically restart. While the web service is stopped users will be unable to access the software interface but panels, doors and elevators will continue to operate as normal.

Service and System Management

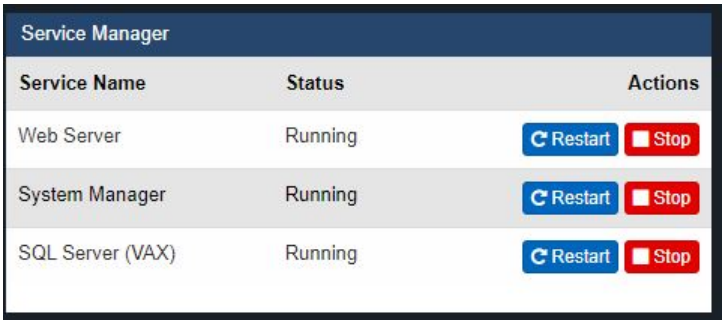
The **System Manager UI** allows for control over the VAX web server service and the SQL Server service being used by VAX. As well as providing the ability to reboot or shutdown your system, this is useful when the PC is not easily accessible and provides a quick method of restarting the services or to check if it is running.

Managing Services

1. Click on **'System'** in the top menu when logged into the system manager UI.

2. You will see a Service Manager section for the VAX Web Server and SQL Server.

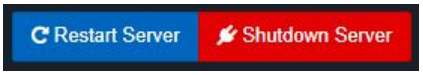
Figure 5.6. Managing Services



3. From here you may Start/Stop/Restart and see the status of the services.

Shutting Down or Restarting Your Server

1. Click on **'System'** in the top menu when logged into the System Manager UI.
2. **Figure 5.7. Shutting down or Restarting your server.**



3. You will see two buttons corresponding to rebooting or shutting down your system.

Networking Settings in System Manager

The **System Manager** now provides limited support for configuring your network. This is not meant to replace the network configuration options within Windows, but rather provide a simpler interface for changing or checking basic network settings. For advanced setup we encourage you to use the traditional Windows networking options.

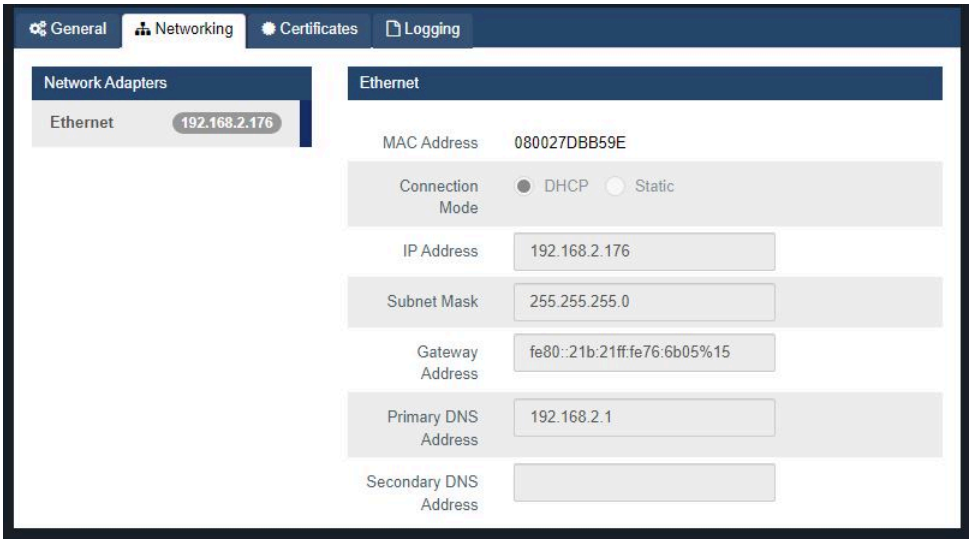
Caution

Changing network settings can cause a loss of connection to the System Manager and the VAX software. Please take care in ensuring you are entering valid network configuration options. If you are unsure of the correct values please contact your system administrator.

Configuring Your Network

1. Click on **'Networking'** in the top menu when logged into the System Manager UI.
2. You will now be presented with the network configuration page.

Figure 5.8. Network Configuration Page



Note

Changing your host-name will require a system restart.

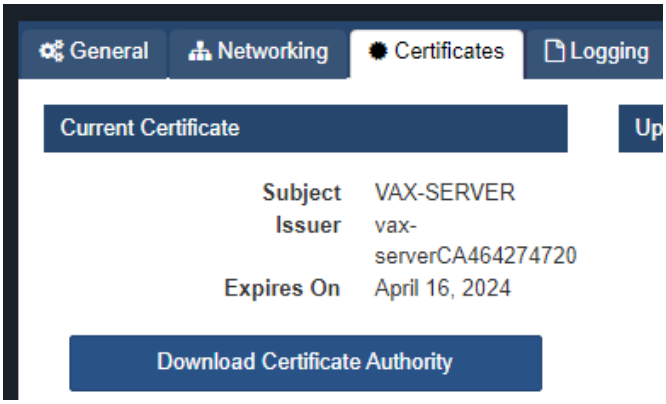
SSL Certificates

This section of the manual will cover **SSL certificates** and how to install/manage them within **System Manager**. This will cover the default Self-Signed Certificate, as well as how to import your own into System Manager. As well, it will give a general guide on how to export your self-signed certificate and how to install it into the computers Certificate Store allowing the bypass of the "Connection is not Secure" message.

Introduction to Certificates

Within the **System Manager** page of **VAX**, the user can navigate to the Certificates sub-tab under the Settings Tab. The user will be presented with 2 elements. **Current Certificate**, which will show the current certificate installed, it's subject, the issuer and when it expires. Second is the **Update Certificate** section which allows the user to choose what kind of certificate/method they wish to install and use. Selecting choices here will **dynamically change** the section below which is used for generation of the self-signed certificate, options for uploading and installing **PEM** or **PFX certificates** and lastly a list of certificates in your PC's Certificate store.

Figure 5.9.



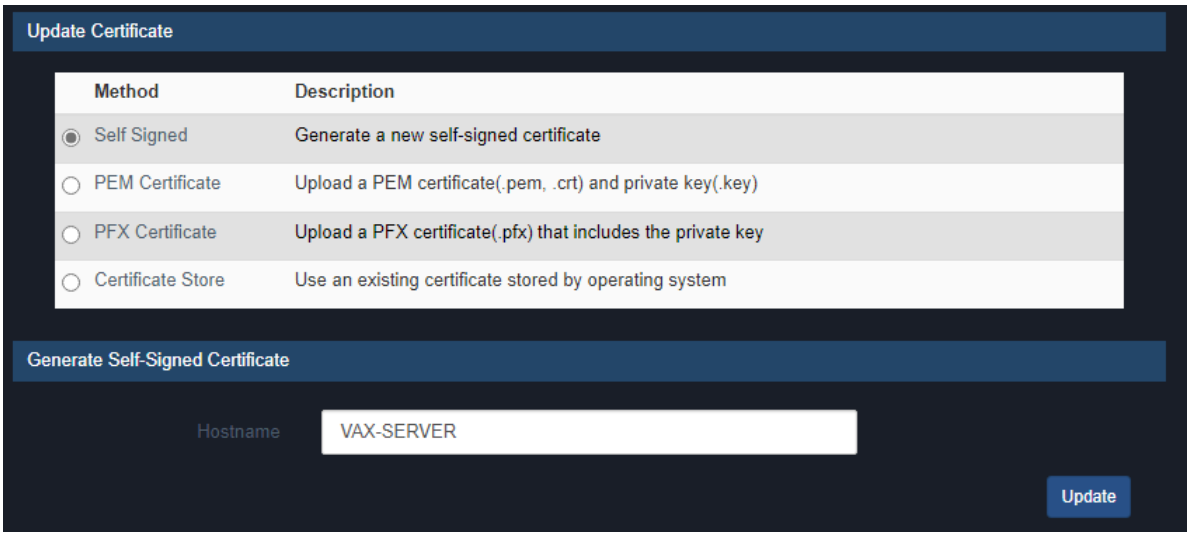
Self Signed Certificates

During the initial installation of **VAX**, the user will be presented with an option to generate a **self-signed certificate.** This however is not the only place this can be done. Post installation, the user can generate a new one via the System Manager. Use cases for this include expiring certificate as well as changes like computer Hostname changes that could impact reachability. The user will be presented with a box which should automatically be filled in with the computers Hostname. This can be changed as needed. Clicking Update will shutdown the VAX services and install the newly generated certifiate.

Tip

Using a Self-signed certificate will result in the user being presented with an Unsecure Connection warning message upon browsing to the server as it is not signed by a valid and recognized certificate authority. Bypassing this will be covered in another section.

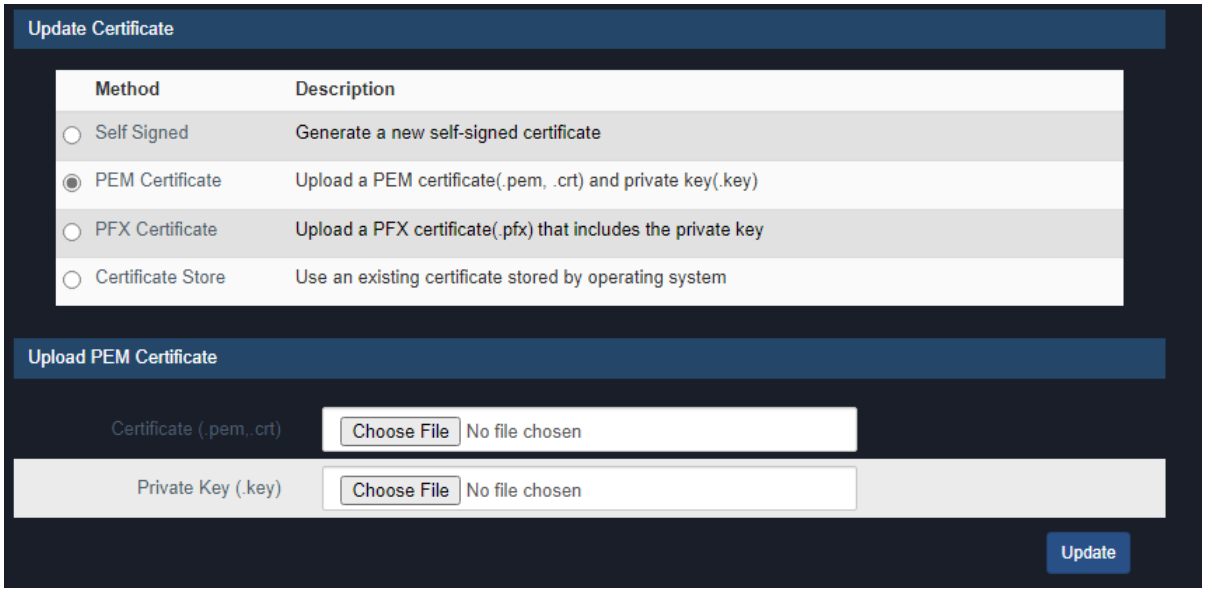
Figure 5.10.



PEM Certificates

PEM certificates are a pair that comes with two files. The **certificate file (either a .pem or .crt)** and the **private key file (.key).** Both of these are required as the private key essentially confirms the certificate is a valid certificate from a verifed **Certificate Authority (CA)**. The process of obtaining these are beyond the scope of this manual, for further information on obtaining these, please reach out to your IT specialist or the provider the Certificate was purchased from. The actual proccess of the installation is simple. Just upload the two files to the respective upload boxes and click update. Services will reboot and once up and running the user can verify by browsing to the server in a web browser and checking if the Certificate shows as valid in the Web Browser.

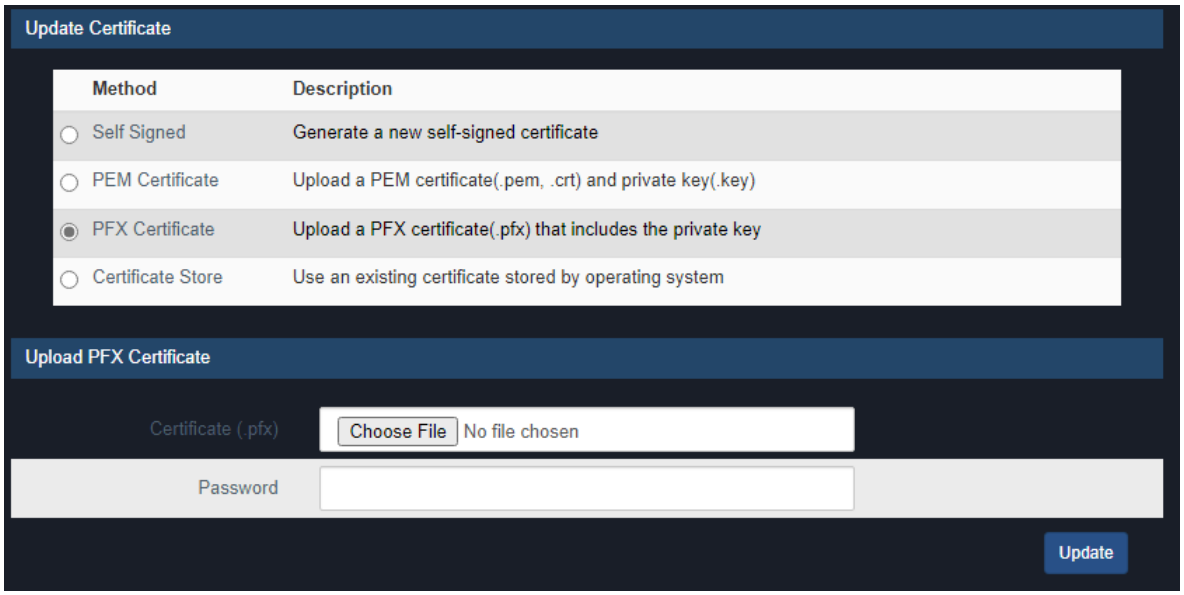
Figure 5.11.



PFX Certificates

PFX certificates are a bit different than PEM. Rather than having the Certificate file and the Key file, it has instead been combined into one single password protected file. Typically this password is set when generating the CSR in IIS or a 3rd party tool like Digicert. **This part falls out of scope of the manual and recommend reaching out to your IT Specialist or Cert provider**. To install the certificate, you simply upload the **.pfx file** into the upload box and provide the password used to encrpyt it. Click update and the services will reboot once the certificate is installed. Users can verify the certificate is working by browsing to the server in a web browser and checking if the Certificate shows as valid in the Web Browser.

Figure 5.12.

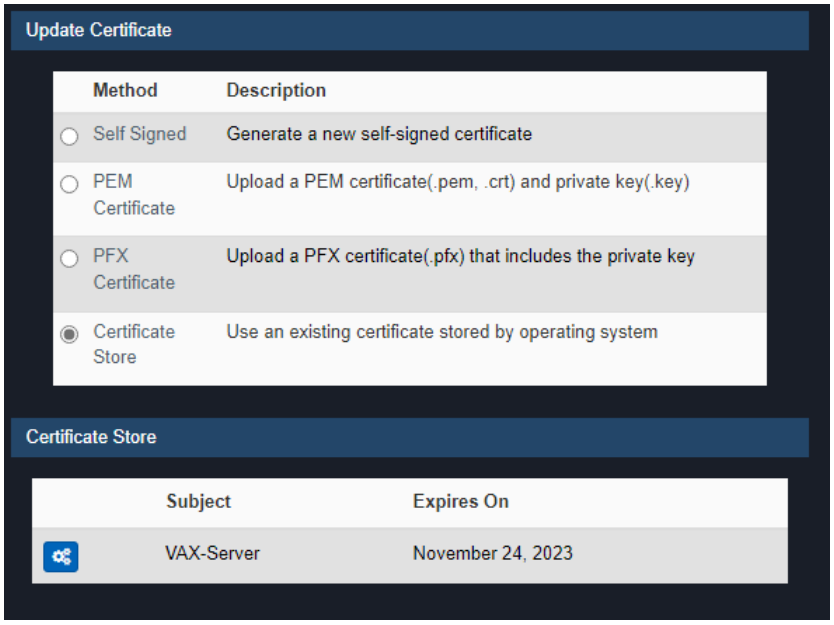


Certificate Store

In many cases, if the company running the Server has their own SSL certificate in use, it can also be used for **VAX**. These certificates are likely already installed into the PC or User certificate store itself

and can be selected and applied. Like the other methods, the services will reboot once the certificate installation is completed. Users can verify the certificate is working by browsing to the server in a web browser and checking if the certificate shows as valid in the web browser.

Figure 5.13.



Installing a Certificate into the Certificate Store

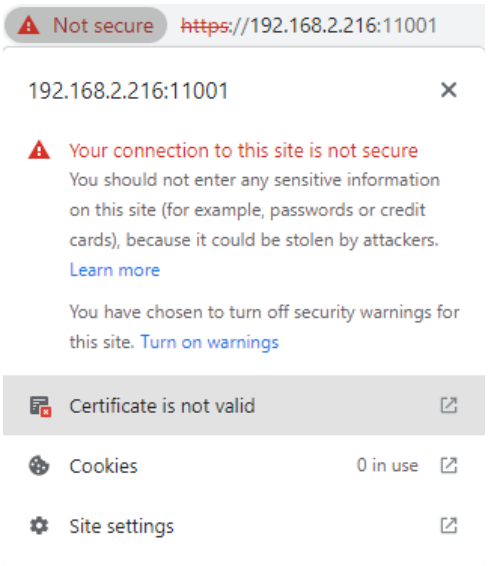
When using a Self-Signed certificate, as mentioned above, the user will be presented with a Connection Unsecure page when browsing to the server in a web browser. There is method which will be detailed below to bypass.

Note

This does not actually secure the connection or validate the certificate. This process differs slightly between web browsers. The guide below will be using Google Chrome as the template.

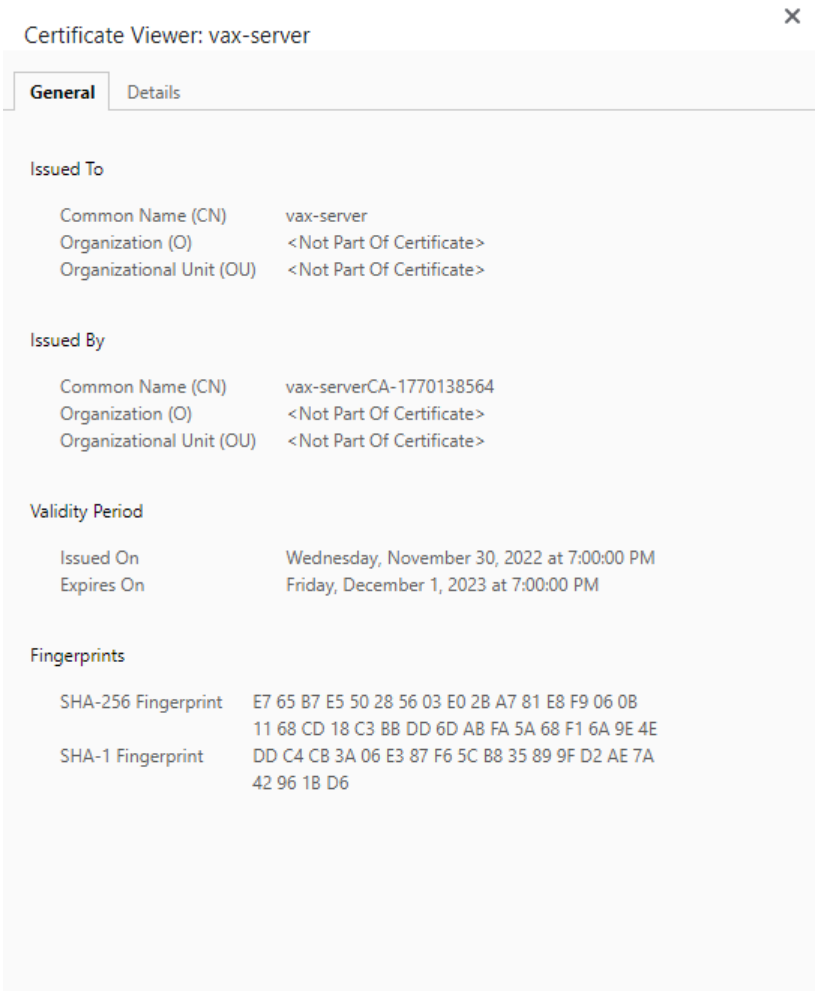
1. Browse to the server in question and click where it says **"Not Secure"** to the left of the URL and click **"Certificate is not Valid"**

Figure 5.14.



2. A new window will come up, in the bottom right corner there will be an "Export" button. Click this and select a location to save the certificate file to.

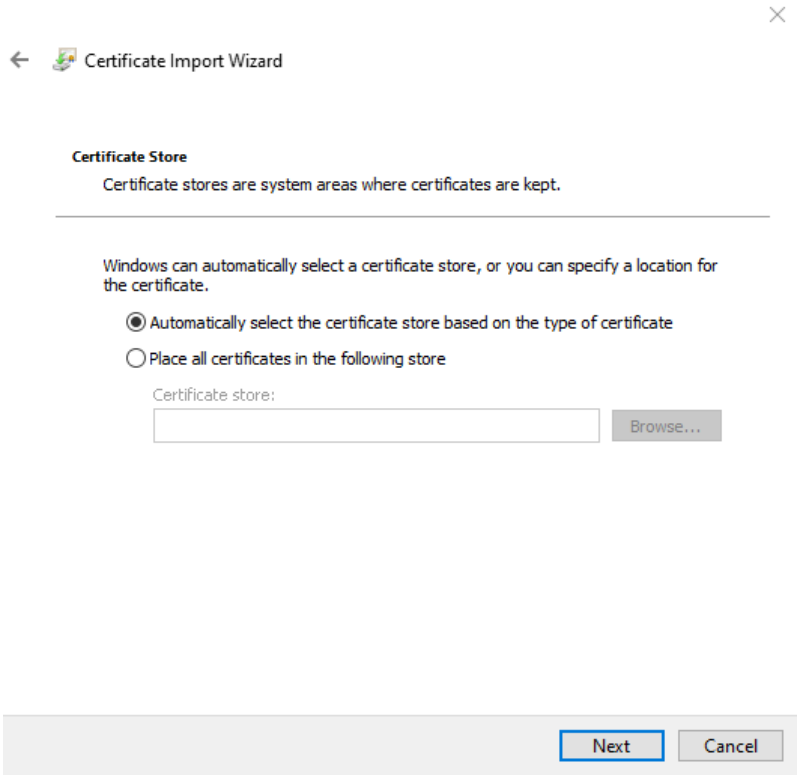
Figure 5.15.



3. Double click the newly saved certificate file. THis will present the user with a SSL certificate import wizard. Click "Install Certificate" to begin the process. The user will be presnted with a store location - Choose "Local Machine" and click Next.

4. Leave the default option to allow Windows to automatically pick the store we are installing it to and click Next. This last page will give a summary of the changes, user can click Finish here. To see this in effect, reboot the web browser and clear the browswer cache. There should no longer be any messages about an unsecure connection. For further troubleshooting, it is recommended to reach out to your IT Specialist as anything beyond this falls out of scope of Vicon Support

Figure 5.16.



Multi-Tenant

Multi-Tenant is configured from the System Manager UI. Please see the section called “Multi-Tenant Mode Configuration” for more information on this feature.

Chapter 6. Planning an Access Control Deployment

This chapter is meant to help technicians in their planning stages of VAX deployments, and can also help end-users and installers understand the terminology/concepts specific to our software. The hardware section will cover the topology of how our product communicates, the cables and standards commonly used with our product and references to diagrams in other chapters of this book. The software sections will go over the order of operations and the concepts of major software components.

Hardware

This section will go over hardware specifications, the communication topology of how our Panels interact with the VAX server and how to identify a Panel model on the physical Panel.

There are 4 main pieces of hardware that are used in different combinations. The following table describes them.

Note

The following table is a list of sub assemblies. When ordering you will use separate part numbers which will contain 1 or more of these sub assemblies along with accessories, enclosures and other needed parts.

Table 6.1. Hardware Boards

Hardware	Description
VAX-1D-1/ VAX-2D-1	PoE powered door controller with integrated lock power, aux relays and inputs. Communicates over Ethernet. Can be ordered with several options and firmware configurations. Controls 1-2 doors depending on firmware loaded.
VAX-EXP-2D	12VDC powered 1-2 door controller. Requires VAX-MDK for communication and power distribution. Communicates on RS485 bus.
VAX-IO-EXP8-PCB	12VDC powered input/output controller. Requires VAX-MDK for communication and power distribution. Communicates on RS485 bus.
VAX-MDK	12-13.5 VDC powered controller. Communicates and distributes power to up to 4 VAX-EXP-2D modules as an 8 door controller or with up to 8 VAX-IO-EXP8-PCB modules to control up to 64 inputs and outputs or up to 64 elevator floors (one additional VAX-EXP-2D required for elevator reader ports).

Hardware Specifications

Figure 6.1. VAX-1D-1/VAX-2D-1

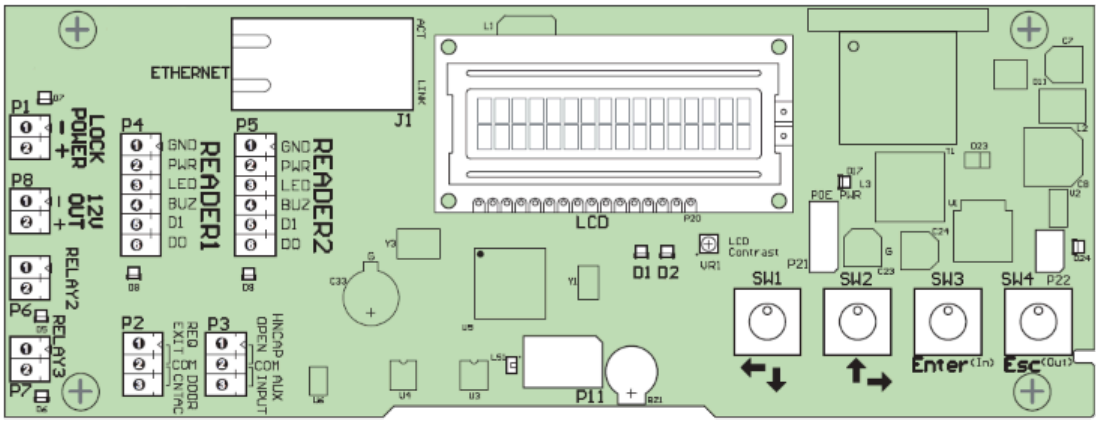


Table 6.2. Hardware Specifications VAX-1D-1/VAX-2D-1

Category	Item and Description
Power	
Supply	802.3af PoE (providing up to 20 W)
Lock Power	Solid State 12VDC 500mA / 24 VDC 250 mA (with opt. converter) with over-current protection
Auxiliary Output	12 VDC 500mA (shared with reader ports current)
Network	
Speed	10/100 Mbps
Modes	Static or DHCP
MAC	Unique
Outputs/Inputs	
Lock Relay	1 x Wet Contact Solid State Relay
Auxiliary Relays	2 x Dry Contact Solid State Relay (24VDC 1A limit)
Inputs	4 x Supervisor or Digital (REX, Door Contact, HDCP Opener, Auxiliary)
Reader	
Reader Port	2 x Wiegand (D0, D1, BUZ, LED, VCC 12VDC 500mA, GND)
User Interface	
LEDs	2 x Power Indicator 2 x Reader Data Flow Indicator 3 x Relay Status Indicator 2 x Ethernet Status Indicator 2 x On-Board Info 3 x Off-Board Info (PIR)
LCD Display	1 x 16 channel, 2-line LCD with Backlight
Push Buttons	4 x Tactile Switch

Category	Item and Description
Sound	1 x 90 db Piezo
Integrated Motion	
Passive PIRs	5.0 m Detection Performance 94° Horizontal / 82° Vertical Detection Area 64 Detection Zone 170uA Consumption Tri-Color LED (Red, Green, Orange)
Protection	
PoE	In-Rush Current Limit and Overall Current Limit
Over-Current	Strike, Relays, 12VDC Output
Surge	Strike, Readers, Inputs
Tamper	Photo Tamper Sensor
Time Keeping	
Date/Time	1 x On-Board Real-Time Clock (no battery required - maintains up to 1 month without power)
Memory	
Flash Memory	8.0 Mb
Housing and Back Plate	
Molded ABS Plastic	Removable Cover for Quick Access Flat Surface Mount Back Plate w/Cabling Port Available in Black Matte Finish; Off-White Available. Paint-able
Options	
Loud Buzzer	100 db at 100 cm (3 feet)
Dry Contact Converter	Converts Wet to Dry Contact
Expansion Boards	Extra Memory, Elevator Expander Panels, I/Os (for future expandability)
RS-485 Plug-In Module	Used for communicating with Assa Abloy Aperio products and the Elevator Expander Boards

Figure 6.2. VAX-EXP-2D

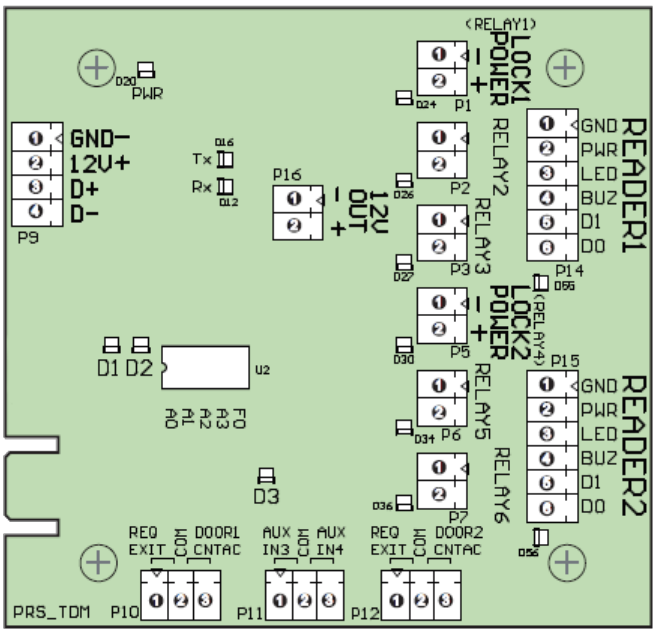


Table 6.3. Hardware Specifications VAX-EXP-2D

Category	Item and Description
Power	
Supply	1 x 12VDC power input provided by VAX-MDK or from external power supply. Up to 1.25A approximately.
Lock Power	2 x Solid State 12VDC 500mA / 24 VDC 250 mA (with opt. converter) with over-current protection
Auxiliary Output	1 x 12 VDC 350mA (shared with reader ports current)
Network	
Communication	RS485 bus communicating to VAX-MDK. Star or daisy chain supported.
Outputs/Inputs	
Lock Relay	2 x Wet Contact Solid State Relay 12VDC 500mA
Auxiliary Relays	4 x Dry Contact Solid State Relay (24VDC 1A limit)
Inputs	6 x Supervisor or Digital (REX, Door Contact, HDCP Opener, Auxiliary)
Reader	
Reader Port	2 x Wiegand (D0, D1, BUZ, LED, VCC 12VDC 350mA, GND)
User Interface	
LEDs	2 x Power Indicator 2 x Reader Data Flow Indicator 6 x Relay Status Indicator 2 x RS485 Status Indicator 2 x On-Board Info
Protection	
12VDC input	In-Rush Current Limit and Overall Current Limit

Category	Item and Description
Over-Current	Strike, Relays, 12VDC Output
Surge	Strike, Readers, Inputs
Tamper	Photo Tamper Sensor
Dimensions	
Steel Enclosure	29 cm (W) X 43.5 cm (H) X 7.5 cm (D) (11.41” X 17.41” X 2.95”)
PCB Dimensions	9.5 cm (W) X 9 cm (H) (3.740” X 3.543“).
Options	
Loud Buzzer	100 db at 100 cm (3 feet)
24 VDC Converter	Converts 12VDC to 24VDC
Dry Contact Converter	Converts Wet to Dry Contact

Figure 6.3. VAX-IO-EXP8-PCB

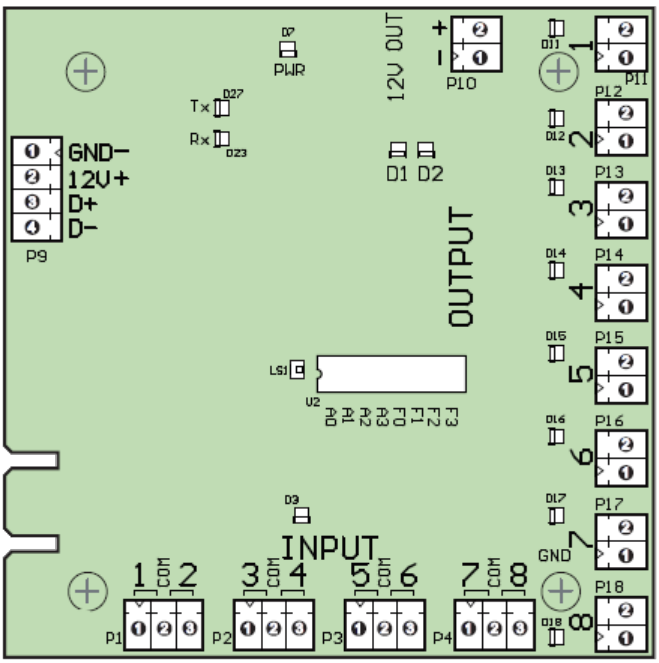


Table 6.4. Hardware Specifications VAX-IO-EXP8-PCB

Category	Item and Description
Power	
Supply	1 x 12VDC power input provided by VAX-MDK or from external power supply. Up to 0.35A approximately.
Auxiliary Output	1 x 12 VDC 350mA
Network	
Communication	RS485 bus communicating to VAX-MDK. Star or daisy chain supported.
Outputs/Inputs	
Auxiliary Relays	8 x Dry Contact Solid State Relay (30VDC 1A limit)
Inputs	8 x Supervisor or Digital
User Interface	
LEDs	1 x Power Indicator

Category	Item and Description
	8 x Relay Status Indicator 2 x RS485 Status Indicator 2 x On-Board Info 1 x Input Activity
Protection	
12VDC input	In-Rush Current Limit and Overall Current Limit
Tamper	Photo Tamper Sensor
Dimensions	
Steel Enclosure	29 cm (W) X 43.5 cm (H) X 7.5 cm (D) (11.41” X 17.41” X 2.95”)
PCB Dimensions	9.5 cm (W) X 9.5 cm (H) (3.740” X 3.740“).
Options	
Loud Buzzer	100 db at 100 cm (3 feet)
Dry Contact Converter	Converts Wet to Dry Contact

Figure 6.4. VAX-MDK

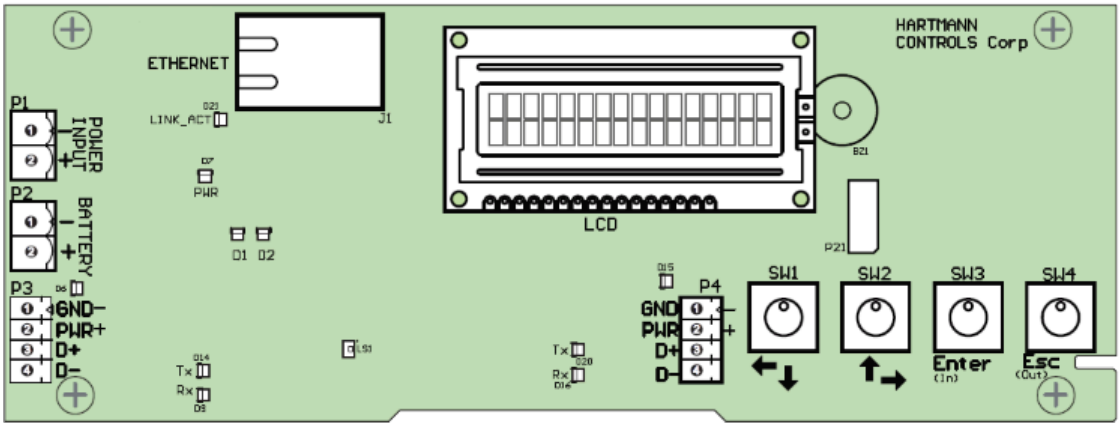


Table 6.5. Hardware Specifications VAX-MDK

Category	Item and Description
Power	
Supply	1 x 12-13.8 VDC Input. Up to 6A of current. 5A typical.
Battery Backup	1 x connection to supplementary external battery backup (12-13.8VDC in). Primary backup power should be located in external power supply.
Power Output	2 x 12VDC output for connection to VAX-IO-EXP8-PCB or VAX-EXP-2D modules. Up to 2.5A per output. 5A total.
Network	
Speed	10/100 Mbps
Modes	Static or DHCP
MAC	Unique
Communication	2 x RS485 outputs for communication to up to 4 VAX-EXP-2D modules or 8 VAX-IO-EXP8-PCB modules.
User Interface	

Category	Item and Description
LEDs	3 x Power Indicator 1 x Ethernet Status Indicator 2 x On-Board Info 4 x RS485 Status Indicator
LCD Display	1 x 16 channel, 2-line LCD with Backlight
Push Buttons	4 x Tactile Switch
Sound	1 x 90 db Piezo
Protection	
Over-Current	12VDC outputs
Surge	12-13.8VDC Input
Tamper	Photo Tamper Sensor
Time Keeping	
Date/Time	1 x On-Board Real-Time Clock maintains up to 1 month without power)
Dimensions	
Steel Enclosure	29 cm (W) X 43.5 cm (H) X 7.5 cm (D) (11.41” X 17.41” X 2.95”)
PCB Dimensions	9.5 cm (W) X 9.5 cm (H) (3.740” X 3.740“).

Communication Topology

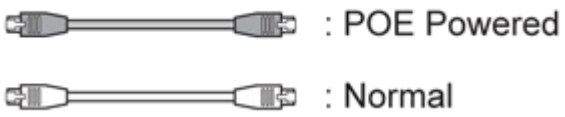
This section goes over the overall communication topology of a VAX deployment.

Vicon Industries VAX-1D-1 and VAX-2D-1 door controllers are powered by Power-over-Ethernet (PoE). This power is provided via either a PoE network switch or a PoE injector. The controllers communicate by TCP/IP over Cat5e/Cat6 cable, often through the same cable it receives power from.

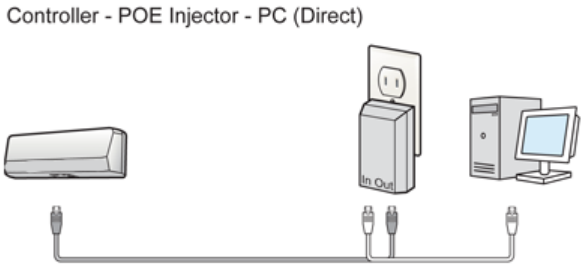
12VDC powered door, IO and elevator controllers such as the VAX-MDK do not use PoE, but the network topology is the same.

Below we have several configuration examples of how the controllers can communicate over a variety of network infrastructures.

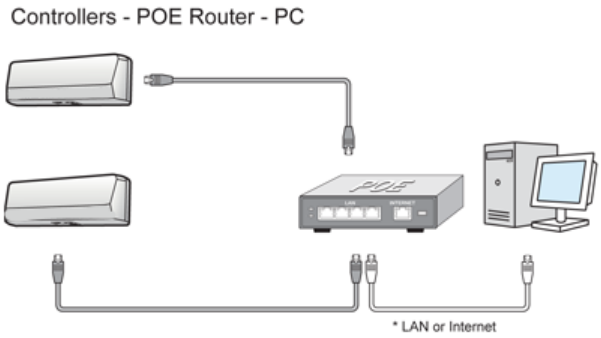
PoE Power. PoE Power may be supplied directly by switch or, alternatively, injected via single port injector between switch/router and the controller.



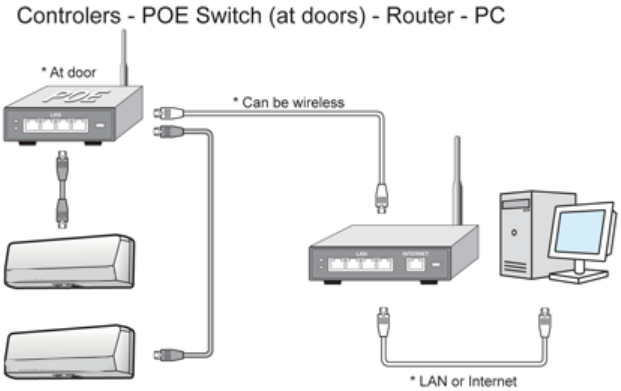
Controller - PoE Injector - PC (direct). In this scenario, the controller is being powered by a PoE injector that is connected right to the VAX server. Scenarios like this happen a lot when there isn't very much network infrastructure to work with.



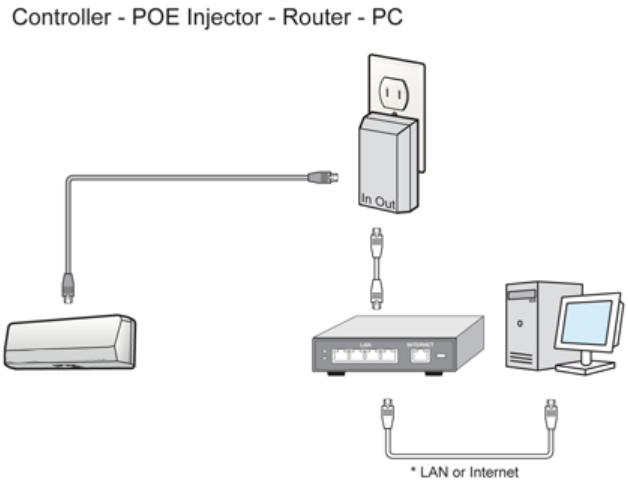
Controllers - PoE Switch/Router - PC. This is a more typical scenario and is seen quite often in the field. The controllers are powered by a PoE switch (located in a closet or electrical room), which connects to the on-site server using the site's existing network infrastructure, or an off-site server via an internet connection.



Controllers - PoE Switch (at Doors) - Router/Switch - PC. In this scenario the controllers are powered by a PoE switch (above/near the door), which connects (wireless or a single cable) to the site's existing network infrastructure, or an off-site server via an internet connection. This topology is used when it's difficult to run Cat5e to the door, or when the doors are very close to each other.



Controller - PoE Injector - Router/Switch - PC. In this scenario, the VAX-1D is being powered by a PoE injector that is connected to the network infrastructure of the site. This example is seen a lot in single door sites where it's not cost-effective to buy a PoE switch.



As you can see, the VAX-1D-1 can be very flexible in how it is deployed to a site, and various Panels can be deployed in any combination of the above examples.

Cables, Standards and Best Practices

This section includes a list of cable specifications that are used with our hardware, references to visual diagrams and some best practices for deployments of Vicon VAX systems.

Cable Specifications and Standards

This section contains information about various cable standards used with our products.

Table 6.6. Cable Standards

Name	Max Distance	Cable Type (Use thicker gauge for longer runs)	Code
PoE Cable	100 m (328')	Twisted pair, 4 pairs	Cat5 100Base-T or better
Reader Cable	152 m (500')	6 conductor stranded (not twisted), 24 AWG or thicker. Overall shielded.	Belden 9537 or equivalent
Door Strike Cable	152 m (500')	2 conductor stranded 18 AWG	Belden 9740 or equivalent
Output Cable	152 m (500')	2 conductor stranded 22 AWG	Belden 8740 or equivalent
Input Cable	152 m (500')	2 conductor stranded 22 AWG	Belden 8740 or equivalent
RS-485 cable with power	600 m (2000')	4 conductor stranded, twisted pair, 2 pairs, 22 ~ 16 AWG, shielded	Belden 9402 or equivalent

VAX-MDK Master Power Requirements

This section will go over power requirements of the 12VDC style panels.

The VAX-MDK will require between 1.5A and 6A @ 12-13.8 VDC from the external power supply.

The following describes the power distribution from a VAX-MDK controller to connected VAX-EX-P-2D expansion modules via the PVAX-MDK P3 and P4 ports in a Door Configuration (up to 4 VAX-

EXP-2D's that equates to 8 doors/readers, which is maximum configuration) and what steps must be observed in regard to ensuring sufficient current is available to connected peripherals such as readers, electrified strikes and optionally used 12VDC out consumption.

The single VAX-MDK controller and four VAX-EXP-2D's modules require 50mA total for board operation. This excludes any device connected to and powered from the 12VDC output port P16 of a VAX-EXP-2D. A 10% available current cushion is also considered.

Each power distribution point on a VAX-MDK (output port P3 and P4) can provide up to 2.5A maximum to its bank of connected expansion modules via direct wiring or interconnect data and power strips. Neither Bank #1 or Bank #2 consumption can exceed 2.5A each. In the event that additional current is required to power a connected device, it may require the implementation of a secondary UL Listed low-voltage Class 2 power limited supply to reduce the bank current load to 2.5A or less.

Each power bank should be calculated as:

(VAX-EXP-2D Quantity x 10mA) + (Reader Quantity x Reader Peak rating in mA) + (# Powered Strikes Quantity x Strike Inrush in mA) + (Quantity of Devices connected to 12VDC output x Device rating in mA)

Example 6.1. Power calculation example

An eight door system using 380mA rated strikes on all doors, eight doors using a standard proximity reader rated at 80mA with no additional power connected devices.

Bank #1: (2 VAX-EXP-2D x 10mA) + (4 readers x 80mA) (4 strikes x 380mA) + (0 devices x 0mA) = 1860mA (1.86A)

Bank #2: (2 VAX-EXP-2D x 10mA) + (4 readers x 80mA) (4 strikes x 380mA) + (0 devices x 0mA) = 1860mA (1.86A)

With each bank consumption now determined, the minimum estimated UL Listed external power supply current availability for aVAX-MDK is calculated as indicated below: (Bank #1 + Bank #2) + ((Bank #1 + Bank #2) x 10%) + 10mA

Minimum Power Supply Current Rating = (1.86 + 1.86) + ((1.86 + 1.86) x 10%) = 4092mA (4.09A)

Identifying a Panel

This section covers how to identify the model of a Panel physically and in the software.

Vicon Industries designs and manufactures a variety of Panel models to meet the needs of a variety of deployments. The following chart lists each model and the unique features of each model.

Table 6.7. Panel Model Reference

Model	Max Doors	Max Readers	Motion REX	Brief Explanation
VAX-MDK-Door-Master-OSDP (MD-K_MASTER)	8	8	No	1-8 door controller traditional style mounted in steel enclosure with OSDP V2 support. Up to 8 doors per VAX-MDK controller with appropriate amount of VAX-EXP-2D two door expansion boards. Powered via external 12VDC power supply.
VAX-MDK-Door-Master (MD-K_MASTER)	8	8	No	1-8 door controller traditional style mounted in steel enclosure. Up to 8 doors per VAX-MDK controller with appropriate amount of VAX-EXP-2D

Model	Max Doors	Max Readers	Motion REX	Brief Explanation
				two door expansion boards. Powered via external 12VDC power supply.
VAX-IO-STR-2	N/A	N/A	N/A	Supports general Input/Output devices in various use cases and configurations. Up to 64 Inputs/ Outputs per VAX-MDK Panel with 8 IO-Boards. Powered via external 12VDC power supply.
VAX-IO-STR	N/A	N/A	N/A	VAX-IO-STR-2 reccomended for new installs. Supports general Input/Output devices in various use cases and configurations. Up to 64 Inputs/ Outputs with 8 IO-Boards. PoE power.
VAX-ELV-STR-2	N/A	N/A	N/A	Supports Access Control to Elevator Cabs in various configurations with Expander Boards. Up to 64 Floors per cab with the appropriate amount of Expander Boards. Powered via external 12VDC power supply.
POE-Elevator-64	N/A	N/A	N/A	VAX-ELV-STR-2 reccomended for new installs. Supports Access Control to Elevator Cabs in various configurations with Expander Boards. Up to 64 Floors per cab with the appropriate amount of Expander Boards. PoE power.
POE-APERIO-8	8	8	No	ASSA ABLOY Aperio master controller capable of controlling up to 8 Aperio devices via 1 - 8 Aperio Hubs with PoE power
VAX-2D-1	2	2	No	Two-Door controller with PoE power
VAX-2D-1-REX	2	2	Yes	Two-Door controller with PoE Power and Integrated Motion
VAX-1D-1	1	2	No	Single-Door controller with PoE Power
VAX-1D-REX-1	1	1	Yes	Single-Door controller with PoE Power and Integrated Motion

All Vicon Industries Panels are fully tested prior to shipping, and after the testing is successful the Panel receives the Vicon Industries seal of approval in the form of a sticker on the Panel to the right of the LCD screen. This sticker contains the model and the serial number, which is used for warranty purposes.

If the Panel is not easily accessible, but connected to the network, you can identify the Panel by logging into the Panel web interface and checking the firmware version. For more information on accessing the Panel web interface, please see the section called “Panel HTTP Configuration Interface”.

Software

This chapter goes into great detail about software configuration concepts specific to VAX. Each configuration section also provides links to configuration chapters associated with the topic concept. Whether you're new or well-versed in access control, this is the most important chapter in this book.

Order of Operations

Configuration of VAX is fairly flexible, however there is a general order of operations that should be adhered to.

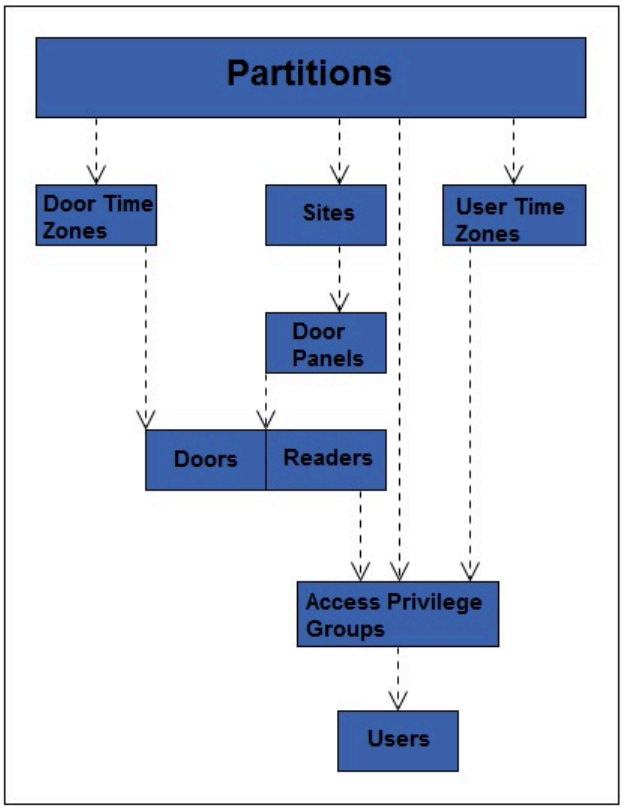
This table is meant as an overview and general guideline for the order of configuration. Each item will go into more detail later in this chapter.

Table 6.8. Order of Operations: Software Configuration

#	Configuration Item	Configuration Order	Additional Notes
1	Partitions	The foundation of any configuration must be completed first.	Default Partition can be used effectively on small sites, single door deployments or instances where fine grained administrative control is not required.
2	Sites	Must be configured after Partitions are finalized.	Default Site can be used effectively on small deployments; we recommend renaming the Site to its location for better visual understanding.
3	Panels	Must be configured after Sites are finalized. Once associated with a Site, you can change which Site the Panel is associated with (only within the same Partition).	If being configured prior to being on site: if you cannot obtain the MAC addresses of the Panels, use placeholder MAC addresses such as "123456789123".
4	Door/Floor Schedules	Configure additional Door/Floor Schedules if required; can be done before or after Doors and Elevators are added. We recommend doing it before.	Default Door Schedules "Always Card Access", "Always Unlocked", "Locked Down", "Card Access 9-5" can be renamed and messaged to fit the deployment needs.
5	Doors/Elevators	Doors/Elevators should be configured after Door/Floor Schedules have been finalized and must be configured after Panels are added.	Readers (which are under Door Configuration) also need to be configured prior to the next steps.
6	User Schedules	User Schedules must be configured after Partitions, and before Access Privilege Group.	Default User Schedules "Always Access", "No Access", and "Access 9AM to 5PM" can be renamed and messaged to fit the deployment needs.
7	Access Privilege Groups	Partitions, User Schedules, Doors and Readers need to be configured prior.	Should be planned/configured with the client.
8	Users	Should be configured after Partitions, Access Privilege Groups, Doors/Readers and Access Privilege Group.	If you don't have any Access Privilege Groups, you can assign a user to a Partition.

The following is a visualization of the chart.

Figure 6.5. VAX Order of Configuration



Partitions

In this section we will cover the basic concepts of **Partitioning** within the VAX. We will also cover some basic examples of how Partitioning has been used in the field. For configuration of Partitions, please see Chapter 19, *Partition and Site Configuration*.

Concepts

The word **"Partitions"** has several literal and figurative meanings in many aspects of security, information technology, law, and even mathematics. In the context of VAX, Partitioning is a method of logically separating the access control system into distinct sections and defining specific permissions for Administrators. For more information on **Administrator Configuration**, visit Chapter 20, *Administrators and Privileges*.

Factors to keep in mind when planning a VAX deployment that may affect if the deployment will utilize Partitions:

- Will the deployment span multiple buildings/sites?
- Who will be administrating the system once deployed? (Receptionist, security staff, building managers, etc.)
- Could the deployment benefit from parts of the system being segregated from each other?
- If you're a certified Vicon Industries dealer, take a moment to consult the client and take their opinion on if it would be appropriate to segregate the system.

Naming Scheme for Partitions. During the planning of the deployment, you'll need to keep in mind a consistent naming scheme for your Partitions and Sites. You can name the Partitions whatever you want, as long as you can understand what they are exactly. In a lot of cases, Sites are named exactly or very similarly to the Partition it is assigned to.

Examples

This section will cover several examples of the Partitioning feature being used. The names and companies in these examples are arbitrary.

Example 1: School System. A school board has VAX Panels configured in three different schools (A, B and C), with a single VAX server at the head office. In a traditional flat system, an Administrator in the access control software would have access to all Doors across all three schools. Using Partitioning, we can have three different Partitions (A, B and C) and create an Administrator account for each school. Now each school only has control over their own system, reducing the risk of configuration issues and cleaning up the interface of each Administrator account with only information relevant to them.

Example 2: Condo Management Company. A condo management company is using VAX to manage various condo sites across various locations. Doors they are managing include main entrances, parking gates, laundry rooms, storage and garbage/recycling at each building. By utilizing Partitions, they can create a consistent naming scheme and streamline management of individual Partitions.

Example 3: Office/Data Center. An office with a data center on site is using Vicon Industries door controller to manage the data center and the public entrance. Using Partitions, the owner can create two Partitions. One for the front Door, and one for the data center entrance. Now the owner can create an Administrative account for the front Door to give to the front desk receptionist. This gives the owner more control over who can be granted access to the data center. He could also give the receptionist Administrator account the ability to see events for the data center entrance, but not give control over adding users or Overriding the data center door.

Sites

In this section we'll go over **Sites**, and how they interact with Partitions, Panels and other aspects of VAX.

Sites are the method that Panels are associated with Partitions. You cannot directly assign a Panel to a Partition; you must first create a Site in the Partition, and then assign the Panel to the Site assigned to the Partition that Panel needs to be in. If using a single Partition, Sites can be useful for separating your deployment into sections to make management easier on the eyes, especially when you have several front doors across multiple buildings. If Panels will be residing in different Schedules, it is recommended to separate those Panels into separate Sites; this will ensure the Panels always report events in the Schedule applicable to their location.

Examples

This section will cover several examples of Sites being used. The names and companies in these examples are arbitrary.

Example 1: Hospital. A hospital with several buildings across a small area is using VAX Door Panels. By utilizing Sites, each building can be its own Site and objects such as User Schedules, Door Schedules, Holidays and Access Privilege Groups can be used throughout the access control system. Perhaps in this same scenario, an Administrator creates a separate Partition for the administrative staff. These Users can be shared across multiple Partitions, but would require their own User Schedules and Access Privilege Groups.

Example 2: Municipal Government. A town government has chosen to use VAX to manage their doors in offices and facilities. Using Sites, the building manager creates a Site for the town hall, water management buildings, fire stations and even community centers. Sites and Partitions can be used in this scenario to simplify management and create logical separators. For example, the community center would likely be its own Partition, and could be managed by on site staff while still maintaining a central authority at city hall.

Door Schedules

In this section we'll cover the concepts of **Door Schedules** within VAX and a couple of examples of Door Schedules that are used in the field. For configuration of Door Schedules, please see Chapter 9, *Door Schedule Configuration*.

Concepts

Door Schedules are how we can configure the Doors to behave, and when we want them to behave that way. Door Schedules in VAX are very flexible. Doors currently have 8 different states they can be in, and there are several methods of changing these states, including: **Door Overrides**, **One Time Run Zones (OTR)** and **Triple Swipe Actions**. A Door Schedule schedule can change up to 20 times a day, not including overrides, OTR and triple swipe actions. The following section shows all 8 Door states, and a brief explanation of what they mean.

Lockdown. When red is used to define a period or zone within a Schedule schedule, the resultant action is that the Door using this Schedule is now in a secure state (locked). No access via any credential permits a cardholder through a Door in a lockdown state unless that cardholder has its 'Is Master' setting activated within its account.

Card Only. When yellow is used to define a period or zone within a Schedule schedule, the resultant action is that the Door using this Schedule is now in a secure state (locked). In conjunction with a combination proximity/keypad Reader or standard proximity Reader, requires a valid card presented to grant access through the Door.

Pin Only. When blue is used to define a period or zone within a Schedule schedule, the resultant action is that the Door using this Schedule is now in a secure state (locked). In conjunction with a combination proximity/keypad Reader or keypad only Reader, requires a valid PIN entry on the keypad to grant access through the Door.

Card or Pin. When aqua is used to define a period or zone within a Schedule schedule, the resultant action is that the Door using this Schedule is now in a secure state (locked). In conjunction with a combination proximity/keypad Reader, keypad only or standard proximity Reader, requires a valid card presented or PIN entry on the keypad to grant access through the Door.

Card and Pin. When purple is used to define a period or zone within a Schedule schedule, the resultant action is that the Door using this Schedule is now in a secure state (locked). In conjunction with a combination proximity/keypad Reader, requires both a valid card presented and PIN entry on the keypad (in that order) to grant access through the Door.

Unlocked. When green is used to define a period or zone within a Schedule schedule, the resultant action is that the Door using this Schedule is now in a public state (unlocked), not requiring a valid credential to grant access through the Door.

First Credential In. When light green is used to define a period or zone within a Schedule schedule, the resultant action is that the Door using this Schedule is now in a secure state (locked) in a 'Waiting for Credential' mode, awaiting a valid card presented or valid PIN entry before changing state into a public (or unlocked) state. Only cardholders with 'First Card In Enabled' option included in their User profile will change the state of the Schedule to Public. Other cardholders may be granted access based on their particular access privilege rule but the Door will stay in a **Secure - Waiting for Credential Mode**. The typical usage of First Credential In is to prevent unauthorized entry to a facility based on a public Door schedule. For example, you wouldn't want the Door to unlock unless an employee was inside the building.

Dual Credential. When gray is used to define a period or zone within a Schedule schedule, the resultant action is that the Door using this Schedule is now in a secure state (locked). In order for access to be granted, two valid credentials must presented to the reader within 5 seconds of each other before the Door will unlock and grant access. For additional security, you can configure the Door to only accept a Dual Credential if the first credential presented has the User Privilege **'Supervisor'**. This option is configurable in the **Options Tab** of the **Edit Door Screen**.

Door Schedule Factors. Factors to keep in mind when planning your Door Schedules include the following:

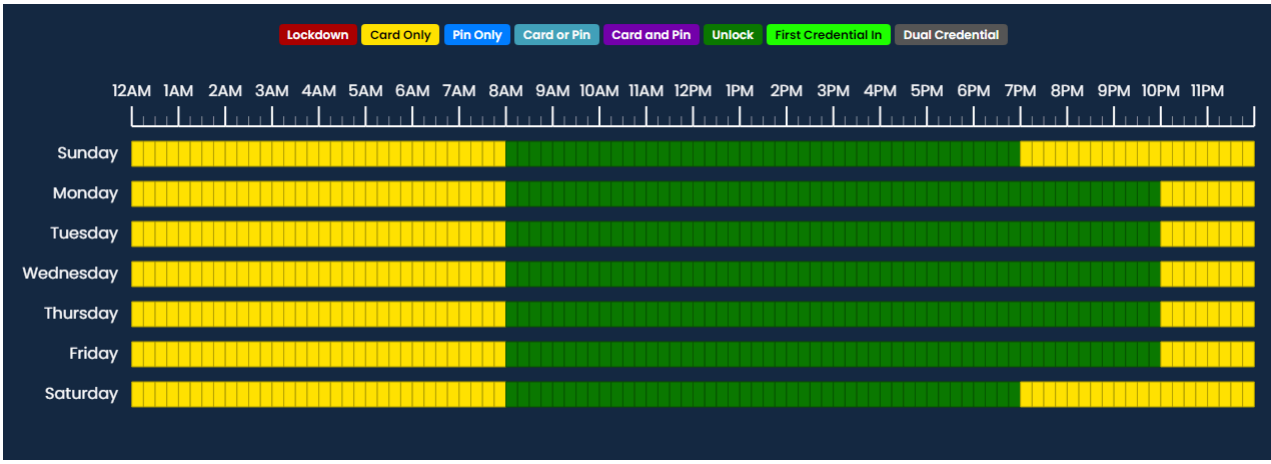
- Will the deployment have a public Door? If so when should that Door change to a locked state? Should that Door use **First Card In**?
- Is the deployment using combination prox/keypads? Do any of these Doors require **Card AND Pin/ Card OR Pin/Pin Only**?
- Is there any ultra secure locations within the deployments (data centers, vaults, etc.)? Would they benefit from a **Card and Pin** or **Dual Credential** Door Schedule?

Planning a Door Schedule. When planning for your access control deployment, you'll need to ask yourself (and/or the client) how they would like their Doors to behave. Any combination of Door states can be scheduled in a Door Schedule, and can be applied to multiple Doors.

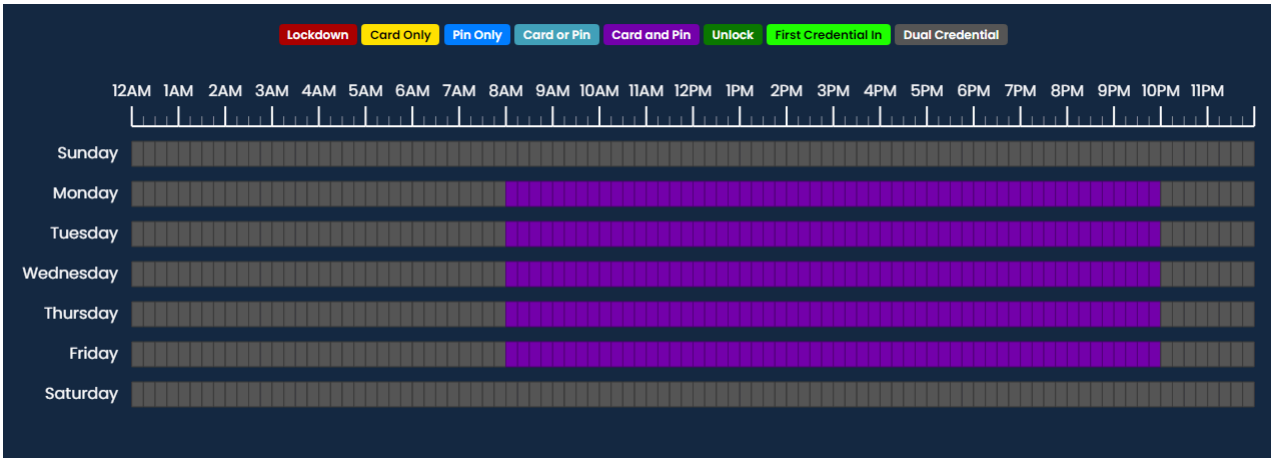
Examples

This section will go over a few real world examples of Door Schedules, and may help you visualize how these Door Schedules actually look like in the software.

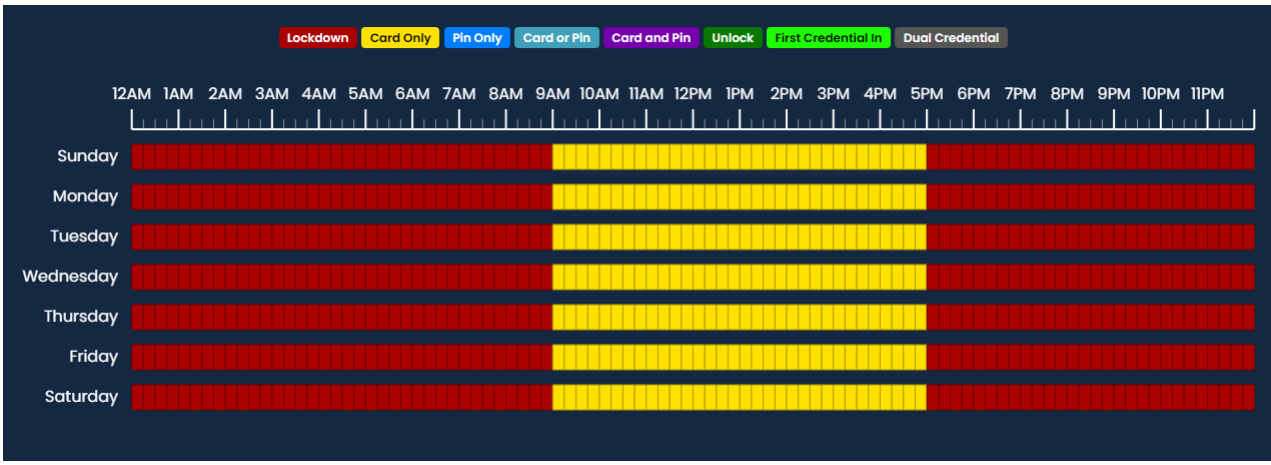
Example 1: Grocery Store Public Entrance. In this example, we have a Door Schedule that will be assigned to the front public Door of a grocery store; it is set up to **Unlock** during store hours, and card only otherwise for staff.



Example 2: Data Center Door. In this example, we have a high security Door Schedule that will be assigned to data center entrance; this Schedule utilizes **Card and Pin** during office hours, and **Dual Credential** during off hours.



Example 3: Office Employee Entrance. In this example, we have a card access 9 to 5 Door Schedule that will be assigned to the front Door of an office. This is one of the default Door Schedules included in VAX.



User Schedules

In this section we'll cover the concepts of **User Schedules** within VAX and an example of a User Schedule. For configuration of User Schedules, please see Chapter 10, *User Schedules*.

Concepts

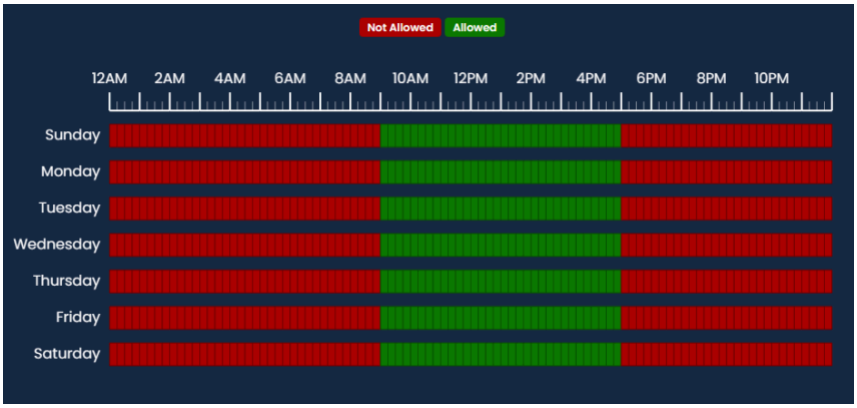
Similar to Door Schedules, User Schedules are the method in which Users are validated if they have access to a specific Reader **(Access** or **No Access**). The only exception that would affect an Allowed access and prevent the cardholder from being granted access is when the particular Door is currently in a Lockdown state, whereby only Users with the **Master Privilege** set will be granted access. **User Schedules** are applied to **Access Privilege Groups**, as opposed to **Door Schedules**, which are applied to **Doors**.

Note

By default, VAX comes with 3 default User Schedules ('No Access', 'Always Access' and 'Access 9am to 5pm'). These User Schedules can be edited or deleted as needed, but in most cases will be enough for smaller deployments.

Examples

In this example, we have a slightly modified version of the default User Schedule "Access 9am to 5pm". We've modified it for a more flexible schedule of 7am to 6pm.



Access Privilege Groups

In this section we'll go over the concepts of **Access Privilege Groups** (APGs), and what their role is in VAX. For instructions on how to configure Access Privilege Groups, see Chapter 11, *Access Privilege Groups*.

Concepts

Access Privilege Groups in VAX are the link that permits a **Users** access at a **Reader** or **Floor** based on the **User Schedule** and the **Door/Floor Schedule**. Access Privilege Groups are generally configured once the following have been met:

- **Panels**, **Doors** and **Readers** have been configured
- **Door Schedules** have been configured
- **User Schedules** have been configured
- **Floor Schedules** have been configured (if using Elevator Panel)

Planning Your Access Privilege Groups

An important concept that makes VAX unique from other systems is that Users can be part of more than one Access Group. This gives us the flexibility to create APGs based on similar Doors and assign an individual User to multiple APGs based on which Doors the User will need. Factors to keep in mind to determine how many access groups you'll need include the following:

- Are Users divided into different groups that will require different access privileges (example, engineering, HR staff, managers, etc.)?
- Do some Users need more access than others?
- Does the Access Privilege Group you're adding need to be in more than one Partition?
- Should the Access Privilege Groups be grouped by Users or based on different types of Doors/Floors (exterior Doors, R&D Doors, groups of elevator Floors)?

Style APG Structure: Groups Based On Users

The traditional structure of access groups usually entails a group with many Doors/Floors in the system (in some cases, all). This style of groups is based on the type of Users in the group, such as:

Table 6.9. APG Example: 1

APG Name	APG assigned Doors
Engineering Staff	Would have access to engineering Doors, front Door, production room Door.
HR Staff	Would have access to office Doors, front Door.
IT Staff	Would have access network closets, office Doors, front Door.
Sales	Would have access office Doors, front Door.

Advantages of Groups Based On Users:

- Quicker to initially configure (due to each User being in a single group).
- Works well if most Users need the same permissions. In the above example, we have 4 groups, with potentially hundreds of Users in each one.

Disadvantages of Groups Based On Users:

- Difficult to change permissions for specific Users. In the above example, if someone from Sales needed access to the Engineering Doors, they would need their own separate group because placing that User into the Engineering APG would result in a conflict due to the Front Door being in both groups.
- Can't easily give additional access to a User without giving additional access to the APG.

Style APG Structure: Groups Based On Doors/Floors

This access group structure, unique to VAX, takes advantage of the fact that Users can be part of more than one APG. These groups entail smaller, more specific groups that are based on a few Doors, usually of similar type such as exterior Doors, engineering Doors. Users would be placed into several groups based on what Doors/Floors they need access to (and what times they need access to those Doors/Floors), such as:

Table 6.10. APG Example: 2

APG Name	APG assigned Doors
Engineering Doors	Would have access to engineering Doors, production room Door.
Office Doors	Would have access to office Doors.
Network Closets	Would have access network closet Doors.
Exterior/Common Doors	Front Door and any other Common Doors

Advantages of Groups Based On Doors/Floors:

- Easier to maintain in the long run since more specific User access can be specified.
- User permissions can be more specific and it is easier to make changes to what Doors/Floors a User has access to. In the above example, if someone in Sales needed access to the Engineering Doors, that User can simply be placed into both groups.

Disadvantages of Groups Based On Users:

- More time consuming to initially configure (depending on the amount of Users).

Note

In some situations, it may be beneficial to do a hybrid approach, where exterior Doors and common Floors have their own separate groups, while maintaining other APGs as User based. The important part is to communicate to your client about their needs, and build effective APGs together.

Naming Your Access Privilege Groups

A consistent name for your access groups is highly recommended. Generally the best practice is to name the group after the type of User inside the group, or after the Doors/Floors that are in the group.

Holidays

This section will cover **Holidays** in VAX. This section will cover concepts and some examples. For configuration of Holidays please see Chapter 13, *Holiday Configuration*.

Holidays within VAX are used to define exceptions to the regular daily access schedule in response to a specific calendar occurrence. This occurrence can be a specific day or, alternatively, be setup to occur annually.

Each Holiday is assigned a date as well as one or more User Holiday Groups or Door Holiday Groups, and the schedule each group will follow on the given date.

Concepts

Holidays take a few configuration steps due to how they interact with Users and Doors. Just like how Doors and Users have separate Schedules (User Schedules and Door Schedules), Holidays have 2 Schedules called **Door Holiday Schedules** and **User Holiday Schedules**. In large deployments such as those spanning multiple countries, it can be very flexible.

Note

On the day of the Holiday, Door Holiday Schedules and User Holiday Schedules will override what the Doors and Access Privilege Groups would normally do on Doors and Access Privilege Groups the Holiday Groups are assigned to.

There are 5 components to Holidays; each one will be explained below:

Door Holiday Schedules. Door Holiday Door Schedules define the schedule a Door will follow on a Holiday. The schedule configuration is very similar to the regular Door Schedule configuration. All normal Door states are present and can change up to 4 time in a schedule. By default, VAX comes installed with one Door Holiday Schedule called **'Closed During Holiday'** with a schedule of lock-down all day.

Door Holiday Groups. Door Holiday groups are a collection of Doors that will follow the same schedule on a Holiday. This can be assigned to a Door when created or edited. By default, VAX comes installed with two Door Holiday Groups: **'Standard Holidays'** and **'No Holidays'**.

User Holiday Schedules. User Holiday Schedules define a schedule a User account will follow on a Holiday. The schedule configuration is very similar to the regular User Schedule configuration. Available User modes include: **'Not Allowed'** and **'Allowed'**. By default, VAX comes installed with two User Holiday Groups: **'Holiday Access 9am to 5pm'** and **'Holiday No Access'**.

User Holiday Groups. User Holiday Groups are collection of Holiday Schedule schedules Users will follow on a Holiday. This is assigned to Users via Access Privilege Group when created or edited. By default, VAX comes installed with two User Holiday Groups: **'Standard Holidays'** and **'No Holidays'**.

Holidays. The Holidays page resides under 'Home/Day to Day'. This is where you add the Holidays, define the date and assign the Holiday to either Door Holiday Groups, User Holiday Groups or both.

Note

If your deployment will be using Elevator Controllers to manage access to Floors, there are two additional Holiday components:

- Floor Holiday Groups (similar to Door Holiday Groups)
- Floor Holiday Schedules (similar to Door Holiday Schedules)

Examples

This section will go over some examples of Holidays being used in the field, along with some of the components and decision making that was put into each Holiday. When adding a Holiday, it can be assigned to Door Holiday Groups, Floor Holiday Groups and User Holiday Groups (with appropriate Holiday Schedules). By default, VAX comes installed with two Holidays: **'Christmas'** and **'New Years'**.

Some questions you may ask yourself when adding a Holiday may include the following:

- What do I want my Doors to do on this Holiday? Should they be locked down, card only, open, etc.?

- Should all my Sites/Partitions be affected by this Holiday (for example, Sites in other countries where the Holiday may not be present)?
- Should this Holiday affect my Users, my Doors, Floors or both?
- If utilizing Elevator controllers, should this holiday affect how they behave as well?
- Are there any Users that need access to the Door(s) on the Holiday?

Example 1: Independence Day. A small business would like to be closed on the Fourth of July; they want the Door locked down on this Holiday. They can simply ensure all their Doors are using the **Door Holiday Group 'Standard Holidays'**. They add the Holiday on the **Holidays** page and attach it to the **Standard Holidays** Door Group with the **Door Holiday Schedule** set as **'Closed During Holiday'**. As you can see, the default Door Groups and Schedules work well for most situations.

Example 2: Canada Day: Large Company. A large company with offices in the US and Canada would like to lock their offices in Canada but not in the US. If their system is utilizing Partitions, they can simply add Canada Day to the default Door Holiday Group in the Partition with the Canadian offices.

Chapter 7. Setting up Your Panel

Adding a Panel to VAX

This section will cover the basic process of adding a Panel in VAX, in most deployments its a fairly easy process and can be done in two different ways.

Note

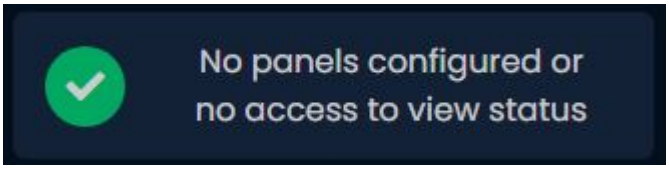
This section appears in an earlier chapter of this guide. If you have already added a Panel you can proceed to the section called “Advanced Panel Configuration”.

Method 1: Adding a Panel Via Notification

This section will cover adding a Panel to the software after the Panel has been configured to look for the server.

The Panel is configured to find the server by **Name** or **IP Address**. (Please see the section called “Panel IP Settings: Static IP” and the section called “Communication Mode Configuration: Server Name (DNS)” for details on configuring a Panel to find a VAX server)

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer
3. On the **Side Bar**, pay attention to the **Notifications** section on the right side of the page.



4. After a few moments, if the Panel is configured correctly and there are no third-party firewalls blocking TCP port 9876, the Panel will connect to the server and a Notification will appear(pictured below).

5. This Notification indicates that the server was contacted by a Panel that the server is not aware of. The Notification will show the mac address of the Panel trying to connect. If this address matches a Panel you'd like to configure, click on the Notification.
6. Once you click on the Unknown Panel Notification, you'll be taken to the **Add Door Panel** screen with the **Mac Address** field pre-populated with the mac address displayed in the Notification.

7. Please proceed to the section called “Adding a Panel: Basic Configuration” for continued instructions on adding a Panel.

Method 2: Adding a Panel Manually With Mac Address

This section will cover adding a Panel manually in VAX. You may choose this method for the following reasons:

- You have not yet configured the Panel to communicate with the server yet.
- You are pre-configuring the software prior to the deployment of the Panels.
- If the deployment is large, adding the Panels via Notifications can be difficult.

The following information should be collected prior to manually adding Panels:

- The Panel model (can be found on the physical Panel to the right of the LCD screen) for each Panel.
- Mac address of each Panel.
- If the Panels will be using DHCP or static addresses.
- Location of the Panels (generally used for naming the Panels).
- If the Panel is a Door Panel, will it be using a Door contact?

Note

If not all of this information is available, you can use placeholder values for the mac addresses and names.

Once you've collected this information, we can now begin adding the Panels. Please Proceed to the section called “Adding a Panel: Basic Configuration”

Adding a Panel: Basic Configuration

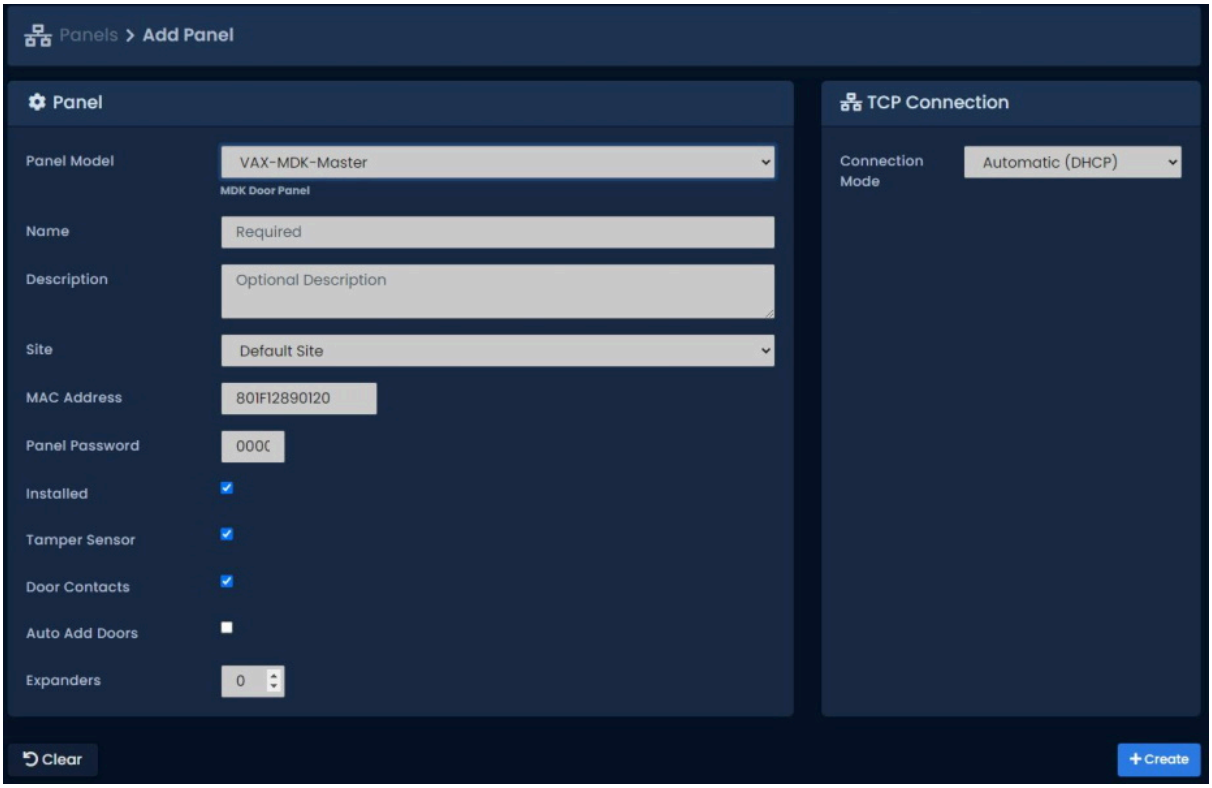
This section will cover the various fields that need to be populated in order to add a Panel in VAX. It is advised to fill them in the order they are shown on the screen, the exception being the mac address if it is pre-populated.

If you are not already on the **Add Door Panels** screen:

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Hardware**, click on the **Door Panels** icon (pictured below).

4. On the **Door Panels screen**, click the **Add** button.

On the **Add Door Panels** screen you'll be presented several drop-down menus, text fields and check-boxes to fill.



The following table describes the common fields.

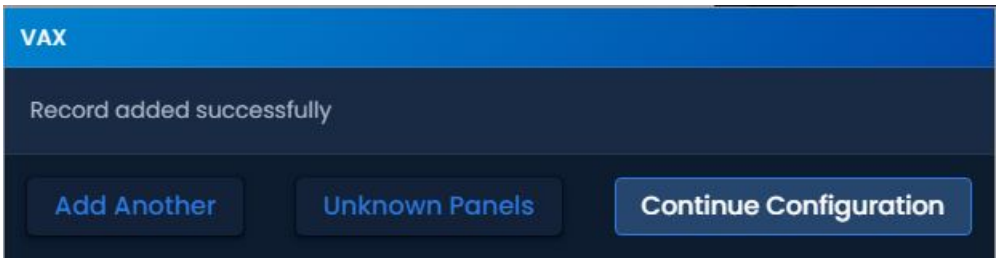
Table 7.1. Add Panel

Drop Down/Text Box/Check box	Description
Panel Model	Select the Panel model using this drop-down menu, depending on the model you choose; additional options may be displayed.
Name	The name of the Panel, we recommend naming the Panel based on its location on the site. Accepts 4 to 60 characters.
Description	Optional description of the Panel. Accepts 0 to 255 characters.
Site	Select the site the Panel will reside on. This cannot be changed once the Panel is added.
Mac Address	The unique network address built into every Panel. May be pre-populated if you're adding the Panel through a Unknown Connection From Panel Notification. Must be 12 characters.
Panel Password	The password required for access to the administration menu built into the Panel. Valid values are 0 to 9999. Default value is '0000'.
TCP connection: Connection Mode	The method in which the Panel receives its IP address, DHCP or Static. Selecting static will bring up additional fields to fill.

Note

If you've already configured the Panel with a static IP address, you'll need to enter it in the software as well.

You can now click **Save**, you'll be asked to correct any information that is missing or invalid. Once corrected press **Save** again. A message box will appear that will say **Door Panel Added Successfully**.



Warning

Prior to your first update to the Panels, we advise configuring the advanced settings of your Panels. This can be found in the section called “Advanced Panel Configuration”.

Advanced Panel Configuration

This section covers configuration aspects of Panels after the Panel has been added to the software. Once the Panel is added, additional configuration options are available such as the Input/Output configuration.

To get to the Panel advanced settings:

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Panels** icon (pictured below).

4. On the**Panels screen**, you'll see any Panels you've already added to the software. Click the **blue** button (Advanced Settings) next to the Panel you'd like to configure.
5. On the **Edit Panel** screen, there are four tabs. The **General** and **Connectivity** tabs are what we configured when adding the Panel. Most of these options can be modified as needed. The **Options** and **I/O** tabs are automatically filled based on which Panel model you selected when adding the Panel. These settings will be covered in the next section.

Note

Some options may not be available depending on the Panel model being configured.

General Tab

The General tab allows you to change any of the information provided when the Panel was added. Encryption options also appear on this tab. The following items can be changed:

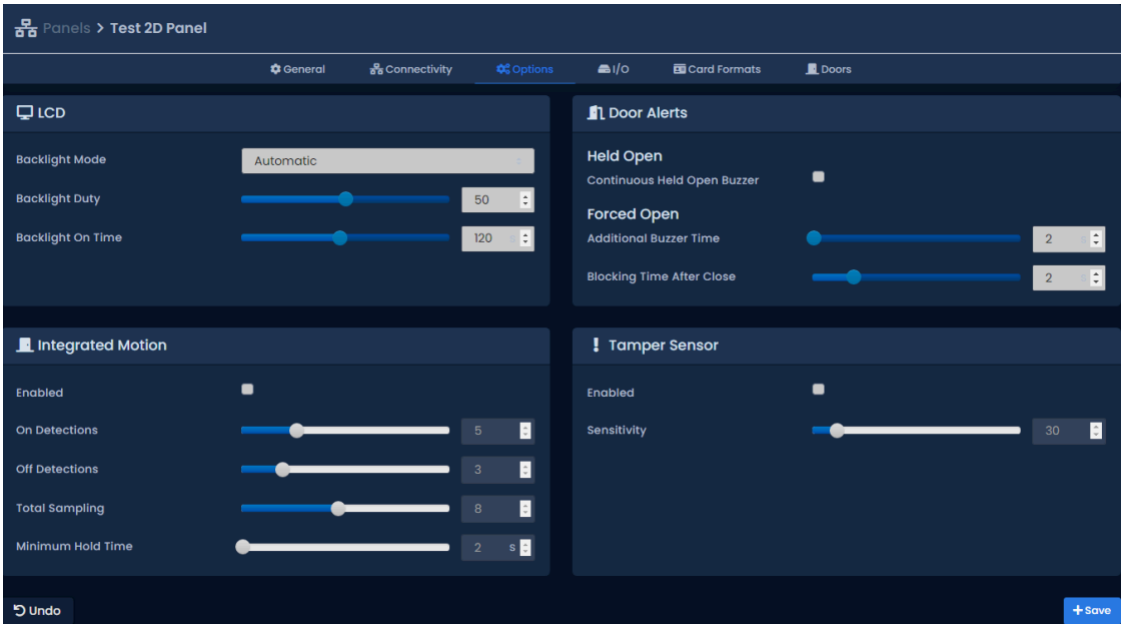
Table 7.2. Add Panel

Drop-down/Text Box/Check box	Description
Name	The name of the Panel. Accepts 4 to 60 characters.
Description	Optional description of the Panel. Accepts 0 to 255 characters.

Drop-down/Text Box/Check box	Description
Site	The site the Panel will reside is on. Can be changed to a different site on the same Partition.
MAC Address	The unique network address built into every Panel.
Panel Password	The password required for access to the administration menu built into the Panel. Valid values are 0 to 9999. The default value is '0000'.
Installed	Enables if the panel is installed and set to communicate. Unchecking will stop the panel from contributing to the panel count on the top right on most screens.
Expanders (select models only)	Amount of expander modules. Either IO or door modules. Enter the correct amount (1-8 for IO modules, 1-4 for door modules).
Auto Firmware Update (select models only)	Enables if the panel will receive firmware updates automatically (only supported on select models).
AES Mode	Can be set as '256bit AES' when higher security is required. Defines the encryption method between the VAX server and the Panel.

Options

This section will cover the configuration items in the options tab when configuring a Panel.



The **Options** tab is divided into 6 sections: **LCD**, **Forced Open**, **Tamper Sensor** and **Integrated Motion**. Each section has several slider bars that are used to easily change the settings. You can also use the text box next to the slider to manually enter a value.

Table 7.3. Options Tab

Configuration Item	Description
LCD	
Backlight Mode	The operating mode of the Panel's integrated LCD. Values are Automatic, Always On, Always Off.
Backlight Duty	The light level of the Panel's integrated LCD. Increments by 1. Valid values are 0 to 100.

Configuration Item	Description
Backlight On Time	The time the Panel's integrated LCD backlight will stay active after receiving User Input. Increments by 1 s. Valid values are 0 s to 254 s.
Held Open	
Continuous Held Open Buzzer	Determines if held open alarm connected to external or global buzzer will be in a continuous state of closed or if it will pulse the buzzer. Default is pulse.
Forced Open	
Additional Buzzer Time	The additional time a forced open buzzer will be activated after a forced open event is raised. Increments by 1 s. Valid values are 0 s to 255 s.
Blocking Time After Close	Total blocking time after Forced Open event. Increments by 1 s. Valid values are 0 s to 10 s. This is a buffer time to prevent forced open alarm right after a valid door opening and closing. This occurs if a valid person goes through a door, but immediately goes back out the door.
Tamper Sensor	
Enabled	Enable/Disable the integrated tamper sensor. The tamper sensor will provide an audible alarm if it detects the cover of the Panel has been removed. Some installers disable this during installation and testing.
Sensitivity	The sensitivity of the integrated tamper sensor. A higher value allows more light to be exposed to the sensor before triggering an alarm. A higher value is useful in situations where the Panel is exposed to sunlight. Increments by 1. Valid values are 0 to 255.
Integrated Motion	
Enabled	Enable/Disable the integrated Motion Sensor (if applicable).
On Detections	Motion On Detections. Increments by 1 . Valid values are 1 to 16.
Off Detections	Motion Off Detections. Increments by 1 .Valid values are 0 to 15.
Motion Total Sampling	Motion Total Sampling. Increments by 1 . Valid values are 1 to 16.
Minimum Hold Time	Motion Minimum Hold Time. Increments by 1 s. Valid values are 0 s to 255 s.
Anti-passback	
Reset Anti-passback At Midnight	If enabled, Local Anti-passback will be reset at midnight.

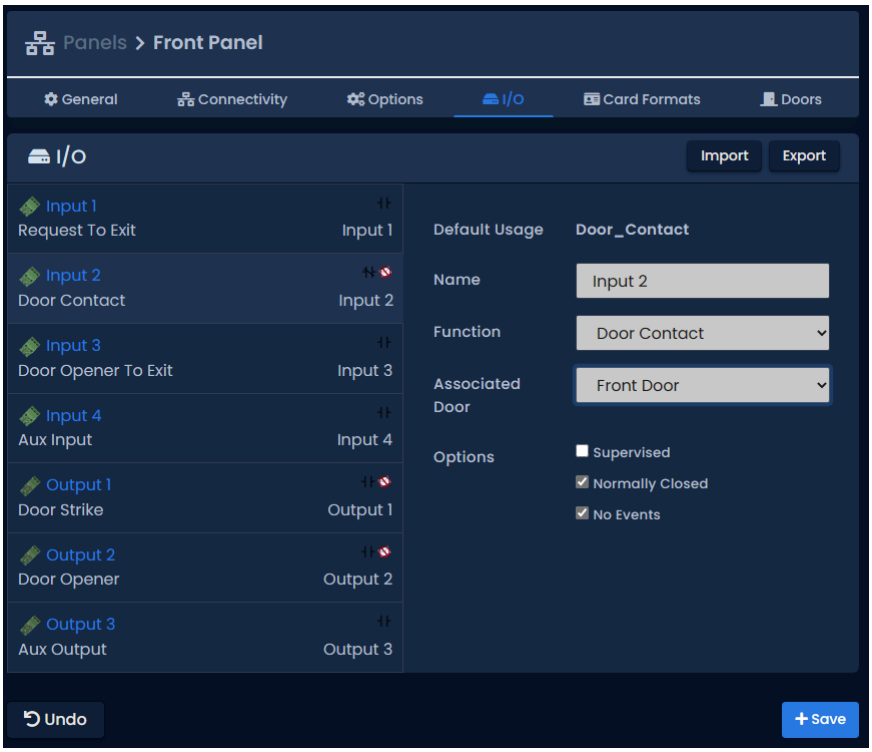
Note

In most cases, the default values for the Integrated Motion options work fine, however if you need to lower or raise the sensitivity of the sensor, please see the section called “Integrated Motion: Changing Sensitivity”.

Input/Output Configuration

This section covers configuration options in the **Input/Output (I/O)** tab. Depending on the Panel model selected when adding the Panel, the software will change what the default values are. For example: If you add a VAX-2D-1; Output 1 and Output 2 will both be mapped as Door strikes. The I/O tab is unavailable on Elevator Panels. VAX-MDK panels will have a dropdown menu for accessing IO settins for multiple expanders.

Figure 7.1. VAX-1D-1 Typical I/O Tab



On the I/O tab, the left hand column shows each Input and Output along with the current function beneath it. The currently selected Output/Input (shaded in gray) will have its information shown on the right side. This information includes:

- The Name of the Input/Output (to be shown in notifications)
- Associated Door (used to determine which door an input or output corresponds to)
- Function, see below
- If the Output/Input is Normally Closed/Open
- Disable/Enabled Events for this Output/Input

The following table will go over the 10 different Input functions and the 8 different Output functions on PoE powered controllers.

Table 7.4. Input/Output Functions VAX-1D-1

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.

Function	Description
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.

Warning

If your Panel is not using a Door contact, select the Door contact Input(s) and change the drop-down function to 'Disabled'.

Aux Input Actions

This section covers additional actions that can be programmed into an **Aux Input** in VAX. The following table are actions supported on PoE powered panel models.

Table 7.5. Aux Input Actions

Input Action	Description
Activate Selected Output	Allows the Input to activate an Output (selectable from drop-down menu). The Output will stay activated until overridden in the software or by another Aux Input action.
Deactivate Selected Output	Allows the Input to deactivate an Output (selectable from drop-down menu).
Toggle Selected Output	Allows the Input to toggle an Output (selectable from drop-down menu). Toggle will change the state from the Output's current state. The Input will need to return to its normal state, and then change again in order for the state of the Output to change.
Pulse Selected Output	Allows the Input to activate an Output (selectable from drop-down menu) for 1.5 seconds, after which the Output will deactivate.
Activate Selected Output with Sound	Allows the Input to activate an Output (selectable from drop-down menu) with an audible alert that the Output was activated. The Output will stay activated until overridden in the software or by another Aux Input action.
Deactivate Selected Output with Sound	Allows the Input to deactivate an Output (selectable from drop-down menu) with an audible alert that the Output was deactivated.
Toggle Selected Output with Sound	Allows the Input to toggle an Output (selectable from drop-down menu) with an audible alert that the Output was activated. Toggle will change the state from the Output's current state. Each state change will be accompanied with an audible alert that the Output state was changed. The Input will need to return to its normal state, and then change again in order for the state of the Output to change.
Pulse Selected Output with Sound	Allows the Input to activate an Output (selectable from drop-down menu) for 1.5 seconds with an audible alert that the Output was activated, after which the Output will deactivate.
Activate Alarm Interface	Allows an Input (such as a button) to activate an Output that is assigned as an alarm interface. The circuit changes to a closed state for 1.5 seconds before changing to an open state. In most cases this can be used to arm an alarm system.
Deactivate Alarm Interface	Allows an Input (such as a button) to deactivate an Output that is assigned as an alarm interface.
Toggle Alarm Interface	Allows an Input (such as a button) to activate an Output that is assigned as an alarm interface. The circuit changes to a closed state for 1.5 seconds before changing to an open state. In most cases this can be used to arm an alarm system.
Activate Alarm Interface with Sound	Allows an Input (such as a button) to activate an Output that is assigned as an alarm interface with an audible alert. The dry contact changes to a closed state for 1.5 seconds before changing to an open state. In most cases this can be used to arm an alarm system.
Deactivate Alarm Interface with Sound	Allows an Input (such as a button) to deactivate an Output that is assigned as an alarm interface with an audible alert.
Toggle Alarm Interface with Sound	Allows an Input (such as a button) to activate an Output that is assigned as an alarm interface with an audible alert. The dry contact changes

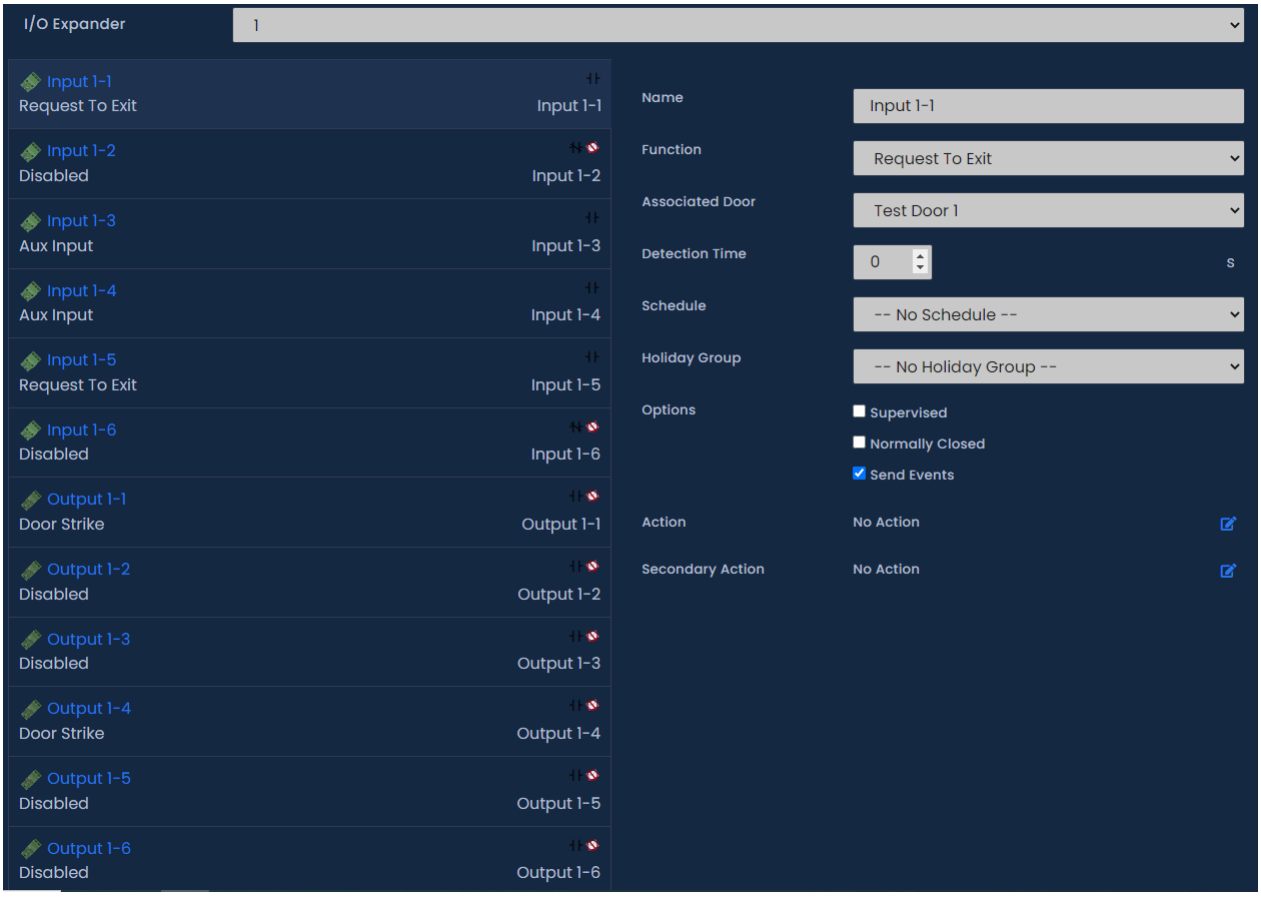
Input Action	Description
	to a closed state for 1.5 seconds before changing to an open state. In most cases this can be used to arm an alarm system.
Play Sound 0-4	Allow an Input to trigger a sound on the Panel; allows a drop-down menu with several options.
Play Warning Sound	Allow an Input to play a warning sound.
Override Doors with Crisis Level	Allows an Input to change the Crisis Level of the Door to an assignable value from a drop-down list.
No Action	The Input will have no action.

Warning

Inputs connected to the Panel must be **Dry**, no power. Failure to follow this instruction could lead to the Panel being damaged.

Once you've made the desired changes to the Panel settings, you can now click the **Save** button on the bottom of the page. Once you've added and configured your other Panels, you'll likely want to move on to updating your Panel. Please see the section called “Updating Your Panel”.

VAX-MDK



12VDC powered controllers have some additional input/output features that will be noted in this section. Some specific differences include:

- The I/O Expander dropdown selects which expander inputs and outputs to display.
- Detection time can be configured on inputs so that the function and/or action will occur only if the input state is maintained for the defined number of seconds.

- Inputs can be assigned an Input Schedule, which will restrict when the function of the input will work or assigned actions. For example, you may want a schedule on an external motion sensor. Supports holiday schedules.
- Outputs configured with the function Aux Output can be assigned an Output Schedule. Supports holiday schedules.
- Inputs can all be assigned an Action similar to Aux Input actions on other panel types. Action can occur regardless of input function.
- Inputs can all be assigned a second Action similar to Aux Input actions on other panel types called an On Action. The On Action can occur regardless of input function in addition to the set action.

The following table contains a list of Actions.

Table 7.6. VAX-MDK Panel Input Actions

Triple Swipe Actions	Brief Explanation
No Action	Actions are optional; an event will still be generated when input conditions are met and server side script triggers can still execute.
Output Activate	Activates an output, selectable via drop down list.
Output Toggle	Toggle an output to the opposite state, selectable via drop down list.
Output Deactivate	Deactivate the selected Output, selectable via drop down list.
Output Pulse High	Pulse an Output to close, configure a delay and the duration of the pulse.
Output Pulse Low	Pulse an Output to open, configure a delay and the duration of the pulse.
Output Pulse Opposite	Pulse an Output to the opposite of its current state, configure a delay and the duration of the pulse.
Output Activate Multiple	Activate multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Output Deactivate Multiple	Deactivate multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Output Toggle Multiple	Toggle multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Input Disable	Disable a selected input. Selectable from a drop-down list with delay and duration.
Override < Door Mode>	This Triple Swipe Action will override the state of the Door depending on the selection you configure in the software. These Door Overrides must be resumed from the software or a separate action that will Resume the door state. Modes include: Lockdown, Card, Pin, Card or Pin, Card and Pin, Unlock, First Card In. Door and mode selectable from drop-down list
Override < Door Mode> With Auto-Resume	This Triple Swipe Action will override the state of the Door depending on the selection you configure in the software. These Door Overrides instruct the Door to Resume normal schedule when the Door Schedule assigned to this Door is scheduled to change. Can also be resumed from the software or a separate action that will Resume the door state. Modes include: Lockdown, Card, Pin, Card or Pin, Card and Pin, Unlock, First Card In. Door and mode selectable from drop-down list
Door Resume Override	Resumes a Door from an overridden state. Selectable via drop-down list.

Triple Swipe Actions	Brief Explanation
Door Set Crisis Level	Initiate crisis level on a door. Selectable via drop-down list for door and mode.
Door Reset Crisis Level	Set the crisis level back to default on the selected door. Selectable via drop-down list.
Door Disable Held Open Buzzer	Temporarily disable a held open alarm/buzzer on the selected door. Selectable via drop-down list for door and duration (1-600 seconds).
Emergency Alarm Disengage	Deactivates the emergency alarm function which will resume any override caused by the emergency alarm function.
Emergency Alarm (Silent) - Unlock Doors	Activates the emergency alarm function. Readers will not beep (silent). Will not exclude doors with the "Unlock on Emergency Alarm" option disabled. Affected doors selectable via list.
Emergency Alarm (Silent) - Unlock Unprotected Doors	Activates the emergency alarm function. Panel will not beep (silent). Will exclude doors with the "Unlock on Emergency Alarm" option disabled. Affected doors selectable via list.
Emergency Alarm - Sound	Activates the emergency alarm function. Panel will beep until the Emergency Alarm Disengage function is activated. Will not affect door state.
Emergency Alarm - Unlock Doors	Activates the emergency alarm function. Panel will beep until the Emergency Alarm Disengage function is activated . Will not exclude doors with the "Unlock on Emergency Alarm" option disabled. Affected doors selectable via list.
Emergency Alarm - Unlock Unprotected Doors	Activates the emergency alarm function. Panel will not beep (silent). Will exclude doors with the "Unlock on Emergency Alarm" option disabled. Affected doors selectable via list.
Buzzer	Provides several options to deactivate reader buzzers or outputs configured as external buzzers. Buzzer will reactivate if another event activates the buzzer such as a door forced open.
Alarm Interface Activate	Used to activate an output that is assigned as an alarm interface. In most cases this can be used to arm an alarm system.
Alarm Interface Deactivate	Used to deactivate an output that is assigned as an alarm interface. In most cases this can be used to disarm an alarm system.

Card Formats Tab

The Card Formats tab has several miscellaneous card format settings. This tab also displays available combinations of card formats. For more information on card formats, please see the section called “Edit Sites and Areas: Card Formats”. This section will outline the other options available on this tab.

Table 7.7. Card Format Options

Option	Description
Use Fixed Site Code of 60000	When checked, all credentials presented to readers on this panel will report a sitecode of 60000. This is useful on sites where there are too many site codes or there is no site code.
Remap Site Code 0 to 60000	When checked, all credentials presented to readers on this panel will report a sitecode of 60000 if the original sitecode was 0 and the format of the credential data is anything other than 8 bit burst. This is useful on sites where treating sitecode 0 as a PIN is not desireable.
Suppress invalid card format events	When checked, this panel will not report events related to invalid card formats.

Option	Description
Suppress unknown card format events	When checked, this panel will not report events related to unknown card formats. Useful when there is frequent noise on the reader lines that cannot be resolved.

Integrated Motion: Changing Sensitivity

This section covers how to raise or lower the sensitivity of the **Integrated Motion**. Ensure "Unlock By Motion" is not disabled under **Options Tab** of the **Edit Door Screen**.

Lowering The Sensitivity. To decrease the sensitivity time of the sensor, raise the value of the **Motion Total Sampling**, and lower the value of **On Detections**.

Raising The Sensitivity. To increase the sensitivity time of the sensor, lower the value of the **Motion Total Sampling**, and lower the value of **Off Detections**.

Updating Your Panel

This section will cover the process of updating your Panels. Updating your Panels pushes relevant information into the Panels flash memory. Updating the Panels must be done in order for changes in the software to be applied to the Panels. For example: If you add a new User to the software, the Panel will not be aware of that User until it is updated.

You can update all Panels from any page in the VAX software. Simply click the update Panels button on the top right of the page (pictured below).

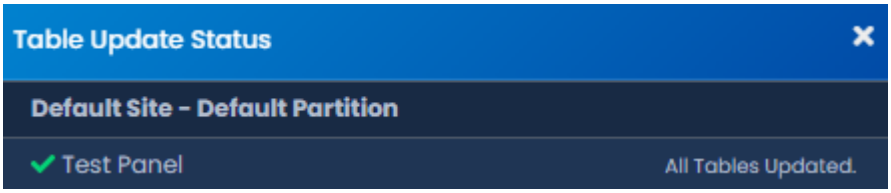
Figure 7.2. Update Panels Button

First Panel Update. Whenever you're doing your first update to your Panels after successfully connecting them for the first time, there are a couple items you should review to ensure your Panels come back online after updating.

- Is the correct server address or name in "Home>System Settings>Server Address"?
- Are your Panels using Door contacts? If not, have they been disabled in the Panel configuration I/O tab?
- If you're doing additional work on the physical Panel, it may be helpful to temporarily disable the Tamper Sensor, which can be changed in "Home>Hardware>Panels>Options>".

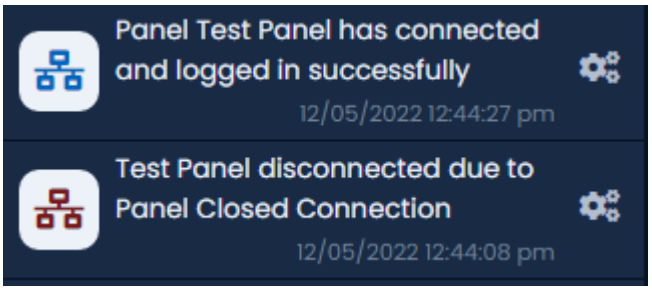
When you click on Update Panels, you'll be prompted by your browser if you are sure you'd like to do this action. Click Yes/Continue/OK. A window will appear in the middle of the screen that will show the status of the updates being sent to the Panel.

Figure 7.3. Panel Update Status Window



After the Panel receives all this information, it will disconnect from VAX for a couple moments and then will attempt to reconnect to VAX.

Figure 7.4. Typical Panel Update Notifications



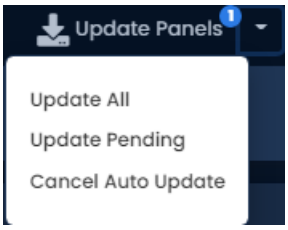
My Panel won't come back online after my first update. If your Panel doesn't come back online after its first update, check "Home>System Settings>Server Address". If it is a name, the Panel may be having trouble resolving the name into an IP through DNS. Consult IT staff; if a stable DNS server is not available you may need to change your server communication mode to static IP.

Auto Panel Update

VAX is capable of updating your Panels automatically after you make changes. This behavior is enabled by default.

Every time you make a change to a Partition, a configurable timer will start counting down. A notification will be displayed on the bottom top any screen. Once this timer reaches 0, the VAX server will automatically update Panels attached to Partitions that have had changes. If you make any additional changes after the timer has begun, it will reset the timer back to the configured default and start again.

Figure 7.5. Auto Update Message



The auto-update timer is a Partition level configuration. To change auto-update settings:

1. On the **Side Bar**, scroll down to the section titled **System**; click on the **Partitions** icon (pictured below).

2. On the Partitions screen, you'll see the a list of all Partitions in the system. Click the blue Edit button next to any Partitions you'd like to configure auto update on.

3. On the Edit Partition page, there will be a checkbox called "Auto Panel Update". If you want to enable auto update, ensure this checkbox is checked.

   You can also configure the Auto Update Timer. 15 minutes is the default, but can be set between 5 minutes and 1440 minutes. If you made any changes, click Save.

Figure 7.6. Auto Update Settings

Panel Firmware Updates

Periodically when we enhance VAX, firmware upgrades to your Panels will be required with the software updates. Updating a Panel's firmware is a relatively straight forward process.

Warning

While in firmware update mode Panels are non-functional. They will not respond to card presentations, do not generate notifications and place the Door into a lock-down state. To limit the impact this has on your site, we suggest only placing 1 Panel at a time into Firmware Update Mode.

1. When a Panel attempts to connect to the VAX application and the firmware is found to be out of date, you will see an indicator near the top of the screen that 1 or more Panels require a firmware update (beside the Panels Online indicator).

Figure 7.7. Firmware Out of Date Notification

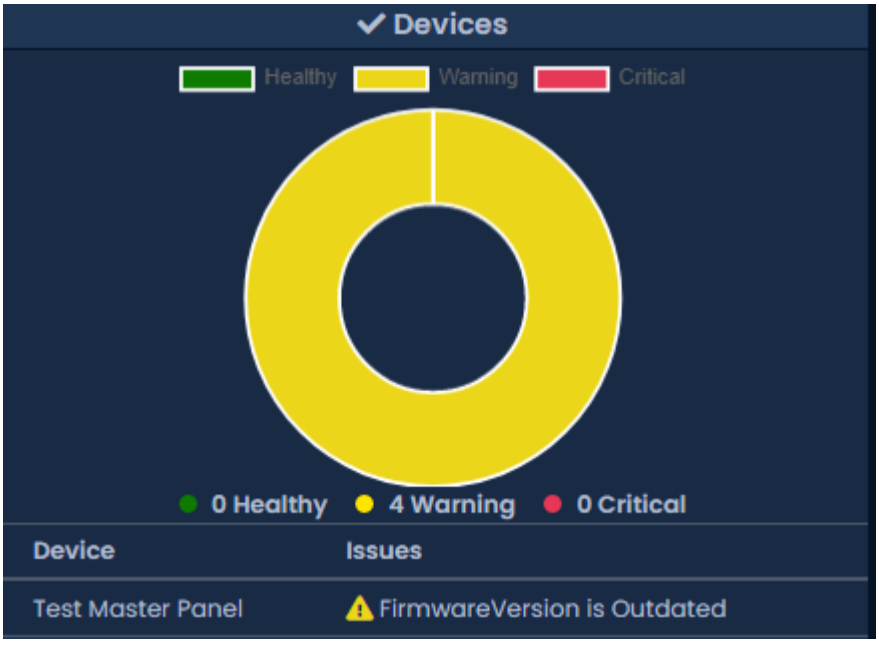
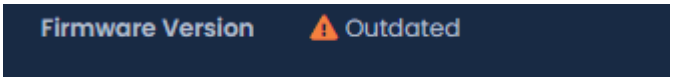
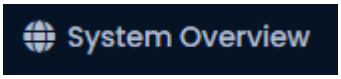


Figure 7.8. Firmware Out of Date Notification



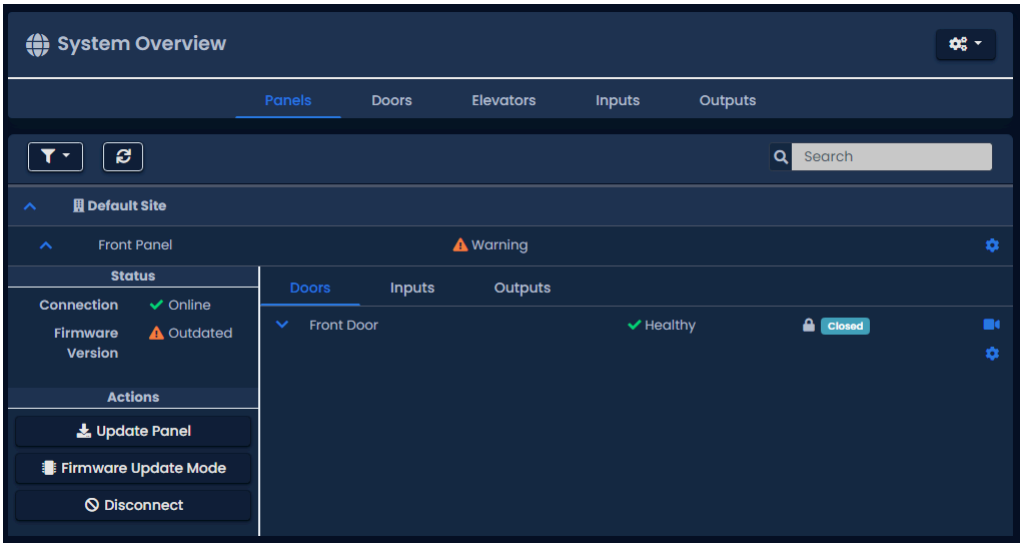
2. In order for a Panel to have its firmware updated we must place it into Firmware Update Mode. To do this we will navigate to the System Overview page in the software. Click on the "x/x Panels

Online" box above the Notifications area **or** on the home page, scroll down to the section titled **System** and click on **System Overview**.



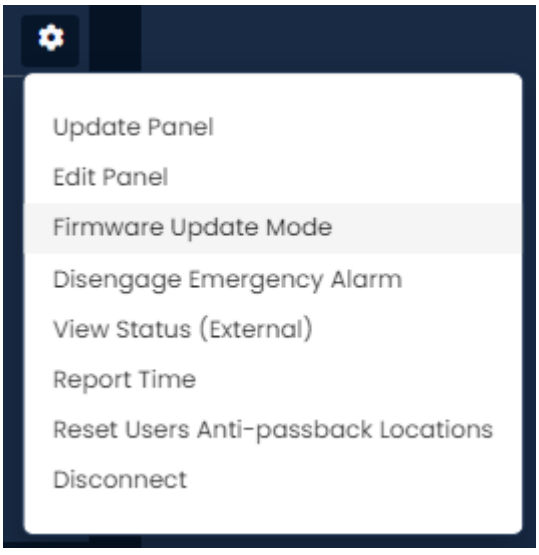
3. On the System Overview you will see a list of all Panels in your system. Any Panels that require a firmware update will have a message displayed next to its name.

Figure 7.9. System Overview Showing Firmware Out of Date Message



4. The next step is to place your Panels into Firmware Update Mode. This can be accomplished on the System Overview page.

   a. On the right side of Panel, click on the gear icon, pictured above. A context menu will appear as pictured below.



   b. Select 'Firmware Update Mode' from the context menu.

   c. The Panel will now disconnect and attempt to update its firmware.

5. The VAX server will accept incoming connections from Panels in firmware update mode on **UDP Port 9876** and automatically apply the latest matching firmware for your Panel. Once complete, the server will instruct the Panel reboot into normal mode, at which point the Panel will resume

normal operation. If the panel does not connect to the server on UDP 9876 within 60 seconds, the panel will reboot.

6. Repeat the above process on all Panels that indicate they require a firmware update. After all Panels have had their firmware updated, we recommend doing a update to all your Panels. The 'Update Mode' status icon above the notifications window will disappear automatically, or you can refresh the page.

Troubleshooting Firmware Update Problems

Panel continues to show firmware out of date after placing it into firmware update mode. If a Panel continues to show it requires a firmware update after placing the panel into firmware update mode and coming back online, ensure there isn't any third party firewall blocking **UDP port 9876**. Ensure there are no enterprise firewall solutions between the server and the Panel on the network blocking UDP port 9876.

Panel does not come back online after placing into firmware update mode. If a panel does not come back online after several minutes, we recommend physically checking the LCD of the panel.

- If the LCD shows the message "Run Application Timeout", power down the panel by unplugging the Cat5 from the left side of the board. Press and hold the button labeled Enter (SW3) while plugging in the cat5. This will place the panel back into firmware update mode.

- The LCD on the panel will show the current server address it is looking to update its firmware from, if you see this set as 192.168.2.10, it could indicate it had a problem during the update. Try the above suggestion or change the VAX server's IP address temporarily to 192.168.2.10 with a 255.255.255.0 subnet mask.

Chapter 8. Setting Up a Door

This chapter will go over all configuration aspects of a Door. Adding a Door is the next logical step after configuring your Door Panels; if during your planning stages you decided you needed additional Door Schedules, we recommend creating these before adding your Doors. Please see Chapter 9, *Door Schedule Configuration*.

Adding a Door

This section will go over the process of adding a Door. When adding a Door, not all aspects are configurable. After you've added the Door, more settings and configuration will be available.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Hardware**, click on the **Doors** icon (pictured below).

4. On the **Doors** screen, you'll notice any Doors you've already configured listed here. Click the **Add** button on this screen.
5. On the **Add Door** screen, you'll have several fields to populate.

Tip

You can also get to the Add Door screen from the Doors tab on the Edit Panel screen.

Figure 8.1. Add Door Screen

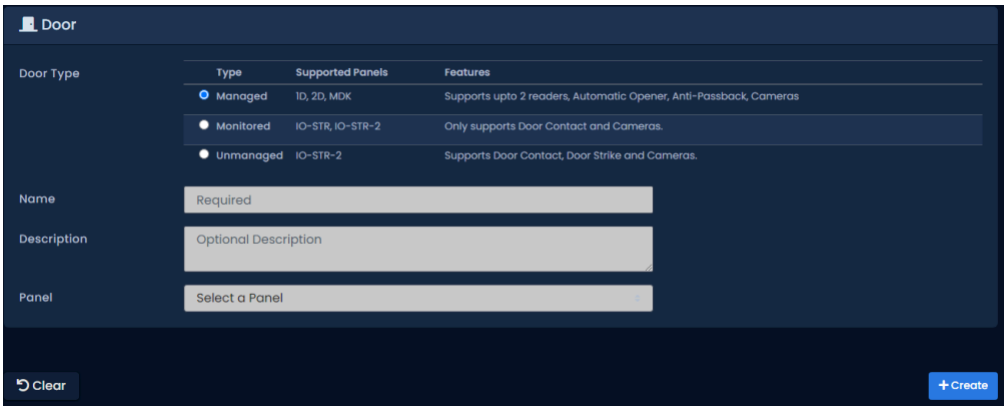


Table 8.1. Add a Door

Text Box/ Drop-down Menu	Description
Door Type	Select Managed for doors with locks and readers. For more information on Unmanaged doors, see the section called “Unmanaged and Monitored Doors with IO-Boards”.
Name	Unique name of your Door. Accepts 4 to 255 characters. We recommend naming your Door by its location or function.

Text Box/ Drop-down Menu	Description
Description	Optional description of the Door. Accepts 4 to 255 characters.
Panel	Once you select a Panel with open ports, additional configuration options will appear on the screen. Select the Panel this Door will be attached to.
Port on Panel	This port represents the index of the Input/Output classifications. Usually you'll increase it sequentially.
Schedule	This is the most important configuration aspect of adding a Door. Select the desired Door Schedule (default or custom). This can be changed after the Door is added.
Door Holiday Group	Here you can select a Door Holiday Group. The default selection is 'No Holidays'. This can be changed after the Door is added.
Reader 1 Name	Unique name of your Reader. Accepts 4 to 255 characters. We recommend naming your Reader by its location, including if it's an IN or OUT Reader.
Reader 1 Description	Optional description of your Reader. Accepts 4 to 255 characters.
Reader 1 Port On Panel	Select a port for the Reader. The port number reflects the physical Reader port on the Panel.
Reader 2	Reader 2 is not supported when the motion controller on the Panel has been enabled. If you wish to use an inside and outside Reader, disable motion on the Panel advanced settings. Once disabled fill in the Reader 2 fields.

6. Once all the required fields are filled, click the **Save** button to add the Door. You'll be prompted with the options to add an additional Door, or to **Continue Configuration**, which will bring you to **Advanced Door Configuration** for the Door you just added.

Advanced Door Configuration

This section will cover the advanced Door configuration options. These settings can only be configured after a Door has been added. For information about adding a Door, please see the section called “Adding a Door”.

1. If you're not already on the Edit Door screen, scroll down on the **Side Bar**, to the section titled **Hardware**, click on the **Doors** icon (pictured below).

2. On the **Doors** screen, you'll notice any Doors you've already configured listed here. Click the blue button next to the Door you'd like to configure.

3. On the **Edit Door** screen, you'll see 5 tabs each with their own configuration items. Some options are not available on specific models or door types.

General

This section will cover configuration items on the **General** tab of Door Configuration.

Figure 8.2. General Tab

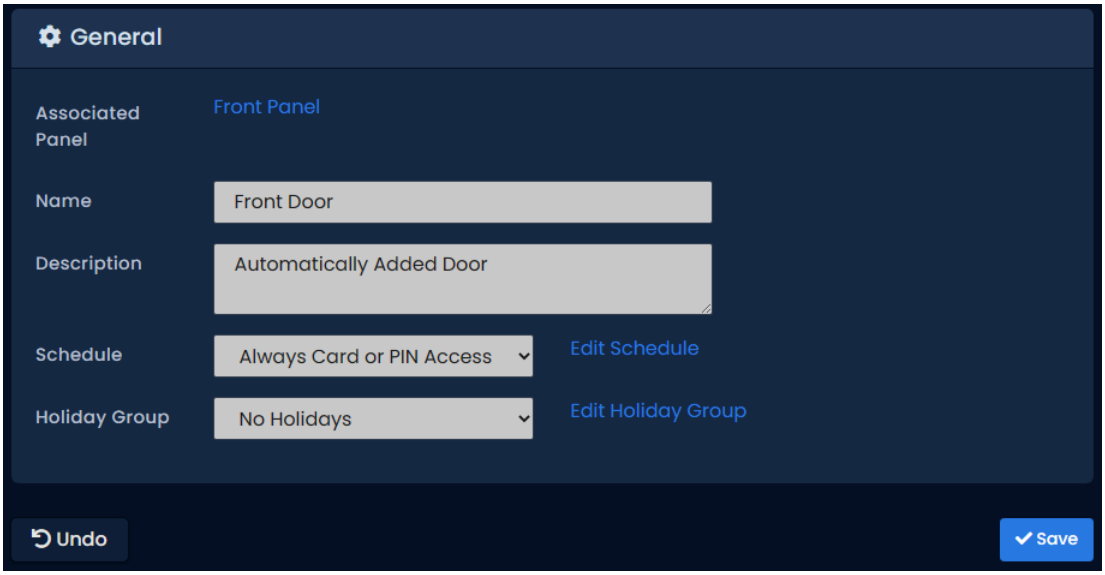


Table 8.2. General Tab

Text Box/ Drop-down Menu	Description
Name	Unique name of your Door. Accepts 4 to 255 characters. We recommend naming your Door by its location or function.
Description	Optional description of the Door. Accepts 4 to 255 characters.
Schedule	This is the most important configuration aspect of a Door. Select the desired Door Schedule (default or custom). You can also edit the selected Door Schedule by clicking the "Edit Schedule" link to the right of the drop-down menu.
Door Holiday Group	Here you can select a Door Holiday Group. The default selection is 'No Holidays'.

Options

This section will cover configuration items on the **Options** tab of Door Configuration.

The first 5 options are miscellaneous:

Figure 8.3. Options Tab

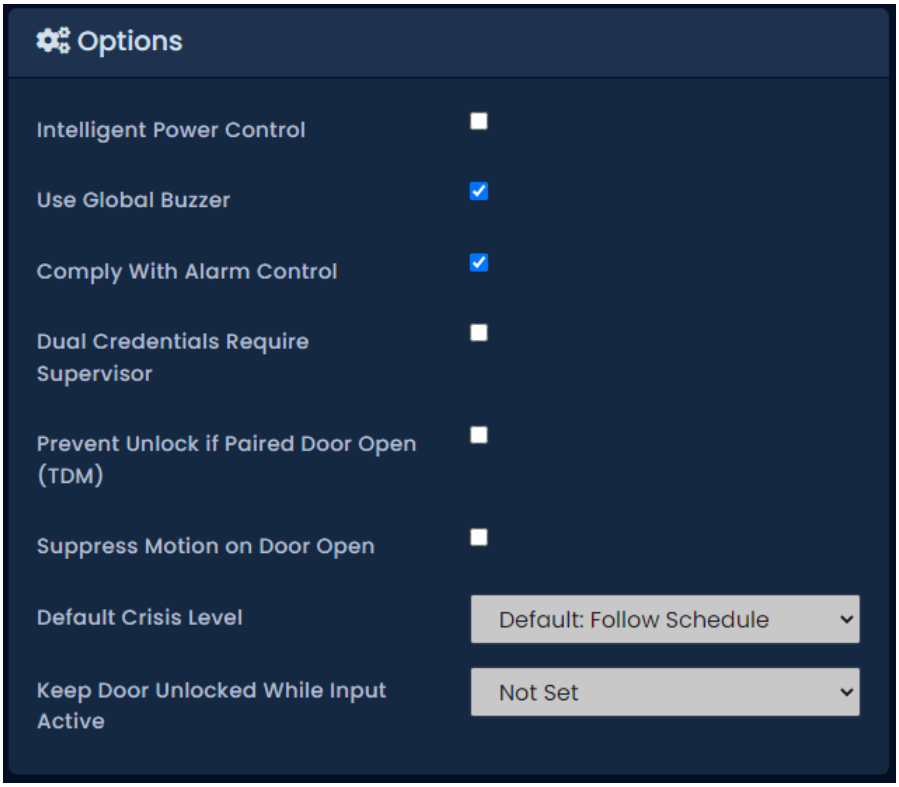


Table 8.3. Door Options Tab

Text Box/ Drop-down Menu	Description
Play Sound on Open	If checked, the Panel will play an audible indicator when the door opens (requires door contact).
Comply With Alarm Control	If checked, the door will change behavior when a configured input with the function External Alarm Status is activated.
Dual Credentials Requires Supervisor	When the Door Schedule indicates Dual Credentials are required, this setting toggles on/off the requirement that the initial Credential presented has the supervisor privilege.
Prevent Unlock if Paired Door Open	This setting enables internal Mantrap logic in Two-Door controllers; for more information on Mantrap configuration, please see Chapter 22, *Mantrap Configuration*.
Suppress Motion on Door Open	Suppresses the Motion Sensor once the Door is open, prevents the motion from unlocking the door or activating door opener when either feature is enabled.
Default Crisis Level	Sets the default crisis level for the door under normal operations.
Keep Door Unlocked While Input Active	Select an input that will keep the door unlocked as long as the input state (closed or open) is maintained.

Timers

The **Timers** section of the options page has various timers with sliders to adjust.

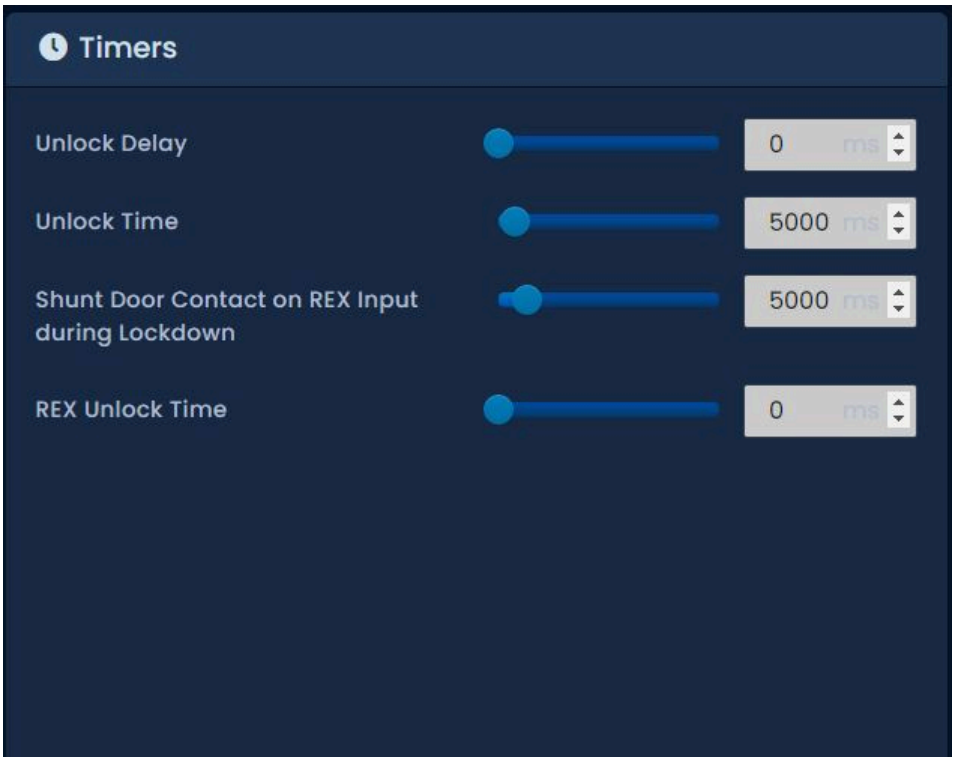


Table 8.4. Timers

Timer name	Description
Unlock Delay	The time delay (in ms) between a credential being authorized and the Door unlocking. Increments by 100 ms. Valid values are 0 ms to 60000 ms.
Unlock Time	The time (in ms) that the Door will stay unlocked after a credential has been authorized. Increments by 100 ms. Valid values are 700 ms to 60000 ms.
Allowed Held Open Time	The Time (in ms) a Door is allowed to be **Held Open** before an alarm is raised. Increments by 100 ms. Valid values are 1000 ms to 300000 ms.
Shunt Door Contact on REX Input during Lockdown	Time (in ms) you may open a door after activating a REX, Motion or Opener button while the door is in Lockdown before it's considered a Forced Open. Increments by 100 ms. Valid values are 2000 ms to 25500 ms.
REX Unlock Time	Alternative unlock time for Request to Exit or Door Opener to Exit activations. Setting to 0 will use the normal Unlock Time. Increments by 500 ms. Valid values are 0 ms to 100000 ms.

Held Open Alarm

The **Held Open Alarm** section of the options page has various options for configuring Held Open Alarms.

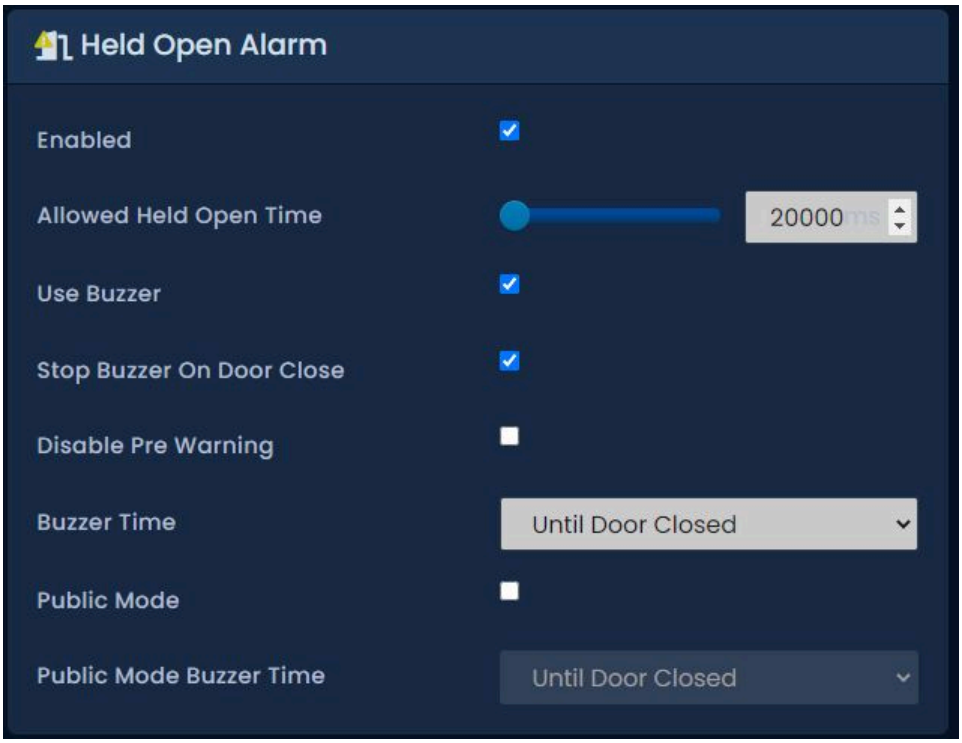


Table 8.5. Held Open Alarm

Held Open Alarm Setting	Description
Enabled	Enables the Held Open Alarm notification and features. Enabled by default.
Allowed Held Open Time	The time (in ms) that the Door will can stay open after the unlock time before a held open event occurs. Increments by 100 ms. Valid values are 1000 ms to 300000 ms.
Use Buzzer	Enables held open to trigger an associated External Buzzer output and fire the internal Buzzer on POE panels. Enabled by Default.
Stop Buzzer on Door Close	When enabled, this feature will stop a Held Open event once the door is closed. Enabled by default. When disabled, requires a valid card swipe to stop a held open event.
Disable Pre Warning	A pre warning buzzer activation that occurs during the Allowed Held Open Time. Unchecked by default.
Buzzer Time	Dropdown with various options for how long the Held Open Buzzer should last. The various options are: Until Door Closed, 5 Seconds, 1 minute, 10 minutes
Public Mode	When enabled, enables Held Open events to occur when the door is in an Unlocked schedule. Unchecked by Default.
Public Mode Buzzer Time	Similar dropdown with various options for how long the Held Open Buzzer should last. Occurs only when the door is in an unlocked state. The various options are: Until Door Closed, 5 Seconds, 1 minute, 10 minutes

Automatic Opener

The **Automatic Opener** section of the options page has various check boxes and sliders for configuration with automatic Door openers. If your deployment does not use an automatic opener, you can move onto the next section.

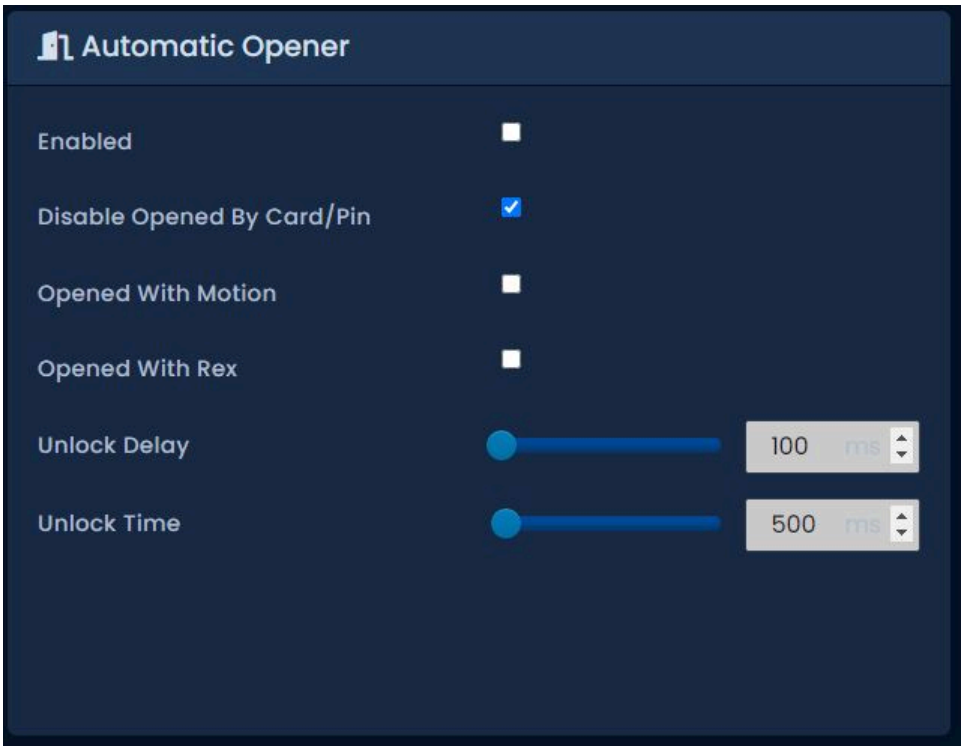


Table 8.6. Automatic Opener

Checkbox/Timer Name	Description
Enabled	Check if an automatic Door opener is attached to this Door. Must be configured in Panel Input/Output configuration.
Disable Opened By Card	If checked, prevents card presentation from triggering the auto opener. The user requires the "Auto Opener" attribute to be enabled.
Opened With Motion	If checked, will allow motion to trigger the auto opener.
Opened With REX	If checked, will allow REX to trigger the auto opener.
Opener Delay	Delay before the activation of the Automatic Opener output. Increments by 100 ms. Valid values are 100 ms to 20000 ms.
Opener On Time	Time that the Automatic Opener output will be activated for. Increments by 100 ms. Valid values are 100 ms to 20000 ms.

Disable

The **Disable** section of the options page has various check boxes. When a checkbox is checked, that item is disabled. For example, if **Unlock By Motion** is checked, the motion sensor will not unlock the Door.

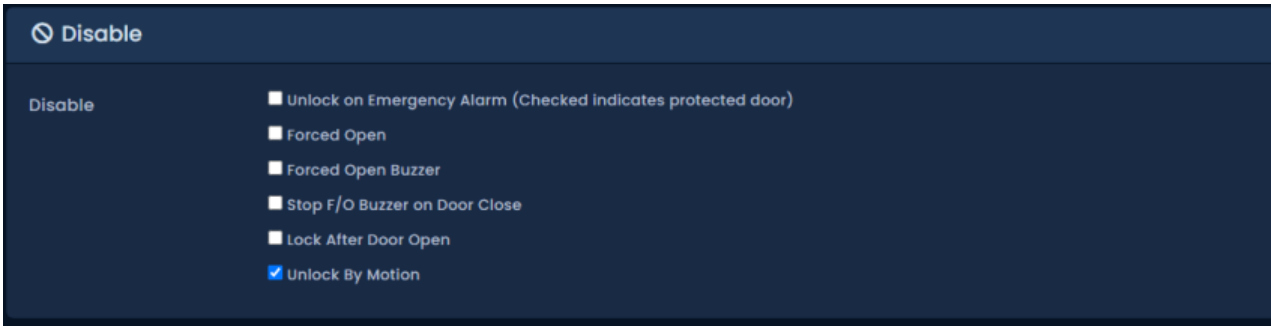


Table 8.7. Disable

Checkbox	Description
Unlock on Emergency Alarm	Prevent Door from unlocking when emergency alarm is triggered.
Forced Open	Disable forced open events from this door.
Forced Open Buzzer	Disable forced open buzzer.
Stop F/O Buzzer On Door Close	By default a forced open event stops when the Door is closed; when disabled, the forced open event continues until a valid credential is presented.
Lock After Door Open	Disable locking the door after the Door opens. Requires a Door Contact.
Unlock By Motion	Disable unlock when motion is triggered.

Once you've made your desired changes, press the **Save** button on the bottom of the page.

Reader Configuration

The **Reader** tabs have various settings for each of the Readers attached to the Panel. Name, description and port number can be reconfigured. There are a couple configuration items that were not available when adding the Door.

Figure 8.4. Reader Tab

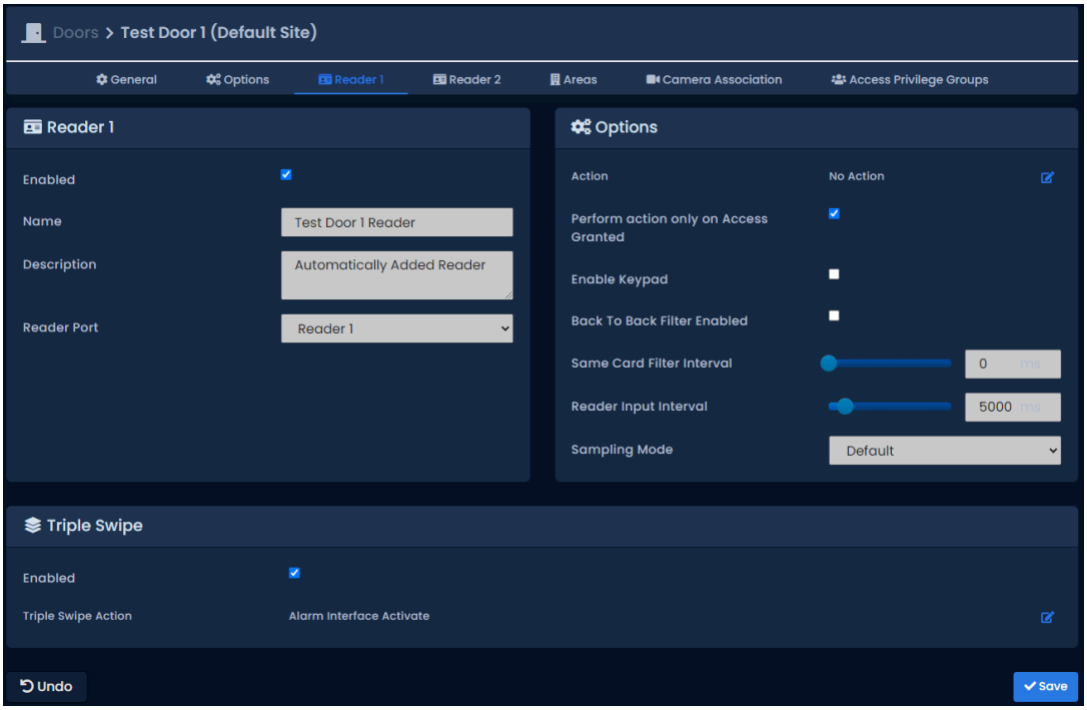


Table 8.8. Reader Configuration Options

Configuration Item	Description
*Action (12VDC models only)	An optional Action is configurable upon a credential being presented to the reader. The available Actions are the sames ones configurable for Triple Swipe. List of actions can be viewed in Chapter 17, *Triple Swipe Features*.

Configuration Item	Description
*Perform action only on Access Granted (12VDC models only))	When checked, any Actions on the previous menu will only occur if the credential is granted access. When not selected, credentials that are denied access will still trigger the Action.
Enable Keypad	Adds keypad functionality for with triple swipe to give more options. Also required for Card and PIN schedules to function as expected. This is not mandatory for Card or PIN schedules or PIN only schedules to function.
Keypad Interval	The allowed time between key presses on a keypad before the Input is considered complete. Increments by 100 ms. Valid values are 100 ms to 10000 ms.
Back To Back Filter Enabled	Enable/Disable the **Back to Back Reader Interference Timer**. Primarily in Reader configurations with an in-out Reader that are back-to-back on the wall. Prevents cards from being scanned by both Readers.
Back To Back Interference Interval	When using back to back Readers the total time after one Reader receives a Credential before the opposing Reader will accept the same Credential. Increments by 100 ms. Valid values are 500 ms to 5000 ms.
Same Card Filter Interval	Multiple credentials of the same value will be ignored for the specified duration. Useful with gates where a long range credential may read several times rapidly. Increments by 100 ms. Valid values are 0 ms to 25000 ms.
Reader Input Interval	Time between swipes before for various actions such as Triple Swipe.
Sampling Mode	This value affects if an interference algorithm is utilized on wiegand reader input with the goal of reducing or eliminating bad card reads caused by interference such as EMI. Values are Default, Mode 1, Mode 2, Mode 4 and Mode 4. Sampling mode can be changed on panel LCD menu for quicker testing.

Once you've made the desired changes, press the **Save** button on the bottom of the page. If you'd like to learn about the Triple Swipe Feature, please see the next section.

Introduction to Triple Swipe

Triple swipe is configured at the Reader level on the bottom of each Reader tab. For examples of triple swipe actions and specific scenarios, please see Chapter 17, *Triple Swipe Features*.

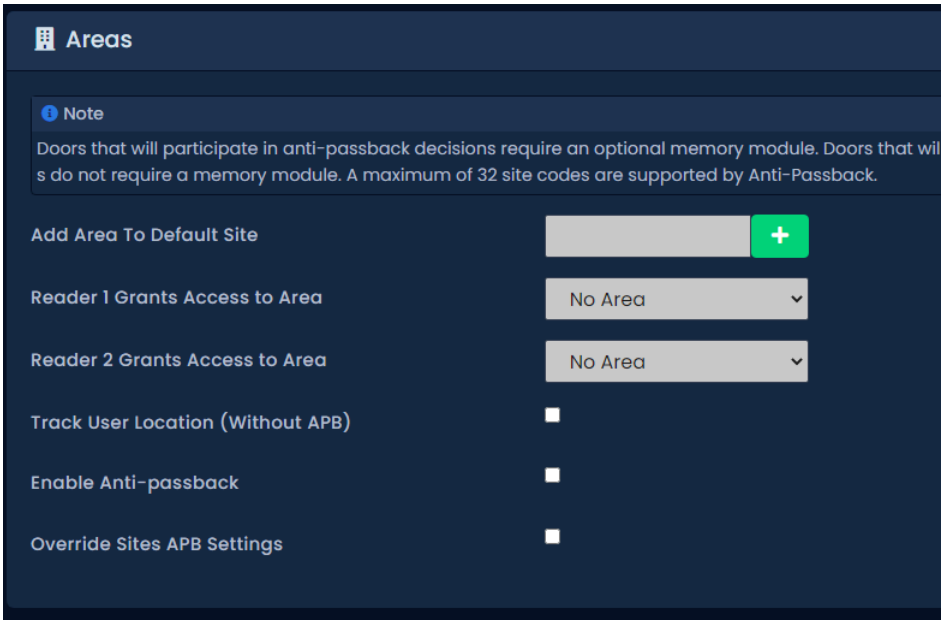
Note

Only Users with the User privilege 'Triple Swipe' or 'Master' are able to perform triple swipe actions. These actions can allow cardholders to lock the door early, arm the alarm system and other useful functions. For more information on User configuration, please see the section called “User Privileges ”.

Areas

The Areas tab contains configuration settings for Area configuration and Anti-passback. For more information on Areas/Anti-passback and configuration requirements, please see Chapter 21, *Areas and Anti-Passback*.

Figure 8.5. Areas Tab



Chapter 9. Door Schedule Configuration

This chapter covers the configuration of Door Schedules in VAX. For information about planning, concepts and examples of Door Schedules, please see the section called “Door Schedules”.

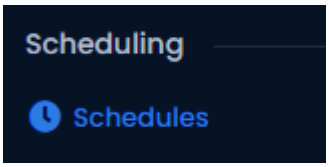
Adding a Door Schedule

Adding a Door Schedule in VAX is a streamlined process that takes full advantage of HTML5. The default Door Schedule 'Always Card Access' is the most commonly used Schedule in the field, however there are hundreds of possible combinations of Door states that can fit many unique situations. Door Schedules can support up to 40 time spans in a day. This section covers how to add a new Door Schedule.

1. Access your VAX system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **Schedules** icon and select the **Doors**Tab. (pictured below).



4. On the **Top Menu** select the section titled *Doors*.

5. On the Door Schedules screen, you'll notice the default Schedules. In a lot of cases these Schedules meet the needs of the system; however, if during your planning stage you (the installer or end-user) decided that additional Door Schedules are needed, click the **Add** button on this screen.

6. On the **Add Door Schedule** screen, you'll have a couple text boxes to populate.

Table 9.1. Add a Door Schedule

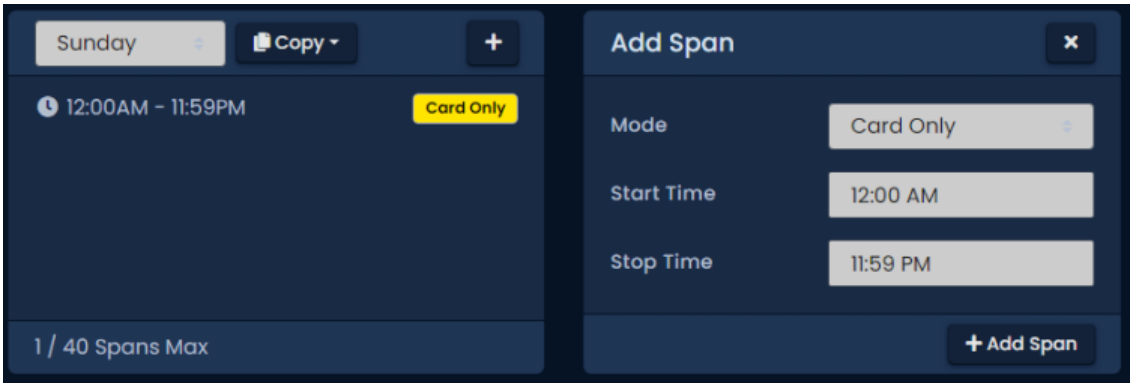
Text Box	Description
Name	Unique name of your Schedule. Accepts 4 to 255 characters. Naming your Schedules by function of the Schedule is recommended.
Description	Optional description of the Schedule. Accepts 4 to 255 characters.
Partitions	Select the Partitions in which you'd like to create this Schedule. If more than one are selected, a copy will be created for each Partition.

7. Creating the **Schedule** is the last step in creating a Door Schedule. The Scheduling section of the *Add Door Schedule* page is pictured below.

Figure 9.1. Door Schedule Editor

8. Select the desired span mode from the options at the top. From here the user can now click-and-drag anywhere on the grid to create a new span. Alternatively, the user can scroll down after simply clicking any day span and scroll down to edit spans in the **Schedule Editor Widget** which provides a list of all spans for the selected day, and a second widget for making changes

Figure 9.2. Span Editor



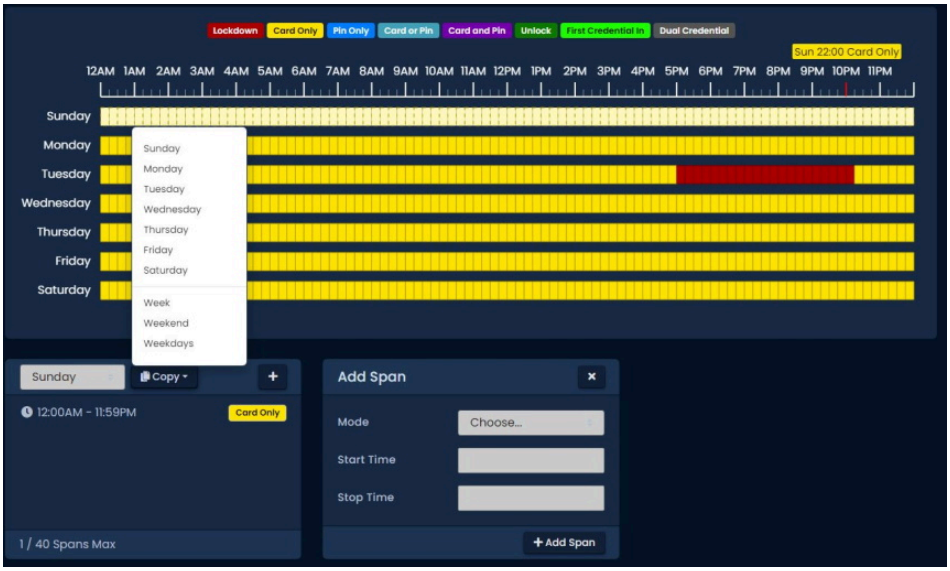
9. Use the **Day Selector** drop-down menu to select the desired day to get a list of all spans for that day. The user can click the + bbutton to add a new span and can use the **Copy** button to copy the entire days schedule to other individual days or multi-day spans such as **Week**, **Weekend** or **Weekdays.**This is useful for defining what state the Door will be in the entire day, or changing the mode for already present spans. (For more information about Door states, please see the section called “Concepts”.)

10. The **Add Span** section of the Schedule editor has 3 fields used for adding a Door Schedule span. The **Start** and **Stop** fields, when clicked, will bring up a clock widget for setting these values. The**Mode** drop-down menu will dictate what Door state the schedule will follow during the defined time span. Once you've completed these fields, click the **Add Span** Button.

11. You should now see the bar you selected color coded to time span you've added. Add additional time spans to that day if required.

    If you'd like the Schedule you've created to be used for several different days, you can click on the **Copy** dropdown list, and select the **Week**, **Weekend**, **Weekdays** or **Days** of the week that is required for the span created.

Figure 9.3. Add Span Widget



12. Once your Door Schedule for all 7 days is as desired, you may now press **Save** to create the Door Schedule in the selected Partitions. For information about how to assign Door Schedules to Doors, please see the section called “Adding a Door”.

Chapter 10. User Schedules

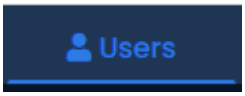
This chapter covers how to add additional User Schedules to VAX. For more information on what a User Schedule is, please see the section called “Concepts”.

Adding a **User Schedule** in VAX closely resembles how we add other Schedules in the software such as **Door Schedules** and **Floor Schedules**. The main differences is that these Schedules are applied to Users through **Access Privilege Groups** and only have two possible states, **Allowed** and **Not Allowed**. User Schedules support up to 8 time spans in a day.

1. Access your VAX system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **Schedules** icon and select the **Users**Tab. (pictured below).



4. On the User Schedules screen, you'll notice the default Schedules. These Schedules can be renamed and modified to fit the deployment needs. If during your planning stage you (the installer or end-user) decided that additional User Schedules are needed, click the **Add** button on this screen.

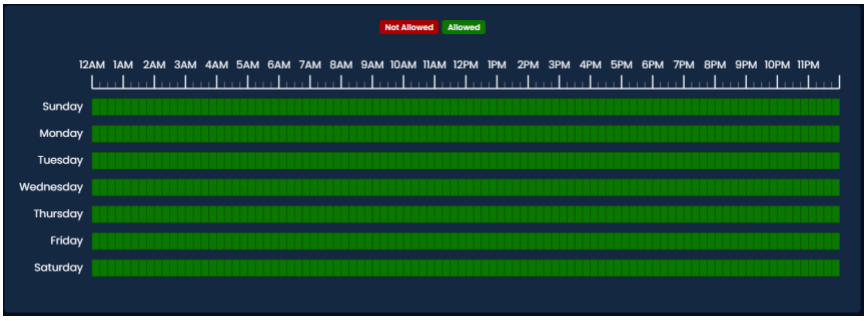
5. On the **Add User Schedule** screen, you'll have a few text boxes to populate.

Table 10.1. Add a User Schedule

Text Box	Description
Name	Unique name of your User Schedule. Accepts 2 to 60 characters. We recommend naming your Schedules by the function of the Schedule.
Description	Optional description of your User Schedule. Accepts 4 to 255 characters.
Partitions	Select the Partitions you'd like to create this Schedule in. If more than one are selected, a copy will be created for each Partition.

6. Schedule: Creating the schedule is the last step in creating a User Schedule. Below is what the schedule part of the Add Schedule page looks like.

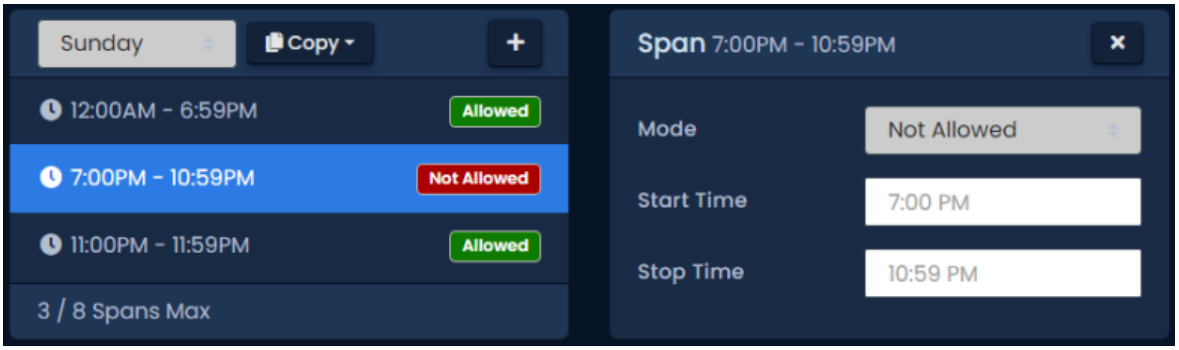
Figure 10.1. User Schedule Editor



7. Select the desired span mode from the options at the top. From here the user can now click-and-drag anywhere on the grid to create a new span. Alternatively, the user can scroll down after simply

clicking any day span and scroll down to edit spans in the **Schedule Editor Widget** which provides a list of all spans for the selected day, and a second widget for making changes

Figure 10.2. Schedule Editor



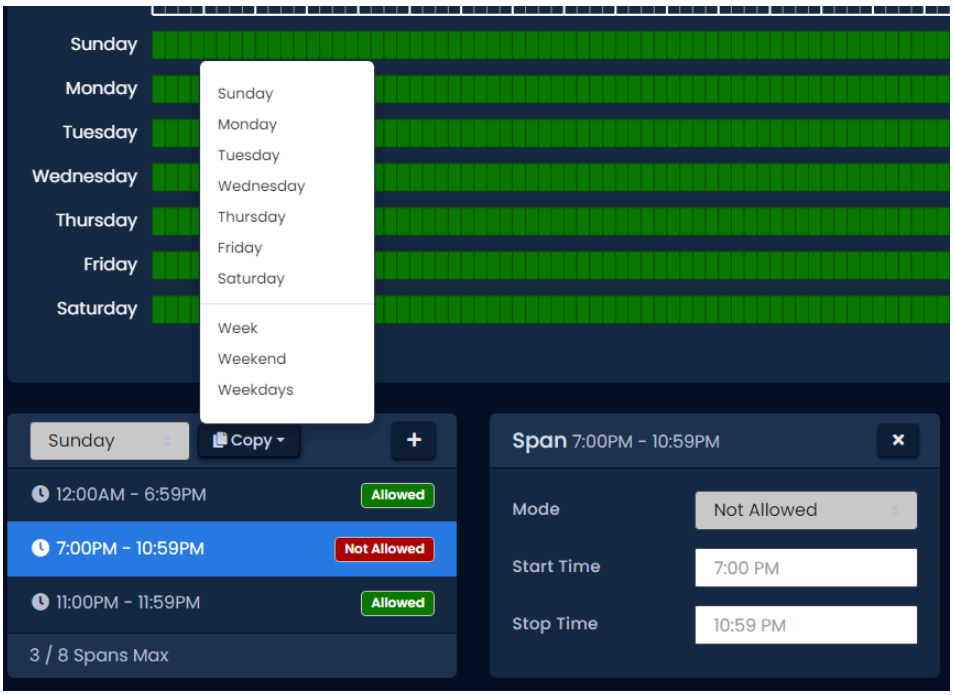
8. Use the **Mode** drop-down menu to select the User access state for the selected span. Only **Allowed** and **Not Allowed** are available.

9. The **Add Span** section of the Schedule editor has 3 fields used for adding a User Schedule span. The **Start** and **Stop** fields, when clicked, will bring up a clock widget for setting these values. The**Mode** drop-down menu will dictate what User Access state the schedule will follow during the defined time span. Once you've completed these fields, click the **Add Span** Button.

10. You should now see the bar you selected color coded to time span you've added. Add additional time spans to that day if required.

    If you'd like the Schedule you've created to be used for several different days, you can click on the **Copy** dropdown list, and select the **Week**, **Weekend**, **Weekdays** or **Days** of the week that is required for the span created.

Figure 10.3. Add Span Widget



11. Once your User Schedule for all 7 days is as desired, you may now press **Save** to create the User Schedule in the selected Partitions. For information about how to assign User Schedules to Users, please see Chapter 11, *Access Privilege Groups*.

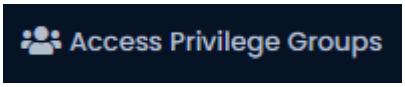
Chapter 11. Access Privilege Groups

This chapter will cover how to add an **Access Privilege Group** in VAX. If you'd like more information about planning an Access Privilege Group and example scenarios, please see the section called “Concepts”.

As mentioned in Chapter 5; Access Privilege Groups are the method that we give **Users Access** or **No Access** to **Reader(s)/Floors**. Users who need the same level of access are placed into one group, where Users with additional access needs are placed in a different group.

Alternately, we can create our Access Privilege Groups based on the Doors/Doors in the group, giving us additional control over which Doors/Floors Users can access.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Users**, click on the **Access Privilege Groups** icon (pictured below).



4. On the Access Privilege Groups screen, you'll notice any groups you've already created. Click the **Add** button on this screen.
5. On the **Add Access Privilege Group** screen, you'll have a few fields to populate.

Table 11.1. Add a Access Privilege Group

Text Box	Description
Name	Unique name of your Access Privilege Group. Accepts 2 to 60 characters. We recommend naming group by the type of Users that will be in the group.
Description	Optional description of your Access Privilege Group. Accepts 4 to 255 characters.
Partitions	Select the Partitions you'd like to create this access privilege group in. **Only Readers from that Partition will be assignable.**

6. Once you've selected a **Partition**, **Users, Readers** and **Floors** that have been configured, that Partition will appear in the three bottom sections of the page.

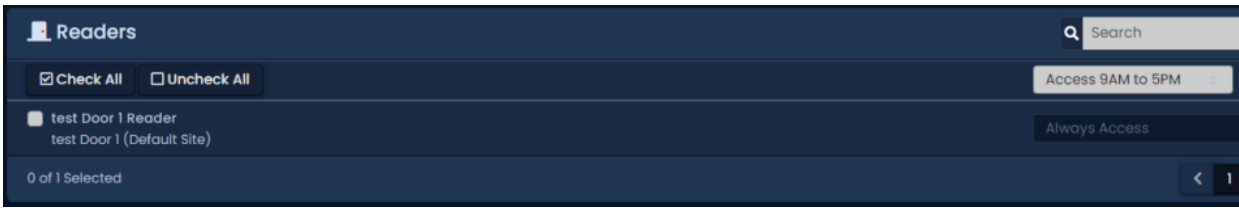
Note

Users are optional when creating an Access Privilege Group. They can be added later as needed.

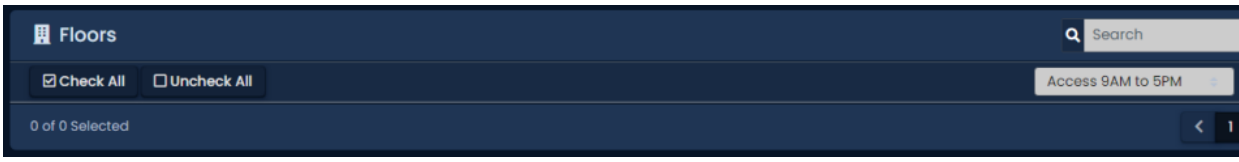
7. In the Readers section: Select the checkbox to the left of any Readers the access group requires access to. Use the drop-down menu on the right side to select the **User Schedule** that will apply to this group at that Reader. If a Reader is not checked, Users in the group will be denied access to unchecked Readers (unless a User is part of a different Access Privilege Group that gives them access).

Note

If none of the User Schedules match the access group requirements, you can create a new User Schedule, please see Chapter 10, *User Schedules*.



8. In the Floors section: Select the checkbox to the left of any Floors the access group requires access to. Use the drop-down menu on the right side to select the **User Schedule** that will apply to this group at that Floor. If a Floor is not checked, Users in the group will be denied access to unchecked Floors (unless a User is part of a different Access Privilege Group that gives them access).



9. Once you've selected the Readers and User Schedules associated with each Reader; you can create the Access Privilege Group. If there are Users in other access groups on the same Partition, you can add them to the group on this screen (as long as their Access Privilege Group doesn't conflict with one being created).

10. Once you're satisfied with the settings (which can be edited later as needed), click the green button **Create**.

Chapter 12. User/Cardholder Configuration

This chapter will cover adding **Users/Cardholders** in VAX, how to apply special User privileges, adding credentials (such as cards, fobs, PINs and pucks), adding pictures of card holders, how to import Users from text files and how to add custom fields to Users.

Adding a User in VAX is a fairly simple process, however there are a variety of options that take advantage of various features of our software.

Prior to adding Users to VAX, you'll generally want some information on the role of each User. If not all this information is available, you can add this information later.

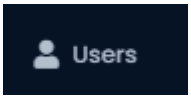
- First name and last name of the User.
- Any special privileges the User may need such as triple swipe access; these privileges will be explained in the next section.
- Credentials of the cards/fobs the User will be assigned. If this is not available, it can be added later.
- Which **Access Privilege Groups** this User will belong to.

Once this information has been gathered, we can now begin adding Users/Cardholders to VAX. Adding Users/Cardholders can be done in several different ways:

- Add each User one at a time.
- Import large amounts of Users at once using a CSV import.
- Enroll the User via clicking the "Unknown User Denied Access" notification generated when an unknown credential is presented to a reader.
- Synchronize VAX with an LDAP provider such as Active Directory (please see Chapter 32, *Active Directory Integration* for more information on LDAP integration).

Adding a User: One User at a Time

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Users**; click on the **Users** icon (pictured below).



4. On the Users screen, you'll see any Users you've already created. Click the **Add** button on this screen.

User Privileges

On the **Add User** page, there will be several text boxes and check boxes to fill, including **Special User Privileges**. The following chart gives a brief explanation of each item in the **General** section of the Add Users page. All general settings are optional except First Name and Last Name.

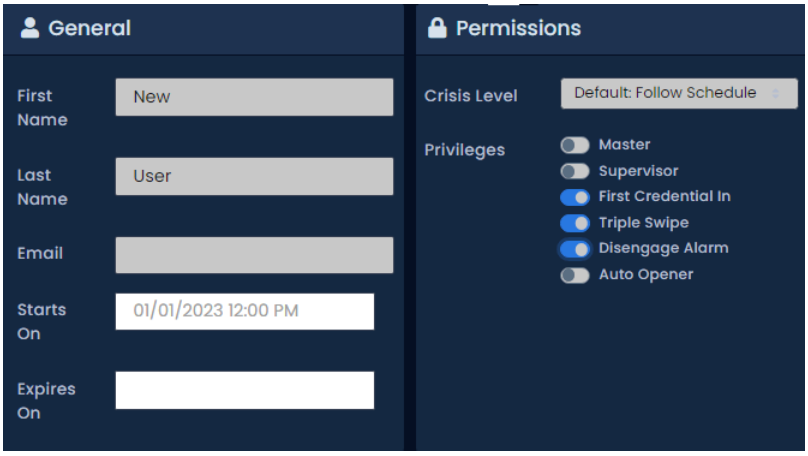
Table 12.1. Add User: General Settings

Text Box/Check box	Description
First Name	The User's first name. Accepts 1 to 60 characters.
Last Name	The User's last name. Accepts 1 to 60 characters.
Starts On	The date the User becomes active. Prior to this date the User will be denied access regardless of Schedule or privilege (optional). Time is accurate to within 10 minutes. Aperio panel models are accurate to the day.
Expires On	The date the Users access will automatically be revoked. Useful for contractors and temporary workers (optional). Time is accurate to within 10 minutes. Aperio panel models are accurate to the day.
Crisis Level	The Security Level the User is granted when Crisis Mode is initialized. If the security level is equal or greater than the Crisis Level, the User will be granted access. For more information about Crisis Levels, please see Chapter 15, *Crisis Levels*
Master	Enable/Disable Master User privilege. Master Users have full access to all Doors and Floors, regardless of schedule or other privileges. Implicitly enables Triple Swipe permissions for the user. Useful for security staff or emergency personnel.
Supervisor	Enable/Disable Supervisor User privilege. Supervisor Users can be used to grant other Users access to Doors where Dual Credential is the Door state and supervisor is required. Supervisors can be granted access to doors when they are in lockdown, but only if their Access Privilege Group permits so.
First Card In	Enable/Disable the First Credential In privilege for this User. This allows the User to trigger a Door unlock mode when the Door is following a First Credential In Schedule.
Triple Swipe	Enable/Disable the User's privilege to trigger any pre-configured triple swipe actions at the Door. For more information about triple swipe options, please see Chapter 17, *Triple Swipe Features*.
Disengage Alarm	Enable/Disable the User's privilege to Disengage Emergency Alarm via double swipe.
Auto Opener	Does this User required an automatic opener to be triggered (if available).

Note

First name and last name are the only required fields in the **General** section of the adding a User page.

Figure 12.1. General Settings example



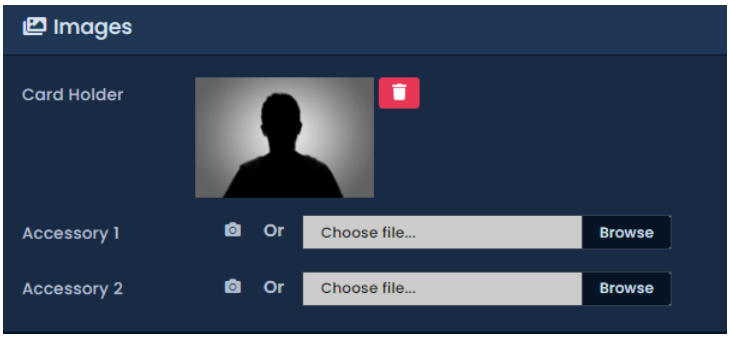
User Card Holder Images

The next section is **Images**. You can upload up to 3 images per User. The Card Holder image is the main image that will appear in the notifications for that User. Accessory 1 and 2 can be used for additional photo badging images. You can also take pictures right from the web browser if an image device is connected to the computer and you are using Google Chrome.

Images are stored on the VAX server in: "<Installation Directory>\VAX\WebServer\content\Uploads\UserProfilePictures".

A card holder image is not required to add a User. An image can be added/edited at any time.

Figure 12.2. Images example



Custom Fields

The next section is **Custom Fields**. If any custom fields have been previously created, they can be populated in this screen for each User.

If you need to create additional custom fields, please see the section called “Adding Custom Fields”.

Figure 12.3. Custom Fields: Example

User Credentials

The next section is **Credentials**. Here you can add a variety of Credentials such as cards, fobs, PINs or a combinations of these credentials.

1. Enter the site code (also referred to as facility code) and card number of the Credential into the **Site Code** and **Card Number** text boxes. A PIN number associated with the Credential will be auto generated for Card and Pin schedules unless the Auto checkbox is unchecked.

   ### Note

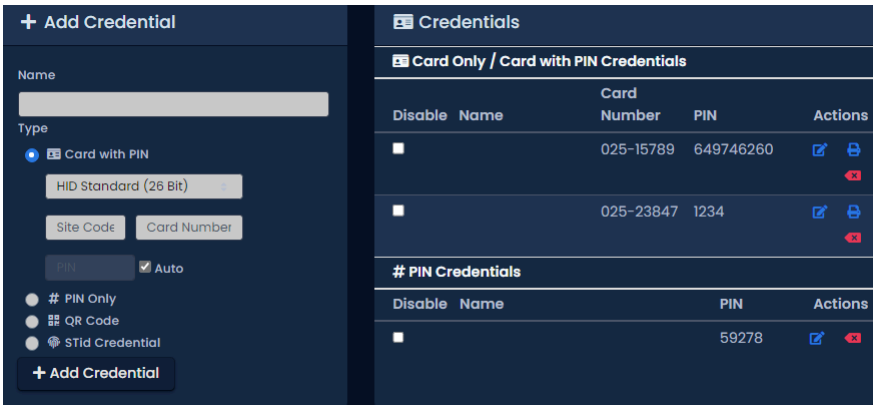
   If your site does not utilize PIN schedules, the auto-generated PIN will be ignored.

2. Once you've entered the Credential information, click the **Add Credential** button. The Credential you entered will be moved to the right side of the screen, indicating success.

3. To add PIN credentials for Pin Only schedules, click the **Pin Only** radio button and enter a PIN (by default, one will be automatically generated). Once entered, click the **Add Credential** button.

You can now enter any additional Credentials associated with the User.

Figure 12.4. Credentials: Example



Depending on the Door Schedule, the reader will expect different types of credentials from the User.

Card Schedules. The reader will expect a card/fob presentation from the User.

Card and Pin Schedules. The reader will expect a card/fob presentation, followed by a PIN entry that matches the associated card. In the example above, a User presents his card '025-23847'. The reader will expect the PIN '1234' after the card presentation.

Card or Pin Schedules. The reader will expect a card/fob or PIN presentation. In the example above, the User can either present one of his two cards, or enter the PIN '59278'. PIN '1234' will not work with this schedule because it is attached to a card.

Pin Only Schedules. The reader will only expect PINs in this schedule. In the example above, PIN '59278' will grant access. PIN numbers attached to cards will not work with this schedule.

Note

Credentials are not mandatory to add a User and can be added after the User is created.

Access Groups

The last section of adding a User is assigning the User to **Access Privilege Groups**. If you haven't created one, please see Chapter 11, *Access Privilege Groups*

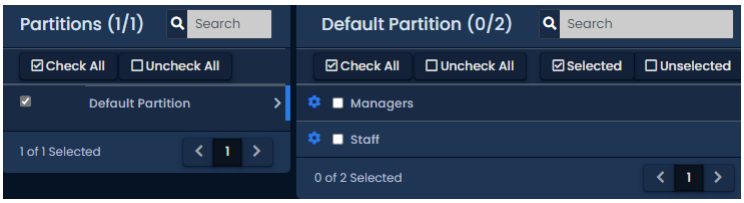
All Partitions you have permission to see will have their associated Access Privilege Groups displayed here. Select the Access Groups the User should belong to.

Note

If no Access Privilege Group is available in the selected Partition, the User can be assigned to that Partition and can be added to an Access Privilege Group at a later time.

Once you have selected the Access Privilege Group and/or Partition the User should belong to, you can now click **Create** to create the User.

Figure 12.5. Access Group: Example



Note

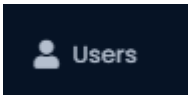
In order to make the door controllers aware of the new credentials and users, you must perform a panel update. Please see the section called “Updating Your Panel”.

User Templates

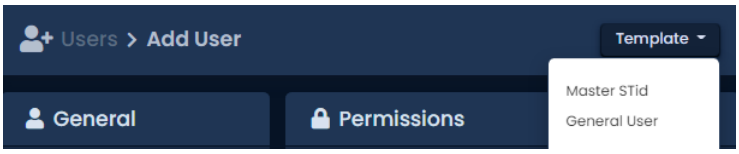
Administrators can create User Templates in order to more quickly add common types of Users.

Adding and updating User Templates is simple:

1. On the **Side Bar**, scroll down to the section titled **Users**; click on the **Users** icon (pictured below).



2. On the Users screen, click the **Add** button.
3. On the top of the Add User screen, the Template drop-down menu will contain any existing templates. Select a template to use it or to update it. Leave it blank if you're creating a new one.



4. Fill out any privileges (triple swipe, First Card In, etc), Starts On, Expires On, Partitions and Access Groups that you want to include in the template.
5. Click Create Template or Update Template on the bottom left of the screen.

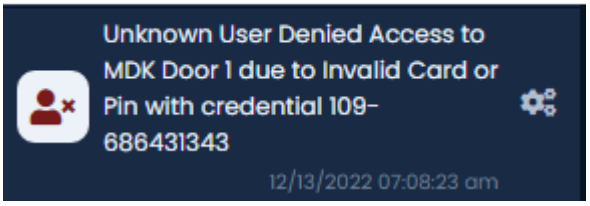
6. You'll be prompted to name the User Template. By default, templates will only be seen by the Administrator who creates it. Setting the template as Global makes it appear for all Administrators, regardless of partitions.
7. Click Save. The template will be created and will now appear in the Templates drop-down menu when adding a User.

> **Note**
>
> If a template provides access to a partition that an administrator does not have permission to, the user created will not be apart of that partition.

Enrolling Cardholders via Notification

It is possible to enroll users/cardholders without typing any credential information into the software. This section covers how we can enroll a User/Cardholder simply by presenting their new Credential at an available reader.

1. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
2. On the main page of VAX, pay close attention to the notification area on the right side of the screen.
3. Obtain the new Credential that is not currently assigned to any Users/Cardholders in VAX.
4. At a nearby Reader, present the new Credential. The Credential will be denied access, and a notification will appear in the software.
5. 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 bring us to the Add User screen, with the credential pre-populated based on credential corresponding to the notification you clicked on.

6. Fill any additional needed fields needed.

Tip

If the site is very busy, you can click the "Stop" button right above the notification area to pause live notifications; this will give you additional time to find and click the right notification to add the new User/Cardholder.

Importing Users and Card Holders

This section covers how to import large amounts of Users and Credentials into VAX. This is often used when there is a large amount of card holders to be added.

Import cards works by parsing a CSV (Comma Separated Values) file that has user data in a pre-defined, consistent manner. This will typically be a spreadsheet or even a text file. The text file will need to be filled prior to importing, and the format of the file will look generally like this:

Brandon, Riley, 24, 6338

Christine, Payne, 24, 7568

Judy, Lawson, 24, 6496

Patricia, Wright, 24, 7674

Kevin, Turner, 24, 8797

Theresa, Sims, 24, 8688

Additional cards, PINs and custom values can also be added here in this file.

Warning

First and last names must not contain any of the following characters; ?, #, $, %, ^, &, *, (,), @, !, <, >, +, =, \, /, :, ;, ", ~

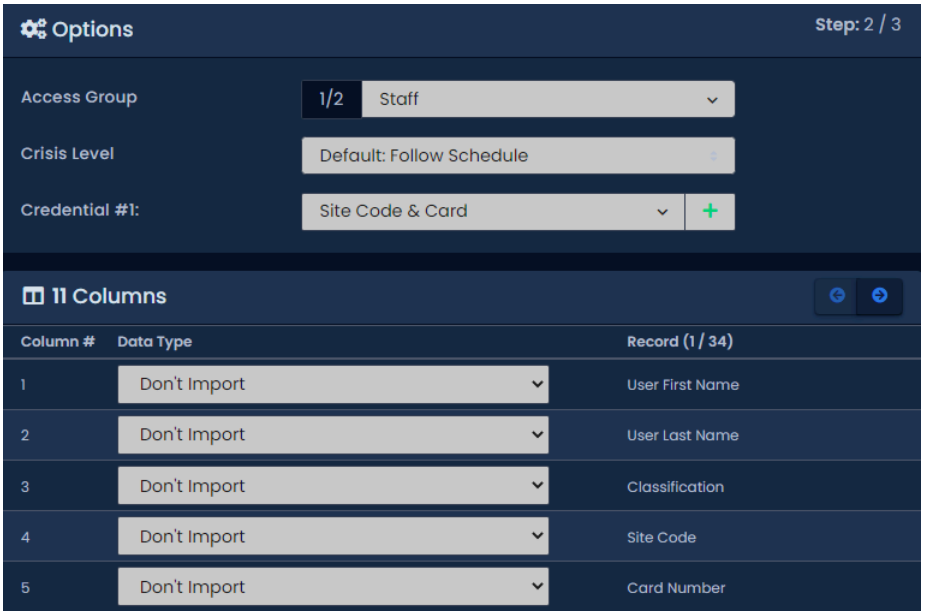
Save the file as **Import.CSV**. You can also use a spreadsheet program, as long as the users are separated by line and the file is saved as a CSV file.

To import the file, follow these steps:

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Users**; click on the **Import Cards** icon (pictured below).

4. On the **Import Cards** screen, click the **Choose File** button in the middle of the screen. A Windows Explorer window will appear; navigate to and select the CSV file.
5. Once you've selected the file, click the **Parse** button on the right side of the screen. VAX will now scan the file and proceed to step 2.

Figure 12.6. Import Options



6. Use the drop-down menu **Access Group** and select the **Access Privilege Groups** these Users will be placed in. You can select more than 1 group.

> **Note**
>
> At least 1 existing access group will need to be selected in the drop down, even when importing the users' Access Privilege Groups as a column.

7. Use the drop-down menu **Crisis Level** and select the appropriate security level for the Users being imported.

8. Use the drop-down menu **Credential #1:**and select the type of credential being imported with each user. Click the + button to add more than one credential.

9. A sample user record and all columns found will be displayed. The Data Type must be selected for each column. Fill in these selections for each column (minimum required selection is First Name, Last Name, Credential #1 Site code, Credential #1 Card Number).

Table 12.2. Import User Data Types

Data Type	Example
First Name	Alice
Last Name	Pierce
Starts On	2014-12-16
Expires On	2014-12-24
Master, Supervisor, First Card In, Triple Swipe, Disengage Alarm, Handicap Opener	True, 1, Yes or ON will enable the attribute for the user. Anything else will be considered 'false'
Credential # Site Code	33
Credential # Card Number	48503
Credential # PIN	1234

10. Click Validate on the bottom of the page once you've filled in all columns and Access Groups.

11. VAX will now validate the records. You can use this chance to review for any errors. Records that cannot be imported will be highlighted in red.

Figure 12.7. Import Preview

12. Click **Import File** to import the Users. Any Users that change to red were not imported due to an error.

You can now edit those Users and add any additional User privileges or add custom field values.

Adding Custom Fields

This section will demonstrate how to add additional Custom Fields to VAX.

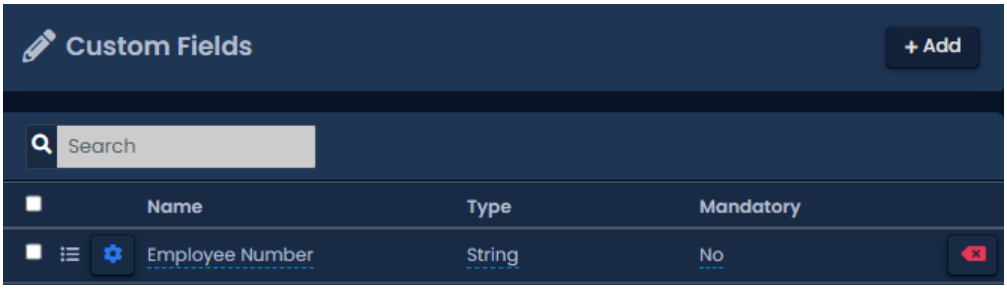
The purpose of custom fields is to allow Administrators to add custom information to Users/Cardholders that is specific to their needs. They can use the custom information to sort and search for users. You can add as many custom fields as you need.

To create additional custom fields, please follow these steps:

1. On the **Side Bar**, scroll down to the section titled **Users**; click on the **Custom Fields** icon (pictured below).

2. On the **Custom Fields** screen, you'll see any custom fields you've already created. To add an additional field, click the **Add** button.

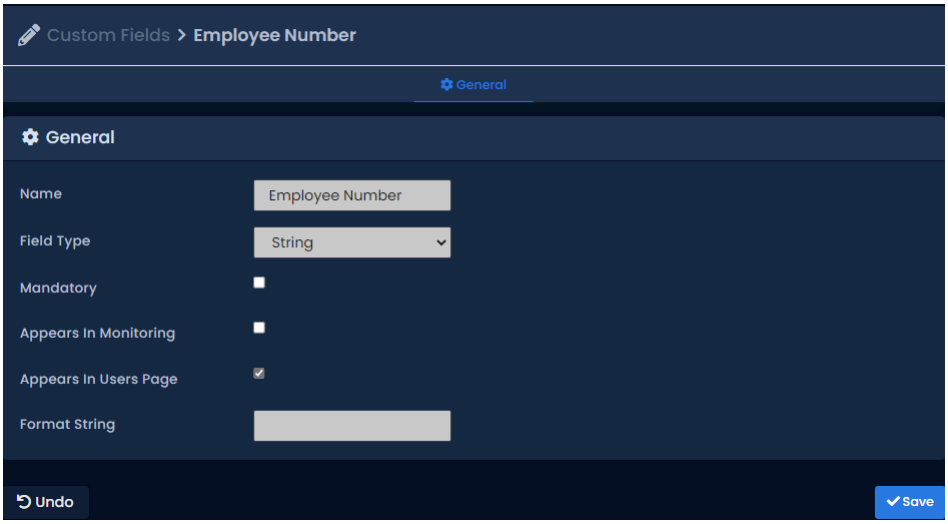
Figure 12.8. Custom Fields



Tip

You can change the order that custom fields appear by clicking and dragging the icon to the left of the custom field name.

Figure 12.9. Add Custom Field



3. On the **Add Custom Fields** screen, fill in the Name of your custom field.
4. Choose a Field Type. The field types are described in the table below.

Table 12.3. Field Types

Field Type	Description
String	Custom field values to be a series of text and/or numbers. Uses a text box when entering values.
Checkbox	Custom field value is displayed as a checkbox. Symbolizes True/False.
Drop-down	Custom field value is displayed as a drop-down menu. When adding the field, you'll select which values are available in the drop-down menu.
Date	Custom field value is displayed as a calendar style date picker.

5. Checking the Mandatory checkbox will make the custom field mandatory when adding a user.
6. Checking the Appears In Monitoring checkbox will make the custom field value appear on the VAX Monitoring screen when a user record is selected.
7. If the Field Type is String, a Format String can be entered to add additional validation when entering values. For example, entering '\d' without the quotes will restrict a string to only numbers. Please see the Microsoft quick reference [https://msdn.microsoft.com/en-us/library/az24scfc(v=vs.110).aspx]on regular expressions.
8. If the Field Type is Date, a format string can be used to define how the date should be displayed/entered (YYYY-MM-DD). See this page [http://momentjs.com/docs/#/parsing/string-format/] for reference.
9. Click **Save**, the custom field will now be available on the **Add/Edit User** screen as well as **Users** screen by selecting **Custom** as the sort option.

Chapter 13. Holiday Configuration

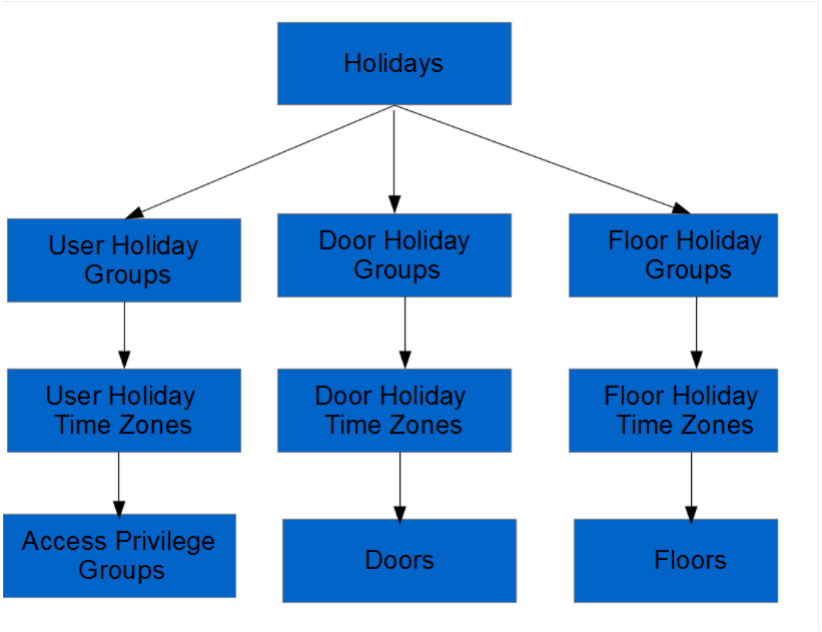
This chapter will cover the configuration of various Holiday components in VAX. We recommend you read the section called “Holidays” prior to reading this chapter for planning how a Holiday should affect your system and an explanation of the components involved.

The 8 components of Holidays in VAX are:

- User Holiday Schedules
- User Holiday Groups
- Door Holiday Schedules
- Door Holiday Groups
- Floor Holiday Schedules
- Floor Holiday Groups
- Holidays

Below is a visualization of how these components apply to each other.

Figure 13.1. Holiday Configuration Diagram



Holiday Order of Operations

Although these Holiday components can be components in any order, there is a general order of configuration that should be adhered to.

1. User/Door/Floor Holiday Schedule:

   After planning how Doors/Floors/Users should behave during a holiday, create these appropriate Holiday Schedules based on what schedules need to deviate from their normal schedules.

2. User/Door/Floor Holiday Group:

If more than the default Holiday Groups are needed, add them.

3. Holidays:

   Add the Holiday and select which User/Door/Floor Groups should be affected by the Holiday, and which Holiday Schedules to adhere to on that Holiday.

4. Assigning User/Door/Floor to Holiday Groups:

   The last part of a Holiday is assigning Doors, Floors and Access Privilege Groups to their appropriate Holiday Groups.

User Holiday Schedules

This section will cover the configuration of **User Holiday Schedules**.

By default VAX comes installed with 2 default User Holiday Schedules:

Holiday Access 9AM to 5PM: with a schedule of 'Allowed' from 8am to 5pm and 'Not Allowed' any other time of the day.

Holiday No Access: with a schedule of 'Not Allowed' all day.

Although this often is enough for most Holiday configurations, it's fairly easy to add additional User Holiday Schedules or to edit the default Schedules.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **Holiday Schedules** icon (pictured below).

4. On the **User Holiday Schedules Screen**, you'll see the default User Holiday Schedules, if you require additional Schedules; click the **Add** button.

5. On the **Add User Holiday Schedule screen**, you'll see it looks almost exactly like other Schedules you've added in the system. Populate the text boxes and check boxes with the appropriate values.

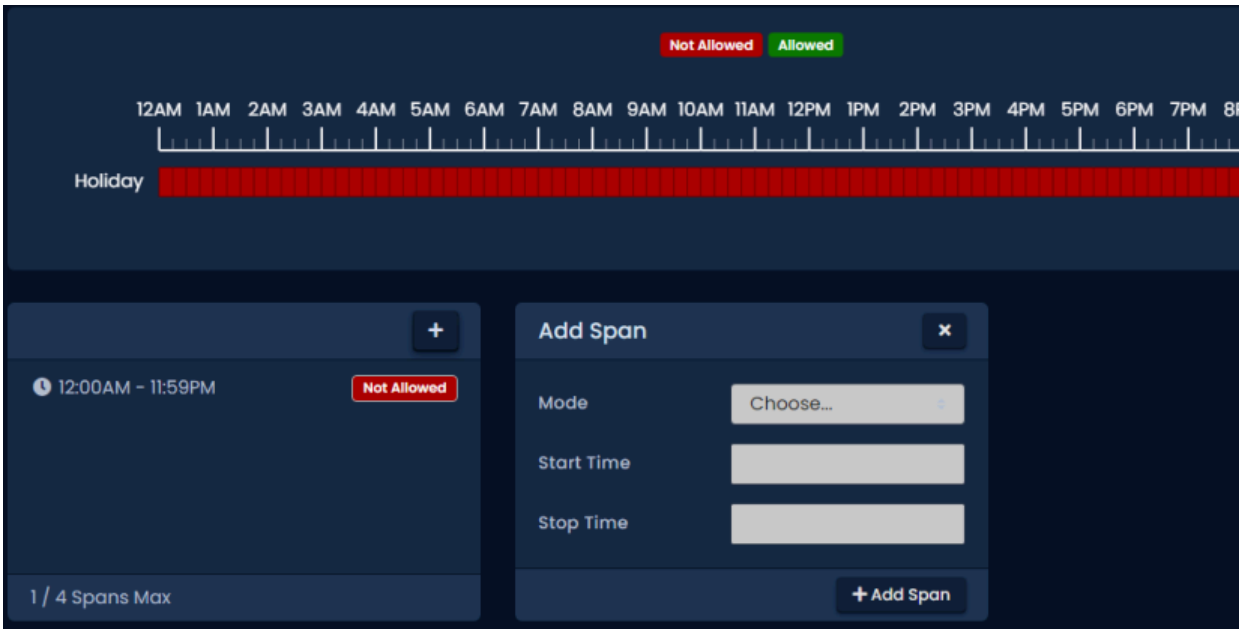
Table 13.1. Add User Holiday Schedule

Text Box/Check box	Description
Name	Unique name of your Holiday User Schedule. Accepts 2 to 60 characters. We recommend naming the Schedule as its function for easier readability.
Description	Optional description of your User Holiday Schedule. Accepts 4 to 255 characters.
Partitions	Select the Partitions you want to create this Schedule in; if more than one are selected, multiple copies of the Schedule will be created.

6. You may now configure the Schedule based on what you want a User group to have access to during a Holiday. You can click the desired Access state from the top and then click-and-drag the desired

timeline for the selected span. Alternatively, you can click on the Red bar next to **Holiday** in the **Schedule** half of the page. This will bring up the **Schedule Editor Widget**.

Figure 13.2. Schedule Editor



7. On the **Schedule Editor**, you will see the already existing schedule spans. You can click the + button to add a new span which will bring up the Add Span box. You can use the **Mode** drop-down menu to select a Access mode for the entire Holiday if you have already selected an existing span. If you need further customization, use the add span section to change the User Holiday Schedule up to 4 times in a day.

8. Once you've completed the schedule, click on the **Save** button. You have now added a User Holiday Schedule.

User Holiday Groups

This section will cover the configuration of **User Holiday Groups**. By default VAX comes installed with 2 default User Holiday Groups:

Standard Holidays - Default Group, and No Holidays. Although this often is enough for most Holiday configurations, it's fairly easy to add additional User Holiday Groups.

1. Access your VAX system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **Scheduling**, click on the **Holiday Groups** icon (pictured below).

4. On the **User Holiday Groups Screen**, you'll see the default User Holiday Groups, if you require additional groups, click the **Add** button.

5. On the **Add User Holiday Groups** page. Populate the text boxes and check boxes with the appropriate values.

Table 13.2. Add User Holiday Group

Text Box/Check box	Description
Name	Unique name for your Holiday User Holiday Group. Accepts 2 to 60 characters. We recommend naming the group as the type of Holidays it will contain or the User group for easier readability.
Description	Optional description of your User Holiday Group. Accepts 4 to 255 characters.
Partitions	Select the Partitions you want to create this group in; if more than one are selected, multiple copies of the group will be created.

6. Once you've completed filling in the fields, click on the **Save** button. You have now added a User Holiday Group, which will now be assignable in **Access Privilege Groups** and will appear when adding **Holidays**.

Door Holiday Schedules

This section will cover the configuration of Door Holiday Schedules. By default VAX comes installed with 1 default Door Holiday Schedule: Closed During Holidays with a schedule of Lockdown all day. Although this often is enough for most Holidays configurations, it's fairly easy to add additional Door Holiday Schedules or edit the default Schedules.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **Holiday Schedules** icon (pictured below).

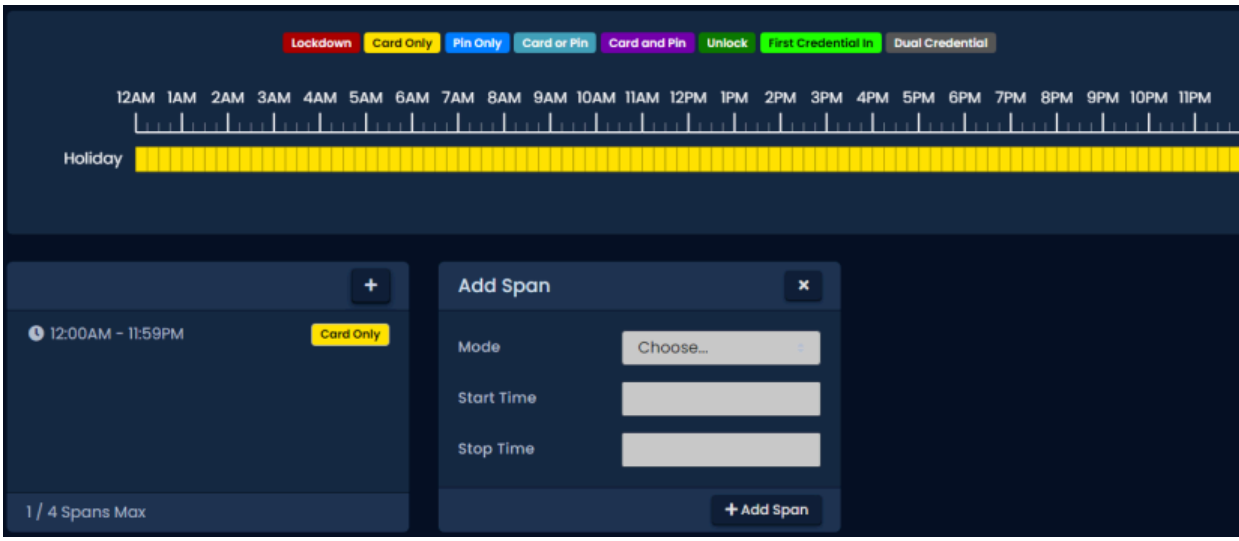
4. On the **Door Holiday Schedules Screen**, you'll see the default Door Holiday Schedule; if you require additional Schedules, click the **Add** button.
5. On the **Add Door Holiday Schedule screen**, you'll see it looks almost exactly like other Schedules you've added in the system. Populate the text boxes and check boxes with the appropriate values.

Table 13.3. Add Door Holiday Schedule

Text Box/Check box	Description
Name	Unique name of your Door Holiday Schedule. Accepts 2 to 60 characters. We recommend naming the Schedule as its function for easier readability.
Description	Optional description of your Door Holiday Schedule. Accepts 4 to 255 characters.
Partitions	Select the Partitions you want to create this Schedule in; if more than one are selected, multiple copies of the Schedule will be created.

6. You may now configure the Schedule based on what you want a Door to do during a Holiday. You can click the desired door state from the top and then click-and-drag the desired timeline for the selected span. Alternatively, you can click on the yellow bar next to **Holiday** in the **Schedule** half of the page. This will bring up the Schedule editor below

Figure 13.3. Schedule Editor



7. On the **Schedule Editor**, you will see the already existing schedule spans. You can click the + button to add a new span which will bring up the Add Span box. You can use the **Mode** drop-down menu to select a Door mode for the entire day if you have already selected an existing span. If you need further customization, use the add span section to change the Door state up to 4 times in a day.

8. Once you've completed the schedule, click on the **Save** button. You have now added a Door Holiday Schedule.

Door Holiday Groups

This section will cover the configuration of Door Holiday Groups. By default VAX comes installed with 2 default Door Holiday Groups: Closed During Holidays and No Holidays. Although this often is enough for most Holiday configurations, it's fairly easy to add additional Door Holiday Groups.

1. Access your VAX system through your HTML5 browser of choice

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **Holiday Groups** icon (pictured below).

4. On the **Doors Tab**, you'll see the default Door Holiday Groups; if you require additional groups, click the **Add** button.

5. On the **Add Door Holiday Groups** page, populate the text boxes and check boxes with the appropriate values.

Table 13.4. Add Door Holiday Group

Text Box/Check box	Description
Name	Unique name for your Door Holiday Group. Accepts 2 to 60 characters. We recommend naming the group as the type of Holidays it will contain or the User group for easier readability.

Text Box/Check box	Description
Description	Optional description of your Door Holiday Group. Accepts 4 to 255 characters.
Partitions	Select the Partitions you want to create this group in; if more than one are selected, multiple copies of the group will be created.

6. Once you've completed filling in the fields, click on the **Save** button. You have now added a Door Holiday Group. which will now be assignable in **Door Configuration** and will appear when adding **Holidays**.

Floor Holiday Schedules

This section will cover the configuration of Floor Holiday Schedules. By default VAX comes installed with 1 default Floor Holiday Schedule: Closed During Holidays with a schedule of Lockdown all day. Although this often is enough for most Holiday configurations, it's fairly easy to add additional Floor Holiday Schedules or edit the default Schedules.

1. Access your VAX system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **Holiday Schedules** icon (pictured below).

4. On the **Floor Holiday Schedules Screen**, you'll see the default Floor Holiday Schedule; if you require additional Schedules, click the **Add** button.

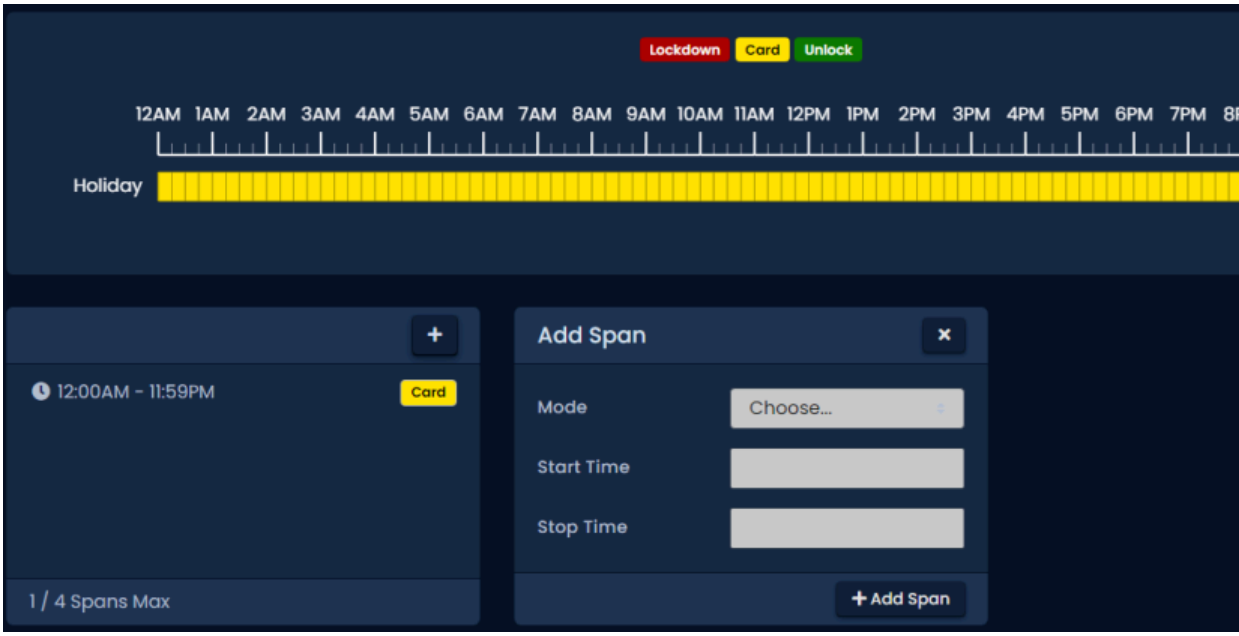
5. On the **Add Floor Holiday Schedule screen**, you'll see it looks almost exactly like other Schedules you've added in the system. Populate the text boxes and check boxes with the appropriate values.

Table 13.5. Add Floor Holiday Schedule

Text Box/Check box	Description
Name	Unique name of your Floor Holiday Schedule. Accepts 2 to 60 characters. We recommend naming the Schedule as its function for easier readability.
Description	Optional description of your Floor Holiday Schedule. Accepts 4 to 255 characters.
Partitions	Select the Partitions you want to create this Schedule in; if more than one are selected, multiple copies of the Schedule will be created.

6. You may now configure the Schedule based on what you want a floor to do during a Holiday. You can click the desired floor state from the top and then click-and-drag the desired timeline for the selected span. Alternatively, you can click on the yellow bar next to **Holiday** in the **Schedule** half of the page. This will bring up the Schedule editor below

Figure 13.4. Schedule Editor



7. On the **Schedule Editor**, you will see the already existing schedule spans. You can click the + button to add a new span which will bring up the Add Span box. You can use the **Mode** drop-down menu to select a Floor mode for the entire day if you have already selected an existing span. If you need further customization, use the add span section to change the Door state up to 4 times in a day.

8. Once you've completed the schedule, click on the **Save** button. You have now added a Floor Holiday Schedule.

Floor Holiday Groups

This section will cover the configuration of Floor Holiday Groups. By default VAX comes installed with 1 default Floor Holiday Groups: Default Holiday Group. Although this often is enough for most Holiday configurations, it's fairly easy to add additional Floor Holiday Groups.

1. Access your VAX system through your HTML5 browser of choice

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **Holiday Groups** icon (pictured below).

4. On the **Floors Tab**, you'll see the default Floor Holiday Groups; if you require additional groups, click the **Add** button.

5. On the **Add Floor Holiday Groups** page, populate the text boxes and check boxes with the appropriate values.

Table 13.6. Add Floor Holiday Group

Text Box/Check box	Description
Name	Unique name for your Floor Holiday Group. Accepts 2 to 60 characters. We recommend naming the group as the type of Holidays it will contain or the User group for easier readability.
Description	Optional description of your Floor Holiday Group. Accepts 4 to 255 characters.
Partitions	Select the Partitions you want to create this group in; if more than one are selected, multiple copies of the group will be created.

6. Once you've completed filling in the fields, click on the **Save** button. You have now added a Floor Holiday Group, which will now be assignable in **Floor Configuration** and will appear when adding **Holidays**.

Adding a Holiday

This section will go over how to add additional Holidays to VAX. This section assumes you have planned out how this Holiday should affect your system. For more information on planning your Holidays, please see the section called “Holidays”.

1. Access your VAX system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **Holidays** icon (pictured below).

4. On the **Holidays Screen**, you'll see the Holidays (Christmas and New Years). If you require additional Holidays, click the **Add** button.

5. On the **Add Holiday** page, populate the text boxes and check boxes with the appropriate values.

Table 13.7. Add Holiday

Text Box/Check box	Description
Name	Unique name for your Holiday. Accepts 2 to 60 characters.
Description	Optional description of your Holiday. Accepts 4 to 255 characters.
Initial Date	The initial date of the Holiday, selected in the date picker widget.
Occurs Annually	When this option is enabled this Holiday is observed every year on the same date.
Use Preset Holidays	When this option is enabled, Canadian, American, and Jewish holidays will be selectable options with a drop down list of the associated preset holidays. Selecting the holiday from the drop down list will also populate the Name and Initial Date fields.
User Groups	Use the check box to select which **User Holiday Groups** you'd like the Holiday associated with. Once checked, use the drop-down next to the group to select the **User Holiday Schedule** that will be applied to that group.

Text Box/Check box	Description
Door Groups	Use the check box to select which **Door Holiday Groups** you'd like the Holiday associated with. Once checked, use the drop-down next to the group to select the **Door Holiday Schedule** that will be applied to that group.
Floor Groups	Use the check box to select which **Floor Holiday Groups** you'd like the Holiday associated with. Once checked, use the drop-down next to the group to select the **Floor Holiday Schedule** that will be applied to that group.

6. Once you've completed filling in the fields, click on the **Save** button. You have now added Holiday.

Note

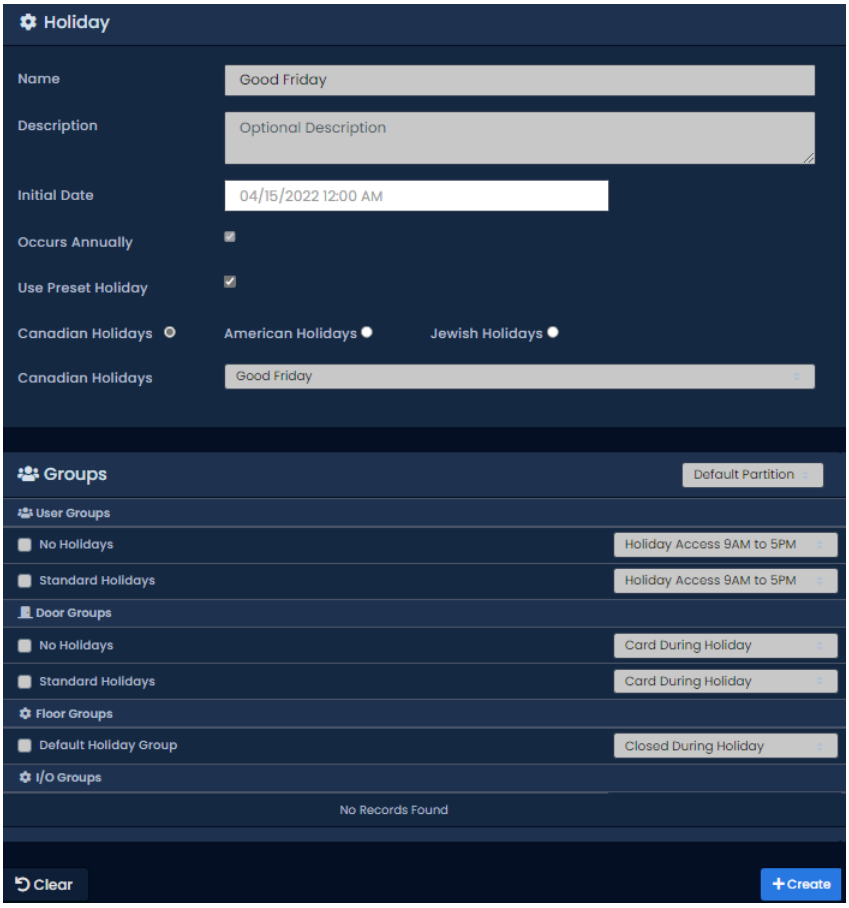
Remember to perform an Update to your Panels in order for them to be aware of the new Holiday.

Holiday Example

This section contains the example of Independence Day being added as a Holiday in VAX.

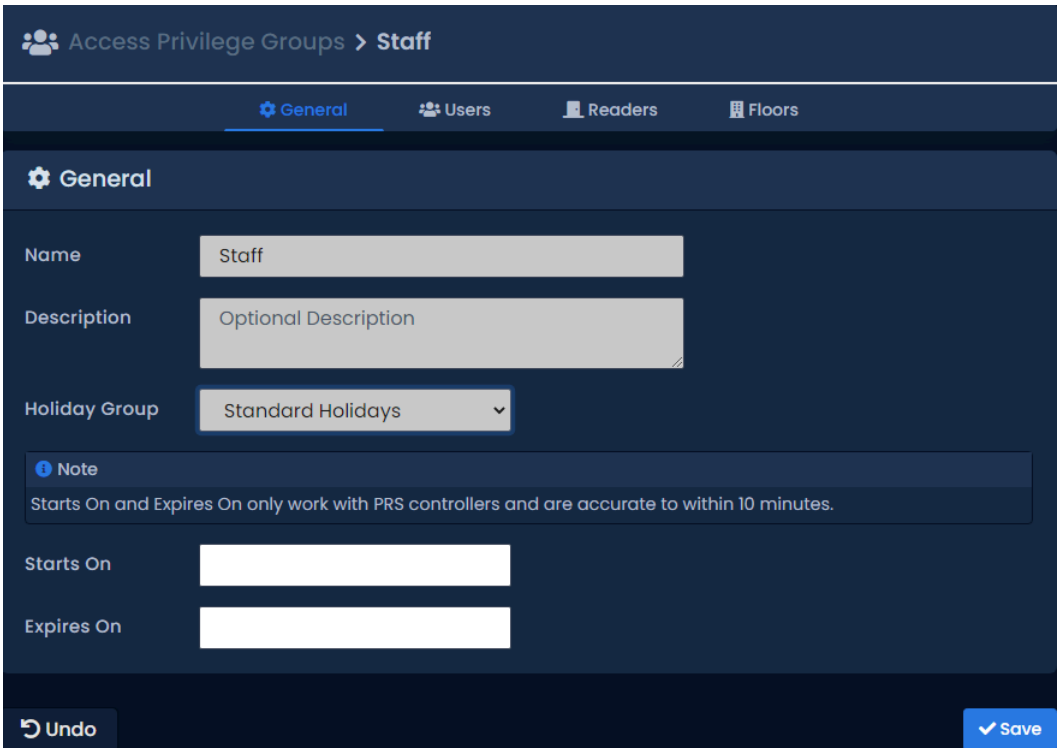
In this example, we will use the default **Holiday Schedules** and **Holiday Groups**. We simply add the Holiday and make sure **Doors** have the **Door Holiday Group** applied to them, the **Access Privilege Groups** have the **User Holiday Group** applied to them, and the **Floors** have the **Floor Holiday Group** applied to them

Figure 13.5. Adding Good Friday



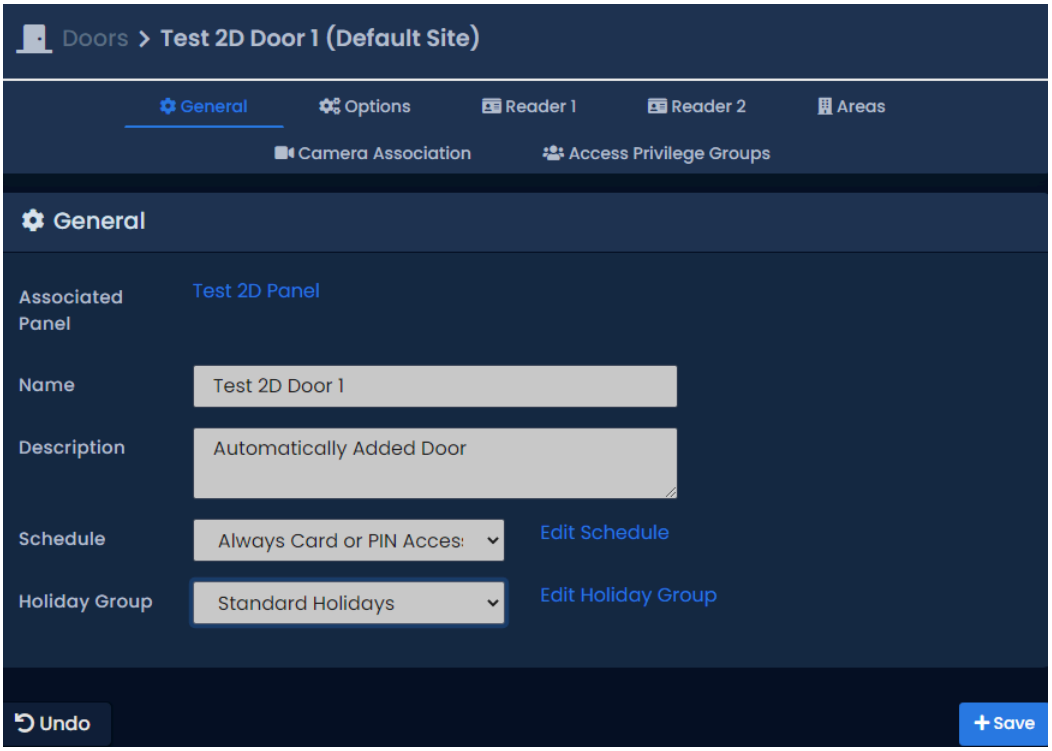
After the above Holiday has been added, we'll need to make sure the **Access Privilege Groups**, **Doors** and **Floors** that the Holiday should affect have the appropriate **Holiday Groups**.

Figure 13.6. Access Privilege Groups: Holiday Group



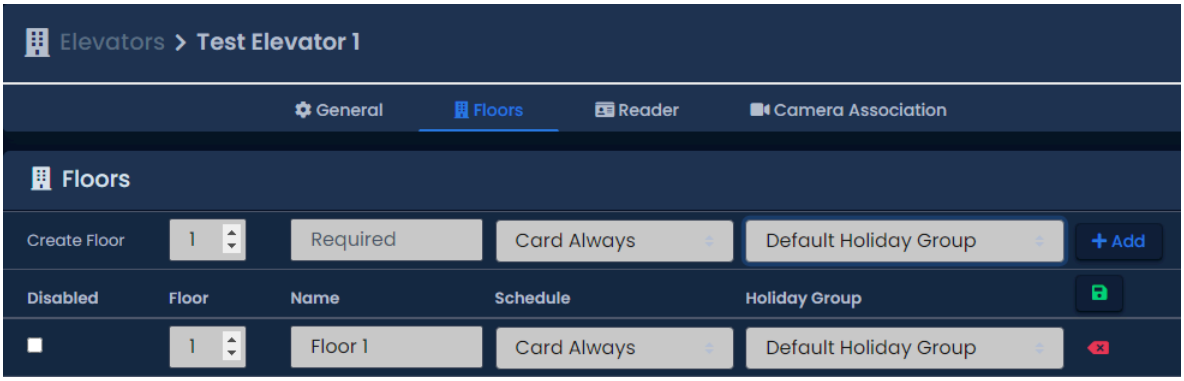
In the above screen shot, you see we've changed the **Holiday Group** drop-down menu to the **Standard Holidays User Holiday Group**, which is the User group we've added the Holiday to earlier.

Figure 13.7. Door: Holiday Group



In the above screen shot, you see we've changed the **Holiday Group** drop-down menu to the **Standard Holidays Door Holiday Group**, which is the Door group we've added the Holiday to earlier.

Figure 13.8. Floor: Holiday Group



In the above screen shot, you see we've changed the **Holiday Group** drop-down menu for each Floor to the **Default Floor Holiday Group**, which is the Floor Group we've added the Holiday to earlier. Note that we can have Floors with different Holiday Groups.

Chapter 14. One Time Run Zones

One Time Run Zones (OTR) are used to create one time events where a Door or Floor state changes on a specific day for a predetermined amount of time.

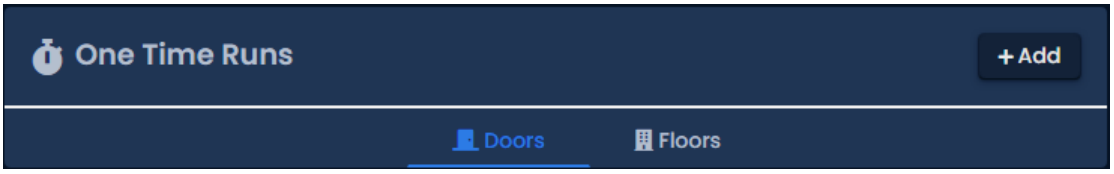
This feature can be useful for events that require the Door/Floor to deviate from its normal schedule.

Adding a One Time Run Schedule

This section covers the steps to adding a OTR on VAX.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Scheduling**. Select the **One Time Runs**icon. (Picture Below)

4. At the top of the One Time Runs screen, **Doors** and **Floors** will be the two options available for adding a One Time Run. (Picture Below)



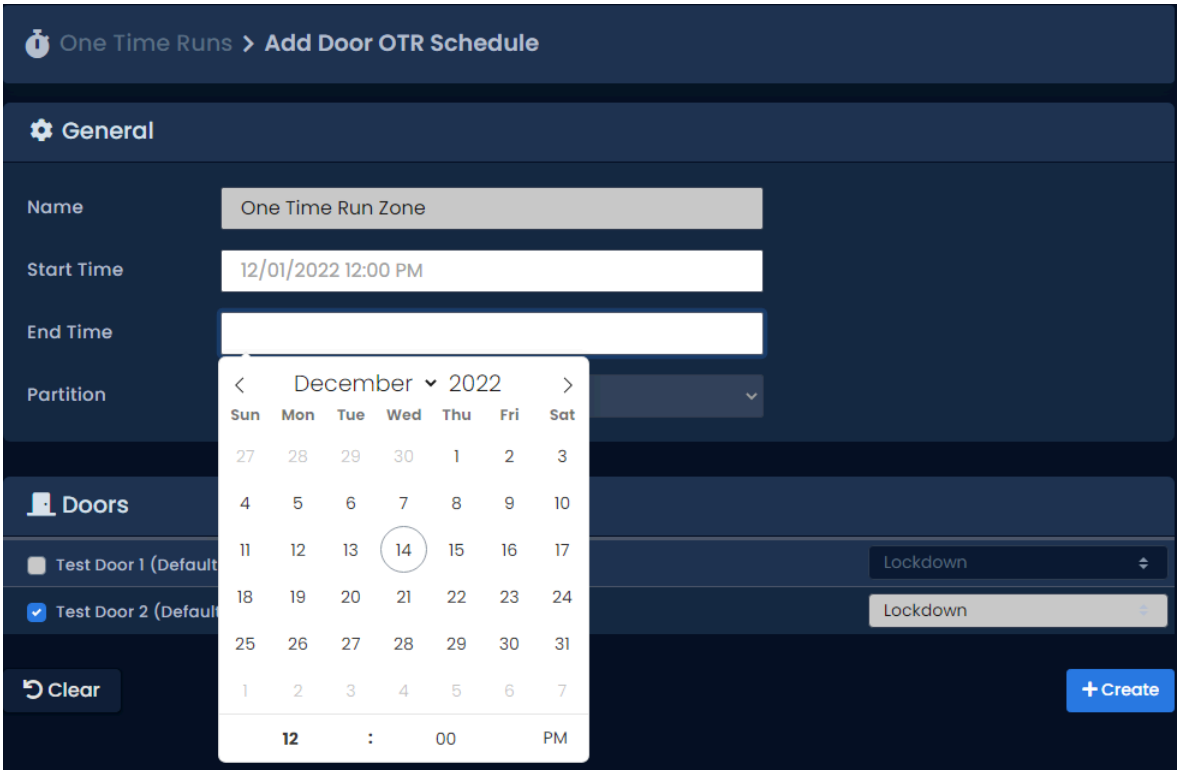
5. On the OTR screen, you'll see the previous OTRs that have been created click the **Add** button on this screen.
6. On the **Add OTR** screen, you'll have a couple text boxes to fill.

Table 14.1. Add a One Time Run Schedule

Text Box	Description
Name	Unique name for your one time run Schedule. Accepts 2 to 60 characters. We recommend naming your OTR based on the reason its being created, such as emergency maintenance, extended holidays, birthday party.
Start/Stop Time	The date and time the Schedule begins. Upon clicking the date picker widget will appear. Use the calendar and time picker to select the date & time to start/stop for the OTR.
Partition	Use the Partition drop-down menu to change which Doors can be selected for this OTR.
Affected Doors/Floors	Select the Doors/Floors you'd like this OTR to affect and use the drop-down menu on the right side to select which of the 8 Door states or 3 Floor states will be applied during this OTR.

7. Once you've selected the Name, Start Time, Stop Time, Partition, Doors/Floors and Door/Floor state, you can now click **Create** to create the OTR. If more than one Partition is selected, an OTR will be created for each one.

Figure 14.1. Date Picker Widget



Tip

You can configure an OTR to span multiple days. This can be useful for holidays lasting more then a day.

Chapter 15. Crisis Levels

This chapter will cover how Crisis Levels work in VAX, along with how to customize them and use them effectively.

Crisis Levels give Administrators the ability to change the behavior of Doors quickly during emergency situations with a variety of configurable severity levels. Up to 16 Crisis Levels can be configured; by default only 4 are active.

Making Changes to Crisis Levels

This section will cover how to make adjustments to the names and behavior of Crisis Levels.

To view and make changes to how each Crisis Level behaves, use the following steps:

1. Access your VAX system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **Administration**; click on the **Crisis Levels** icon (pictured below).

4. On the Crisis Levels screen, you'll see all 16 available levels.

Figure 15.1. Crisis Levels Screen

5. All items underlined with dots can be edited by clicking on them. You can customize the name of each Crisis Level, if the level is disabled, and what Door State a Crisis Level is associated with. Once you make a change, it will be saved automatically.

Configuring User Security Levels

When a Crisis Level is applied to a Door with an applied Door State of Card Only, Users will **NOT** be granted access upon presenting their Credential unless the **User Security Level** is equal to or greater than the Crisis Level being applied, the exception being if the User has the **Master** privilege activated.

User security levels can be changed on the **Edit User** Screen.

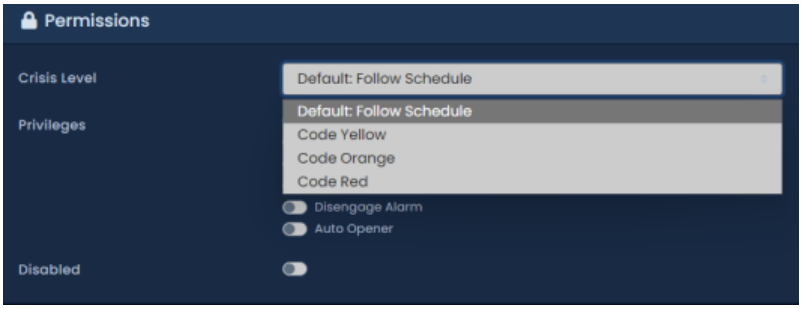
1. On the **Side Bar**, scroll down to the section titled **Users**; click on the **Users** icon.

2. On the Users screen, click the blue button (edit) next to the User you'd like to change.

3. On the **General** tab of the User, the Crisis Level drop-down menu represents that User's security level. By default a User Crisis Level is set to level 1, Default: Follow Schedule.

4. If you've changed the User Crisis Level, click **Save**. The Panels will need to be updated before the change will take effect.

Figure 15.2. Changing a User Crisis Level

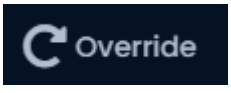


Applying Crisis Levels to Doors

This section will cover the two methods that can be used to apply Crisis Levels to Doors. The first method is through the VAX software; the second method is through the use of AUX Inputs on the Panels.

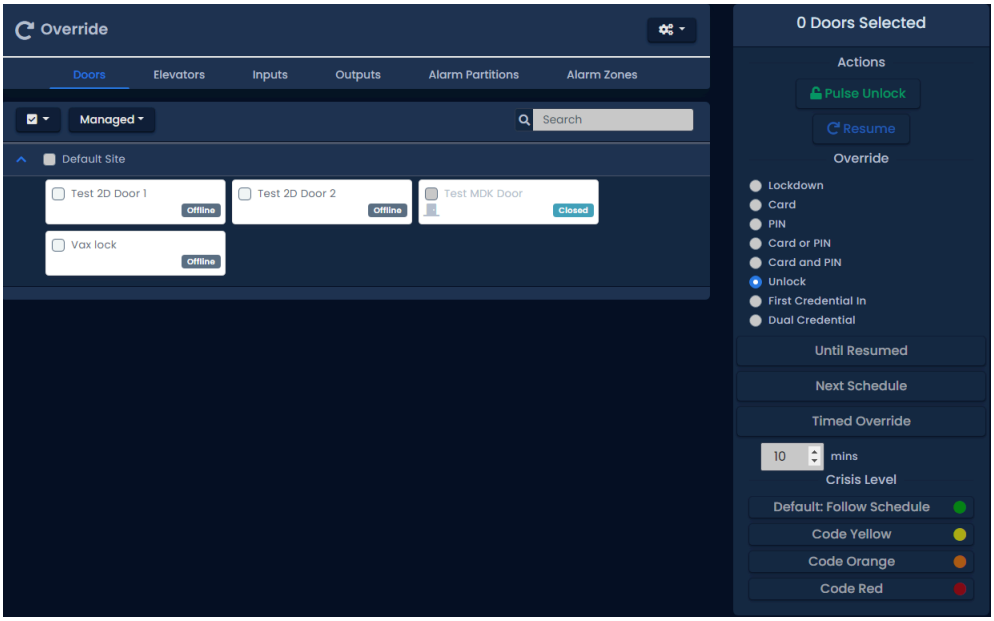
Applying Crisis Levels in VAX

Applying a Crisis Level in VAX can be done from any page in the VAX interface. The Crisis Levels menu is located on the top right corner (pictured below).



Click on the Crisis Levels icon to bring down the Crisis Levels menu. Here you will see all Sites in the system, and the Doors attached to each Site.

Figure 15.3. Crisis Levels Menu



Clicking the checkbox next to a Site will select all Doors in that Site. Alternatively, you can select individual Doors. Once you have selected the Doors, click on the Crisis Level on the right side that best matches how you want the Door to behave (based on how you've configured your Crisis Levels), keeping in mind that this may block access to Users if their security level is too low.

To Resume the Door from Crisis Mode, select the Doors and click the Crisis Level **Default: Follow Schedule**.

Applying Crisis Levels With an Aux Input

The second method of applying a Crisis Level to a Door is through an Aux Input. For more information on Input/Output configuration, please see the section called “Input/Output Configuration”.

Once an Aux Input is setup to start a Crisis Level, that Input can be triggered by a button or a dry contact from some other system, such as a fire alarm. When the Input is triggered, only the Panel with the Aux Input configured will be placed into Crisis Mode. Initiating a Crisis Level through an Aux Input does not change the state of the door, only the Crisis Level.

Warning

Once an Aux Input triggers a Crisis Mode, the way to resume to normal schedule is through the VAX software interface, or by having an additional Input with an Aux Input trigger that places the Door into Default: Follow Schedule.

Chapter 16. VAX Override Features

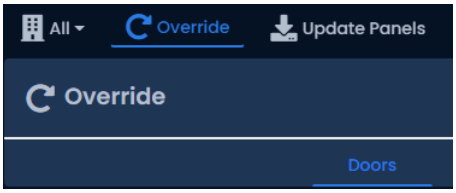
This chapter will cover the various Override features in VAX, including how to Override a Door, an Output or an Elevator Floor through the software in real time.

Warning

Overrides are the highest level of state a Door, Output or Floor will obey. Overrides supersede Holidays, OTRs, Crisis Levels and the Door Schedules (with the exception of Override until next schedule).

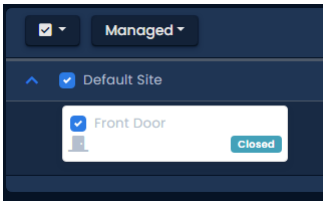
Override Doors

This section covers how to Override a Door in VAX using the **Override Doors** menu. Overriding a Door can be done from any page in the software by clicking on the Override button and then the Doors button on the top of the page (pictured below).



Click on the Override Doors icon to bring down the Override Doors menu. Here you will see all Sites in the system and the Doors attached to each Site. Only Doors that are online and connected to VAX will be shown; Doors that are offline will be grayed out.

Figure 16.1. Override Doors Menu



Clicking the checkbox next to a Site will select all Doors in that Site. Alternatively, you can select individual Doors. Once you have selected the Doors, the buttons on the right side can be used to manipulate the state of the Door instantaneously.

The Override Doors menu is divided into 3 sections, **Actions**, **Override** and **Crisis Level**.

General. The most common Override is the **Pulse Unlock** action, which will unlock a Door and then return to its normal schedule a moment later. The **Resume** action can be used on any type of Door Override to return the Door to its normal schedule. When a Door is resumed, you will see the Notification: **Door has resumed from an overridden state**.

Override Until Resume. The 4 momentary overrides can be used to change the state of the Door (lockdown, unlock, card, pin). Once the Door is overridden, it will remain in that state until the Door is resumed with the Resume button. In System Overview, you can see the Door state and if the Door is Overridden.

Override Until Next Schedule. The behaviour of these Overrides differ slightly from Override Until Resume. These Overrides will change the Door state, and the Door will remain overridden until the Door is scheduled to change state, at which point the Door will resume its normal schedule. Resuming the Door with the resume button will also change the Door state to its normal schedule.

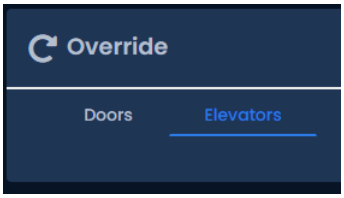
Example: A company has a public Door that is unlocked 9-5, and card only after hours. It's a slow day and the manager decides to close up early. He browses to VAX using his smart phone and initiates an Override until next schedule, with a Door state of Card Only. The Door will stay in this state until 5 PM that evening, when it would resume its normal schedule.

Note

Door Overrides can also be performed by configuring Triple Swipe Actions. This can be useful for a variety of situations, such as locking up early. For more information on triple swipe options, please see Chapter 17, *Triple Swipe Features*.

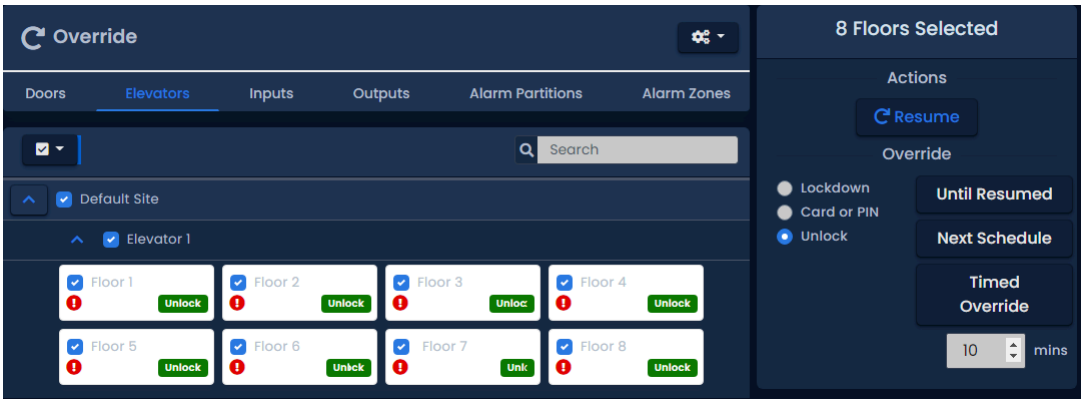
Override Floors

This section covers how to Override an Elevator Floors in VAX using the **Override Elevator** menu. Overriding a Floor can be done from any page in the software by clicking on the Override Floors button on the top right of the page (pictured below).



Click on the Override icon to bring down the Override menu. Click Elevators icon to bring down the Floor Override menu. Here you will see all Sites in the system and the Elevators and Floors attached to each Site. Click an elevator drop down icon to show Floors. Only Floors that are online and connected to VAX will be shown; Floors that are offline will be grayed out.

Figure 16.2. Override Floors Menu

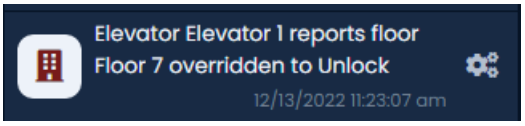


Clicking the checkbox next to a Site will select all Floors in that Site. Clicking on an Elevator will select all Floors attached to that Elevator. Alternatively, you can select individual Floors. Once you have selected the Floors, the buttons on the right side can be used to manipulate the state of the Floor instantaneously.

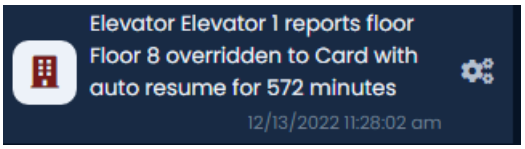
The Override Floors menu is divided into 3 sections, **General**, **Override until resume** and **Override until next schedule**.

General. The **Resume** action can be used on any type of Floor Override to return the Floor to its normal schedule. When a Floor is resumed, you will see the Notification: **Floor Override Disabled**.

Override Until Resume. These Overrides can be used to change the state of the Floor (lockdown, unlock, card). Once the Floor is Overridden, it will remain in that state until the Floor is Resumed with the Resume button. In System Overview, you can see the Floor state and if the Floor is Overridden.



Override Until Next Schedule. The behaviour of these Overrides differ slightly from Override Until Resume. These Overrides will change the Floor state, and the Floor will remain overridden until the Floor is scheduled to change state, at which point the Floor will resume its normal schedule. Resuming the Floor with the Resume button will also change the Floor state to its normal schedule.

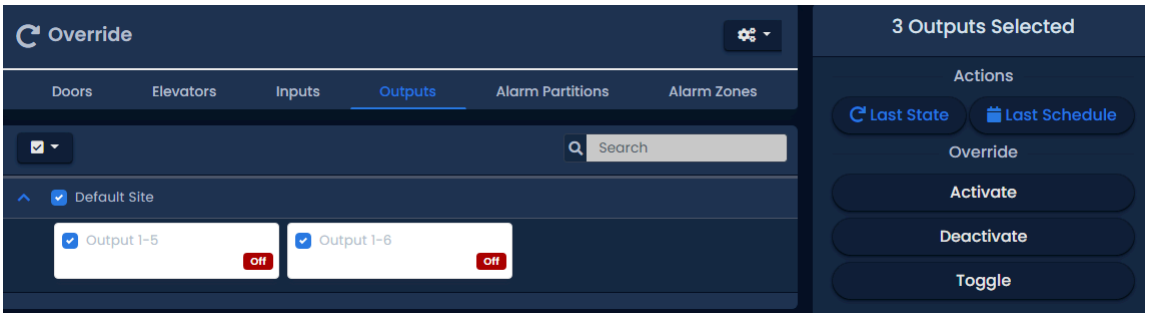


Override Outputs

This section covers how to Override Outputs in VAX. The process is very similar to Overriding Doors. Overriding an Output can be done from any page in the software by clicking on the Override Outputs button on the top right of the page (pictured below).

Click on the Override Outputs icon to bring down the Override Outputs Menu. Here you will see all Sites in the system and available Outputs attached to each Site; Outputs connected to Panels that are offline will be grayed out.

Figure 16.3. Override Outputs Menu



Clicking the checkbox next to a Site will select all Doors in that Site. Alternatively, you can select individual Outputs. Once you have selected the Output, the buttons on the right side can be used to manipulate the state of the Output instantaneously.

Activate. Changes the Output to an active state, also known as a closed state.

Deactivate. Changes the Output to an inactive state, also known as an open state.

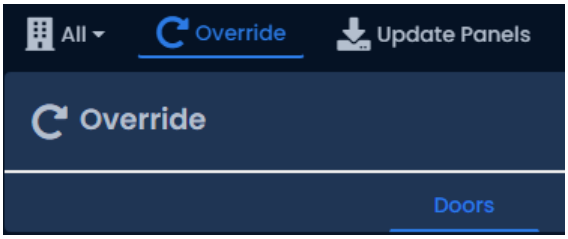
Resume. Resumes the Output to its natural state (defined in Panel I/O configuration as normally closed or normally open).

Note

Output Overrides can also be performed by configuring Triple Swipe Actions. This can be useful for a variety of situations, such as locking up early. For more information on triple swipe options, please see Chapter 17, *Triple Swipe Features*

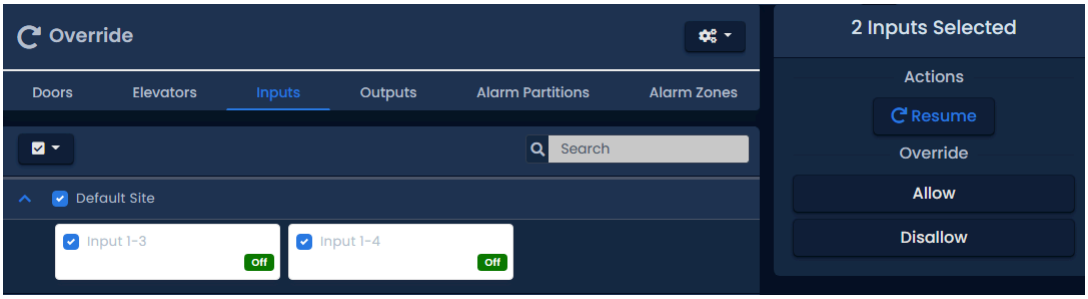
Override Inputs

This section covers how to Override Inputs in VAX. The process is very similar to Overriding Outputs. Overriding an input can be done from any page in the software by clicking on the Override button on the top of the page (pictured below).



Click on the Override Outputs icon to bring down the Override Inputs Menu. Here you will see all Sites in the system and available Inputs attached to each Site; Inputs connected to Panels that are offline will be grayed out.

Figure 16.4. Override Inputs Menu



Clicking the checkbox next to a Site will select all Doors in that Site. Alternatively, you can select individual Inputs. Once you have selected the Input, the buttons on the right side can be used to manipulate the state of the Input instantaneously.

Resume. Resumes the Input to its natural state. It would resume its normal schedule..

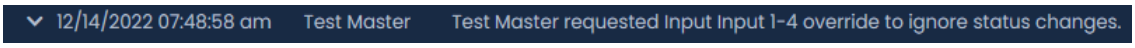
Note

Input Overrides can also be performed by configuring Triple Swipe Actions. This can be useful for a variety of situations, such as triggering an ACE action plan. For more information on triple swipe options, please see Chapter 17, *Triple Swipe Features*

Figure 16.5. Override Inputs Menu

Disallow. Disallow override requests the Input to ignore all attempts to change the input while in Disallow Override. If Resumed the Input would return to its natural state.

Figure 16.6. Override Inputs Menu



Allow. Allow override requests the Input to monitor and allow all attempts to change the Input while in Allow Override. The Input would resume its natural schedule if Resumed from this state.

Figure 16.7. Override Inputs Menu

Override Alarm Partitions

The Alarm Override sections of the Override menu allows for Alarm overrides of sites and alarms. For more information on these sections please refer to Chapter 38, *DSC IP Alarm integration*.

Chapter 17. Triple Swipe Features

Triple Swipe is a feature in VAX which allows a Credential to be presented to a Reader 3 times in concession to perform pre-defined actions. These actions include overriding the state of the Door, triggering Outputs on the Panel and activating Alarm Interfaces. This chapter will cover the available options and common examples of how they are used in the field. Outputs that are triggered by Triple Swipe actions can also be wired into an Aux Input on the Panel for additional actions.

User Requirements to Use Triple Swipe

In order for a user to perform a Triple Swipe action, the Triple Swipe user attribute must be selected when adding or editing the user. The Supervisor user attribute is required when using Triple Swipe with high security Door Schedules Dual Credential and Card and PIN. PIN credentials can activate Triple Swipe actions by pressing '#' on the keypad 3 times after entering the PIN. For more information on user attributes, see the section called “User Privileges ”.

List of Triple Swipe Options

This list contains the currently configurable Triple Swipe Actions. 12VDC powered panel models have a different set of triple swipe options; they are displayed in the following section. Only users/cards with the triple swipe user attribute will be able to perform a triple swipe. For more information on user attributes, please see Chapter 12, *User/Cardholder Configuration*.

Table 17.1. Triple Swipe Features

Triple Swipe Actions	Brief Explanation
Activate Aux Output	Activates the selected Output.
Deactivate Aux Output	Deactivates the selected Output.
Toggle Aux Output	Toggles the selected Output (if the Output is activated, this action will deactivate the Output).
Pulse Aux Output	Activates the selected Output for about a second before deactivating it again.
Activate Alarm Interface	Activates the Output that has an assigned function of Alarm Interface for about a second before deactivating it again.
Deactivate Alarm Interface	Deactivates the Output that has an assigned function of Alarm Interface (if the interface is currently active).
Toggle Alarm Interface	Activates the Output that has an assigned function of Alarm Interface for about a second before deactivating it again.
Disengage Emergency Alarm	If a Panel has an Input set as an Emergency Alarm, if the alarm is engaged, this Triple Swipe Action will reset the Panel to its normal state.
Override <Door Mode>	This Triple Swipe Action will override the state of the Door depending on the selection you configure in the software. These Door Overrides must be resumed from the software or with the Triple Swipe Action "Cancel Override". Modes include: Lockdown, Card, Pin, Card or Pin, Card and Pin, Unlock, First Card In.
Override <Door Mode> With Auto-Resume	This Triple Swipe Action will override the state of the Door depending on the selection you configure in the software. These Door Overrides instruct the Door to Resume normal schedule when the Door Schedule assigned to this Door is scheduled to change. Can also be resumed from the software or with the Triple Swipe Action

Triple Swipe Actions	Brief Explanation
	"Cancel Override". Modes include: Lockdown, Card, Pin, Card or Pin, Card and Pin, Unlock, First Card In.
Override Toggle <Door Mode>	This Triple Swipe Action will override the state of the Door depending on the selection you configure in the software. These Door Overrides must be resumed from the software, with the Triple Swipe Action "Cancel Override" or by performing a second Triple Swipe which will "toggle" the state back to normal. Modes include: Lockdown, Card, Pin, Card or Pin, Card and Pin, Unlock, First Card In.
Cancel Override	Resumes any Doors from an overridden state.
Cancel Output Override	Resumes any Outputs from an overridden state.

Note

If you are using a keypad, you can configure up to 7 Triple Swipe Actions based on a key press after a Triple Swipe. You must press # 3 times after you have presented your credentials followed by the number corresponding to the action you wish to execute. You must press # one last time to execute the action.

Table 17.2. VAX-MDK Panel Triple Swipe Features

Triple Swipe Actions	Brief Explanation
No Action	Actions are optional; an event will still be generated when input conditions are met and server side script triggers can still execute.
Output Activate	Activates an output, selectable via drop down list.
Output Deactivate	Deactivates an output, selectable via drop down list.
Output Toggle	Toggle an output to the opposite state, selectable via drop down list.
Output Deactivate	Deactivate the selected Output, selectable via drop down list.
Output Pulse High	Pulse an Output to close, configure a delay and the duration of the pulse.
Output Pulse Low	Pulse an Output to open, configure a delay and the duration of the pulse.
Output Pulse Opposite	Pulse an Output to the opposite of its current state, configure a delay and the duration of the pulse.
Output Activate Multiple	Activate multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Output Deactivate Multiple	Deactivate multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Output Toggle Multiple	Toggle multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Input Disable	Disable a selected input. Selectable from a drop-down list with delay and duration.
Override < Door Mode>	This Triple Swipe Action will override the state of the Door depending on the selection you configure in the software. These Door Overrides must be resumed from the software or with the Triple Swipe Action "Cancel Override". Modes include: Lockdown, Card, Pin, Card or Pin, Card and Pin, Unlock, First Card In. Door and mode selectable from drop-down list
Override < Door Mode> With Auto-Resume	This Triple Swipe Action will override the state of the Door depending on the selection you configure in the software. These Door

Triple Swipe Actions	Brief Explanation
	Overrides instruct the Door to Resume normal schedule when the Door Schedule assigned to this Door is scheduled to change. Can also be resumed from the software or with the Triple Swipe Action "Cancel Override". Modes include: Lockdown, Card, Pin, Card or Pin, Card and Pin, Unlock, First Card In. Door and mode selectable from drop-down list
Override Toggle < Door Mode>	This Triple Swipe Action will toggle override the state of the Door depending on the selection you configure in the software. This option allows a triple swipe to toggle the door into and out of an overridden state. Modes include: Lockdown, Card, Pin, Card or Pin, Card and Pin, Unlock, First Credential In, Dual Credential. Door and mode selectable from drop-down list
Door Resume Override	Resumes a Door from an overridden state. Selectable via drop-down list.
Door Set Crisis Level	Initiate crisis level on a door. Selectable via drop-down list for door and mode.
Door Reset Crisis Level	Set the crisis level back to default on the selected door. Selectable via drop-down list.
Door Disable Held Open Buzzer	Temporarily disable a held open alarm/buzzer on the selected door. Selectable via drop-down list for door and duration (1-600 seconds).
Emergency Alarm Disengage	Deactivates the emergency alarm function which will resume any override caused by the emergency alarm function.
Emergency Alarm (Silent) - Unlock Doors	Activates the emergency alarm function. Readers will not beep (silent). Will not exclude doors with the "Unlock on Emergency Alarm" option disabled. Affected doors selectable via list.
Emergency Alarm (Silent) - Unlock Unprotected Doors	Activates the emergency alarm function. Panel will not beep (silent). Will exclude doors with the "Unlock on Emergency Alarm" option disabled. Affected doors selectable via list.
Emergency Alarm - Sound	Activates the emergency alarm function. Panel will beep until the Emergency Alarm Disengage function is activated . Will not affect door state.
Emergency Alarm - Unlock Doors	Activates the emergency alarm function. Panel will beep until the Emergency Alarm Disengage function is activated. Will not exclude doors with the "Unlock on Emergency Alarm" option disabled. Affected doors selectable via list.
Emergency Alarm - Unlock Unprotected Doors	Activates the emergency alarm function. Panel will not beep (silent). Will exclude doors with the "Unlock on Emergency Alarm" option disabled. Affected doors selectable via list.
Buzzer	Provides several options to deactivate reader buzzers or outputs configured as external buzzers. Buzzer will reactivate if another event activates the buzzer such as a door forced open.
Alarm Interface Activate	Used to activate an output that is assigned as an alarm interface. In most cases this can be used to arm an alarm system.
Alarm Interface Deactivate	Used to deactivate an output that is assigned as an alarm interface. In most cases this can be used to disarm an alarm system.

Configuring Triple Swipe

As explained previously in this guide, Triple Swipe Actions are configured on the Reader tab of the Edit Door Screen.

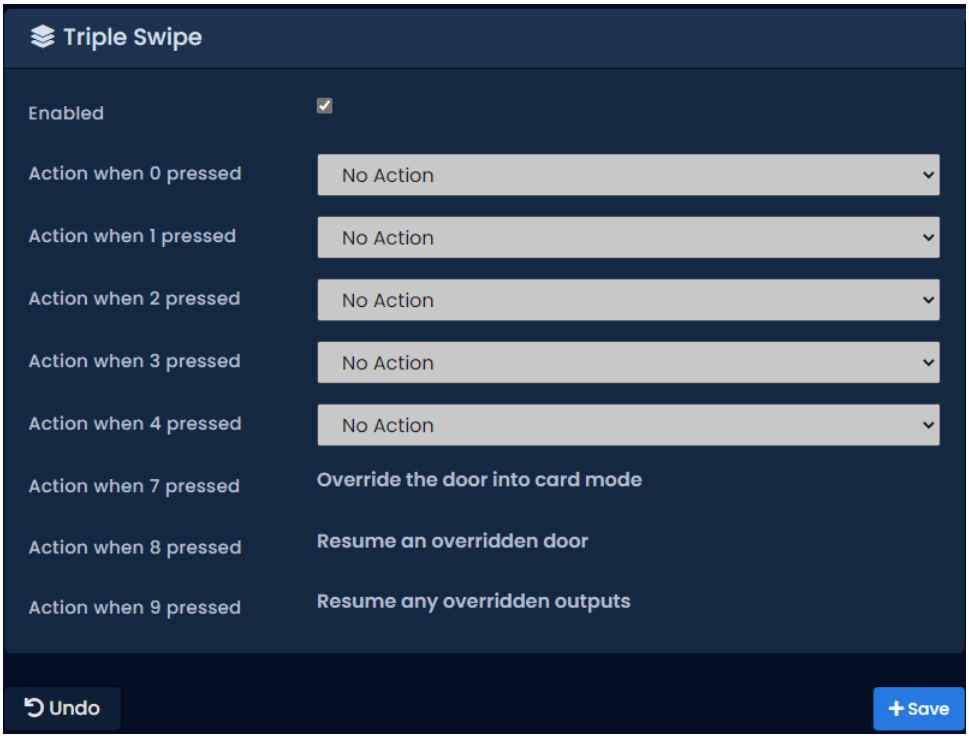
To get to this screen:

1. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Doors** icon (pictured below).

2. On the **Doors** screen, your configured Doors will be listed. Click the blue button next to the Door you'd like to configure.

3. On the **Edit Door** screen, you'll see 4 tabs. Click on the **Reader** tab, scroll down to the bottom of the Reader tab and you'll see the options for Triple Swipe Actions.

Figure 17.1. Reader Tab: Triple Swipe with Keypad Options



Triple Swipe Examples

This section contains real world examples of how Triple Swipe can be used by our dealers/end users.

Arm/Disarm Alarm System. Many Users of our product use our system to Arm/Disarm their alarm systems. It's as easy as triple swiping a card on the way out of the office to arm the system, and doing the same on the way in the next day to disarm. For more information about interfacing with alarm systems, please see the relevant section within the master tech guide.

Close a Public Door Early. Some installations have Public Doors, Doors that are unlocked during a period of the day (9 am to 5 pm). If the Door needs to be closed early, you can Override it to Card Only Until Next schedule. The Door will now be Card Only until the next day when it will resume its normal unlock schedule.

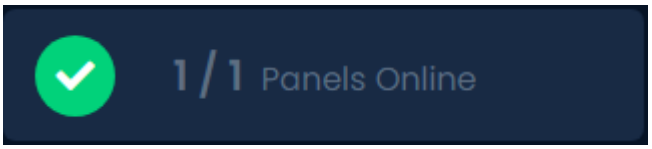
We can also accomplish the above via a Triple Swipe Action. Below are instructions for locking the Door early, but also to tell the Door to **Resume** normal schedule the next day when it's scheduled to unlock.

1. Go to “Home/Hardware/Door Panels”.
2. Choose the Door you want to be able to lock early and click on the blue button (edit).
3. Click on either the **Reader 1** or **Reader 2** tab depending upon which Reader you require this function.
4. Enable Triple Swipe by checking the check box.
5. From the **Triple Swipe action** drop-down menu; choose **Override Auto-Resume Card** then click **Save Reader** at the bottom right.
6. Go to the “Home/Users”.
7. On the General tab, go down the list checking the **Triple Swipe** option for the Users you would like to have this capability and click Save to the right of that User.
8. Update Panels.

Chapter 18. System Overview

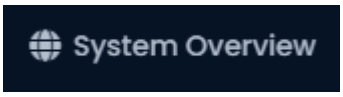
This chapter will cover the System Overview screen in VAX and how it can be used to simplify actions, including updating Panels individually, placing Panels into Firmware Update Mode,viewing all Doors and Outputs in the system and viewing the status of Elevators and Floors.

The System Overview page can be accessed from any page in our software. You can simply click on the Panels Online icon above the Notification bar on the right side where your Panel status is displayed.



Alternatively, you can navigate to System Manager using the following steps:

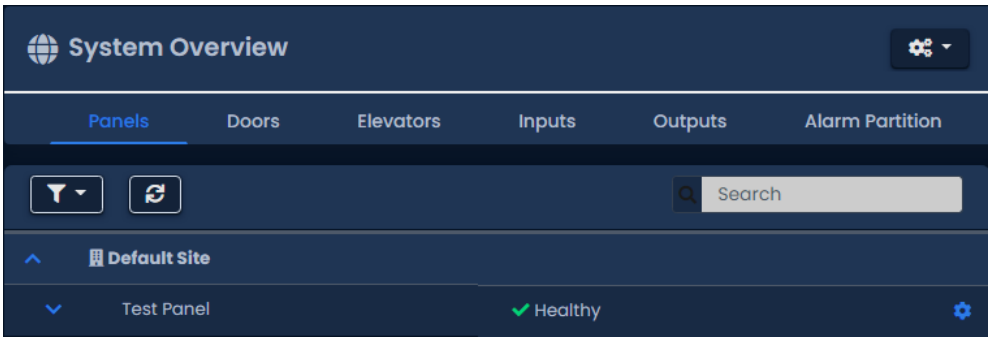
1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll to the top section titled under **Home**; click on the **System Overview** icon (pictured below).



Once on the **System Overview** screen, you'll see all the Partitions and Sites created in your system and each of the Panels connected to them, along:

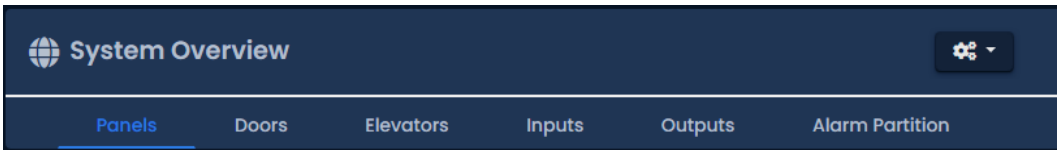
- If the Panel is Online or Offline.
- If the Panel requires a Firmware Update.

Figure 18.1. System Overview Screen: Default View



You can use the  button to expand each Panel to reveal the Doors/Floors associated with your Panels. This will show if the Door/Floor is in an overridden state or following schedule, or if the Door is open or closed (if a Door contact is available). The Doors are color coded to show which of the 8 Door states the Door is currently in.

You can change your view in System Overview with the menu across the top. Select **Doors** to only view Doors in your system. Select Inputs to only view **Inputs** on your system. Select **Outputs** to view only Outputs in your system. Select **Elevators** to view Elevators and Floors in your system.



To the right of each object in System Overview is a gear shaped icon. If you click on this icon, a drop-down menu with several options will appear. Depending on the type of object, the menu will have different options available. The following chart explains each of these objects and options.

Table 18.1. System Overview Menu Items

Menu Item	Description
	Panel Object Menu Items
Update Panel	Performs a Panel update to that individual Panel. Useful for testing and troubleshooting.
Edit Panel	Opens the Edit Panel screen for the selected Panel.
Firmware Update Mode	Places the Panel into firmware update mode.
View Status	Displays the connection status of the Panel in a new window.
Report Time	The Panel will report what it believes is the current time. A Notification will appear with the result.
Reset Users Anti-passback Locations	The Panel will change the current location of any credentials to 'No area'.
Disconnect (for one minute)	The Panel will disconnect from the server and wait 1 minute before trying to reconnect.
	Door Object Menu Items
Pulse Door	Pulses the Door unlocked; works the same as the Pulse Unlock action in the Door Overrides menu.
Resume	Resumes the Door from an overridden state; works the same as the Resume action in the Door Overrides menu.
Edit Door	Navigates to the door edit page.
	Output Object Menu Items
Edit Panel	Navigate to the panel edit page.
	Elevator Object Menu Items
Resume Floor	Resumes the Floor from an overridden state; works the same as the Resume action in the Floor Overrides menu.

Chapter 19. Partition and Site Configuration

This chapter will cover the software aspects of setting up Partitioning and Sites in VAX. If you're not entirely sure what a Partition is, please visit the section called “Partitions” prior to reading this chapter.

The majority of complexity with Partitions is the result of how certain objects are shared across multiple Partitions, where as others are per Partition. The following chart might help give you an idea how these objects interact with Partitions.

Table 19.1. How Objects Interact With Partitions

Object Type	Partition
Schedules (Door, User, Holiday, etc)	Per Partition
One Time Run Schedules	Per Partition
Holidays	Per Partition
Sites	Per Partition
Access Privilege Groups	Per Partition
Door Panels	Single Partition by Site
Doors	Single Partition by Site
Elevators	Single Partition by Site
Floors	Single Partition by Elevator
Readers	Single Partition by Site
Users	Multiple Partitions
Administrators	Multiple Partitions
Crisis Levels	Multiple Partitions
Custom Fields	Multiple Partitions

Adding Partitions

Although the concepts behind VAX Partitions are complex, the configuration is relatively simple and straightforward.

1. Access your VAX system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **System**; click on the **Partitions** icon (pictured below).

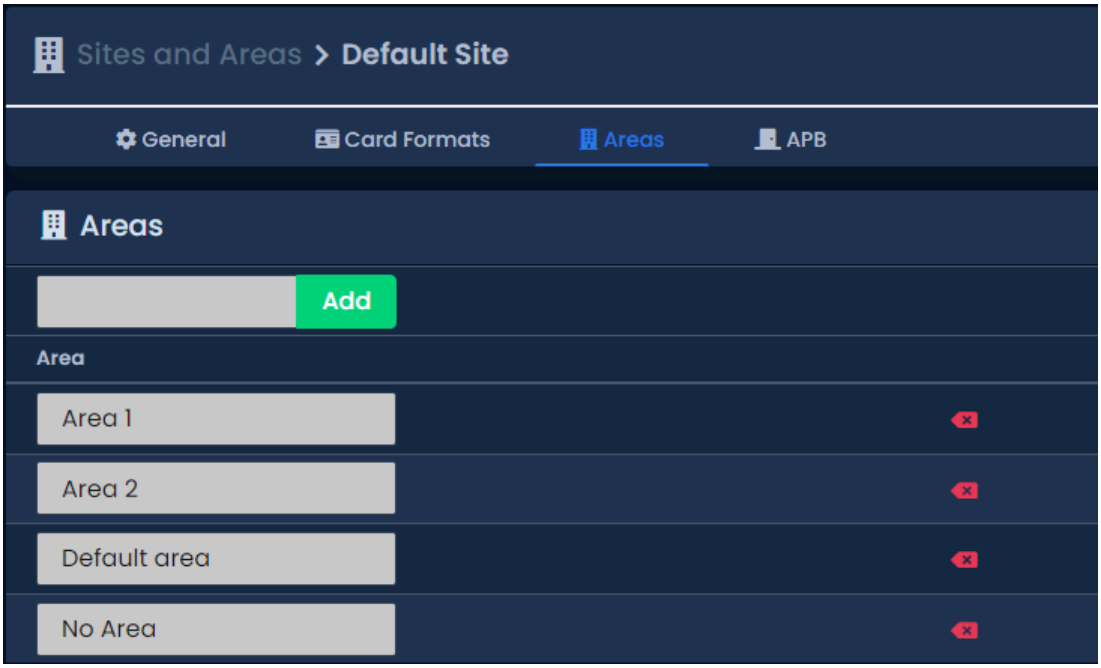
4. On the Partitions screen, you'll see 'Default Partition' that is created by default. In most cases a single Partition meets the needs of the system; however, if during your planning stage you (the installer or End User) decide that utilizing Partitions would benefit your deployment, click the **Add** button on this screen.

5. On the **Add Partition** screen, you'll have two text boxes to fill.

Table 19.2. Add a Partition

Text Box	Description
Name	Unique name of your Partition. Accepts 4 to 255 characters.
Description	Optional description of the Partition. Accepts 4 to 255 characters.

Figure 19.1. Add Partition Screen



6. Once you've filled the name and description of your Partition, click the **Save** button to create the Partition. The next step is to create Sites associated with those Partitions.

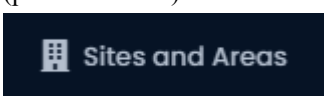
Adding Sites and Areas

Adding Sites in VAX is similar to adding Partitions, as they go hand in hand with each other. If you're not entirely sure what a "Site" is please see the section called "Sites".

1. Access your VAX system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **System**; click on the **Sites and Areas** icon (pictured below).



4. On the **Sites and Areas** screen, you'll see the default Site named **Default Site**, as with Partitions; small deployments generally only use one Site.

5. If your deployment requires more than one Site, or will be using multiple Partitions, you'll need to add more Sites. Click the **Add** button on this page. On the **Add Site** screen, you'll have several fields to fill.

Table 19.3. Add a Site

Text Box/Option	Description
Name	Unique name of your Site. Accepts 4 to 255 characters.
Description	Optional description of the Site. Accepts 4 to 255 characters.
Time Zone	The local time zone that Site resides in.
Partition	Select the Partition you wish that Site to reside in.

6. Once you've filled the required fields, click the **Save** button to create the Site.
7. After you've added your Sites and Areas you'll likely want to add your **Panels**; please see the section called "Adding a Panel to VAX Access Control".
8. When editing a Site, you'll have several options not available when adding a Site. The following section will cover those additional options.

Edit Sites and Areas: Areas

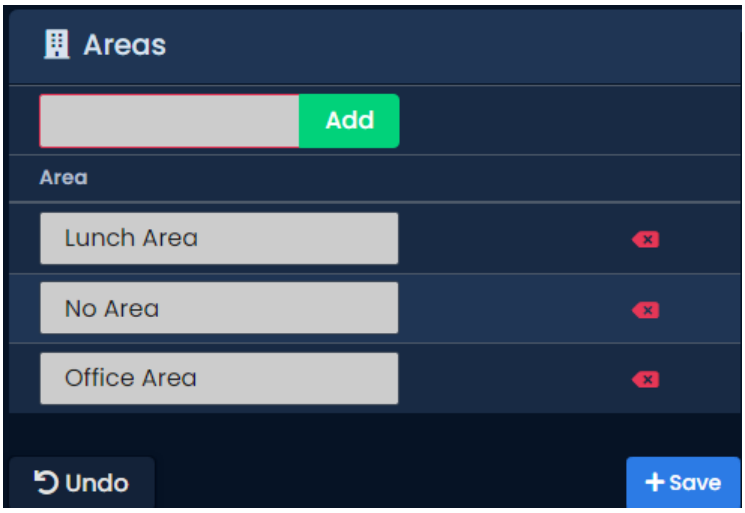
Areas are created and assigned to Doors so the system can know which readers grant access to which areas. Primarily used for Anti-passback and User location tracking (Muster Report). To add additional areas:

1. On the Edit Site screen, click on the **Areas** tab.
2. On the **Areas** tab, enter a name for your new area and click the **Add Area** button on the right side.

> **Note**
>
> The default area 'No Area' cannot be deleted.

You have now successfully added an Area to VAX.

Figure 19.2. Adding an Area



For more information on Anti-passback, please see Chapter 21, *Areas and Anti-Passback*.

Edit Sites and Areas: Card Formats

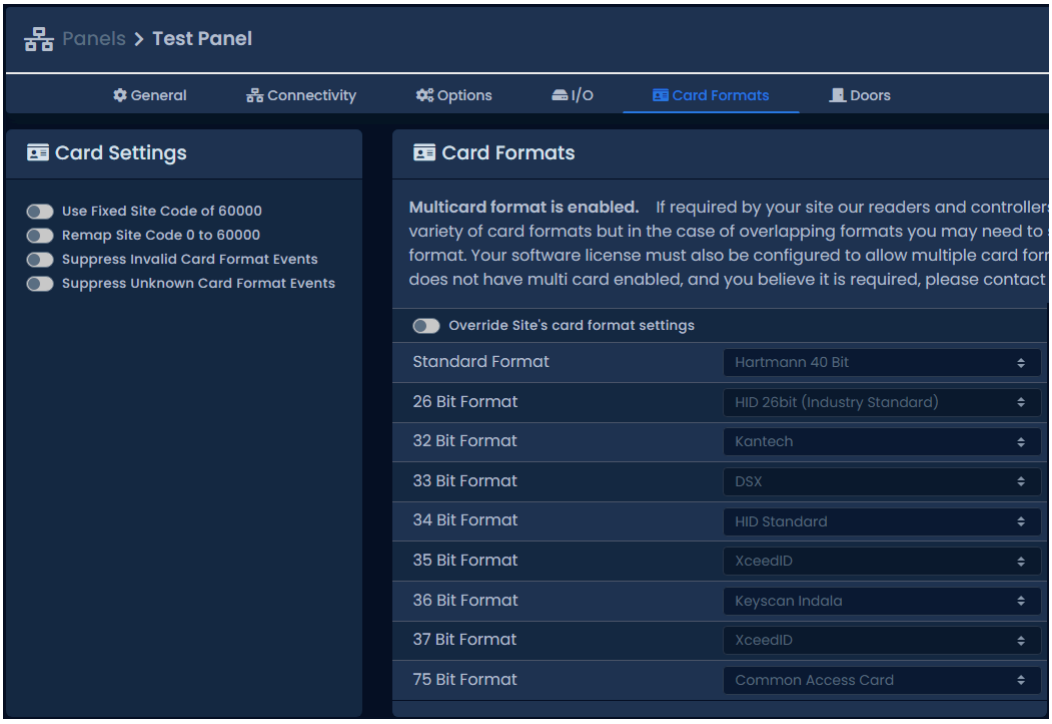
VAX supports a variety of card formats. The use of third party card formats (any format other than Vicon 40 bit) requires that the Multicard feature be enabled by your VAX license. If you are in a trial

period, Multicard will be enabled by default. If your license does not have Multicard enabled, and you believe it is required, please see Chapter 4, *Software Licensing*.

Card formats are configured at the Site level, it can also be overridden on a per Panel basis. In the case of overlapping formats you may need to specify your preferred format.

1. On the Edit Site screen, click on the **Card Formats** tab.
2. On the **Card Formats** tab, you can review the current formats. Specify your preferred format where required.
3. Click the **Save** button on the bottom right once you've made any changes.

Figure 19.3. Card Formats



Chapter 20. Administrators and Privileges

VAX This chapter will cover how to add creating and managing **Administrator Accounts**, explain how Security Groups and privileges work and the advanced authentication options available. Administrator accounts are especially useful with multiple Partitions; for more information about Partitions, please see the section called “Concepts” and Chapter 19, *Partition and Site Configuration*.

Administrators

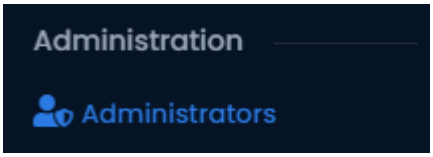
Administrators manage and monitor all aspects of the access control system from either the web interface, or using the mobile app. Administrators can have varying privileges to one or all Partitions, allowing limited access to be granted. This section will cover how to create an Administrator account, how Administrators can manage their own settings, and how System Administrators can manage other Administrators and generate API keys.

Adding an Administrator Account

1. Access your VAX Access Control system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. In the left navigation menu, click on **Administrators** under the Administration section near the middle of the navigation menu.



4. On the **Administrators Screen**, you'll see the initial Administrator account that was created during the initial setup. Click the **Add** button on this screen.

5. Under the **Administrator** section, select which **Type** of authentication they will use. Depending on authentication configuration you will have the following options:

   - **Local** The credentials for the administrator are managed locally within the system.

   - **LDAP** The email, and name for the administrator are synchronized and credentials authenticated from the configured LDAP server. This option will only appear if LDAP is configured.

   - **Service Account** The administrator only accesses the system using an API key and does not have credentials.

   - **OAuth** The email, and name for the administrator are synchronized and credentials authenticated from one of the configured OAuth providers such as Google or Microsoft.

     ### Note

     The OAuth must be added under System Settings for this option to appear. See the section called “OAuth Authentication”

6. Depending on the Type selected, fill in the shown fields in the **Administrator** section.

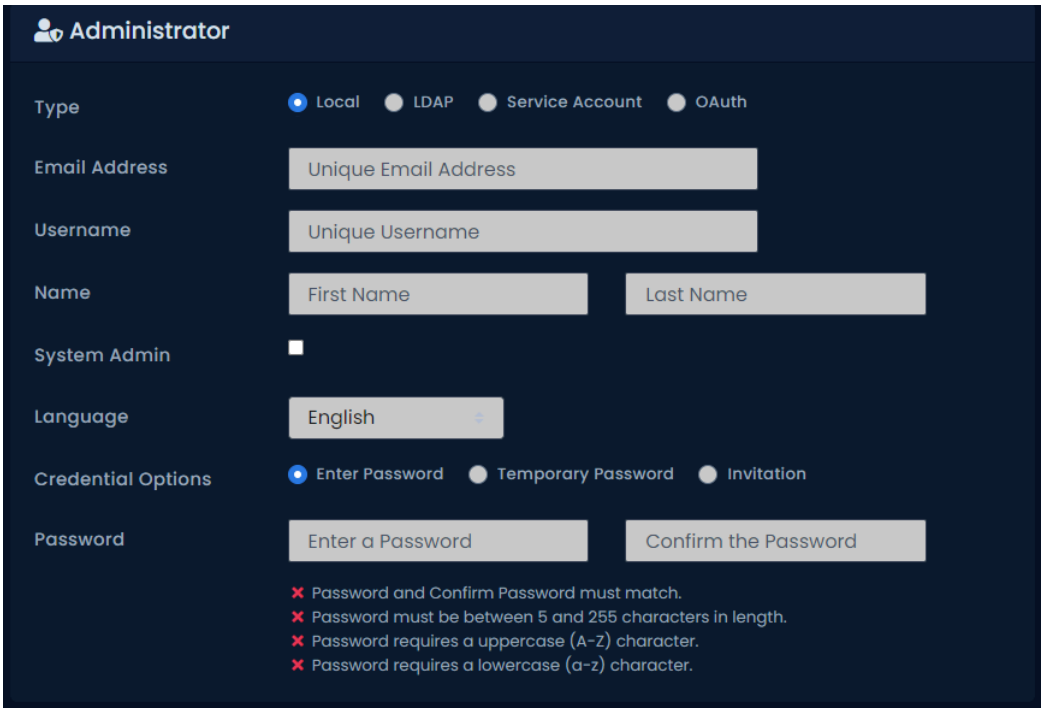


Table 20.1. Add an Administrator: Options

Text Box/Drop-down Menu/ Checkbox	Description
Type	The method of authentication to authorize the Administrator. Options are: **Local**, **Service Account**, **OAuth** and **LDAP** (if LDAP is configured; see Chapter 32, *Active Directory Integration*).
Email Address	Unique email address of the Administrator. By default it is the same as the username, but the username may be unique.
Username	Unique Username of the Administrator. Accepts 5 to 255 characters.
First Name	Administrators first name. Accepts 2 to 64 characters.
Last Name	Administrators last name. Accepts 2 to 64 characters.
System Admin	Enables System Admin, giving the administrator full access to all features. Actions requiring System Admin are covered in the privileges section.
Language	Language shown in the UI for the Administrator.
Credential Options	For Local Administrators, select how their credentials will be created. **Enter Password** - Specify the password for the administrator now. **Temporary Password** - Specify a password that must be changed on login. **Invitation** - If configured, sends an email invitation to the Administrator to have them specify a password.
Password	Administrators password. Accepts 6 to 16 characters.
Confirm Password	Administrators password. Accepts 6 to 16 characters.

Note

Administrators with the **System Admin** checked are not bound by Partition permissions; they have unlimited access to all aspects of the system.

7. The second part of adding an Administrator is assigning **Partition Access and Privileges**. Privileges dictate what an Administrator may do within the system. An Administrator may have privileges across multiple Partitions, however some actions are limited to only **System Admins**, and will not be accessible to normal Administrators regardless of Partition privileges. See the the section called “Privilege Assignment” section for more information on assigning privileges.

8. Alternative or additionally, you may assign the Administrator to one or more Security Groups. Security Groups are a way of assigning privileges to a group of Administrators.

9. After selecting the permissions, you can now click **Save** to add the Administrator. You can now login to the account you've created and verify that the permissions are as expected. If making changes to an Administrator account that is logged in, the Administrator may need to log out and log in for the changes to take affect.

Administrator Settings

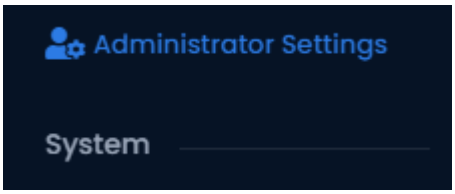
This section will cover the various things an Administrator can do in the **Administrator Settings** page that is available to all Administrators.

Updating Administrator Settings

1. Access your VAX Access Control system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. In the left navigation menu, click on **Administrator Settings** near the end of the Administration section.



Alternatively, you may click on the dropdown at the top-right of the page where it shows the Administrator's first name and click **Settings.**

4. Under the **Administrator** section, you may update the following settings.

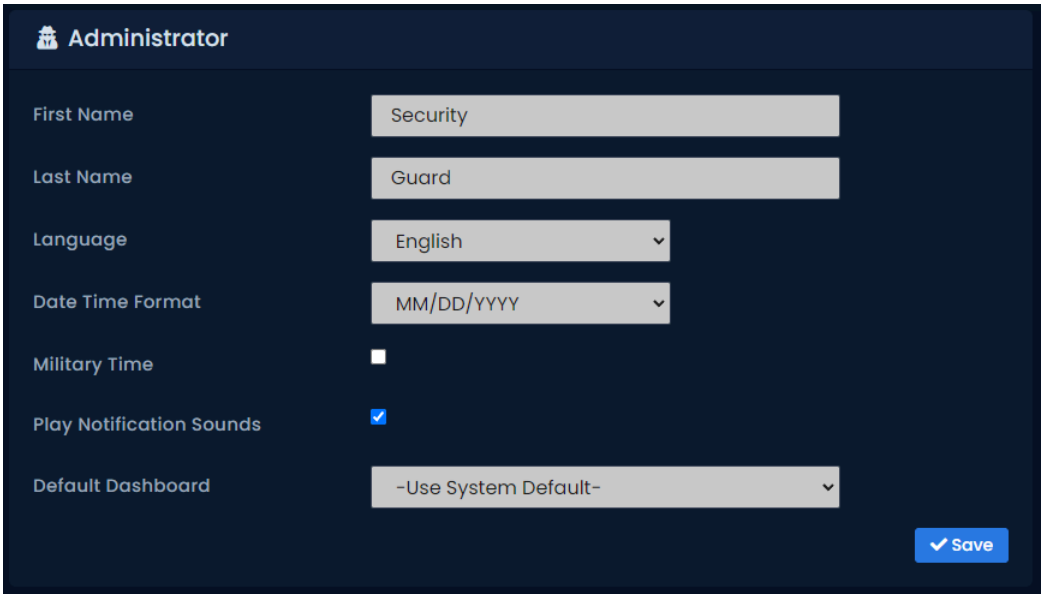


Table 20.2. Administrator Settings

Text Box/Drop-down Menu/ Checkbox	Description
First Name	Administrators first name. Accepts 2 to 64 characters.
Last Name	Administrators last name. Accepts 2 to 64 characters.
Language	Language shown in the UI for the Administrator.
Date Time Format	The format used to display the date within the UI.
Military Time	Whether to display the time in 12 AM/PM or 24 hour military time.
Play Notification Sounds	Set whether to allow VAX to play notification sounds when certain notifications are received.
Default Dashboard	The default dashboard to display when logging into VAX.

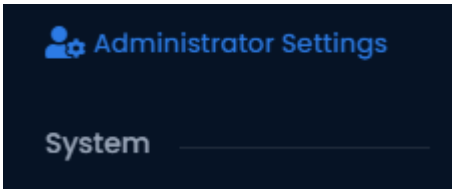
5. Click **Save** to save any changes you've made.

Change Password

1. a. Access your VAX Access Control system through your HTML5 browser of choice.

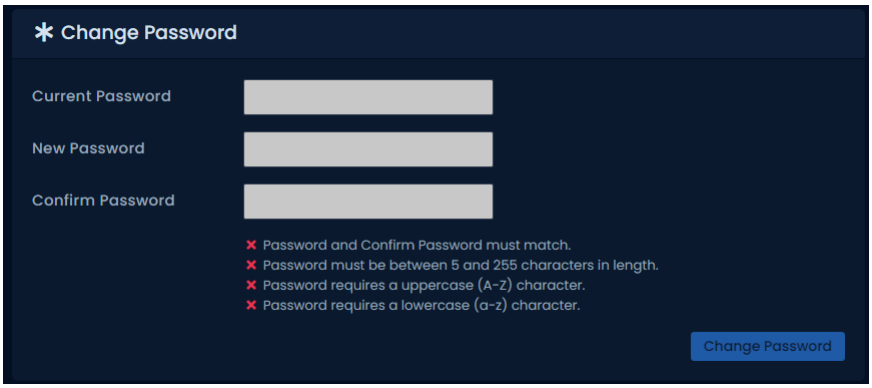
   b. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

   c. In the left navigation menu, click on **Administrator Settings** near the end of the Administration section.



   Alternatively, you may click on the dropdown at the top-right of the page where it shows the Administrator's first name and click **Settings.**

   d. Under the **Change Password** section, enter your **Current Password**.

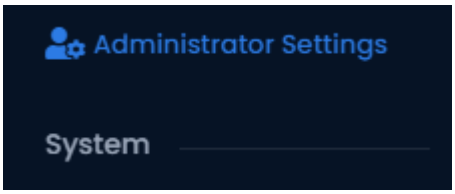


   e. Enter your new password under the **New Password** and **Confirm Password** fields. Ensure your new password meets the requirements shown.

   f. Click **Change Password** to update your password.

Enroll Two Factor Authentication

1. Access your VAX Access Control system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. In the left navigation menu, click on **Administrator Settings** near the end of the Administration section.



   Alternatively, you may click on the dropdown at the top-right of the page where it shows the Administrator's first name and click **Settings.**

4. Under the **Two Factor Authentication** section, you may see two options:
   - **One Time Password (TOTP)** Enroll VAX on a third party authenticator application, such as Google Authenticator or Microsoft Authenticator. The app will generate a six digit code that will change every thirty seconds. This six digit code must be entered must logging when to validate you have access to the second form of authentication.
   - **Security Token (FIDO)** Enroll VAX with a security authenticator, such as a smart phone or hardware security key with a supported browser. When logging in, the browser will ask the operating system to prompt you to use your authenticator to validate you have access to the second form of authentication.

Enroll One Time Password (TOTP) TFA

1. Click the **One Time Password (TOTP)** button on the Administrator Settings page.
2. Open your preferred TOTP Authenticator and enroll a new site using the QR Code. How to perform this will vary depending on app used.
3. Scan the QR code shown in the **Two Factor Authentication Enrollment** modal. Once you've enrolled the site, enter the current **TFA Code** into the modal to confirm enrollment.
4. Click **Enroll** to complete the enrollment of TOTP two factor authentication.

Enroll Security Token (FIDO)

1. Click the **Security Token (FIDO)** button on the Administrator Settings page.
2. The browser will prompt you with your available authentication options. Depending on your device and browser, various options may be available to you including:
   - **External security key or built-in sensor** Select a external security key, such as a Yubikey, or a built-in sensor such as Windows Hello or biometric sensor built in your device. The external security key either needs to be plugged in, or can use NFC for mobile devices when supported.
   - **Add a new Android phone** On Chrome browsers, you may use an Android phone as the second factor. This will require you to open a notification on the phone and place it near your device to perform two factor authentication.
3. Follow the instructions shown by your browser to complete the enrollment process.

Service Account Administrators for Third-party Services

Service account is available as an account type when adding an Administrator. The purpose of this account is to allow third party services to interact with the VAX REST API. Administrator Service Accounts use the same permission system as a normal Administrator; this allows you to scope the permissions of a third-party service to only what that service needs (for example, a service such as a telephone entry system would typically only need the Pulse Door permission).

Generating API Key

1. After you add the Administrator, navigate to the Edit Administrator screen for the Service Account Administrator.

2. Navigate to the API Key tab

Figure 20.1. API Key Tab on Edit Administrator

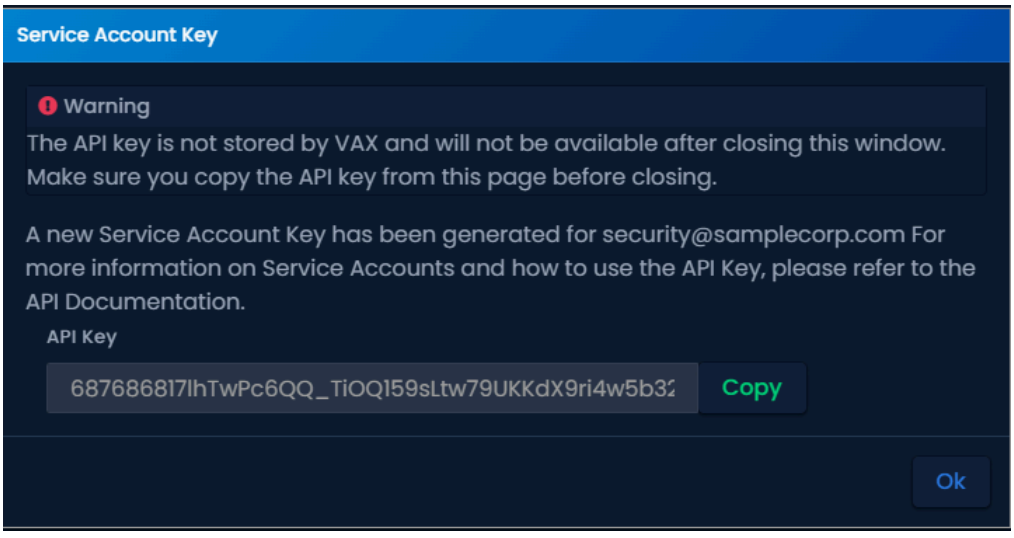
3. Click the Generate button to generate the API Key.

4. The API key will now appear and can be copied somewhere for safe keeping. The AI Key will be valid for 1 year from the date it is generated. When the API Key expires, it must be regenerated and reentered into any devices or services using it. The API Key can be regenerated or disabled at any time.

Warning

The API Key is not stored by VAX and will not be available after closing this window. Make sure you copy the API Key from this page before closing.

Figure 20.2. Generated API Key



IP Whitelist

All devices and services that are going to use an API Key through a Service Account Administrator must be white-listed by its IP address. This is a security feature to mitigate the risk of a misplaced API Key being used for malicious purposes.

Use the following steps to add IP addresses to the IP Whitelist:

1. After you add the Administrator, navigate to the Edit Administrator screen for the Service Account Administrator.
2. Navigate to the API Key tab.
3. On the bottom half of the screen, enter the IP address of the device or service that will be using the API Key. Wildcards are supported such as 192.168.2.* or 10.*.*.*. Multiple addresses are supported.
4. Click the Add button. The IP address entered will be added to the IP Whitelist.
5. Repeat the steps above if more than 1 IP Address is needed in the IP Whitelist.
6. Click Save on the bottom of the screen.

Figure 20.3. IP Whitelist

Using an API Key

The API Key is used when sending commands to the VAX REST API. Details on how to use the API key is covered in API documentation. Please see the section called “API Integration” for information on accessing the API documentation.

Administrator Privileges

VAX offers a very granular permissioning system, combined with Partitions, allowing you to give restricted access to various stakeholders while being assured they can only view and manage what's necessary. This section will go over how the permission system works, how to assign privileges to Administrators and Security Groups and a list of permissions available.

Terminology

System Administrator	An administrator that has full permissions to perform any action on the system.
Privilege Assignment	A permission granted globally or for a specific partition to an Administrator or a Security Group. For example, allow Add Users on Default Partition.
Permission	Consent for an Administrator to view information or perform an action. For example: View Users, Add Panels, Override Doors.
Scope	A permission can be applied or scoped to three different targets: Global, Partition, and Actor.

Global scope applies to all partitions or is an action that is performed at a global level. For example: Add Custom Fields, Manage LDAP Settings).

Partition scope applies the privilege to a specific partition. For example: Allow Add Holidays on Partition 1.

Actor scope applies the privilege for a specific actor(User,Door,Panel,etc..). For Example: Exclude Edit Users for CEO.

Privilege Overview

All Administrators that are not System Admins require one or more permissions to view information and perform actions. Permissions are granted by assigning privileges directly to an Administrator or indirectly through membership of a Security Group.

A privilege either allows or denies a permission for a Administrator or Security Group. The privilege specifies whether its applied globally to all partitions, for a specific partition, or for one or more specific actors. Multiple privileges for the same permission same can be granted to the same Administrator, either with different scopes or by Security Group membership.

When performing authorization of whether an Administrator can perform an action, all privileges assignments for the given permission. Since Administrators can have multiple privileges for the same permission, they are sorted in the following order:

1. Deny Global
2. Deny Actor
3. Deny Partition
4. Allow Actor
5. Allow Partition
6. Allow Global

The authorization check will compile a list of allowed and denied partitions and actors based on the sorted privilege list filter the results accordingly. Effectively being explicitly denied permission takes precedent over being explicitly granted permissions if there are conflicting privileges.

For example, an Administrator has two privileges: Allow View Users in Partition A, and Deny View Users Secret User. They would see all users in Partition A, except Secret User (assuming they are a member of Partition A). Since the Deny Actor privilege is sorted higher than the Allow Partition privilege, the Secret User is hidden.

Effectively a permission check will result in one of the four results:

- **None** No privileges were found for the Administrator, or they were Deny privileges, denying them from performing the permission.
- **Specific Partitions/Actors** Only Allow Actor or Allow Partition privileges were found for the Administrator, giving them access to perform the permission on specific partitions or actors only.
- **All Except** A Allow Global and one or more Deny Actor or Deny Partition privileges were found for the Administrator, giving them access to perform the permission all partitions except for the specified denied partitions or actors.

- **Global Allow** Only a Allow Global privilege was found for the Administrator, giving them access to perform the permission on all partitions.

Privilege Assignment

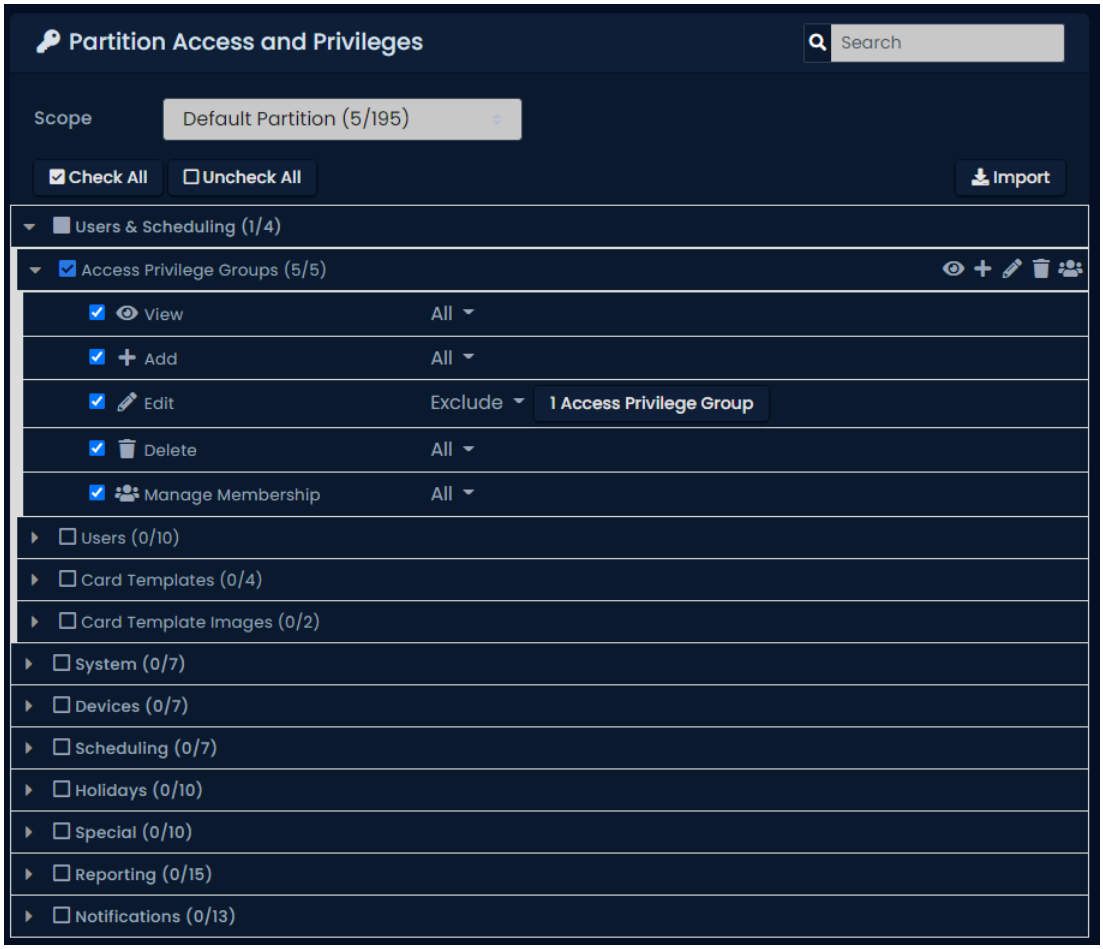
Privileges can be given either to Administrators individually or to a group of Administrators using Security Groups using the Partition Access and Privilege UI. Only System Administrators can assign privileges on the Add or Edit pages of Administrators and Security Groups.

On the top of the list, there is a **Scope** dropdown. This can either be set to **Global**, which will apply the permissions selected below to every partition, or set to a specific partition.

Note

*Certain permissions will only appear under the **Global** scope, such as the Global section and Add Partition.*

Figure 20.4. Partition Access and Privilege UI



1. At the top, select the **Scope** of where you want to grant the Administrator or Security Group privileges to.
2. Click on the right arrow of the category that has the permission you wish to grant.
3. You may select all permissions for an actor by clicking the checkbox, or click on the left arrow to see every individual permission available for the actor.
4. For each selected permission, you may further scope the privilege by selecting the **All** dropdown to the right of the permission.

5. Depending on the scope of the permission, the following options will appear in the dropdown:

   - **All** The privilege will allow the permission for all of the actors under the scope. For example, allowing a Administrator to view all users in a partition.

   - **Include** The privilege will allow the permission only the selected actors, rather than the entire scope. For example, allowing a Administrator to only view and edit their office door.

   - **Exclude** The privilege will explicitly deny the permission for the selected actors, rather than the entire scope. For example, denying a Security Group from viewing certain users.

   - **Except** The privilege will allow for all of the actors under the scope except the selected actors. For example, allowing a Administrator to view all maps except the map of the secret underground bunker.

   - **Deny** The privilege will explicitly deny the permission for all of the actors under the scope. For example, explicitly denying a Security Group from overriding the vault door.

6. If Include, Exclude or Except are selected, a button will appear to the right of the dropdown. Clicking on the button will allow you to select which actors are affected by the privilege.

To assist in assigning privileges, there are a few options to help:

- **Search** In the top right corner of the UI, there is a search field that will filter and expand any permissions that match the searched term. Pressing enter in the search will select all shown permissions.

- **Check All / Uncheck All** Below the Scope dropdown, there are buttons that select or deselect every permission in the selected scope.

- **Import** In the top right below the search, there is a Import button that will allow you to select a Administrator or Security Group to import all their privileges and replace the existing selection.

Security Groups

Security Groups are a way of assigning privileges to a group of Administrators without having to individually edit each one. Additionally Security Groups are used by non-system admins when creating Administrators to grant privileges that are pre-defined by system admins. Security Groups can only be managed by system admins, although non-system admins can be granted view privileges to Security Groups to be allowed to grant them to new Administrators.

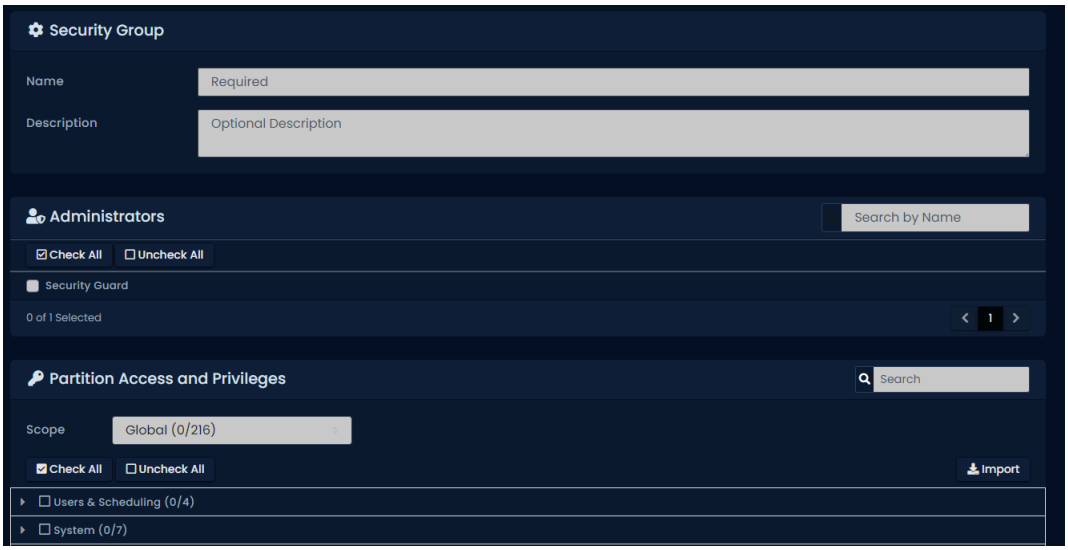
Create a new Security Group

1. Access your VAX Access Control system through your HTML5 browser of choice.

2. Log in using a System Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. In the left navigation menu, click on **Security Groups** under the Administration section near the middle of the navigation menu.

4. On the **Security Groups** page, click the **Add** button.



5. Enter a **Name** and **Description** in the Security Group section.

6. Select which **Administrators** you wish to grant privileges to with the group.

7. Under the **Partition Access and Privileges** section, select which privileges you wish to assign to the Administrators selected above. For more information, check the the section called “Privilege Assignment” section.

8. Once you've selected your Administrators and their new privileges, click **Create**.

Privilege Examples

Depending on which permissions you give an administrator, the amount of icons and sections of the software they can access will be different. This section will show a couple examples of how these permissions can be used to help end users of the system be more efficient.

Example: Secretary

After the system is commissioned, the security integrator hands over an Administrator account to the organization that purchased the system. The security staff gives an Administrator Account to the secretary at the front desk with the following permissions:

- View, Add and Edit Access Privilege Groups, Manage Access Privilege Group Membership
- View, Add and Edit Users, Manage User Credentials
- Reporting User Activity
- Update Panel
- View Status

Once the new Administrator logs in, he or she will only see icons based on their Administrator permissions. This administrator will be allowed to change/add Users, change which doors they have access to via Access Privilege Groups, run User Activity Reports and Update Panels whenever she/he makes changes. The view status privilege will allow the Administrator to see any notifications if they are logged in and see if any controllers are offline.

Figure 20.5. Administrator With Limited Permissions

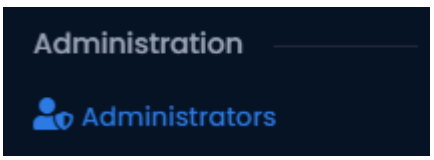
Privilege Report

The Privilege Report in the Edit Administrators page allows you to easily see the final result of all privileges applied to an Administrator. It lists every permission in collapsible sections, with each scope, Global and each Partition, as columns.

1. Access your VAX Access Control system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. In the left navigation menu, click on **Administrators** under the Administration section near the middle of the navigation menu.



4. On the **Administrators Screen**, find the non system admin you wish to see their Privilege Report and click the gear button to the left of their name to open the Edit Administrators page.

5. Select the **Privilege Report** tab at the top of the page.

Figure 20.6. Privilege Report Example

The left arrows can be expanded and collapsed to show all permissions under each section.

Permissions

VAX offers an extensive list of permissions to perform every actions in the system. There are a few important things to know about how permissions work.

In order to reduce complexity and keep backward comparability, certain permissions allow an Administrator to see other information that is required to use the permission. For example, the Add Access Privilege Group permission will allow an Administrator to query a list of Readers and Floors amongst other things that are required.

View permissions serve a couple different roles. A view permission is required in order to use any corresponding Add, Edit or Delete permissions, as they are all accessed from the list page. A view permission allows you to open the edit pages as read-only to view additional information not shown on the list page.

View permissions can also be used to prevent the actor from being assigned as a value. For example, excluding a door from being viewed will prevent its readers from showing up to be assigned to an Access Privilege Group.

Some other things of note regarding permissions:

- Privileges from all partitions a user is a member of are considered when performing user permission checks, since Users can belong to multiple partitions.
- Excluding viewing a panel does not hide the devices attached to a panel such as Doors and Elevators, that have their own permissions.

- Edit Action Plan is one of the most powerful permissions that can be granted. As Action Plans actions do not perform any permission checks, this permission effectively give the ability to perform most actions in the system.

System Administrator Permissions

Most abilities that were System Admin exclusive previously have been converted into Global permissions. However there are still a few things that remain exclusive to System Admins, including:

- **Adding, Editing or Deleting Security Groups** Non-system admins can only view Security Groups so that they can assign them to new administrators.
- **Add or Edit Administrator Privileges** Non-system admins may only assign Security Groups to grant privileges if allowed.
- **Reset Admin Lockout** Resetting other administrators lockout from too many bad password attempts can only performed by System Admins.
- **Configure Authentication** Since misconfiguring authentication could prevent system admins from accessing the system, configuring authentication is restricted to System Admins.
- **Approve Service Accounts** As Service Accounts request their own permissions, this action can only be performed by System Admins.
- **Set Master Permission on Users** Given Users unique ability of belonging to multiple partitions, allowing non-system admins set master permission may allow them to gain access in other partitions the Administrator may not have permission to.
- **Change Other Administrator Credentials or API Keys** To prevent non system-admins from gaining access to more privileged accounts, only System Admins can change passwords of other Administrators, remove TFA from their account, or generate API Keys.

Users & Scheduling Permissions

Table 20.3. Users & Scheduling Permissions

Permission	Scope	Description
View Access Privilege Groups	Actor	View the list of Access Privilege Groups and their user and reader assignments.
Add Access Privilege Groups	Partition	Add new Access Privilege Groups with Reader and Floor permissions. **Note:**Manage Membership permission is required to assign users to new groups.
Edit Access Privilege Groups	Actor	Edit details about existing Access Privilege Groups, including their Reader and Floor assignments.
Delete Access Privilege Groups	Actor	Delete existing Access Privilege Groups from the system.
View Users	Actor	View the list of Users and their permissions and credentials.
Add Users	Partition	Add new users with credentials and access group assignments.
Edit Users	Actor	Edit a users general settings and permissions.
Manage Users Custom Fields	Actor	Edit a users custom field values.
Manage Users Images	Actor	Add and remove profile and accessory pictures for users.
Manage Users Credentials	Actor	Add, edit and remove credentials, PINs and Mobile Credentials for users.
Manage Users Actions	Actor	Assign actions to perform upon being granted access to specific readers for users.

Permission	Scope	Description
View Users PINs	Actor	Ability to view assigned PINs for users.
Manage Users Anti Pass-back	Actor	Ability to view and reset the anti-passback position for users.
View Card Templates	Actor	View the list of card templates in the partition or system.
Add Card Templates	Partition	Add new card templates to the system.
Edit Card Templates	Actor	Edit existing card template details and their design and layout.
Delete Card Templates	Actor	Delete existing card templates from the partition or system.
View Card Template Images	Partition	View uploaded images for card templates in the partition or system.
Delete Card Template Images	Partition	Delete existing card template images from the system.

System Permissions

Table 20.4. System Permissions

Permission	Scope	Description
View Partitions	Actor	View the list of partitions in the system and their configuration.
Add Partitions	Global	Add new partitions to the system.
Edit Partitions	Actor	Edit name, description and auto update settings for existing partitions.
Delete Partitions	Actor	Delete existing partitions from the system.
View Health Status	Partition	View the health status of the partition.
View Sites	Actor	View the list of sites and their area and anti-passback configurations.
Add Sites	Partition	Add new sites to existing partitions.
Edit Sites	Actor	Configure site details, card formats, areas and APB settings.
Delete Sites	Actor	Delete sites from the system.
Manage Sites Antipass-back	Actor	Ability to reset the APB position for everyone in the site
View Engage Sites	Actor	View the list of Schlage Engage sites and their configuration.
Add Engage Sites	Partition	Add new Schlage Engage sites to the system.
Edit Engage Sites	Actor	Edit details about existing Engage sites.
Delete Engage Sites	Actor	Delete Engage sites from the system.
View Map List	Actor	View list of maps in the partition or system and their configuration.
Add Maps	Partition	Add new maps to partitions or sites.
Edit Maps	Actor	Edit the map details, image and objects shown on the map.
Delete Maps	Actor	Delete maps from the system.
View Map	Actor	View the actual map and its objects rendered on it.
View Action Triggers	Actor	View the list of action triggers in the partition or system and their configuration.
Add Action Triggers	Partition	Add new action triggers to the system.
Edit Action Triggers	Actor	Edit details about existing action triggers.

Permission	Scope	Description
Delete Action Triggers	Actor	Delete action triggers from the system.
View Action Plans	Actor	View the list of action plans but not the actual contents.
Add Action Plans	Partition	Add new action plans to the system.
Edit Action Plans	Actor	Edit the contents of existing action plans. **Note:** This permission effectively grants the ability to do many things as Action Plans do not have any permission checks.
Delete Action Plans	Actor	Delete action plans from the system.
Execute Action Plans	Actor	Execute normal security system action plans.
Execute High Security Action Plans	Actor	Execute high security system action plans.
View Dashboards	Actor	View the list of dashboards and the actual dashboard itself.
Add Dashboards	Partition	Add new dashboards to the system.
Edit Dashboards	Actor	Edit existing dashboards and their widgets.
Delete Dashboards	Actor	Delete dashboards from the system.

Device Permissions

Table 20.5. Device Permissions

Permission	Scope	Description
View Doors	Actor	View the list of Doors and their configuration in the partition or system.
Add Doors	Partition	Add new Doors to the Partition or system.
Edit Doors	Actor	Edit configuration of Doors in the partition or system except their readers or camera assignment.
Delete Doors	Actor	Delete Doors from the partition or system.
Manage Doors Readers	Actor	Assign and configure the inside and outside reader of doors in the partition or system.
Manage Doors Anti Passback	Actor	Configure areas and anti-passback settings of doors in the partition or system.
Manage Doors Cameras	Actor	Configure association of cameras and PTZ presets of doors in the partition or system.
View Elevators	Actor	View the list of elevators and their configuration in the partition or system.
Add Elevators	Partition	Add new elevators to the partition or system.
Edit Elevators	Actor	Edit configuration of existing elevators in the partition or system except their floors, reader and camera assignment.
Delete Elevators	Actor	Delete elevators from the partition or system.
Manage Elevator Floors	Actor	Configure floor details and Schedules assignments for elevators in the partition or system.
Manage Elevator Reader	Actor	Assign and configure the reader in the cab of elevators in the partition or system.
Manage Elevator Cameras	Actor	Configure association of cameras and PTZ presets of elevators in the partition or system.
View Panels	Actor	View the list of panels and their configuration in the partition or system.

Permission	Scope	Description
Add Panels	Partition	Add new panels to the partition or system.
Edit Panels	Actor	Edit configuration of panels in the partition or system except their I/O, and panel password.
Delete Panels	Actor	Delete panels and their attached devices from the partition or system.
Manage Panel IO	Actor	Configure the inputs and outputs of panels in the partition of system.
Manage Panel Password	Actor	View and edit the password used to access the panel interface.
Perform Panel Commands	Actor	Send various commands to the panel including report time and disconnect the panel from the server.
Update Panel Firmware	Actor	Command the panel to update to the latest firmware available from the server.
View Camera Integrators	Actor	View the list of camera integrators in the partition or system.
Add Camera Integrators	Partition	Add new camera integrators to the partition or system.
Edit Camera Integrators	Actor	Edit configuration of camera integrators in the partition or system and synchronize and assign cameras to the software.
Delete Camera Integrators	Actor	Delete camera integrators from the partition or system.
View Cameras	Actor	View the live or recorded video from cameras associated to the partition or system.
View Alarm Panels	Actor	View the list of alarm panels in the partition or system.
Add Alarm Panels	Partition	Add new alarm panels to the partition or system.
Edit Alarm Panels	Actor	Edit configuration of alarm panels in the partition or system.
Delete Alarm Panels	Actor	Delete alarm panels and their partitions and zones from the partition or system.
View Alarm Partitions	Actor	View the list of alarm partitions in the partition or system.
Edit Alarm Partitions	Actor	Edit configuration of the alarm partitions in the partition or system.
Arm / Disarm Alarm Partitions	Actor	Arm or disarm the alarm partition to secure the area or gain access.
Perform Alarm Actions	Actor	Perform actions such as fire or aux panic and silence trouble beeps.
Bypass Zones	Actor	Bypass zones to allow arming of partitions with an open zone.

Scheduling Permissions

Table 20.6. Scheduling Permissions

Permission	Scope	Description
View Door Schedules	Actor	View the list of Door Schedules in the partition or system.
Add Door Schedules	Partition	Add new Door Schedules to the partition or system.
Edit Door Schedules	Actor	Edit existing Door Schedules and their time span configuration.
Delete Door Schedules	Actor	Delete existing Door Schedules from the partition or system.
View Floor Schedules	Actor	View the list of Floor Schedules in the partition or system.
Add Floor Schedules	Partition	Add new Floor Schedules to the partition or system.

Permission	Scope	Description
Edit Floor Schedules	Actor	Edit existing Floor Schedules and their time span configuration.
Delete Floor Schedules	Actor	Delete existing Floor Schedules from the partition or system.
View Door One Time Runs	Actor	View the list of Door One Time Runs in the partition or system.
Add Door One Time Runs	Partition	Add new Door One Time Runs to the partition or system.
Edit Door One Time Runs	Actor	Edit existing Door One Time Runs and their time span configuration.
Delete Door One Time Runs	Actor	Delete existing Door One Time Runs from the partition or system.
View Floor One Time Runs	Actor	View the list of Floor One Time Runs in the partition or system.
Add Floor One Time Runs	Partition	Add new Floor One Time Runs to the partition or system.
Edit Floor One Time Runs	Actor	Edit existing Floor One Time Runs and their time span configuration.
Delete Floor One Time Runs	Actor	Delete existing Floor One Time Runs from the partition or system.
View User Schedules	Actor	View the list of User Schedules in the partition or system.
Add User Schedules	Partition	Add new User Schedules to the partition or system.
Edit User Schedules	Actor	Edit existing User Schedules and their time span configuration.
Delete User Schedules	Actor	Delete existing User Schedules from the partition or system.
View Input Schedules	Actor	View the list of Input Schedules in the partition or system.
Add Input Schedules	Partition	Add new Input Schedules to the partition or system.
Edit Input Schedules	Actor	Edit existing Input Schedules and their time span configuration.
Delete Input Schedules	Actor	Delete existing Input Schedules from the partition or system.
View Output Schedules	Actor	View the list of Output Schedules in the partition or system.
Add Output Schedules	Partition	Add new Output Schedules to the partition or system.
Edit Output Schedules	Actor	Edit existing Output Schedules and their time span configuration.
Delete Output Schedules	Actor	Delete existing Output Schedules from the partition or system.

Holidays Permissions

Table 20.7. Holidays Permissions

Permission	Scope	Description
View Holidays	Actor	View the list of Holidays and the groups they affect in the partition or system.
Add Holidays	Partition	Add new Holidays to the partition or system.
Edit Holidays	Actor	Edit existing Holidays in the partition or system.
Delete Holidays	Actor	Delete existing Holidays from the partition or system.
View Door Holiday Groups	Actor	View the list of Door holiday groups in the partition or system.
Add Door Holiday Groups	Partition	Add new Door holiday groups to the partition or system.

Permission	Scope	Description
Edit Door Holiday Groups	Actor	Edit existing Door holiday groups in the partition or system.
Delete Door Holiday Groups	Actor	Delete existing Door holiday groups from the partition or system.
View Door Holiday Schedules	Actor	View the list of Door holiday Schedules in the partition or system.
Add Door Holiday Schedules	Partition	Add new Door holiday Schedules to the partition or system.
Edit Door Holiday Schedules	Actor	Edit existing Door holiday Schedules in the partition or system.
Delete Door Holiday Schedules	Actor	Delete existing Door holiday Schedules from the partition or system.
View Floor Holiday Groups	Actor	View the list of Floor holiday groups in the partition or system.
Add Floor Holiday Groups	Partition	Add new Floor holiday groups to the partition or system.
Edit Floor Holiday Groups	Actor	Edit existing Floor holiday groups in the partition or system.
Delete Floor Holiday Groups	Actor	Delete existing Floor holiday groups from the partition or system.
View Floor Holiday Schedules	Actor	View the list of Floor holiday Schedules in the partition or system.
Add Floor Holiday Schedules	Partition	Add new Floor holiday Schedules to the partition or system.
Edit Floor Holiday Schedules	Actor	Edit existing Floor holiday Schedules in the partition or system.
Delete Floor Holiday Schedules	Actor	Delete existing Floor holiday Schedules from the partition or system.
View User Holiday Groups	Actor	View the list of User holiday groups in the partition or system.
Add User Holiday Groups	Partition	Add new User holiday groups to the partition or system.
Edit User Holiday Groups	Actor	Edit existing User holiday groups in the partition or system.
Delete User Holiday Groups	Actor	Delete existing User holiday groups from the partition or system.
View User Holiday Schedules	Actor	View the list of User holiday Schedules in the partition or system.
Add User Holiday Schedules	Partition	Add new User holiday Schedules to the partition or system.
Edit User Holiday Schedules	Actor	Edit existing User holiday Schedules in the partition or system.
Delete User Holiday Schedules	Actor	Delete existing User holiday Schedules from the partition or system.
View Device Holiday Groups	Actor	View the list of Device holiday groups in the partition or system.
Add Device Holiday Groups	Partition	Add new Device holiday groups to the partition or system.
Edit Device Holiday Groups	Actor	Edit existing Device holiday groups in the partition or system.
Delete Device Holiday Groups	Actor	Delete existing Device holiday groups from the partition or system.

Permission	Scope	Description
View Input Holiday Schedules	Actor	View the list of Input holiday Schedules in the partition or system.
Add Input Holiday Schedules	Partition	Add new Input holiday Schedules to the partition or system.
Edit Input Holiday Schedules	Actor	Edit existing Input holiday Schedules in the partition or system.
Delete Input Holiday Schedules	Actor	Delete existing Input holiday Schedules from the partition or system.
View Output Holiday Schedules	Actor	View the list of Output holiday Schedules in the partition or system.
Add Output Holiday Schedules	Partition	Add new Output holiday Schedules to the partition or system.
Edit Output Holiday Schedules	Actor	Edit existing Output holiday Schedules in the partition or system.
Delete Output Holiday Schedules	Actor	Delete existing Output holiday Schedules from the partition or system.

Special Permissions

Table 20.8. Special Permissions

Permission	Scope	Description
Pulse Door	Actor	Momentarily unlock doors in the partition or system.
Override Door	Actor	Override doors to different modes in the partition or system.
Override Door Lockdown	Actor	Override doors to lockdown in the partition or system.
Override Door Crisis Level	Actor	Override doors to a crisis level in the partition or system.
Override Floor	Actor	Override floors to different modes in the partition or system.
Override Input	Actor	Override inputs to different modes in the partition or system.
Override Output	Actor	Override outputs to different modes in the partition or system.
Disengage Emergency Alarm	Actor	Disengage the emergency alarms that have been triggered on panels in the partition or system.
View Status	Partition	See the real time status of devices in the partition or system.
Update Panel	Actor	Update the configuration of panels in the partition or system.

Reporting Permissions

Table 20.9. Reporting Permissions

Permission	Scope	Description
User List	Actor	View the list of every user's credential in the partition or system.
Door Activity	Actor	View historical report of door notifications in the partition or system.
User Activity	Actor	View historical report of user notifications in the partition or system.
Floor Activity	Actor	View historical report of floor notifications in the partition or system.

Permission	Scope	Description
Configuration	Partition	View configuration of devices and scheduling in the partition or system.
IO	Partition	View historical report of input and output notifications in the partition or system.
User Time Tracking	Actor	View duration of time user's have spent within areas in the partition or system.
Action Plans	Actor	View historical report of action plan notifications in the partition or system.
Monitoring	Partition	View full screen notification monitoring page.
Elevator Activity	Actor	View historical report of elevator notifications in the partition or system.
APB	Partition	View real time positions of user's for anti-passback in the partition or system.
Alert History	Partition	View historical report of notifications that were configured as alerts and the acknowledgement of the alerts in the partition or system.
Notifications	Partition	View historical report of all notifications in the partition or system.
Administrative Log	Actor	View historical activity of all actions taken by Administrators in the system.
DSC Alarm Activity	Actor	View historical report of alarm notifications in the partition or system.

Global Permissions

Table 20.10. Global Permissions

Permission	Scope	Description
View Administrators	Actor	View the list of administrators in the partition or system.
Add Administrators	Global	Add new non-system administrators to the system using Security Groups to assign privilege.
Edit Administrators	Actor	Edit details about other administrators in the system.
Delete Administrators	Actor	Delete existing administrators from the system.
View Security Groups	Actor	View the list of security groups in the system. Security Groups membership can be changed when granted the Add Administrator or Edit Administrator permission.
View Custom Fields	Actor	View list of all custom fields in the system.
Add Custom Fields	Global	Add new custom fields to the system.
Edit Custom Fields	Actor	Edit existing custom fields and their options in the system.
Delete Custom Fields	Actor	Delete existing custom fields from the system.
Crisis Levels	Global	Manage levels of Crisis Levels that are available and which Schedule mode they perform.
LDAP	Global	Configure LDAP settings and mapping of LDAP attributes to credentials or custom fields.
Manage Customer	Global	Configure global customer settings such as Server Address and dealer information.
Email Settings	Global	Configure the SMTP settings used to send emails from VAX.

Permission	Scope	Description
Licensing	Global	Allow Administrators to update the licensing information.
Database	Global	View totals and purge notifications and administrative logs from VAX.
Data Migrator	Global	Ability to export and import data into the software. **Note:** This permission grants the ability to add or update most values in the software and should be selectively given when necessary.
STid Credentials	Global	When integrated to the STid portal, permission will allow administrators to view and enroll paid STid credentials.
View Health Settings	Global	View configured health issues and their thresholds and actions in the system.
Edit Health Settings	Global	Configure health issues, thresholds and actions performed in the system.
Reporting Health Issues	Global	View historical report of health issues that log the issue in the system.

Notification Permissions

Table 20.11. Notification Permissions

Permission	Scope	Description
View Rules	Partition	View the list of notification rules that determines where processed notifications are sent to in the partition or system.
Manage Admin Rules	Partition	Configure notification rules to affect how notifications are sent to the administrator from the partition or system.
Manage Global Rules	Partition	Configure notification rules to affect how notifications are processed globally for all administrators in the partition or system.
Manage Database Rules	Partition	Configure database notification rules that affect which notifications are stored in the database for reporting and their retention policy.
Manage Admin Styles	Partition	Configure styles to affect how real time notifications appear in the UI for the administrator from the partition or system.
Manage Global Styles	Partition	Configure styles to affect how real time notifications appear globally for all administrators in the partition or system.
Manage Admin Live Camera Rules	Partition	Configure which notifications will trigger the live camera to appear in the UI for the administrator from the partition or system.
Manage Global Live Camera Rules	Partition	Configure which notifications will trigger the live camera to appear globally for all administrators in the partition or system.
Manage Alert Rules	Partition	Configure which notifications should be considered alerts and require acknowledgement in the partition or system.
Manage Rule Groups	Partition	Configure rule groups, which allows you to configure a group of administrators that can acknowledge an alert in the partition or system.
Acknowledge Alert	Partition	Ability to acknowledge a standard alert in the partition or system.
Acknowledge Supervisor Alert	Partition	Ability to acknowledge a supervisor alert in the partition or system.

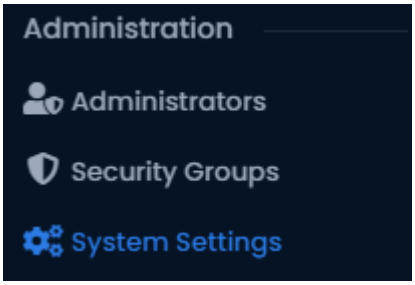
Permission	Scope	Description
Push Notifications	Partition	Allow notifications to be sent to the administrators using web push.

Authentication

VAX offers several different ways of authenticating Administrators to access the software. This section will go over how to configure these various authentication options. As changing authentication settings could prevent System Administrators from logging in, view and editing these settings is restricted to System Admins only.

Local Authentication

1. Access your VAX Access Control system through your HTML5 browser of choice.
2. Log in using the System Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. In the left navigation menu, click on **System Settings** near the end of the Administration section.



4. Click on the **Authentication** tab at the top of the System Settings page.
5. Under **Local Authentication Settings**, you may update the following settings.

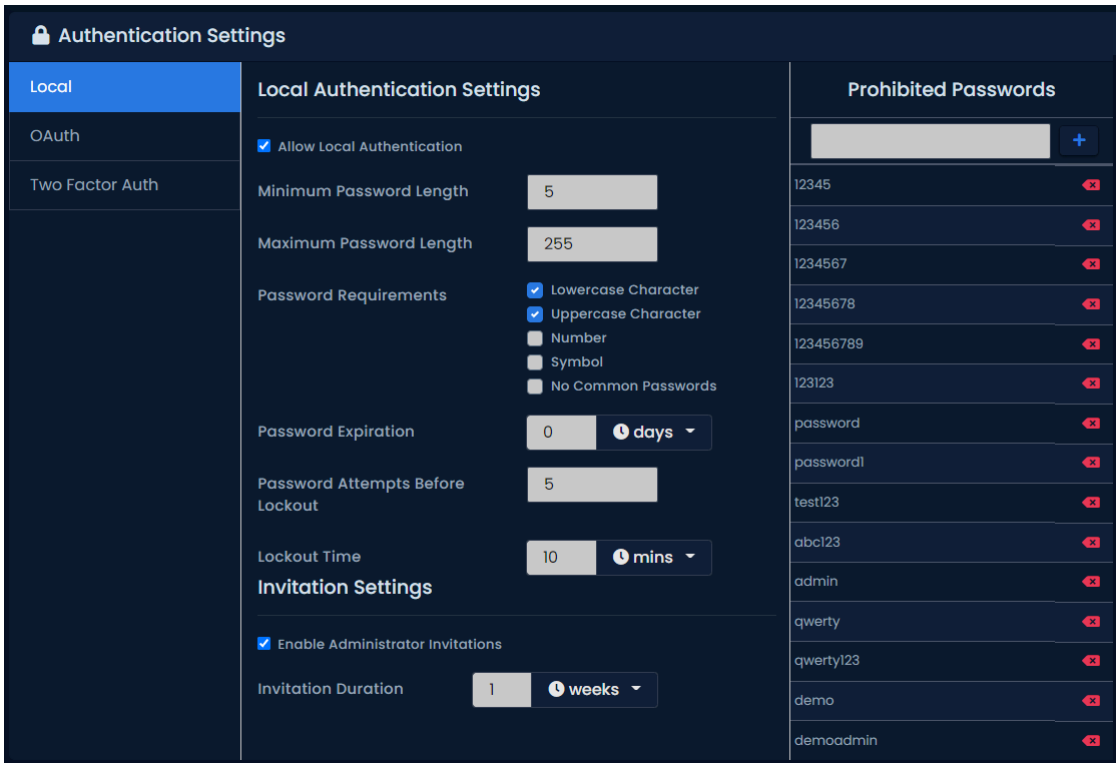


Table 20.12. Local Authentication Settings

Text Box/Drop-down Menu/ Checkbox	Description
Allow Local Authentication	Sets whether Administrators are allowed to login using local authentication.
Minimum Password Length	Minimum length of the password required.
Maximum Password Length	Maximum length of the password allowed.
Password Requirements	Complexity requirements to ensure passwords are secure. • **Lowercase Character** A lowercase character (a-z) is required. • **Uppercase Character** A uppercase character (A-Z) is required. • **Number** A number (0-9) is required. • **Symbol** A non-alphanumeric symbol (!, #, $, etc..) is required. • **No Common Passwords** Any passwords on the Prohibited Password list are not allowed.
Password Expiration	An optional time in days before a password will expire and be required to changed to login. Setting this value to 0 disables password expiration. An Administrator can have **Password Never Expires** set in Edit Administrator to ignore this requirement.
Password Attempts Before Lockout	Number of bad password attempts on an Administrator account before locking any login attempts for a specified time.
Lockout Time	Time in minutes to lockout an Administrator account after too many bad password attempts.
Enable Administrator Invitations	Enable sending an invitation email to new Administrators to have them enroll and set a password.
Invitation Duration	Duration in days the invitation to the new Administrator is valid for.
Prohibited Passwords	List of password that are prohibited from being set when **No Common Passwords** is enabled.

6. Click **Save** in the bottom right once you've updated your settings.

OAuth Authentication

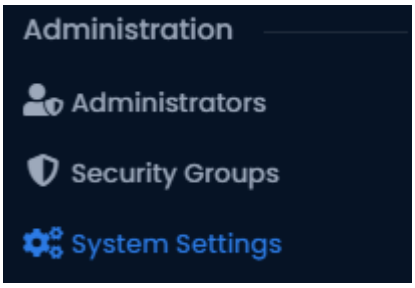
OAuth authentication uses third party authentication providers, such as Google or Microsoft, to authorize Administrators to VAX. When the Administrator wants to logs in, VAX will redirect to the third party provider where they will enter their existing credentials. Once the third party provider authenticates their credentials, it redirects back to VAX with a unique code that it uses to retrieve a security token validating that the Administrator authorized.

In order to perform authentication, the OAuth provider will require a Redirect URI to redirect back to VAX. This URL needs to be valid where ever the software is accessed from, which generally will require it to be a valid DNS address that resolves back to the server.

1. Access your VAX Access Control system through your HTML5 browser of choice.

2. Log in using the System Administrator account you created during the initial setup or provided to you by your dealer/installer.

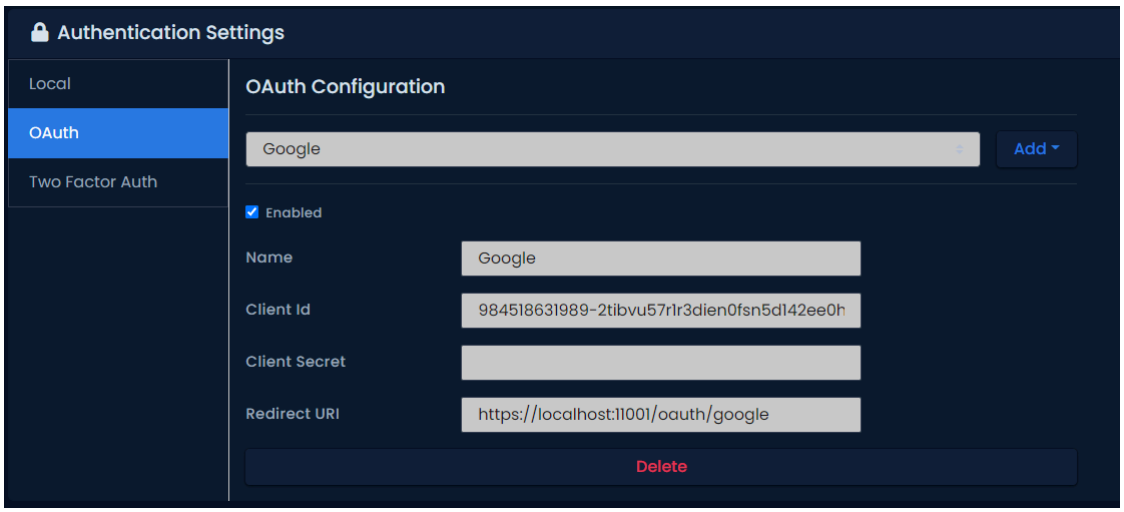
3. In the left navigation menu, click on **System Settings** near the end of the Administration section.



4. Click on the **Authentication** tab at the top of the System Settings page.

5. Click the **OAuth** tab on the left menu. Under **OAuth Configuration**, you may add and manage existing third party OAuth providers.

6. Click on the **Add** dropdown to select one of the supported (**Google**, **Microsoft**) providers or a **Custom** provider.



7. Depending on the provider selected, varying fields will be shown to configure the OAuth provider. For all providers, you will need to register on their system to retrieve a Client Id and Client Secret. They should also have a section with more information to fill in the other fields if using the a custom provider.

Table 20.13. OAuth Configuration

Text Box/Drop-down Menu/ Checkbox	Description
Enabled	Sets whether this OAuth provider can authenticate Administrators.
Name	Name of the OAuth provider shown on the Login page.
Client Id	Unique identifier provided by the OAuth provider to identify the VAX server to the OAuth provider.
Client Secret	Secret provided by the OAuth provider to authenticate the VAX server when obtaining access tokens.
Redirect URI	URI that the OAuth provider will redirect the Administrator back to VAX with the authentication code. This should follow the following syntax: https://[ServerAddress]:11001/oauth/[OAuthId] OAuthId will either be Google or Microsoft for the supported providers, or a GUID for custom providers.

Text Box/Drop-down Menu/ Checkbox	Description
Scopes *	Scopes requested from the OAuth provider to retrieve the email and subscriber information.
Auth URL *	URL of the OAuth provider to redirect the Administrator to perform login request.
Token URL *	URL to request access token from OAuth provider using authentication code sent back to VAX in the Redirect URI.
Email Claim *	Claim in the access token representing the email address of the Administrator
Identifier Claim *	Claim in the access token representing the unique identifier of the OAuth account.
Load Metadata *	Sets whether to synchronize First Name, Last Name and Language claims from the OAuth provider on login.
First Name Claim *	Claim in the access token representing the first name of the Administrator.
Last Name Claim *	Claim in the access token representing the last name of the Administrator.
Language Claim *	Claim in the access token representing the language of the Administrator.

8. Click **Save** in the bottom right once you've updated your settings.

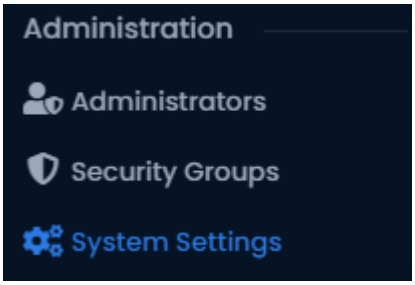
Two Factor Authentication

Two Factor Authentication requires an Administrator to present a second form of authentication beyond just their password. This form of authentication can be a six digit TOTP token or using a hardware authenticator such as a security key or mobile phone.

Warning

Using FIDO two factor authentication requires the URL used to access VAX to match the **Web Address** field in System Settings in order to authenticate. Additionally a valid SSL Certificate is required in order to use these higher security features.

1. Access your VAX Access Control system through your HTML5 browser of choice.
2. Log in using the System Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. In the left navigation menu, click on **System Settings** near the end of the Administration section.



4. Click on the **Authentication** tab at the top of the System Settings page.
5. Click the **Two Factor Auth** tab on the left menu. Under **Two Factor Authentication**, you may configure which TFA options are available.

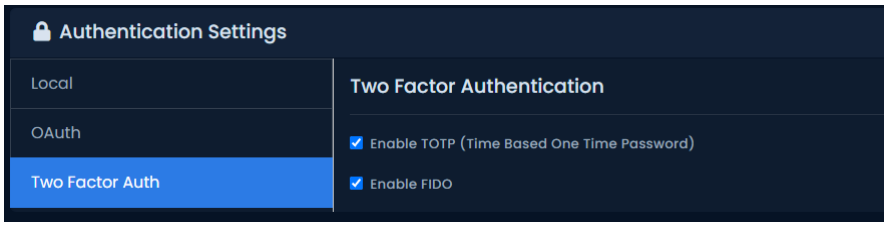


Table 20.14. Two Factor Authentication Settings

Text Box/Drop-down Menu/ Checkbox	Description
Enable TOTP (Time Based One Time Password)	Allow Administrators to enroll Time Based One Time Password authenticators as their second form of authentication.
Enable FIDO	Allow Administrator to enroll FIDO authenticators, such as security tokens like Yubikeys, as their second form of authentication.

6. Click **Save** in the bottom right to save your changes.

Chapter 21. Areas and Anti-Passback

This chapter covers the configuration of Anti-Passback in VAX.

Anti-passback is a feature that will prevent a Credential (card/fob/PIN) from being used twice to gain access to an area without exiting the monitored area first. VAX supports Global and Local anti-passback.

Local anti-passback: Works on a per controller basis operating with just two areas (in and out). Can operate without the VAX server.

Global anti-passback: Works across multiple controllers, required when there are more than one entrance to an area or when areas are nested inside areas such as multi level parking structures. Requires the VAX server be available in order for user locations to be updated between controllers.

Note

Anti-passback will be abbreviated to 'APB' for the remainder of this chapter.

Hardware

This section will outline hardware requirements for anti-passback.

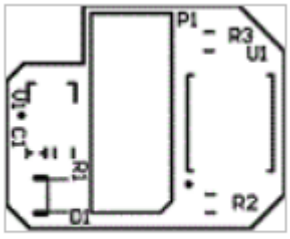
- Panel must be a door controller. Other Panel models like elevator and IO panels do not support this feature.
- If a Panel must make anti-passback decisions, it will require a **Memory Module**. Please see the following section on the APB Memory Module.
- Each Site may not have more than 4 different Site Codes/Facility for anti-passback to function fully. PINs do not contribute to this limit.

APB Memory Module

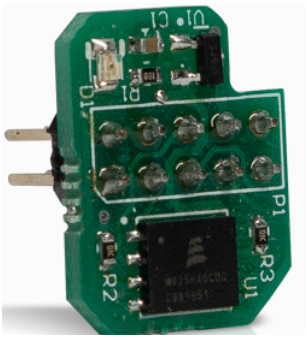
In order for a controller to make anti-passback decisions, it must have a Memory Module installed. Panels without a memory module will be unable to raise anti-passback violations but can report to the server when a User enters an Area, which can be forwarded to other Panels assigned to the same Areas.

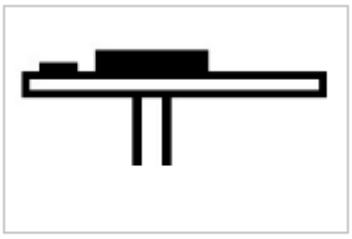
Hardware Specifications:

- Memory Size: 512KB
- Power Indicator LED
- Part#: APB-MEM



Top View





Side View

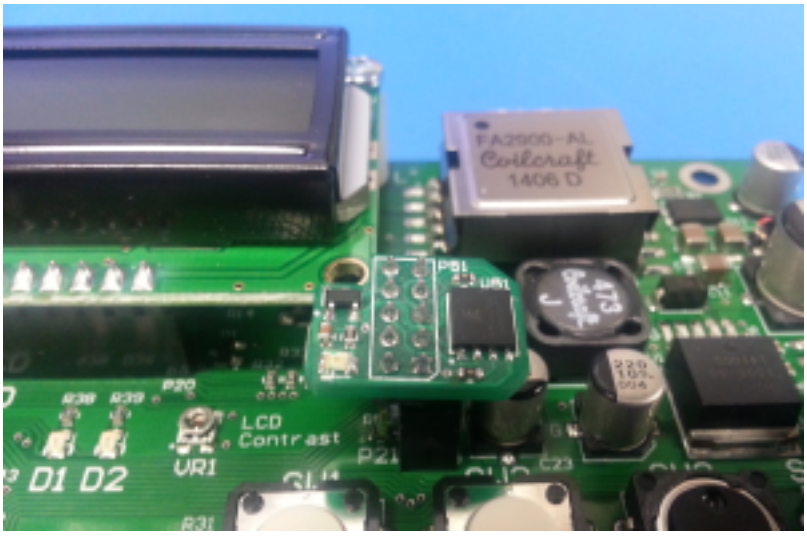
Memory Module Installation

The APB Memory Module is inserted into port P21 with the notched corner of the module to the upper left when facing the Panel directly so that the notch goes around the lower right corner of the LCD screen. Ensure that all pins are securely seated into the socket and that none are bent.

Warning

The memory module should only be inserted into port 21 on a controller when the controller is not powered otherwise damage may occur to the module.

Figure 21.1. Memory Module Installed



Anti-passback Software Configuration

There are three main components for configuring APB. This section will cover all of them.

- **Areas:** Created and assigned to doors so the system can know which readers grant access to which areas and what area a user should be in before being granted access to another area.
- **APB Settings:** Site level APB configuration. Can be overridden at the panel level.
- **APB Status:** Status screen that gives you an overview of where Users are in the system, which areas they were in, last activity, etc.

Configuring anti-passback should be done in the following order:

- Add any required Areas
- Configure Site level APB settings
- Assign Areas and enable APB on any Doors requiring APB
- Test and monitor APB status

Note

There is a maximum limit of 32 Site Codes supported by APB

Adding Areas

Areas are a configuration item used with APB. At least one Area should be created in order to configure APB. To add an Area:

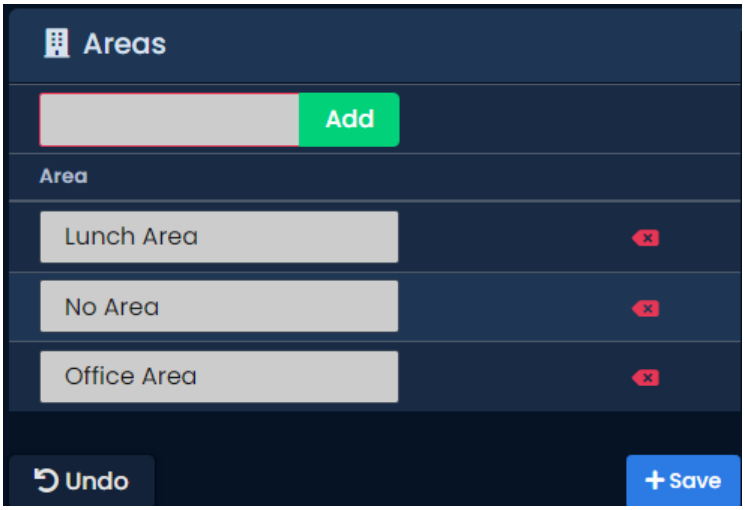
1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **System**; click on the **Sites and Areas** icon (pictured below).

4. On the **Sites and Areas** screen, you'll see any sites you've created. Click the blue button (advanced settings) next to the Site you'll be using APB with.
5. On the Edit Site screen, click on the **Areas** tab.
6. On the **Areas** tab, enter a name for your new area and click the **Add Area** button on the right side.

> **Note**
>
> The default area 'No Area' cannot be deleted.

You have now successfully added an Area to VAX, and can continue configuring APB.

Figure 21.2. Adding an Area



Anti-Passback Configuration

APB specific settings such as Timeout, Soft APB and Expiry are configured at the Site level. Any Doors attached to panels on the Site will adhere to these settings, but can be overridden on the APB tab of the Edit Door screen.

1. On the **Side Bar**, scroll down to the section titled **System**; click on the **Sites and Areas** icon (pictured below).

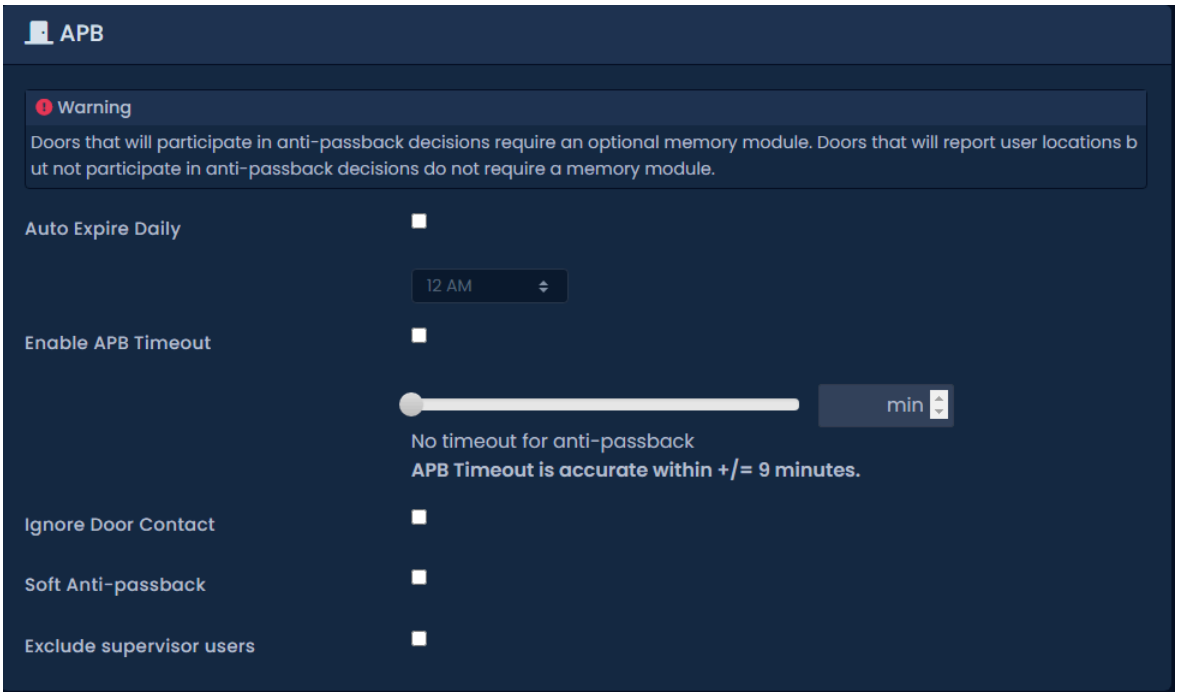
2. On the **Sites and Areas** screen, you'll see any sites you've created. Click the blue button (advanced settings) next to the Site you'll be using APB with.
3. On the Edit Site screen, click on the **APB** tab.

4. Configure the following settings based on the requirements of the Site. If you have some Doors that require different settings compared to the majority of Doors on the Site, you can individually set these same settings from the Edit Door screen.

Table 21.1. Anti-passback Configuration Items

Configuration Item	Description
Auto Expire Daily	Enable if you require the User Areas on the site to reset at a specific time each day. Enable and select an hour of the day when Users on the Site will reset to 'No Area'.
APB Timeout	The amount of time (in minutes) after a User is granted access to an area that the User will be allowed through the Door/Gate without raising an APB violation. APB Timeout is accurate within +/= 9 minutes. Supports 30 to 2550 minutes.
Ignore Door Contact	If checked, APB will ignore the Door contact. A Credential presentation will count as the User moving through to the configured Area. If unchecked, a User Credential presentation will only count as moved to the configured Area if the Door contact detects the Door opening.
Soft Anti-passback	When checked, APB violations will be reported, but access will be granted. If unchecked, an APB violation results in the User being denied access.
Exclude Supervisor Users	Users with the User Privilege "Supervisor" will be exempted from APB violations.

Figure 21.3. APB Settings



Click on the **Save** button once configuration is complete.

Assigning Areas to Readers

This section will demonstrate how to activate APB on a Door and assign each reader to an Area.

1. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Doors** icon (pictured below).

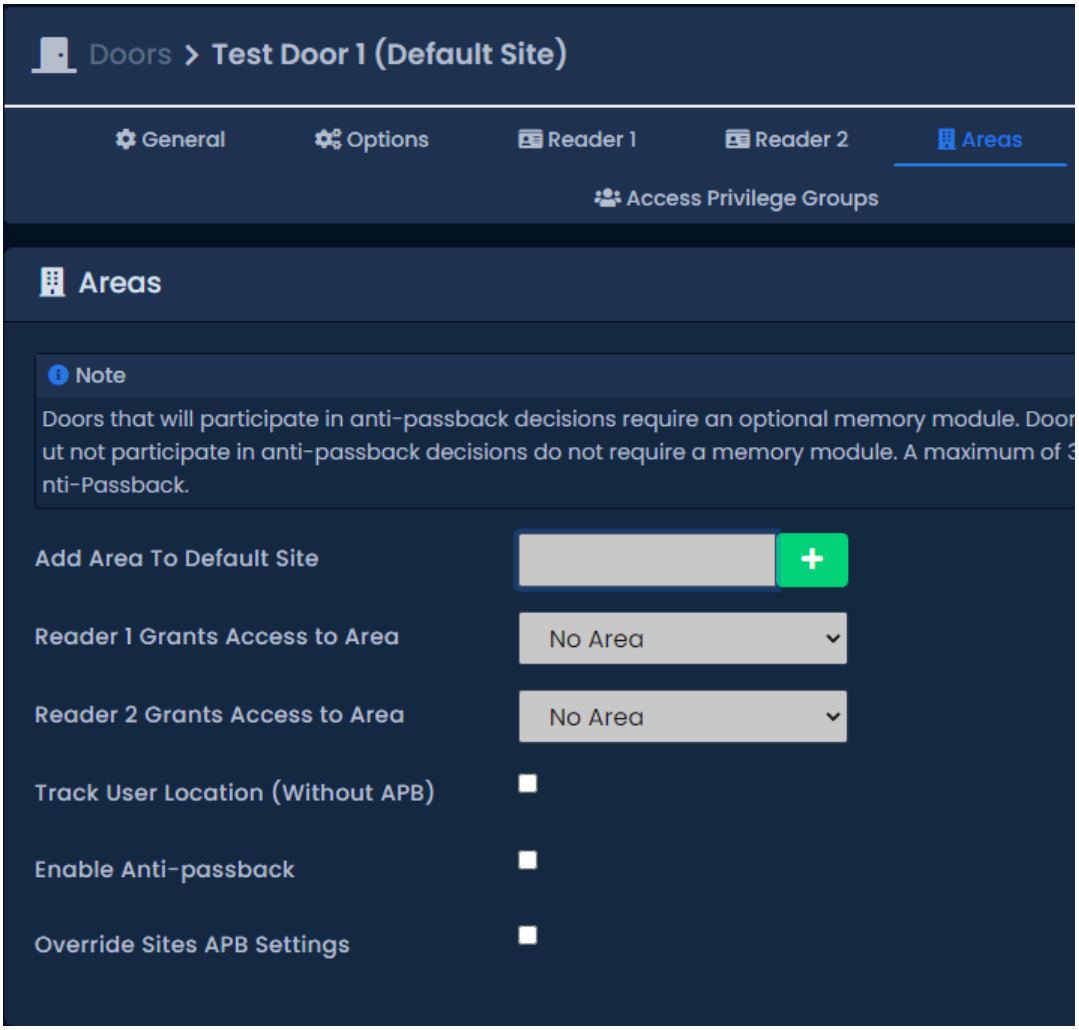
2. On the **Doors** screen, you'll see any Doors you've already configured listed here. Click the blue button next to the Door you'd like to configure APB on.

3. On the **Edit Door** screen, you'll see 5 tabs. Click on the **Areas** tab. The configuration items on this screen are explained below:

Table 21.2. Anti-passback Configuration Items

Configuration Item	Description
Reader 1 Grants Access to Area	The Area that Reader 1 grants access to. Select a custom Area or 'No Area'.
Reader 2 Grants Access to Area	The Area that Reader 2 grants access to. Select a custom Area or 'No Area'. If there is no Reader 2, an area should still be selected.
Enable Anti-Passback	Selecting this option will enable Anti-Passback. Doors without Panels with Memory Modules will report User Area location changes when enabled but will not make APB decisions.
Override Sites APB Settings	Select if APB settings on this Door should be different than the APB settings defined on the Edit Site screen.

Figure 21.4. Areas Tab on Edit Door



4. Click on the **Save** button once configuration is complete.
5. Panels should be updated after these changes. You can now begin testing and monitoring APB.

APB Status and Violations

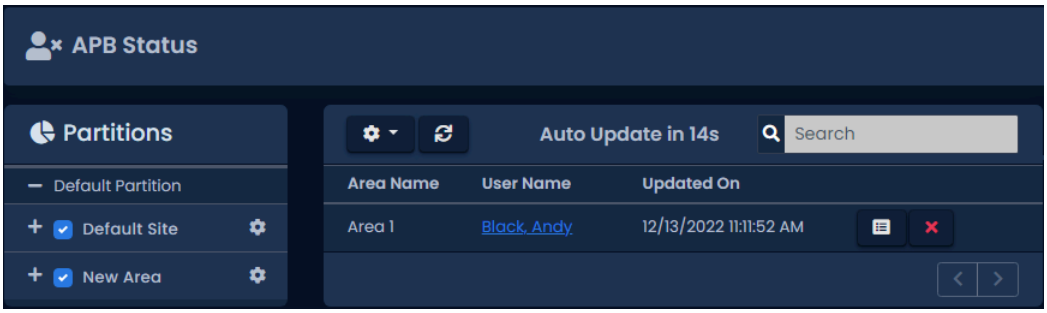
This section will outline the monitoring options for APB and how violations work.

Most monitoring of APB can be done from the APB Status screen.

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **APB Status** icon (pictured below).

2. The APB Status page will be displayed. Here you can view live status of what Areas Users are currently in. If a User is in the area 'No Area' they will not be displayed here.

Figure 21.5. APB Status Screen



This screen will automatically refresh every few seconds; the refresh timer can be adjusted using the gear icon above the user location grid. You can toggle which areas are displayed via the list on the left side.

Reset User Anti-passback Locations

In some circumstances it may be necessary to reset the location of a User. This can occur if a User tailgated into an Area or was unable to read out of an area. There are several ways to reset the location of a User. You can reset the entire Site, an individual User or a single Door Controller. This section will outline these methods.

Note

When a User has its location reset, the User will not raise violations on the next valid card. Be wary of resetting locations when utilizing nested Areas (Areas inside Areas).

- **Reset Individual User:** On the APB Status screen, click the blue gear icon to the right of any User. From the context menu, you can select 'Reset User's Location' to reset the User. You can also reset the User from the Anti-passback tab of the Edit User screen (if the context menu disappears, this is due to the list being refreshed based on the refresh timer).
- **Reset All Site Locations:** On the APB Status screen, you can click the gear icon next to any Site name on the left side of the screen. From the context menu, you can select 'Reset All Site Locations' to reset all User locations of Users currently located in any Areas on the selected Site.
- **Auto Expire Daily:** If required, an individual Site can be configured to reset all User locations at a specific hour of the day. See the section called “Anti-Passback Configuration” for configuration options.

APB Violations

An APB violation occurs when a User attempts to enter an Area they are already in or attempt to enter a nested Area without entering the previous Area.

By default, an APB violation will result in the User being denied access. If Soft Anti-passback is enabled, a violation will be raised but the User will be granted access to the Area.

APB violations can be configured to send an email and/or trigger a camera view. For more information, please see the section called “Email Notifications”.

Figure 21.6. APB Violations

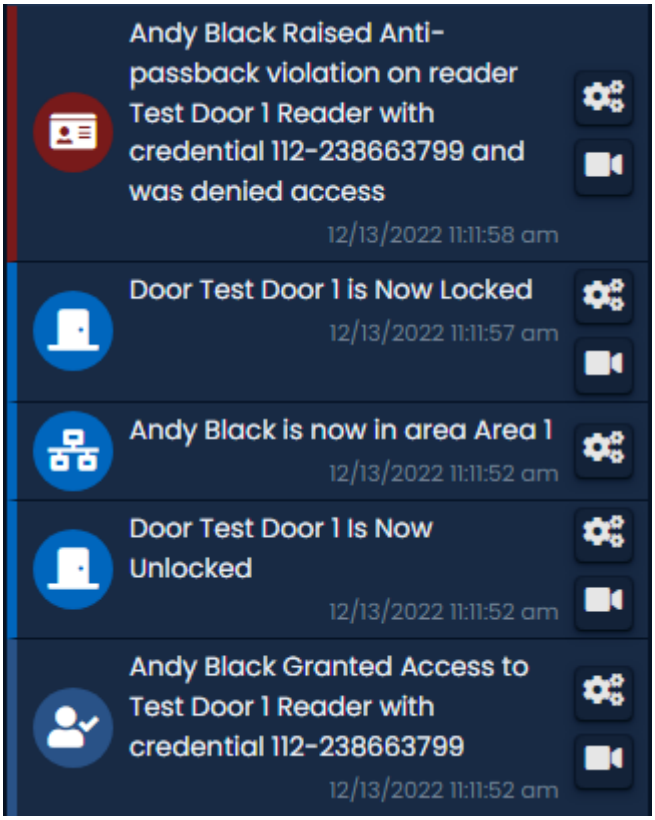
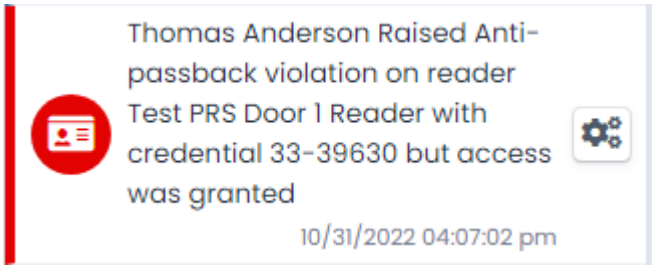


Figure 21.7. APB Violations Soft APB



Chapter 22. Mantrap Configuration

This chapter covers the configuration of Mantraps in VAX. This feature is available in version 3.1+ and is only supported on select Panel models and may require additional wiring in order to function.

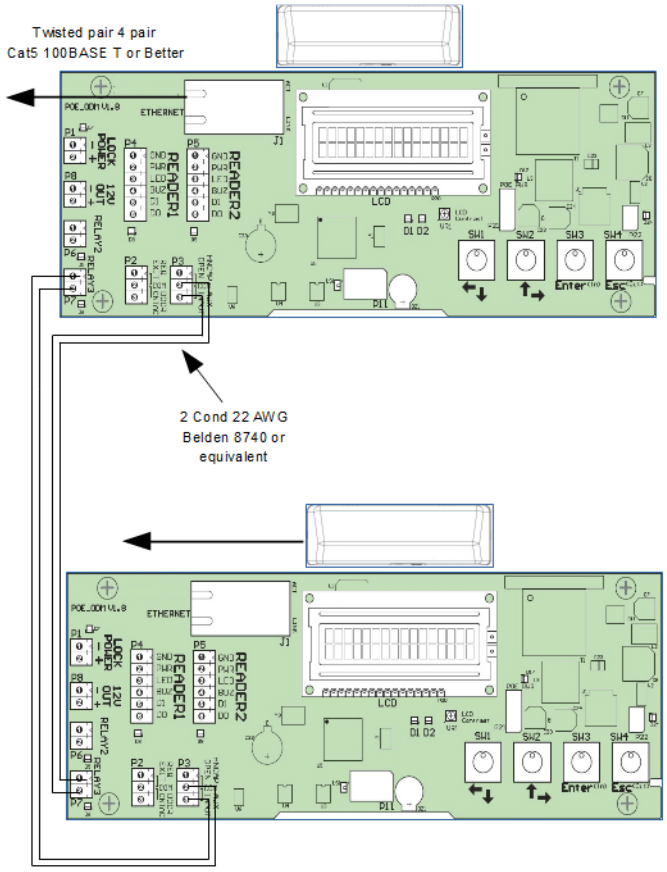
Mantrap (also called air lock or access control vestibule) is commonly used in high security areas where a cardholder enters an enclosed space between two (or more) doors. When the first door is opened or unlocked, the second door will receive a signal from the opened door instructing it not to open or unlock. The second door will not allow passage through until the first door is closed. This works in reverse as well.

Mantrap Hardware Setup

Mantrap configuration is supported by multiple controllers (2 x VAX-1D-1 or 12VDC door controllers) and between two doors on a singleTwo-Door Panel (1 x VAX-2D-1).

Seperate Panel: This setup requires both Panels with doors in the mantrap to have 1 Available Output and 1 Available Input. An Output from each Panel will connect to an Input on the other Panel in the Mantrap configuration. Please see the diagram below.

Figure 22.1. Seperate Controller Mantrap



Once the above diagram has been implemented, use the following steps to configure the Input/Outputs.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.

3. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Panels** icon (pictured below).

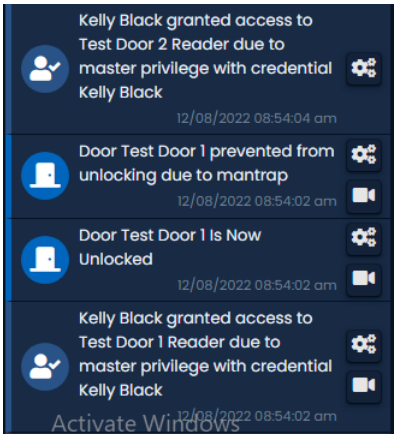
4. Click the **blue** button (Advanced Settings) next to the Panel you'd like to configure.

5. On the **Edit Panel** screen, you'll see 4 tabs. Click the **I/O** tab. We can now configure the Input that will signal the door not to open or grant access, and the Output that will signal the other door that the door on this Panel is open or unlocked.

6. Select the Input that will be receiving a signal from the Panel when another Door in the Mantrap configuration is unlocked or open. Change the Function drop-down menu to "Door Prevent Unlock".

7. Select the Output the Panel that will be signaling the other Panel. Change the Function drop-down menu to "Door Unlocked or Open".

8. Your I/O screen should look very similar to the example below:



9. Press the **Save**button on the bottom of the screen. Perform a Panel Update and begin testing.

   Repeat this process on any additional Panels that will be participating in the Mantrap.

Both Doors on Same VAX-2D-1 Configuration: This setup does not require any additional Inputs or Outputs to function when using a Two-Door Panel. We only need to configure a software setting in order for both doors to behave in the same manner as two Single-Door controllers linked together.

Once both Doors have been added to the Panel, use the following steps to enable Mantrap functionality.

1. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Doors** icon (pictured below).

2. On the **Doors** screen, you'll see any Doors you've already configured listed here. Click the blue button next to one of the Doors that will be using the Mantrap.

3. On the **Edit Door** screen, you'll see 5 tabs. Click on the **Options** tab.

4. On the **Options** tab there will be a check box labeled "Prevent Unlock if Paired Door Open". Ensure it is checked.

5. Press the **Save** button on the bottom of the screen. Perform a Panel Update and begin testing.

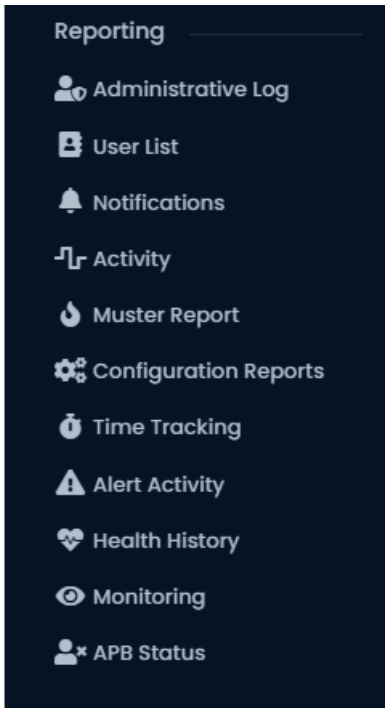
Chapter 23. Reporting

This chapter will be an overview of the various reporting features in VAX. These reports can be useful for tracking Users, Doors, Floors, past Notifications and Administrators. Each section in this chapter will cover one of the items in the reporting category on the Home page.

Table 23.1. VAX Reports

Administrative Log Report	User List Report
Notifications Report	Door Activity Report
Muster Report	Floor Activity Report
Elevator Activity Report	User Activity Report
Input Activity Report	Output Activity Report
Configuration Reports	Action Plan Activity Report
Alert Activity Reports	Alarm Partitions Activity Reports

Figure 23.1. Reporting Options



Administrative Log

This section covers what the Administrative Log is and how to run it in VAX.

The Administrative Log is a report used for tracking the activities of other Administrators in VAX. This report allows you to see what settings other Administrators have changed, and when the Administrator made that change. Options for exporting the report are also available.

Note

Only Administrator accounts with the System Admin privilege will have access to run this report. For more information on system admin privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to run an Administrator Log report:

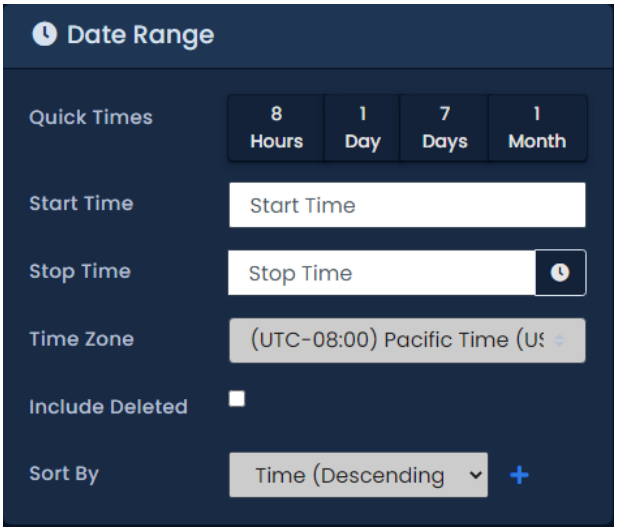
1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Administrative Log** icon (pictured below).

2. Once on the **Administrative Log** screen, you'll have 3 sections to populate:

   a. **Date Range:** Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to select the date & time to start/stop the report.

   You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

Figure 23.2. Date Picker Widget

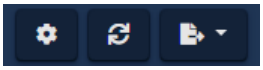


   b. **Administrators:** Select the Administrators you'd like to run the report against. You can select more than one at a time, or just an individual Administrator.

   c. **Output:** Choose the Output format of the report. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

3. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

User Activity

This section covers what the User Activity Report is and how to run it in VAX.

This report allows you to see what Doors, Floors and Readers a User account has been in contact with, including access granted and access denied. Options for filtering, sorting and exporting the report are also available.

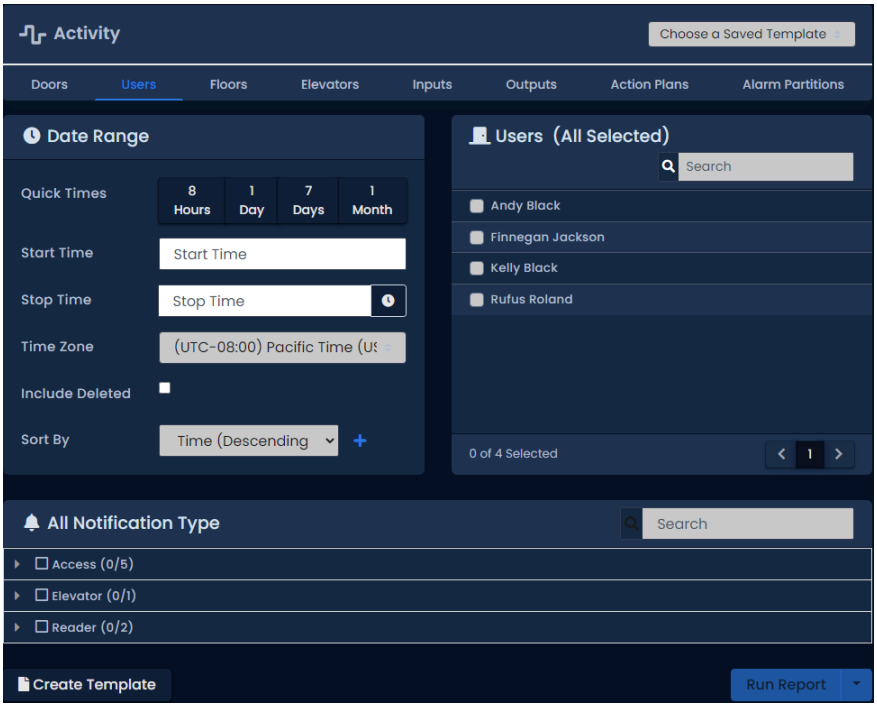
Note

Administrators who are not System Admins will require the **User Activity** Administrator privilege turned on; only Users in that Partition will be visible to the Administrator. For more information on Administrator Privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to run a User Activity Report:

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Activity** icon (pictured below).

2. Select **Users**from the list of option at the top of the Activity page.

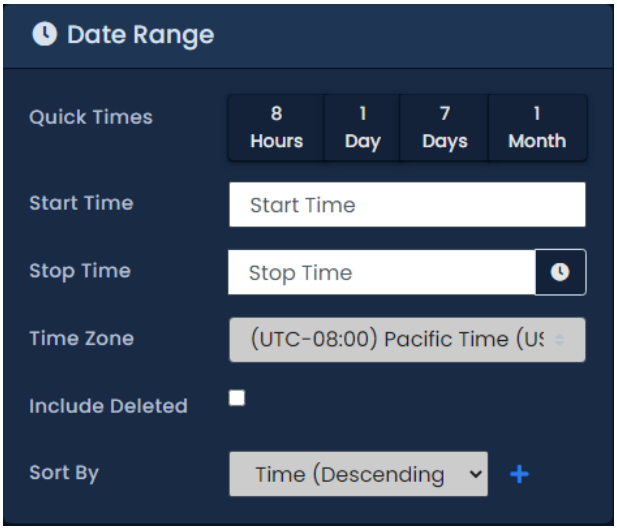


3. Once on the **User Activity** screen, you'll have 5 sections to populate.

   a. **Date Range:** Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to select the date & time to start/stop the report.

      You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

Figure 23.3. Date Picker Widget



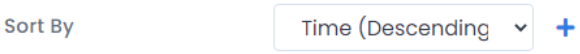
b. **Users:** Select the Users you'd like to run the report against. You can select more than one at a time, or just an individual User. The search bar can be used to find Users quickly.

c. **Notification Types:** You can filter which notifications appear in the report in this section. All notification types are selected by default. You can filter Access Denied, Anti-passback violations and many other filters.

Figure 23.4. Notification Types

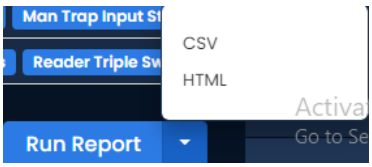
d. **Sorting:** You can configure how the results of the report will be sorted. Default is Time Descending. You can sort by multiple factors simultaneously.

Figure 23.5. Sorting



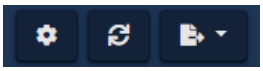
e. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.6. Run Report



4. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

Information that is presented on exported User Activity Reports includes the following:

- **Time:** The date & time of the event.
- **Site:** The Site the event occurred on.
- **User:** The first and last name of the User the event is associated with.
- **Card Number:** The Credential (PIN or Card) that the User used with the event.
- **Device 1:** The Reader or Floor the event occurred on.
- **Device 2:** The Door or Elevator attached to Device 1.
- **Message:** Additional information about the event, such as Access Granted/Access Denied, the User, Credential, Reader or Floor.

Door Activity

This section covers what the Door Activity Report is and how to run it in VAX.

The Door Activity Report is used for tracking the activities of Doors in VAX. This report allows you to see what Doors have been doing, when they were opened, when they were unlocked and what Users were granted access or denied to these Doors. Options for exporting the report are also available.

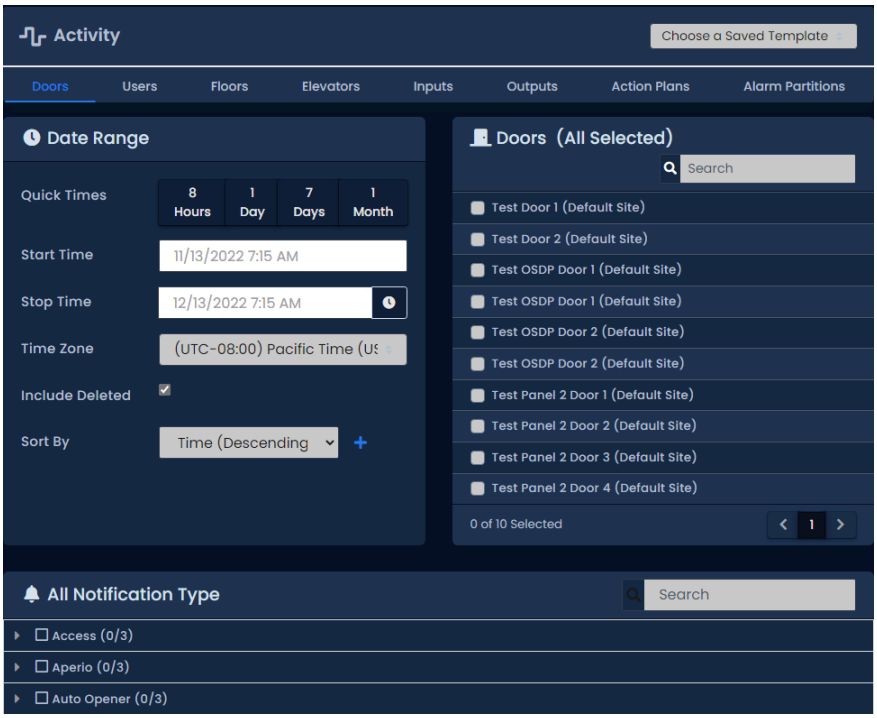
Note

Administrators who are not System Admins will require the **Reporting Door Activity** Administrator privilege turned on; only Doors attached to Panels in that Partition will be visible to the Administrator. For more information on Administrator privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to run a Door activity report:

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Activity** icon (pictured below).

2. Select **Doors**from the list of option at the top of the Activity page.

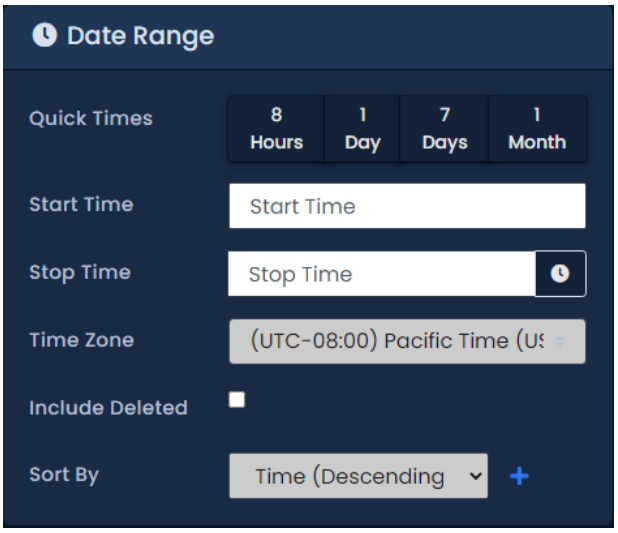


3. Once on the **Door Activity** screen, you'll have 5 sections to populate.

   a. **Date Range:** Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to pick the date & time to start/stop the report.

      You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

Figure 23.7. Date Picker Widget



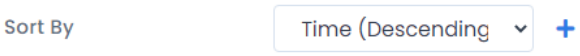
   b. **Doors:** Select the Doors you'd like to run the report against. You can select more than one at a time, or just an individual Door. The search bar can be used to find Doors quickly.

   c. **Notification Types:** You can filter which notifications appear in the report in this section. All notification types are selected by default. You can filter Door Forced open, held open and many other filters.

Figure 23.8. Notification Types

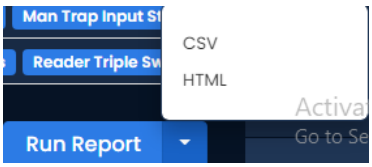
d. **Sorting:** You can configure how the results of the report will be sorted. Default is Time Descending. You can sort by multiple factors simultaneously.

Figure 23.9. Sorting



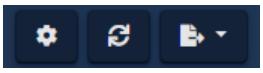
e. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.10. Run Report



f. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

Information that is presented on exported Door Activity Reports includes the following:

- **Time:** The date & time of the event.
- **Site:** The Site the event occurred on.
- **Door:** The name of the Door the event is associated with.
- **Reader:** The Reader the event is associated with.

- **User:** If a User is associated with the event, the first name and last name will be displayed here.
- **Card Number:** If a Credential was involved with the event, it will be displayed here.
- **Message:** Additional information about the event, such as Access Granted/Access Denied, the User, Credential, Reader and Floor.

Note

Overrides, exit buttons and OTRs will not have an entry in the Reader, User and Card Number category.

Floor Activity Report

This section covers what the Floor Activity Report is and how to run it in VAX.

The Floor Activity Report is used for tracking the activities of Floors in VAX This report allows you to see what Floors have been doing, when they were accessed, and what Users were granted or denied access to these Floors. Options for exporting the report are also available. This reports differs from the Elevator Activity Report in that it is focused on the floors rather than individual elevator cabs. You will not see user activity in this report if they are not using button sensing.

This report is focused on individual floors and will not display user activity if the elevator is not using Button Sensing. Use the Elevator Activity report instead if the elevator is not using button sensing. See Elevator Activity Report.

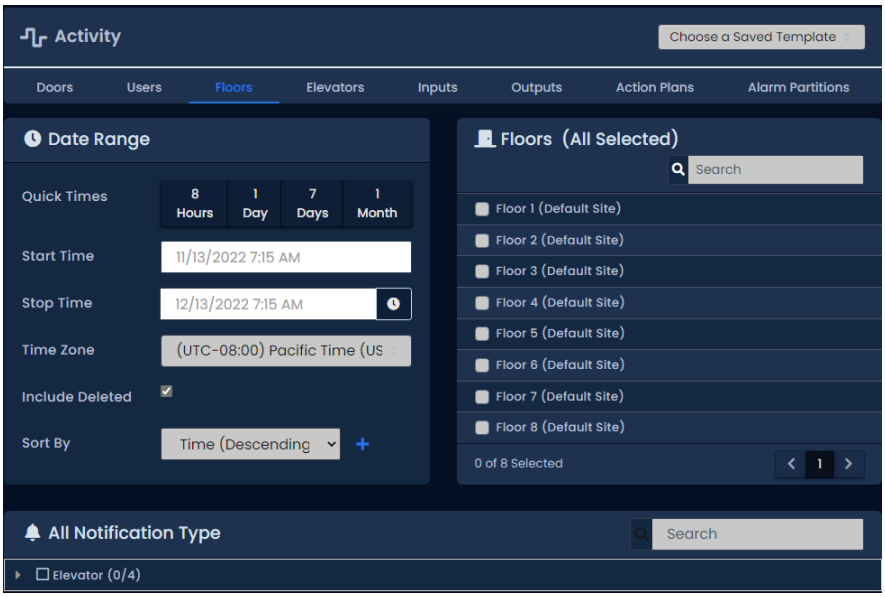
Note

Administrators who are not System Admins will require the **Reporting Floor Activity** Administrator privilege turned on; only Floors attached to Panels in that Partition will be visible to the Administrator. For more information on Administrator Privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to run a Floor activity report:

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Activity** icon (pictured below).

2. Select **Floors**from the list of option at the top of the Activity page.

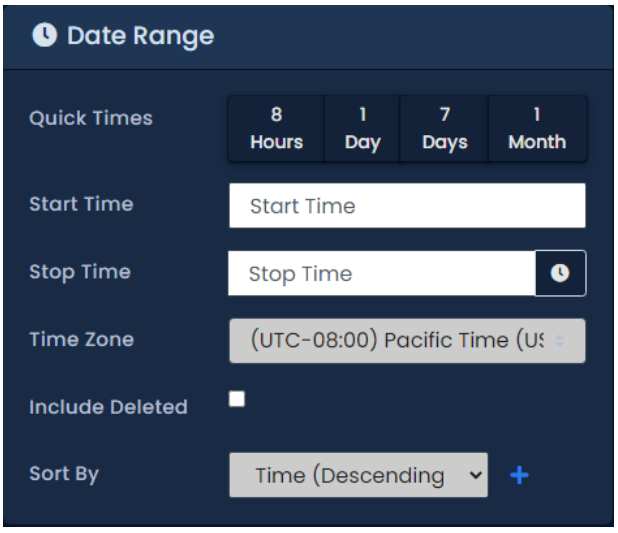


3. Once on the **Floor Activity** screen, you'll have 5 sections to populate.

   a. **Date Range:** Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to pick the date & time to start/stop the report.

      You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

Figure 23.11. Date Picker Widget



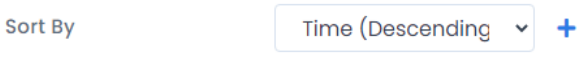
   b. **Floors:** Select the Floors you'd like to run the report against. You can select more than one at a time, or just an individual floor. The search bar can be used to find Floors quickly.

   c. **Notification Types:** You can filter which notifications appear in the report in this section. All notification types are selected by default. You can filter Access Denied, Floor Overridden and many other filters.

Figure 23.12. Notification Types (more available)

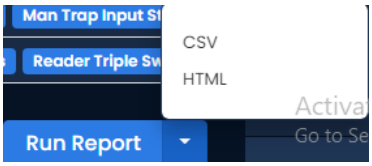
d. **Sorting:** You can configure how the results of the report will be sorted. Default is Time Descending. You can sort by multiple factors simultaneously.

Figure 23.13. Sorting



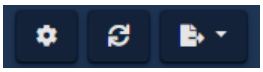
e. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.14. Run Report



f. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

Information that is presented on exported Floor Activity Reports includes the following:

- **Time:** The date & time of the event.
- **Site:** The Site the event occurred on.
- **Elevator:** The name of the Elevator the event is associated with.
- **Floor:** The name of the Floor the event is associated with.
- **User:** If a User is associated with the event, the first name and last name will be displayed here.
- **Card Number:** If a Credential was involved with the event, it will be displayed here.
- **Message:** Additional information about the event, such as Access Granted/Access Denied, the User, Credential, Reader and Floor.

Note

Overrides and OTRs will not have an entry in the User and Card Number category.

Elevator Activity Report

This section covers what the Elevator Activity Report is and how to run it in VAX.

The Elevator Activity Report is used for tracking the activities of elevator cabs in Vicon Access Control. This report allows you to see what cabs have been doing, when they were accessed, and what Users were granted or denied access to these cabs. Options for exporting the report are also available. This reports differs from the Floor Activity Report in that it is focused on the elevator cabs rather than individual floors.

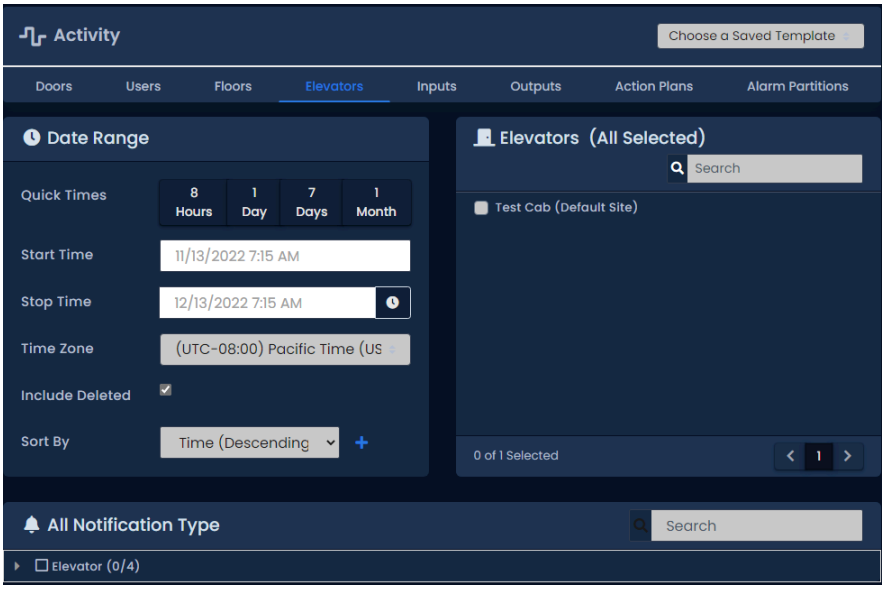
Note

Administrators who are not System Admins will require the **Reporting Elevator Activity** Administrator privilege turned on; only Elevators attached to Panels in that Partition will be visible to the Administrator. For more information on Administrator Privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to run an elevator activity report:

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Activity** icon (pictured below).

2. Select **Elevators**from the list of option at the top of the Activity page.

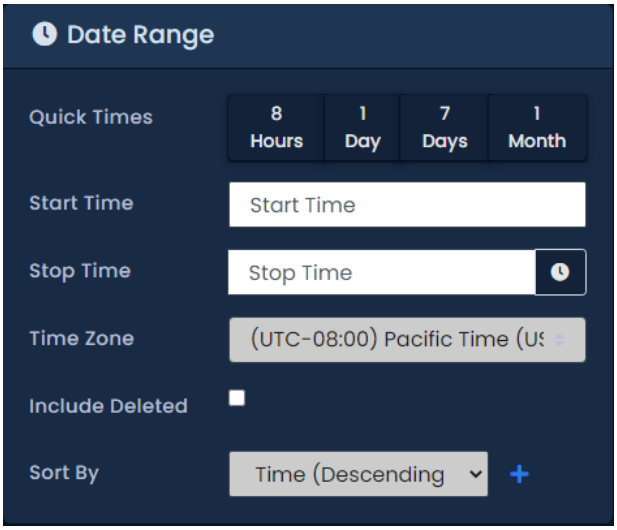


3. Once on the **Elevator Activity** screen, you'll have 5 sections to populate.

   a. **Date Range:** Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to pick the date & time to start/stop the report.

   You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

Figure 23.15. Date Picker Widget



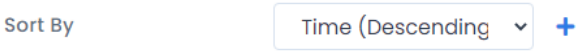
b. **Elevators:** Select the Elevators you'd like to run the report against. You can select more than one at a time, or just an individual cab. The search bar can be used to find Elevators quickly.

c. Notification Types: You can filter which notifications appear in the report in this section. All notification types are selected by default.

Figure 23.16. Notification Types

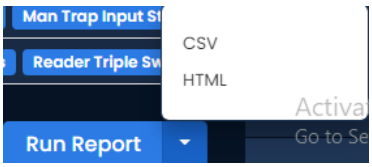
d. **Sorting:** You can configure how the results of the report will be sorted. Default is Time Descending. You can sort by multiple factors simultaneously.

Figure 23.17. Sorting



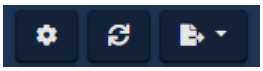
e. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.18. Run Report



f. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

Information that is presented on exported Elevator Activity Reports includes the following:

- **Time:** The date & time of the event.
- **Site:** The Site the event occurred on.
- **Elevator:** The name of the Elevator the event is associated with.
- **Floor:** The name of the Floor the event is associated with.
- **User:** If a User is associated with the event, the first name and last name will be displayed here.
- **Card Number:** If a Credential was involved with the event, it will be displayed here.
- **Message:** Additional information about the event, such as Access Granted/Access Denied, the User, Credential, Reader and Floor.

Note

Overrides and OTRs will not have an entry in the User and Card Number category.

User List

This section covers what the User List report is and how to run it in VAX.

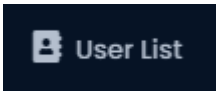
The User List Report is used to view all Users in the system (that you have permission to view). This includes Custom Fields, Permissions, Access Groups and more. Options for exporting the report are also available.

Note

Administrators who are not System Admins will require the **Reporting User List** Administrator privilege turned on. Only Users in that Partition will be visible to the Administrator in the User List. For more information on Administrator Privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to run the User List Report:

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **User List** icon (pictured below).



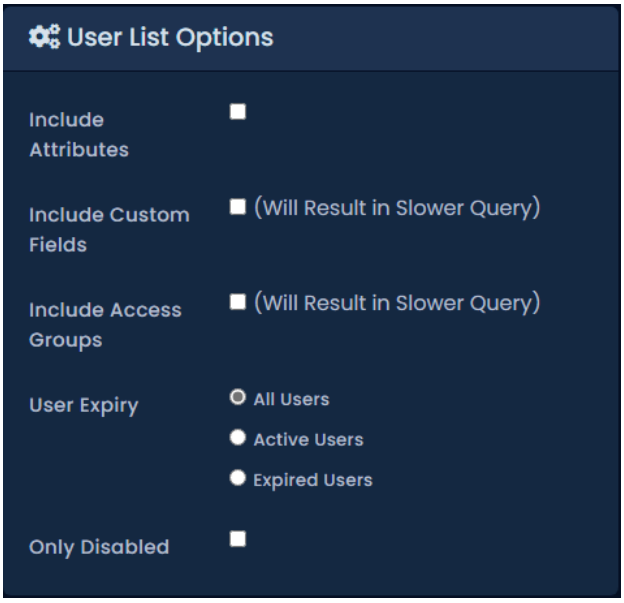
2. Once on the **User List** screen, you'll have 4 sections to populate.

   a. **User List Options:** Optional information can be selected to be included in the report results.

Table 23.2. Anti-Passback Configuration Items

User List Option	Description
Include Attributes	Permissions such as Triple Swipe, First Card In and Auto Opener will be included in the output of the report if selected.
Include Custom Fields	Custom fields will be included in the output of the report if selected. Will result in slower query.
Include Access Groups	The name of any Access Privilege Groups users are a part of what will be included in the output of the report if selected. Will result in slower query.
User Expiry	Allows you to filter Expired, Active or all users. All Users is selected by default.

Figure 23.19. User List Options



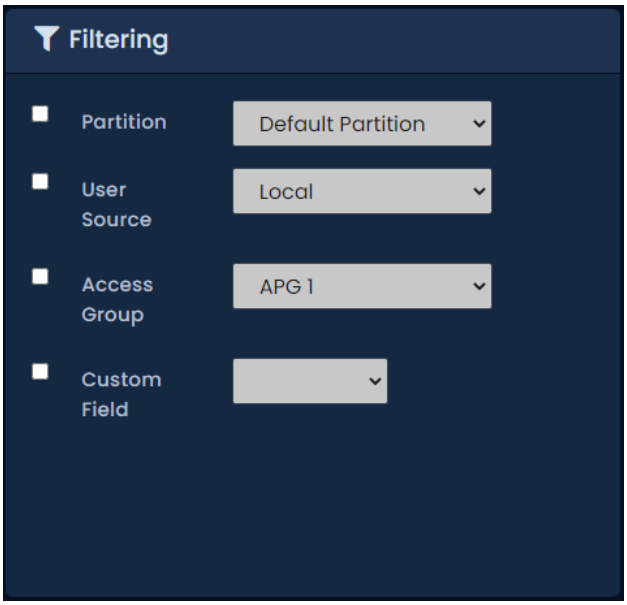
b. **Filtering:** You can further filter which Users appear in the report results here.

Table 23.3. Anti-Passback Configuration Items

User List Filter	Description
Partition	Check and select a Partition to filter the report to only include users in the selected Partition.
User Source	Check and select the source of the user origin. Select local for local system, or select LDAP for server integration
Access Group	Check and select an Access Group to filter the report to only include users in the selected Access Group.
Custom Field	Check and select a custom field. You can set the filter to 'Starts With', 'Ends With', 'Contains' or 'Equals'. Fill in a custom field

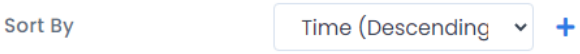
User List Filter	Description
	value to filter the report to only include Users that have the custom field based on your filter.

Figure 23.20. User List Filtering



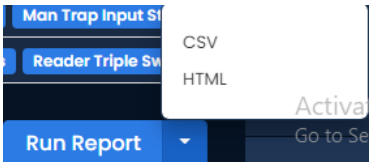
c. **Sorting:** You can configure how the results of the report will be sorted. Default is First Name, Last Name, Card number. You can sort by multiple factors simultaneously.

Figure 23.21. Sorting



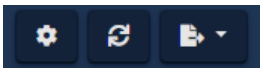
d. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.22. Run Report



e. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

Notifications Report

This section will cover what the Notifications Report is and how to run it in VAX.

The Notifications Report is used to view previous Notifications, such as Panels connecting, Doors opening, Users being granted/denied access, and many other Notification types. Options for exporting the report are also available.

Use the following steps to run a Notifications report:

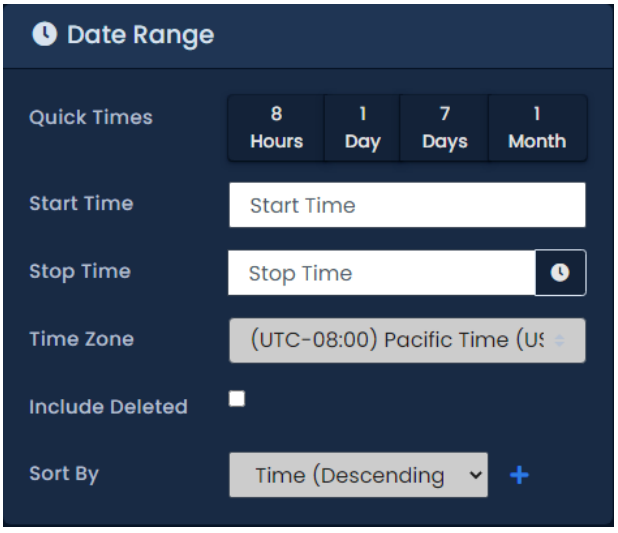
1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Notifications** icon (pictured below).

2. Once on the **Notifications** screen, you'll have 3 sections to populate.

   a. **Date Range:** Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to select the date & time to start/stop the report.

   You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

Figure 23.23. Date Picker Widget

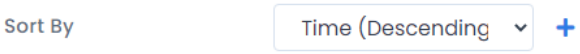


   b. **Notification Types:** You can filter which notifications appear in the report in this section. All notification types are selected by default.

Figure 23.24. Notification Types

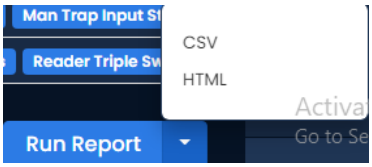
c. **Sorting:** You can configure how the results of the report will be sorted. Default is Time Descending. You can sort by multiple factors simultaneously.

Figure 23.25. Sorting:



d. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.26. Run Report



3. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.

Note

Depending on the size of the report, it may take several minutes to generate.

Information that is presented on exported Notifications Reports includes the following:

- **Time:** The date & time of the Notification.
- **Event:** Event type of the Notification.
- **Message:** Message associated with the event.

Muster Report

This section covers what the Muster Report is and how to run it in VAX.

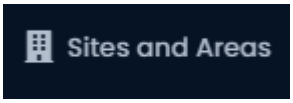
The Muster Report obtains a list of Users who are in particular areas based on what doors grant access to those areas. This report requires that Areas be configured on each site and the "Reader 1 Grants Access to Area" and "Reader 2 Grants Access to Area" fields on the Edit Door screen are populated for any doors there is a potential need to run this report against. Options for exporting the report are also available.

Note

Administrators who are not System Admins will require the **Reporting Muster** Administrator privilege turned on; only Doors attached to Panels in that Partition will be visible to the Administrator. For more information on Administrator privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to configure Areas and assign them to Doors:

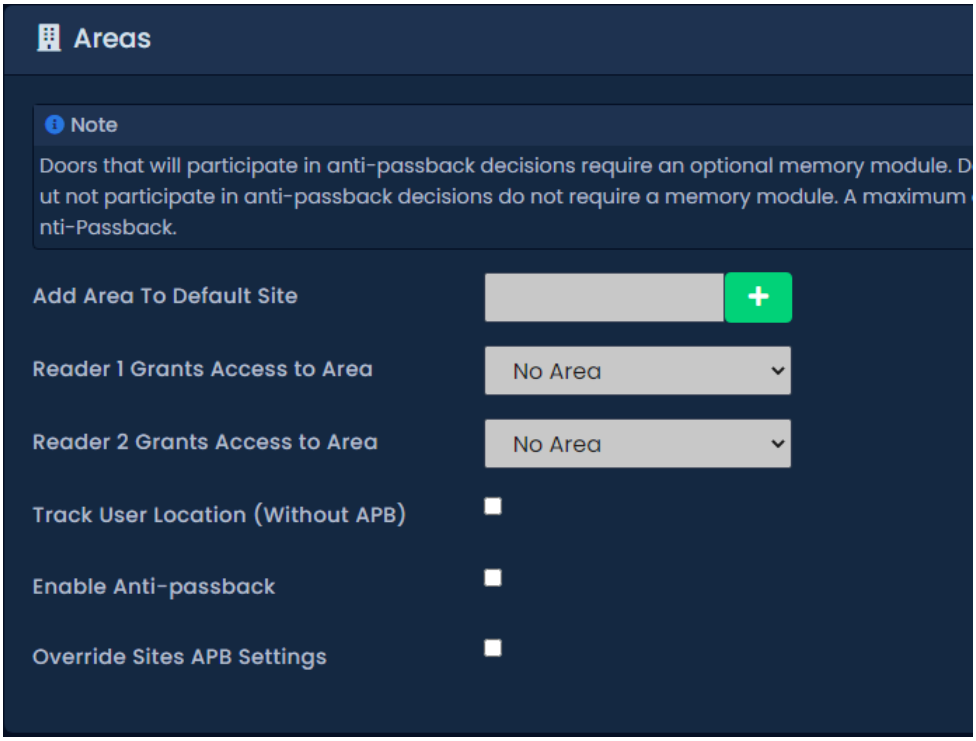
1. On the **Side Bar**, scroll down to the section titled **System**; click on the **Sites and Areas** icon (pictured below).



2. On the **Sites and Areas** screen, you'll see any sites you've created. Click the blue button (advanced settings) next to the Site you'd like to add Areas to.
3. On the Edit Site screen, click on the **Areas** tab.
4. On the **Areas** tab, enter a name for your new area and click the **Add Area** button on the right side. Add additional Areas as needed.
5. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Doors** icon (pictured below).

6. On the **Doors** screen, you'll see any Doors you've already configured listed here. Click the blue button next to the Door you'd like to configure Areas on.
7. On the **Edit Door** screen, you'll see 5 tabs. Click on the **Areas** tab. The configuration items on this screen are explained below.

Figure 23.27. Area Settings



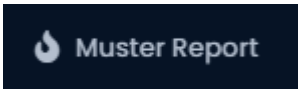
8. **Reader 1 Grants Access to Area:** The Area that Reader 1 grants access to. Select a custom Area or 'No Area'.

   Reader 2 Grants Access to Area: The Area that Reader 2 grants access to. Select a custom Area or 'No Area'. If there is no Reader 2, an area should still be selected.

9. Once you configure Areas on any additional Doors you should update the controllers or wait for the auto update timer to update them automatically.

Use the following steps to run a Muster Report:

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Muster Report** icon (pictured below).

2. Once on the **Muster Report** screen, you'll have 4 sections to populate.

3. **Date Range:**

   a. Select the **Start Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to select the date & time to start the report. The report will inquire for data between the Start Time and the current time.

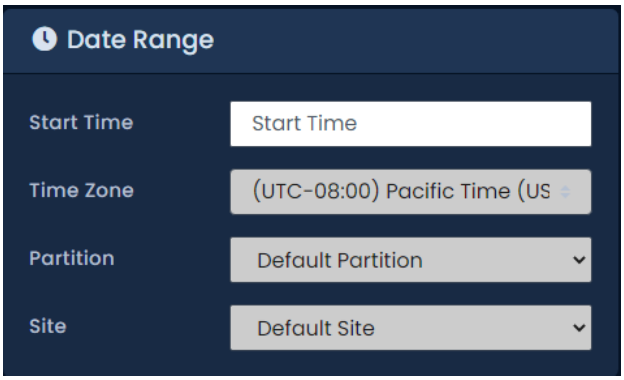
   b. Select the **Start Time** to indicate the time frame for the report to run.

   c. Select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

   d. Select the **Partition** that the areas reside in that you want to run the report against.

   e. Select the **Sites** that the areas reside in that you want to run the report against.

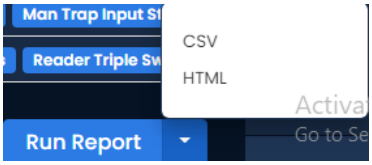
Figure 23.28. Date Picker Widget



4. **Areas:** Select the **Areas** you'd like to run the report against. You can select more than one at a time, or just an individual Area. The search bar can be used to find Areas quickly. By default, if no Areas are chosen, the report will run against all Areas in the selected Partition and Site.

5. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.29. Run Report



6. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

Information that is presented on exported Door Activity Reports includes the following:

- **Areas:** The name of the Area the User is currently in based on the last reader activity.
- **User:** The name of the User.
- **Reader:** The name of the last Reader the User was granted access to.
- **Last Activity:** The date and time of the last known activity involving the User.

Configuration Reports

Configuration Reports are a series of reports in VAX that let you export system information. This can include network information for all your Panels, names and schedule for all your doors, how your scheduless are configured and many more.

This section will cover where and how to run these reports and some information on each individual Configuration Report.

Note

Only Administrator accounts with the Reporting Configuration privilege will have access to run this report. For more information on Administrator privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to run any of the Configuration Report:

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Configuration Reports** icon (pictured below).

2. Once on the **Configuration Report** screen, you'll choose which Partition you'd like to run the report in (you can select more than 1) and which type of report you would like to run.

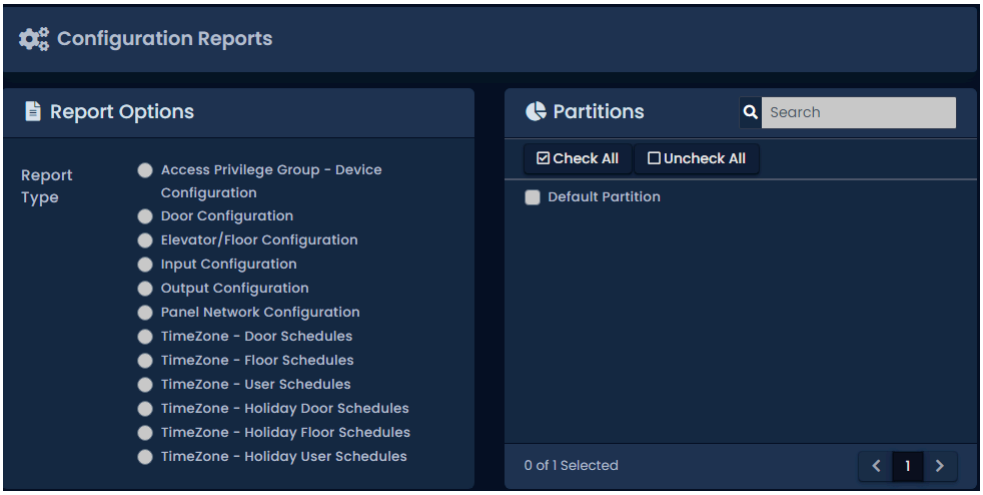
   The following table outlines each of the configuration reports:

Table 23.4. Configuration Reports

Report	Description
Access Privilege Group - Device Configuration	Will create an exportable list of all Access Privilege Groups in the selected Partitions, along with any Readers or Elevator floors in each group and the name of the User Schedule associated with each Reader/Floor.
Door Configuration	Will create an exportable list of all Doors in the selected Partitions along with the name of the Door Schedule and Holiday Group each door is using. Includes the names of any Readers associated with each Door and the name of which Door Controller each Door is attached to.
Elevator/Floor Configuration	Will create an exportable list of all Elevator Floors in the selected Partitions along with the name of the Floor Schedule and Holiday Group each door is using. Includes the names of any Readers associated with each Elevator and the name of which Elevator Panel each Elevator is attached to.
Input Configuration	Will create an exportable list of all Inputs attached to all Panels in the selected Partitions, including Door Panels and IO-Boards. Will list usage Input function, Name, Input Schedules, Holiday Groups and Actions for IO-Board Inputs.
Output Configuration	Will create an exportable list of all Outputs attached to all Panels in the selected Partitions, including Door Panels and IO-Boards. Will list Output function, Name, Output Schedule on IO-Boards and Holiday Groups.
Panel Network Configuration	Will create an exportable list of all Panels in the selected Partitions along with their network configuration and model name including: Connection mode, IP Address, Subnet Mask, Gateway and DNS.
Schedule - Door Schedules	Will create an exportable list of all Door Schedules in the selected Partitions along with the configured time spans and associated modes for each day of week.
Schedule - Floor Schedules	Will create an exportable list of all Floor Schedules in the selected Partitions along with the configured time spans and associated modes for each day of week.
Schedule - User Schedules	Will create an exportable list of all User Schedules in the selected Partitions along with the configured time spans and associated modes for each day of week.
Schedule - Holiday Door Schedules	Will create an exportable list of all Holiday Door Schedules in the selected Partitions along with the configured time spans and associated modes for each day of week.

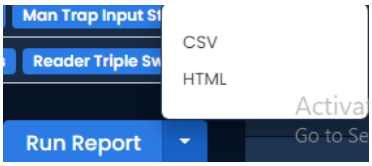
Report	Description
Schedule - Holiday Floor Schedules	Will create an exportable list of all Holiday Floor Schedules in the selected Partitions along with the configured time spans and associated modes for each day of week.
Schedule - Holiday User Schedules	Will create an exportable list of all Holiday User Schedules in the selected Partitions along with the configured time spans and associated modes for each day of week.

Figure 23.30. Configuration Reports Screen

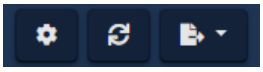


3. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.31. Run Report



4. Once you've run the report and the parameters are as desired, you can Output the report to a CSV or HTML file using the **Export** button drop-down menu on the right side of the Output tab.



Note

Depending on the size of the report, it may take several minutes to generate.

Input Activity

This section covers what the Input Activity Report is and how to run it in VAX.

The Input Activity Report is used for tracking the activities of Aux Inputs in VAX. This report allows you see when specific Inputs changed state, including Aux Inputs on Door Panels and IO-Panels. Options for exporting the report are also available.

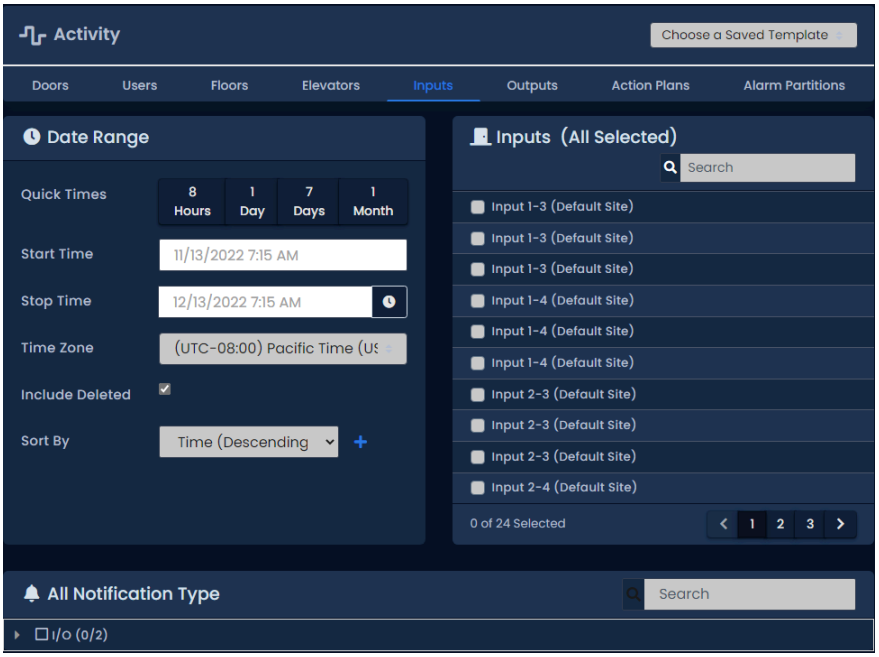
Note

Administrators who are not System Admins will require the **Reporting Input Activity** Administrator privilege turned on; only Inputs attached to Panels in that Partition will be visible to the Administrator. For more information on Administrator privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to run a Input activity report:

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Activity** icon (pictured below).

2. Select **Inputs**from the list of option at the top of the Activity page.

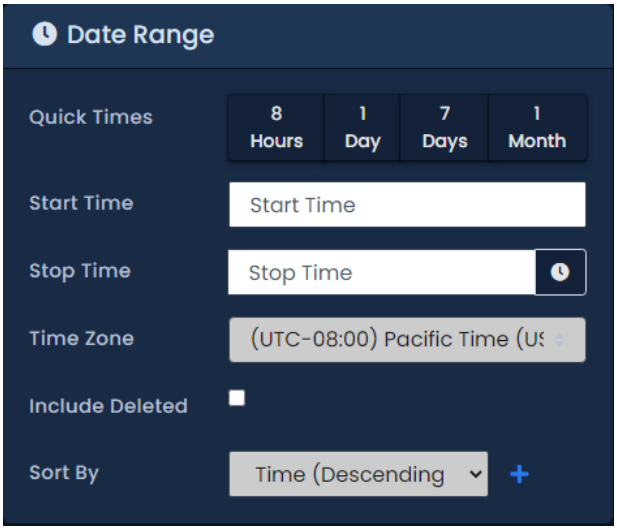


3. Once on the **Input Activity** screen, you'll have 5 sections to populate.

   a. **Date Range:** Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to select the date & time to start/stop the report.

   You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

Figure 23.32. Date Picker Widget



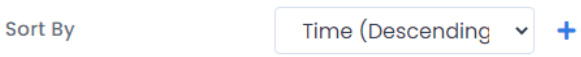
b. **Inputs:** Select the Inputs you'd like to run the report against. You can select more than one at a time, or just an individual Input. The search bar can be used to find Inputs quickly.

c. **Notification Types:** You can filter which notifications appear in the report in this section. All notification types are selected by default. You can filter Input Status Changed and several other filters.

Figure 23.33. Notification Types

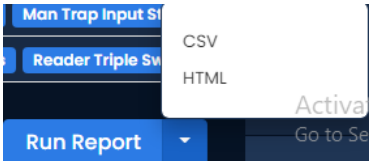
d. **Sorting:** You can configure how the results of the report will be sorted. Default is Time Descending. You can sort by multiple factors simultaneously.

Figure 23.34. Sorting



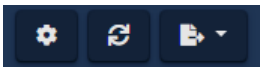
e. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.35. Run Report



4. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

Information that is presented on exported Input Activity Reports includes the following:

- **Time:** The date & time of the event.
- **Input:** The name of the Input the event is associated with.
- **Message:** Additional information about the event, such as "IO-Board Reports Input 1 Changed to Off".

Note

Only Inputs defined as "Aux Input" will appear in the list of selectable Inputs.

Output Activity

This section covers what the Output Activity Report is and how to run it in VAX.

The Output Activity Report is used for tracking the activities of Aux Outputs in VAX. This report allows you see when specific Outputs changed state, including Aux Outputs on Door Panels and IO-Panels. Options for exporting the report are also available.

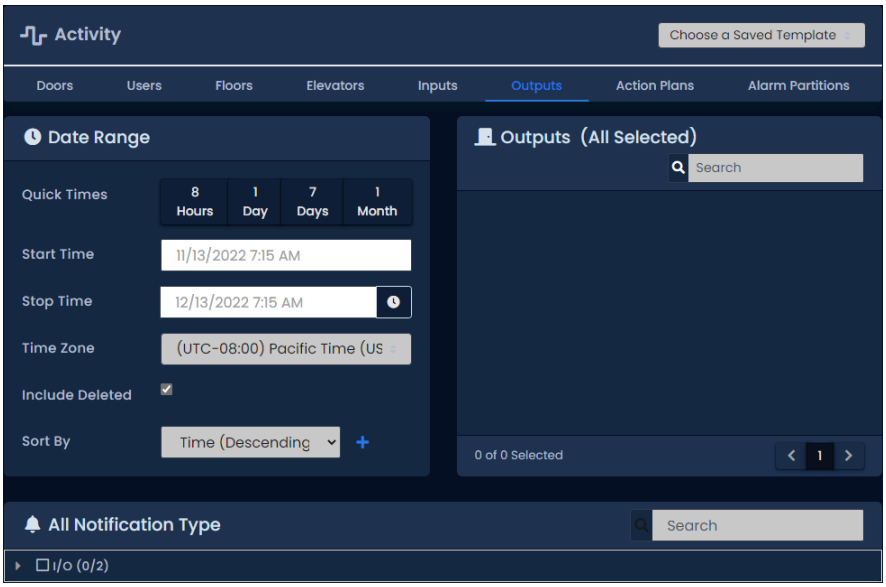
Note

Administrators who are not System Admins will require the **Reporting Output Activity** Administrator privilege turned on; only Outputs attached to Panels in that Partition will be visible to the Administrator. For more information on Administrator privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to run a Output activity report:

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Activity** icon (pictured below).

2. Select **Outputs**from the list of option at the top of the Activity page.

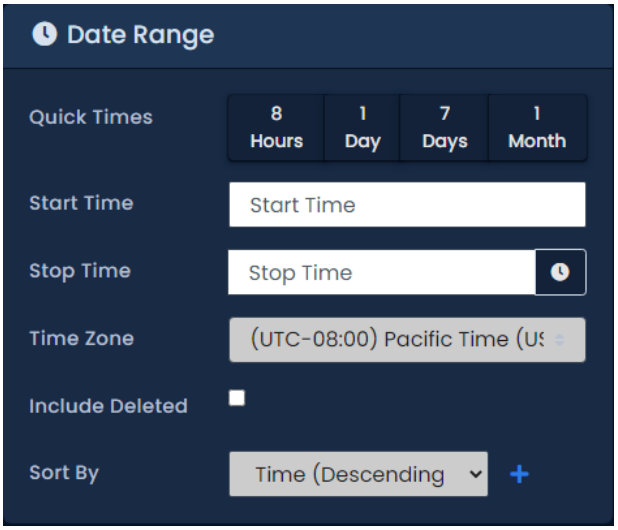


3. Once on the **Output Activity** screen, you'll have 5 sections to populate.

   a. **Date Range:** Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to select the date & time to start/stop the report.

   You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

Figure 23.36. Date Picker Widget



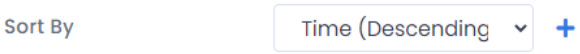
   b. **Outputs:** Select the Outputs you'd like to run the report against. You can select more than one at a time, or just an individual Output. The search bar can be used to find Outputs quickly.

   c. ` **Notification Types:** You can filter which notifications appear in the report in this section. All notification types are selected by default. You can filter Output Status Changed, Output Schedule Changed and several other filters.

Figure 23.37. Notification Types

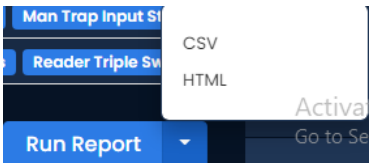
d. **Sorting:** You can configure how the results of the report will be sorted. Default is Time Descending. You can sort by multiple factors simultaneously.

Figure 23.38. Sorting



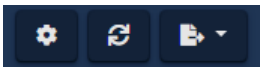
e. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.39. Run Report



4. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

Information that is presented on Aexported Output Activity Reports includes the following:

- **Time:** The date & time of the event.
- **Output:** The name of the Output the event is associated with.
- **Message:** Additional information about the event, such as "IO-Board Reports Output 1 Changed to Off".

Note

Only Outputs defined as "Aux Output" will appear in the list of selectable Outputs.

Action Plan Activity

This section covers what the Action Plan Activity Report is and how to run it in VAX.

The Action Plan Activity Report is used for viewing notifications generated by Action Plans utilized by ACE. Options for exporting the report are also available.

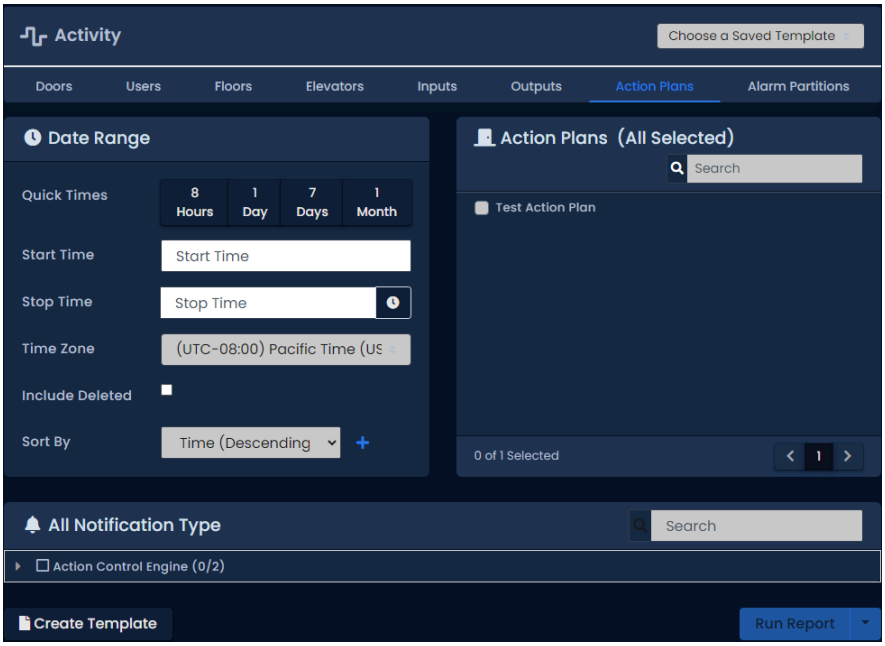
Note

Only Administrators who are System Admins can run this report.

Use the following steps to run a Action Plan activity report:

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Activity** icon (pictured below).

2. Select **Action Plans**from the list of option at the top of the Activity page.

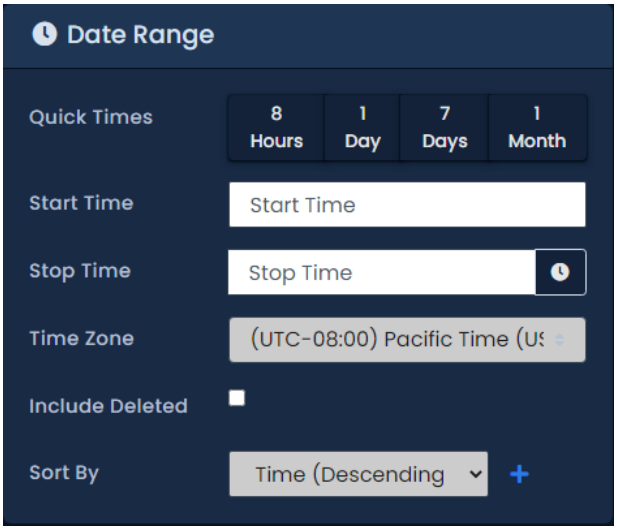


3. Once on the **Action Plan Activity** screen, you'll have 5 sections to populate.

   a. **Date Range:** Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to select the date & time to start/stop the report.

   You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

Figure 23.40. Date Picker Widget



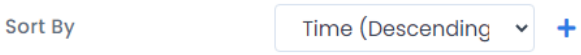
b. **Action Plans:** Select the Action Plans you'd like to run the report against. You can select more than one at a time, or just an individual Action Plan. The search bar can be used to find Action Plans quickly. All are selected by default.

c. **Notification Types:** You can filter which notifications appear in the report in this section. All notification types are selected by default. You can filter Action Plan Status Changed and several other filters.

Figure 23.41. Notification Types

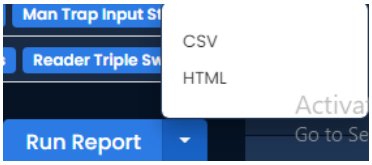
d. **Sorting:** You can configure how the results of the report will be sorted. Default is Time Descending. You can sort by multiple factors simultaneously.

Figure 23.42. Sorting



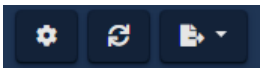
e. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.43. Run Report



4. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

Information that is presented on exported Action Plan Activity Reports includes the following:

- **Time:** The date & time of the event.
- **Action Plan:**The name of the Action Plan the event is associated with.
- **Message:** Additional information about the event, such as the content of a log action message.

Time Tracking

This section covers what the Time Tracking Report is and how to run it in VAX.

The Time Tracking Report is used for tracking how long users are in an area based on user credentials being used at specific readers. This information can be used for payroll and other purposes. Options for exporting the report are also available.

Note

Administrators who are not System Admins will require the **Reporting UserTimeTracking** Administrator privilege turned on; only Users who are members of that Partition will be visible to the Administrator. For more information on Administrator privileges, please see Chapter 20, *Administrators and Privileges*.

In order to properly utilize Time Tracking, ensure there are two credential readers located in such a way that users can present their credentials (cards, fobs, PINs) when entering/leaving the premises. This is important if you plan on using the time tracking report for payroll purposes.

Use the following steps to run a Time Tracking report:

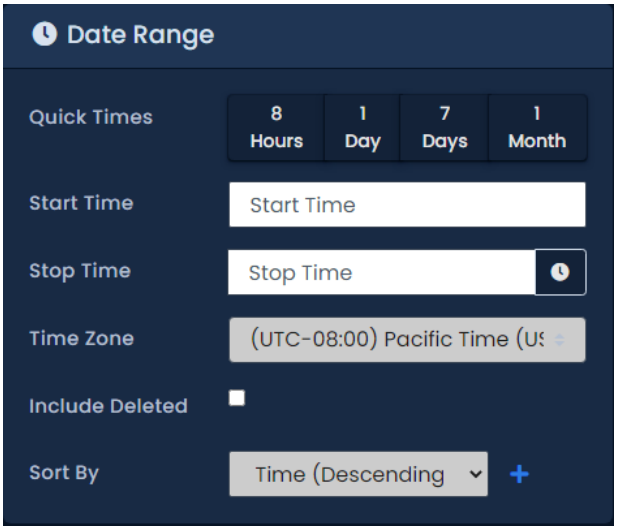
1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Time Tracking** icon (pictured below).

2. Once on the **Time Tracking** screen, you'll have 4 sections to populate.

   a. Saved Reports (templates): Report settings can be saved and recalled from this drop-down menu. This can save you from having to reselect options when running a report. Leave blank or select a saved template.

   b. Date Range: Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar to select the date & time to start/stop the report.

Figure 23.44. Date Picker Widget

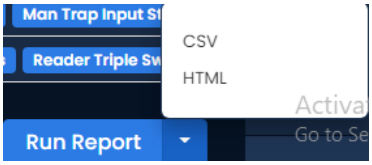


c. In Readers: Select one or more readers from the list. The selected readers will be referenced to track entry time on any users who have been granted access.

d. Out Readers: Select one or more readers from the list. The selected readers will be referenced to track exit time on any users who have been granted access.

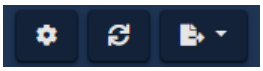
e. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.45. Run Report



3. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report or the results will start downloading.

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

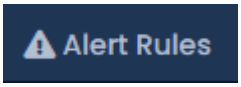
Alert Activity

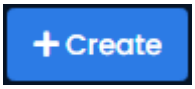
Alert Activity is used for tracking the activity of system alerts in VAX. This Report will provide the administrator with a list of messages with dates that reflect the alert notification rules that was set prior to the alert event. Messages are able to be added to the alerts for acknowledgement and administrator personal records.

Note

Administrators who are not System Admins will require the **Reporting Alert Activity** Administrator privilege turned on. For more information on Administrator Privileges, please see Chapter 20, *Administrators and Privileges*.

Use the following steps to setup a Alert Activity Notification rule:





Note

Alert Activity will only poplulate after the alert notification rules are created.

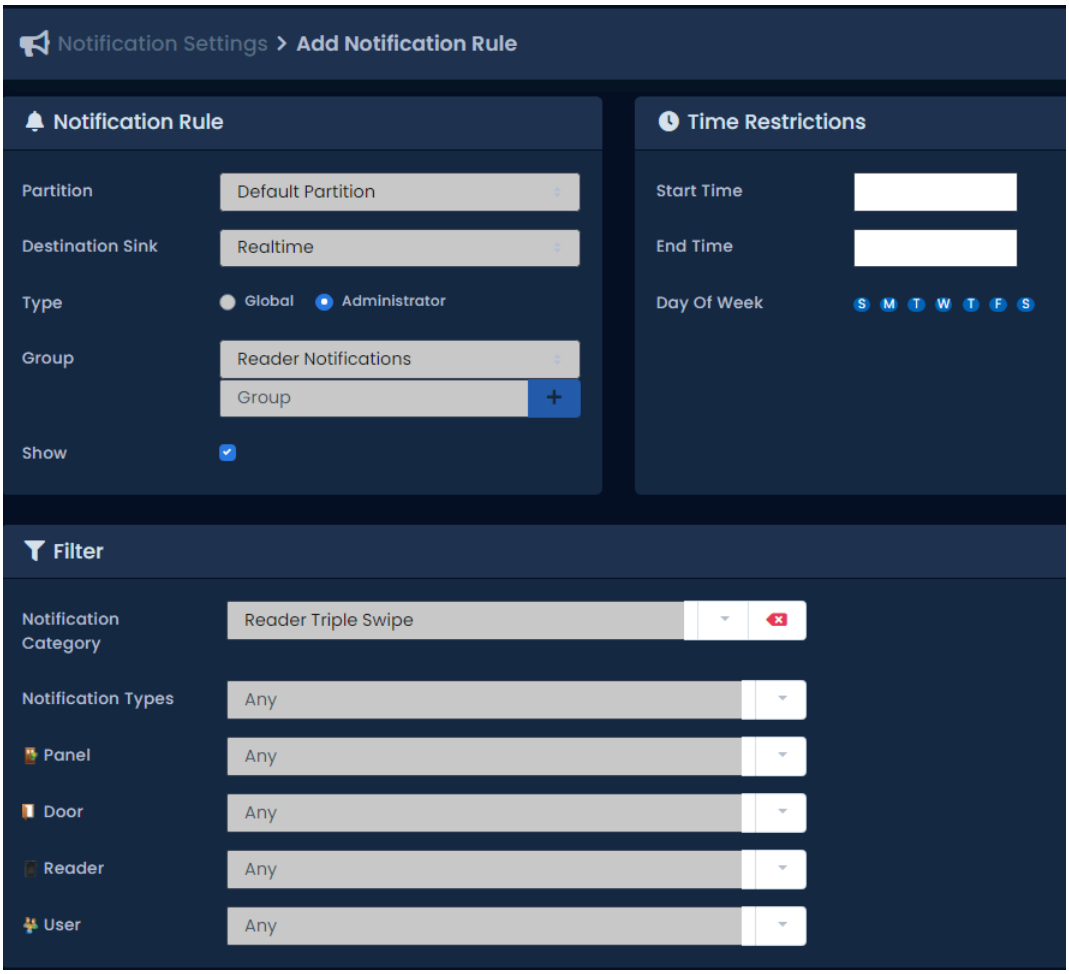
1. On the **Side Bar**, scroll down to the section titled **Administration**; click on the **Notification Settings** icon (pictured below).

2. At the top of the page there will be 5 setting options to choose from. Select **Alert Rules**(pictured below) .

3. Select the +buttom to add a new rule.

4. Once on the **Add Alert Rule**screen, The **Alert Rule** section, and the **Acknowledgements**section needs to be completed. The **Rule**and **Time Restrictions**sections can be complete as needed.



Note

Multiple Acknowledgements can be created by selecting the + **New Acknowledgement**button. Each acknowledgement will have the option to select: Any, Group, Administrator, and if a supervisor is required.

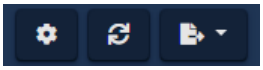
5. After all sections are complete, the rule can be created by selecting the + **Create**Button. (pictured Below)

Use the following steps to run a Alert Activity Report:

Once on the **Alert Activity** screen, you'll have 3 sections to populate.

1. On the **Side Bar**, scroll down to the section titled **Reporting**; click on the **Alert Activity** icon (pictured below).

If you'd like to change the parameters of the report, you can switch back to the Parameters by clicking the Gear icon. You can refresh the results of the report with the refresh button. You can export the report from the inline results using the export button.



Note

Depending on the size of the report, it may take several minutes to generate.

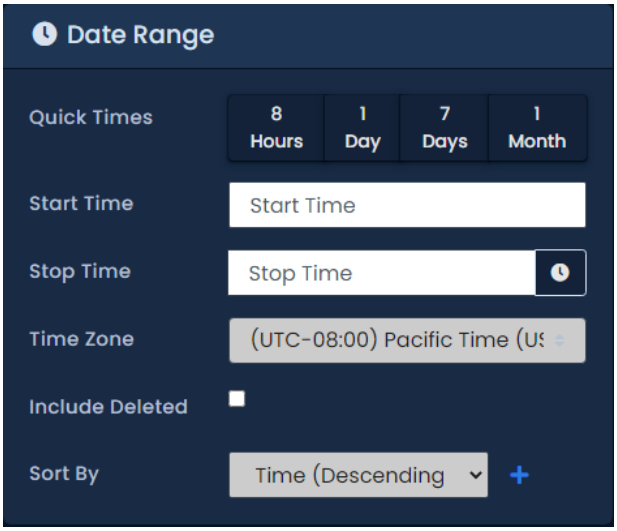
Information that is listed on a generated report are as follows:

- **Date:** The date and time of the Alert.
- **Message:** The initial notification along with the acknowledgement message.

1. **Date Range:** Select the **Start Time** and **Stop Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to select the date & time to start/stop the report.

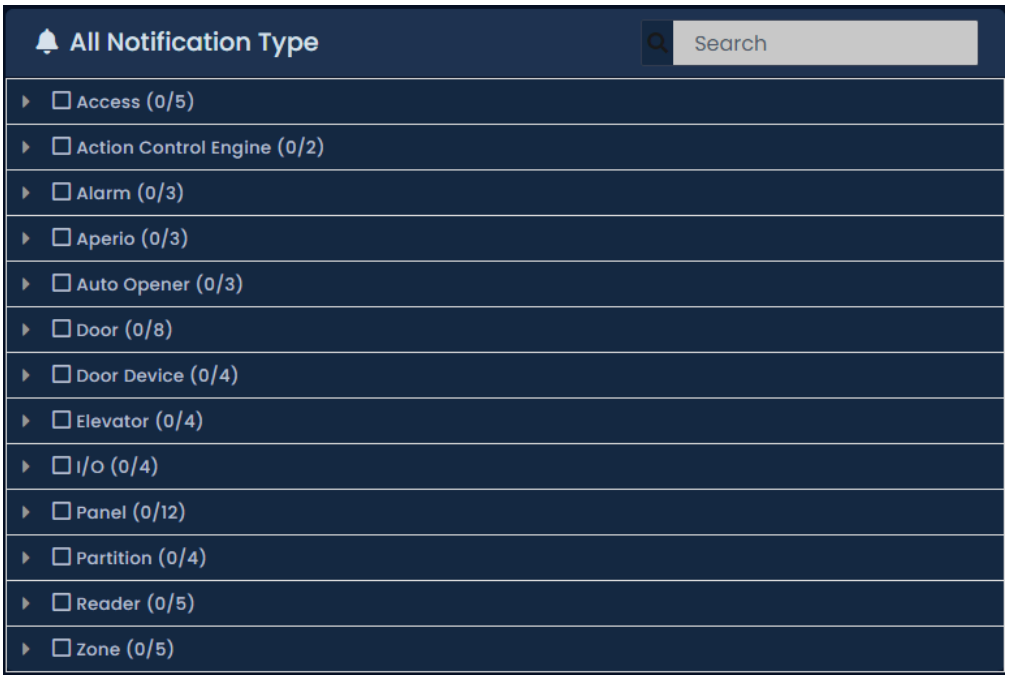
   You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

   Figure 23.46. Date Picker Widget

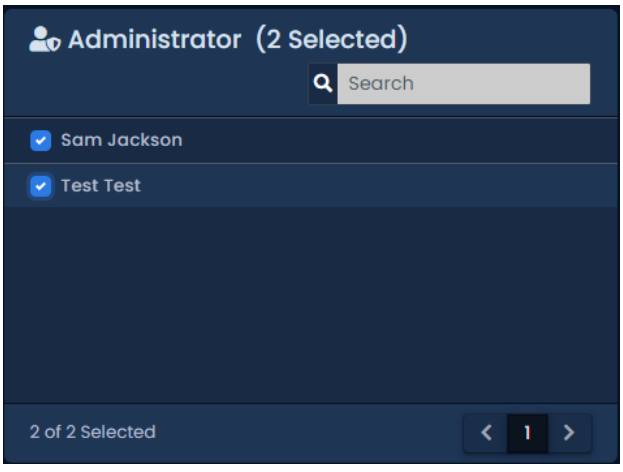
2. **All Notification Types:** You can filter which notifications appear in the report in this section. All notification types are selected by default.

Figure 23.47. Notification Types



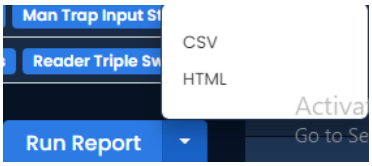
3. **Administrators:** You can select which Administrator was logged in for the report. All are selected by dedault

Figure 23.48. Administrators:



4. **Output:** Choose the Output format of the report from the **Run Report**dropdown list. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.

Figure 23.49. Run Report



5. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the results of the report.

Note

Acknowledegments can be viewed and a message can be created in the **Alerts**screen by selecting the Alerts Icon at the top of the VAX screen.. (pictured below)

Alarm Partitions

Alarm Partitions activity is used for tracking the Alarm system that is integrated into VAX

Note

Only Administrator accounts with the Reporting Configuration privilege will have access to run this report. For more information on Administrator privileges, please see Chapter 20, *Administrators and Privileges*.

Chapter 24. Notifications

Devices in VAX such as Panels, Doors or Readers generate notifications about various status changes and actions that occur. Notifications are sent in real time from the panel to the server. Offline panels will store up to 50,000 events, deleting on a first-in-first-out basis once full. VAX processes every notification through a series of rules for each destination to accept or reject it. Notifications can be configured to be shown in real time on the web interface, emailed to Administrators, pushed to devices using Web Push and stored in the database for reporting.

Destinations

There are four destinations that accept notifications: Real Time, Email, Web Push and Database. Each destination has its own set of rules that determine whether a notification will be accepted or rejected.

Real Time

In the VAX web interface, Administrators are shown notifications in real time as they are received. Depending on screen size, they are either shown on the right sidebar, from a drop down at the top of the page, or on a dedicated page on mobile. The Monitoring Screen provides a full screen view of notifications in real time, allowing for easy photo verification at guard stations or concierge desks.

Email

When VAX receives a notification, it can be configured to send that notification in an email to all or specific Administrators. A single email is sent per notification, with each recipient addressed using BCC (Blind Carbon Copy). An example of the email sent is pictured below.

Web Push

Web Push allows VAX to push notifications to your web browser, even when it's not focused or even open in the browser. Web Push requires confirmation in the browser to allow VAX permission to send push notifications. VAX encrypts the notification and sends it to a browser manufacturer (Google, Mozilla, Microsoft) push server. The push server sends the notification to the browser, which displays the notification. Notification appears in system or browser notification tray depending on the device and browser.

Prerequisites

Web Push requires a valid SSL certificate to function; self-signed certificates are only supported by Firefox. The following web browsers currently support Web Push:

Table 24.1. Supported Browsers

Browser	Minimum Version
Windows	
Chrome	Version 50 or higher
Firefox	Version 44 or higher
Edge	Version 17 or higher
Opera	Version 42 or higher
Mac/Linux	
Chrome	Version 50 or higher

Android	
Chrome	Version 81 or higher
Firefox	Version 68 or higher

Subscribing to Web Push

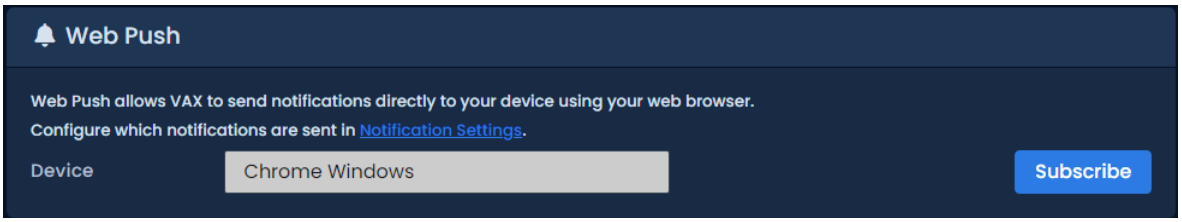
Administrators can subscribe to one or more web browsers to receive Web Push notifications on the **Web Push** tab of the **Administrator Settings** page.

To subscribe a web browser to receive push notifications:

1. Open **Administrator Settings** under the System section of the Home page.

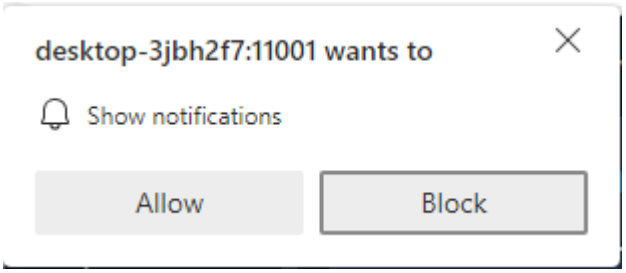
2. Open the **Web Push** tab at the top of the page.

3. You may enter a **Device** name to help identify browser subscriptions in the list below.



4. Click **Subscribe**

5. The browser will prompt you to allow VAX to send push notifications.



6. Once allowed, your subscriptions will be added to the list below and an option to Unsubscribe will appear instead.

Database

When VAX receives a notification, by default it will store all notification types except Reader Credential Errors in the database to allow historical reporting.

Notification Settings Page

The **Notification Settings** page allows you to manage the rules that decide where notifications are sent, stored and styled. Administrators require the **Manage Notification Rules** permission to view this section. Adding or editing global rules requires **System Admin** permission.

Notification Rules

Every notification is processed against a list of Notification Rules for each destination. The first rule that matches the notification for each destination determines whether the destination should accept or reject the notification.

Destinations

In VAX, notifications can be sent or stored to different destinations. Each destination has its own set of rules that decides whether to accept or reject each notification.

- **Realtime:** Shown in real-time on the web interface.
- **Email:** Emailed to all or specific Administrators.
- **Web Push:** Pushed to browsers of all or specific Administrators.
- **Database:** Stored in database for historical reporting.

Types

Notification Rules can apply to either all Administrators in the Partition or a specific Administrator.

- **Global:** Rule applies to all Administrators in Partition.
- **Administrator:** Rule applies to specific Administrator who created rule.

Administrator type rules are higher priority and are processed before any Global type rules.

Note

This does not apply to Database rules, which are always global.

Groups

Notification Rules for the Realtime destination can be overridden using Rule Groups. Rule groups can be selected on the Notification Sidebar and the Alert Monitoring page. Once selected, new notifications are processed against the rules in the group to determine whether to be shown on that page.

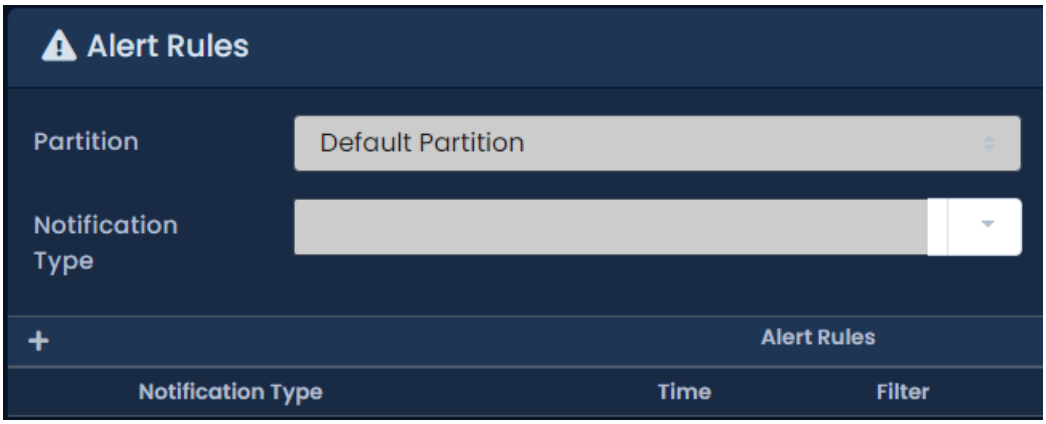
Accessing the Notification Settings Screen

On the **Side Bar**, scroll down to the section titled **System**; click on the **Notification Settings** icon (pictured below).

There are three sections on the Notification Settings page:

- **Rules:** List of rules for each destination.
- **Styles:** Rules that customize the sound, color and image on real time notifications.
- **Live Camera:** Rules that determine whether live camera stream should be shown.

The **Partition** and **Notification Type** options allow you to select a type of notification that will be displayed and from which partition. With the **Notification Type** blank, all notifications will be displayed. (pictured below)



Rules List

In the Rules section, there is a list of rules for each destination of a notification. Each list of rules is shown in the order in which they are processed. Rule priority can be changed by clicking and dragging a rule above or below another rule.

Note

Administrator rules will always have higher priority than Global rules and cannot be re-ordered below Global rules and vice versa.

Creating a Notification Rule

1. Use the +**Add** button (pictured below) next to the **Destination** you would like created. **Realtime**, **Email**, **Web Push** and **Database** are available options. This will bring you to **Add Notification Rule** screen.

2. The **Partition** and **Destination Sink** should already be selected based on the previous screen. A rule must be associated to a Partition and a Destination.

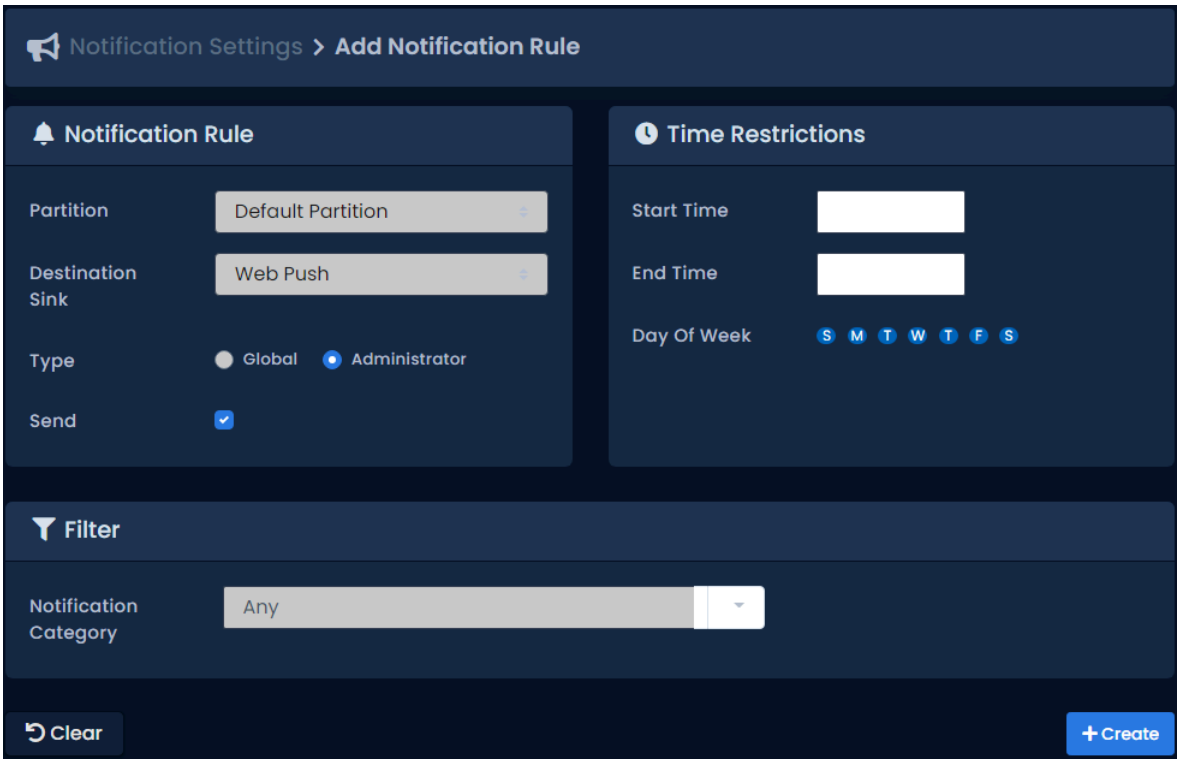
3. Choose whether the new rule will affect all Administrators in Partition (Global) or the specific Administrator adding the rule (Administrator).

Note

Only system admins can create Global rules.

4. For Realtime rules, a Group may be selected or created. **Groups** can be selected to filter notifications shown on the real time interface.

5. The **Accept** field decides whether this rule should allow the notification to be sent to the Destination or if it should reject it. Unchecking Accept will mean the destination will not receive the notification if matched.



6. Notification Rules can specify certain notifications or devices to match. By default, a rule will apply to all notifications unless a Filter is specified. A **Notification Category** can be selected in the drop-down. When a Notification Category is selected, additional Filter options may appear to further limit the rule.

7. Time Restrictions can be implemented in order to restrict when the rule should be active. The rule will only match notifications that occur within specified time frame.

8. Select Save to save your configuration. You will now be able to view your **Notification Rule** in the **Notification Settings** screen. The new rule will immediately apply to all subsequent notifications received. Previous notifications will not be impacted by the new rule.

Notification Styles

Notification Styles change how notifications appear on the Sidebar Notifications and Alert Monitoring pages. Styles can change various aspects of a notification, including:

- **Background Color:** Change the background color of the notification.

- **Notification Sound:** Upload an MP3 to be played when notification occurs.
- **Notification Picture:** Upload an image to be shown when notification occurs.

Notification Styles are either a Global-type or Administrator-type. This defines whether the style should be applied globally to all Administrators, or specific to the Administrator who created the style. Administrator Styles will always take priority over Global Styles. Global Styles can only be added/edited by System Administrators.

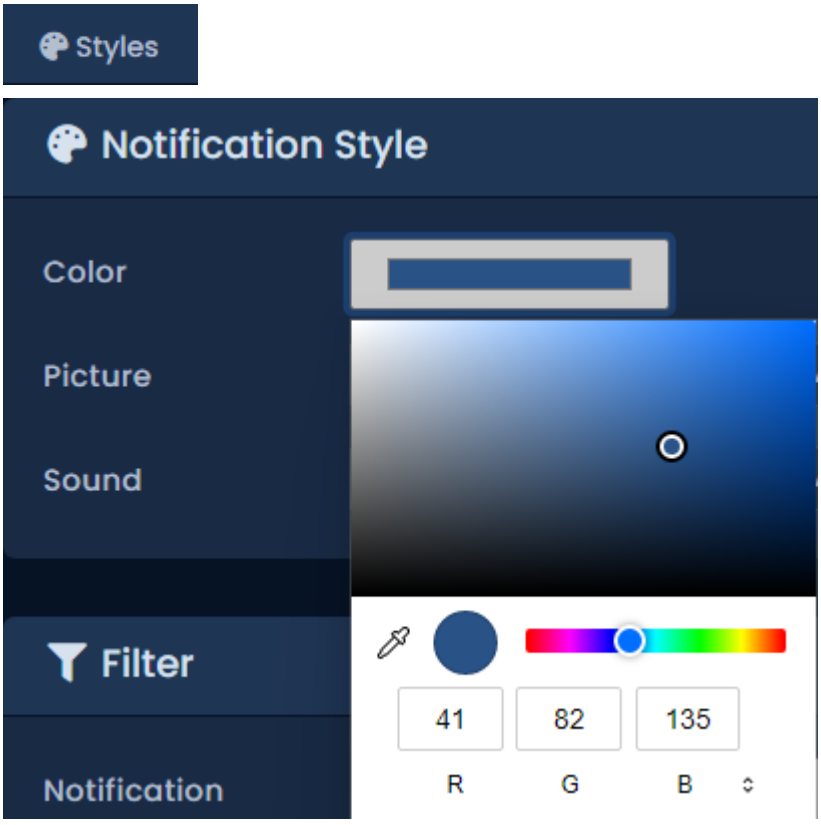
By default, there are 3 types of Notifications:

- Neutral (blue): Notifications that are not positive or negative. This includes Panel Logins, Inputs and Outputs changing state and more.
- Positive (green): Notifications that are positive. This includes Access Granted messages for Users.
- Alerts (red): Notifications that are negative. This includes Door Forced Open, Tamper Sensor Triggered and Panel Disconnects. Any notification type can become an alert.

Creating a Notification Style Rule

1. Use the +**Add** button (pictured below) next to **Administrator** or **Global** types. This will bring you to **Add Notification Style** screen.

2. The **Partition** field will be pre-selected from the **Notification Settings** page. The **Type** field will be pre-selected depending on which Add button is pressed.
3. If you wish to change the background color of the notification, choose theAA Color by selecting the colored square or by entering an HTML color code. (pictured below)



4. If you wish to upload a custom image to be shown, click **Choose File** and select a PNG, JPG or BMP file with a maximum size of 5MB.

5. If you wish for a sound to be played when the notification is shown, click **Choose File** and select an MP3 file with a maximum size of 2MB.

6. Notification Styles can specify certain notifications or devices to match. By default, a style will apply to all notifications unless a Filter is specified. A Notification Category can be selected in the drop-down. When a Notification Category is selected, additional Filter options may appear to further limit the style.

7. Time Restrictions can be implemented in order to restrict when the style should be active. The style will only be used by notifications that occur within the specified time frame.

8. Select Save to save your configuration. You will now be able to view your Notification Style in the Notification Settings screen. The new style will immediately apply to all new notifications as they occur.

Live Camera Rules

Live Camera Rules specify which notifications should cause a live camera feed to be shown on the Sidebar Notification pane and Alert Monitoring page. A live camera feed is shown only when a rule matches AND the device generating the notification has a camera associated to it.

Live Camera Rules are either a Global-type or Administrator-type. This defines whether all Administrators should be shown the camera feed, or whether the rule is specific to the Administrator who created the rule.

Administrator Rules will always take priority over Global Rules.

Creating a Live Camera Rule

1. Use the +**Add** button (pictured below) next to **Administrator** or **Global** categories. This will bring you to **Add Notification Style** screen.

2. The **Partition** field will be pre-selected from the **Notification Settings** page. The **Type** field will be pre-selected depending on which Add button is pressed.

3. Live Camera rules can specify certain notifications or devices to match. By default, the rule will apply to all notifications unless a Filter is specified. A Notification Category can be selected in the drop-down. When a Notification Category is selected, additional Filter options may appear to further limit the rule.

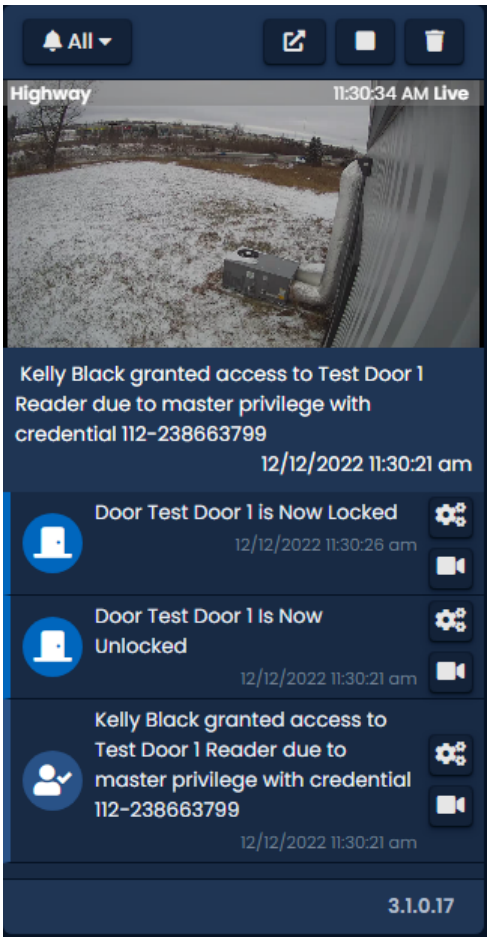
4. Time Restrictions can be implemented in order to restrict when the style should be active. The style will only be used by notifications that occur within the specified time frame.

5. Click **Save** to store the new Live Camera rule. The rule will be applied immediately to all new incoming notifications.

Notification Sidebar

On large screen sizes, you'll see the Notification Sidebar on the right side of the screen. The Notification Sidebar displays the most recent 20 notifications received in real time. A live camera stream from the most recent notification can be configured to be shown at the top of the sidebar.

Figure 24.1. Notification Sidebar



Tip

On smaller screen sizes, the Notification Sidebar will disappear. It can be accessed by clicking on the Arrows icon on the top of the screen, pictured below.

Sidebar Controls

The Notification Sidebar has a row of buttons at the top that allow for easy control of the sidebar.

Figure 24.2. Notification Sidebar Controls

Rule Groups

The Rule Group drop-down allows for easy filtering of real time notifications. When a Rule Group is selected, all subsequent notifications will be processed through the rule group to determine whether they should be shown. Rule Groups can be configured in the Notification Settings page; see the section called “Groups” for more details. The selected Rule Group will be remembered by the browser upon subsequent page loads.

External Camera View

The External Camera View button will move the live camera stream from the top of the sidebar to its own page in a new window. The External Camera View will update as new notifications are received in the sidebar. While the External Camera View is open, the sidebar will not show the camera stream at the top.

Pause / Play

The Pause/Play button will stop the sidebar from showing new notifications. The sidebar can be resumed showing new notifications by clicking the Play button. Notifications that occurred while paused will not be shown, only new notifications.

Clear

The Clear button will remove all notifications from the side bar.

Live Camera

A live camera stream can be configured to show at the top of the sidebar when certain notifications occur. Notifications from devices such as doors or elevators that have cameras associated with them will show a camera icon in the notification that, when clicked, will show historical video in a popup. A camera stream can be moved to its own window by clicking the External Camera View button. Rules for which notifications will show a live camera can be configured in the Notification Settings page; see the section called “Live Camera Rules” for more details.

Quick Rules

Notifications in the sidebar have a gear button on the bottom left corner which opens a context menu. The context menu shows the notification type and options to quickly create rules to affect future notifications.

Each option will open the proper Add Rule page with the Notification Category, Partition, Accept and Destination Sink (if applicable) set based on the notification and the option selected as follows:

- **Hide:** Add Realtime Rule with Accept unchecked.
- **Notify:** Add Email/Web Push Rule with Accept checked.
- **Show Live Camera:** Add Live Camera Rule.
- **Customize:** Add Notification Style.

See Notification Settings section for more information on adding rules.

Monitoring Screen

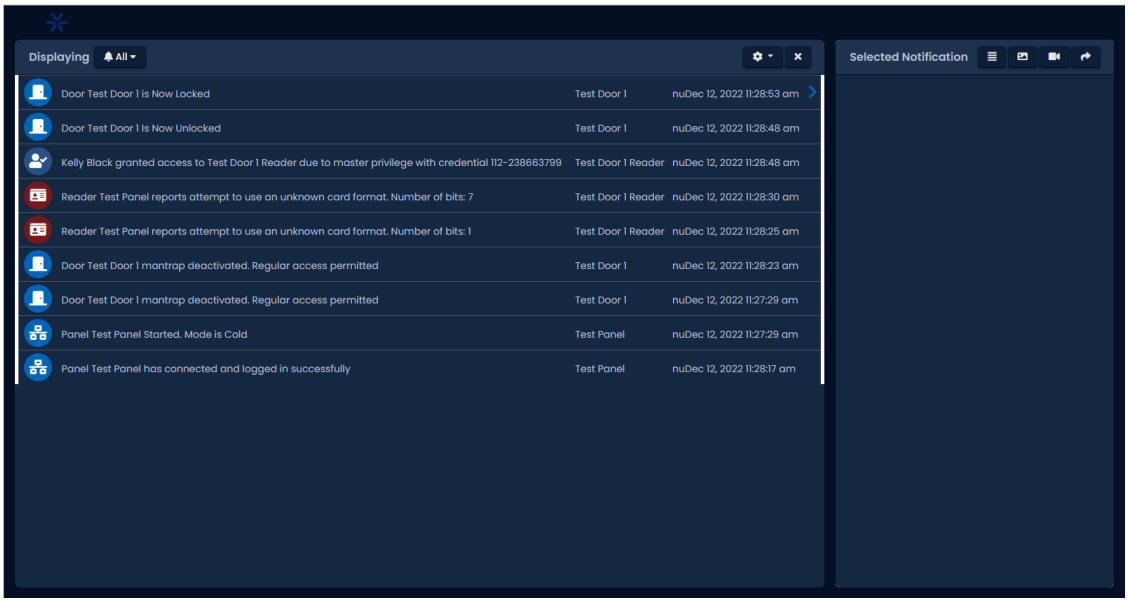
The Monitoring Screen is a dedicated page in VAX with enhanced notification viewing capabilities. This page is often used by guards and security staff to monitor for specific types of notifications or for video/photo verification. This section will cover where to find the Monitoring Screen and how to customize it.

Accessing the Monitoring Screen

1. On the **Side Bar**, scroll down to the top section titled **Day to Day**; click on the **Monitoring** icon (pictured below).

2. Clicking the Monitoring icon will open a separate window/tab.

Figure 24.3. Monitoring Screen



Customizing Displayed Notifications

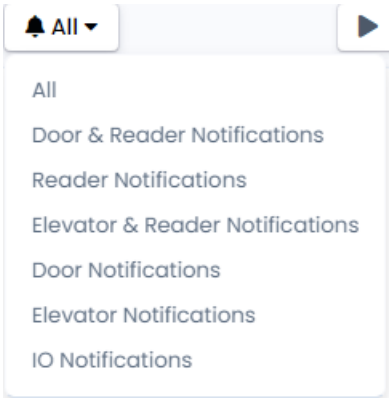
By default, all notifications that are accepted by Realtime Notification Rules will appear on the Monitoring Screen. Groups of rules can be created to change which notifications will be shown.

To change which Notification types appear:

1. On the Monitoring Screen, click on the "Displaying: All Notifications" on the left side. A drop-down menu will appear with the notification groups that have been created in **Notification Settings**.

2. Select which Notification filter group you would like to apply. This filter will affect only future notifications; it will not change notifications that are currently displayed.

Figure 24.4. Notification Filters



Note

To add additional notification filter groups refer to the section called “Groups”.

Monitoring Options

This section will explain additional configuration options that affect how Notifications are displayed.

On the right side of the main Notification area are two icons. The garbage can will clear the Notification grid. The other will show you additional options.

Figure 24.5. Monitoring Options

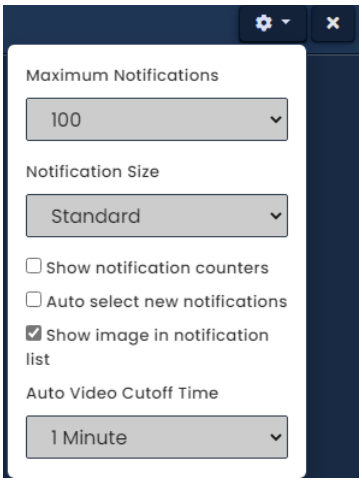
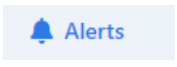


Table 24.2. Monitoring Options

Checkbox/Drop-down	Description
Maximum notifications	The maximum number of Notifications that can be displayed at once. Options are 25, 50, 100, 500.
Notification Size	How much space each Notification will take up in the Notification area. Options are Standard, Large, Horizontal Tiles and Vertical Tiles. Large can make it easier to read. Tiles are better when you need the ability to review profile pictures of many users rapidly.
Show notification counters	If checked, a Notification counter will appear above the Selected Notification area. It will display the total Notifications received, total viewed and total missed.
Auto select new notification	If checked, new notifications will automatically be selected.
Show image in notification list	If there is an image associated with a Notification, it will be displayed in the Notification area with the notification.
Auto video cutoff time	If there is a camera associated with a Notification that is selected, it may appear in the Selected Notification area. This setting will influence if Historical video is played or Live video.

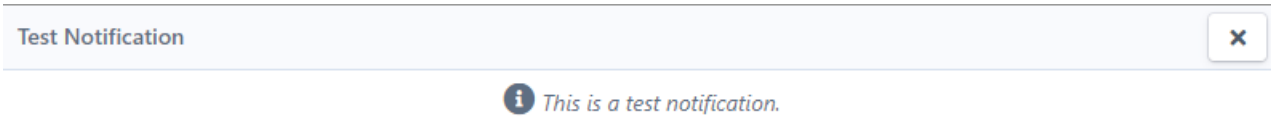
Alert Acknowledgement

Figure 24.6. Alert Icon



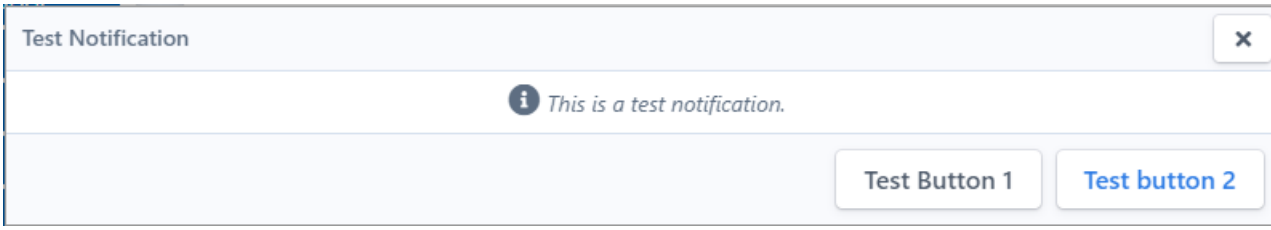
This section will discuss Alert Acknowledgment. Alerts can be sent to an Administrator with an online status. Alerts will present a window with an action.

Figure 24.7. Alert Icon



If the notification is produced by an action plan, some of these actions can be changed in the action plan related to the notification. Other notifications will be related to the health of the system. For this type of notification please refer to Chapter 40, Health Monitoring Chapter 42, *Health Monitoring in VAX*. You can close a notification window by pressing an action. Closing the window will also be considered acknowledgment of the alert without action. By acknowledging the action the window will disappear but can be viewed again using reports.

Figure 24.8. Alert Icon



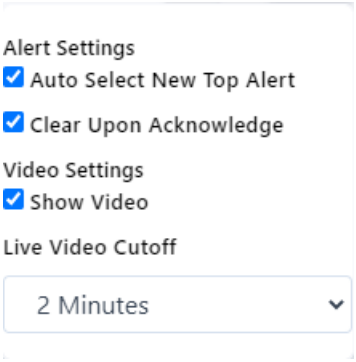
To navigate to the Alert section scroll to the top of the sidebar. The Alerts section will list Unacknowledged Alerts. These alerts were issued without an Administrator online or were not handled by an Administrator. Click the gear icon dropdown to view Alert Settings.

Figure 24.9. Alert Icon

Here you can toggle Auto Select New Top Alert, Clear Upon Acknowledgment. Video settings in the same drop down include Show Video and Live Video Cutoff with a time limiter selector between 2-10 minutes.

Figure 24.10. Alert Icon

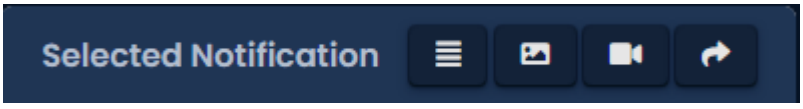
A



Selected Notification Options

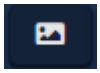
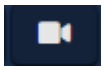
The Selected Notification section is on the right side and will display information relevant to the currently selected Notification. This can include the device, associated user, credential, profile picture or associated cameras.

Figure 24.11. Monitoring Options



The following settings are very simple and are either On or Off. When a setting is on the icon will be white. When the setting is off the icon will be gray. The following table explains what each setting does.

Table 24.3. Monitoring Options

Configuration Item	Description
	Displays the Notification message of the selected Notification when enabled.
	Displays the picture associated with the Notification when enabled (if available).
	Displays any associated cameras with the Notification when enabled (if available).
	This option will toggle any displayed cameras to appear on a separate window.

Chapter 25. Database

This chapter will cover the options available in the Database screen in VAX, Control, specifically the purging of Notifications and administrative log entries to reduce the size of the database and retain performance. Configurations are available for alerting administrators when the database reaches a certain size.

Purging Notifications

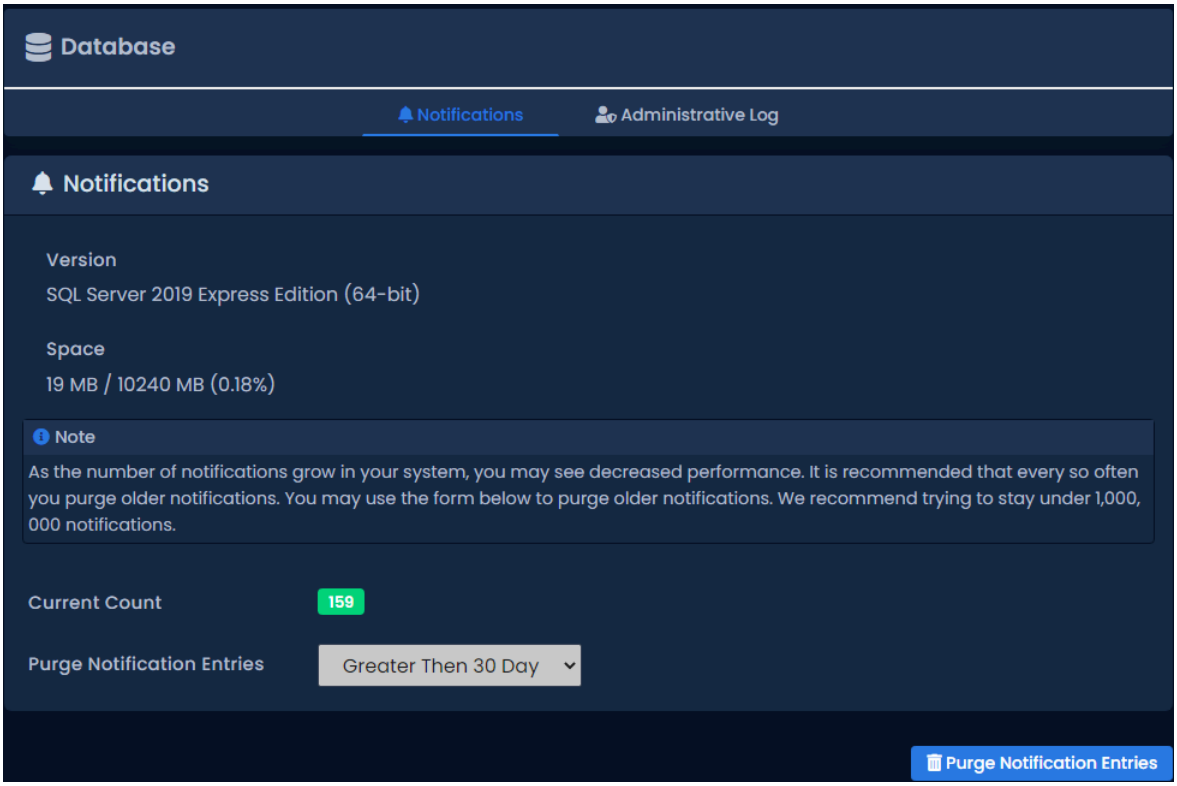
This section will cover how to purge Notifications in VAX Access Control. Large amounts of Notifications over time can hurt the performance of VAX Access Control, especially with deployments with hundreds of active Panels and thousands of Users.

Use the following steps to access the database notification purging form in VAX Access Control:

1. On the **Side Bar**, scroll down to the section titled **Administration**; click on the **Database** icon (pictured below).

2. Once on the **Database** screen, you'll see the amount of Notifications currently in the database.

Figure 25.1. Database Purge Screen



3. We recommend trying to stay under 1,000,000 Notifications. For smaller deployments this could take several years, but for larger ones it could be a few months.

4. To purge Notifications, use the **Purge Notifications** drop-down menu and change how old the Notifications need to be in order to be deleted. The date ranges from Notifications older than 5 years to Notifications older than 30 days. You can also select to purge all Notifications.

5. Once you've made your selection, click the **Purge Notifications** button on the bottom right side. The Notifications that match the date parameter will now be deleted. The Current Count will update once the purge is complete.

Purging the Administrator Log

This section will cover how to purge entries in the Administrator Log in VAX Access Control. Most changes in VAX (such as adding a user) will add an entry to the Administrative Log. These logs should be purged periodically to maintain performance.

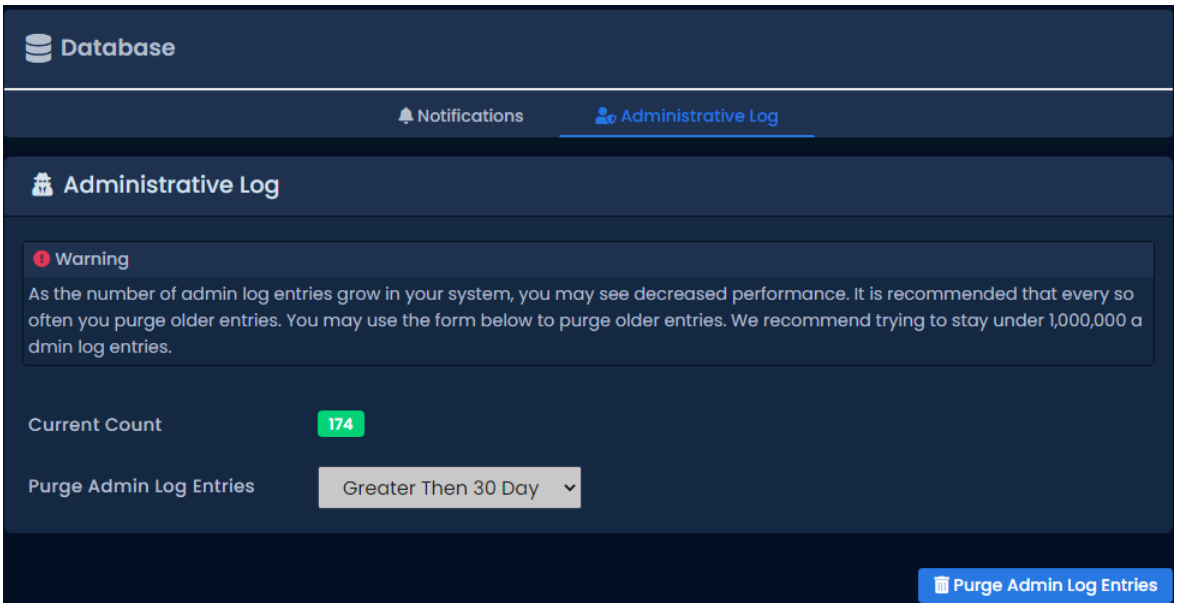
Use the following steps to access the database Administrative Log purging form in VAX Access Control:

1. On the **Side Bar**, scroll down to the section titled **Administration**; click on the **Database** icon (pictured below).

2. Once on the **Database** page, click the tab titled Administrative Log.

3. Once on the **Administrative Log** tab, you'll see the amount of administrative log entries currently in the database.

Figure 25.2. Database Purge Screen



4. We recommend trying to stay under 1,000,000 Administrative Log entries. For smaller deployments this could take several years, but for larger ones it could be a few months.

5. To purge Administrative Log Entries, use the **Purge Admin Log Entries** drop-down menu and change how old the log entries need to be in order to be deleted. The date ranges from entries older than 5 years to entries older than 30 days. You can also select to purge all entries.

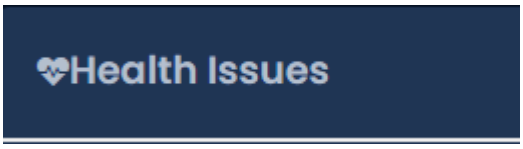
6. Once you've made your selection, click the **Purge Admin Log Entries** button on the bottom right side. The entries that match the date parameter will now be deleted. The Current Count will update once the purge is complete.

Database Size Warning

This section will cover how to configure a database size warning notification in VAX. Large amounts of Notifications and Admin Logs over time can hinder the performance of VAX, specifically involving deployments with hundreds of active Panels and thousands of Users. This section will allow you to notify system admins and users when a database is approaching maximum size

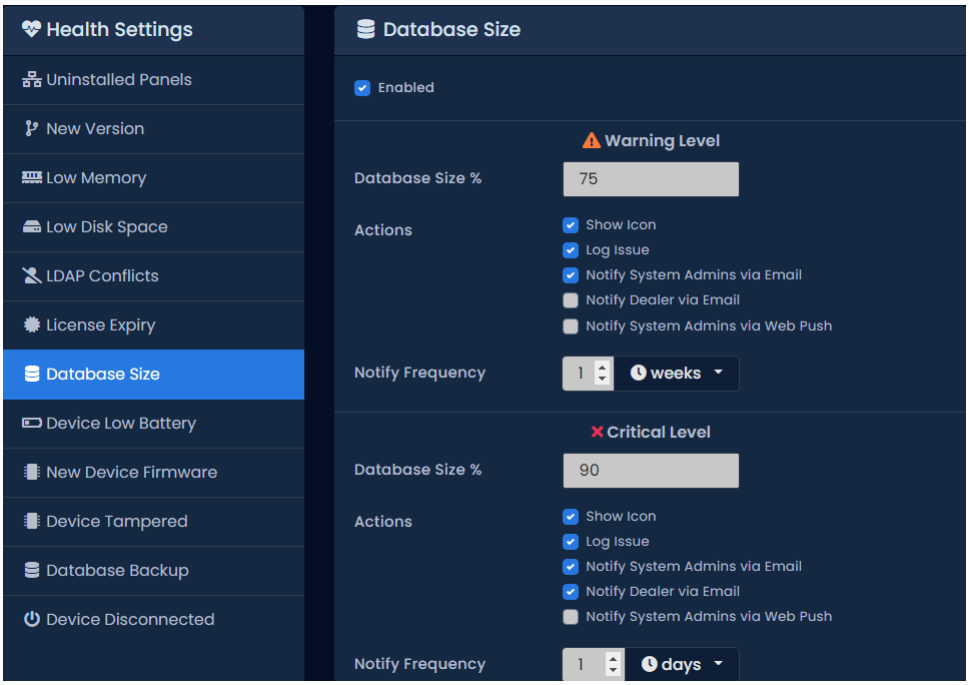
Use the following steps to access the database size warning form in VAX:

1. On the **Side Bar**, scroll down to the section titled **Administration**; click on the **Health Settings** icon (pictured below).



2. Once on the **Health Issues** screen, you'll see on the left side list titled **Health Settings**, the Database Size option.

Figure 25.3. Size Warning Page



3. Select the **Warning Percent** by either inputting the desired amount or use the up/down arrows provided within the text box.

4. Select options including, but not limited to, Show Icon, Log Issue, Notify System Admins via Email, Notify Dealer via Email, and Notify System Admins via Web Push.

5. Once you've made your selection, click the **Save** button on the bottom right side.

Chapter 26. System Settings

This chapter covers the System Settings of VAX. Most of these settings are the same fields that are configured during the Initial Configuration of VAX. They include dealer information, the server address, communication ports, security and email configuration for email alerts.

To access the system settings page:

1. Access your VAX system through your HTML5 browser of choice.

2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer

3. On the **Side Bar**, scroll to the section titled **Administration**; click on the **System Settings** icon. (pictured below)

On the System Settings screen, there will be five tabs of settings. They are **General Configuration**, **Security**, **Email Configuration**, **Service Requests**, and **Purge Notification**.

General Configuration

This section will cover the General Configuration tab in VAX System Settings. These settings and a description are included in the following table:

Table 26.1. General Configuration Fields

Field	Brief Description
Name	This is the name of the host, customer or company name (not specific site).
Description	An optional description of the host, customer or company.
Account Number	Your Vicon Industries account number. This is provided by Vicon on initial activation. Accepts 2 to 30 characters.
Dealer Name	This is the name of the dealer installing the system and/or responsible for supporting the End User of the system.
Dealer Phone Number	This is the primary contact phone number of the dealer installing the system and/or responsible for supporting the End User of the system. No dashes between sections of number (e.g.: 800-348-4266).
Dealer Website	This is the website address of the dealer installing the system and/or responsible for supporting the End User of the system. Format as "www.dealerwebsite.com"
Dealer Email	This is the primary contact email address of the dealer installing the system and/or responsible for supporting the End User of the system.

Server Address

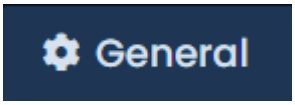
The server address is configured at the bottom of the General tab; these fields are pushed to the Panel during a Panel update and dictate how the Panels communicate with the VAX server.

Table 26.2. Connection Config Fields

Field	Brief Description
Server Address	By default, the name of the PC that VAX is installed on. This field is what is pushed to your Panels and will dictate how they communicate with the server. You can keep this as a name if DNS is active, or change it the **Static IP** of the Server.
Web Address	The URL Address used to send links for Mobile Credential enrollment, Admin App QR Code and Password Reset emails. By Default if not set the server will use the referring URL
Default Card Format	The card format to be used. By default HID Standard (26 bit).
Default Site Code	The default SiteId.
Default STid	The default access Token for STid devices.
Default Dashboard	The default dashboard format to use.

Once you made the desired changes to your settings, click on the **Save** button on the bottom right of the screen.

Figure 26.1. General



Security

This section will cover the Security Configuration tab in VAX System Settings.

Enhanced Manual PIN Security

Enhanced manual PIN security is often enabled in deployments where **PIN Only** Door Schedules are used. When enabled the system will refuse manual PIN numbers that are too similar to existing PIN numbers, greatly reducing the changes of unauthorized access due to PIN similarity.

To enable, simply check the **Enhanced Manual PIN Security** checkbox under the **General** Section of **System Settings**.

Email Configuration

This section will cover Email Configuration in VAX. The Email Configuration tab is used to configure an email address to send emails for password recovery and Notification alerts.

Email Settings

Fill the following fields in the Email Configuration tab of the System Settings.

Note

Email Settings are optional, but recommended. Can be used to recover a forgotten password and to receive notification emails.

Table 26.3. Email settings Fields

Field	Brief Description
SMTP Server	This is the name of the SMTP server required for sending emails (e.g.: mail.ISPdomain.com).
SMTP Server Port	This is the port used for send emails via SMTP (port 25 is common however your settings may vary).
Requires SSL	Check the Secure Socket Layer checkbox if your email client requires and uses SSL for encrypting email messages.
Reply Address	This is the email address email alerts and email recovery will be sent from. It can be the same as the sender email address.
Username	This is the Username required for authenticating and sending email via SMTP.
Password	This is the password required for authenticating and sending email via SMTP.
Send Test on Save	If checked, a test email will be sent from the reply address to itself to verify that the settings are correct.

Once all required fields have been set, click Save. If the checkbox Send Test on Save was checked, a test email will be sent to the reply address from the reply address.

Email Notifications

Email Notifications is a feature in VAX that allows you to receive emails when certain events happen in your access control system. For example, if someone was denied access to a reader, you may want to receive an email alert about it.

Note

In order for email notifications to function, you must properly setup VAX Email Configuration.

To setup email notifications, please follow these steps:

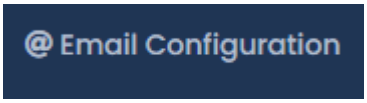
1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, click on the **Notification Settings** icon.

4. On the Notifications Settings Screen, you'll see 16 sections and 3 columns. Each section contains a header about the type of notification beneath it.
5. Each notification has an Alert, Email and Live Camera button on the left side. When the Email button next to a notification is set to On, an email will be sent to the logged in Administrator when this notification happens, along with information about the notification, such as the involved User/Door/Reader/Time.

   When the Alert button is selected, that notification will appear as red in the live notifications and optionally produce a sound in the web browser.

   When Live Video is selected, an inline video feed will spawn if the notification is related to a Door or Elevator with Cameras associated with it.

Figure 26.2. Email Configuration



Mobile APP Configuration

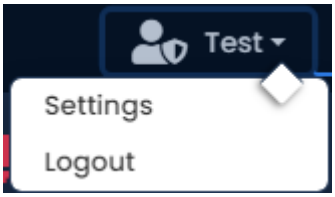
This section will cover how to generate a QR Code in VAX to configure your mobile app. The QR code can be scanned with your mobile app for easy server integration.

Generating a QR Code

A mobile version of VAX is available for download via your mobile device. The download files can be found via your device's application store. With the app installed, you can use a QR code to add your existing VAX server settings to the app on your mobile device.

To generate a QR code, please follow these steps:

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the Home Screen, click on the **Administrative Settings** icon on the top of the screen. A drop-down menu will appear. Select **Settings**.



4. Alternatively, the mobile tab can also be reached on the **Side Bar**. Scroll to the section titled **Administration**; click on the **Administrator Settings** icon (pictured below).

5. On the **Administrator Settings** page, a Notifications tab and a Mobile tab become available. Select the **Mobile** tab.
6. Scan the generated QR code within your VAX app with your mobile device's camera.

Note

The generated QR Code will represent the current address being used to access VAX. (i.e., localhost, PCName, IP Address, Public IP). Ensure that you are currently accessing VAX with an address that can be found via your mobile device.

Service Requests

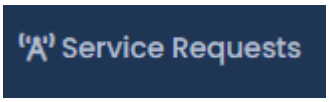
This section will cover the Service Requests tab in VAX System Settings. Service Requests displays a list of Third Party Service Requests for an API Key. Third party applications request API Keys to integrate with VAX. The information about these third party applications are displayed and described by the following information displayed in this table:

Table 26.4. Service Requests

Name	Brief Description
Name	Application Name.
Requested	Date requested.
IP Address	IP address of third party application.
CallBack URL	URL Link to direct callback information.

For more information on Third Party Integration please see Chapter 35,Chapter 35, *Third Party Integration* .

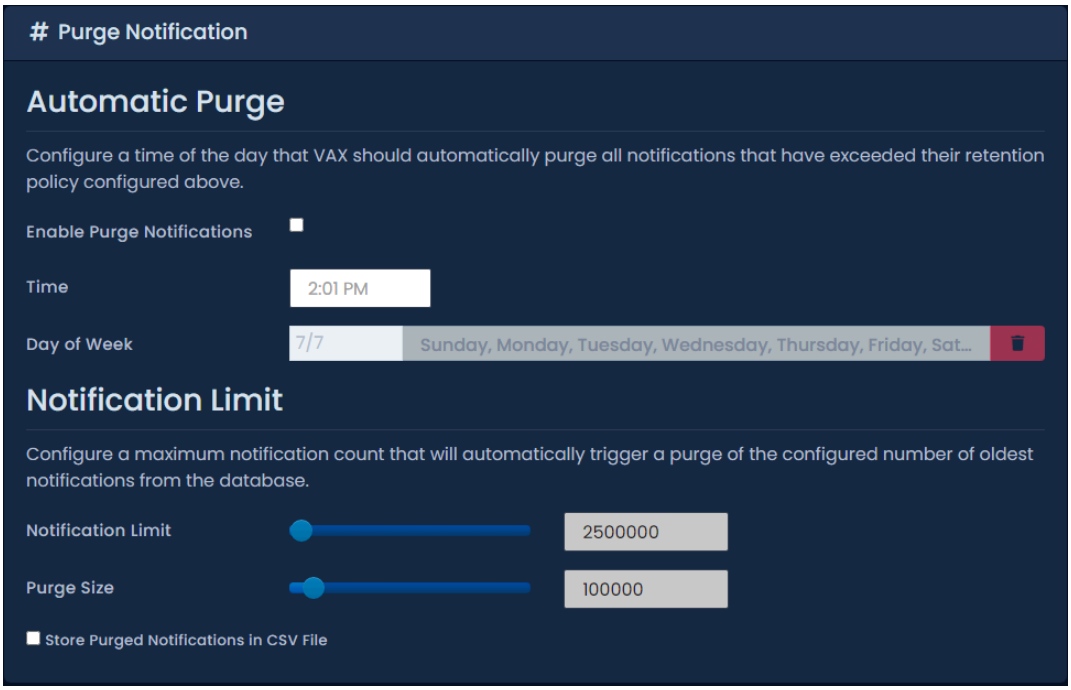
Figure 26.3.



Purge Notification

This section of System Settings handles the removal of notifications. Please see Chapter 25, the section called “Purging Notifications” for more information on Purging Notifications.

Figure 26.4.



Chapter 27. Elevator Hardware

This chapter will cover the access control hardware components required to configure elevators in VAX.

The following items are required:

Table 27.1. Elevator Hardware

Part Number	Description
Elevator Master Panel	The Elevator Master Panel. A controller with special firmware to interact with Vicon Industries Elevator Expanders through an RS-485 connection.
Elevator IO Expander Board (VAX-IO-EXP8-PCB)	Daughter-boards with 8 Inputs and 8 Outputs. Controlled from the Elevator Master Panel through an RS-485 connection. Dip switch addresses 1-8.
Reader Expander Board (VAX-EXP-2D)	Daughter-boards with 2 wiegand reader ports, 4 dry outputs, 2 wet outputs and 6 inputs. Primarily used on the context of elevators for the reader ports. Dip switch address 9.

Connecting the Elevator Master Panel to the Expander Boards

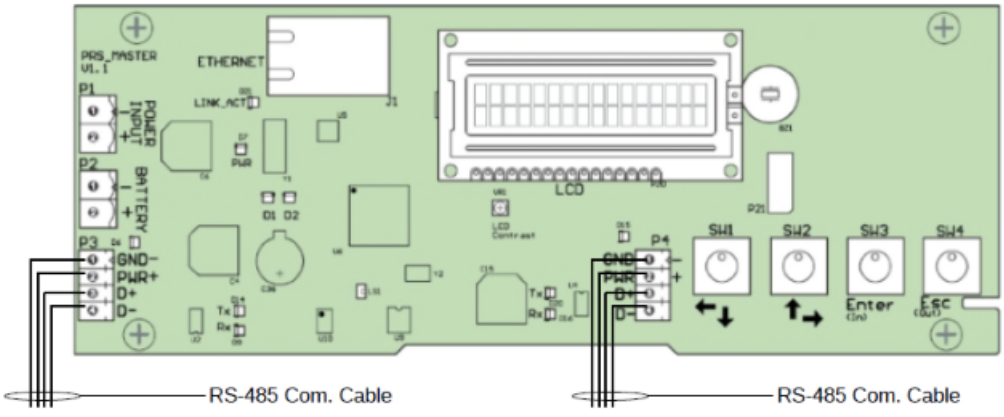
The **Elevator Master Panel** communicates with the **Expander Boards** using **RS-485 interconnect strip(s) or wiring**. When choosing to wire the expander boards to the VAX-ELV-STR-2 instead of the interconnect strips, it is recommend to use 2-pair twisted shielded 18 AWG.

Elevator kits such as the VAX-ELV-STR will typically come pre-wired and include interconnect strips. The Elevator Master Panel will plug into either the P3 or P4 header connection to the expanders P9 header connection. Use the folllwing instructions of wiring the Elevator Master to the expanders via 2-pair twisted.

1. Master controller will have two dedictaed RS-485 + power ports (P3, P4) and if interconnect strips are used, 2 ports near the bottom of each strip (EP2). Connect power connections via 2 conductor 18 AWG (GND, PWR+) and connect data connections via 2 conductor twisted 18-22 AWG (D+, D-) to the corosponding spot on the IO expander (P9).

The Panel will look as follows:

Figure 27.1. Elevator RS-485 Connection

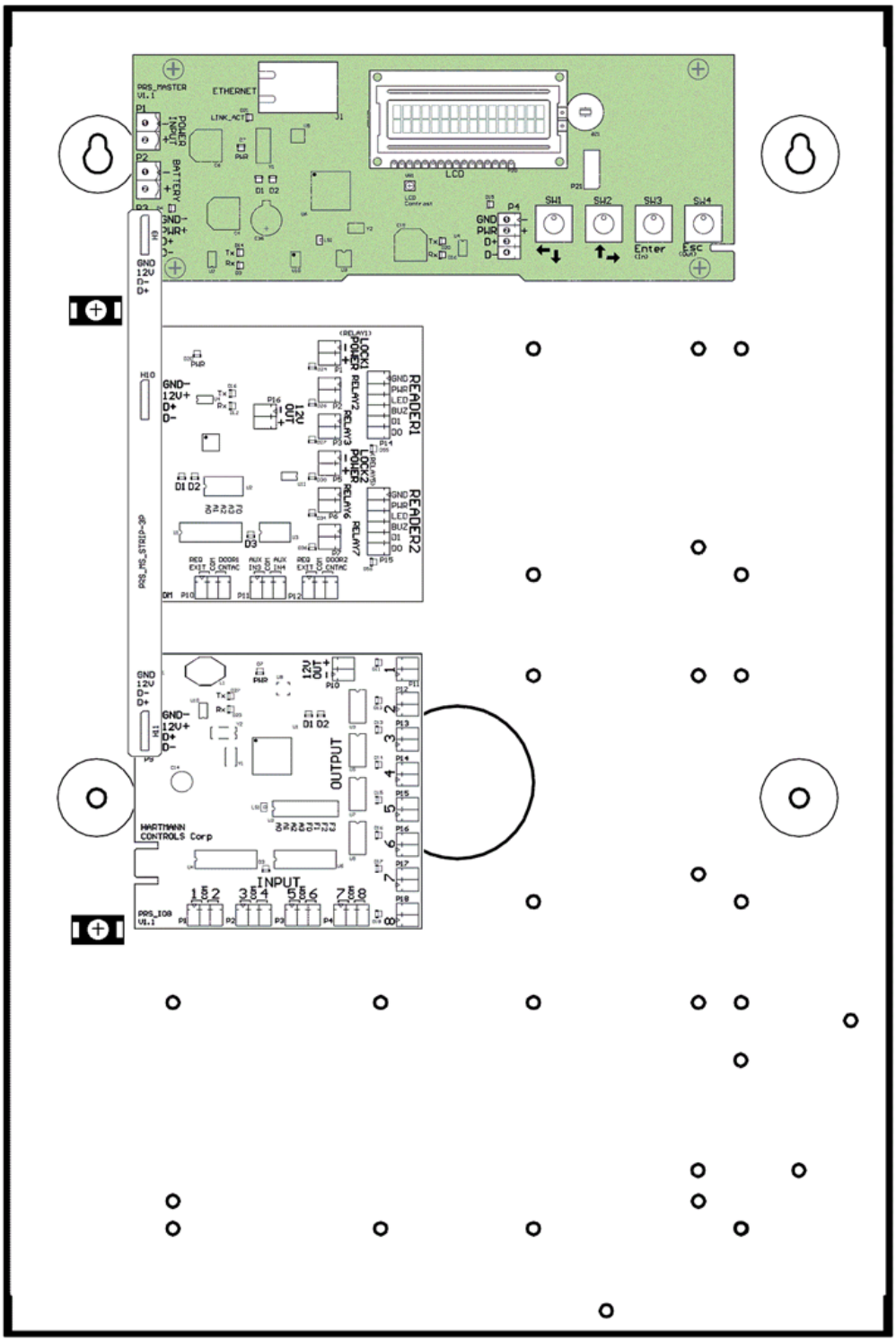


On the first expander:

1. Connect the other end of the **'12V** pair from the Elevator Master to the **'GND-**' and **'12V+'** on the 4-pin header on the left side of the **first Expander Board**. Ensure polarity matches.

2. An additional RS-485 cable will be run from the first **Expander Board** to the second using the same header block. Ensure polarity matches. Continue this chain for all additional **Expander Boards**.

Figure 27.2. Elevator Master Panel

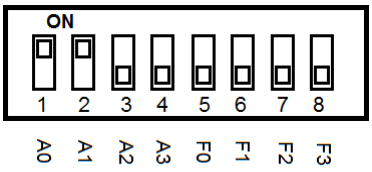


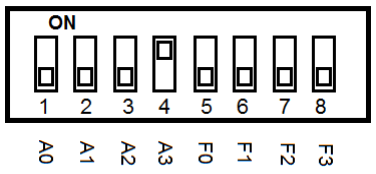
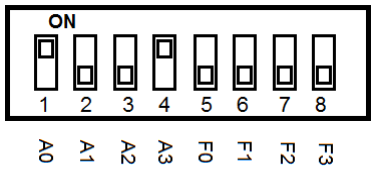
Configuring Expander Board Addresses

Each **Expander Board** on the RS-485 bus requires a sequential **Panel Address**. The address is configured using the first 4 DIP switches on the **Expander Boards**. The reader expander for elevator kits must be set to 9. The first **IO Expander Board** needs an address of '1', the second an address of '2' and so on.

The following chart will demonstrate the DIP switch positions and the corresponding Expander Board Address:

Table 27.2. Expander Panel DIP Switch Address

DIP Switch Position	Resulting Panel Address
	Panel Address: 1 A3 ~ A0: 0001
	Panel Address: 2 A3 ~ A0: 0010
	Panel Address: 3 A3 ~ A0: 0011
	Panel Address: 4 A3 ~ A0: 0100
	Panel Address: 5 A3 ~ A0: 0101
	Panel Address: 6 A3 ~ A0: 0110
	Panel Address: 7 A3 ~ A0: 0111

DIP Switch Position	Resulting Panel Address
	Panel Address: 8 A3 ~ A0: 1000
	Panel Address: 9 A3 ~ A0: 1001

Once you have wired up your **Expander Boards** to the **Elevator Master Panel** and configured the DIP switch **Panel Addresses**, you can now power up the **Elevator Master Board** via 12-13.5VDC power source.

Warning

Prior to wiring the Inputs/Outputs on the Expander Board into your elevator system, we strongly recommend configuring the software prior to this. Please see Chapter 28, *Elevator Software Components*.

Expander Board Input/Output Test

The IO Expander board scan be placed into testing mode via a pre-defined DIP switch configuration (all switches set to OFF except F3, see figure below). In test mode, the Expander Board will sequentially activate its 8 Outputs. After all 8 Outputs have been tested, they will turn off and Inputs will be available for testing. To test an Input, simply short the Input and the corresponding Output will be activated. If any of these tests fail, please contact Vicon Industries. See Chapter 37, *Support*.

Figure 27.3. DIP Switch: Input/Output Test

Expander Board Tamper Sensor

The Expander board has a built in Tamper Sensor. This sensor will send a Notification to VAX if it detects a change in the light level. If the Expander Boards are located in the same container as the Elevator Master Panel, you likely don't need the Expander Board tamper sensor enabled. If the Expander Boards are in a different location, at least one Expander Board should have it enabled. To Enabled the Tamper Sensor, simply turn F2 to ON. Keep A0 - A3 the same. See below.

Figure 27.4. DIP Switch: Tamper Sensor

Chapter 28. Elevator Software Components

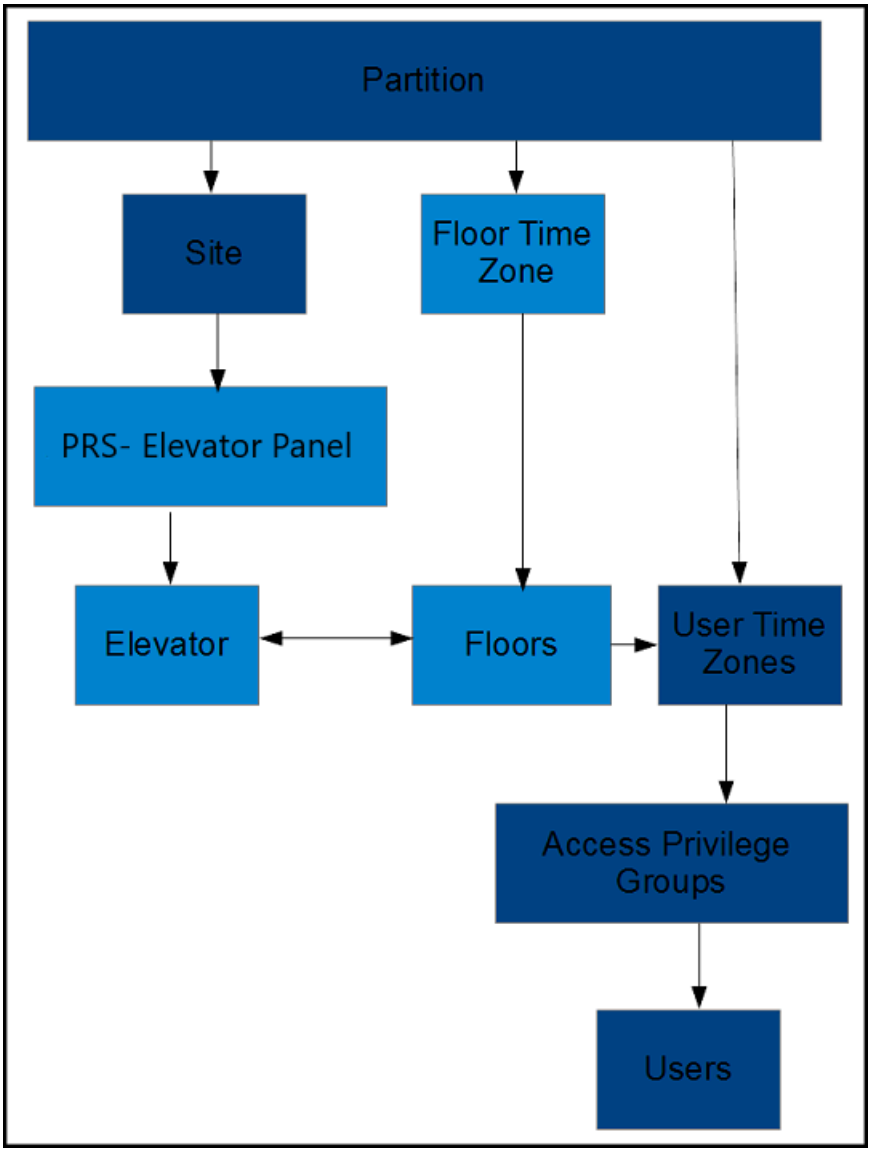
This chapter will be an overview of the various elevator components within VAX 2.1.0+.

The Elevator software components are as follows:

- Elevator Panels (the VAX-ELV-STR-2)
- Elevators
- Floors
- Floor Schedules
- Floor One Time Run Zones (Floor OTR)
- Floor Holiday Groups
- Floor Holiday Schedules

The following diagram demonstrates the primary components of elevators and how they interact with already existing software elements of VAX.

Figure 28.1. Elevator Configuration Items



Adding an Elevator Panel

Adding an Elevator Panel to VAX is very similar to adding a Door Panel. This section goes over this process.

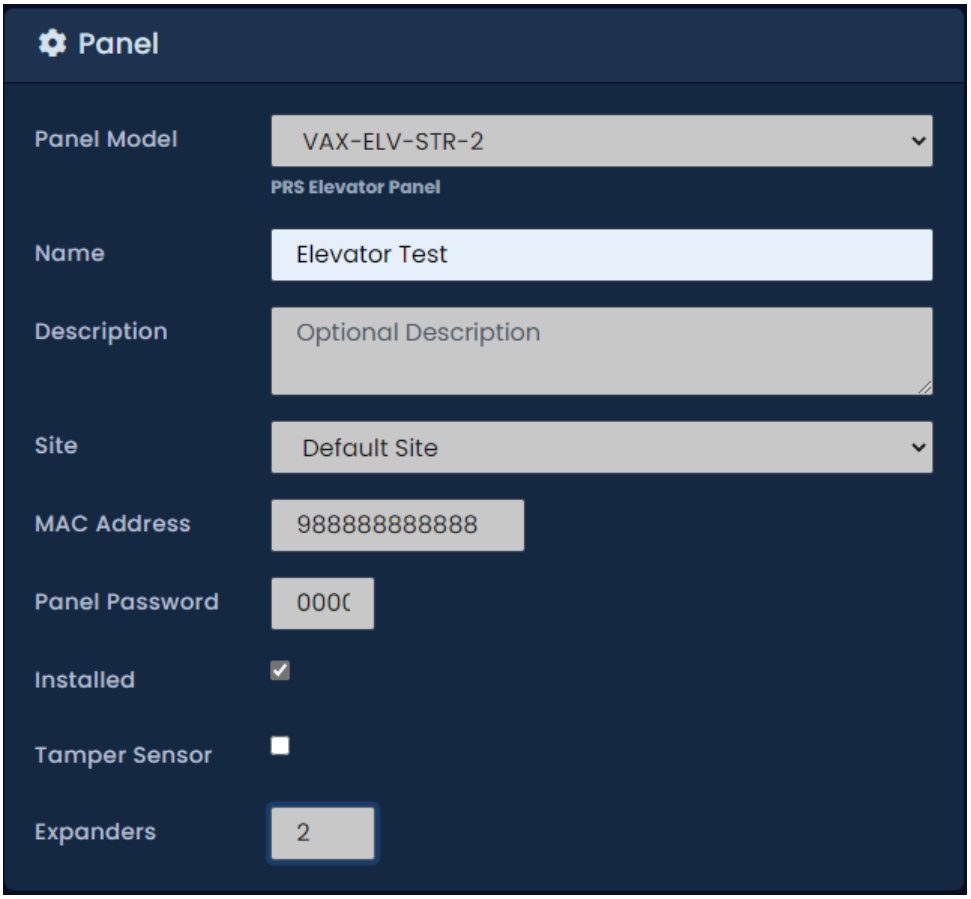
1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Panels** icon (pictured below).

4. On the **View Panels screen**, click the **Add** button.

On the **Add Panels** screen you'll be presented with several drop-down menus, text fields and check boxes to populate.

Ensure the **Panel Model** drop-down menu is set to: **VAX-ELV-STR-2**.

Figure 28.2. Add Panels Screen



The following table describes the fields to be filled in.

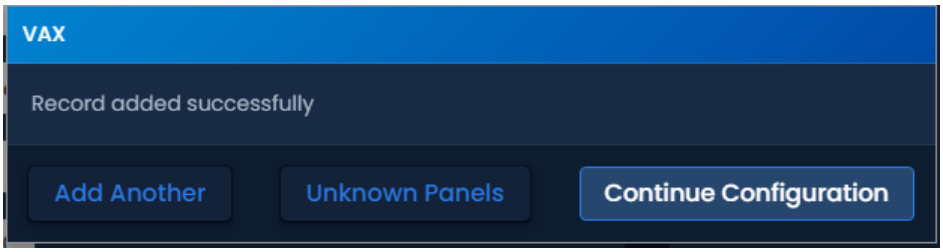
Table 28.1. Add Panel

Drop-down/Text Box/Check box	Description
Panel Model	Select VAX-ELV-STR-2.
Name	The name of the Panel; we recommend naming the Panel based on its location on the site. Accepts 4 to 60 characters.
Description	Optional description of the Panel. Accepts 0 to 255 characters.
Site	Select the site the Panel will reside on. This cannot be changed once the Panel is added.
MAC Address	The unique network address built into every Panel. May be pre-populated if you're adding the Panel through a Unknown Connection From Panel Notification. Must be 12 characters.
Panel Password	The password required for access to the administration menu built into the Panel. Valid values are 0 to 9999.
Expanders	The amount of Expander Boards attached to the Elevator Panel. Valid values are 1 to 8.

Drop-down/Text Box/Check box	Description
TCP Connection: Connection Mode	The method in which the Panel receives its IP address, DHCP or Static. Selecting static will bring up additional fields to fill.

Once you've filled in the required fields, click the **Create** button on the bottom of the screen.

If successful you'll be shown the message: **'Panel added successfully'** with the options to add an additional Panel, or to continue to the edit Panel screen of the Panel we just added.



Adding an Elevator

After adding an Elevator Panel, the next step is to add an Elevator. This object will contain configuration for Floors, including Floor Schedules and Holiday Groups.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Elevators** icon (pictured below).

4. On the**View Elevators Screen**, click the **Add** button.

On the **Add Elevator** screen you'll be presented with several drop-down menus, text fields and check boxes to populate.

The following table describes the fields to be filled in.

Table 28.2. Add Elevator

Drop-down/Text Box/ Check box	Description
Name	A unique name for your Elevator. Accepts 2 to 60 characters.
Description	A optional description for your Elevator. Accepts 0 to 255 characters.
Panel	Select the Elevator Panel this Elevator will be attached to.
Button Sensing	Disable/Enable if button sensing is available. For more information on button sensing please see the section called “Button Sensing”.
Starting Floor Number	Starting Floor Number. Valid values are -55 to 200.
Number of Floors	Number of Floors. Valid values are 0 to 255. If there are more than 8 Floors, more than one Expander Boards will be required. If no ports are available, you will be notified upon saving.

Once you've filled in the required fields, click the **Save** button on the bottom of the screen.

If successful you'll be shown the message: **'Elevator added successfully'** with the options to add an additional Elevator, or to continue to the **Edit Elevator screen** of the elevator we just added.

On the **Edit Elevator Screen**, there are three tabs: **General, Floors**, **Readers**. They are outlined below:

General. On the **General Tab** you can rename the **Elevator**, add/edit the description and enable/disable **Button Sensing**. (For more information on button sensing please see the section called “Button Sensing”.)

Two options are only available on the General tab after adding the Elevator:

Figure 28.3. General Tab

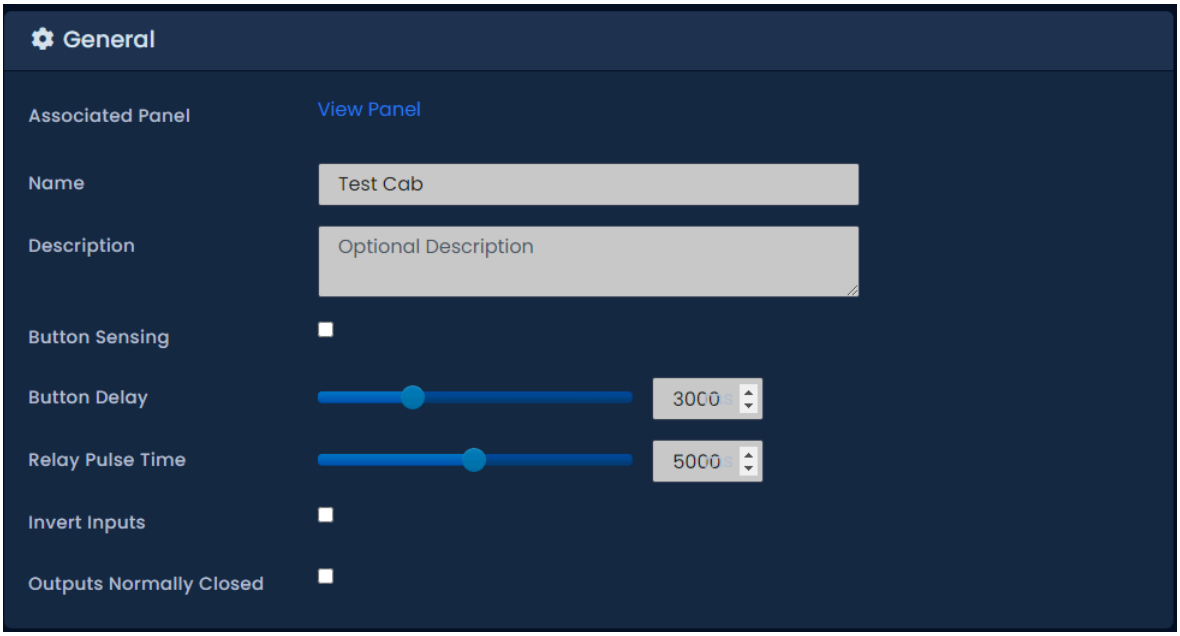
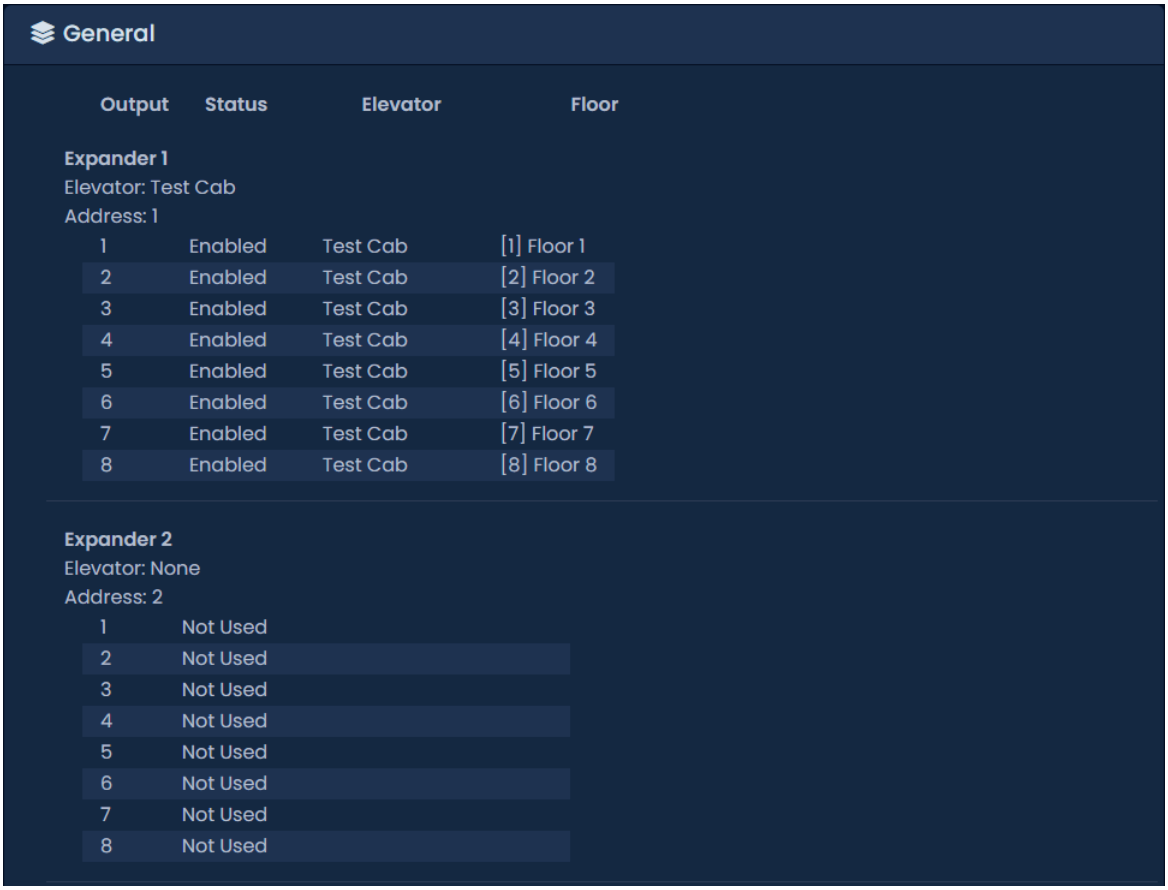


Table 28.3. General Tab

Drop-down/Text Box/Check box	Description
Button Delay	If using button sensing, how long in between presenting a credential and pushing a button that the button push is considered valid. Increments by 100 ms. Valid values are 0 ms to 10000 ms.
Relay Pulse Time	How long the relay(s) will be closed once access has been granted to a particular floor or group of floors. Increments by 100 ms. Valid values are 100 ms to 2000 ms.

Floors Tab. The **Floors Tab** is where you can edit, add or delete Floors. It's where you assign the **Floor Schedules** and the **Floor Holiday Group**.

Figure 28.4. Floors Tab



Reader. The **Reader Tab** is where you can enable the Reader, name/re-name the Reader and assign which Reader port the Reader is attached to. A Reader is required for proper Floor control. Elevator cabs without Readers can only operate on schedules.

Figure 28.5. Reader Tab

Button Sensing

This section will cover the concepts of button sensing. Button sensing is enabled/disabled in the General Tab when editing an Elevator or when creating an Elevator.

Button Sensing: Enabled. Should be enabled when the buttons in an elevator (corresponding to a Floor) are connected to the **Inputs** on the **Expander Board**. When a button in the elevator is pushed without an authorized Credential being presented, the corresponding **Output** will remain off (the exception being if the corresponding Floor has a **Floor Schedule** mode of **Unlocked**).

When a button in the elevator cab is pushed after an authorized Credential has been presented (the **User** has an **Access Privilege Group** that gives them access to that specific Floor), the corresponding **Output** will fire.

The primary benefit of **Button Sensing** is that **Administrators** in VAX are able to see exactly what Floor the **User** selected to go to (live through **Notifications** or through **Floor Activity Report/User activity Report**).

Button Sensing: Disabled. Should be disabled when it's not possible to connect the buttons in the elevator cab to the **Input** on the **Expander Board**. In this scenario, the **Outputs** on the **Expander Board** will be between the button interpreter and the elevator logic controller.

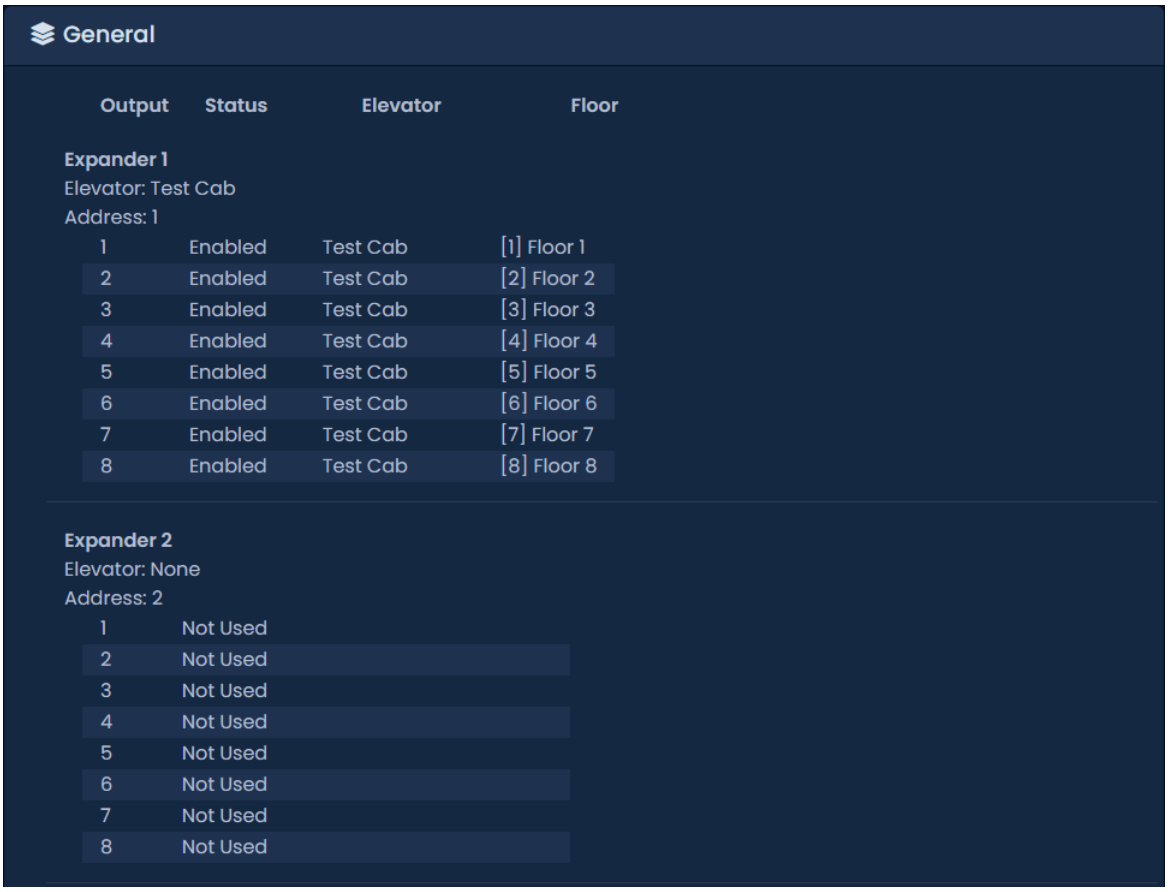
Since the **Expander Board** can't interpret which Floor the User wants to select, when an authorized Credential has been presented (the User has an **Access Privilege Group** that gives them access to specific Floors), all **Outputs** associated with **Floors** the **User** has access to will become closed. Buttons in the elevator cab that are associated with one of the closed Outputs will flow normally to the elevator logic controller.

The disadvantage of not having **Button Sensing** is that **Administrators** in VAX won't be able to see which **Floor** the **User** selected. A record of the **User** presenting his/her Credential to the **Reader** in the cab will be visible **Floor Activity/ User Activity Reports**.

Floor I/O Map

The Floor I/O Map is a tab in the Edit Panel screen that shows a map of all the Outputs on the Expander Board and the corresponding Floors and Elevators based on the current configuration. The Floor I/O map is extremely useful for a wiring reference. This screen will display the Expander Board Addresses of each Expander, which Elevator the Expander is associated with, and the Output each Floor is associated with.

Figure 28.6. Floor I/O Map



Floor Schedules

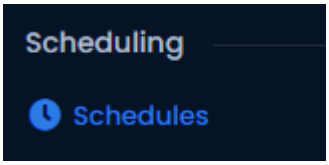
This section covers adding additional **Floor Schedules** to VAX.

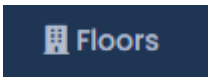
Floor Schedules are applied to **Floors** in the **Floors Tab** of the **Edit Elevators Screen**. Unlike **Door Schedules**, **Floor Schedules** only have three possible states: **Card**, **Unlock** and **Lockdown**. By default, there are 3 default **Floor Schedules**:

- Card Always
- Locked Always
- Unlocked Always

To add more Floor Schedules:

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **Schedules** icon (pictured below). Select the **Floors**tab.





4. On the Floor Schedules screen, you'll see the default Schedules. To add schedules, click the **Add** button on this screen.

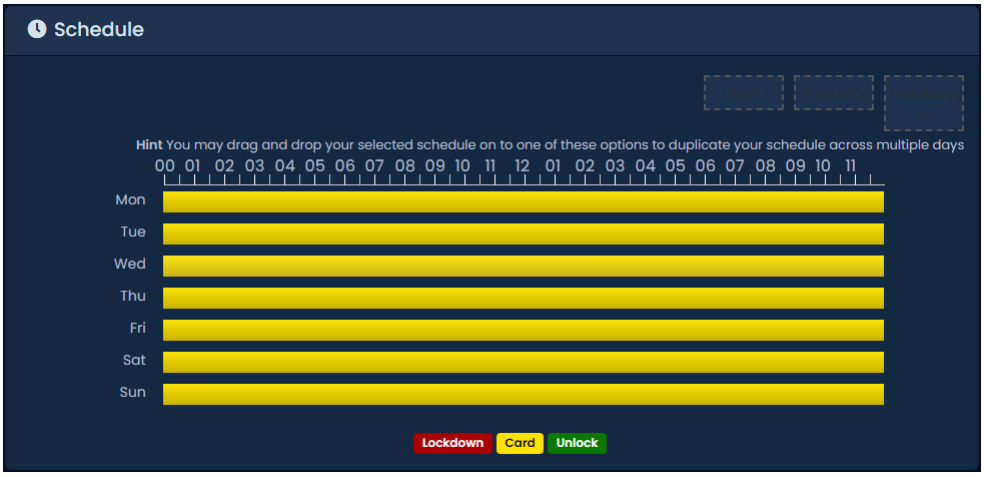
5. On the **Add Floor Schedule** screen, you'll have a few text boxes to fill in.

Table 28.4. Add a Schedule

Text Box	Description
Name	Unique name of your Floor Schedule. Accepts 2 to 60 characters. We recommend naming your Schedules by the function of the Schedule.
Description	Optional description of your Floor Schedule. Accepts 4 to 255 characters.
Partitions	Select the Partitions you'd like to create this Schedule in. If more than one is selected, a copy will be created for each Partition.

6. Schedule: Creating the schedule is the last step in creating a **Floor Schedule**.

Figure 28.7. Floor Schedule Schedule

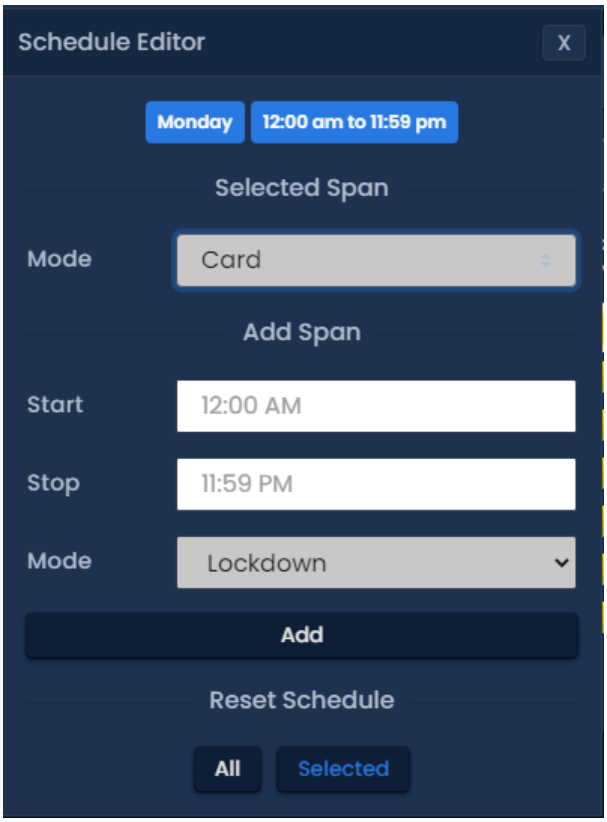


Note

In Floor Schedules, you may have up to 8 time spans, meaning the state of the floor can change up to 8 times in a schedule.

7. Click on any of the horizontal bars in the time schedule to bring up the **Schedule Editor Widget**. The Schedule editor widget is a simple and powerful tool for creating **Schedules**.

Figure 28.8. Schedule Editor



8. Use the **Mode** drop-down menu to select the Floor access state for the span. Only **Card**, **Unlock** and **Lockdown** are available.

9. The **Add Span** section of the Schedule editor has 3 fields used for adding a Floor Schedule span. The **Start** and **Stop** field, when clicked, will bring up a slider menu for selecting the stop and start time. The second **Mode** drop-down menu will dictate what Floor access state the schedule will follow during the defined time span. Once you've completed these fields, click the **Add** Button.

10. You should now see the bar you selected color coded to the time span you've added. Add time spans to that day if required.

    If you'd like the Schedule you've created to be used for several different days, you can click on the bar with your completed Schedule, and select the **Copy** dropdown list to select which day of the week the schedule should be copied to. The Schedule will be replicated based on which date option is selected.

11. Once your schedule for all 7 days is as desired, you may now press **Save** to create the Floor Schedule in the selected Partitions.

Assigning User Access to Floors

This section will cover how to assign User permissions to access specific Floors using Access Privilege Groups. This process is fairly straight forward and works with VAX components you may already be familiar with.

Once you have added your Elevator(s) and assigned Floor Schedules to each Floor, you can now assign Users permission to these Floors using Access Privilege Groups and User Schedules in the same manner you would assign a User permission to a Reader.

For more detail on assigning Floors to Access Privilege Groups, please see Chapter 11, *Access Privilege Groups*.

Chapter 29. Open Supervised Device Protocol (OSDP V2)

OSDP is a communications protocol developed by the Security Industry Association (SIA). The primary use case in the context of VAX is to enhance security with peripheral devices such as card readers.

This chapter will cover the benefits of OSDP, supported Vicon Industries panel models and how to setup OSDP readers to work with our controllers from a hardware and software perspective.

Benefits of using OSDP

OSDP has several benefits over traditional reader communication protocols (Wiegand, clock and data). We will outline them here:

- **Simplified Cabling:** Readers that communicate with OSDP Readers use less conductors than other methods. You can typically use four (4) conductor twisted pair such as Belden 3107A or even CAT6 cable. Any cable that meets the TIA485/EIA-RS-485 specification should be able to work.
- **Encryption:** OSDP supports 2 way encrypted communication via AES-128. This prevents specific attack vectors such as ease dropping and spoofing.
- **Tamper and Disconnection Detection:** Traditional readers don't normally come with a way to detect tampering or disconnection (such as someone removing the reader from its mounted position). The ones that did would require additional pairs to accomplish this and usually had additional costs. Because OSDP is two-way communication, the access control panel can detect if the reader is disconnected or removed from its mounted position.
- **Longer Distances:** Wiegand readers typically only supported a maximum length of 500'. OSDP uses RS-485, which theoretically supports up to 2000' (as long as you had DC power closer than 500').

Supported Door Controller Models

OSDP is currently supported on VAX-MDK door controllers with OSDP specific firmware. When ordering door controllers, you must specify that you require OSDP firmware. VAX-EXP-2D modules also require specific firmware in order to support OSDP. There is no inter-compatability between OSDP hardware and non-OSDP hardware. Wiegand readers can still be used on OSDP panels.

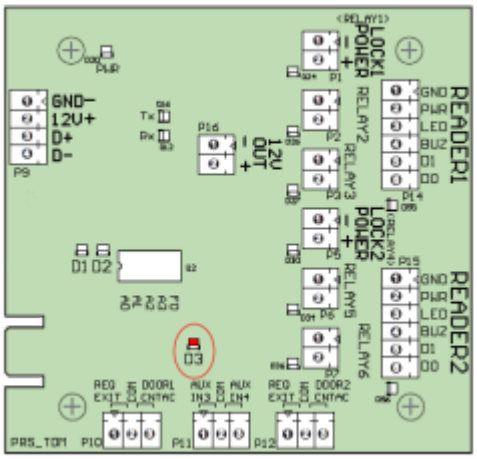
How to Check if Firmware Supports OSDP

VAX-MDK: Use the following steps to check the firmware version:

1. On the physical controller, press and hold the ESC (SW4) button on the Panel for approximately 3-4 seconds until the panel beeps twice.
2. Using the white up and down buttons on the Panel, locate the option titled Firmware Version (option 16).

3. If the controller is using OSDP firmware, the firmware version will start with PMO. If the controller is using Wiegand firmware, it will start with PMS.

VAX-EXP-2D: When a VAX-EXP-2D with OSDP firmware is powered up, the LED labeled D3 will blink 3 times. The LED will also blink every 30 seconds. This LED will also turn on when input state changes, temporarily removing inputs that may be needed for proper identification.



Wiring Up an OSDP Reader

The reader manufacturer will supply their own documentation regarding how to wire up the reader. The recommended cabling is 4 conductor twisted pair shielded such as Belden 3107A. Other types of twisted pair can be suitable such as CAT6.

OSDP Connection Points

There are several points where you can connect OSDP readers on VAX-MDK OSDP controllers. The VAX-MDK controller has two RS-485 bus connections. Both RS-485 buses are also used to communicate to VAX-EXP-2D expansion modules. When interconnect strips are utilized, the bottom of the strip will also have a connection point.

Figure 29.1. OSDP Connection Points (RS-485) on VAX-MDK

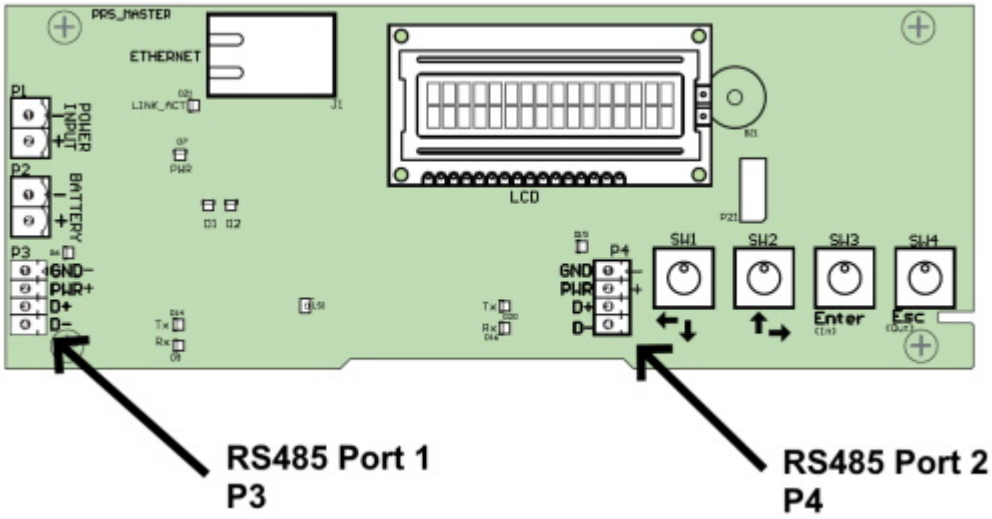
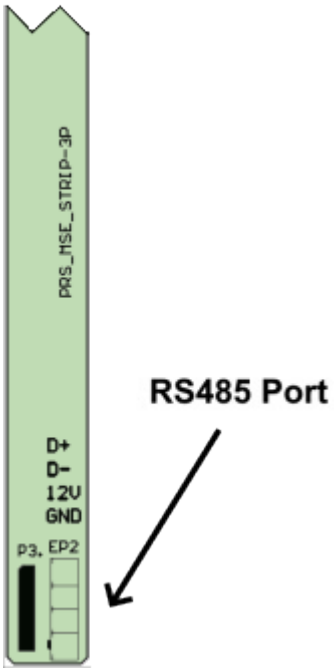


Figure 29.2. OSDP Connection Points (RS-485) on Interconnect Strip



Warning

Due to the short protection on the RS-485 bus connections, a short across PWR and GND on any RS-485 connection will cause the door controller to power cycle and drop power to all expanders on the same bus. For this reason it may be suitable to externally power OSDP readers with their own power source. The GND and PWR connection on 12V OUT (P15) on an individual VAX-EXP-2D has its own short protection and may be well suited when external power isn't an option.

Warning

A short across D+ and D- or GND on any RS-485 connection will cause any connected devices on the same bus (such as VAX-EXP-2D) to stop communicating. For this reason it may be suitable to wire up communication to OSDP readers and other RS-485 devices in such a way that the readers are not on the same RS-485 bus as the other devices.

Termination Resistors

Some OSDP reader manufacturers will recommend that one or more resistors be placed on the RS-485 bus and potentially a termination resistor on the last device on the RS-485 bus. Please refer to the documentation for the reader for specific instructions on resistor use.

Setting up OSDP Communication

Each OSDP device will have an address. Most devices will come with a default device address of 0. Through the LCD menu there are options to change an address, test communication and enable secure communication mode. It is sometimes possible to use third-party software to change these settings on the reader or you can order the reader pre-configured with a specific address. Address 1 to 4 are reserved for expanders. Addresses 5-16 are available for OSDP readers.

Note

You should connect one reader at a time when configuring addresses, as multiple readers with the same address will cause communcation issues.

Setting OSDP Reader Address Through LCD Menu

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

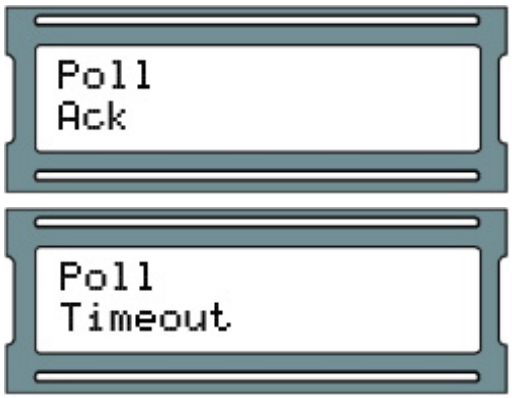
2. If the panel is using the default password ('0000'), press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. If the panel already has a password, you will enter it now using the white up and down buttons and the ENTER button (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout).

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'OSDP' and then press the ENTER button.

4. You will now choose an OSDP address to make changes or test. If you're not sure what the address is you should start with 00. Using the white up and down buttons on the Panel, locate the address you want to change or test and press the Enter button.

5. The default option in the next menu is to Poll the device. It's highly recommended that you poll the device (successfully) before you attempt to change the address. To poll the device, press the Enter button.

6. The result of the poll will now be displayed. You will see Ack if there was a device with RS-485 address you selected in the previous menu that is able to respond. Timeout will be displayed if there are no connected devices with the selected address.



7. Press the ESC button to return to the previous menu.

8. If you need to change the address of the current device, use the white up and down buttons on the Panel to locate the menu option Change Address. Press the ENTER key to enter the change address menu.

9. You can now choose the new address. Use the white up and down buttons on the Panel to increment/decrement the address. When you are ready to choose the address, press the ENTER button.

10. If successful, you will see the old and new address displayed with the message Success. Record the new address and press the ESC button to leave this menu. Timeout will be displayed if the address you were trying to change from was unreachable.

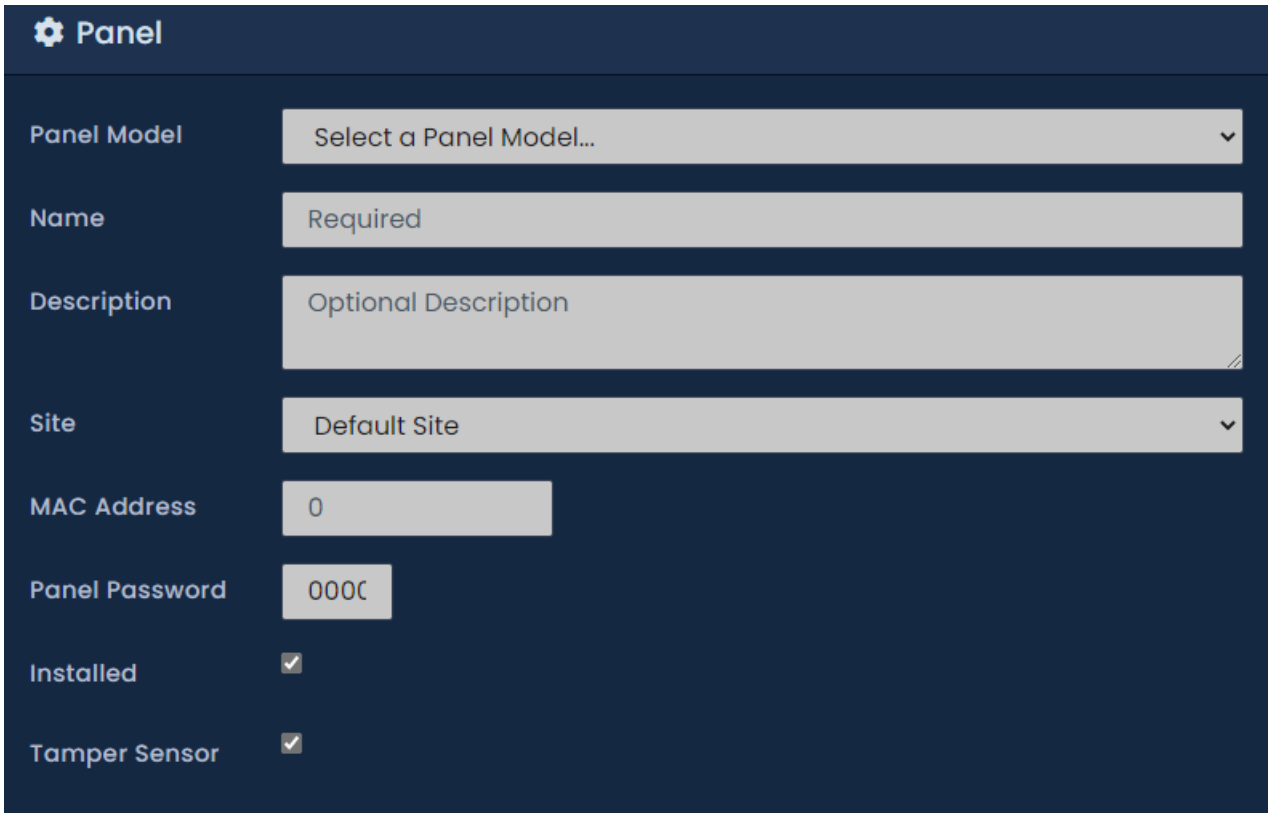
OSDP Software Communication Settings

This section will summarize software settings required for OSDP communication. Encryption settings will be covered later in this chapter.

1. Setup TCP communication between the door controller and the VAX software as outlined in the section called “Panel Initial Configuration”.

2. Add the controller to the software as outlined in the section called “Adding a Panel to VAX Access Control”, making sure to select VAX-MDK-Master-OSDP as the Panel Model.

3. When adding a door (as outlined in the section called “Adding a Door”) to an OSDP panel, there will be a radiobox that allows you to select OSDP as the reader interface. Enter the OSDP address of the reader you wish to associate to this door.



Setting OSDP Secure Channel Mode

Secure Channel Mode is a feature of OSDP that allows you to utilize AES-128 bit encryption between the controller and the reader. Setting up Secure Channel Mode is not mandatory for OSDP to work but is reccomended for maximum security. Encryption keys are set at the VAX software interface. VAX-MDK OSDP door controllers have an option through the LCD to enable Secure Channel Mode on an attached reader. On a per reader basis, you may choose to only allow secure communcations.

Depending on the reader manufacturer, Secure Channel Mode could be enabled via programming card or reader configuration mobile app specific to the reader. This section will show software settings related to OSDP encryption and show how to enable secure channel mode through the LCD interface on the panel.

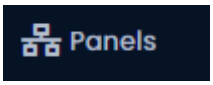
Warning

Secure Channel Mode should not be activated until encryption keys/codes have been sent to the reader. VAX has the ability to do this from the software and will be covered in the next section.

Setting Encryption Keys

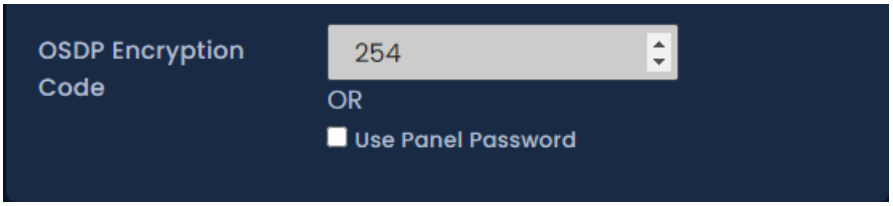
This section covers how to set encryption keys for OSDP readers from the VAX software. This should be done before Secure Channel Mode is enabled via the panel LCD interface. The panel must be added to the system before you can follow these steps. For information on adding a panel, please see the section called “Adding a Panel to VAX Access Control”.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Panels** icon (pictured below).



4. On the**Panels screen**, you'll see any Panels you've already added to the software. Click the **blue** button (Advanced Settings) next to the Panel you'd like to configure.

5. On the **Edit Panel** screen, you'll be in the General tab. Scroll down to view OSDP settings. These options will only appear if the controller has OSDP firmware.



6. OSDP Encryption code supports 255 pre-defined encryption keys that can be used with Secure Channel Mode. This field will accept 0-254.

   Alternatively, the panel password can be used as the encryption key. Check the Use Panel Password checkbox if you wish to use the panel password as the encryption key or enter the value of the encryption key you would like to use.

7. Update your panels to send them the encryption keys. They will not be used untill Secure Channel Mode is enabled as outlined in the next sections.

Enabling Secure Channel Mode on OSDP Readers

After you have sent encryption keys to the controller, you must enable Secure Channel Mode on the reader itself. You can do this from the panel LCD menu or in some cases the manufacture of the reader may have other means to do this, such as programming card or configuration app.

1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.

2. If the panel is using the default password ('0000'), press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. If the panel already has a password, you will enter it now using the white up and down buttons and the ENTER button (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout).

3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'OSDP' and then press the ENTER button.

4. You will now choose an OSDP address to make changes or test. If you're not sure what the address is you should start with 00. Using the white up and down buttons on the Panel, locate the address you want to change or test and press the Enter button.

5. At the OSDP menu for the address you selected, use the white up and down buttons on the Panel to locate the menu option 4 Enable SC mode and press the ENTER key.

Software: Restricting OSDP Communication to Secure Channel Mode

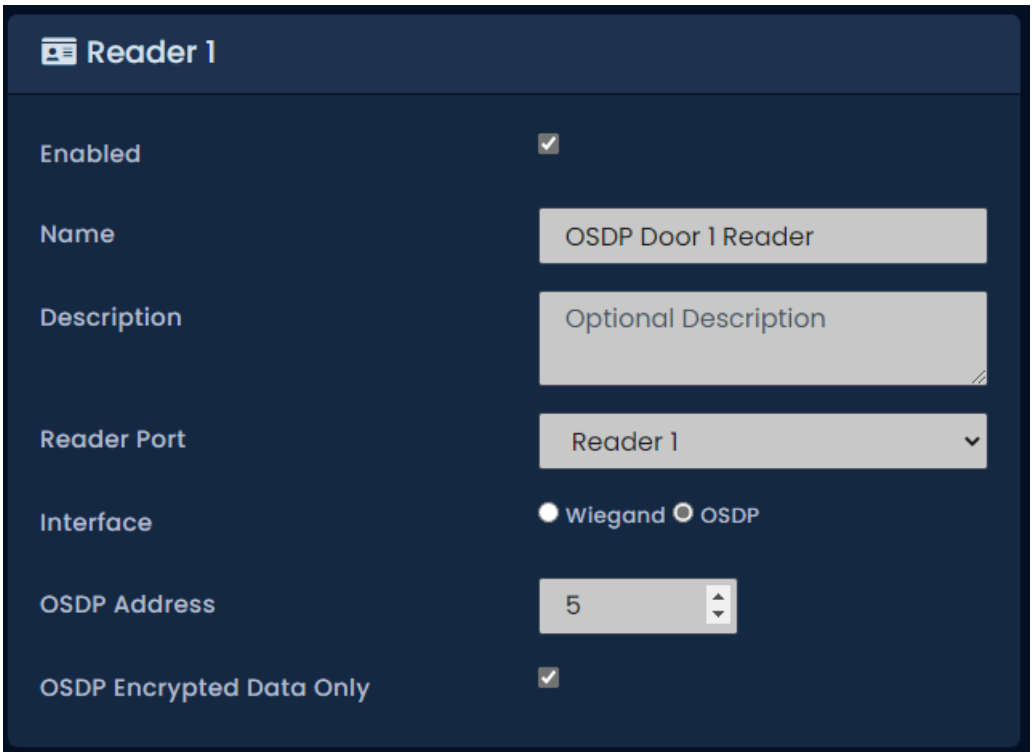
The last step in securing your OSDP readers is to configure the reader settings (from the software) to restrict any non-secure communcation. Use the following steps only if the encryption keys have already been sent to the controller and readers have been changed to Secure Channel Mode from the panel LCD menu.

1. From the **Side Bar**, scroll down to the section titled **Hardware**, click on the **Doors** icon (pictured below).

2. On the **Doors** screen, you'll notice any Doors you've already configured listed here. Click the blue button next to the Door you're ready to finish setting up Secure Channel Mode for.

3. On the **Edit Door** screen, navigate to the Reader 1 tab (you may need to repeat these steps for Reader 2 tab if using back to back readers).

4. On the Reader tab, there is a checkbox titled OSDP Encrypted Data Only. Check the checkbox and click Save at the bottom of the page



5. Enable OSDP Encrypted Data Only on any other readers that need to be set and update your panels.

Chapter 30. Input/Output Boards

Introduction

The Input/Output Board (IO-Board) is a general purpose input/output controller. It has the capability of switching its on-board solid state relays based on schedules or pre-defined actions based on dry contact inputs. Can be used to monitor up to 16 unmanaged doors (doors with locks, door contacts, inputs but no reader) per master controller or up to 64 monitored doors (doors that only have door contacts) per master controller.

This chapter is designed to assist you in planning and configuring our Input/Output boards.

Tip

If you aren't planning on using any Input/Output Boards, you can safely skip this chapter.

IO Board Part Numbers

This section contains relevant part numbers and their descriptions. Part numbers will usually have a combination of sub-assemblies which are covered in more detail in the next section.

Table 30.1. IO Part Numbers

Part Number	Description
VAX-IO	Input/Output Starter Kit with VAX-MDK, and VAX-IO-EXP8-PCB expansion module. 12VDC powered with external power supply. Complete in steel vented and lockable enclosure. Add up to 7 more expanders to control up to 64 I/O's per Master controller.
VAX-IO-EXP8-PCB (IO-Board)	8-Floor Expander (or 8-Port IO Expander) board only without enclosure (requires VAX-ELV-STR or VAX-IO kit to function)

Hardware Setup

This section covers an overview of the components involved, the hardware setup of connecting the IO boards to the IO-Master controller and some examples of typical external hardware.

List of components:

IO Master: A Master controller, powered by 12VDC power. Provides power and communication to up to 8 IO-Boards via RS-485 bus providing up to 64 Inputs and 64 Outputs.

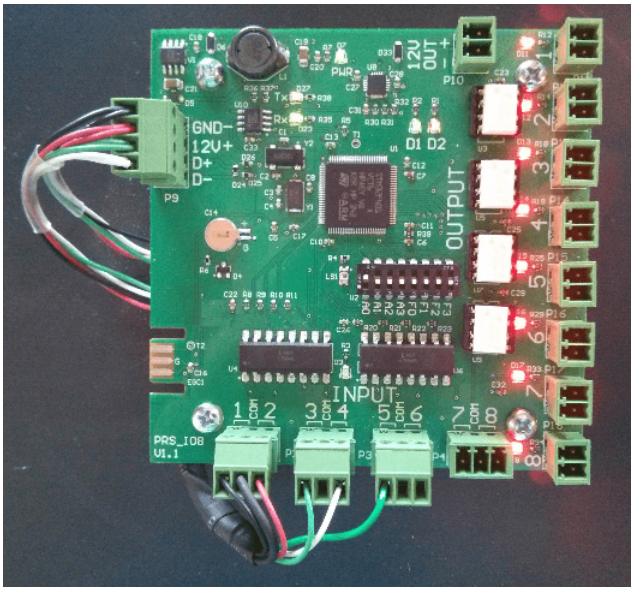
IO-Board: Daughter-boards that are powered and controlled by the IO-Master Panel. Each IO-Board is equipped with:

- 8 x Solid state Outputs:
  - Solid State Relay Dry Contact, 30VDC, 500mA Limit, fully configurable, no mechanical parts.
  - Can be placed on schedules, change state up to 11 times in a single day.
  - Configurable as normally closed or normally open.
  - Can be placed on a Holiday schedule, change state up to 5 times in a single holiday.

- Can be manipulated from any Input on the same IO-Master controller.

- 8 x Dry Contact Inputs:
  - Can be triggered via buttons, door contacts, alarm inputs, relays, external systems.
  - Can be placed on schedules to only monitor the inputs during specific times. Up to 5 schedule changes in a single day.
  - Configurable as normally closed or normally open.
  - Can be configured to trigger various events on any Outputs on the same IO-Master controller.

Figure 30.1. IO-Board



If you purchase the IO-Controller/Boards in a kit, the communication and power between the IO Master and the IO-Boards will be pre-wired for you with interconnect strips/rails.

Connecting the IO-Master to the IO-Boards

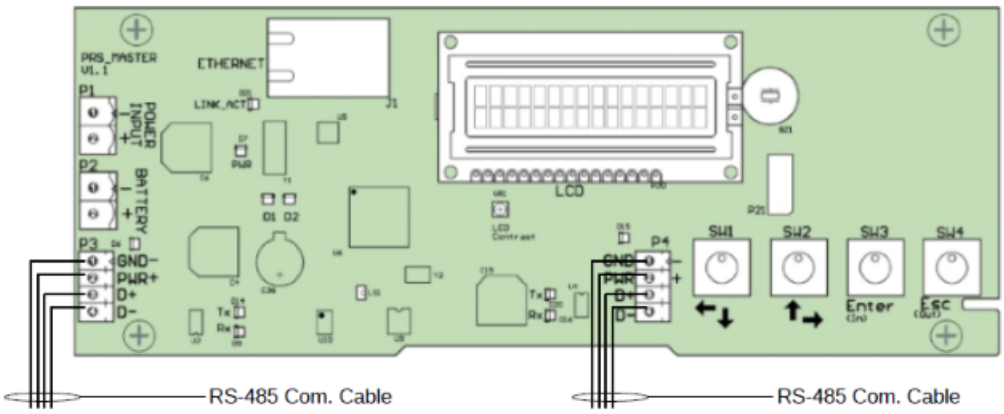
IO kits will come with the IO-boards pre-wired together with either standard wiring or through convenient interconnect strips. This section can be skipped if you do not plan to connect IO boards remotely.

The **VAX-MDK RS-485 Connection**

1. Master controller will have two dedictaed RS-485 + power ports (P3, P4) and if interconnect strips are used, 2 ports near the bottom of each strip (EP2). Connect power connections via 2 conductor 18 AWG (GND, PWR+) and connect data connections via 2 conductor twisted 18-22 AWG (D+, D-) to the corosponding spot on the IO expander (P9).

Your Panel should look exactly as follows:

Figure 30.2. IO Master Controller RS-485 Connections



On the first **IO-Board**:

1. Connect the other end of the **'12V** pair to the **'GND-'** and **'12V+'** on the 4-pin header on the left side of the **IO-Board**. Ensure polarity matches.

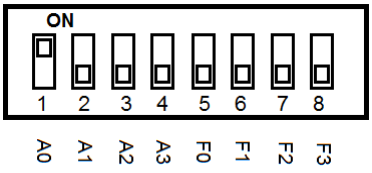
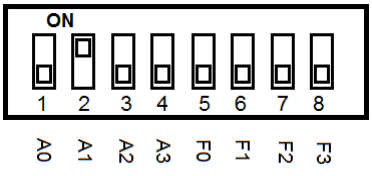
2. If more than 1 **IO-Board** is being used, an additional RS-485 cable will be run from the first **IO-Board** to the second using the same header block. Ensure polarity matches. Continue this chain for all additional **Expander Boards**.

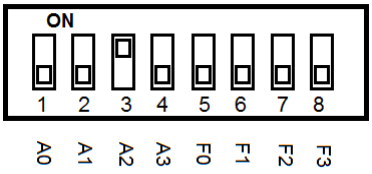
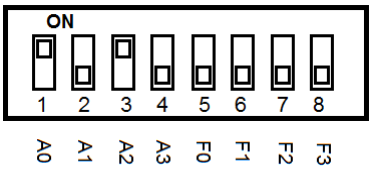
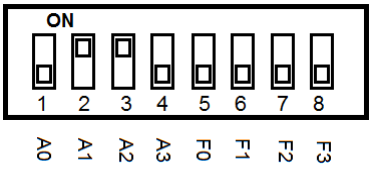
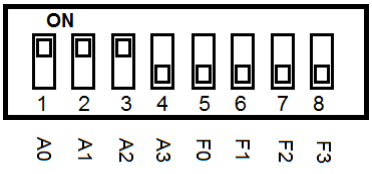
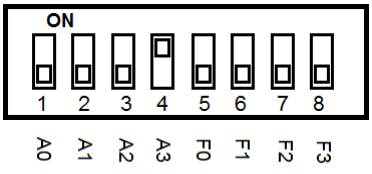
Configuring IO-Board Addresses

Each **IO-Board** on the RS-485 bus requires a sequential **Panel Address**. The address is configured using the first 4 DIP switches on the **IO-Board**. The first **IO-Board** needs an address of '1', the second an address of '2' and so on.

The following chart will demonstrate the DIP switch positions and the corresponding IO-Board Address:

Table 30.2. Expander Panel DIP Switch Address

DIP Switch Position	Resulting Panel Address
	Panel Address: 1 A3 ~ A0: 0001
	Panel Address: 2 A3 ~ A0: 0010
	Panel Address: 3 A3 ~ A0: 0011

DIP Switch Position	Resulting Panel Address
	Panel Address: 4 A3 ~ A0: 0100
	Panel Address: 5 A3 ~ A0: 0101
	Panel Address: 6 A3 ~ A0: 0110
	Panel Address: 7 A3 ~ A0: 0111
	Panel Address: 8 A3 ~ A0: 1000

Once you've wired up your **Expander Boards** to the **IO-Master Panel** and configured the DIP switch **Panel Addresses**, you can now power up the **IO-Master Board** via 12-13.7VDC power source. You can change the dip switch values while the controllers are powered up.

IO-Board Input/Output Test

The IO-Board can be placed into testing mode via a pre-defined DIP switch configuration (all switches set to OFF except F3, see figure below). In test mode, the IO-Board will sequentially activate its 8 Outputs. After all 8 Outputs have been tested, they will turn off and Inputs will be available for testing. To test an Input, simply short the Input and the corresponding Output will be activated. If any of these tests fail, please contact Vicon Industries. See Chapter 37, *Support*.

Figure 30.3. DIP Switch: Input/Output Test

IO Software Configuration

This section will cover the various software configuration needed to successfully plan and deploy an IO-Master Panel and its connected IO-Boards.

The following list contains each of the software components relevant to IO-Board configuration:

- Input/Output Settings on the Edit Panel screen
- Input Schedules
- Input Holiday Schedules
- Output Schedules
- Output Holiday Schedules
- IO Holiday Groups
- Unmanaged Doors
- Monitored Doors

Adding the IO Master Panel to VAX

Adding an IO Master Panel to VAX is very similar to adding a Door Panel. This section goes over this process.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Panels** icon (pictured below).

4. On the **View Panels screen**, click the **Add** button.

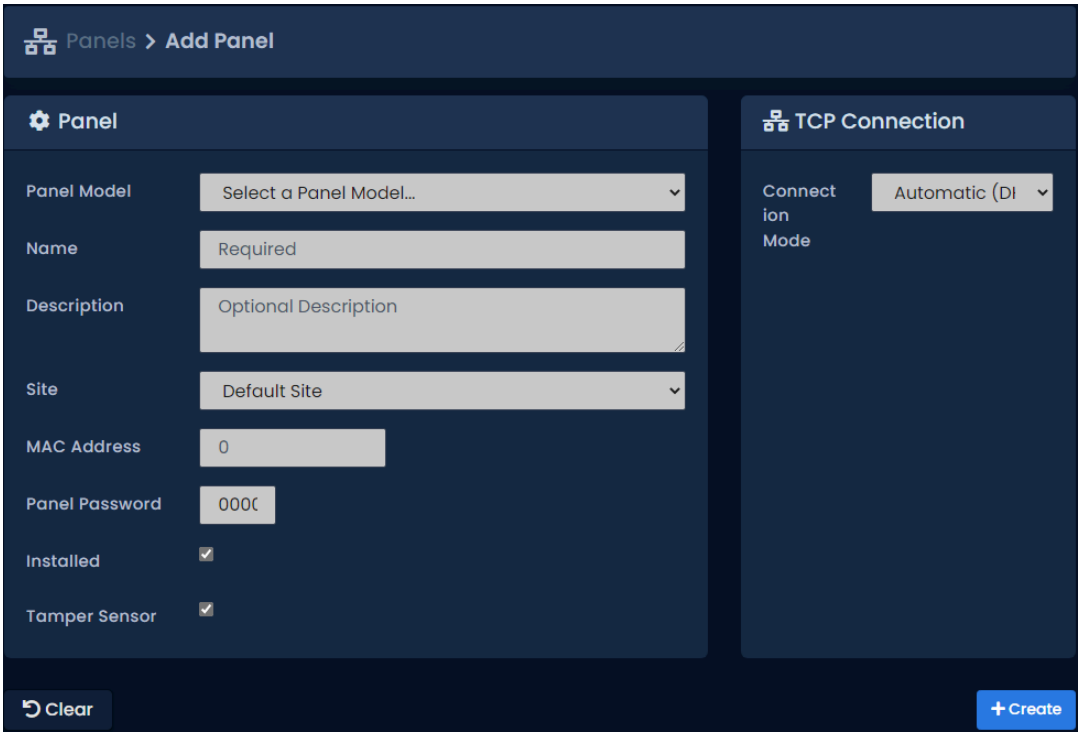
Tip

You can also get to the Add Panels screen from the Unknown Panels screen which will auto fill most information.

On the **Add Panels** screen you'll be presented with several drop-down menus, text fields and check boxes to populate.

Ensure the **Panel Model** drop-down menu is set to **VAX-IO-STR-2**.

Figure 30.4. Add Panels Screen



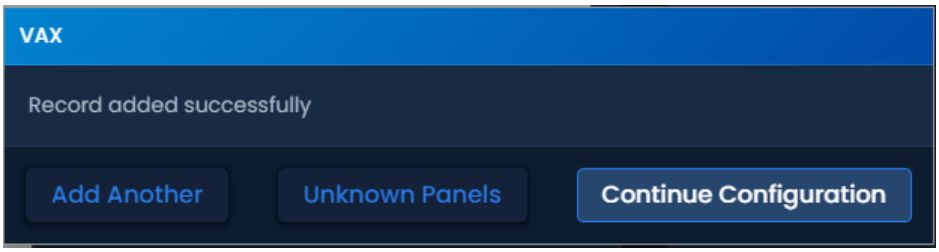
The following table describes the fields to be filled in.

Table 30.3. Add Panel

Drop-down/Text Box/Check box	Description
Panel Model	Select VAX-IO-STR-2
Name	The name of the Panel; we recommend naming the Panel based on its location on the site. Accepts 4 to 60 characters.
Description	Optional description of the Panel. Accepts 0 to 255 characters.
Site	Select the site the Panel will reside on. This cannot be changed once the Panel is added.
MAC Address	The unique network address built into every Panel. May be pre-populated if you're adding the Panel through a Unknown Connection From Panel Notification. Must be 12 characters.
Panel Password	The password required for access to the administration menu built into the Panel. Valid values are 0 to 9999.
Expanders	The amount of IO-Boards attached to the IO Master Panel. Valid values are 1 to 8.
TCP Connection: Connection Mode	The method in which the Panel receives its IP address, DHCP or Static. Selecting static will bring up additional fields to fill.

Once you've filled in the required fields, click the **Save** button on the bottom of the screen.

If successful you'll be shown the message: **'Panel added successfully'** with the options to add an additional Panel, or to continue to the edit Panel screen of the Panel we just added.



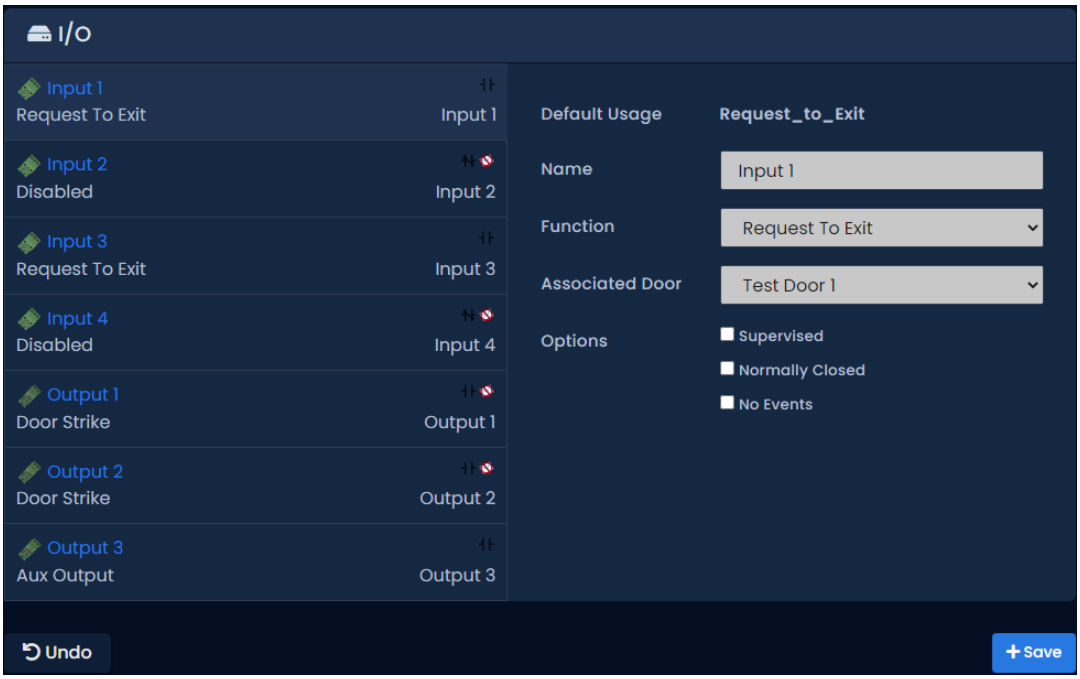
Configuring Inputs and Outputs

Once you've added the IO Master Panel, you'll be able to edit the Inputs and Outputs on the IO-Boards in the software.

1. Navigate to the Edit Panel screen for the IO Master Controller.
2. Click on the IO tab on the Edit Panel screen.
3. By default, all Inputs and Outputs will be disabled. You can switch between which IO-Board you are editing with the "I/O Expander" drop-down near the top.

   Inputs and Outputs are listed on the left side of the screen. The selected Input/Output will be grey and will have its options displayed on the right side.

Figure 30.5. I/O Tab



The following table demonstrates each of the fields available when an Input is selected:

Table 30.4. Input Options

Function	Description
Name	Unique name of your Input. Accepts 4 to 60 characters. We recommend naming your Input based on its function or device that will be connected to it.
Function	Function will dictate what input options are available.

Function	Description
Detection Time	How long (in seconds) that the input must change state before it is considered "triggered". Actions and alerts associated with the Input will not occur until the Detection Time has passed.
Schedule	Optional. Select an Input Schedule from the drop-down list. This schedule will instruct the IO Master to only monitor this input during a specific time.
Holiday Group	Optional. Select a Holiday Group from the drop-down list. This option will instruct the IO-Master to use an alternate schedule which can be defined when adding Holidays to the system.
Action	Choose from the list of actions available. Available actions will be covered in the next table.
Option: Supervised	Choose if you are using resistors to supervise the input from tampering (can be ignored in most cases).
Option: Normally Closed/Inverted	Choose if the Input is normally closed. This is the case often with door contacts.

VAX-IO-STR-2Input Functions

VAX-IO-STR-2 panels have additional input functions due to increased processing power. These are used for unmanaged and monitored doors. See the section called “Unmanaged and Monitored Doors with IO-Boards”for more information.

Table 30.5. VAX-IO-STR-2 Input Functions

Function	Description
Door Contact	This Input function is used for Inputs that track if the Door is open or closed such as magnetic door contacts. Also referred to as a door position switch.
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.
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.
Aux Input	This Input function has the most configurable options, including Input actions such as pulsing Outputs, overriding Doors, activating alarms.

Actions:

Actions are optional when configuring Inputs; these actions can target a single or up to 5 Outputs connected to the same IO Master Panel. Only Outputs configured as Aux Outputs can be targeted by an action. The following are the various actions you can perform with Inputs.

Table 30.6. VAX-IO-STR-2 Input Actions

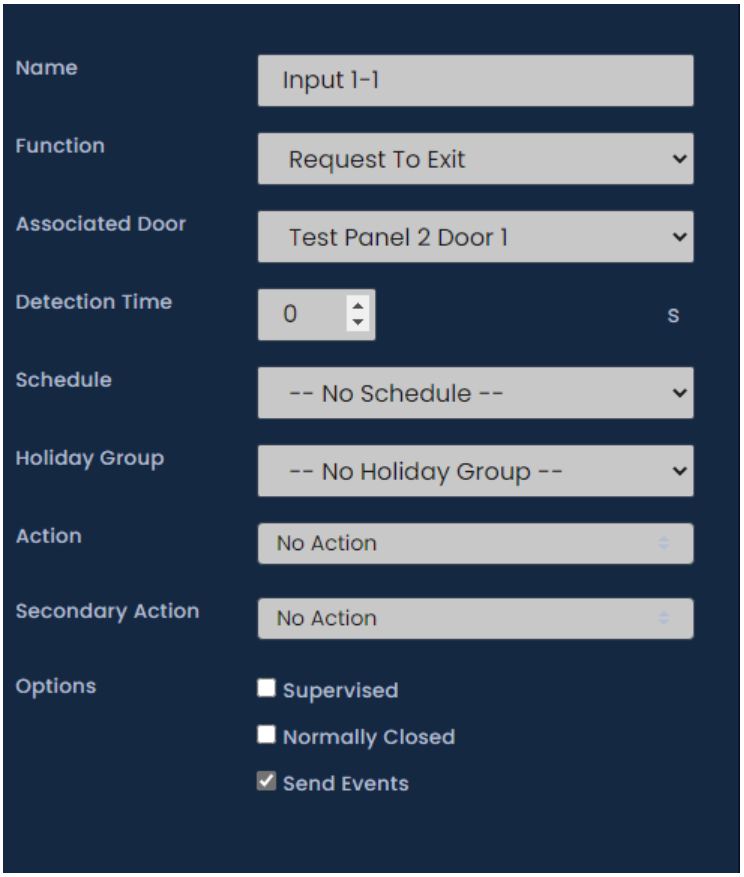
Action	Description
No Action	Actions are optional; an event will still be generated when input conditions are met and server side script triggers can still execute.
Output Activate	Activates an output, selectable via drop down list.
Output Toggle	Toggle an output to the opposite state, selectable via drop down list.
Output Deactivate	Deactivate the selected Output, selectable via drop down list.

Action	Description
Output Pulse High	Pulse an Output to close, configure a delay and the duration of the pulse.
Output Pulse Low	Pulse an Output to open, configure a delay and the duration of the pulse.
Output Pulse Opposite	Pulse an Output to the opposite of its current state, configure a delay and the duration of the pulse.
Output Activate Multiple	Activate multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Output Deactivate Multiple	Deactivate multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Output Toggle Multiple	Toggle multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Input Disable	Disable a selected input. Selectable from a drop-down list with delay and duration.
Unmanaged Door - Resume	Resumes an unmanaged door back to its normal schedule based on its Output Schedule.
Unmanaged Door - Override Lock	Override a selected unmanaged door to a locked state. State will remain until resume command.
Unmanaged Door - Override Unlock	Override a selected unmanaged door to an unlocked state. State will remain until resume command.
Unmanaged Door - Override Lock with Auto Resume	Override a selected unmanaged door to a locked state. State will resume its normal schedule at the next scheduled transition in the Output Schedule.
Unmanaged Door - Override Unlock with Auto Resume	Override a selected unmanaged door to a unlocked state. State will resume its normal schedule at the next scheduled transition in the Output Schedule.

Tip

VAX-IO-STR-2 panels have an additional input action called "On Action". It allows you to choose an additional action to occur and can be combined with other input functions such as door contact and request to exit.

Figure 30.6. Input Options



The following table demonstrates each of the fields available when an Output is selected:

Table 30.7. Output Options

Function	Description
Name	Unique name of your Output. Accepts 4 to 60 characters. We recommend naming your Output based on its function or device that will be connected to it.
Function	Function will dictate what Output options are available.
Associated Door	Select which door ports or door name the output will be associated to.
Schedule	Optional. Select an Output Schedule from the drop-down list. This schedule will instruct the IO-Master to only monitor this input during a specific time.
Holiday Group	Optional. Select a Holiday Group from the drop-down list. This option will instruct the IO-Master to use an alternate schedule which can be defined when adding Holidays to the system.
Option: Normally Closed	Choose if the Output is normally closed.
Options: No Events	Outputs with this option selected will not generate events when the Output changes state.
Options: Protected	Outputs with this option selected cannot be targeted by any Input actions.
Options: Initially On (If No Schedule Selected)	The Output will start as "on" (closed) until it is affected by an Input action or Override from the server.

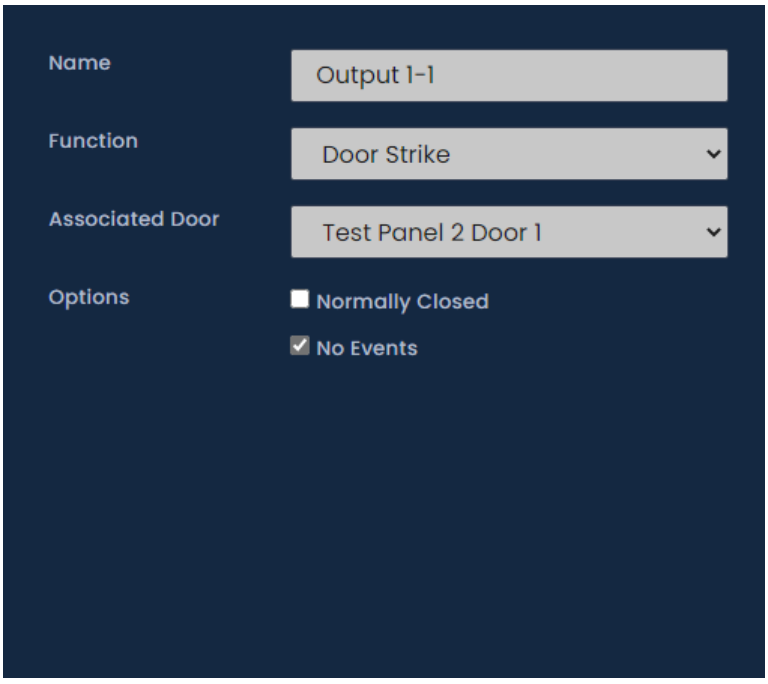
VAX-IO-STR-2 Output Functions

VAX-IO-STR-2 panels have additional input functions due to increased processing power. These are used for unmanaged and monitored doors. See the section called “Unmanaged and Monitored Doors with IO-Boards”for more information.

Table 30.8. VAX-IO-STR-2 Output Functions

Function	Description
Door Strike	Configures the output to act as if a lock is connected such as a door strike, maglock, gate, etc. Uses Output Schedule set on output options.
Secondary Door Strike	Configures the output to follow the state of the door strike associated to the same door.
Door Unlocked or Open	Configures the output to activate when the associated door is open via door contact state or open unlocked based on door strike state.
External Buzzer	Configures the output to activate when the associated door is forced or held open.
Global Buzzer	Configures the output to activate when any doors on the same VAX-IO-STR-2 panel are forced or held open. Configurable which doors will do this.
Aux Output	General purpose output that can have a schedule based on Output Schedule. Can change state based on overrides or input actions.

Figure 30.7. Output Options



Input and Output Schedules

This section will cover Input and Output schedules. Inputs and Outputs on IO-Boards can be placed on a schedule.

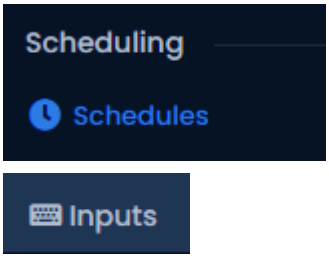
Input Schedules

Input Schedules are schedules you can place on Inputs to dictate when it will be monitored and when the Input will be ignored.

Two modes are available: Not Monitored and Monitored. In a single day you can transition between these modes up to 5 times.

To add a Input Schedule:

1. On the **Side Bar**, scroll down to **Scheduling**; click on the **Schedules** icon (pictured below). Select the **Inputs**tab (pictured Below).



2. On the Input Schedules screen, you'll see the default Schedules. If additional Input Schedules are needed, click the **Add** button on this screen.

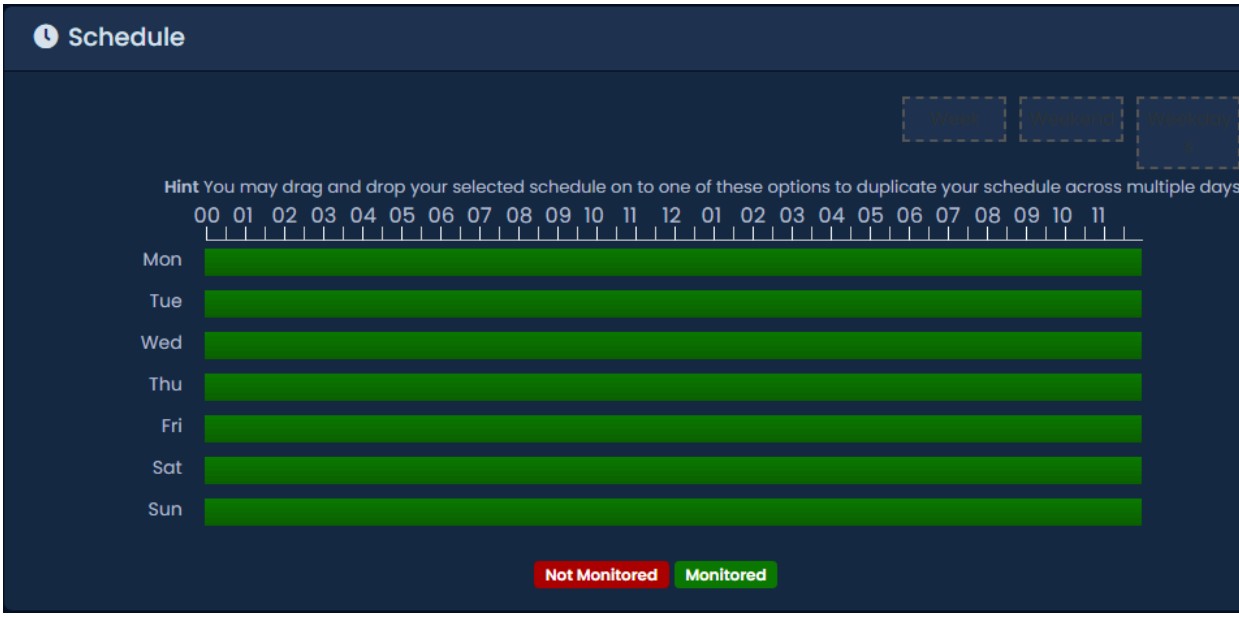
3. On the **Add Input Schedule** screen, you'll have a couple text boxes to populate.

Table 30.9. Add Input Schedule

Text Box	Description
Name	Unique name of your Schedule. Accepts 4 to 255 characters. We recommend naming your Schedules by the function of the schedules.
Description	Optional description of the Schedule. Accepts 4 to 255 characters.
Partitions	Select the Partitions you'd like to create this Schedule in. If more than one are selected, a copy will be created for each Partition.

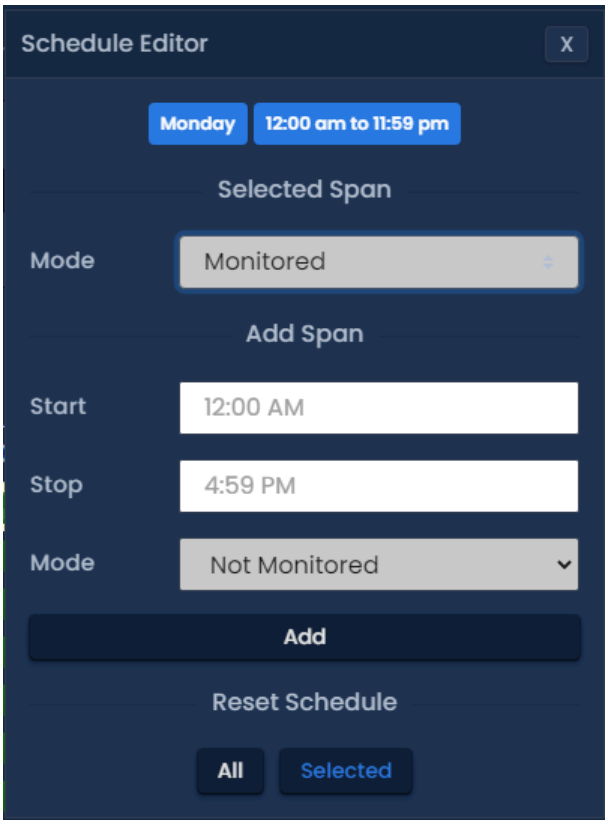
4. Creating the **Schedule** is the last step in creating a Input Schedule. Below is what the schedule part of the add Schedule page looks like.

Figure 30.8. Input Schedule Schedule



5. Click on any of the horizontal bars in the time schedule to bring up the **Schedule Editor Widget**. The Schedule editor widget is a simple and powerful tool for creating schedules.

Figure 30.9. Schedule Editor



6. Use the **Mode** drop-down menu to select the Input state for the **selected** time span. This is useful for defining what state the Input will be in the entire day, or changing the mode for already present spans.

7. The **Add Span** section of the Schedule editor has 3 fields used for adding a Input Schedule span. The **Start** and **Stop** fields, when clicked, will bring up a slider menu for selecting the stop and start times. The second **Mode** drop-down menu will dictate what Input state the schedule will follow during the defined time span. Once you've completed these fields, click the **Add** Button.

8. You should now see the bar you selected color coded to time span you've added. Add additional time spans to that day if required.

   If you'd like the Schedule you've created to be used for several different days, you can click on the bar with your completed Schedule, and select the **Copy** dropdown list to select which day of the week the schedule should be copied to. The Schedule will be replicated based on which date option is selected.

9. Once your Input Schedule for all 7 days is as desired, you may now press **Save** to create the Input Schedule in the selected Partitions. The Input Schedule can now be assigned to Inputs when adding or creating IO-Master Panels.

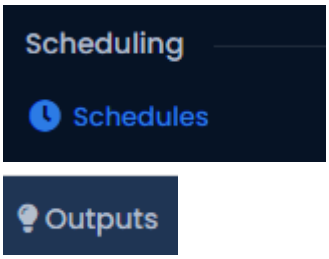
Output Schedules

Output Schedules are schedules you can place on Outputs to dictate when it will be Open or Closed (On or Off).

Two modes are available: On and Off. In a single day you can transition between these modes up to 11 times.

To add a Output Schedule:

1. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **Schedules** icon (pictured below). Select the **Outputs**tab, (pictured below).



2. On the Output Schedules screen, you'll see the default Schedules. If additional Output Schedules are needed, click the **Add** button on this screen.

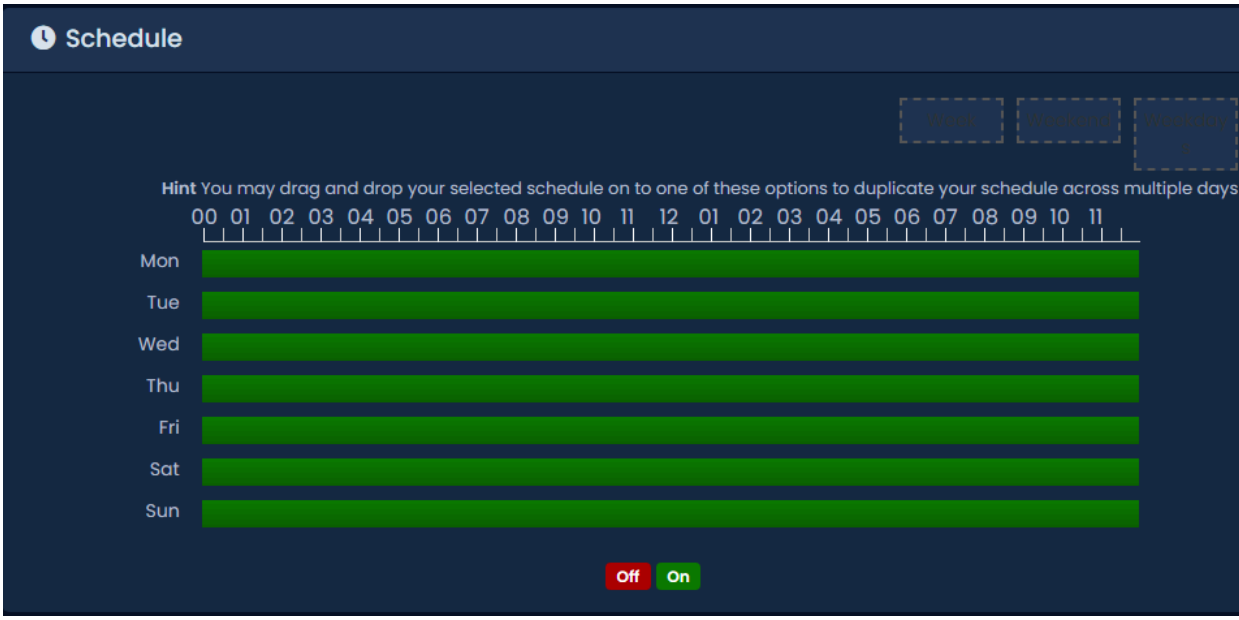
3. On the **Add Output Schedule** screen, you'll have a couple text boxes to populate.

Table 30.10. Add Output Schedule

Text Box	Description
Name	Unique name of your Schedule. Accepts 4 to 255 characters. We recommend naming your Schedules by the function of the schedules.
Description	Optional description of the Schedule. Accepts 4 to 255 characters.
Partitions	Select the Partitions you'd like to create this Schedule in. If more than one are selected, a copy will be created for each Partition.

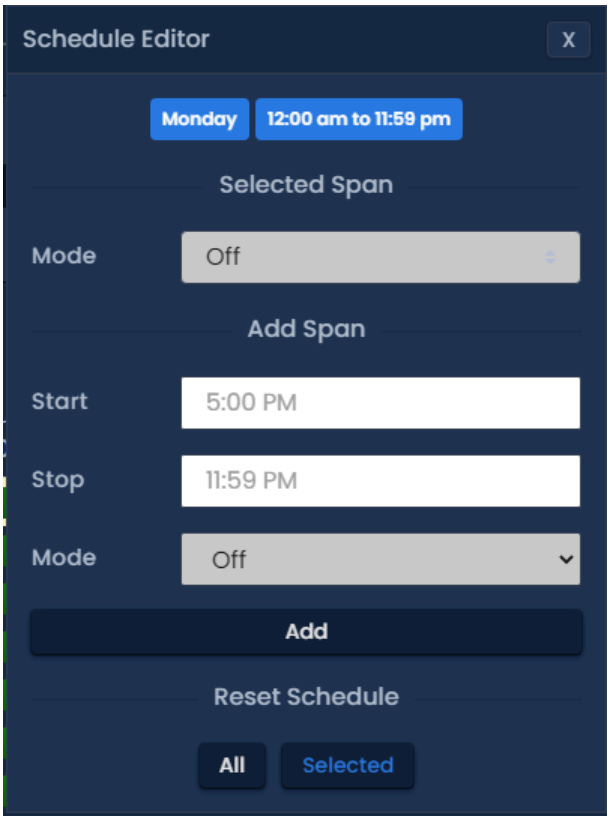
4. Creating the **Schedule** is the last step in creating a Input Schedule. Below is what the schedule part of the add Schedule page looks like.

Figure 30.10. Output Schedule Schedule



5. Click on any of the horizontal bars in the time schedule to bring up the **Schedule Editor Widget**. The Schedule editor widget is a simple and powerful tool for creating Schedules.

Figure 30.11. Schedule Editor



6. Use the **Mode** drop-down menu to select the Output state for the **selected** time span. This is useful for defining what state the Input will be in the entire day, or changing the mode for already present spans.

7. The **Add Span** section of the Schedule editor has 3 fields used for adding a Output Schedule span. The **Start** and **Stop** fields, when clicked, will bring up a slider menu for selecting the stop and start times. The second **Mode** drop-down menu will dictate what Output state the schedule will follow during the defined time span. Once you've completed these fields, click the **Add** Button.

8. You should now see the bar you selected color coded to time span you've added. Add additional time spans to that day if required.

   If you'd like the Schedule you've created to be used for several different days, you can click on the bar with your completed Schedule, and select the **Copy** dropdown list to select which day of the week the schedule should be copied to. The Schedule will be replicated based on which date option is selected.

9. Once your Output Schedule for all 7 days is as desired, you may now press **Save** to create the Output Schedule in the selected Partitions. The Output Schedule can now be assigned to Outputs when adding or creating IO-Master Panels.

Unmanaged and Monitored Doors with IO-Boards

Unmanaged and Monitored doors are openings that do not have controlled access (reader or method of controlling access) but do have other door hardware such as door contacts as door strikes. The input from the door contact is used to determine if the door is open or closed. Additional actions can be configured to occur when the door opens. This section will review how to add these types of doors.

The following chart defines the difference between these types of doors:

Table 30.11. IO Door Types and Features

Door Type	Supported Panel Type	Features
Monitored	VAX-IO-STR-2	Only supports door contact and camera associations. Limited output functions. 64 Door limit per VAX-IO-STR-2
Unmanaged	VAX-IO-STR-2	Supports door contact, door strike, REX, motion sensor, camera associations, remote override and additional output functions. 16 door limit per VAX-IO-STR-2

Use the following steps to configure an unmanaged or monitored door.

1. Navigate to the Edit Panel screen for the IO-Master Controller that you are connecting your unmanaged door to (Home, Panels, Edit Panel) .

2. Click on the IO tab on the Edit Panel screen. Use the I/O Expander drop-down menu and select the appropriate expander that your door hardware is connected to.

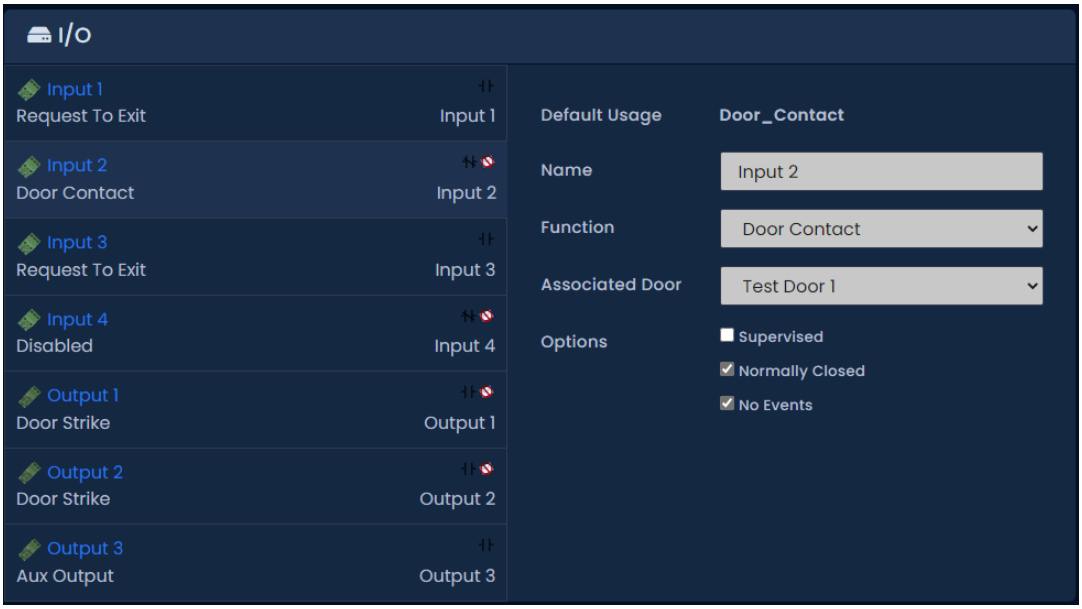
3. Select the input your door hardware is connected to on the left side of the page.

4. You can rename the input to make the system easier to understand.

5. Change the Function drop-down menu to Door Contact or the appropriate function. Door contact must be configured before you can add a Monitored door.

6. You can optionally configure the input to perform other actions just like you would any other input. You may want to configure the input as normally closed if the function is a door contact.

Figure 30.12. IO Board Door Contact



7. For VAX-IO-EXP8-PCB inputs and outputs, you must select an associated door in order for the input to function. Repeat the above process for any inputs and outputs connected to door hardware.

8. After changing any required inputs to door contacts or other input and output functions, click Save on the bottom of the page.

9. From the **Side Bar**, scroll down to the section titled **Hardware**, click on the **Doors** icon (pictured below).

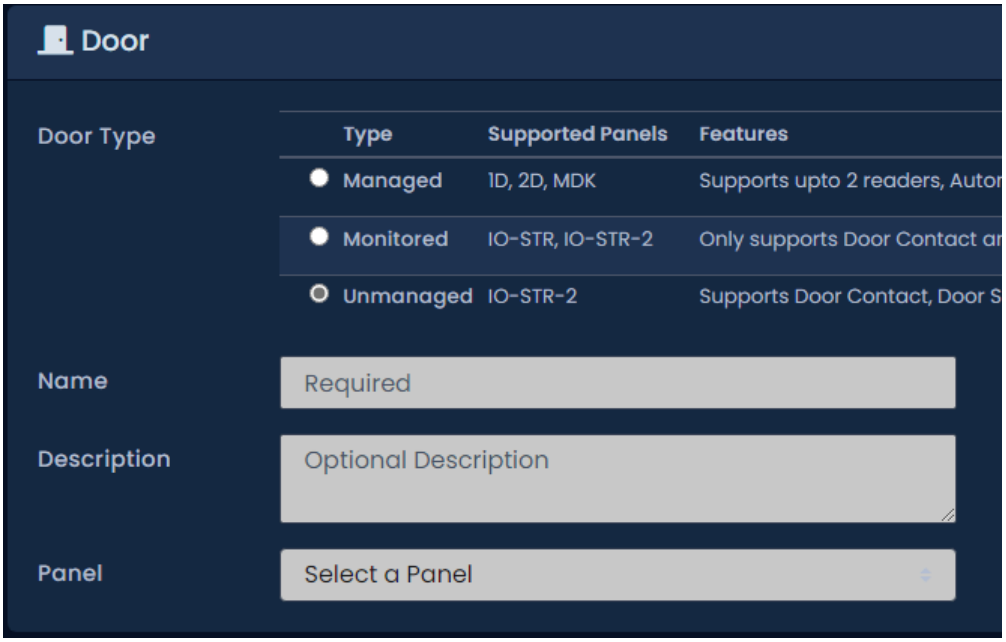
10. On the **Doors** screen, you'll notice any Doors you've already configured listed here. Click the **Add** button on this screen.

11. On the **Add Door** screen, select Unmanaged as the Door Type.

12. Select the IO board your door contact is connected to on the Panel drop-down menu.

13. Select the input your door contact is connected to on the Input drop-down menu.

Figure 30.13. Add Door Screen



14. Click Save.

15. Once added, you will be able to change door specific settings, associate a camera to the door and view the status of the door on the System Overview page, Map Viewer and others. Notifications related to the door will appear just like other door notifications.

Real World Applications For Inputs and Outputs

By utilizing multiple Input and Output functions, the IO boards can be used for a huge verity of purposes. Below are several common situations where security integrators have used our IO-Boards.

- **Camera System Action Trigger**:

  Most modern camera NVR/DVR systems support dry contact inputs that can trigger specific actions such as 'start recording camera downstairs' or 'change camera position to location B'. By utilizing certain Output functions from our regular door controllers, you can connect one of the extra relays to an Input on an IO-Board. The door controllers can now be configured to give a signal to the Camera systems through the IO-Boards based on specific parameters such as:

  - Door Forced or Held Open
  - Door Unlocked or Open

- **External Devices/Systems:**

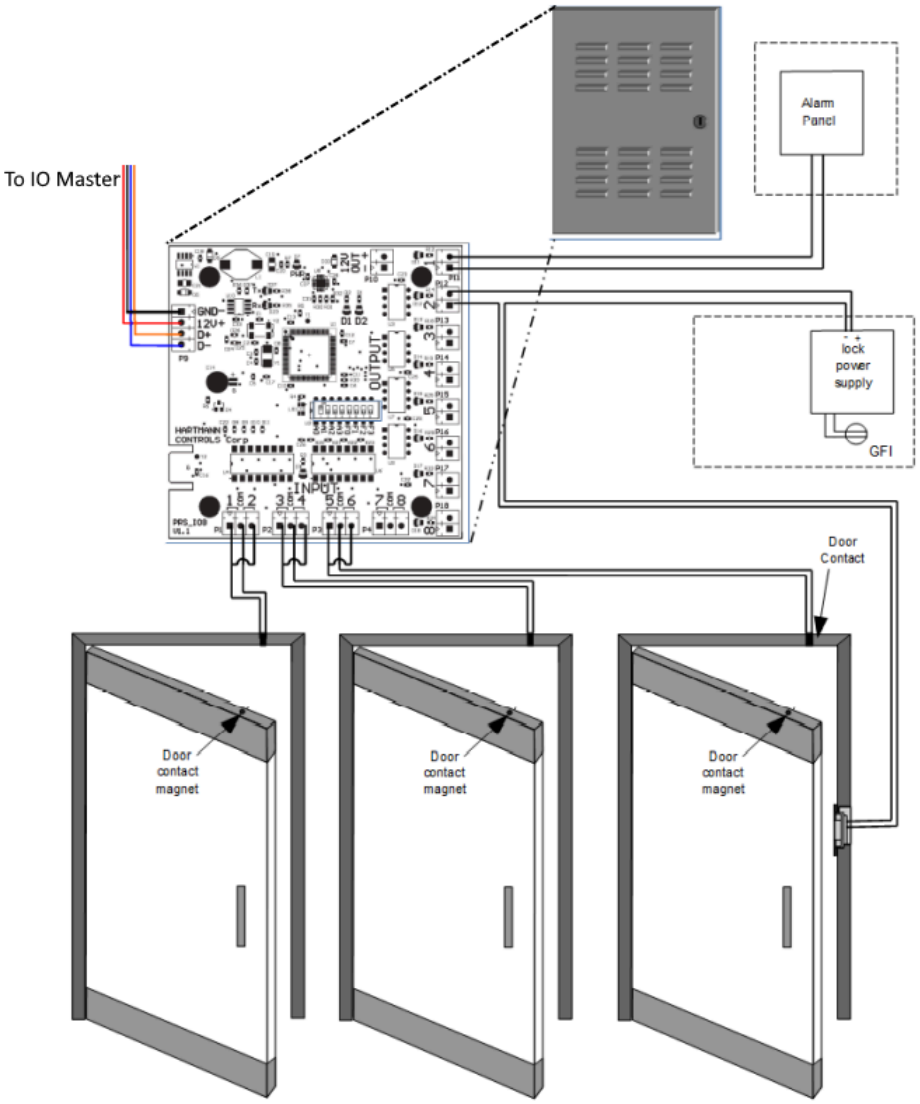
  It is possible for other external systems and devices to interact with the IO-Boards, as long as they are able to provide the IO-Board a dry contact to close the Input to one of the common grounds on the IO-Board. This can include various inputs such as sensors, buttons, switches or Output devices such as motors or lights. The following table will demonstrate some examples of external devices that may be capable of interfacing with the IO-Board:

Table 30.12. External Devices

Device	Description
Glass Break Detector	Unique name of your Output. Accepts 4 to 60 characters. We recommend naming your Output based on its function or device that will be connected to it.
Glass Break Detector	Connect multiple Glass break detectors to quickly get notified of a glass break event and notify the alarm system.
Photoelectric Beams	Monitor these beams during off business hours to detect intruders. Use outputs to notify the alarm system and activate sounders/lights.
Motion sensors	Monitor motion sensors during off business hours to detect intruders. Use outputs to notify the alarm system and activate sounders/lights.
Shock Detectors	Can be used on a verity of applications.
Temperature Sensor	Configure the sensor to only trigger when specific temperature criteria has been met.
Buttons/Switches	Buttons and key switches can easily trigger an Input on the IO-Board.

The following diagrams demonstrate how some external devices can be connected to the IO-Board.

Figure 30.14. IO-Board Example



Chapter 31. Camera System Integration

VAX is capable if integrating with a variety of Video Management Software (VMS) and some Network Video Recorders (NVR). Integrating with VMS systems allows you to perform the following functions:

- Integrate with cameras from multiple VMS systems, including instances across LAN/WAN/Internet.
- Real time video monitoring displays imported cameras from the VMS right in your web browser. Real time video can be displayed based on pre-defined alerts such as Door Held Open, Door Forced Open, etc.
- Associate cameras with Doors and Elevators. Associate PTZ cameras based on camera preset positions.
- Linking of video and notifications based on pre-defined events provided by the access control software.

VAX currently integrates with the following Video Management Systems:

Table 31.1. Video Management Systems

System	Minimum Version	Notes
ViconNet	8.0	Web Server must be enabled.
Milestone xProtect	2016	Web Server must be enabled.
Exacq exacqVision	7.4.3	Web Server must be enabled. SSL Certified needs to be generated.
Digital Watchdog DW Spectrum	2.4	Web Server must be enabled.
Vicon Valerus	1.2	SSL Certificate may need to be generated.

Supported Browsers

This section will display which camera systems are compatible with which web browsers.

Table 31.2. Video Management Systems

System	Support Browsers	Notes
Vicon Valerus	Internet Explorer 11	• Requires Valerus Plug-in. • Supports multiple cameras in matrix. • Good video quality and performance. • Very Low video latency. • No mobile support.
Vicon ViconNet	Internet Explorer 11	• Requires Silverlight Plug-in. • Supports multiple cameras in matrix. • Supports iris and focus adjustments. • Good video quality and performance.

System	Support Browsers	Notes
		• No mobile support.
Milestone xProtect	Internet Explorer 11 Opera 35.0 Google Chrome Mozilla Firefox Apple Safari	• Uses HTML5, supported on many platforms. • Stream utilizes JPEGs, medium performance and quality. • Shows on-screen when recording or motion detected. • Mobile supported.
Exacq exacqVision	Internet Explorer 11 Opera 35.0 Google Chrome Mozilla Firefox Apple Safari	• Uses HTML5, supported on many platforms. • Stream utilizes JPEGs, medium performance and quality. • Web Sockets supported. • Mobile supported.
Digital Watchdog DW Spectrum	Opera 35.0 Google Chrome Mozilla Firefox Apple Safari	• Uses HTML5 streaming via WebM protocol. • Good video quality and performance. • Buffers live stream, causing 5-10 second delay for real-time video. • Limited mobile support.

Enable the VMS Web/Mobile Server

This section will outline what is required before VAX can synchronize and view cameras on the VMS.

Each system will need their respective VMS Web Server enabled. For more specific details on enabling and configuring the web server on a specific VMS, please contact the dealer/installer of the VMS or the VMS manufacturer.

Enable Web Server: Valerus Configuration

1. Valerus will have HTTP server enabled by default.
2. Import or create self-signed SSL certificate as outlined by Valerus documentation or Vicon support.
3. Proceed to the section called “Adding a Camera System”.

Enable Web Server: ViconNet

1. Login to a ViconNet Nucleus.
2. Enable the ViconNet web and mobile server as outlined in the ViconNet Installation and Configuration Guide.
3. If you are using HTTPS (recommended), use a web browser and browse to the URL of the ViconNet server. Accept any certificate warnings and proceed.
4. You should add the Self-Signed ViconNet SSL certificate; this process is outlined in the section called “Adding Website Certificates for Camera Integration”.

5. Proceed to the section called “Adding a Camera System”.

Enable Web Server: Milestone XProtect Mobile

1. Login to the server hosting Milestone XProtect.
2. Install the Milestone Mobile Server component as outlined by the XProtect Mobile Administrator's Manual.
3. Create self-signed SSL certificate as via XProtect Mobile certification manager.
4. Setup IFrame configuration with the following steps:
   a. Browse to "C:\Program Files\Milestone\Milestone Mobile Server\Web" on the Milestone Mobile server.
   b. Copy and paste the folder "C:\Program Files (x86)\Vicon\VAX\WebServer\milestone" from the VAX web server into the Web folder from the previous step. Rename the milestone folder to VAX.
   c. On the Milestone Mobile server, open VideoOS.MobileServer.Service.exe.config from the installation directory with administrative privileges. You can use a file editing program such as notepad.
   d. Search for the key "Content-Security-Policy". Add "https://computer:11001" at the end of "frame-src ‘self’". It should look like:

      ```
      <add key="Content-Security-Policy" value="default-src 'self'; script-src 'self'; connect-src 'self' ws://* wss://*; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; frame-src 'self' https://VAX:11001" />
      ```

   e. Search for the key "PlainTextAuthenticationEnabled". Set the value as "True".
   f. Search for the key "X-Frame-Options". Remove "DENY" from the value. Leave the value blank or set it to "ALLOW-FROM https://servername:11001".
5. Use a web browser and browse to the URL of the XProtect Mobile server. Accept any certificate warnings and proceed.
6. You should add the Self-Signed XProtect Mobile SSL certificate; this process is outlined in the section called “Adding Website Certificates for Camera Integration”.
7. Proceed to the section called “Adding a Camera System”.

Enable Web Server: Exacq exacqVision Web Services

1. Login to the server hosting exacqVision.
2. Enable the exacqVision Web Service as outlined in the Web Service User Manual.
3. Use a web browser and browse to the URL of the exacqVision web interface. Accept any certificate warnings and proceed.
4. You should add the Self-Signed exacqVision SSL certificate; this process is outlined in the section called “Adding Website Certificates for Camera Integration”.
5. Proceed to the section called “Adding a Camera System”.

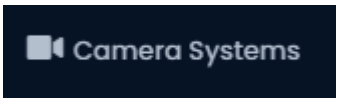
Enable Web Server: Digital Watchdog DW Spectrum

1. DW Spectrum Web Server should be enabled by default.
2. If you are using HTTPS (recommended), use a web browser and browse to the URL of the DW Spectrum web interface. Accept any certificate warnings and proceed.
3. You should add the Self-Signed DW Spectrum SSL certificate; this process is outlined in the section called “Adding Website Certificates for Camera Integration”.
4. Proceed to the section called “Adding a Camera System”.

Adding a Camera System

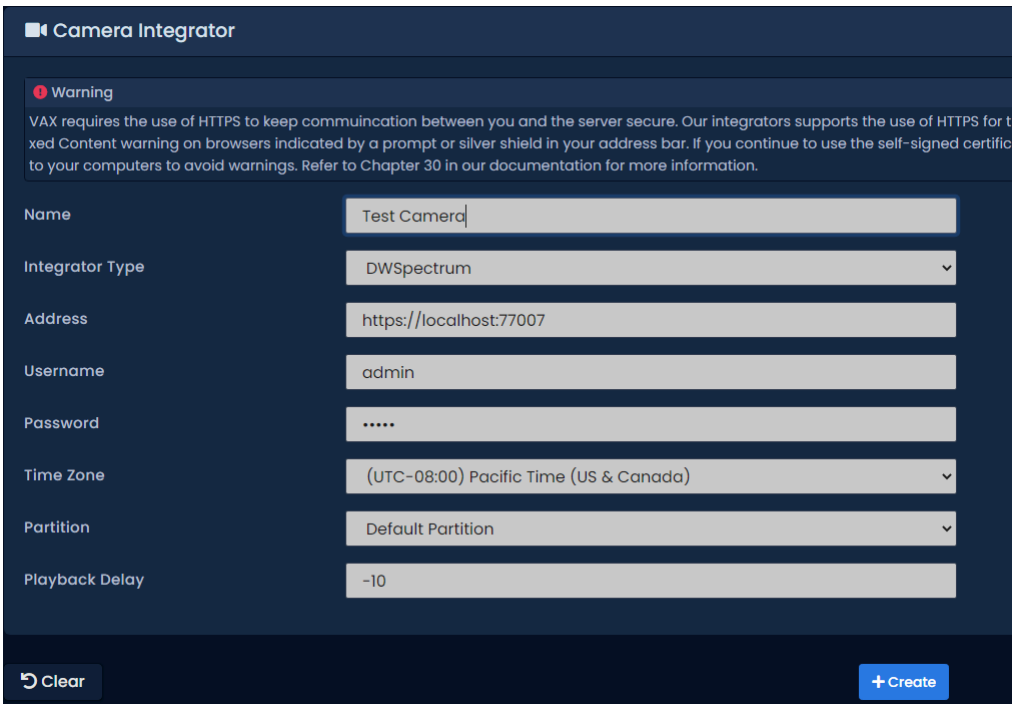
Adding a camera system (VMS) allows you to associate cameras to Doors/Elevators and view historical playback and real-time video.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Camera Systems** icon (pictured below).



4. On the **Camera Systems** screen, you'll see any other camera systems you’ve already added. You can connect to multiple camera systems if required. Click the **Add** button on this screen.

Figure 31.1. Add Camera System Screen



5. On the **Add Camera System** screen, you'll have a few text boxes to populate.

Table 31.3. Add Camera System

Text Box	Description
Name	Unique name of your camera system. Accepts 2 to 255 characters. We recommend naming your camera system based on location or function.
Integrator Type	Choose the correct integrator type based on the VMS you'd like to integrate with.
Address	The address of the server/computer hosting the VMS. This can be a name or an IP address. Include http/https header. Include the port number used by the video management software if not using default port 80. The port number is only required if not using the default port 80 (http) or 443 (https).
Username	The username that will be used to access the VMS. This can be located in your camera management software.
Password	The password for the VMS account that will access the VMS. This can be located in your camera management software.
Time Zone	The local time zone the camera system will reside in.
Partition	The partition the camera system will be located in.
Playback Delay	Number of seconds difference to sync notification time to recording time.

6. Once you have filled in the required fields, you may now press **Save** to create the camera system in the selected partition. You'll be prompted to add another system, or continue configuration for camera system you just added.

Warning

If the VMS is using HTTPS (recommended), you will likely need to add the SSL certificate of the VMS to any client computers that will be viewing cameras through VAX. Please see the section called “Adding Website Certificates for Camera Integration” for more details on this process.

Manage Camera Systems

Once you've added a camera system, the next step is to synchronize the available cameras from the VMS and enable which cameras you would like to integrate with VAX.

If you just added a Camera System, clicking **"Continue Configuration"** will bring you to the **Manage Cameras Screen**; otherwise:

1. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Camera Systems** icon (pictured below).

2. On the **Camera Systems** screen, you'll see any camera systems you've already added. Click the blue edit button next to the camera system you would like to modify.

Once on the **Manage Camera Systems** screen for a specific camera system, the next step is to synchronize cameras (retrieve a list of available cameras or camera groups) and select which cameras you want the Access Control System to have access to.

1. Click the **"Synchronize Cameras"** drop-down button and choose if you want to synchronize all cameras on the camera system, or by certain camera groups (if the VMS supports it). Synchronizing cameras by groups allows you to import pre-defined groups from the camera management software; this is useful on sites with a large number of cameras.

   ### Note

   Depending on the number of cameras in the video management software, this process may take up to a few minutes. The process will also let you know if it fails to communicate with the server.

2. Once the synchronization process is complete, you'll see a list of available cameras that was retrieved from the VMS System.

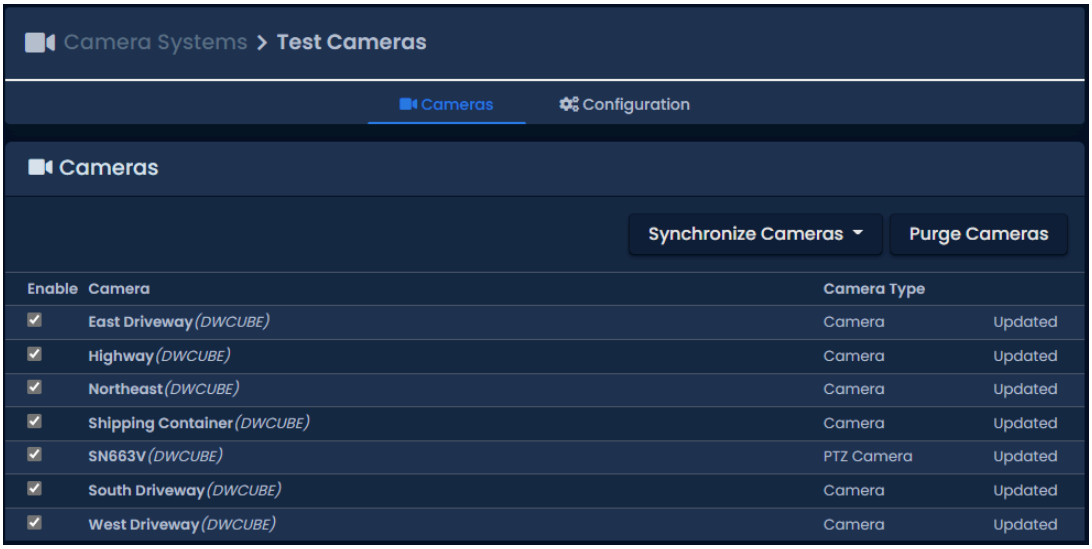
3. Each camera in the list will contain the name of the camera imported from the VMS, the camera type, if it's a new or missing camera and if the camera is enabled.

4. The **Enable** checkbox beside each camera dictates if the camera is available to the Access Control System for door association or viewing.

   ### Warning

   Once a camera is enabled, this will count towards the camera limit imposed by your product license.

Figure 31.2. Manage Cameras Screen



Purging Cameras

When a camera in the camera management software is removed or renamed, the cameras will need to be re-synchronize. If the access control software detects that a camera that was available previously no longer exists, it will be labelled as "Not Found". When this happens, and the camera is not expected to be available again, we can purge the camera from the system. This will remove the camera and all associations that camera has to Doors and Elevators.

To remove cameras that no longer exist, simply synchronize cameras to detect which cameras are no longer available; click the**"Purge Cameras"** button once if you see any cameras that are "Not Found".

Figure 31.3. Purging Cameras

GPU Acceleration

On the configuration tab of the **Edit Camera System** page, there is an option titled **GPU Acceleration** may appear if the VMS supports it. This option is used to borrow processing power from the computer video card when clients are viewing cameras; this can help offload CPU load on the client computer.

Note

This feature requires a compatible video card and web browser.

WebSockets

The configuration option Use WebSockets may appear if the VMS supports it. This option is used to use WebSocket transport protocol and can make transporting camera playback more efficient.

Note

This feature requires compatible operating systems (Windows 8 or higher).

Use Proxy

This is exclusively an option for Valerus. When enabled, requests to view, and commands to cameras will use the VAX web server as a proxy for web requests. This will bypass some SSL certificate errors when HTTPS is used.

Viewing Synchronized Cameras

Viewing cameras in VAX can be done in several ways; we also support inline camera view that can be triggered based on events such as Access Denied or Door Forced Open. This section will cover viewing live video and playback video.

Warning

In order to view cameras in VAX over HTTPS communication, you must first create a trust between the client computer browsing to VAX and the VMS web server. In order to do this we must import a certificate from the VMS server or the SSL certification needs to be registered with valid Certificate Authority. Please see the section called “Adding Website Certificates for Camera Integration” for more details on this process.

1. On the **Side Bar**, scroll down to the section titled **Day to Day**; click on the **Camera Viewer** icon (pictured below).

On the Camera Viewer screen, you'll have several options for viewing cameras in your system.

Figure 31.4. Camera Viewer

Tip

You can quickly view live feed of a single camera by clicking directly on the camera icon next to the name of each camera on this screen.

Viewing Live Video

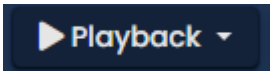
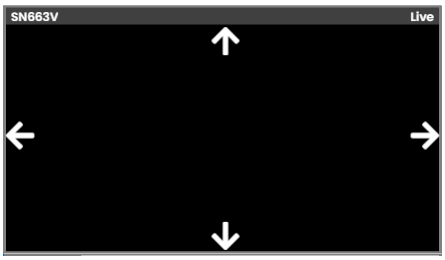
To view live video on the View Cameras screen, input the following parameters:

1. **Camera System**: Select the Camera System you would like to view.
2. **Matrix Size**: If the VMS supports a video matrix, you can select a matrix size. By default, the system will automatically choose the best size for the amount of cameras you are viewing.
3. **Mode**: Select **Live Video** as the mode.
4. **Cameras**: Select which cameras you would like to view. You can select multiple cameras if the VMS supports a video matrix.
5. Once you've selected the camera(s), you can now click the **"View Live Video"** button on this screen.

Figure 31.5. Camera Viewer

6. A new window will appear over your current screen. This is the **Camera Viewer**. It will show live video of the camera you selected. You'll have several options on this screen; some will be dependent on the type of camera or VMS you are viewing:

Table 31.4. View Camera Options

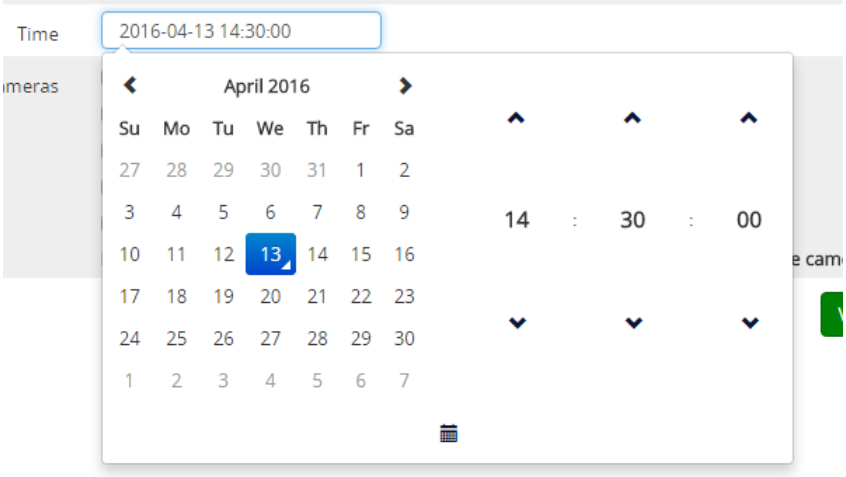
Option	Description
	This button will change the camera mode to playback. You can use the Up arrow to select where to start playback based on the current time or select a time with the date and time picker.
	PTZ Only. Pan Speed will influence how fast a PTZ camera will move when changing positions manually or with auto pan.
	PTZ Only. The Apply button will move the camera to the selected preset position; this also allows you to set presets based on the current camera position with the Set button.
Camera Quality	ExacQ Only. Low quality can be selected to save bandwidth at the expense of stream quality.

7. If your screen is black or has any errors on the bottom such as "Error Retrieving Video" or "source", please see the applicable chapter in our Tech Guide.

Viewing Playback Video

To view playback video on the View Cameras screen, input the following parameters or click:

1. **Camera System**: Select the VMS system you would like to view.
2. **Matrix Size**: If the VMS supports a video matrix, you can select a matrix size. By default, the system will automatically choose the best size for the amount of cameras you are viewing.
3. **Mode**: Select **Playback Video** as the mode.
4. **Time**: When the mode is selected as **Playback Video**, the **Time** field will need to be filled. Clicking in the text box will present the time and date widget; select the time you would like to view video playback.



5. **Cameras**: Select which cameras you would like to view.

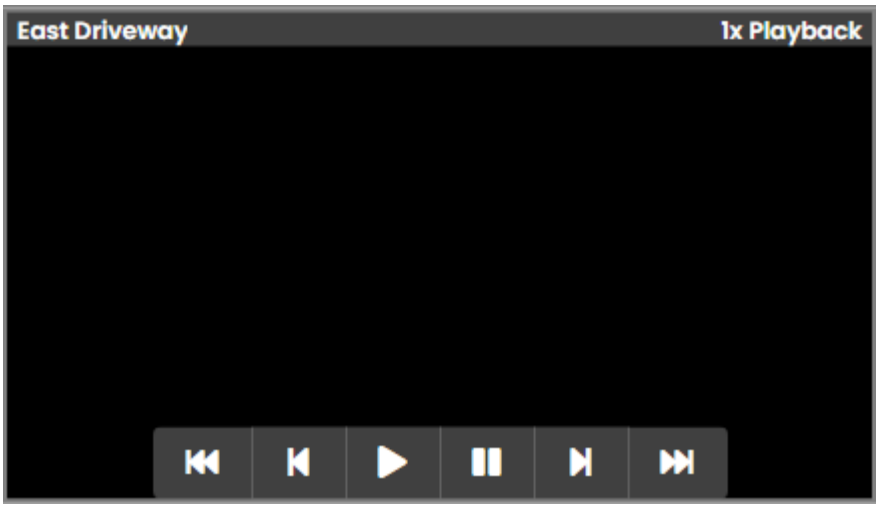
6. Once you've selected the cameras, you can now click the **"View Playback Video"** button on this screen.

7. A new window will appear; this is the playback camera viewer. It will begin playback at the time selected.

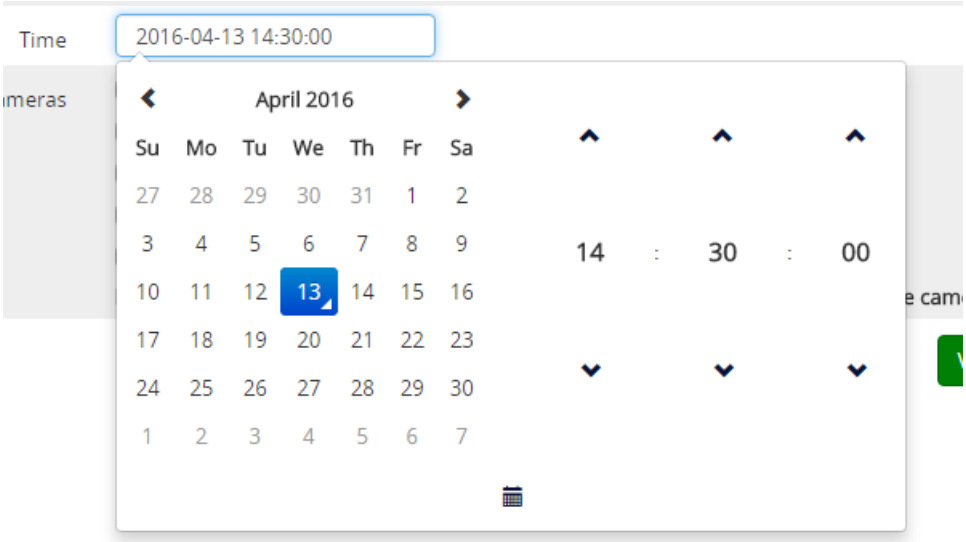
Tip

You can switch back to live video at any time by pushing the **Live Video** button on the camera viewer.

8. On the camera viewer, you'll have options specific to video playback.



9. You can choose a new time for the video playback by clicking the button displayed below:



Associating Cameras with Doors and Elevators

VAX allows support for cameras to be associated with Doors/Elevators. This is so notifications can be linked to playback video.

Door/Elevator to cameras associations also allow us to display an inline camera view when alerts occur on a door associated with that camera, such as Door Forced Open and Door Held Open.

Use the following steps once your cameras have been synchronized and enabled in the system:

Camera Associations: Door

1. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Doors** icon (pictured below).

2. On the **Doors** screen, you'll see any Doors you've already configured listed here. Click the blue button next to the door for which you'd like to configure a camera association.

3. On the **Edit Door** screen, you'll see there are 6 tabs, each with their own configuration items. Click on the **Camera Association** tab; this is where we will configure camera associations for this door.

Figure 31.6. Camera Association tab of the Edit Door screen

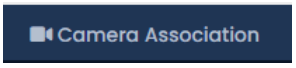
4. Select the camera you would like to associate with the door. If the VMS supports matrix views, you may select more than one.

Tip

You can associate a camera with a preset position if the camera is a PTZ camera.

Camera Associations: Elevator

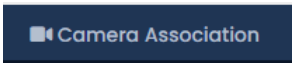
1. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Elevators** icon (pictured below).



2. On the **Elevators** screen, you'll see any elevators you've already configured listed here. Click the blue button next to the elevator for which you'd like to configure a camera association.

3. On the **Edit Elevator** screen, you'll see there are 4 tabs, each with their own configuration items. Click on the **Camera Association** tab; this is where we will configure camera associations for this elevator.

Figure 31.7. Camera Association tab of the Edit Elevator screen.



4. Select the cameras you would like to associate with the elevator.

Tip

You can associate a camera with a preset position if the camera is a PTZ camera.

Camera Notifications

Once a camera is associated with a door/elevator, an icon will appear next to all notifications related to that device, including live and playback video. Clicking the camera icon will bring up a playback

camera viewer that will match the time of the event. Any reports will also have a camera link next to each entry that includes a device with a camera associated to it.

Figure 31.8. Door Notifications With Camera Link

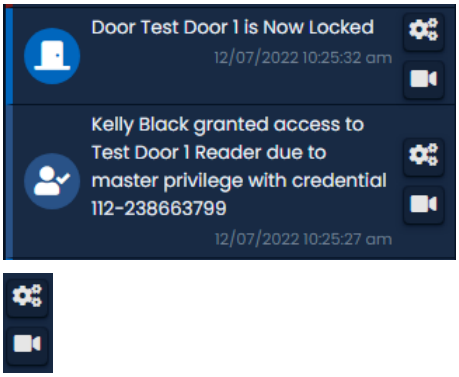


Figure 31.9. Elevator Notifications With Camera Link

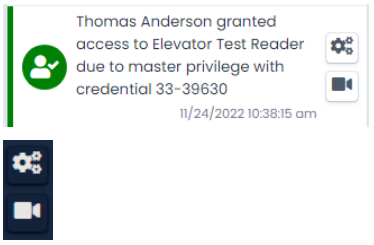
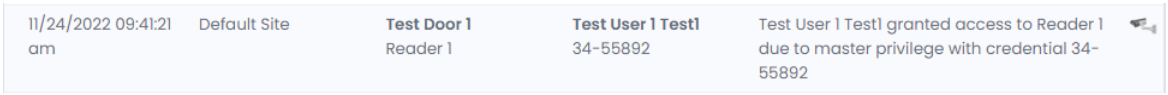


Figure 31.10. Door Activity Report With Camera Link

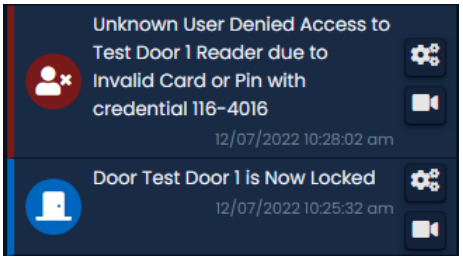


Configuring Live Camera Alerts

Once doors and elevators have camera associations, VAX supports configuration for event messages to display an inline video feed above the notifications area.

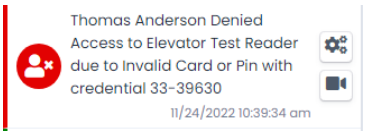
This is useful for time critical events such as Door Forced Open, Door Held Open, or cards being denied access to a secured area. This section will go over the configuration of these alerts.

Figure 31.11. Inline Camera View based on Denied Access



Configuring specific notifications for use with the inline camera viewer is covered in the section called “Live Camera Rules”.

We can open an external display for live video notifications using the button highlighted below.



While this external display is open, notifications with the live video option will display in the new window, not the notification bar.

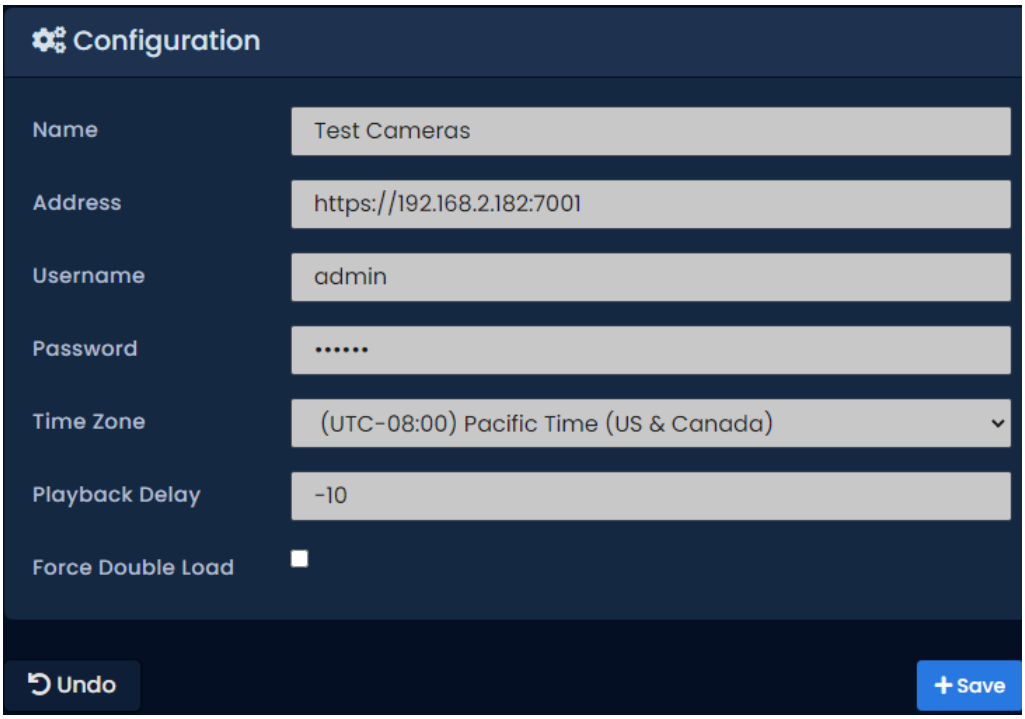
Adding Website Certificates for Camera Integration

VAX uses secure HTTPS secure communication. If the VMS is using HTTPS as well, we must create a "trust" between the client PC and the VMS. If the VMS web server is using a self-signed certificate (as opposed to an official certificate purchased from a company, such as godaddy.com), you must add the self-signed certification generated by the VMS web server. This does not apply if you are using regular HTTP communication.

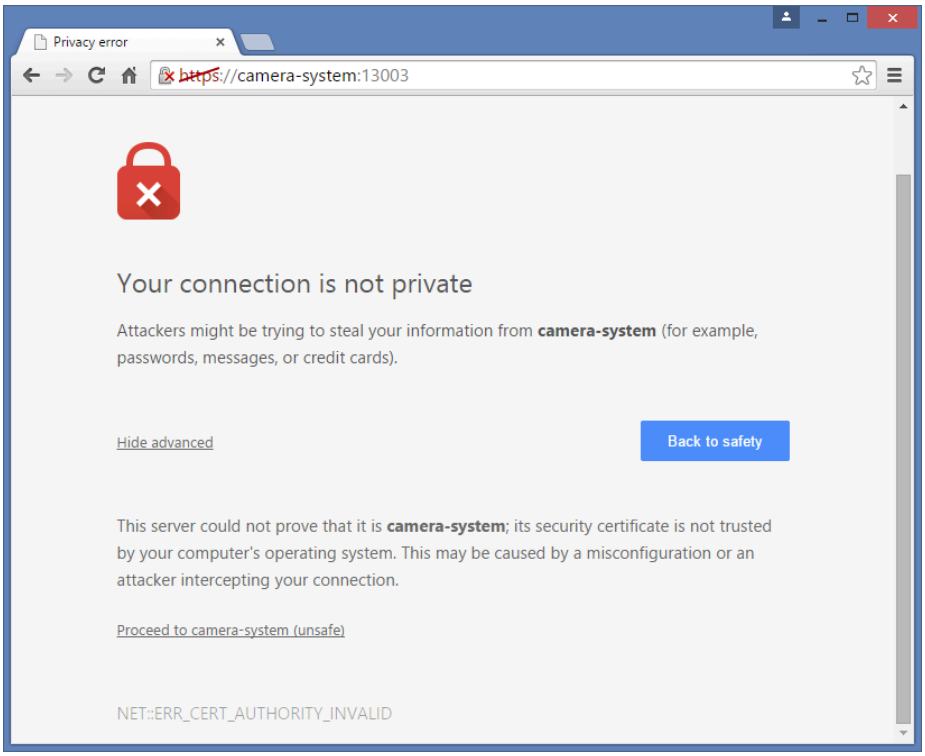
The following instructions will work on most operating systems and web browsers.

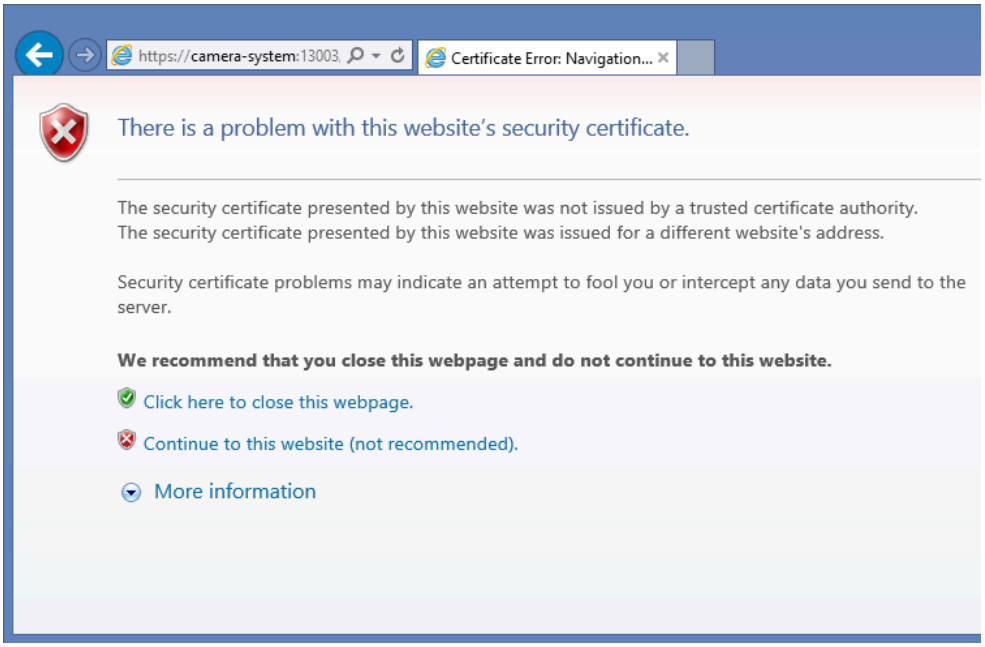
1. Log into VAX. On the main page scroll down to the section titled "Hardware"; click on the Camera Systems icon.

2. Click the blue edit button next to the camera system you would like to add a certification for. Click on the "Configuration" tab.



3. On the configuration tab, copy the text box titled "Address". We will need to browse to this address in another tab of our web browser in order retrieve the certification file. Copy the URL and place it into a web browser address bar. Press enter and you should see the following message (depending on your browser).

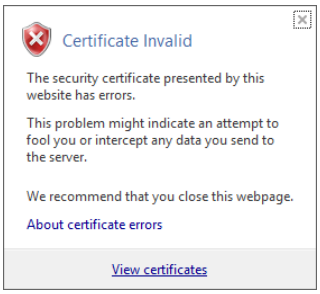




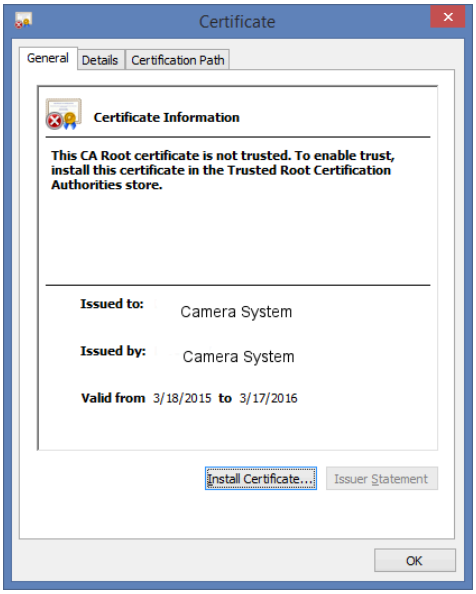
4. The next step is to extract the certification so that we can install it on our computer.

Importing Certification in Internet Explorer

1. In Internet Explorer, click "Continue to this website"; once the site loads you'll see a red button in the URL titled "Certificate Error". Click on this button; a small pop-up will appear. Click "view certificates".

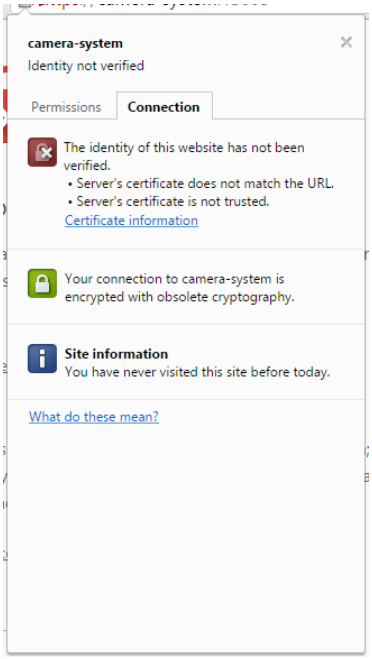


2. On the certificates window, click "install Certificate" on the bottom of the window. The certificate Import Wizard will now appear. Please proceed to the section called “Importing Certificates with the Certificate Import Wizard” to continue the certificate import process.

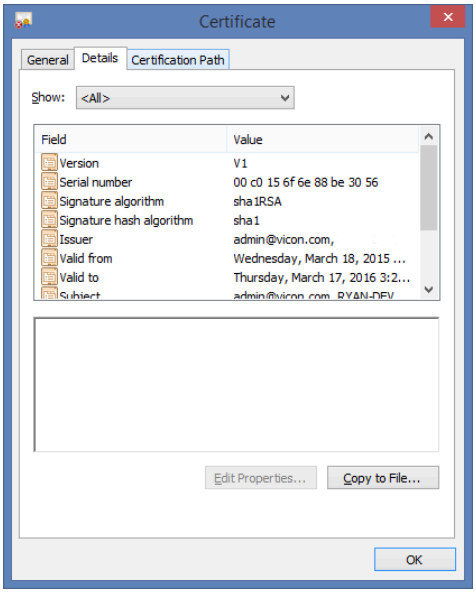


Importing Certification in Google Chrome.

1. In Google Chrome: Once you see the message "Your connection is not private", click on the icon that looks like a padlock in the URL with an "X" through it. A small window will appear.

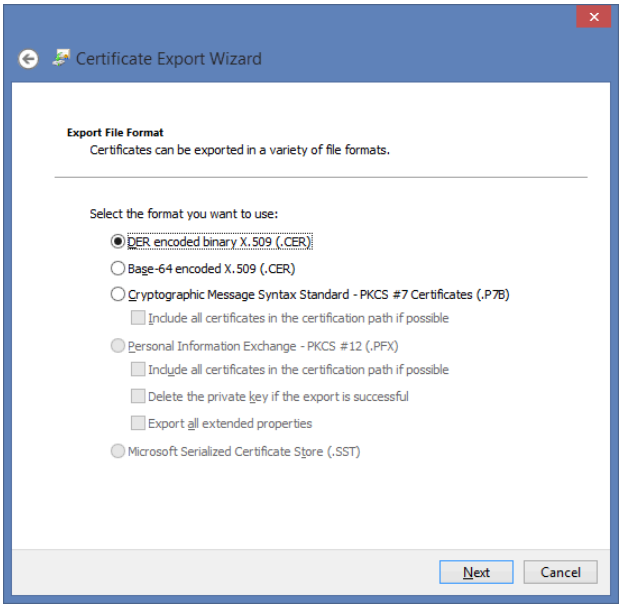


2. On this window, click the link titled "Certificate Information". A new window will appear. Click on the Details tab of this window.

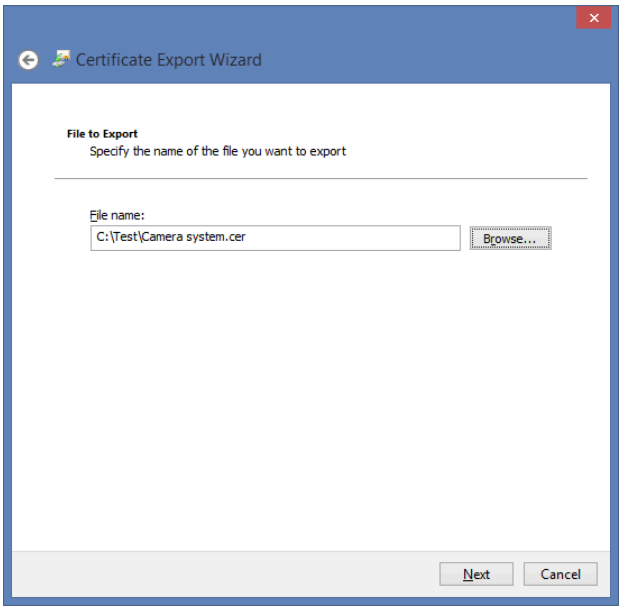


Click on the "Copy to File" button on this screen. This will launch the Certificate Export Wizard.

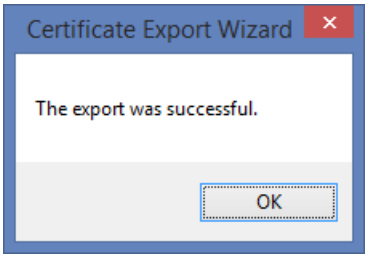
3. On the first page of the certificate export wizard, click "Next". On the "Export File Format" screen, click "Next".



4. On the "File to Export" screen, browse to the location you would like to save the certificate. You must name the file as well. Click "Next".



5. On the last screen, click "Finish". The certification filed will now be exported to the selected location.

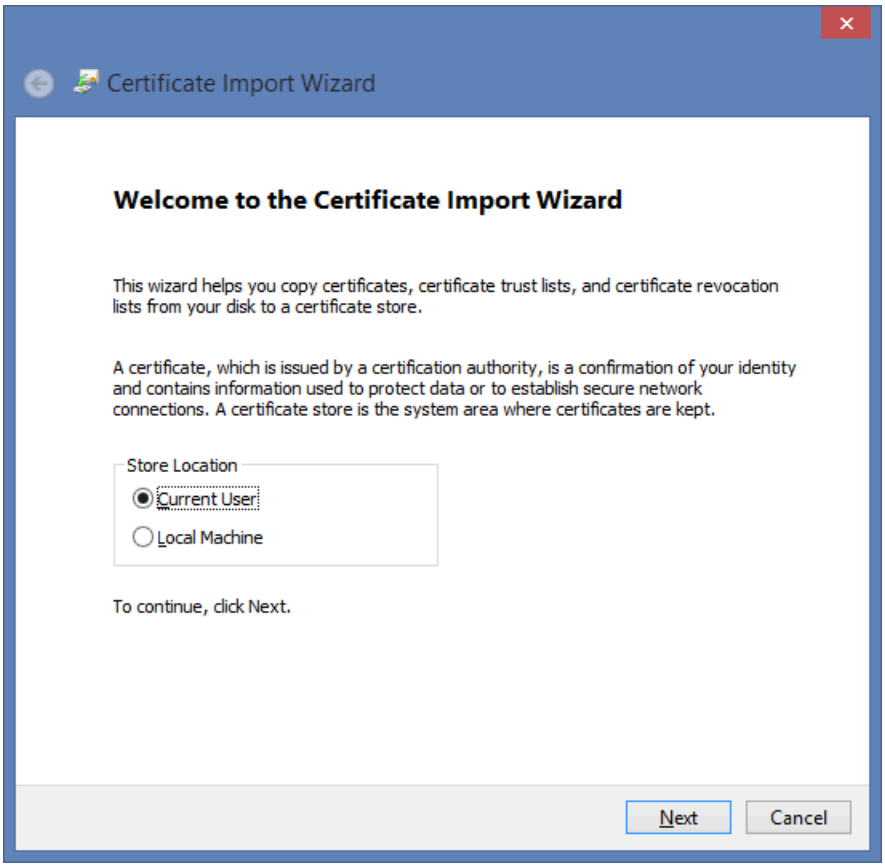


6. Browse to the location you exported the certification file. Right click on the file and select "Install Certificate". This will now launch the Certificate Import Wizard. Please proceed to the section called “Importing Certificates with the Certificate Import Wizard” for further instructions.

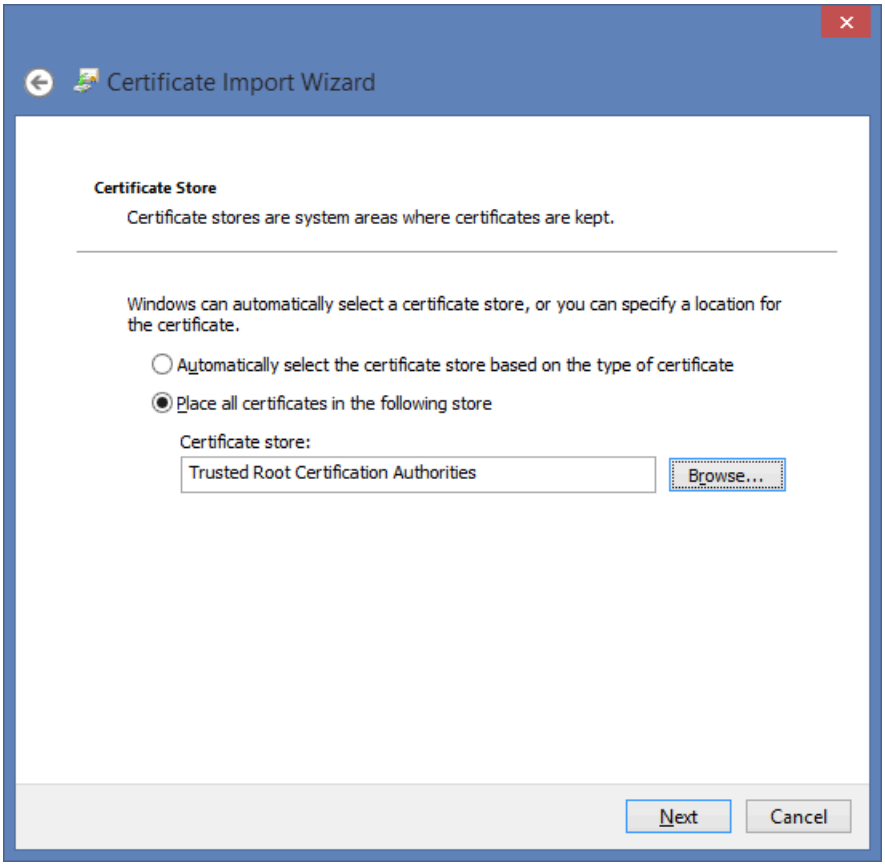
Importing Certificates with the Certificate Import Wizard

This section covers how to proceed once you bring up the certificate import wizard. This can be accessed by clicking "Install certificate" in Internet Explorer, or after exporting a certificate from Google Chrome and double clicking the saved file.

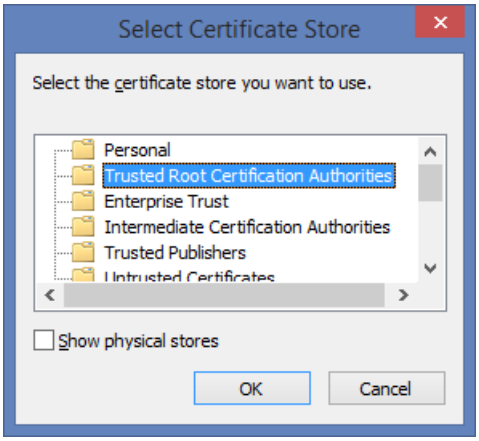
1. On the first screen of the import wizard, select "Current User" as the Store Location; if more than one Windows user will be utilizing the VAX web interface, select "Local Machine". Click Next.



2. On the next screen, select "Place all certificates in the following store" and click the browse button.



3. A small window will appear with various folders; select "Trusted Root Certificate Authorities" as the certificate store. Click "OK". Click "Next" again.



4. On the last screen, click "Finish". You will be prompted that you are about to install a certificate. Click "Yes" to install the certificate.

5. You must restart your web browsers and clear your browser cache before the new settings will take affect.

Note

This process must be done on all client computers that will be viewing camera systems through VAX via HTTPS protocol. Failure to do so will result in the error "Failed to load list of sites".

Multi-vendor Camera Matrix

The Camera Matrix is a full screen in VAX dedicated to viewing cameras in a grid view. Cameras from multiple vendors can be viewed simultaneously. A maximum matrix size of 4 x 4 is supported.

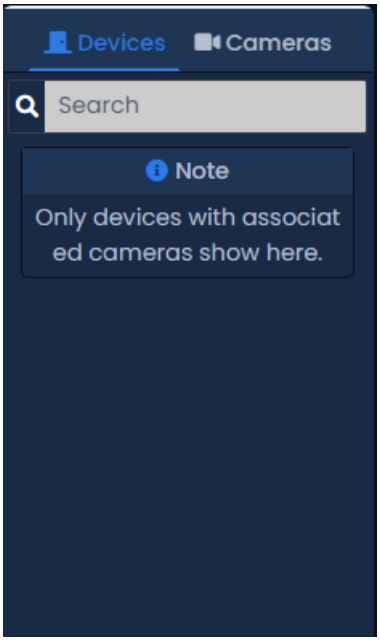
On the **Side Bar**, scroll down to the section titled **Day To Day**; click on the **Camera Matrix** icon (pictured below).

The Camera Matrix screen will open in another tab or external window.

Figure 31.12. Camera Matrix With Cameras

On the left side of the screen is your **Devices** list and **Camera** list.

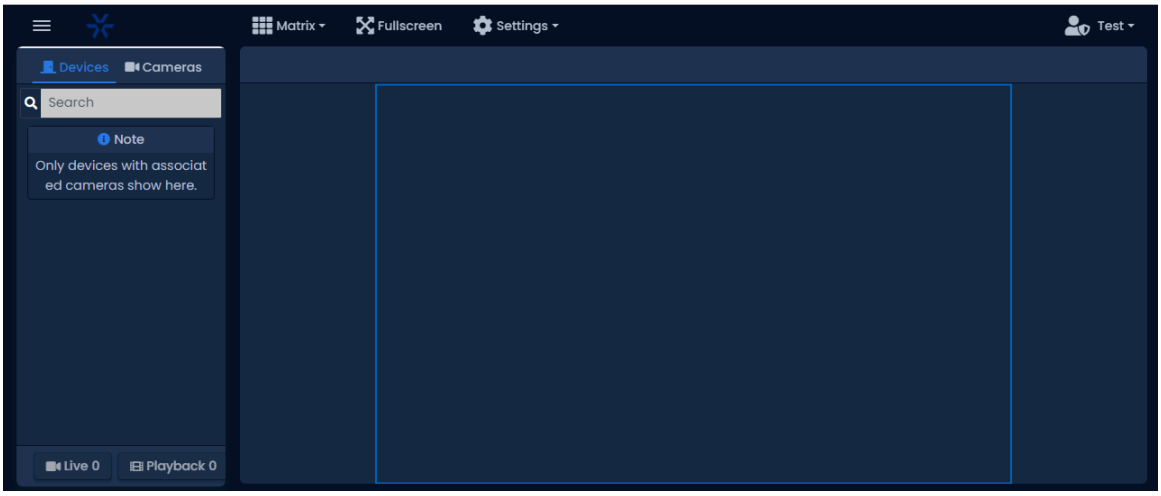
Figure 31.13. Devices List



When **Devices** is selected, you'll get a list of Doors and Elevators with cameras associated to them. When **Cameras** is selected, you'll get a list of camera systems and cameras.

On the top left side of the screen are various page options.

Figure 31.14. Devices List



Click **Devices** to toggle the device list on the left side. Use this to maximize screen space for viewing cameras.

Click **Matrix** to select a Matrix size. 1x1 to 4x4 are available.

Click **Fullscreen** to make the current web browser into full screen mode. Use this to maximize screen space for viewing cameras.

Click **Settings** to reveal page specific settings. Enable Restore On Load to allow the page to remember which cameras were being displayed upon reload. Show PTZ Controls can be toggled to remove PTZ controls from the inner window when viewing PTZ cameras.

Viewing Cameras in Matrix

To view live video or playback, do the following:

1. Click Settings on the top of the page. Select the appropriate Matrix Size.
2. On the Devices and Camera list, expand the tree view. When you want to view a camera, simply click and drag a camera or device into one of the video windows in the middle of the screen. You can check multiple cameras off and click Live or Playback on the bottom of the screen.
3. When a camera is being viewed

Tip

You can right click on the inner window when viewing a camera to quickly change between Playback and Live video. You can also access PTZ presets this way.

Chapter 32. Active Directory Integration

This chapter will outline the benefits and steps needed to integrate VAX with an LDAP provider such as **Microsoft Active Directory(AD)**. An IT administrator is strongly recommended and likely required in order to successfully integrate. This chapter should be reviewed in its entirety before AD integration is attempted.

Integration Overview

Active Directory integration allows VAX to do the following:

- Import Users from an existing Active Directory (AD) server and give them access to Doors/Floors based on the AD Security Groups they are in.
- Synchronize VAX Users with AD Users based on a timer or triggered manually from VAX.
- Users in AD that are disabled will have their access rights to Doors/Floors removed (depending on AD polling time).
- Associate custom fields in VAX with AD User Attribute fields.
- Import Credential information (Card/Fob/PIN) from AD User Attribute fields.
- Allow LDAP authentication for VAX Administrators. Allows VAX Administrators to login to VAX with AD domain credentials.

AD Integration Order of Operations

In order to maximize efficiency and minimize configuration time, we recommend the order of operations outlined by this guide. Each item in this list will be detailed in its own section.

1. Planning: What AD Information will be Synchronized
    a. Groups (optional): Create or choose Groups in AD that VAX will monitor. Note the Organizational Unit (OU) chain required to narrow the scope to those groups. VAX will only synchronize AD Users that are members of the selected groups.
    b. Credentials (optional): Credential information (Cards/Fobs/PINs) can be imported from AD User Attributes in Active Directory. Requires one or more available User Attribute Fields.
    c. Custom Fields (optional): AD User Attributes such as Address, Phone Number and many others can be associated with Custom Fields in VAX.
    d. LDAP Authentication (optional): If enabled, adding new Administrators in VAX will give you the option of using LDAP authentication instead of creating a username and password. No special configuration needed in AD.
2. Configure Service Accounts for VAX
    a. Choose or create a Service Account in Active Directory.
    b. Add the Service account as a member to the AD group "Read-only Domain Controllers" or an equivalent Group that gives the service account access to read Active Directory Users and Groups.

c. Add the local policy "Logon as a Service Right" to the Service Account VAX will run as on the server VAX will be installed on.

3. Install VAX

   a. Install VAX on a computer that is part of the domain; ensure the services are configured to run as the service account created in Active Directory.

   b. If required, change database permissions locally in SQL so that the Service Account has access to create/modify the VAX MSSQL database.

4. LDAP Integration Settings in VAX

   a. Perform initial configuration of VAX and login with the Initial Administrator (if not already done).

   b. Enter the Fully Qualified Domain Name in LDAP Integration Settings.

   c. Choose a Polling Time in LDAP Integration Settings (how often VAX will check for AD changes).

   d. Enter the Root Group OU (Optional). This will narrow the scope to the OU that contains the Groups that VAX will synchronize and monitor for Users.

5. Create Associations between AD Groups and Access Privilege Groups

   a. Create Associations between AD Groups and Rules that will define which Doors/Floors Users in those Groups will be given access to.

6. Importing Credentials From AD (Optional):

   a. Create Associations between AD User Attributes and a Credential Type.

7. Importing Custom Fields From AD (Optional):

   a. Create Custom Fields in VAX.

   b. Create Associations between AD User Attributes and VAX Custom Fields.

8. Synchronize AD: Perform first LDAP synchronization.

   a. Once all previous steps are complete, perform your first synchronization.

Planning: What AD Information will be Synchronized

This section will outline factors that should be considered in the planning phases of LDAP integration.

The following list contains information that is synchronized automatically for AD Users:

- First Name and Last Name
- User Expiry Date (expired users will no longer have access rights)
- User Status (disabled/enabled)
- Group Membership (only groups that have been added in VAX)

All other information (i.e.,credentials, custom fields) are optional and outlined in the next sections.

AD Groups, Membership and Structure

VAX synchronizes users based on the AD Security Groups in which they are members. You will choose the AD Security Groups from which you want to monitor/synchronize users.

Optionally, access can be granted to Doors/Floors based on the AD Security Groups in which the Users are members.

The following are factors that should be considered during this process:

- How granular do permissions to Doors/Floors need to be?
  - Anyone in AD should have access to all Doors/Floors:
    - An existing group (such as 'Staff' or 'Domain Users') can be used to give employees access to all Doors/Floors in the system.
  - Very specific groups of people require different access at different times:
    - If there isn't dedicated AD Security Groups for each type of user (HR, IT, Office, etc): Dedicated Security Groups should be created in AD to give access to Doors/Floors. AD Users should be assigned to the appropriate AD Groups prior to deployment.
- Should giving employees access to Doors/Floors be done from Active Directory or VAX?
  - Active Directory:
    - In this case, there should be one or more AD Groups specifically made for Access Control. Existing employees will be placed in one or more of these groups. VAX will be configured to give access to Doors/Floors based on AD Group membership.
    - Most administration will be done in AD. New employees will be placed into Access Control AD Groups and automatically given permissions to Doors/Floors.
  - VAX:
    - In this case, AD Users will by synchronized based on one or more groups. Once synchronized, a VAX administrator will give access to Doors/Floors based on VAX Groups.

User Credentials

User credentials (cards, fobs, biometrics, PINs) are what Users in VAX use to get access to Doors/Floors.

Credential information can either be added to Users in VAX after they've been synchronized from AD or credential information can be stored in AD User Attribute Fields and imported with the User.

The benefits of storing credential information in AD User Attributes include:

- Centralization of access control user management.
- Credentials are backed up and can be easily imported again if the VAX database is destroyed.
- When Users in AD are disabled, any corresponding credentials will have their access rights revoked to Doors/Floors.

Storing User Credential in AD User Attributes

We can import several credential types from one or more AD User Attribute Fields.

- Wiegand Credential from Single AD Attribute Field:

  The credential will start with a Site Code or Facility Code, followed by the Credential Number and a corresponding PIN (optional). Each entry should be separated by a comma. (example: 33,1528,1234 or 33,1529)

- Wiegand Credential with Fixed Site Code:

  The Site Code or Facility code will be set as a specific value in VAX. The Credential Number will be in a single AD User Attribute field. The optional PIN will be in its own field as well.

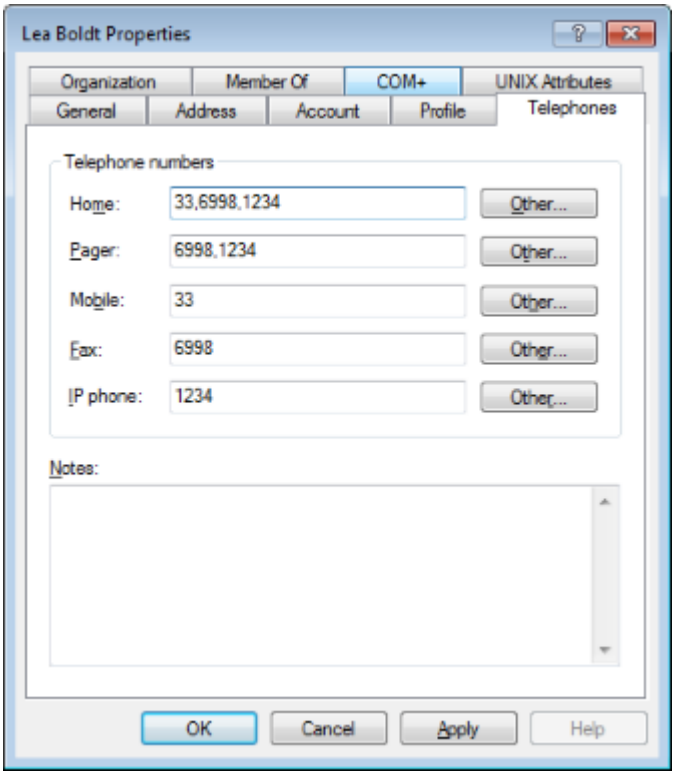
- Wiegand Credential from three Individual Fields:

  The Site Code or Facility Code will be in a single AD User Attribute field. The Credential Number as well as the optional PIN will each be in a single AD User Attribute field.

- PIN:

  The Site Code or Facility code be will be in a single AD User Attribute field.

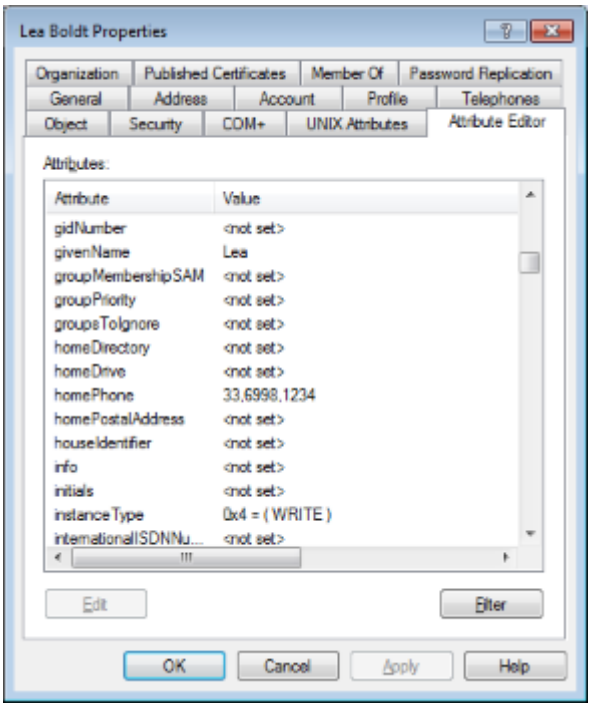
Example 32.1. Example of all types of credentials stored in AD User Attribute Fields



You can edit AD User Attributes in a list view; hidden and commonly unused AD User Attribute Fields can be found in this view.

In Active Directory Users and Computers:

1. Click View from the top menu.
2. Click Advanced Features. The window will refresh.
3. When editing an AD User, a new tab titled Attribute Editor will appear.



Configuring Service Accounts

This section will outline the steps needed to allow VAX to access domain resources, including access to Microsoft Active Directory via LDAP protocol. VAX runs as a Windows Service. It will need to be run as a Windows account that has permission to read LDAP information.

An IT administrator can either create a Managed Service Account (a special Windows account specially made for running services on a domain) or a normal Windows domain account with Domain and Service Account permissions.

Create and Configure Service Accounts

1. Login to a Windows domain controller with a Domain Administrator.
2. Open Active Directory Users and Computers.
3. Navigate to an OU where you will create the Service Account. We recommend using the Managed Service Accounts OU.
4. Right click the OU and select New, followed by User.
5. Create the new User. You can name it VAXService so that it can be easily found later. Record the logon name. Set a password. Make sure "User must change password on login" is not checked.
6. After the User is created, navigate to its Properties.
7. Add the User to the AD Security Group "Read-only Domain Controllers". This permission is required for VAX to make LDAP queries.

Next we must give the Service Account we created local permission to log on as a Service.

1. Login to the Windows computer that VAX will be installed with a domain administrator account or a local administrator.

2. Open "Local Security Policy". You can also find it by searching or entering "secpol.msc" into a Run window.

3. In the Local Security Policy Window, expand the "Local Policies" from the left side and select "User Rights Assignment".

4. In the policy list, right click "Log on as a service" and select Properties from the context menu.

5. On the properties Window, click 'Add User or Group'.

6. Search and select the Windows Domain Account created earlier on the domain. This will allow this account to login as a service.

7. Click OK and OK again on the previous page to apply this setting.

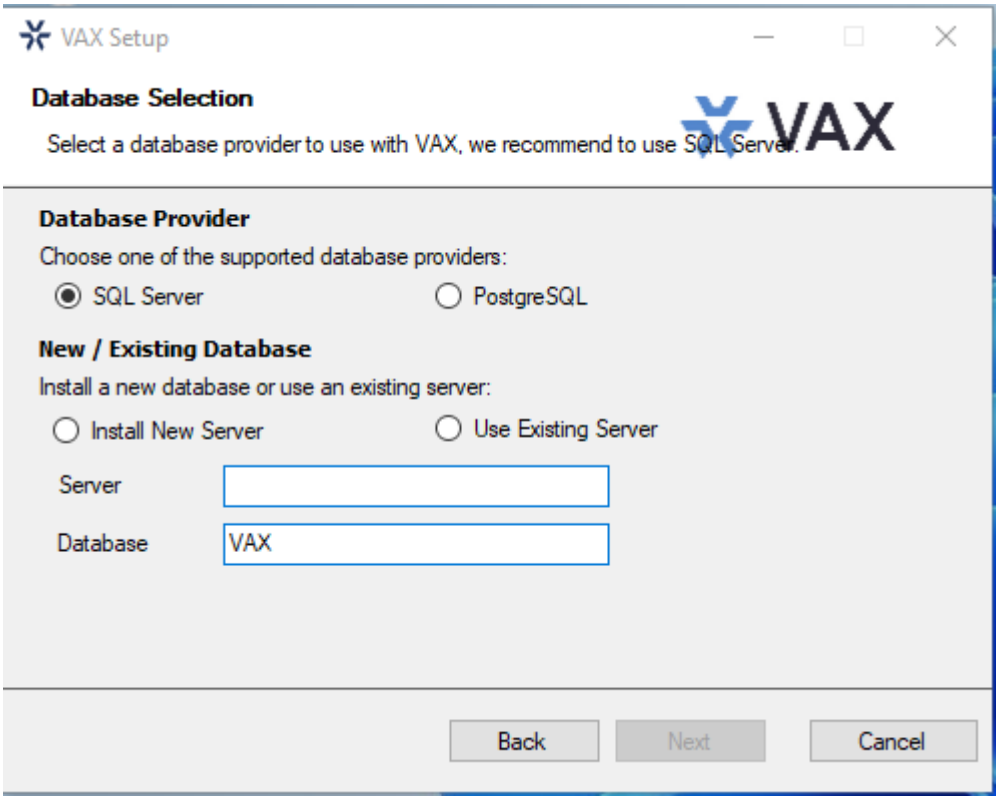
The service account configuration is now complete; you can now move on to installing the VAX server software.

Install VAX

This section will outline the software installation. The VAX software installer is smart. It will detect any missing components and install them for you. The following is a brief overview of the installation procedure. For better understanding or use of advanced settings please see the Installation/Upgrade Guide.

1. Run VAX.exe from the installation media or after downloaded from the web.

2. You will see a list of required components. A checkbox will appear next to any components that are missing.

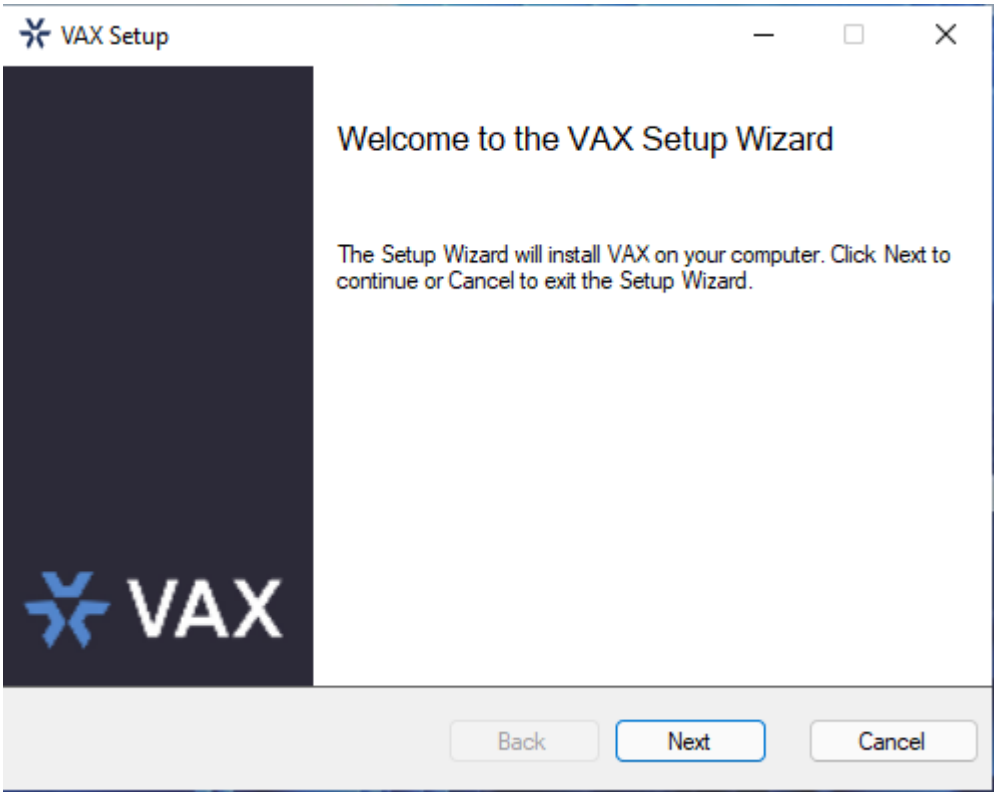


3. Click Install, any checked components will be installed. If you are installing from a VAX installation media; missing components will be installed locally. If installing from a web download, the installer will attempt to install those items from the internet.

Note

If any components fail to install, try restarting the computer and run the installer again. If components continue to fail installation, contact Vicon Industries technical support. Please see Chapter 37, *Support*.

4. Once any missing components are installed, the VAX Setup will begin.



a. Click Next.

b. Accept the EULA and click Next.

c. Select Advanced.

d. Click Next.

e. On the Service Configuration screen, enter the domain and username of the service account that was created in the previous sections (example, "corp\VAXService"). Enter the password of the service account. Repeat this for the System Manager section.

Caution

Do not include a Domain Suffix in the service account "Run as User" fields.

f. Click Next.

g. Click Next.

h. Click Next.

i. Click Install.

Note

If any services fail to install or fail to start, please see the section called “VAX Services Fail to Start”.

LDAP Integration Settings in VAX

This section will cover LDAP Integration settings in VAX.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **LDAP Integration** icon (pictured below).

4. Fill in the following fields on the LDAP Integration screen:

Table 32.1. LDAP Settings

Text Box/Check box	Description
Fully Qualified Domain Name	Enter the domain name associated with the Domain Controller (Example: Corp.local).
LDAP Polling Time	Enter the amount of time (in minutes) that VAX will wait between checking the AD server for changes on any users attached to groups that are being monitored.
Root Group OU (optional)	You can narrow the scope in which VAX will allow you to add/view AD Groups. Enter the OU chain required to get to the OU that will contain the AD Groups you'd like to synchronize/monitor. (Example: OU=NewYork Location,OU=Access Control,OU=Groups)
Allow LDAP Authentication	Check to enable Single Sign on via AD Domain Credentials.
Allow LDAP Group/User Sync	Check to enable LDAP Group/User Sync.

Warning

Do not click the **Force Sync** button or **Force Refresh** button (starts the initial synchronization) until User Credential mapPINg, Custom Field mapPINg and all required AD Groups have been added as Access Privilege Groups. This will be covered in the next sections.

5. Click the **Save** button on the bottom of the screen.

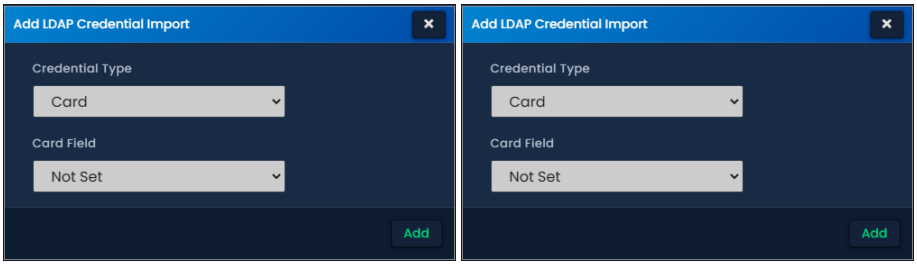
LDAP User Credentials

If it was decided during planning phases that Credentials will be obtained from Active Directory, follow the rest of this section.

1. On the LDAP Integration screen, navigate to the User Credentials tab.
2. Click the  icon to pull up the LDAP Credential Import options.

3. Select a Credential Type from the drop-down list.

4. If you selected Card as the Credential Type, you must select an Import Type. This will help VAX know if the credential information will be in a single field or across multiple AD User Attributes.



5. Select the AD User Attribute Field from any required drop-down menus.

Note

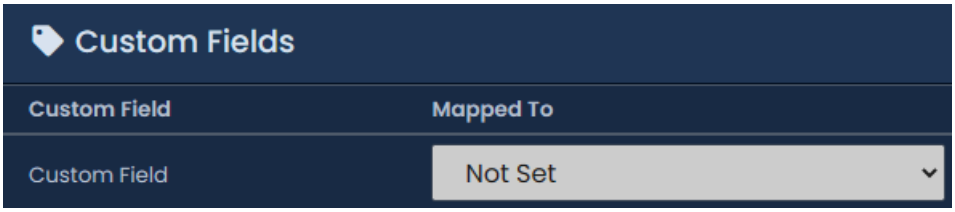
If any PIN Fields are left as "Not Set", we will automatically generate any corresponding PINs for Card and PIN schedules. If the field is set but is empty in AD, it will also be automatically generated. In the case of importing a credential from a single field, we will auto generate a PIN if there is no comma separated entry after Site code and Card Number.

LDAP User Custom Fields

If it was decided during planning phases that one or more AD User Attributes should be synchronized to VAX from Active Directory, follow the rest of this section.

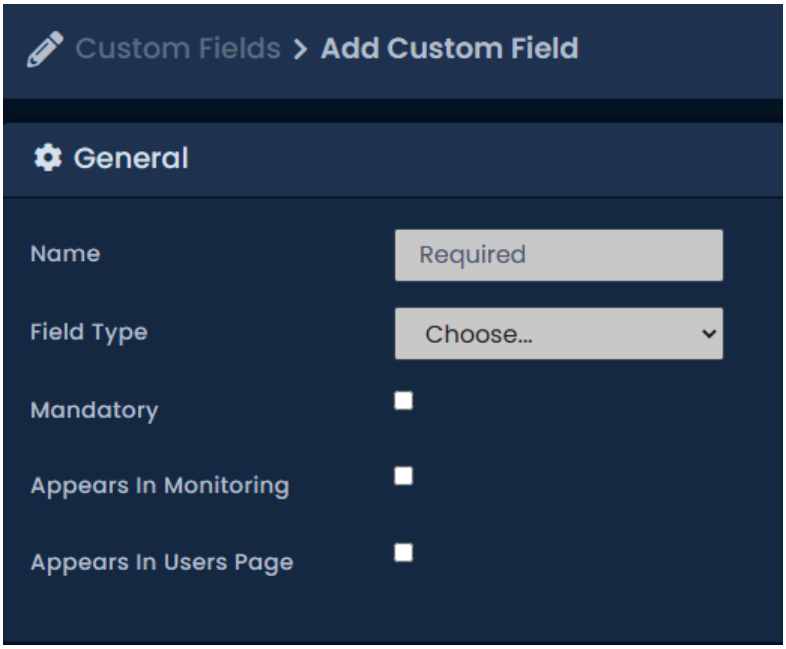
1. Custom Fields should be added in VAX before they are associated with AD Attributes.

2. On the **Side Bar**, scroll down to the section titled **Day To Day**; click on the **Custom Fields** icon (pictured below).



3. On the **Custom Fields** screen, you'll see any custom fields already created. To add an additional field, fill the text box titled **Name of the Field** and click the **Add** button.

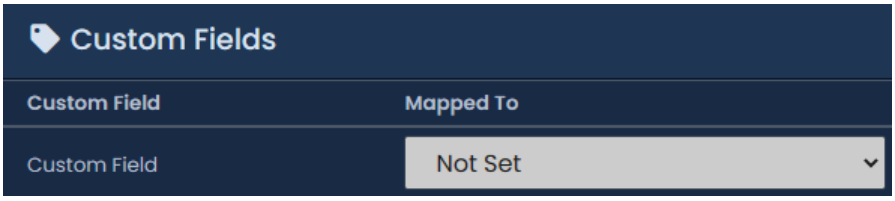
Figure 32.1. Custom Fields: Example



4. After you've added your Custom Fields, we must associate the VAX Custom fields to AD User Attributes.
5. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **LDAP Integration** icon (pictured below).

6. On the LDAP Integration screen, navigate to the Custom Fields tab.
7. You'll see the custom fields added in the previous steps. Use the Mapped To drop-down menu to select an AD User Attribute to associate to each custom field. You can leave the drop-down menu as Not Set; VAX will treat the Custom Field as it normally would.

Figure 32.2. LDAP Custom Fields



8. You can now move on to the next section for creating Access Privilege Group associations to AD Security Groups.

Create Associations Between AD Groups and Access Privilege Groups

In order for an AD User to be synchronized, we must tell VAX which AD Security Groups to monitor and synchronize Users from. For more information on planning Group Structure, please see the section called “AD Groups, Membership and Structure”.

This section will demonstrate how to add a AD Security Group as an Access Privilege Group in VAX.

1. On the **Side Bar**, scroll down to the section titled **Day To Day**; click on the **Access Privilege Groups** icon (pictured below).

2. On the Access Privilege Groups screen, you'll see any groups already created. Click the **Add** button on this screen.

3. Select LDAP as the Group Type. If you want to create any Access Privilege Groups without LDAP, you can select Local.

4. The Group drop-down menu will give you a list of AD Security Groups that VAX was able to see. Select an AD Group you'd like to monitor/synchronize Users from.

Tip

You can narrow the scope of what AD Groups VAX can see by filling in the Root OU section on the LDAP Configuration Screen.

5. (Optional) Fill in a description to help other administrators understand the role/purpose of this group.

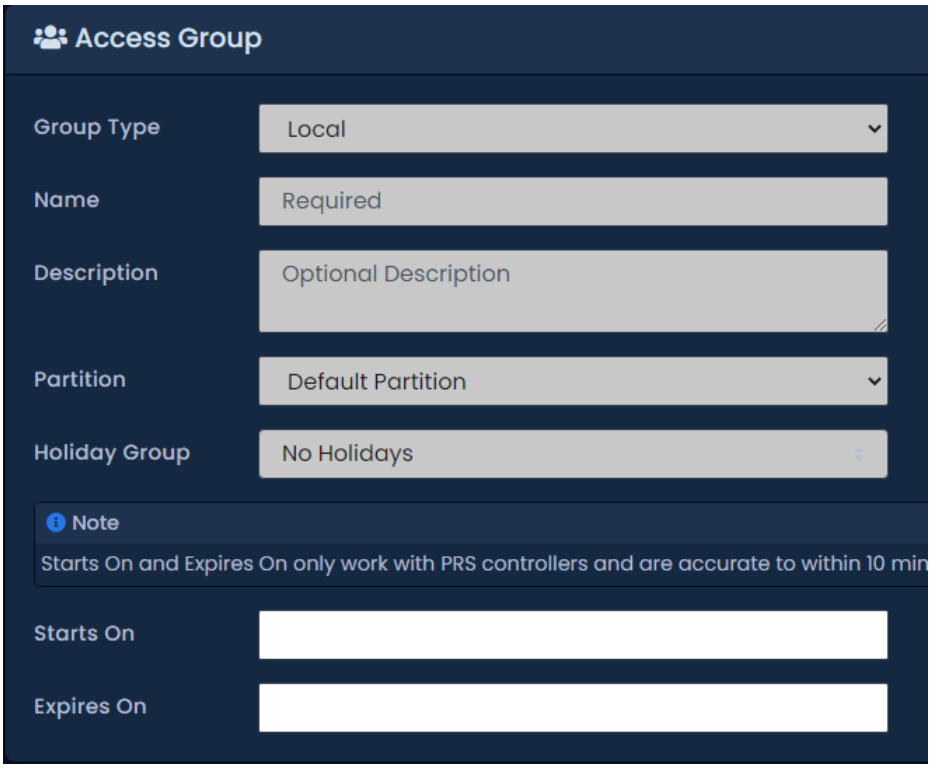
6. Select a Partition to create this Access Privilege Group in.

Note

You can associate the same AD Security Group to multiple Partitions by adding the group multiple times and changing which Partition is selected.

7. If you anticipate that User schedules in this group should behave differently on a Holiday, select Standard Holidays for the Holiday Group. Otherwise, select No Holidays.

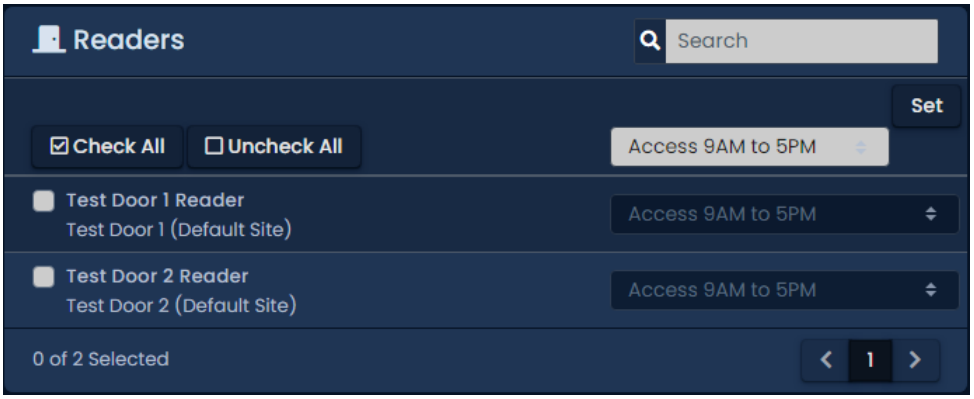
Figure 32.3. Adding a AD Security Group as a Access Privilege Group



8. Readers/Floors:

   If Panels, Doors, Elevators and Readers have been configured, you can optionally give access to Doors/Floors and select a Schedule. AD Users that are synchronized will be given access to the specified Doors/Floors based on the User Schedule selected. Check any applicable Doors/Floors and select a schedule from the drop-down menu.

Figure 32.4. Selecting Readers/Floors



9. Once you're satisfied with the settings (which can be edited later as needed), click the green button **Create**.

10. Repeat this process for any additional AD Security Groups you'd like to add.

Synchronize Users from AD

Before the first LDAP synchronization, please ensure the following have been complete:

- Fully Qualified Domain Name has been entered in LDAP settings.
- If required, User Credentials have been mapped to AD User Attribute fields. Credentials should be entered into the selected User Attribute Fields in Active Directory.
- If required, Custom Fields have been added and mapped to AD User Attribute fields.
- All required AD Security Groups have been added as Access Privilege Groups.

You are now ready to perform the initial AD Synchronization.

1. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **LDAP Integration** icon (pictured below).

2. For the first initial synchronization, press the Force Refresh Button.

The Force Sync button will delete any existing LDAP Users from VAX and then attempt to synchronize those users based on the current LDAP settings and groups.

Warning

Depending on the performance or load on the Domain Controller (AD server), a Force Refresh can take between a few minutes to over an hour. Force Refresh should only be used for the initial sync or if Credential mapping and/or Custom Field mapping are changed or additional AD Security Groups are added as Access Privilege Groups.

3. After the first sync is complete, VAX will check AD for changes based on the LDAP Polling Time. You can also force VAX to sync earlier by pressing the Force Sync button.

LDAP Administrator Authentication

With LDAP configured, VAX can allow Administrator authentication with LDAP providers such as Active Directory for Administrators who log into VAX to manage the system and make changes.

The benefits of using LDAP authentication with VAX include:

- Single sign in allows Administrators to use their Active Directory or Domain Credentials to access VAX.
- Passwords are authenticated with Active Directory. In the event that the password changes in active Directory, VAX will require the new password for the Administrator to log in.

Some of the disadvantages of using LDAP authentication with VAX include:

- If the LDAP provider is offline, administrators cannot log in to make changes to VAX.
- If the LDAP credentials are compromised, VAX can be as well.

To configure LDAP authentication for Administrators:

1. On the **Side Bar**, scroll down to the section titled **Scheduling**; click on the **LDAP Integration** icon (pictured below).

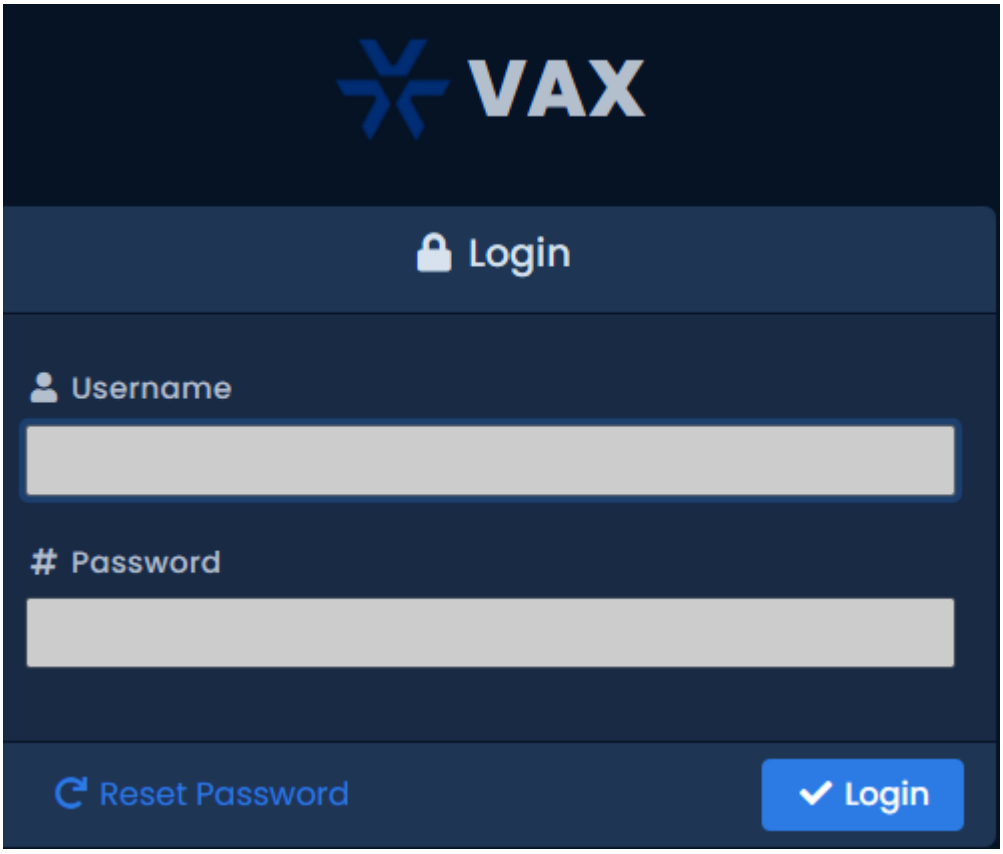
2. Fill in the Fully Qualified Domain Name and check the "Allow LDAP Authentication" check box.
3. Click 'Save' on the bottom of the screen.
4. On the **Side Bar**, scroll down to the section titled **System**; click on the **Administrators** icon (pictured below).

5. Click the "Add" button on this screen.
6. Select LDAP from the Authentication drop-down menu.
7. Fill in the Username with the 'User logon name' from the LDAP provider.

> **Note**
>
> Domain Name prefix isn't needed in most cases in the Username field.

8. Fill in any required permissions for the new Administrator. For more details on these permissions, please see Chapter 20, *Administrators and Privileges*.
9. Click the "Save" button on this screen.
10. The Administrator will now be able to login to VAX using domain credentials.

Figure 32.5. Administrator Login with Domain Credentials



Troubleshooting LDAP Integration

This section will outline troubleshooting for LDAP Integration specific issues.

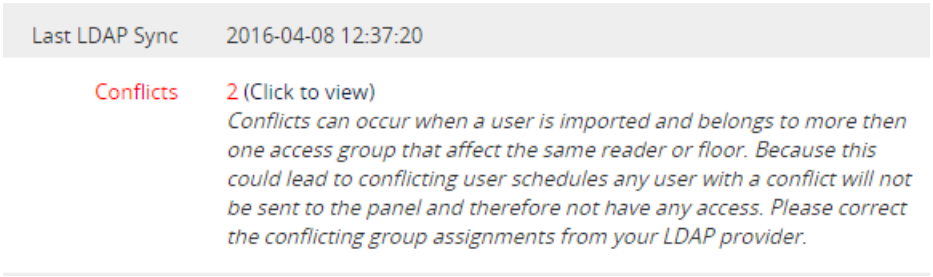
LDAP Conflicts

Once VAX is integrated to an Active Directory Server, it is possible to cause conflicting configuration between Users.

Conflicts can occur when a user is imported and belongs to more than one Access Privilege Group that affect the same Reader or Floor. Because this could lead to conflicting user schedules, any user with a conflict will not be sent to the Panel and therefore not have any access. The issue should be corrected from the LDAP provider.

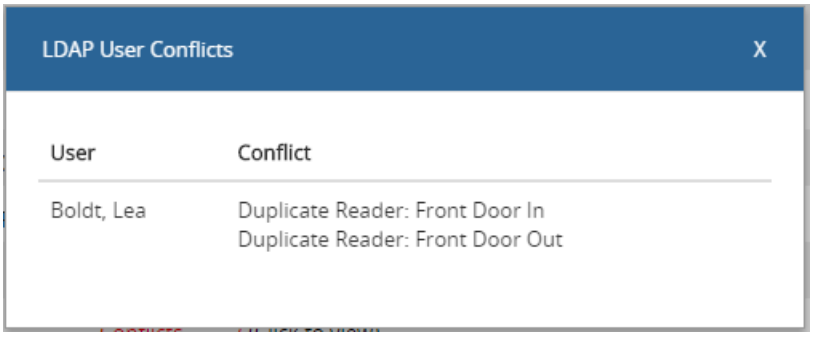
When a conflict occurs, you'll see a red banner on the top of the page and a section on the LDAP Integration screen.

Figure 32.6. Conflict Message



You can click "Click Here" to view more details about the conflicts. A window will appear with the details of the conflict.

Figure 32.7. LDAP User Conflicts Example



In our example, Lea Boldt was accidentally placed into the AD Security Groups "Access Front Door 9 to 5" and "Access Front Door Always Access". The solution in this case is to modify the AD user Lea Boldt and remove the user from one of the two groups. After the polling time has elapsed, the conflict will be resolved. You can also perform a Force Sync to resolve the conflict sooner.

VAX Services Fail to Start

During installation, there may be circumstances where one or both of the VAX services fail to start or fail to install. The reasons and possible resolutions will be detailed in this section.

Checking Log Files

If the service that failed to start was VAXServer, we may be able to check log files for additional information.

1. Navigate to:

   ```
   C:\Program Files(x86)\Vicon Industries\VAX\WebServer\Logs
   ```

2. Your installation path may be different.

3. Open Application.txt in notepad.

4. Check the last few entries in the log file. The following chart can be used to compare against with possible resolutions.

Table 32.2. Service Failed to Start

Log Entry	Possible Resolutions
`ERROR VAX. WebServices. HCAuthProvider [(null)] - LDAP Authentication Error: (VAXwebservice) Logon failure: unknown user name or bad password`	The Service Account specified in the installer has incorrect credentials, verify the username and password. This could also indicate the account password has expired. Windows Event Viewer may also give more information. Contact your Domain Administrator.
`"Verifying Database Migrations"` appears repeatedly until service stops.	The database could not be reached. The service may have not started automatically. Open Services.MSC and check that the service titled "SQL Server(VAX)" is running. You can right click the service and select Start.
`ERROR VAX. StartupHelpers.DbSetupHelper [(null)] - System.Data.SqlClient. SqlException (0x80131904): CREATE DATABASE permission denied in database 'master'.`	The Service Account specified in the installer does not have permissions to create databases. Ask an SQL Administrator to add the SQL Server Role 'dbcreator' to the service account specified in the installer and click 'retry' in the installer window.

If you are still unable to successfully start/install any VAX services, please see Chapter 37, *Support*.

Chapter 33. Action Control Engine

Introduction

The Action Control Engine, which will be referred to as ACE, is a highly anticipated feature available in VAX 2.8.

ACE is a powerful side scripting engine within the VAX software. It allows administrators to define a set of conditions which trigger a series of actions that will occur when these conditions are met.

Warning

We do not recommend using the Action Control Engine for any life safety functionality. ACE will not function if the VAX server is not available or network connectivity is down.

ACE Use Cases

ACE can be configured to accomplish the following:

- Single button/card read lockdown
- Customized guard tour
- Unlock exterior doors with single card read
- Scheduled email of occupancy count of area or building
- SMS/email based on a condition/trigger
- Trigger relay in another building based on a condition/trigger
- Send HTTP requests to third party systems
- Send camera snapshots to administrators based on condition/trigger
- Disable a card if it's used more than a specified amount
- Automatic emailing of reports
- -and many more.

ACE Components

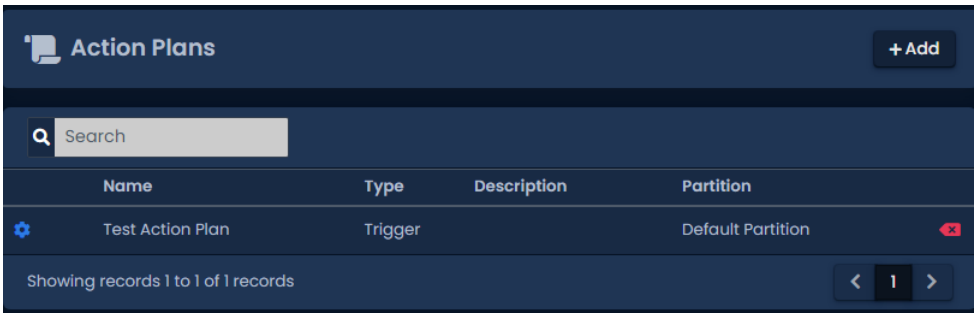
There are two main components to ACE, **Action Plans** and **Action Triggers**. Action plans should be created first.

Action Plans

Action Plans are a series of actions chained together to accomplish a task. There are over 40 actions that can be chained together. Use the following steps to create an action plan:

1. On the **Side Bar**, scroll down to the section titled **System**; click on the **Action Plans** icon (pictured below).

2. On the Action Plans screen, you'll be presented with any existing action plans. Any action plans that can be executed will have an orange execute button to the left of them. Click the Add button to create a new plan.



3. On the Add Action Plan screen, fill in the name of the plan.

Tip

The name should represent what the action plan will do or its purpose. Description is optional.

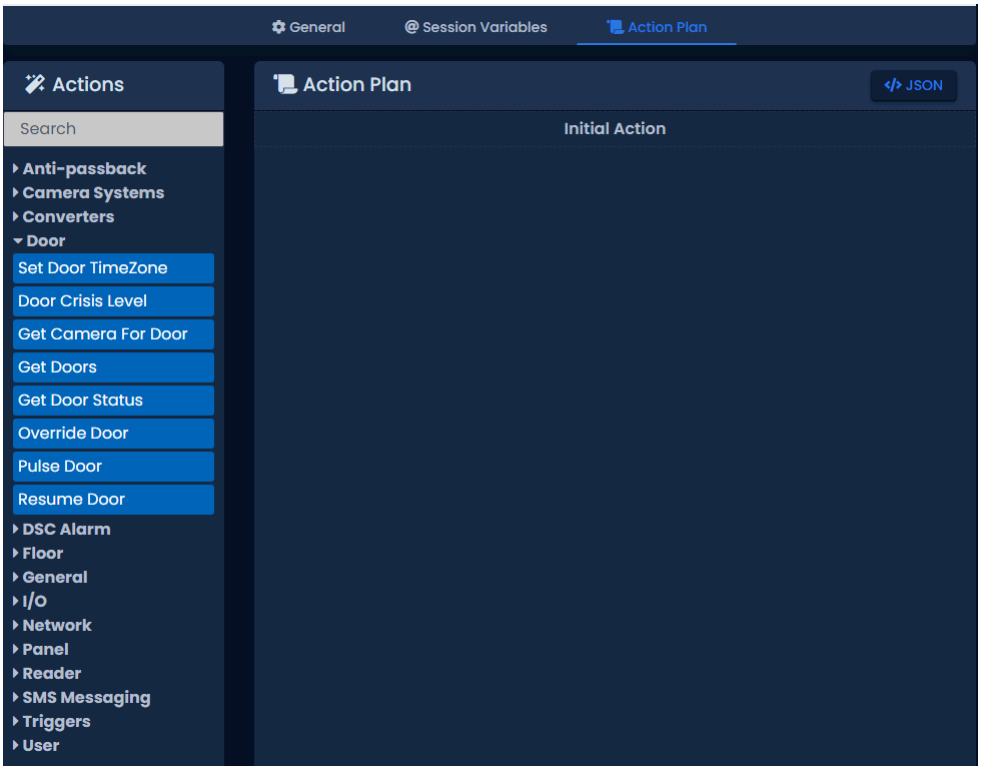
4. Select a Partition to place this plan into.

5. Select a Plan Type. Each plan type is explained below:

   - Trigger Plan Type: Plan is executed via an Action Trigger. When the conditions of the action trigger are met, this plan will execute.

   - System Plan Type: Plan is executed by pushing the execute button while viewing the action plan or on the Action Plans Screen; it can also be executed via web API. These plans can also be called upon by other plans.

6. Click Create. You'll be taken to the Edit Action Plan screen. Navigate to the Action Plan tab.



Actions

On the Action Plan tab, you can configure one or more actions to execute. There are over 40 actions grouped together into categories on the left side of the page. Some actions can resolve into a *Success* or *Fail* condition chain. This means you can create a separate chain of actions based on the success or failure of the previous action.

The following table outlines the actions available in each section. For more detail on all actions, please see the relevant section within the master tech guide for full list of actions.

Table 33.1. Action Categories

Action Category	Description
Anti-passback	Allows you to reset area and user locations in the system, commonly used to reset anti-passback locations
Camera Systems	Actions that are designed to interact with a VMS system
Converters	Actions that can convert numbers/strings to hashes such as MD5 or Base64. Commonly used during authentication with third party systems.
Door	Door related actions such as initiating overrides and crisis levels
Floor	Elevator floor related actions such as initiating overrides
General	Contains actions such as logging, timers, setting variables, if statements and each statements
I/O	Actions used to initiate override commands to inputs or outputs
Network	Actions that take place over the network. This includes sending emails, HTTP requests and PING requests.
Panel	Panel specific actions such as starting the emergency alarm, triggering the piezo speaker and updating panels
Reader	Reader specific actions such as controlling the LED on the reader or the built-in piezo speaker
SMS Messaging	Actions that can send SMS messages. Current SMS vendors are Clickatell and Twilio.
Triggers	Actions that will wait a specified period of time for something to happen such as a door opening or a button push
User	User specific actions such as disabling a user or checking if a user is a member of a specific access privilege group

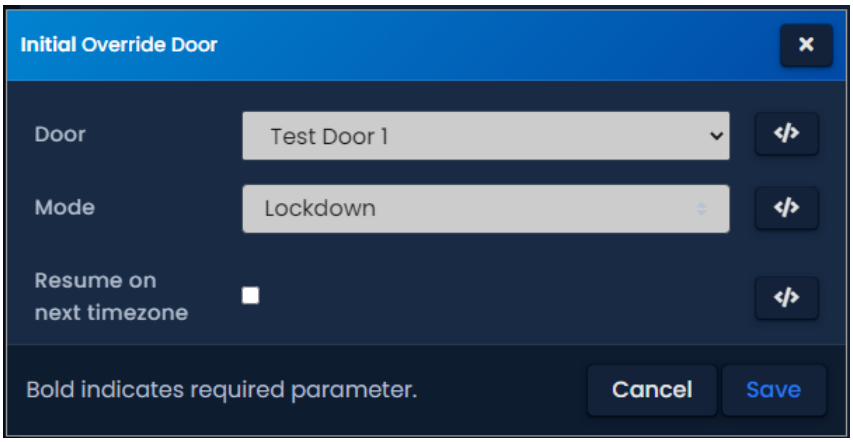
Use these steps to add an action to your Action Plan:

1. Open the corresponding category on the left by clicking on it.

2. Left-click and hold on the action you want to add. You can now drag this action into the middle area of the screen.

3. If it's the first action in the action plan, drag it over to the Initial Action box in the middle section. Let go and a window should appear where you can enter options (parameters) into the action.

4. Fill in any required parameters. In this example we've select Override Door for our initial action. A Door and a Mode must be selected. Click OK.



Use these steps to chain additional actions together:

1. Open the corresponding category on the left by clicking on it.

2. Left-click and hold with your mouse or track pad on the next action you want to add. You can now drag this action into the middle area of the screen.

3. Drag the action over an existing action in the middle of the screen. Depending on the action, you may see an Always box, Success box and a Fail box.

   - If you need your new action to occur after the previous action has completed successfully, drag and let go of the new action into the Success box.

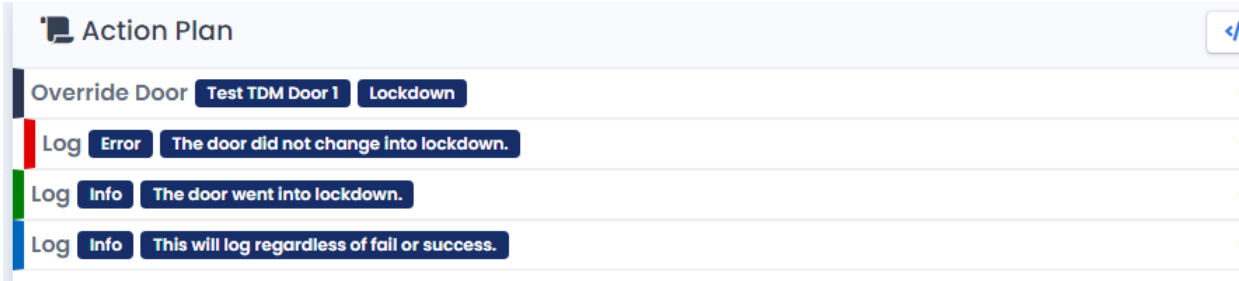
   - If you need your action to occur if the previous action does not succeed, drag and let go of the new action into the Fail box.

   You can have separate actions occur if the previous action fails or succeeds. Chains of actions will be indented and colored.

Tip

An action chained into the Always box will execute regardless of if the previous action resolved as Success or Fail. It will usually execute immediately and will not have access to variables or results of the previous action.

Figure 33.1. Building Lockdown Action Plan

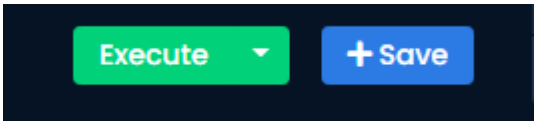


4. Click Save once you've completed your action plan. Executing will also save the action plan.

Executing an Action Plan

If the Action Plan Type was configured as System, it can be executed in one of three ways:

1. Click the orange button on the Action Plans screen to execute it immediately.
2. Click the green Execute button on the Edit Action Plan screen.



3. Execute the action via VAX Web API via HTTP POST request.

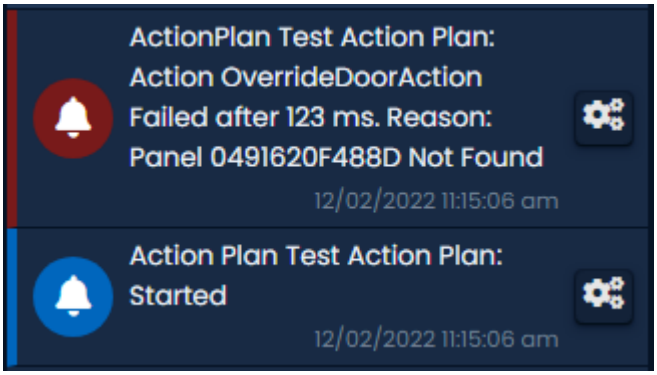
   Example: https://localhost:11001/api/ActionPlans/10/Exec

If the Action Plan Type was configured as Trigger, an Action Trigger must be created and configured to execute that action plan.

Monitoring Action Execution

When an action plan is executed, several notifications are generated when the action occurs. Depending on the action plan, more notifications can be generated. Log actions will also generate a notification titled Action Plan Message.

Figure 33.2. Action Plan Being Executed



Tip

When monitoring more complicated action plans, the Monitoring screen can display hundreds of notifications. Please see Chapter 24, *Notifications*.

To view Action Plan notifications that have already occurred, you can run the Action Plan Activity report. For more information on running this report, please see Action Plan Activity Report.

Note

Action Plans can accomplish much more than shown in this basic example. You can combine hundreds of actions together to meet your specific needs.

Action Triggers

Action Triggers are configurable condition sets that execute an action plan when the conditions are met. An action plan must be of type Trigger in order for an Action Trigger to execute it. These triggers

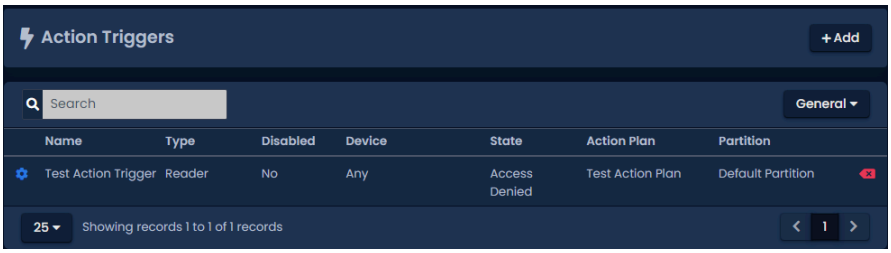
are extremely flexible. You can create as many as you need and make them as specific or generic as you'd like.

Steps to add an Action Trigger:

1. On the **Side Bar**, scroll down to the section titled **System**; click on the **Action Triggers** icon (pictured below).

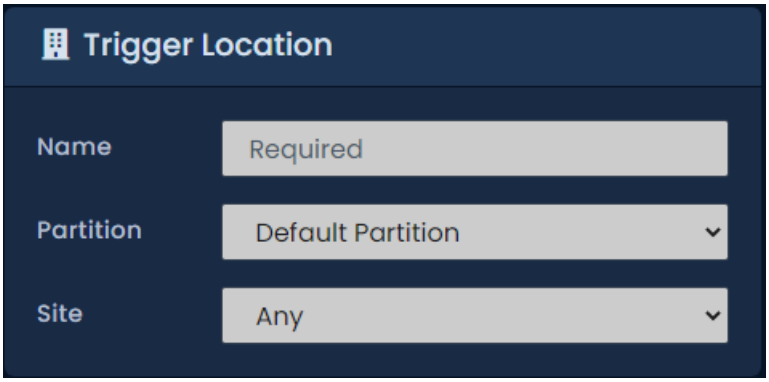
2. On the Action Triggers screen, you'll be presented with any existing triggers. Click the Add button to create a new trigger.

Figure 33.3. Action Triggers Screen



3. On the Add Trigger screen, you will define conditions under which to execute an action plan.

4. Fill in the Trigger Location section. An action trigger can only belong to a single Partition. Select a Site. You can select Any to include all sites in the partition or a specific site.



5. In the Trigger Conditions section, select a Type. Most condition Types will have a State. You can leave this as Any or select a specific State to meet the condition of this trigger.

Table 33.2. Types and States

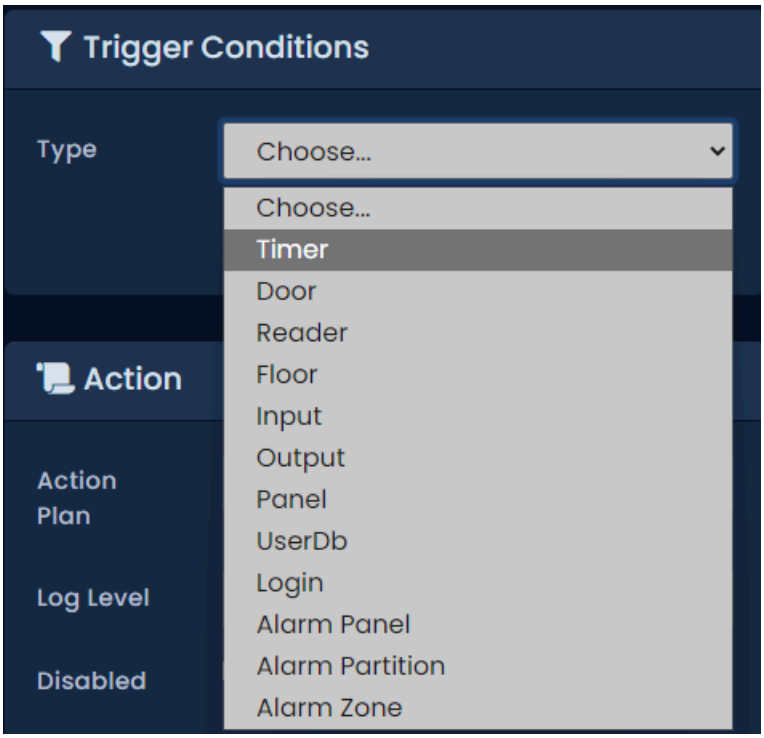
Type	Available States	Parameters
Timer	n/a	Time restrictions: Start Time, Interval, Day of Week
Door	Any, Open, Closed, Unlocked, Locked, Forced Open, Held Open, External Motion On/Off, REX On/Off	Any Door or a specific Door.
Reader	Access Granted, Access Denied, First Card In, Triple Swipe, APB Soft Violation, APB Hard Violation	Any Reader or a specific Reader. Any User or a specific User.
Floor	Unlocked	Any Floor or a specific Floor.

Type	Available States	Parameters
Input	Activated, Deactivated, Shorted, Disconnected	Any Input or a specific Input.
Output	On, Off	Any Output or a specific Output.
Panel	Disconnected, Connected, Tamper Sensor, Emergency Alarm	Any Panel or a specific Panel.
UserDb	Added, Updated, Deleted	n/a
Login	Any, Success, Failure, Lockout	n/a

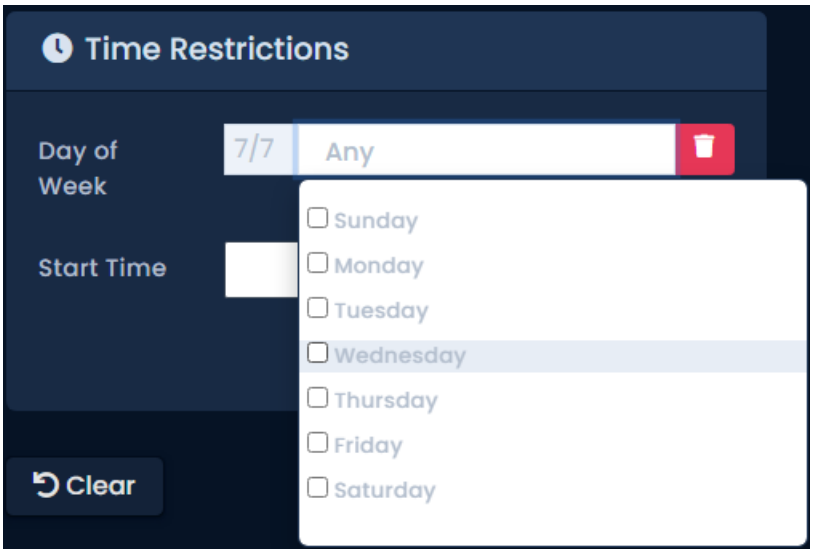
Note

A **Trigger Timer** can be set to repeat daily; the **Interval** setting can be set to 1440 minutes.

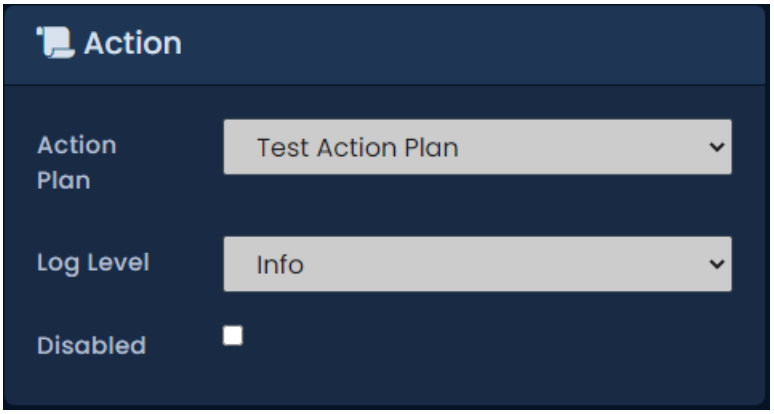
6. If needed, select a State. By default it will be set as Any. Some triggers can optionally have one or more parameters. This will allow you to specify a specific device (reader, door, floor, input, output) or a specific user to meet the Trigger Conditions.



7. Fill in the Time Restrictions section. You can specify which days of the week the trigger can occur and what times of the day via Start Time and End Time. Time Drift will allow notifications (such as forced open or held open) that are not live (i.e., came from a panel that was offline for a period of time) to still meet the conditions of the trigger if the time of the notification is below the allowed time drift.



8. Last section to fill is the Action. Select an action plan from the Action Plan drop-down menu that will execute when the conditions of the action trigger are met.



9. Click Create. The trigger will now execute the action plan if its conditions are met.

Advanced Action Concepts

This section will outline more advanced options available when creating an Action Plan, such as how to use variables, expressions, Each actions, If actions and using the HTTP action.

Variables in Action Plans

Action Plans have support for variables. Variables are used to store information, which can be referenced or used when an action plan is executed. It can also allow you to label information so that it can be read easily.

There are four types of variables available:

- **Session Variables:** Created during the action plan or as part of the action plan. Can contain numbers, strings, arrays, objects, other variables or the result of an expression.
- **Trigger Variables:** Variables that are available to be referenced or used in the action plan that are based on the trigger that executes it. Examples may include information on the administrator to execute the plan or the name of the door/reader/user that activated the trigger.
- **Last Result Variables:** Variables that are only available to be referenced in the action immediately following a HTTP, PING or Each action. These variables will contain results from the previous

action. An example might be an HTTP GET request would have the results of the action stored in a variable called 'LastResult.Content'.

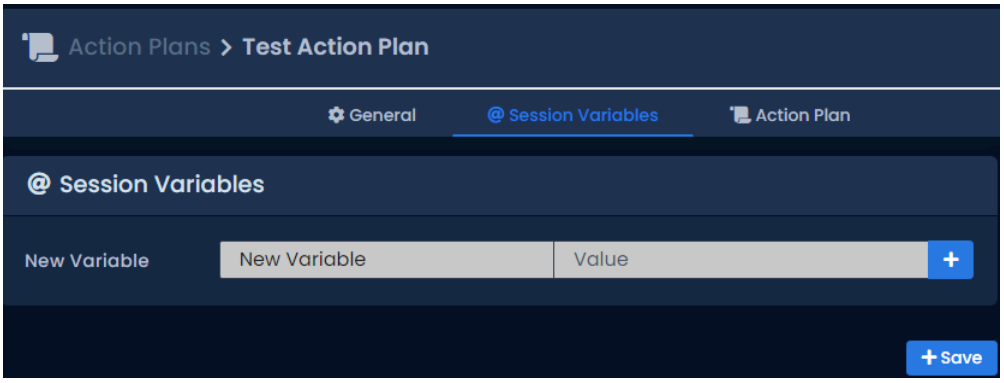
- **Global Variables:** Variables that are available to be referenced globally throughout Action Plans within the same Partition. These variables can contain numbers, arrays, objects, other variables or the result of an expression that can be read, updated or cleared.

Creating a Variable

There are two ways to create variables that can be used during an action plan:

1. a. On the Edit Action Plan screen, navigate to the Session Variables tab.

   b. On the Session Variables tab, you'll see any existing variables. Place a name and value next to the New Variable label.



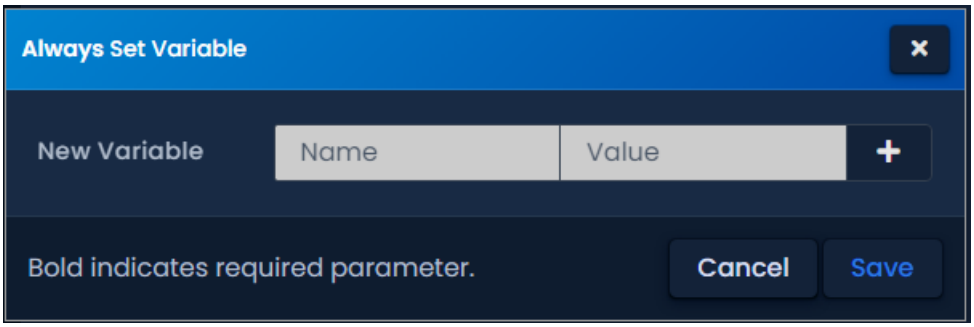
   c. Click the '+' button to the right of the new variable value. You can also edit existing session variables on this page.

   d. Click Save. The session variable can now be referenced as @{Session.VariableName} as any parameter in any action.

2. a. On the Edit Action Plan screen, navigate to the Action Plan tab.

   b. On the actions list on the left, expand the General section.

   c. Click and drag the Set Variable action into the Initial Action or chain it into the Success, Fail or Always condition of any existing action.



   d. Place a name and value next to the New Variable label. The value can contain an expression, another variable or a raw value.

   e. Click the '+' button to the right of the new variable value. You can add as many variables as you need during a set variable action. You can also edit existing session variables from here.

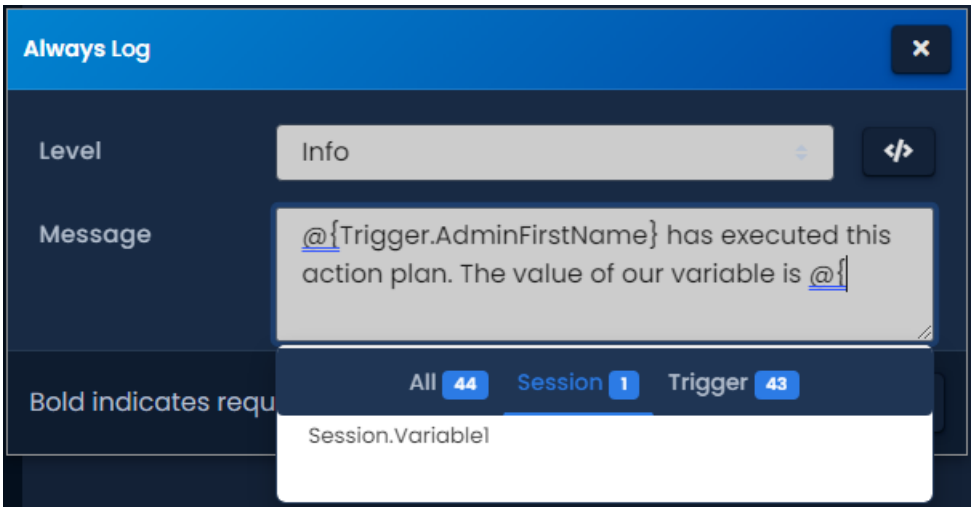
   f. Click OK. The session variable can now be referenced as @{Session.VariableName} as any parameter in any following actions.

Using Variables in Actions

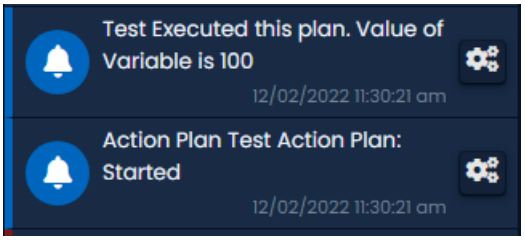
Variables of all types are primarily used as parameters in actions.

When adding an action (such as the Log action), you can use a variable by typing '@{Variable-Type.VariableName}'. If you type '@{' you will see a list of available variables of all types. You can use this instead of typing out the variable name.

Figure 33.4. Variable Auto-fill List



When the action plan is executed, any variable will be substituted or calculated into the value (as seen in our example below).



Expressions in Action Plans

Action Plans have support for Expressions. An expression is a unit of code that is evaluates to a value. This can be used to determine true or false (used with If action) via a comparison operator. You can also do arithmetic operations or string operations.

When adding parameters to an action (such as the Log action), you can use an expression by typing '@[]'. Anything inside the brackets will be evaluated as an expression. You can use variables inside expressions and use expressions to assign a value to a variable. The following chart will demonstrate several examples.

Table 33.3. Expression Examples

Expression	Evaluation
@[100+50]	150
@[1>4]	False
@["TestString".length]	10
@["Test"+"String"]	TestString

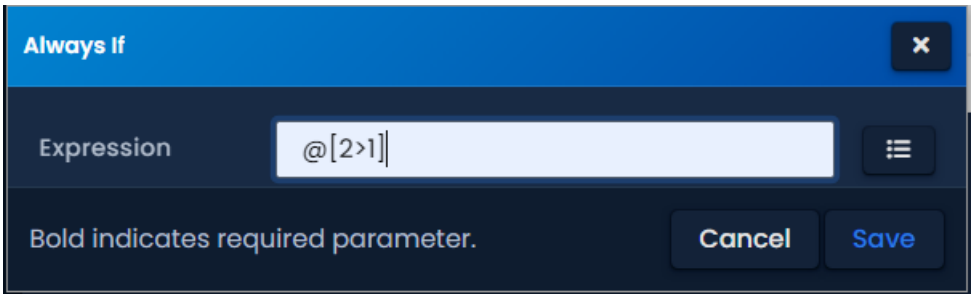
Expression	Evaluation
@[@{LastResult.Index}+1]	Index variable of the previous action + 1
@[100==100]	True
@[100/25]	4

Using expressions can make your action plans more powerful and allow logical operations such as the If action.

If Action

The If action allows you to make conditional chains of actions. The If action will use an expression as its only parameter. If the expression evaluates as true, the next action that is executed after the If action will be the action in the Success condition. If the expression evaluates to anything but true, it will be considered false and execute the action on the Fail condition.

In our example, we've dragged over an If action from the general section into our initial action box.



'@[2>1]' will evaluate as true because 2 is more than 1. We'll configure log actions in the Success (true), Fail (false) and always condition. Now our action plan looks like this:

The If action is a powerful tool that can make action plans more customizable and more reactive to different circumstances.

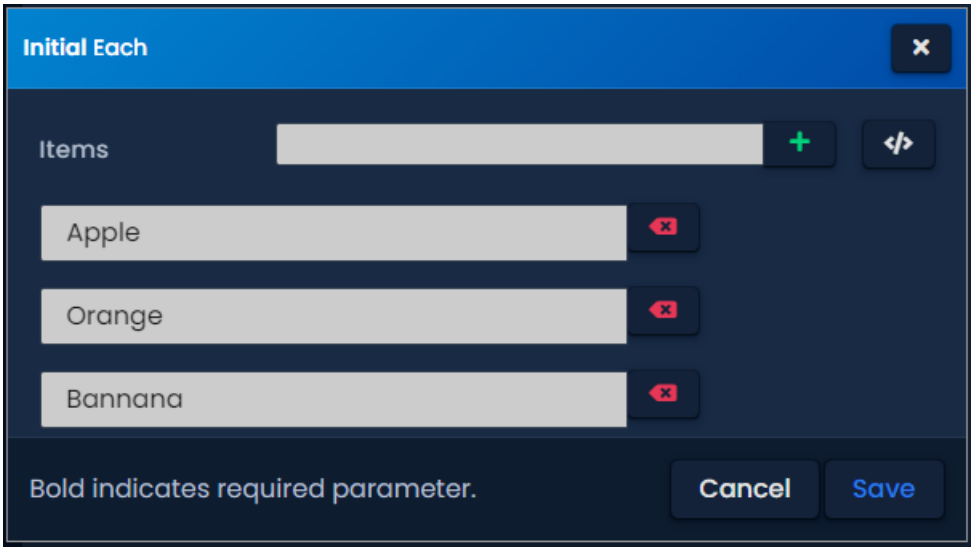
Each Actions

The Each action is used to iterate a collection or an array and chain into an independent action chain for each item found. This action is commonly used to parse results from an HTTP action.

The Each action accepts individual item values or a variable formatted as an object, collection or array.

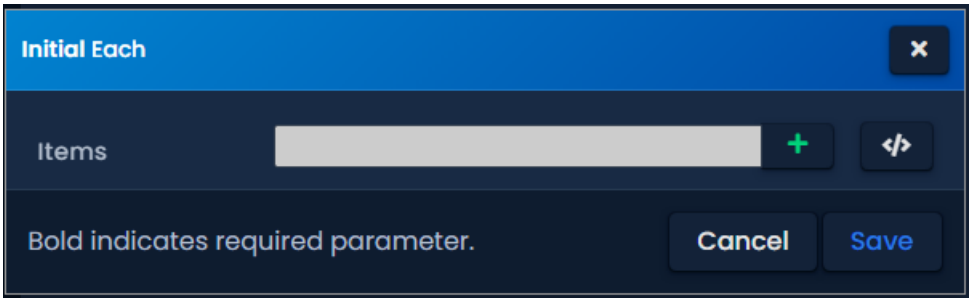
When creating the Each action, you can add individual items by inputting its value and clicking the '+' button.

Figure 33.5. Each Action Example Items



To input a variable as the each action parameter, click the </> button to the right of the Items field. You can now enter a session variable or a last result variable.

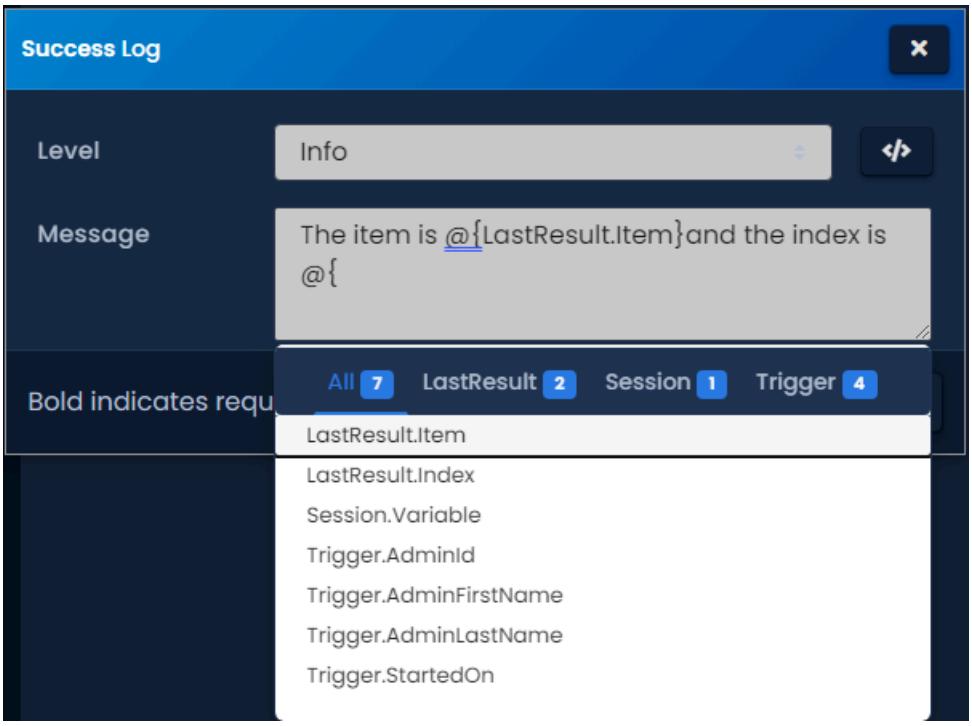
Figure 33.6. Each Action Example Variable



If there is an action inside the Success condition of the Each action, it will have access to 2 unique variables.

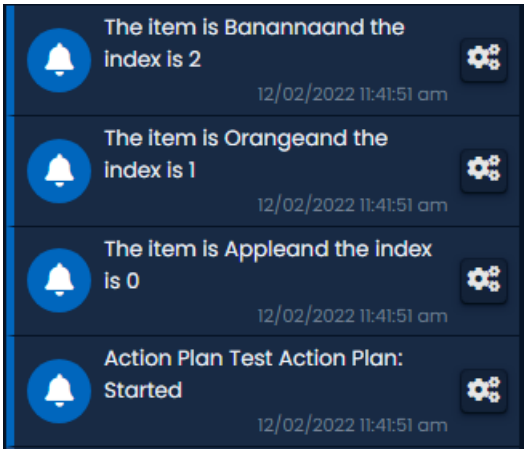
- '@{LastResult.Item}': This variable will contain the item being processed from the Each action. If the item has additional properties (if it's an object) you can access them via '@{LastResult.Item.PropertyName}'
- '@{LastResult.Index}': This variable will contain a number representing where the item being processed sits in the list of items. Index will start at 0.

Figure 33.7. Each Action Last Result Variables



When the Each action is executed, all items will be processed individually into the success chain. Additional actions will run independently of other items actions and will not have access to their variables. They will not run in any specific order. You can use the timer action in conjunction with the LastResult.Index variable if you need each item to run at different intervals.

Figure 33.8. Each Action Executed



HTTP Action

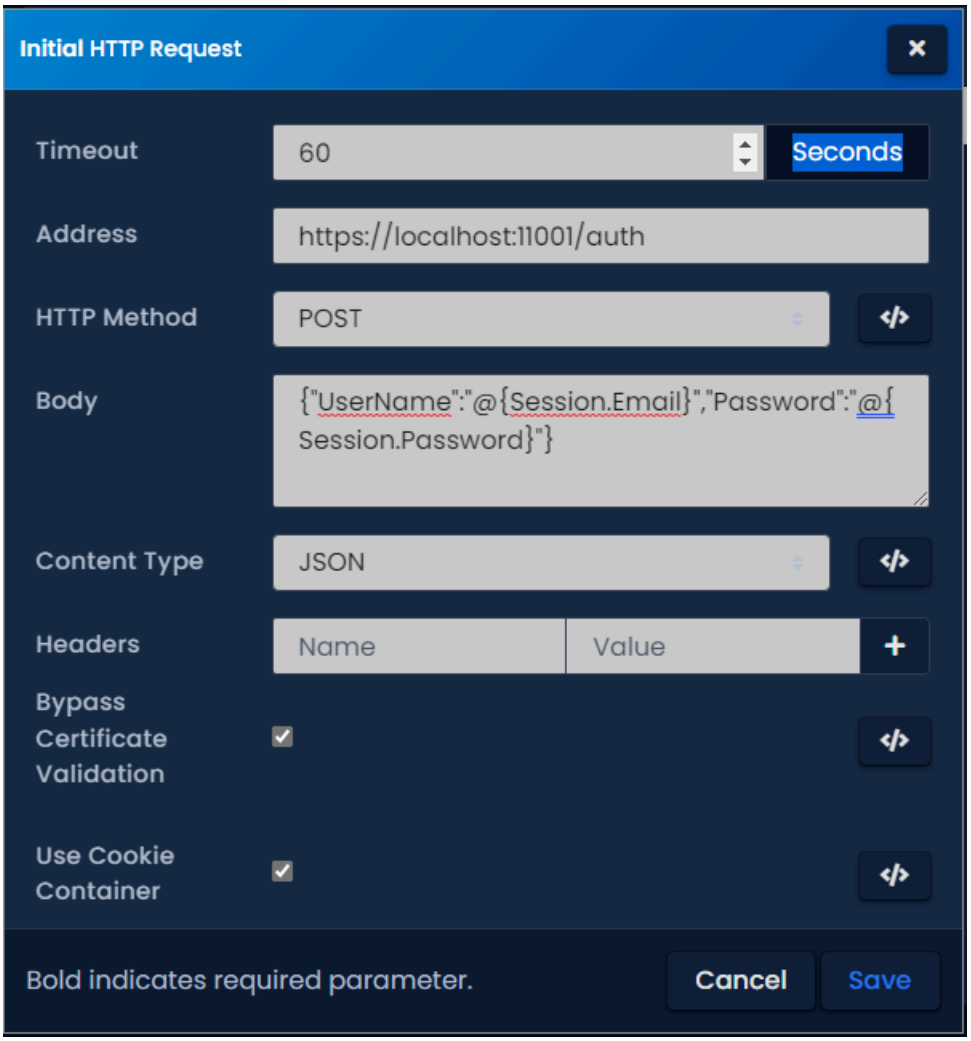
The HTTP action allows you to have the VAX server send HTTP requests to third-party systems, including other web APIs. You can also send HTTP requests back to VAX via the VAX REST web API. Once the request is processed by the destination, the response can also be parsed and used by other actions.

Use the following steps to create an HTTP action:

1. On the Edit Action Plan screen, navigate to the Action Plan tab.

2. On the actions list on the left, expand the Network section.

3. Click and drag the HTTP Request action into the Initial Action or chain it into the Success, Fail or Always condition of any existing action.



4. Define the **Timeout** (60 second default). Amount of time after the request is sent before the action chains into the Fail condition.

5. Define the **Address** the HTTP request will be sent to (example: https://localhost:11001/api/users).

6. Define the **HTTP Method** (GET, PUT, POST, OPTIONS, DELETE). Which method you choose will depend on the third party system. Most requests for information will use GET method.

7. If required, fill in the **Body** of the request. This is where you can include parameters that the receiving system will use.

8. Set the **Content Type** based on the requirements of the third-party system (Any, String, JOSN, XML). Web calls to VAX will use JSON.

Tip

The Content Type 'File' should be used if the result of the request is a file. This can be used to email reports and images.

9. If specific Headers are required, enter the name and value of the header and click the "+" button. You can add multiple headers if required.

10. Check Bypass Certificate Validation if the third-party system or VAX server is using an invalid SSL certificate.

11. Check Use Cookie Container if you want the VAX to manage any cookies corresponding to this HTTP request or subsequent requests. This is useful if logging into other systems.

12. Click OK.

If there is an action inside the Success or Fail condition of the HTTP request action, it will have access to 2 unique variables.

- '@{LastResult.StatusCode}': This variable will contain the HTTP status code returned by the destination address.
- '@{LastResult.Content}': This variable will contain the response returned by the destination address. You can save this variable as a session variable for later use or use this variable in the action following the HTTP request action. If you need to access a specific property you can use '@{LastResult.Content.PropertyName}'

Exporting and Importing Action Plans

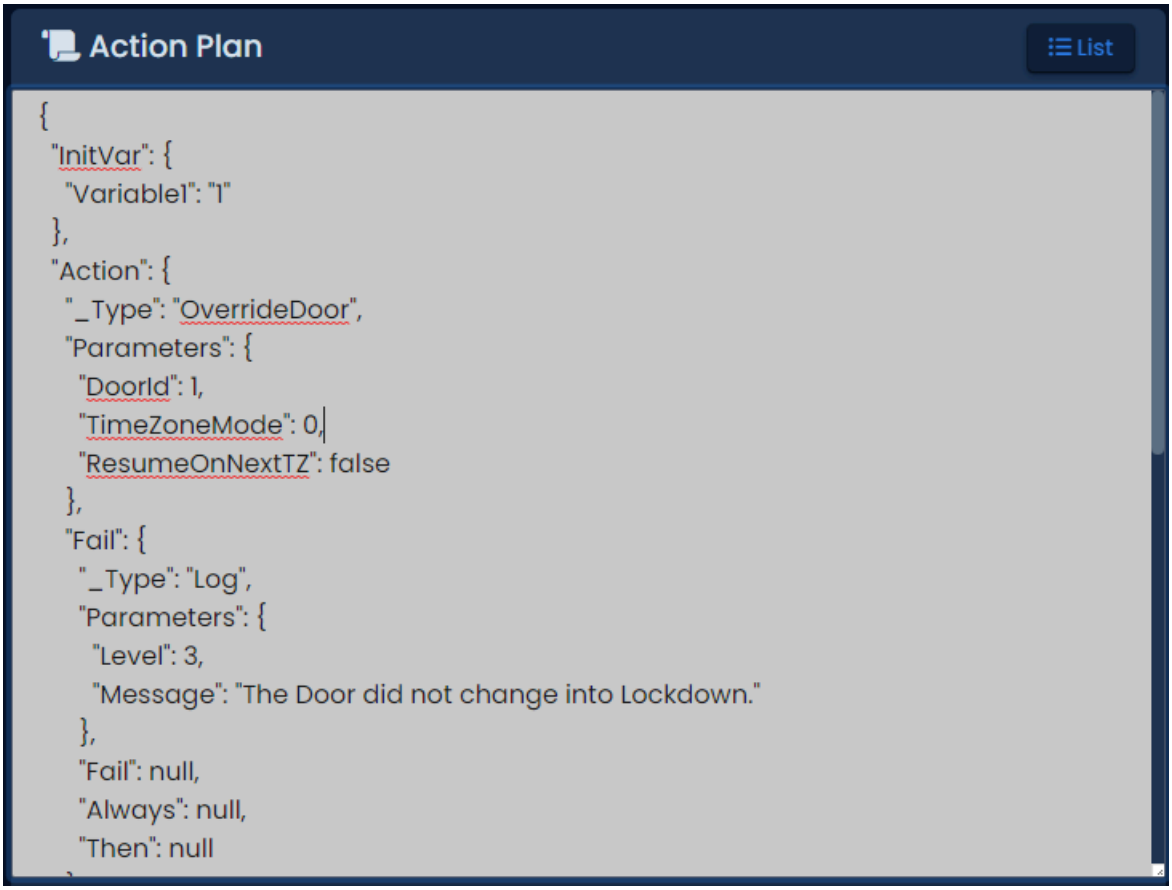
This section will outline how to export and import an action plan.

Action plans in VAX can be exported and imported as JSON strings. Use the following steps to export and import an action plan:

1. On the Edit Action Plan screen, navigate to the Action Plan tab.
2. Click the JSON button to the right side of the screen. The current Action Plan will now display the JSON view of your action plan.

3. In the Action Plan JSON view, select the entire contents of the JSON view.
4. Right click on the screen after selecting the entire JSON view and select 'copy' from the context menu. The contents of the Action Plan is now in your clip board.
5. Navigate to the Edit screen for an existing Action Plan or create a new one.
6. Click on the Action Plan tab.
7. Click the JSON button to the right side of the screen. Select the entire contents of the JSON view.
8. Right click on the screen after selecting the entire JSON view and select 'paste' from the context menu. The Action Plan will now resemble the Action Plan you copied from.

Figure 33.9. JSON View of Action Plan



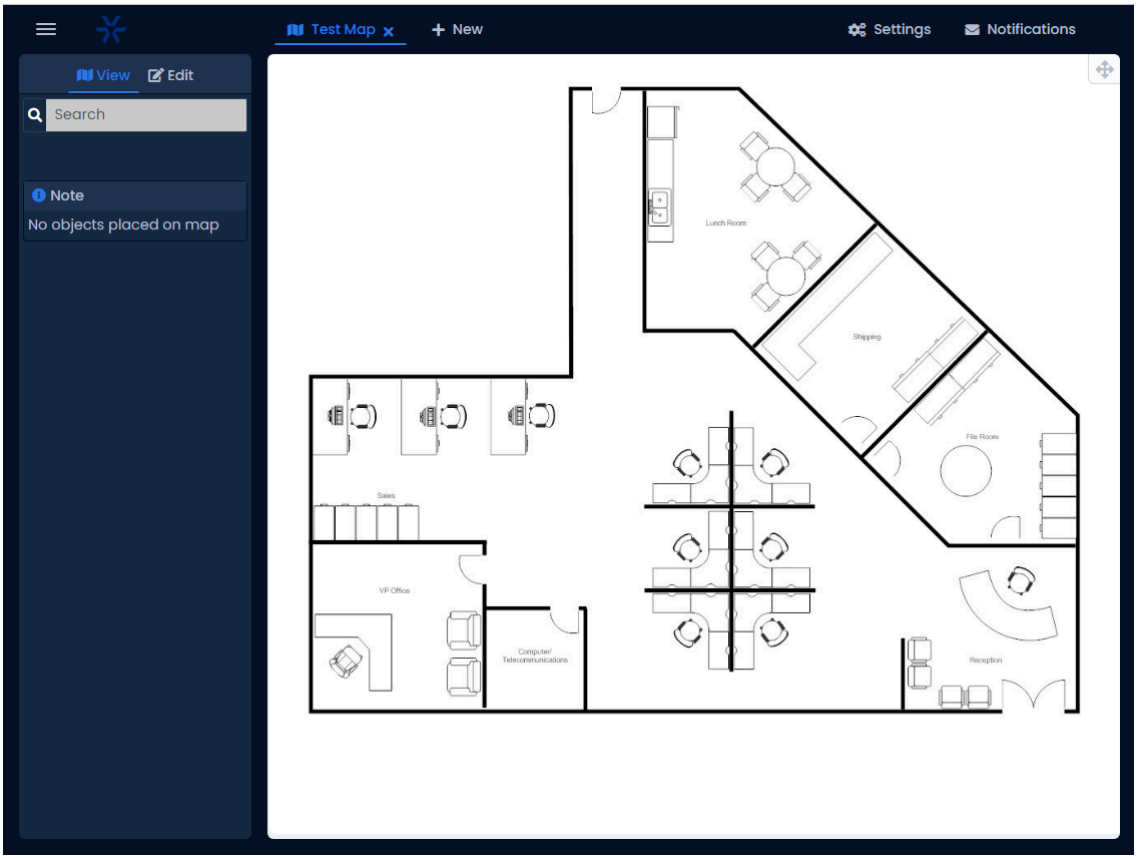
Chapter 34. Interactive Maps

This chapter will demonstrate how to setup and view interactive maps within VAX.

Interactive Maps are used to create a visual representation of a building or site for monitoring purposes. Components of the access control system are placed on top of a layout of the building. This includes:

- Doors
- Elevator Floors
- Inputs
- Outputs
- Cameras
- Areas

Figure 34.1. Map Viewer



Adding a Map

Use these steps to add a map to VAX.

1. On the **Side Bar**, scroll down to the section titled **System**, click on the **Map Configuration** icon (pictured below).

2. On the **Map Configuration** screen, any maps you've already configured are listed here. Click the **Add** button on this screen.

3. On the **Add Map** screen, you'll have several fields to populate.

Figure 34.2. Add Map Screen

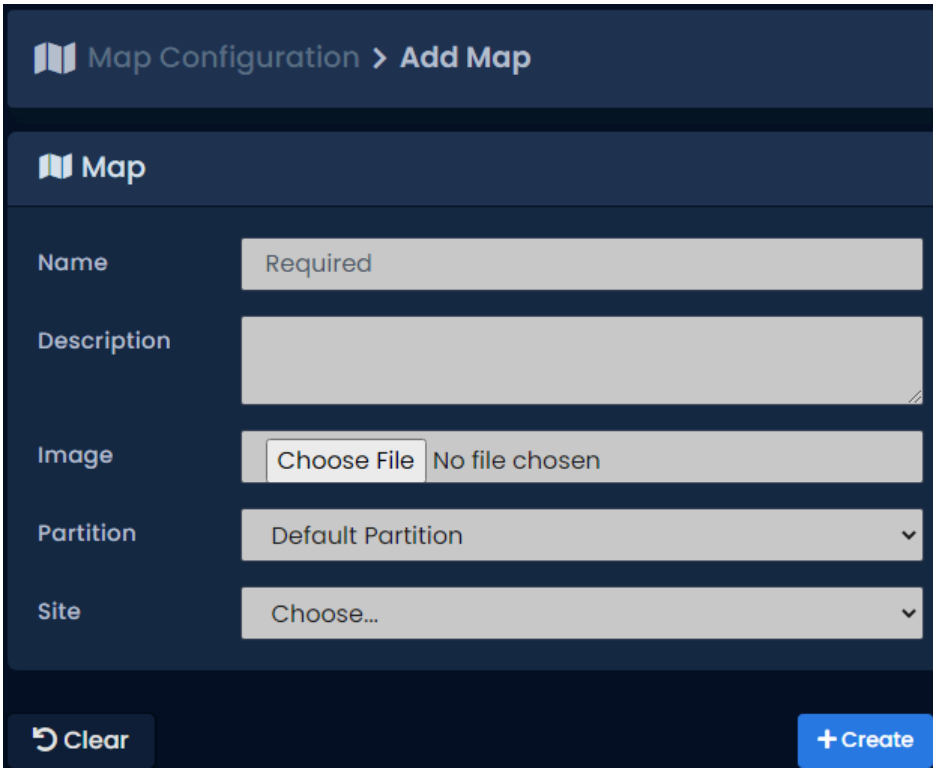


Table 34.1. Add a Map

Text Box/Drop-down Menu	Description
Name	Unique name of your map. Accepts 2 to 100 characters. We recommend naming your map by its location or contents.
Description	Optional description of the map. Accepts up to 255 characters.
Image	Choose a local image to upload as the map background. PNG, GIF, JPG and BMP are supported. Image will be converted to PNG.
Partition	Choose a Partition this map is associated to. This will influence which objects can be placed on the map based on partition scope.
Site	Optional field where a Site can be associated to the map. This will influence which objects can be placed on the map based on site scope.

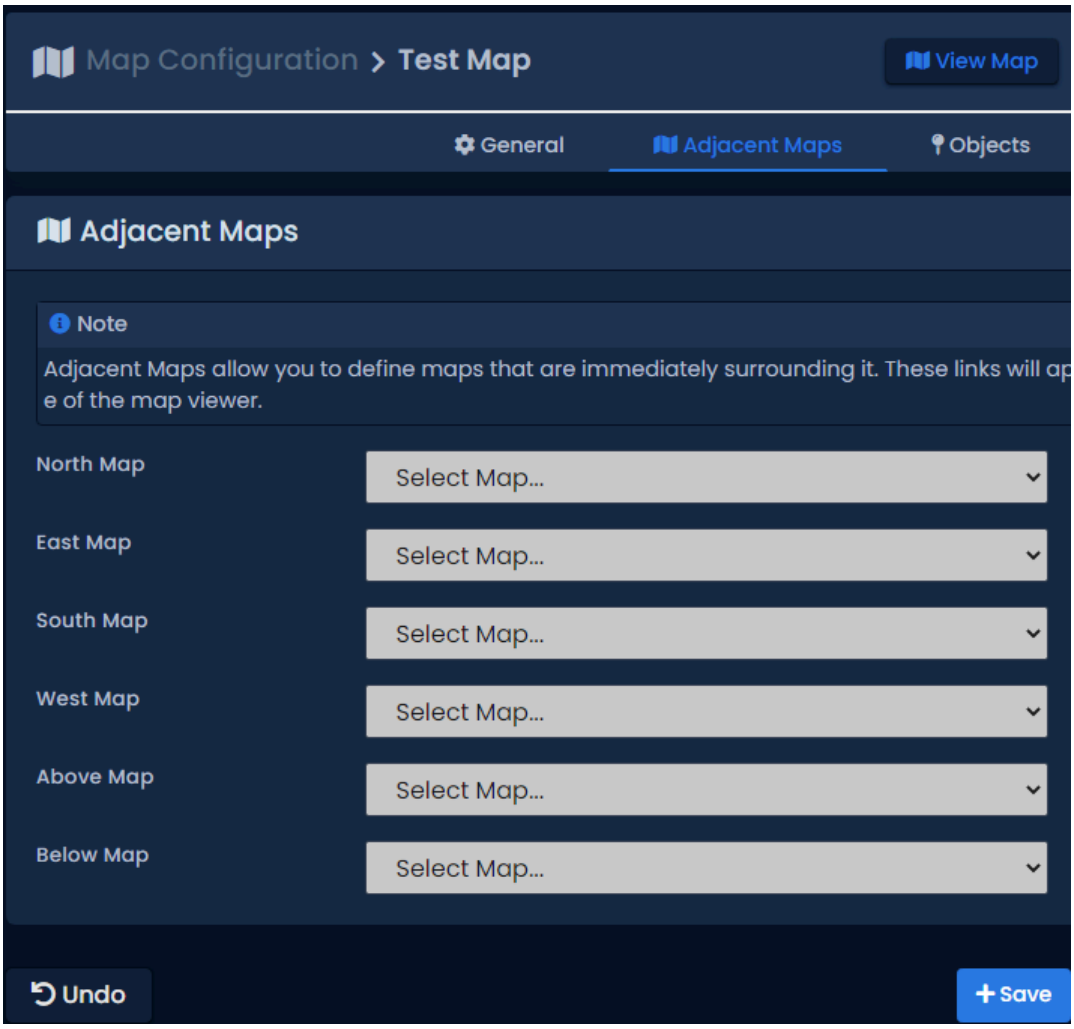
4. Once all the required fields are filled, click the **Save** button to add the map. You'll be prompted with the options to add an additional map, or to **Continue Configuration**, which will bring you to the **Map Configuration screen** for the map you just added.

Adjacent Maps

On systems with multiple floors or buildings to monitor, it may be beneficial to configure where each map is in relation to other maps. If the building has multiple floors, you can configure floor 2 as being above floor 1. This can speed up navigation between maps.

When editing a map, you can assign links between maps on the Adjacent Maps tab. Simply populate any drop-down menu with the name of another map.

Figure 34.3. Adjacent Maps



Adding Objects to Maps

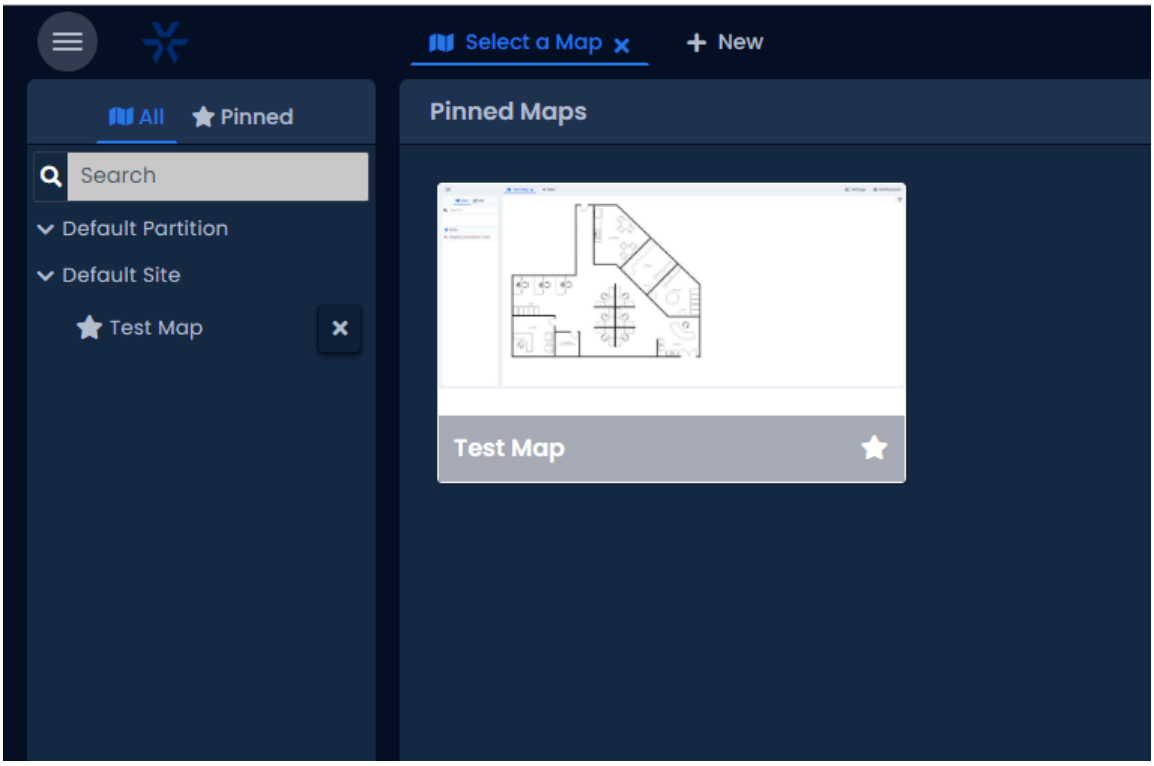
This section will cover how to add various access control objects to a map, such as doors, floors, inputs, outputs, and cameras.

1. On the **Side Bar**, scroll down to the section titled **Day to Day**, click on the **Maps** icon (pictured below). A new window will open in your web browser.

2. On the Map Viewer, you'll be shown the **Select a Map** tab. Any maps you've already configured are listed here. A thumbnail of each map will appear with its title.

Figure 34.4. Select a Map



Tip

Clicking the star icon to the right of the map name will pin the map to the front of the thumbnail list.

3. Select a map by clicking on it. The map will now be displayed.

4. You must click the Edit button near the top left of the screen to add objects to the map.

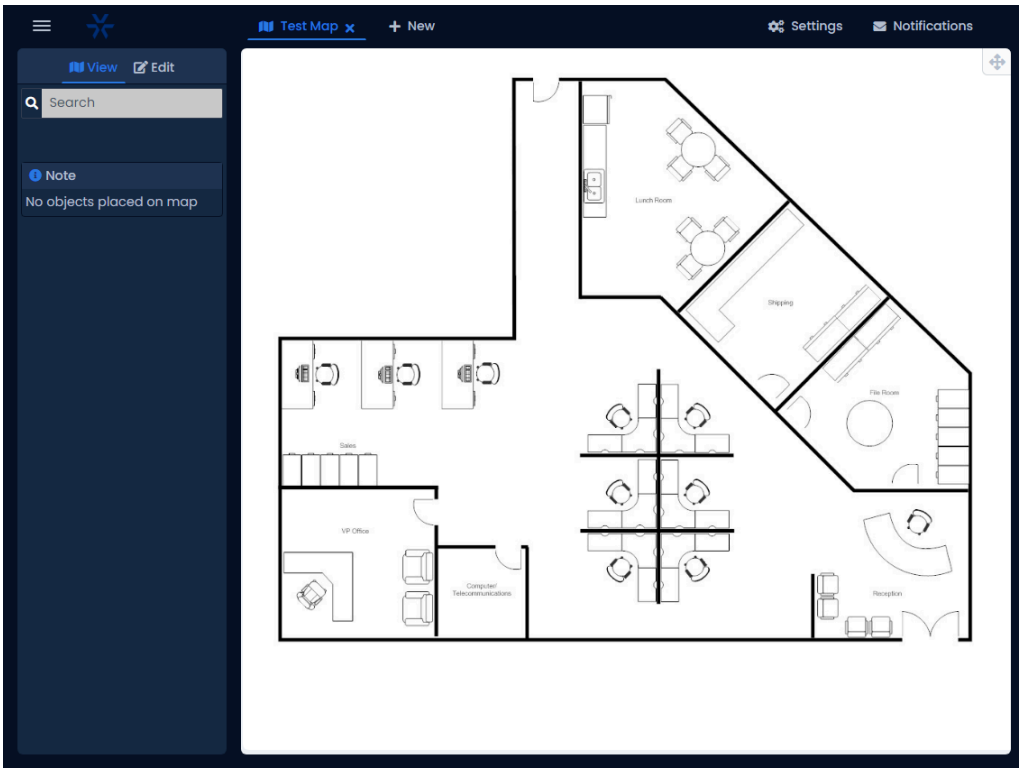
5. After clicking the Edit button, a list of available object types are now displayed in the left side of the page. Click on the name of the object type (Doors, Elevators, etc) to expand the objects of that type. Clicking Doors will show the door objects that can be displayed on the map.

Note

Only objects that are not already placed on the map will appear on the object list.

6. To place an object on the map, click and drag the object from the left side of the screen to the map displayed in the middle. You can now position the object in relation to its real world position.

Figure 34.5. Adding Objects to a Map



7. To remove an object from the map, click the object on the map you want to remove. A menu will appear on the right hand side that will allow you to delete the object from the map.

8. Once you have added any required objects to the map, click the View button on the top left.

Drawing an Area

Areas can be drawn on the map to visually show separation between areas and display who is in each area. More information on areas can be found in the section called “Edit Sites and Areas: Areas”.

Note

Drawing areas is not supported on mobile web browsers.

1. When editing a map, expand the Areas object types by clicking Areas on the left side of the page.

2. Click on the area you wish to draw on the map. A menu will appear on the right side of the screen.

3. You can now draw the area on the map by clicking the corners of the area to create a shape.

Tip

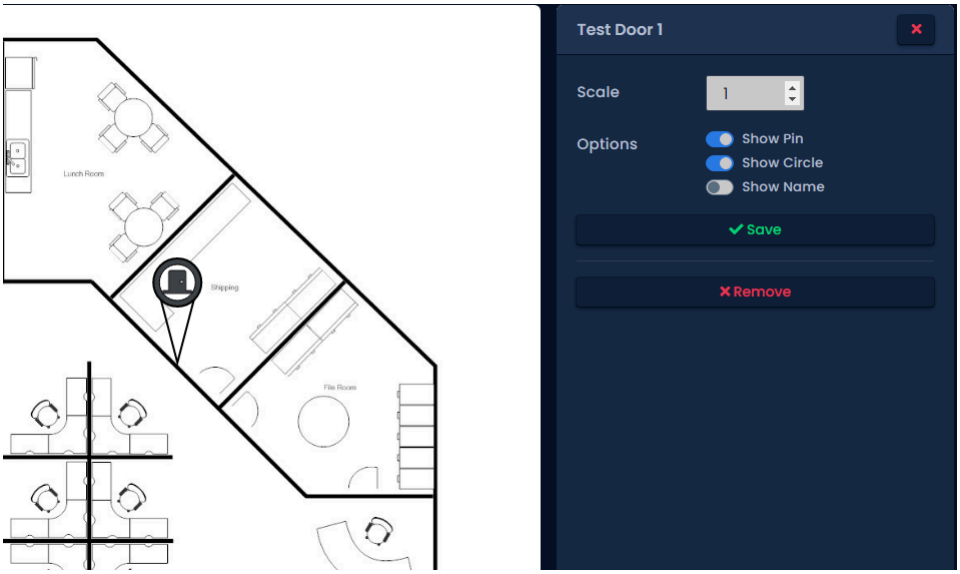
Controls when drawing map:

- Add Point: Left Click
- Remove Point: Right Click
- Move Point (snap): Left Click + Drag
- Move Point (free drag): Shift + Left Click + Drag

4. The color and transparency of the area can be modified on the menu on the right side of the screen if needed.

5. Click Save to save where the area is drawn. Click cancel to start over.

Figure 34.6. Drawing an Area



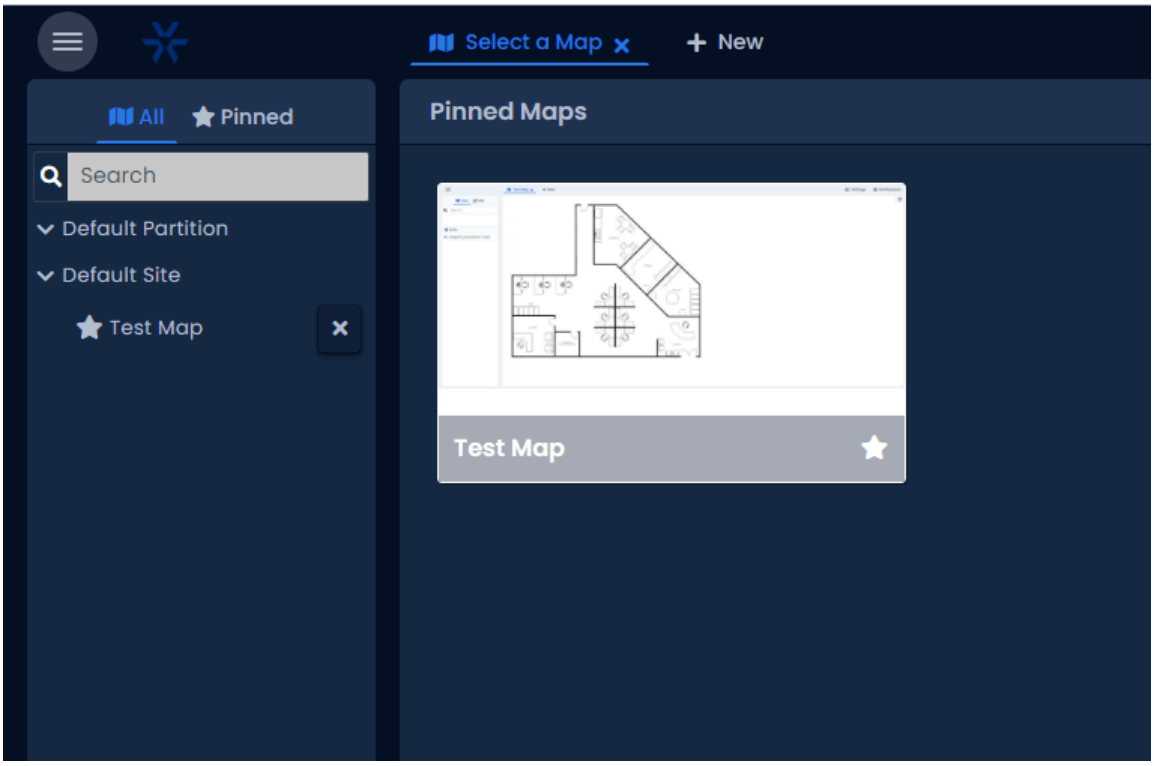
Viewing and Monitoring With Maps

This section will go over options available when viewing a map. Use the following steps to view a map.

1. On the **Side Bar**, scroll down to the section titled **Day to Day**, click on the **Maps** icon (pictured below). A new window will open in your web browser.

2. On the Map Viewer, you'll be shown the **Select a Map** tab, any maps you've already configured are listed here. A thumbnail of each map will appear with its title.

Figure 34.7. Select a Map

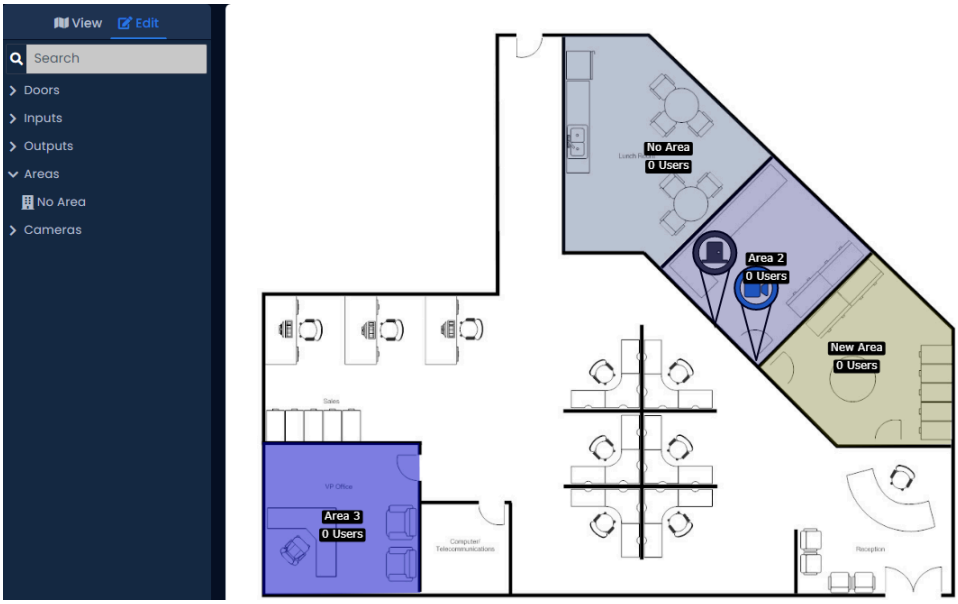


3. Select a map by clicking on it. The map will now be displayed along with any objects that have been placed on the map.

Tip

You can have more than one map open at a time by clicking the New button on the top of the screen. Open maps will be shown as tabs along the top of the page.

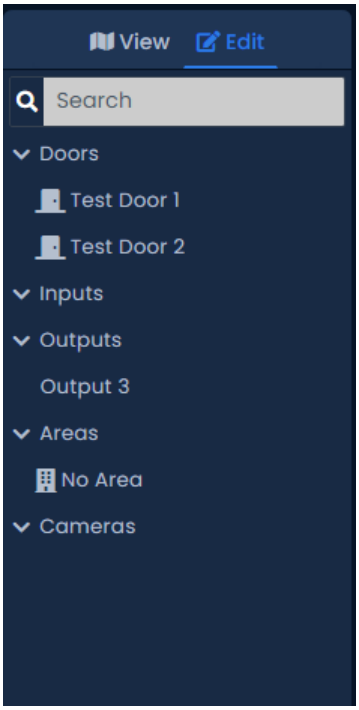
Figure 34.8. Typical Map



Map Objects Sidebar

The left side of the page will include a list of objects that have been placed on the map. Objects are separated into categories. You can expand the category by clicking the category name (Doors, Elevators, Cameras, Areas, Inputs, Outputs, Actions).

Figure 34.9. Map Objects Sidebar



On the map object sidebar, you can see the real-time status of the objects. The same status is shown on the map.

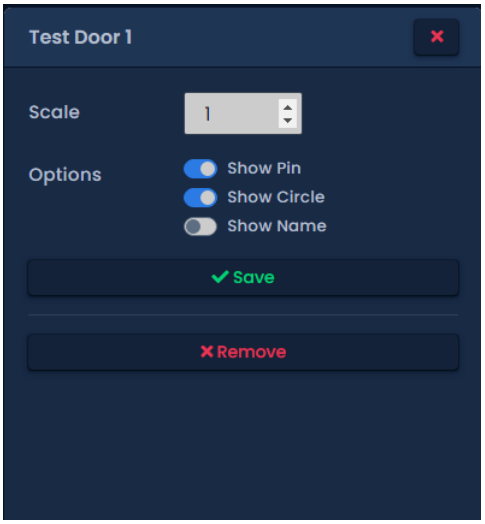
- Doors will show which mode they are in based on color code.
- Doors with door contacts will show if they are open or closed.
- Doors that are held open or forced open will have their name color changed to red and show the alert text right of the name.
- Objects that have been overridden will show their name as red.
- Objects connected to panels that are offline will appear grey.
- Left clicking an object in the list will display its corresponding context menu on the right side of the page and move the map viewer to the object on the map.
- Right clicking an object in the list will display a context menu for the object. You can use this to pulse a door, view a camera and more.

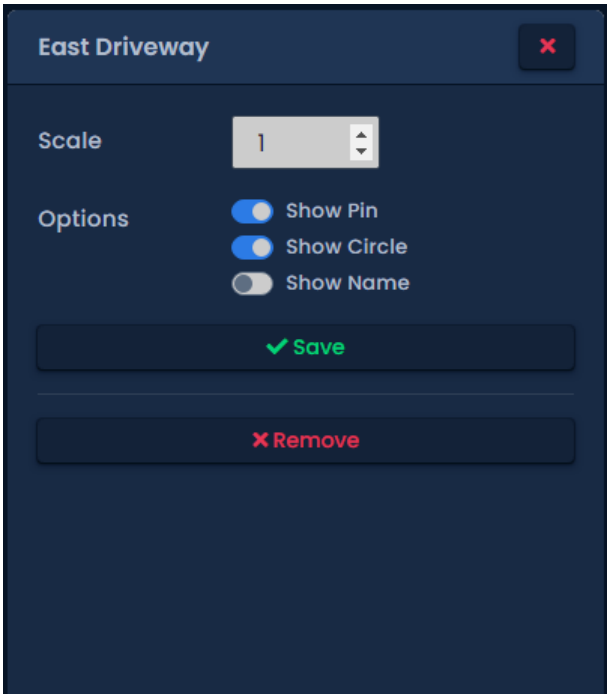
Object Details Sidebar

When an object is selected on the map or from the map objects sidebar, a sidebar will appear on the right side of the page with details and options for the selected object.

The contents of object details will depend on the type of object selected.

Figure 34.10. Object Details Sidebar Examples





Tip

If there is a camera associated with the selected object, a live camera window will appear in the sidebar.

Chapter 35. Third Party Integration

This chapter includes information about how VAX integrates with third party software systems. This includes the cardPresso® photo badging software and ASSA ABLOY wireless lock systems.

Assa Abloy® Aperio™ Lock Systems

This chapter covers the configuration and software/hardware requirements of using Assa Abloy Aperio Lock systems with Vicon Industries PoE controllers. For more information on the Assa Abloy Aperio systems, please visit http://www.assaabloy.ca/en/local/ca/Products/New-Innovative-Product/Aperio-wireless/

Software/Hardware Requirements

Warning

You must be certified by Assa Abloy reseller to order Assa Abloy products from Vicon Industries. Vicon Industries is a certified reseller of Assa Abloy products.

Ensure you have the following items before proceeding to installation:

- VAX Aperio Panel (2, 4 or 8 Door) with RS-485 Interface Plug in Module
- Assa Abloy AH30R12/Aperio Hub Comm RS-485*
- Assa Abloy USB radio dongle programming application tool*
- Aperio Programming Application*
- Aperio License Key file*
- Aperio Wireless Locks

* Included in Aperio Kit

Hardware Setup

This section will cover the hardware aspect of connecting the Aperio Hub to the VAX Aperio Panel. This section includes visual references and cable specifications.

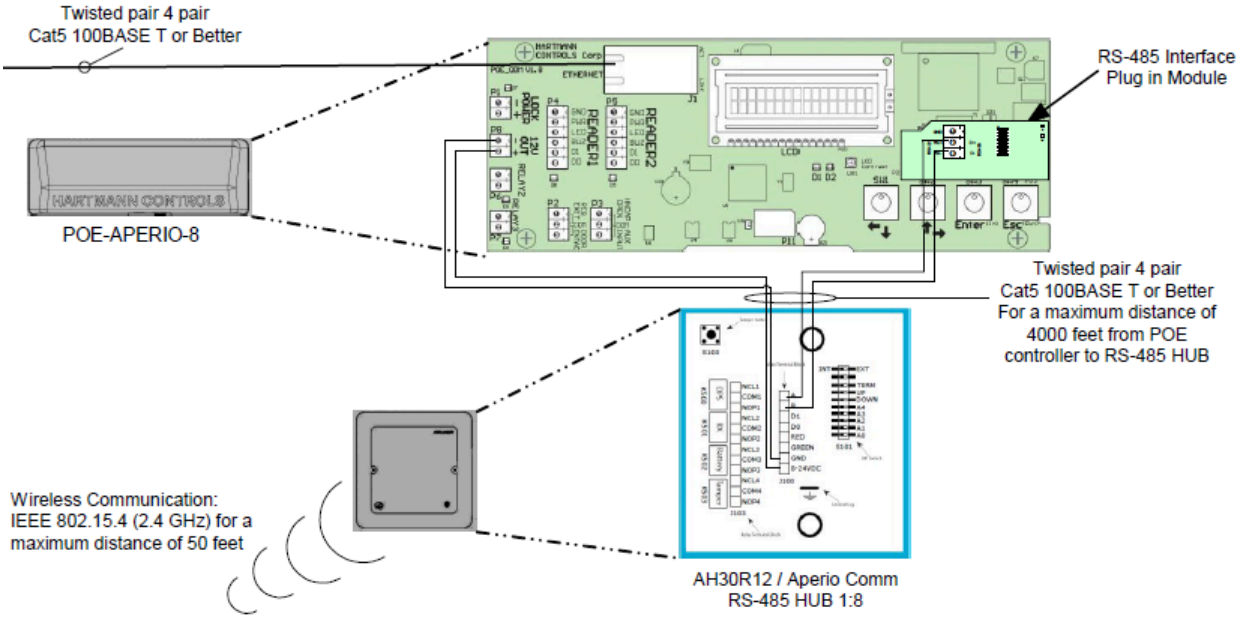
The VAX Aperio Panel communicates with the Aperio Hub via an RS-485 connection. An RS-485 Plug in module is included and installed in all Aperio Panels.

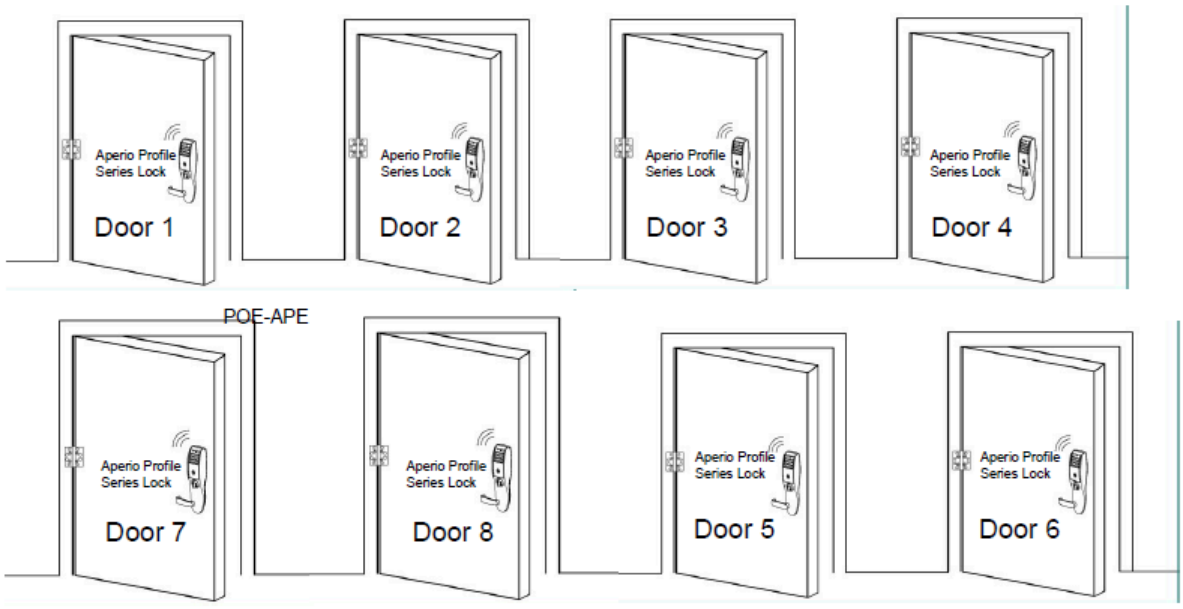
To connect the Aperio Panel to the Aperio Hub, please follow these steps:

1. Designate a pair of the RS-485 cable wires that will be providing power to the Aperio Hub from the Aperio Panel.
2. On the Panel side of the RS-485, connect the negative and positive wire to the 12V OUT header block on the left side of the Panel.
3. On the Aperio Hub, connect the other side of the power designated wires to the header block labelled 9-24VDC and GND. Ensure polarity matches what is connected to the Panel.
4. Designate a pair of the RS-485 cable wires that will be providing communication to the Aperio Hub from the Aperio Panel.
5. On the Panel side of the RS-485 cable, connect the data wires to the RS-485 plug-in Module header block on RX+(D+) and RX-(D-).

6. On the Aperio Hub, connect the other side of the communication designated wires to the header block labelled A and B. RX+ (D+) from the Panel will connect to A on the Aperio Hub. RX- (D-) from the Panel will connect to B on the Aperio Hub.

The following diagram visually demonstrates the communication topology of the Aperio Panel to the Aperio Hub.





Software Setup: Aperio Programming Application

This section will cover the software aspects of setting up the Aperio Hub to communicate with the Aperio Locks via the Aperio Programming Application. It is important to pair all of your locks with the Aperio Hub prior to adding the Doors in VAX.

1. On the laptop or PC you will be programming the Aperio Hub, download the Aperio Programming Application from your Aperio kit or from http://www.assaabloyresources.com.au/downloads/eac/Aperio_Common.zip

2. Unzip the Aperio_Common.zip to your computer and install the application.

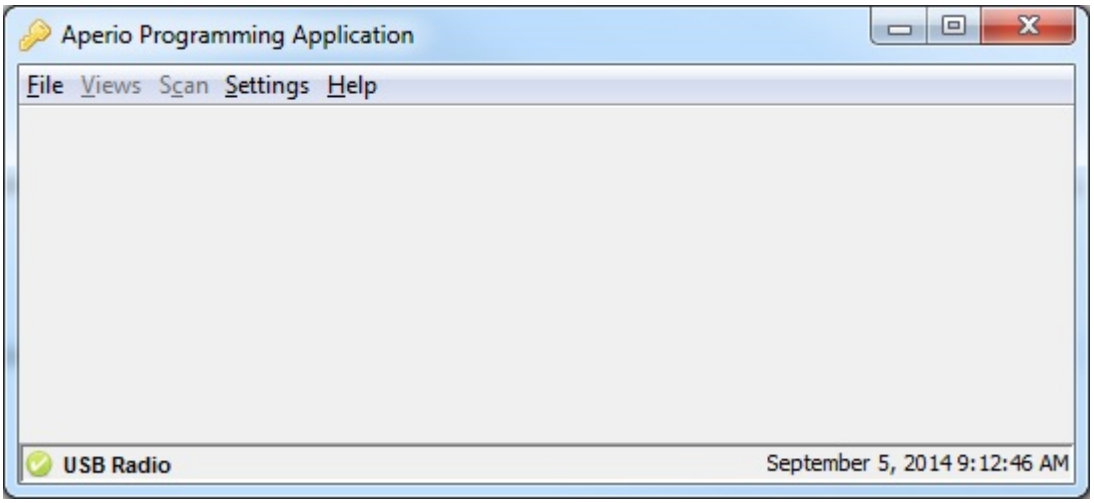
3. Plug in your Assa Abloy USB Radio Dongle and install the driver (located in the installation directory of the Aperio Programming Application).

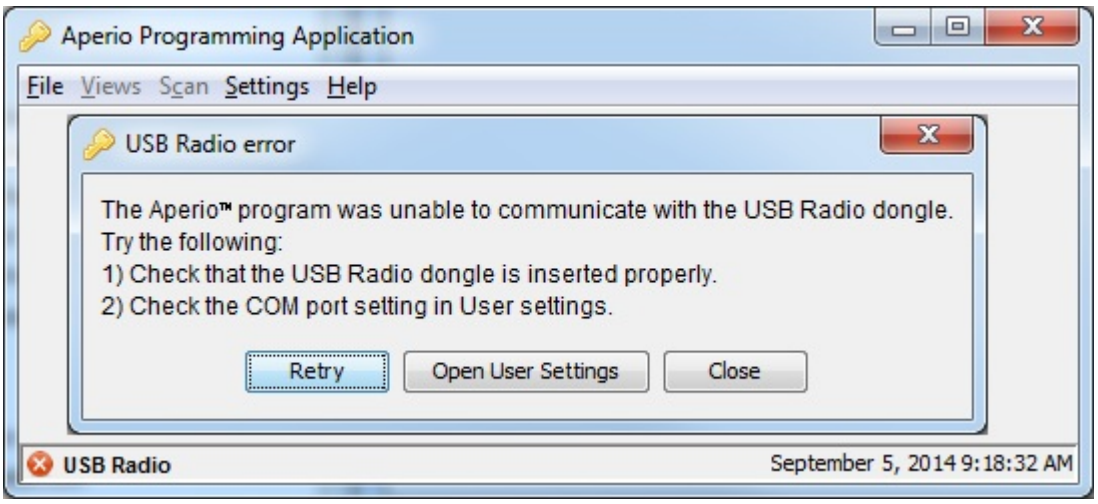
Note

If you're having trouble installing the dongle driver or the Aperio programming Application, please contact your internal tech support or Assa Abloy support.

4. Ensure in Windows Device Manager that the "Tritech TriBee USB" is recognized and functioning.

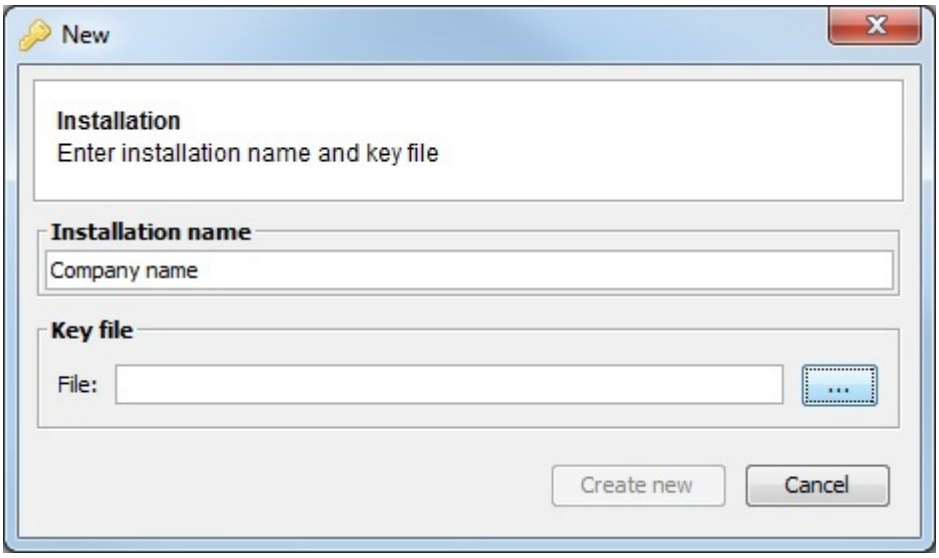
5. Launch the Aperio Programming Application from your start menu. If the Tritech Tribee is installed correctly and plugged in, you'll see a green circle in the bottom left side of the application next to USB Radio. If the USB dongle is not installed correctly or not connected to the PC/Laptop you'll receive an error.



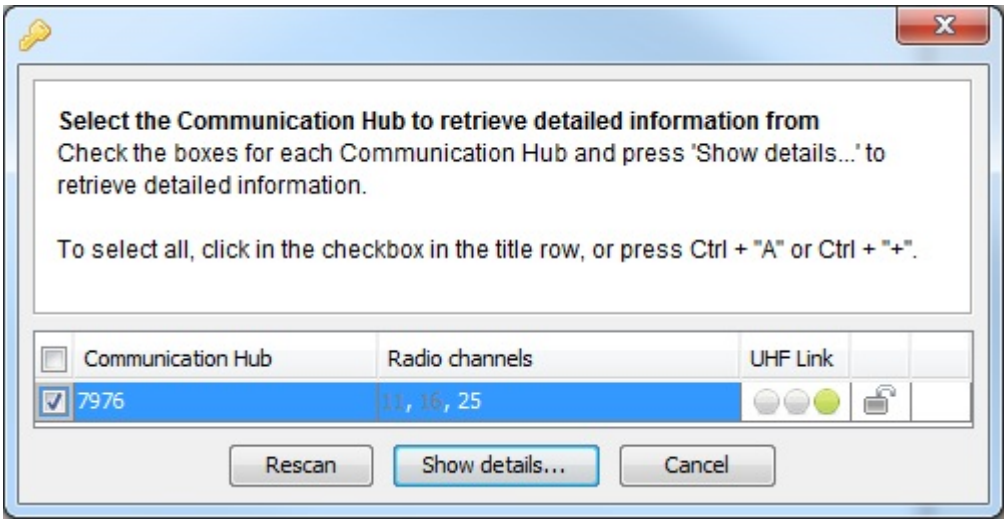


6. Once the Aperio Programming Application has detected your USB Radio, click File and then New on the top menu.

7. Enter an installation name (example: Company name). Browse and select the Key File provided in your Aperio Kit or received from Assa Abloy. Click Create new; you will be prompted to enter a password for the installation. At least 8 characters is required.



8. Once you enter your password, you'll be logged in and the application will automatically begin scanning for Communication Hubs. Click the check box next to the communication hub you wish to configure; click Show Details...

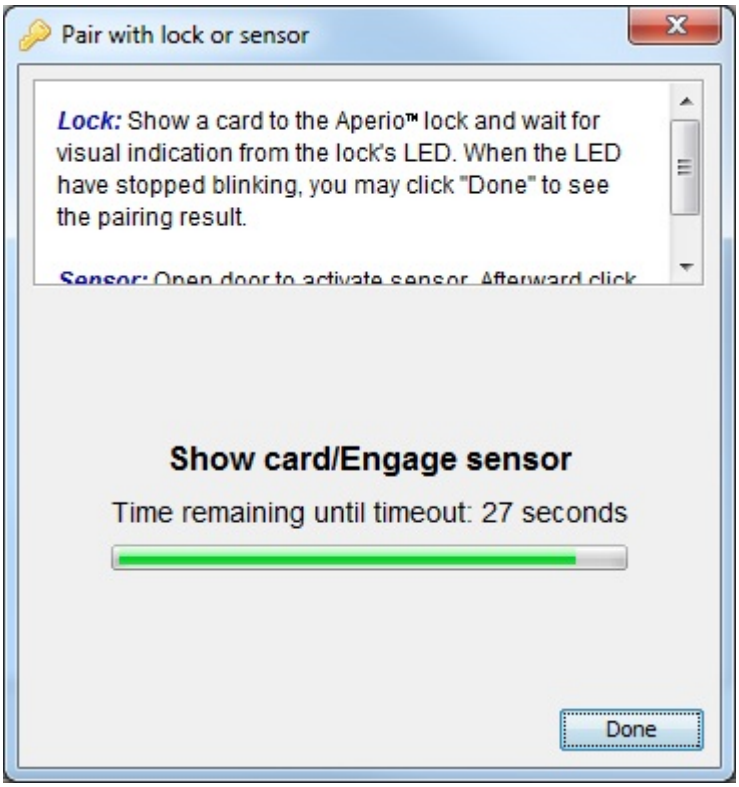


9. We can now begin pairing our locks with the communication hub. Right click on the communication hub you wish to configure. Click the communication hub sub menu on the hub you wish to pair locks with and click "pair with lock or sensor".

Note

Make sure the communication hub number matches the number on the physical hub; this is especially useful when configuring multiple hubs at the same time.

10. The Pair with lock or sensor window will now appear; you will have 30 seconds to present a card to the lock that you want to pair. Wait until the lock LED stops blinking before clicking "Done".



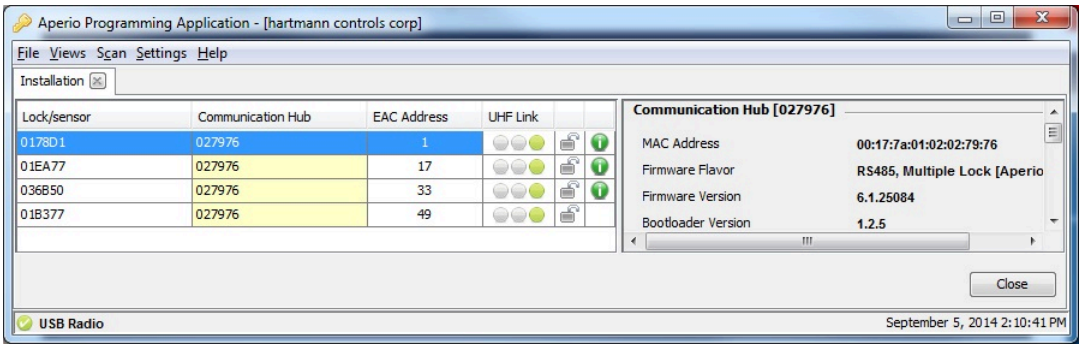
11. If the pairing is successful, you'll see "Communication Hub paired successfully to the following: XXXXXX" in the pair with lock or sensor window, where XXXXXX is the number printed on the back of the lock.

Note

Some lock models require the free egress side of the Door handle to be turned downwards and the card presented before it will sync with the Communication Hub. If your pairing fails, try this before troubleshooting other aspects

12. Repeat the pairing process with all the locks you'd like to configure. Once complete; take note of the EAC address of each lock and the lock sensor ID on the installation window, we'll need the EAC address of each lock in order to set the Door up in VAX

Examples of 4 Locks synced within the Aperio Programming application



Software Setup: VAX Aperio Panels and Doors

This section will cover the software aspect of adding VAX Aperio Panels to VAX and configuring Aperio Locks into VAX that were configured in the Aperio Programming Application. For more information on pairing locks with the Aperio Hub, please see the section called “Software Setup: Aperio Programming Application”.

The following should be completed prior to adding the VAX Aperio (2, 4 or 8 Door) Panel:

- Hardware has been installed, wired and functioning (Aperio Controller and Aperio Communication hub).
- Aperio Locks have been programmed using the Aperio Programming Application.
- EAC Addresses and lock IDs have been noted from the Aperio Programming Application.
- Locks are installed or awaiting installation within 50 feet of the communication hub.

1. Once the above requirements have been met, add the Panel in the same way you would add a normal door Panel, being sure to select the appropriate Panel model when adding. For more detailed information on adding a Panel, please see the section called “Adding a Panel to VAX Access Control”.
2. On the **Side Bar**, scroll down to the section titled **Hardware**; click on the **Doors** icon.
3. On the Doors screen, click Add. On the Add Door screen, enter the fields as you would on a normal Door. You'll notice when you change the Panel drop-down menu to the Aperio Panel, a new text box will appear called Aperio Address. This field is where we'll enter the EAC address of the lock we received from the Aperio programming application.
4. Once you've filled in the required fields, including the corresponding Aperio/EAC address, click Save. For additional information on adding a Door and configuring Readers, please see Chapter 8, *Setting Up a Door*.
5. Repeat the Door adding process on all locks; you'll notice when adding additional Aperio Doors that the Port on Panel will automatically increment in the drop-down menu.
6. Once all your Doors are configured, add a test User and place him in an Access Privilege Group that has access to the Readers you created on your Aperio Doors. Do an update to all Panels and test the card associated with the test User.

Chapter 36. Information for Domain and Network Administrators

Configuring Advanced Remote Access Through the Internet

This section will cover how to connect a Vicon Industries Panel of any type to a VAX server across the Internet. This section will also cover how to connect a web browsing client to the VAX server across the Internet.

How Panels Communicate

The VAX server is a listening device that listens on **TCP/UDP Port 9876** for Panel connections. The Panels reach out to the server by either DNS name or IP on TCP/UDP Port 9876.

After the Panel has been configured with the server IP address, the Panel sends an introductory data "packet" addressed to the IP of the server. The switch or router looks at the IP destination of this packet and applies some logic. It will first check its routing table and compare the address to devices or networks it knows about. If the server was on the same network, it would forward that packet to the switch closest to that server. If the packet does not have an address on the local network, it will forward the packet to its **Default Gateway**, and likely from there go to the Internet.

Once through the Internet, the packet will reach the public IP address of the network where the VAX server resides. An IT Administrator would have set up a **Port Forwarding Rule** to forward any traffic with a destination TCP/UDP port of 9876 to the internal address of the VAX server. Once communication is established and the Panel is added in the VAX software, the Panel and server will communicate both ways to each other, and occasionally check in to see if the other end is still active.

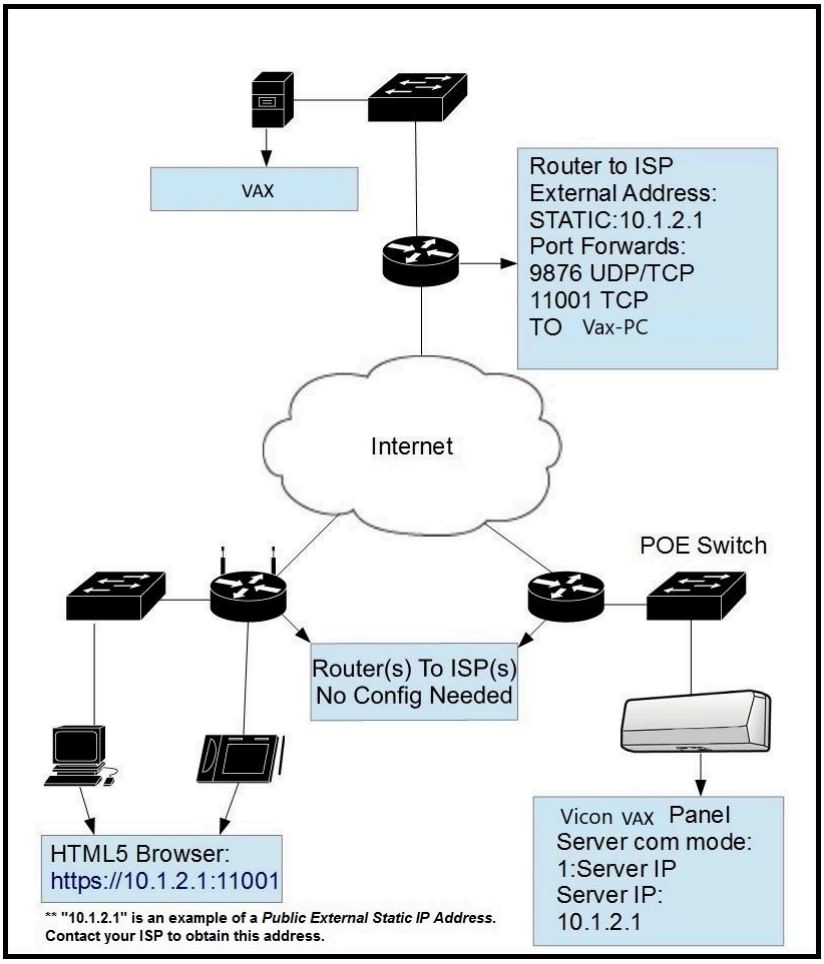
How Web Clients Communicate With VAX

The VAX web service listens on **TCP Port 11001** for incoming web client connections. Clients on the same network can use a web browser directed to the IP address of the server or the name. Clients across the Internet who want to reach the VAX server will need to browse using the **Public Static IP Address** of the router connected to the private network the VAX server resides on. The destination TCP port 11001 will need to be forwarded the internal address of the VAX server via a port forward rule setup on the router. If the client requires access to the System Manager UI, destination **TCP port 11002** will also need a port forward rule.

Remote Access: Network Requirements

This section covers the network requirements in order for a server to receive connections from web clients or Panels through the Internet. These section includes visual diagrams to help you understand the data flow.

Figure 36.1. Network Topology: Remote Clients and Panels



Network Requirements

- The site with the VAX server needs to have a **Public Static IP Address** given to them by their ISP. Call your ISP for details and costs associated with leasing a public IP.
- VAX PC must have a static internal address.
- The main router on the site with the VAX server must be capable of port forwarding. Please consult your router manual for details.
- Destination ports TCP/UDP 9876 must have a port forward rule to the internal address of the server for Panels to communicate through the Internet. Destination ports TCP 11001 and 11002 (if required) must have port forward rules to the internal address of the server for clients to access the web interface through the Internet.

Dynamic DNS. When obtaining a Static IP Address from an ISP is too costly or not feasible, the alternative is to use a Dynamic DNS service. This service is offered by several Internet Service Providers (sometimes free but may be a charge). These services create a domain name that is associated with your dynamic Public IP Address; the IP Address the domain is associated with is updated automatically using some client software or some special router configuration. Vicon Industries does not provide this type of service; for more information on dynamic DNS please talk to local IT staff, or check resources available on the Internet.

Note

The site on which the client and Panels reside do not need any Port forwards or static addresses (in most cases) because they are calling out to the server using dynamic source ports. Only the site with the VAX server requires additional configuration.

Warning

Once you have obtained the static public IP from your ISP, you must enter this address in the Server Address field in the VAX software under Home>System Settings>General Configuration: Server Address. Once you do a Panel update, this will be the address your Panels will use to find the server, overriding any manually configured values.

Table 36.1. Terminology Reference

Term	Description
VAX Server	The computer (can also be a virtual machine) that the VAX web service is running. This computer can be browsed to over the network or Internet/WAN to configure and view your access control system.
Public Static IP Address	This is the address that represents your home network on the Internet. Normally, a public external address is given to you dynamically by your ISP, meaning it will change every few days or so. A static public IP is required for a stable consistent connection to our software.
Port Forwarding	Port forwarding is used to permit external hosts (clients and Panels) to connect to services hosted within an internal network. This allows us to map the destination ports 9876, 11001 and 11002 to the internal address of the server.

Remote Access Examples

This section will include example scenarios of remote access, including scenarios where dealers/installers will host the VAX server.

Example 1: Expansion Into Second Office. A business has expanded into a second office, and installs Vicon Industries Door Panels in its second location. Instead of purchasing a second server and license for the second site, they can configure the Panels at the new site to connect to the server at the main office. The IT staff obtains a static public address from their ISP for the main office. They also set up port forward rules for TCP/UDP port 9876, TCP port 11001 and TCP port 11002 to the internal address of the VAX server. They also make sure the VAX software has been configured to push the new address in 'Home>System Settings>Server Address'. The IT staff will configure any additional firewall rules if needed. Panels and clients may now communicate freely with the VAX server.

Example 2: Dealer Hosted VAX Server. A dealer/installer would like to host his clients VAX servers at his office in order to provide maintenance and ensure proper backups and software upgrades. The dealer company obtains a static IP for its office and creates the appropriate port forward rules to direct client and Panel traffic to the server internally on their network. When the dealer deploys new client's, he can pre-configure the Panels and test them at his office. The dealer will likely utilize Partitions and have a separate Partition for each client along with an Administrator account that can only manage that client's Partition. This way the dealer can host several customers information on one software installation.

Performing Manual Back-up and Restore with MSSQL Command-Line

This section covers advanced Back-up and Restore procedures in VAX. This covers performing database back-ups and database restoration with SQL Command-Line.

Warning

These instructions should only be performed by IT professionals and qualified Vicon Industries installers. If you're having trouble performing Back-Ups and Restores with the System Manager UI, please give this document to your internal IT staff or contact Vicon Industries. Please see Chapter 37, *Support*.

SQL Database Back-up

This section covers how to perform a database back-up via SQL Command-Line.

1. On the computer with VAX installed, open a Command Prompt (search cmd.exe or located in C:\Windows\system32) with Administrator privileges. (To do so, right click on cmd.exe and select "Run as Administrator".)

2. At the Command Prompt, type '**SQLCMD -S .\VAX**' and press **Enter**. (VAX is the default name for the database instance, your instance name may vary. To find your instance name please see the section called “Database Back-Up/Restore: Frequently Asked Questions”.)

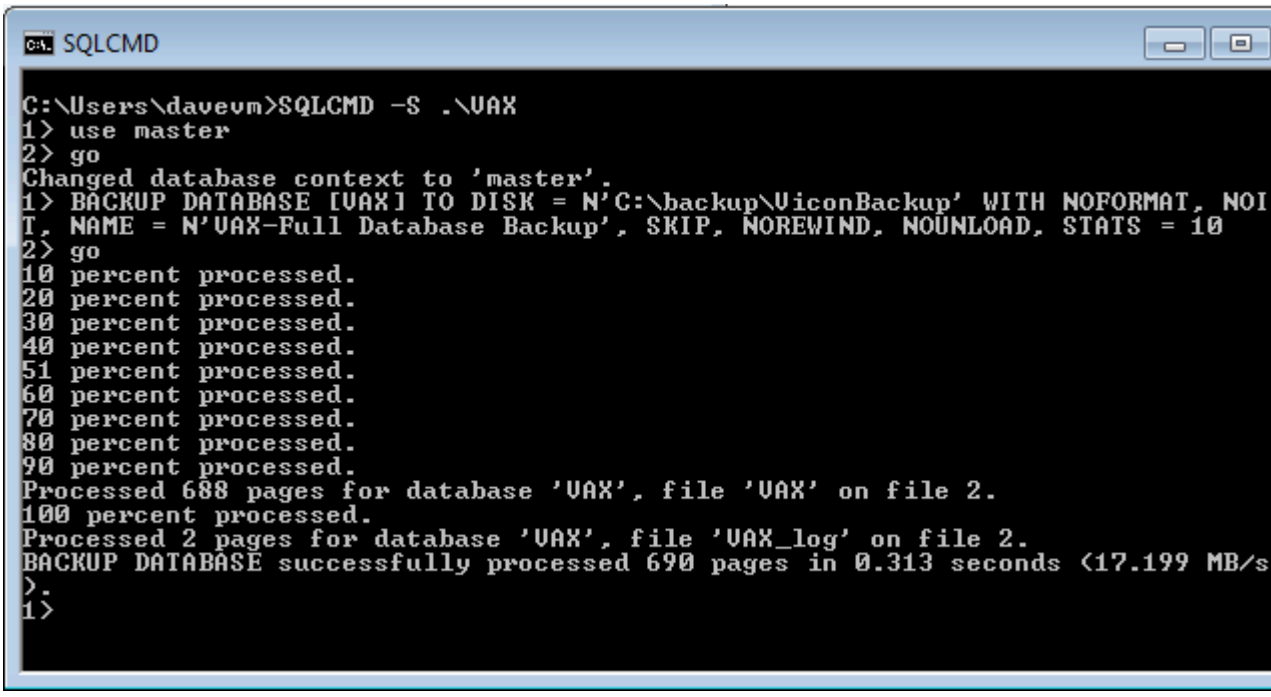
3. Type '**use [master]**' and press **Enter**. Type '**Go**' and press **Enter**.

4. We recommend creating a backup folder located on the root of **"C:/"** drive. In the below example we use "**C:\backup**" as the folder the database is backed up to.

5. Type '**BACKUP DATABASE [VAX] TO DISK = N'C:\backup\VAXbackup' WITH NOFORMAT, NOINIT, NAME = N'VAX-Full Database Backup', SKIP, NOREWIND, NOUNLOAD, STATS = 10**' and press **Enter**.

6. Type '**Go**' and press **Enter**. The backup will now be performed if the database name and backup location are correct.

Figure 36.2. Command Prompt: Backup



SQL Database Restore

This section covers how to perform a database restore via SQL Command-Line.

1. Install VAX on the computer that the database will be restored to. Ensure the version of VAX installed is the same version or newer than the version the database was backed up from.

2. If the backup was performed by command line, move the backup file to the computer (via USB drive or email) to a folder on "**C:/**" called "**backup**".

3. If the backup was performed by the System Manager UI:

   "**VAX_<dateofbackup>.prbak**" will need to be renamed to:

   "**VAX_<dateofbackup>.zip**".

   Extract the file and copy the file "**VAXFullBackup.bak**" to "**C:\backup**".

4. Stop the VAX Web Service via System Monitor (see the relevant section within the master tech guide) or via System Management UI (see Chapter 5, *System Manager UI*).

5. On the computer with VAX installed, open a Command Prompt (search cmd.exe or located in C:\Windows\system32) with Administrator privileges. (To do so, right click on cmd.exe and select "Run as Administrator".)

6. At the Command Prompt, type '**SQLCMD -S .\VAX**' and press **Enter**. (VAX is the default name for the database instance, your instance name may vary. To find your instance name please see the section called “Database Back-Up/Restore: Frequently Asked Questions”.)

7. Type '**use [master]**' and press **Enter**. Type '**Go**' and press **Enter**.

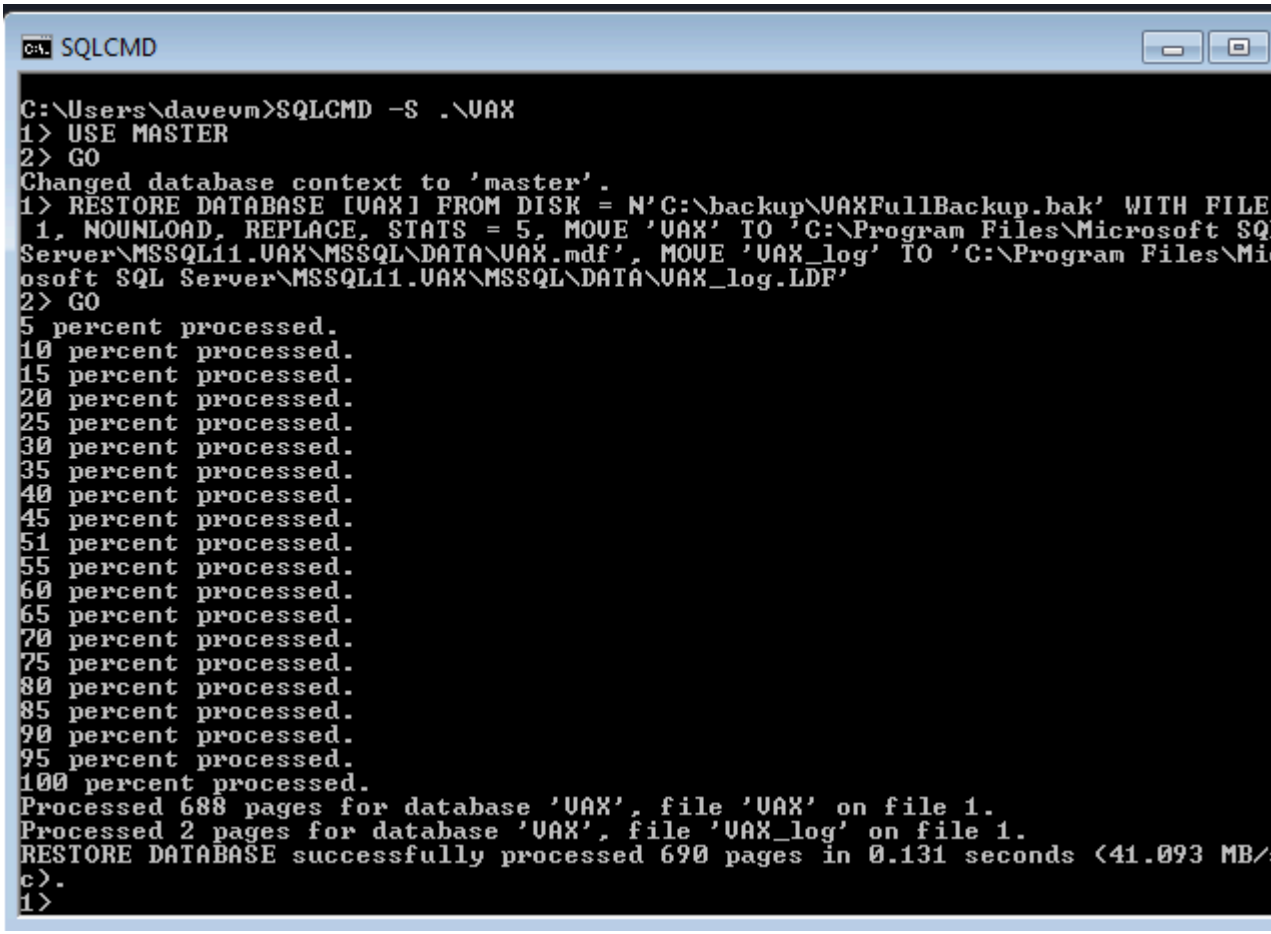
8. Type:

   '**RESTORE DATABASE [VAX] FROM DISK = N'C:\backup\VAXbackup' WITH FILE = 1, NOUNLOAD, REPLACE, STATS = 5, MOVE 'VAX' TO 'C:\Program Files\Microsoft SQL Server\MSSQL11.VAX\MSSQL\DATA\VAX.mdf', MOVE 'VAX_log' TO 'C:\Program Files\Microsoft SQL Server\MSSQL11.VAX\MSSQL\DATA\VAX_log.LDF'** and press **Enter**.

9. Type '**Go**' and press **Enter**. The restore will now be performed if the database name and database path are correct.

10. Start the VAX Web Service and login to confirm the backup was successful.

Figure 36.3. Command Prompt: Backup



Database Back-Up/Restore: Frequently Asked Questions

Q: Why didn't the built-in Restore utility work?

A: Microsoft SQL Server is a fairly sophisticated piece of software, however the locations and behaviors of its associated databases change depending on the Operating System of the computer, the version of SQL server installed and the system architecture (32 or 64 bit). When restoring a VAX database to a different computer, if any of these factors change the database file cannot find the path of the database and requires some extra help.

Q: Where can I find the name of my Database Instance?

A: You can find the name of your database instance on an existing VAX installation using the following steps:

1. Browse to the WebServer folder of your VAX installation directory (usually located in "C:\Program Files (x86)\Vicon Industries\VAX\WebServer").

2. Open the file named "VAX.exe.config" in a text editor such as notepad.

3. Look for the line: 'connectionString="Data Source=pcname\VAX;' where 'pcname' is the name of your computer/server. The name after the PC is the name of the database instance VAX is currently using.

Performing Data Migration with Data Migrator

This section covers importing and exporting data in VAX between partitions.

Exporting Partition Data

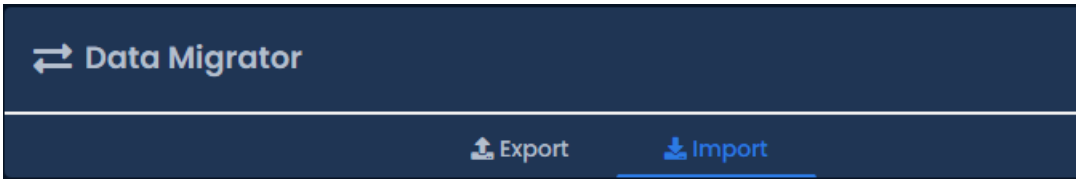
This section covers how to perform an *export* of partition data via data migrator.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Administration**; click on the **Data Migrator** icon (pictured below)

Figure 36.4. Data Migrator Icon

4. Ensure the **Export** tab is selected.
5. Select the Partition(s) you which to export.
6. Select the Options to export.
7. Select **Export** and select a location to save your data file.

Figure 36.5. Data Migrator: Options To Export



Importing Partition Data

This section covers how to perform an *import* of partition data via data migrator.

1. Access your VAX system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Side Bar**, scroll down to the section titled **Data Migrator**; click on the **Data Migrator** icon (pictured below)

Figure 36.6. Data Migrator Icon

4. Ensure the **Import** tab is selected.

5. Click **Choose File**. Browse to the data file's location, select the file and click open.

6. Select **Parse**.

7. Verify the import content and select the partition you would like to import. Create and name a new partition or use the drop-down menus to select an existing partition.

8. Use the checkboxes to select the data you would like to import to the partition.

9. Select **Import**

Figure 36.7. Data Migrator: Import

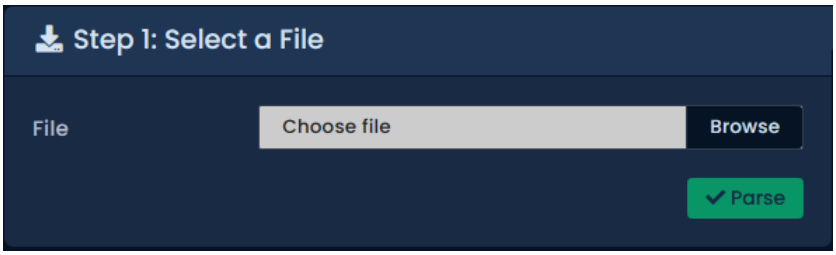


Table 36.2. Conflict Strategy

Strategy	Brief Explanation
Duplicate	Don't match against existing users, duplicate every user into mapped partition.
Credentials	Use existing user if all credentials match imported user.
Name	Use existing user if first name and last name match exactly
Both	Use existing user if all credentials and name match imported user.

API Integration

This chapter will review resources available to access the Restful and Real-time API in VAX

VAX features a REST HTTP API allowing simplified integration with third party systems.

Warning

All APIs are provided as is with no express or implied warranty from Vicon Industries. Vicon Industries does not provide support for any application or project developed using these APIs.

REST API

The REST API provides a REST-FUL web integration platform. This service provides access to most data management functionality within VAX, including querying and adding records to the database. Requests are sent to the VAX server using HTTP and the JSON data format. The REST API is used extensively within the VAX application.

Real-time API

The real-time API provides a smaller subset of operations then the REST API and it's operations are primarily geared towards obtaining live status information from your system. This includes things like the current state of a device or obtaining real-time events from your system. The real-time API uses

SignalR [http://signalr.net/] and requires availability of a client library in your development language of choice.

Accessing API documentation

The Real-time and REST API documentation is available on any version of VAX 2.7 or newer.

If you have an existing system, you can access it with the following:

https://NameOrIPoFServer:11001/apidocs

If you don't have a live system to view the documentation, you can view it online on our demo system.

https://VAXdemo.com:11001/apidocs

Multi-Tenant Mode Configuration

Multi-Tenant is a feature available in VAX that allows IT companies or dealers/installers to host multiple VAX databases on a single system.

Multi-Tenant Mode allows each tenant to have a separate database and entry point to VAX. The server will require a proper domain name, as each tenant will be provided one or more subdomains, i.e., https://**client1**.dealername.com:11001

When multi-tenant mode is enabled, there are some aspects that should be noted:

- Fully qualified domain name is required with a 'DNS A Record' for each tenant.
- A separate database will be created for each tenant. They can be on the same instance or separated.
- Each tenant will require their own VAX license.
- Unknown panels will not generate a unknown panel notification until an association is created from within System Manager UI.
- System Manager UI will allow multiple administrators to be configured.
- Database backups will now be configured and scheduled on a per database basis.

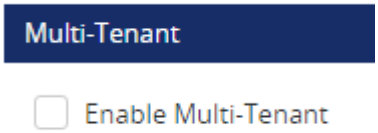
Warning

Enabling multi-tenant cannot be reversed. Carefully consider this before enabling this feature.

Enabling Multi-Tenant Mode

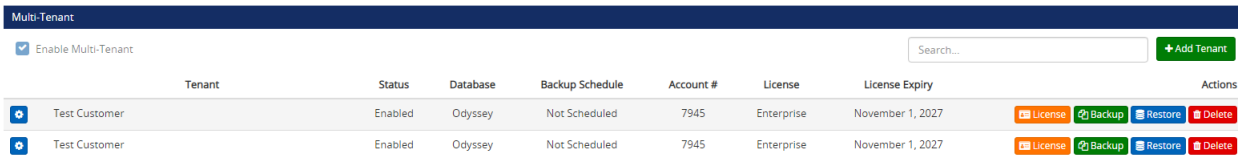
Multi-tenant mode is enabled from the system manager UI. DNS A records and pointers should be configured prior to enabling multi-tenant. Use the following steps to enable multi-tenant:

1. Access the VAX System Manager UI as outlined in the section called “Accessing the System Manager UI”.
2. On the System page of the System Manager UI, check the Multi-Tenant checkbox on the bottom of the screen.



3. A informational prompt will appear. Read it and click OK. Muli-tenant will now be enabled. The VAX web services will be restarted during this process.
4. Log back into the System Manager UI or refresh the page.
5. The existing VAX database will be changed into your first tenant. All tenants will be displayed on the bottom of the System Manager UI. They can be edited with the blue edit button to the left of the tenant name.

Figure 36.8. List of Tenants



Adding Tenants

This section outlines adding additional tenants once multi-tenant mode has been enabled.

1. In the System Manager UI, click the Add Tenant button.
2. On the Create Tenant screen, fill in the name of your tenant. This will usually be the company name or customer name.
3. Enter a valid database Connection String. This will be used to create the database for this tenant.

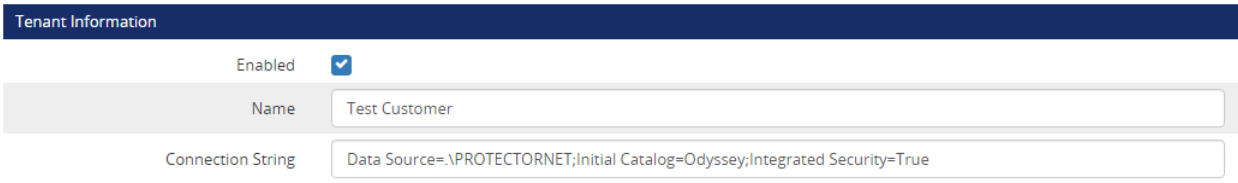
Example 36.1. Database Connection String:

Data Source=VAXSERVER\VAX; Initial Catalog=Client1;Integrated Security=true

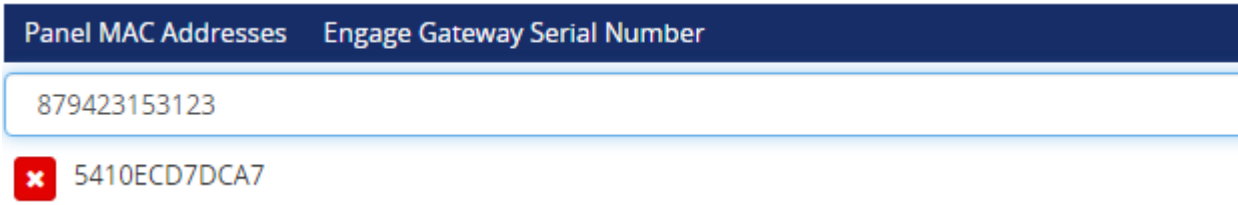
In the above example, **VAXServer** is the name of the computer the database will reside on. **VAX** is the name of the database instance the database will reside on. This can be the same for all tenants. **Client1** is the name of the database that will be created for the tenant. This must be unique.

Note

The VAX web service must be running as a service account that has permission to create databases in the specified database instances.



4. You can optionally configure which panels will be associated to this tenant. You can enter the panel MAC address and click the Add button for each panel. A list of unassociated panels will also be displayed on the bottom of the page. If you see a panel that should belong to the tenant being added, click the '+' next to the panel name. You can add more panels after the tenant is created.



5. Enter any End Points. An endpoint is the subdomain a tenant will use to access their VAX instance. You only need to provide the subdomain portion. Click the Add button next to the endpoint name.

6. Click Save once you've filled in the tenant information. You can now access the tenant via the configured endpoint.

Managing Tenants

While editing a tenant, you can edit all settings available when adding a tenant. This includes associating additional panels and adding endpoints.

Backing up Tenant Databases

Each tenant will have their own database backup and backup schedule. Use the following steps to backup a tenant database:

1. On the home page of the System Manager UI, click the Backup button to the left of an existing tenant.

   or

   When editing a tenant, click the Backup button on the top right of the screen.

2. You will now be on the Backup Options for that specific database. These options are thoroughly covered in the section called “Backing up your VAX Database”.

3. We recommend you set an automatic schedule for your backups. Backups for an individual tenant will include the tenant name in the backup file.

Restoring Tenant Databases

Each tenant database can be restored individually from a previous backup.

Warning

Restoring any tenant database will temporarily restart the VAX web service.

Use the following steps to backup a tenant database:

1. On the home page of the System Manager UI, click the Restore button to the left of an existing tenant.

   or

   When editing a tenant, click the Restore button on the top right of the screen.

2. You will now be on the database Restore screen for that specific tenant. These options are thoroughly covered in the relevant section within the master tech guide.

Accessing Tenant Web Interface With a Subdomain

After the tenant is created and assigned an Endpoint; you should access the web interface of the tenant in order to create a login and input initial information.

Each tenant is accessed via a unique DNS subdomain. Don't forget to include HTTPS header and the port (default is 11001).

https://**client1**.dealername.com:11001

Tip

After a subdomain is added to the DNS record, it may take up to 24 hours before all DNS servers are aware of and able to resolve the new subdomain.

Once you access the web interface, you'll configure the system just like you would normally. See Chapter 3, *Initial Configuration* for details on the initial configuration screen.

Accessing Tenant Web Interface Without a Subdomain

In the case that your multi-tenant system won't be public or you would like to test multi-tenant without obtaining an official subdomain; use the following instructions to allow the server to access individual tenants locally.

1. Open Notepad as an administrator.
2. Open the file titled hosts in "C:\Windows\System32\drivers\etc". You may need to adjust the file type drop-down menu to "All Files" in order to see the hosts file.
3. For each tenant you've added, you'll need to add a new entry (1 per line) to file. It should look like:

   127.0.0.1 client1.computername

   127.0.0.1 can be replaced with the IP of the VAX on remote computers. Add entries as needed.
4. Save the file and you can now access the web interface of a tenant. Don't forget to include HTTPS header and the port (default is 11001).

   https://**client1**.computername:11001
5. Once you access the web interface, you'll configure the system just like you would normally. See Chapter 3, *Initial Configuration* for details on the initial configuration screen.

Chapter 37. Support

End Users:

Vicon Industries does not generally support end users directly as we rely on our vast network of trained dealers and installers to service our products in the field. If your system requires service, we recommend contacting your dealer/installer. If you do not know who your dealer is, you can contact Vicon Industries and we will assist you in finding a local dealer/installer.

Dealers/Installers:

Vicon Industries support is available to dealers Monday to Friday between 9AM and 5PM EST to assist with any installation related issues you may have.

Website

Vicon Industries offers a number of technical guides and resources via our website: https://www.vicon-security.com

Email

Email support is available through our website at https://www.vicon-security.com/learn-and-support/support-and-sales-contacts/. Please allow 24 - 48 business hours for a response.

Phone

If time sensitive support is required, we do offer both local and toll-free support numbers during normal business hours. Outside our regular business hours, please allow 24 to 48 business hours for response. You may reach us at:

- **Toll Free (North America only):** 800-348-4266

Chapter 38. DSC IP Alarm integration

DSC Power Series alarm/intrusions panels are integrated into VAX through a network based communication based on UDP protocol. This chapter will cover the overall features of the integration, how to configure communication, how to functionally use the integration and use cases.

Caution

This chapter assumes that the reader is familiar with DSC Intrusion Panels. Please refer to their documentation for more details.

DSC Integration Features

The integration allows the following options:

- View status of Alarm Partitions and Alarm Zones through the VAX web interface through notifications or System Overview
- Arm (Stay Arm, Away Arm, Night Arm) and disarm through the VAX web interface, Mobile app, Action Plans or through the VAX API
- Bypass zones, contact emergency services, silence trouble beeping
- Configure Alarm related notifications as Triggers within Action Triggers
- Execute reports against Alarm Partitions, Zones and Intrusion specific notifications

High Level Overview of Integration Steps

Successful integration involves configuration within the Intrusion Panel keypad and the VAX web interface. This section will summarize those steps. More details on the individual steps are covered in the proceeding sections.

1. Install and perform initial configuration of the VAX software.
2. Ensure server has a static IP or reliable DNS name and UDP port 3073 is allowed on any relevant firewalls or port forward rules (if the VAX server is remote from the Intrusion Panel).
3. Partitions and Zone definitions are configured within the Intrusion Panel;, such as the names of the Zones and Partitions and is connected to the network.
4. Set the Static IP of the VAX server into the Session 1 Integration Server IP menu within the Intrusion Panel ([*][8][installer code][851][428]) or set the DNS Name of the VAX server into the Session 1 Integration Server DNS menu within the Intrusion Panel ([*][8][installer code][851][431]).
5. If the default port (UDP 3073) is not feasible, you may change the port through the Session 1 Integration Outgoing Port menu within the Intrusion Panel ([*][8][installer code][851][432]).
6. If a Static IP is required for the intrusion Panel (DHCP by default); these options can be set within [*][8][installer code][851][001], [*][8][installer code][851][002], [*][8][installer code][851][003] and [*][8][installer code][851][007].
7. Set Communication Delay within the intrusion panel to 60 seconds ([*][8][installer code][377][002]).
8. Set Alternate Communicator within the intrusion panel to Yes ([*][8][installer code][382][5]).

9. Set Session 1 Integration Toggle Options 2 so that 3 and 5 are set (03 – Integration Over Ethernet, 05 – Integration Protocol) within the intrusion panel ([*][8][installer code][851][425]). LCD should show "--3-5---".

10. Set Session 1 Integration Toggle Options 3 so that 1, 3 and 4 are set (01 – UDP Polling, 03 – Real-time Notification, 04 – Notification Follows Pool) within the intrusion panel ([*][8][installer code][851][426]). LCD should show "1-34----".

11. Integration ID is configured/obtained from the Intrusion Panel ([*][8][installer code][851][422]). The number will be 12 digits long.

12. Integration Access Code is configured/obtained from the Intrusion Panel ([*][8][installer code][851][423]). The default code is 12345678.

13. Installer Code is configured/obtained from the Intrusion Panel ([*][8][installer code][006][001]). Default code is 5555.

14. Master Code is configured/obtained from the Intrusion Panel ([*][8][installer code][006][002]). Default code is 1234.

15. Within the VAX web interface, add the Intrusion Panel via the Alarm Panels section with Name, Type, Site, Integration ID, Integration Access Code, Installer Code and Master Code.

16. Wait until you receive a Notification with the text "Alarm Panel is now Online".

17. Configure Notification Settings, Action Triggers and Action Plans to meet any integration specific goals.

In addition to these steps, hard wired integration may still be used via dry contact relay/input connections.

DSC Panel Communication Setup

This section outlines the steps and information required before adding the DSC Panel to VAX.

The communication architecture between the Intrusion Panel and VAX is client-server. The Intrusion Panel reaches out to a specified IP address using UDP port 3073 by default.

DSC Panels can communicate to up to 4 third-party services. Integration specific settings have a session associated with them. This section is written with Session 1 being assumed as the available session. Please refer to DSC documentation for clarification on which subsections are used for session 2, 3 and 4.

These steps should be taken after the VAX software bas been installed, initial configuration has been completed and Partitions and Zones have been configured on the intrusion panel via the Hardwired LCD Keypad. For assistance with intrusion Panel specific steps, please contact DSC support.

Instructions for navigating to specific menus through the LCD Keypad will be displayed in the same manner they are displayed in DSC documentation.

1. Note down the static IP address or DNS name assigned to the VAX server. If the VAX server is on a different network than the Intrusion Panel;, port forward rules, routing and firewall rules may be required.

2. **If a Static IP Address was chosen as the communication method:** Through the DSC LCD Keypad interface, navigate to the Integration Server IP menu using [*][8][installer code][851][428]. Use the keys to enter the local IP address of the VAX server or public IP address of the router the VAX server is connected to.

3. **If a DNS Name was chosen as the communication method:** Through the DSC LCD Keypad interface, navigate to the Integration Server DNS menu using [*][8][installer code][851][431]. Use the keys to enter the DNS Name of the VAX server or resolvable domain address.

4. The default port used for the integration is UDP 3073. You can change this port if needed through the Integration Outgoing Port menu via the DSC LCD Keypad interface by navigating to [*][8][installer code][851][428] and using the number keys to select the port.

5. If a Static IP is required for the intrusion Panel (DHCP by default); these options can be set via the DSC LCD Keypad interface within:

   - Ethernet IP Address: [*][8][installer code][851][001]
   - Ethernet IP Subnet Mask: [*][8][installer code][851][002]
   - Ethernet Gateway IP Address: [*][8][installer code][851][003]
   - Primary Ethernet DNS IP: [*][8][installer code][851][007]

6. Set Communication Delay to 60 seconds through DSC LCD Keypad interface using [*][8][installer code][377][002] and using the number keys to set the seconds to 60.

7. Set Alternate Communicator within the intrusion panel to Y (Yes) through DSC LCD Keypad interface using [*][8][installer code][382][5] and using the [*] key to set the value.

8. Several integration specific Toggle settings will need to be set in two seperate menus:

   a. Navigate to Session 1 Integration Toggle Options 2 through the DSC LCD Keypad interface using [*][8][installer code][851][425]. Option 3 (03 – Integration Over Ethernet) and option 5 (05 – Integration Protocol) will need to be set. To set these options, use the number keys by pressing 3 and 5; these options should be toggled ON. When completed, the LCD should show LCD should show "--3-5---".

   b. Navigate to Session 1 Integration Toggle Options 3 through the DSC LCD Keypad interface using [*][8][installer code][851][426]. Option 1 (01 – UDP Polling), option 3 (03 – Real-time Notification) and option 4 (04 – Notification Follows Pool) will need to be set. To set these options, use the number keys by pressing 1,3 and 4; these options should be toggled ON. When completed, the LCD should show LCD should show "1-34----".

9. Set or note down the Integration ID through the DSC LCD Keypad interface using [*][8][installer code][851][422]. Use the number keys to adjust the Integration ID if needed. You will need to scroll using the arrow keys to view the entire 12 digit value.

10. Set or note down the Integration Access Code through the DSC LCD Keypad interface using [*][8][installer code][851][423]. Use the number keys to adjust the Integration Access Code if needed. You will need to scroll using the arrow keys to view the entire 8 digit value. The default value is 12345678.

11. Set or note down the Installer Code through DSC LCD Keypad interface using [*][8][installer code][851][011]. Default Installer Code is 5555.

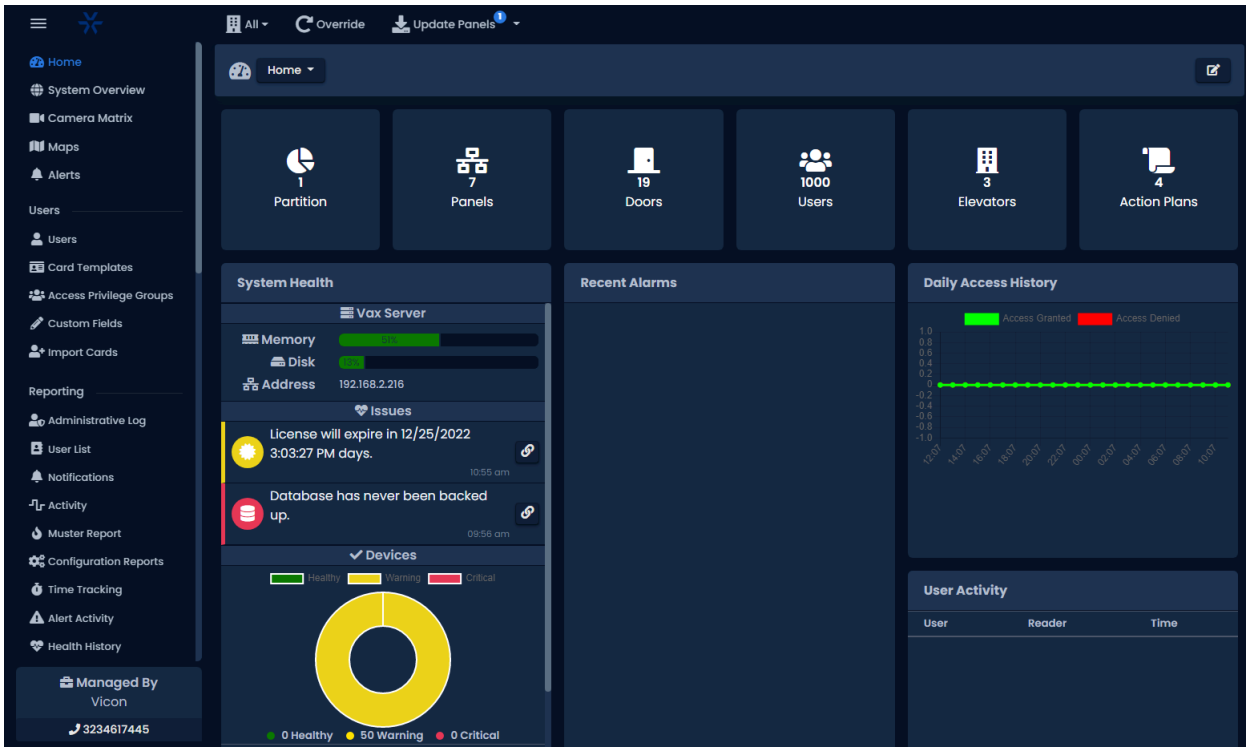
Chapter 39. Dashboard

VAX provides an extremely customizable dashboard that allows the user to have the **most important information** to their day-to-day operations displayed at the top of the homepage. Contents of the Dashboards also dynamically scales and re-adjusts based on the screen resolution of the device viewing it. The user can also save Dashboards as **profiles** that can be switched on the fly, allowing for quick access to any information they need. This chapter will cover the creation and customization of the Dashboards in depth with any and all relevant information for day-to-day operations

Introduction to Dashboards

By default when first installing **VAX**, the Dashboard will come pre-configured and can be seen from the homepage. This default configuration will likely be fine for most users as it provides **basic statistics, system health, recent alarms, User activity and Daily access history.** However some users may want to adjust the placement of these widgets, remove widgets or add more. This can be achieved using a simple **drag-and-drop interface** allowing the user to tailor the Dashboard to their needs and preferences.

Figure 39.1.



Creating Dashboards

To edit the Dashboard, the user will need to click the Edit button along the top of the screen next to the Panels status indicator. This will apply to whichever Dashboard is currently up. To create a Dashboard, select the dropdown bar along the top. By default, it will be marked as "Home". There will be an option to Create New;, click this to be brought to the creation page.

Right at the top, you can give the new Dashboard a name by clicking the box and inputting a name. From there, on the right side of the page will be the **Widget menu**. This section will go over what options and how these can be customized a bit later. To bring a widget onto the screen, just **click and drag** it to where it should be placed. While dragging it, there will be a dotted line indicating where the widget will end up, which can be adjusted after by dragging it elsewhere or by clicking the corner and

dragging it out to re-size it. To delete a widget, simply hit the edit button on the widget and choose the **Delete option**, or drag it into the garbage bin in the bottom right corner.

Figure 39.2.

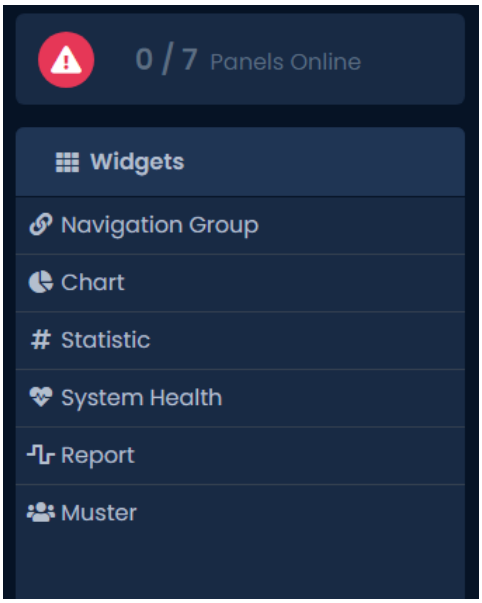


Figure 39.3.

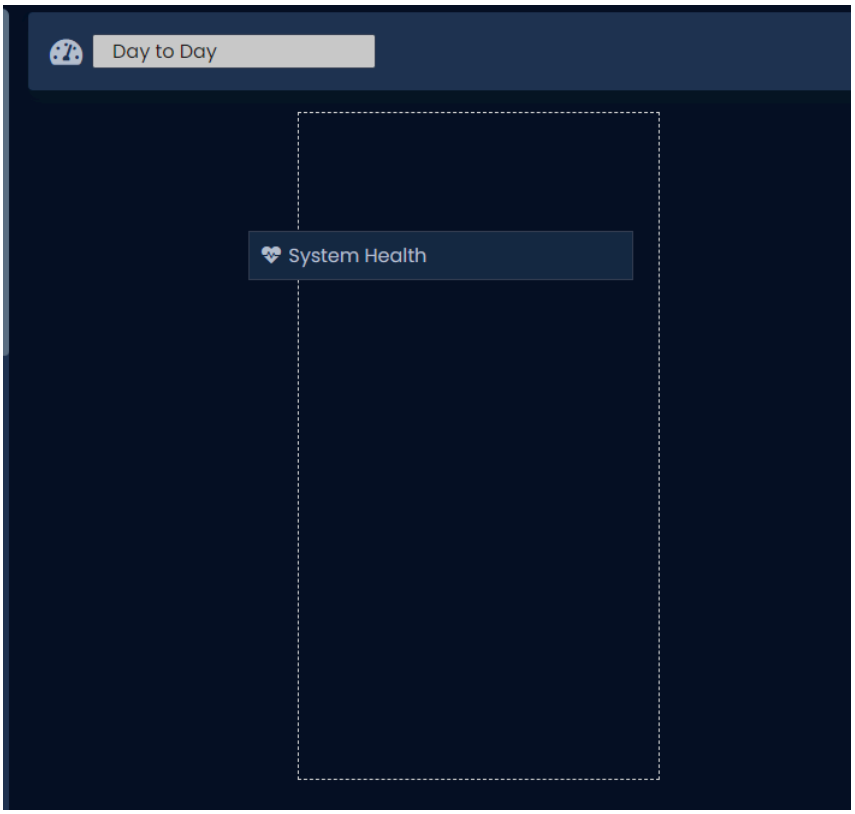


Table 39.1.

Widget	Description
Navigation Group	A customizable widget that allows you to create a shortcut button that links to another page internally or externally.

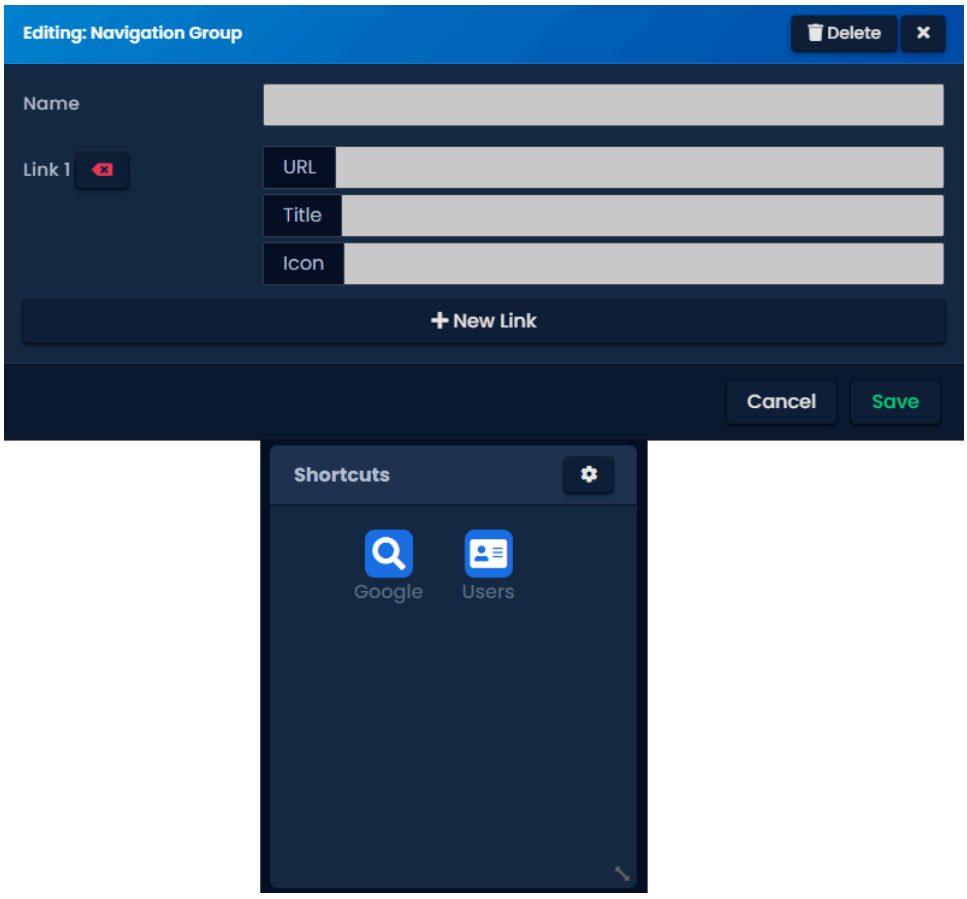
Widget	Description
Chart	A widget that allows the user to choose from multiple different charts that can display information from user-selected datasets.
Statistic	A widget that allows the user to place a small display of certain statistics for quick reference.
System Health	A customizable widget that allows the user a quick look at any Server or Panel related health issues.
Report	A widget that displays a report of the users choice with preset date ranges and notification-type specific filters.
Muster	A widget that displays a report of areas users are in and when they entered.

Navigation Group

Table 39.2. Statistic Widget

Option	Description
Name	Name of the widget
URL	Web address of the site/page you want to link to the button created by the widget
Title	Title for the URL
Icon	Links to an icon to use from the FA library. (Example fa-search.) To find the full library of options, please refer to the Font-Awesome library online.

Figure 39.4.



Chart

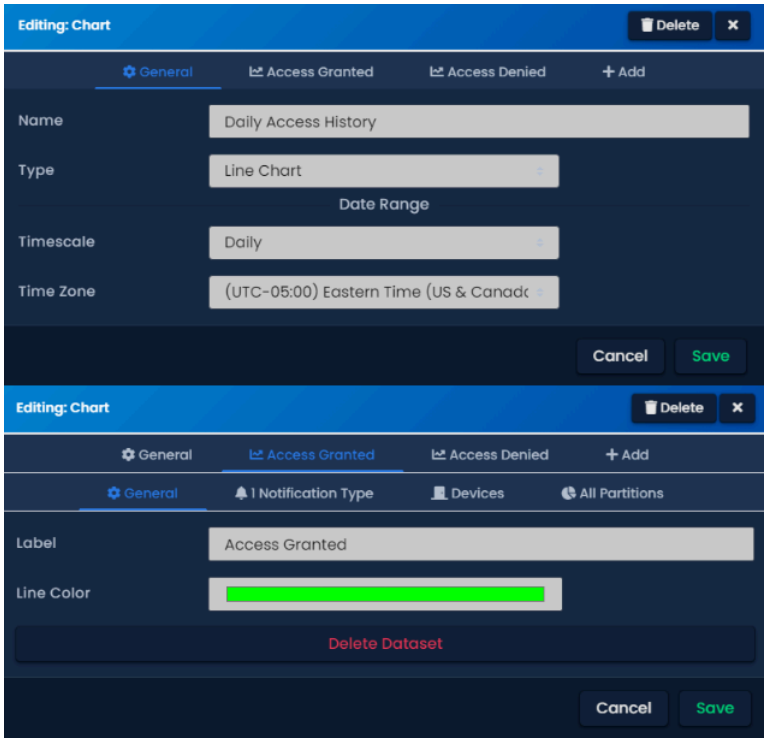
Table 39.3. Chart Widget General Tab

Option	Description
Name	Name of the widget.
Type	A drop down of chart types. This includes Vertical/Horizontal bar Chart, Line Chart and Bubble Chart.
Timescale	A drop down for pre-defined date windows to pull data from. This includes Hourly, Daily, Weekly, Monthly and Yearly.
Timezone	A drop down containing different timezones to choose from.

Table 39.4. Chart Widget Datasets Tab

Option	Description
General	A section that allows the user to name the label of the chart and the color of the line.
Notification Type	A list of notification types to draw from. You can only select one type of notification per dataset or else it will not work.
Devices	A list of device types to draw data and filter from.
Partition	A list of partitions to draw data and filter from.

Figure 39.5.



Statistic

Table 39.5. Statistic Widget

Option	Description
Users	Presents a numerical value for the number of users in the system.

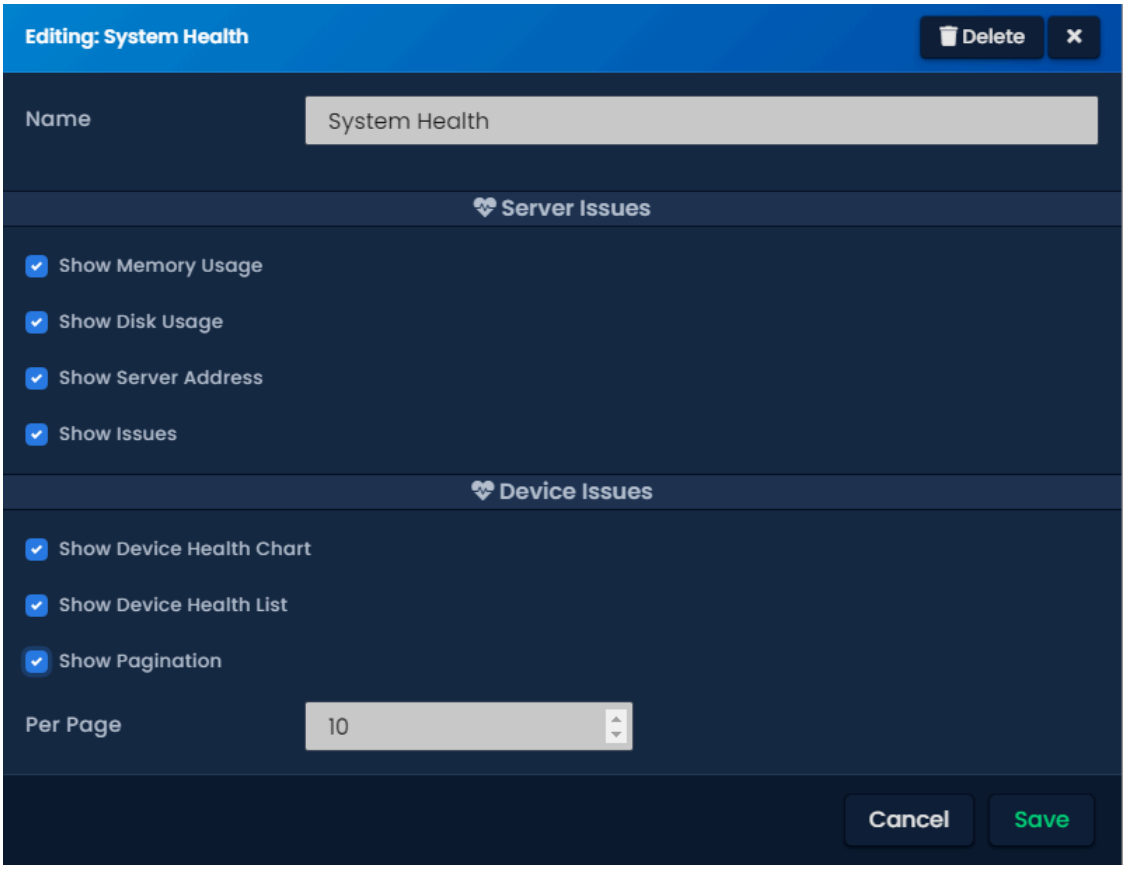
Option	Description
Partitions	Presents a numerical value for the number of partitions in the system.
Panels	Presents a numerical value for the number of panels in the system.
Doors	Presents a numerical value for the number of doors in the system.
Elevators	Presents a numerical value for the number of elevators in the system.
Action Plans	Presents a numerical value for the number of action plans in the system.
Cameras	Presents a numerical value for the number of cameras in the system.
Online Panels	Presents a numerical value for the number of online panels in the system.

System Health

Table 39.6.

Option	Description
Name	Name of the widget tile that is placed along the top of the widget.
Show Memory Usage	A server-related statistic to show current memory usage.
Show Disk Usage	A server-related statistic to show current disk usage.
Show Server Address	Lists the VAX server's current IP address.
Show Issues	Provides a list with timestamps of when server health issues are detected on the server. This includes backup status, offline devices, license expiry as well as any of the aforementioned options on this widget.
Show Device Health Chart	Presents a chart showing the percentage of devices status based on Healthy, Warning and Critical states.
Show Device Health List	Presents a list of devices and health issues they have.
Show Pagination	Adds a page counter at the bottom of the widget allowing the user to see a further back history of device health issues.

Figure 39.6.



Report

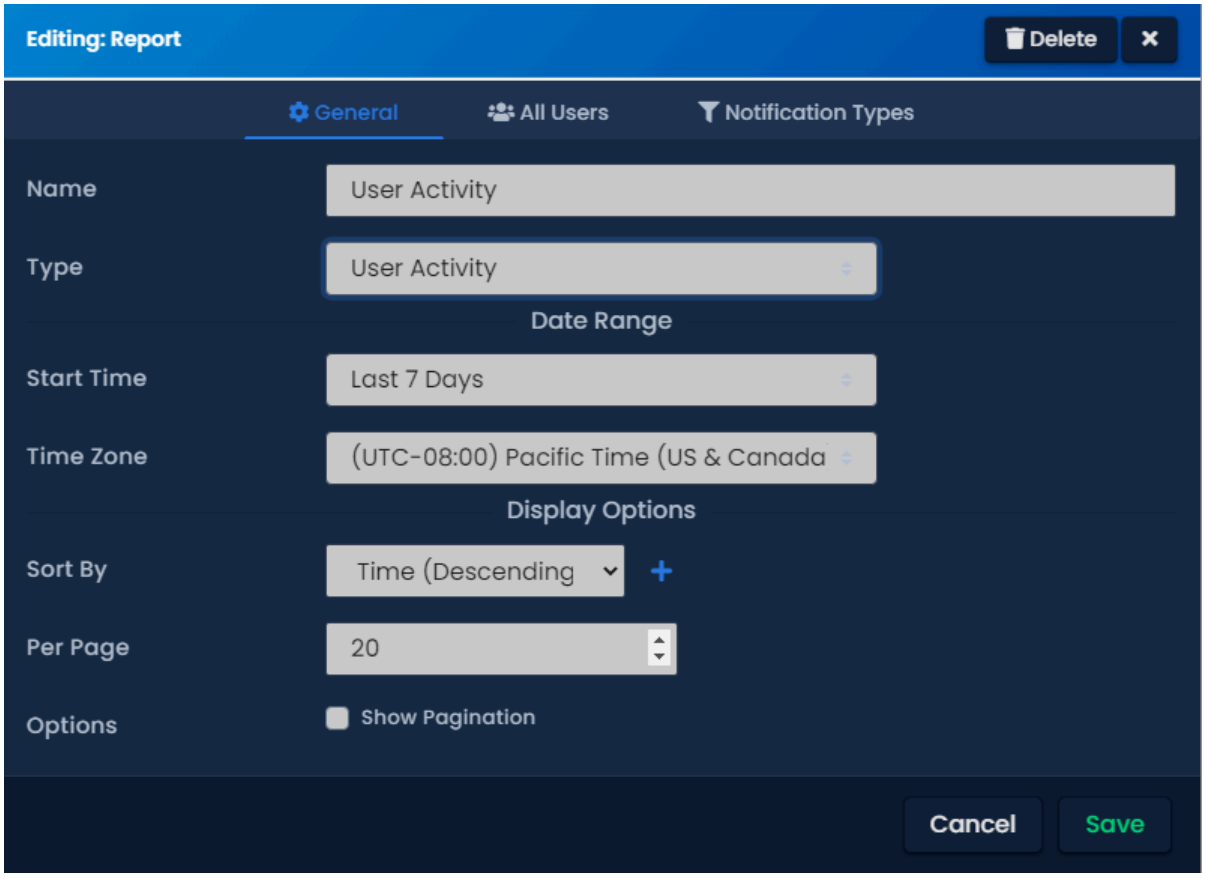
Reporting is one of the more in-depth options, so along with a table presenting some options, this section will go over a bit more detail. Some of the menus will be context sensitive to the type of report selected in terms of what notifications to filter by as well as what datasets will be selectable, such as doors, users, etc.

Table 39.7.

Option	Description
Door Activity Report	Provides a report of recent activity for doors. Can filter by notification type, doors and specify a date range from a drop down with pre-configured options. Also allows for sorting by time, door name, or reader name.
User Activity Report	Provides a report of recent activity for users. Can filter by notification type, user and specify a date range from a dropdown with pre-configured options. Also allows for sorting by time, name, sitecode or card number.
Floor Activity Report	Provides a report of recent activity for floors and elevators. Can filter by notification type, floor and specify a date range from a dropdown with pre-configured options. Also allows for sorting by time, floor name, reader name or elevator name.
Elevator Activity Report	Provides a report of recent activity for floors and elevators. Can filter by notification type, floor and specify a date range from a dropdown with pre-configured options. Also allows for sorting by time, floor name, reader name or elevator name.

Option	Description
Input Activity Report	Provides a report of recent activity for inputs. Can filter by notification type, input (Aux Only) and specify a date range from a dropdown with pre-configured options. Also allows for sorting by time and input name.
Output Activity Report	Provides a report of recent activity for outputs. Can filter by notification type, output (Aux Only) and specify a date range from a dropdown with pre-configured options. Also allows for sorting by time and output name.
Action Plan Activity Report	Provides a report of recent activity for action plans. Can filter by notification type, action plan and specify a date range from a dropdown with pre-configured options. Also allows for sorting by time and action plan name.
DSC Alarm Activity Report	Provides a report of recent activity with DSC Alarms integrated into VAX. Can filter by notification type, partition and specify a date range from a dropdown with pre-configured options. Also allows for sorting by time only.

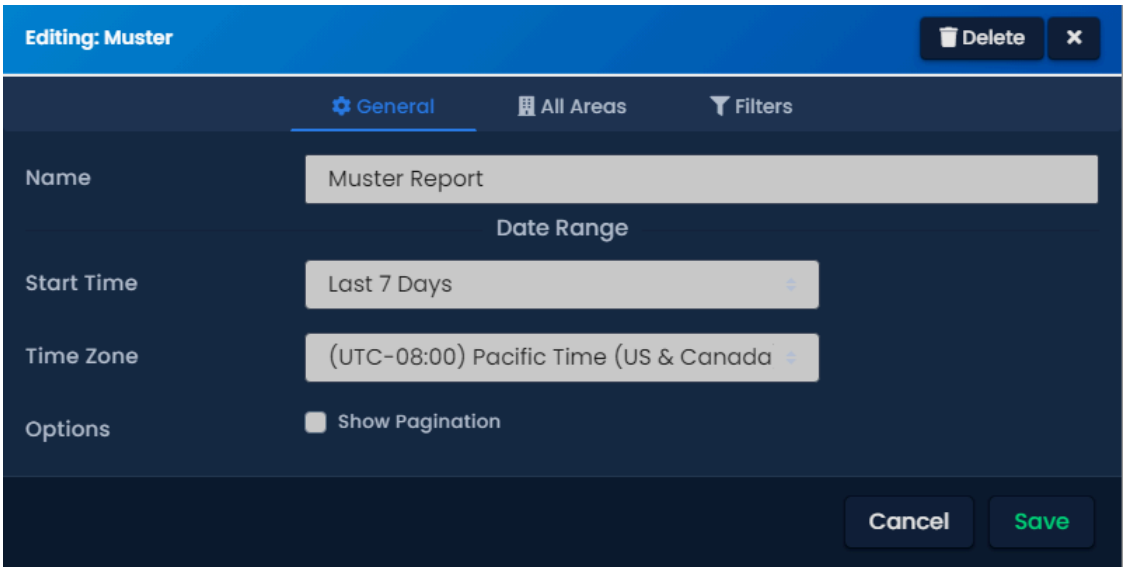
Figure 39.7.



Muster Report

Muster report is similar to the User Activity widget, but instead shows only the last reader a user scanned at. The user can also filter based off of a custom field and specific areas can be specified if desired. Similar to all the other widgets, there are options to pagination and setting the start time of the report from a dropdown list with pre-configured options.

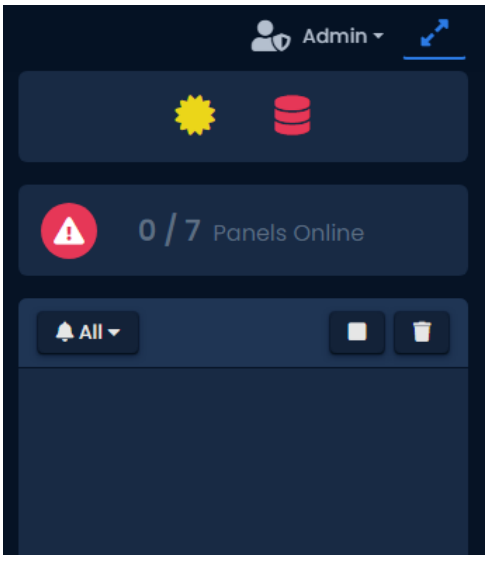
Figure 39.8.



Notification Side-Bar

This brief section will cover the **Panel Overview widget and the notification bar** along the right-side of the screen. Unlike the previous widgets, these are not drag-and-drop capable and will remain static on the side bar. Right at the top is our Panels overview. This will show the current live panel count and updates dynamically as panels connect or disconnect. Clicking on this will bring you to the System Overview page. You can read more about this page in the **System Overview section of the manual,** Chapter 18, *System Overview***.**

Figure 39.9.



Below the panel overview is the notification bar. This provides **live notifications** as they happen in the system. There are a few options here that can help either enhance the experience or provide important system information. Along the top of the notifications bar are three buttons. A drop-down for filtering notification types which can be modified via the Notification Settings. To the right of this are a pause/resume button for pausing the flow of notifications and a clear notification button. These can be useful for collecting necessary data/events for troubleshooting.

Finally along the bottom of the notification bar will be some icons along with the version of software. These icons represent active Warning-level or critical-level alerts. This provides a quick view of what may need to be resolved to ensure optimal system performance. The thresholds for these warnings can be configured under the Health Settings section of VAX.

Figure 39.10.

Chapter 40. Badge Printing

Badge Printing within VAX grants the Administrator the ability to print various designs on printable card credentials.

Badge Printing Overview

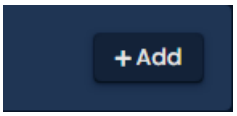
Badge printing can be found under the *Users* section and is labelled *Card Templates*. An unlimited amount of card templates can be created for Administrators to use. Card templates can be used for card holders across different partitions, but must reside in a single partition and can only be accessed by Administrators assigned to theat partition. Badge Printing includes the following features:

- Ability to design various templates for the front and back of cards.
- Print to any card printers available on the network.
- Templates separated by partition.
- Generate Barcodes and QR Codes of various card holder fields, which can then be printed on the cards.
- Download Card Designs as a PNG image.

New Card Editor

To begin designing, the Administrator will first need to navigate to the New Card editor found within Card Templates.

1. On the left side bar, click on *Card Templates*. The photo badging dashboard will now appear.



2. Click the + *Add* button located at the **top right of the page**.

3. Using the dropdown, select a partition for the card to reside in, then click *Create*.

Immediately present in the middle of the screen is a blank card, with icons to the right of the card. The editor is a drag and drop interface, where various shapes, tools, and information can be dragged onto the card, or dragged off the card to be deleted.

Note

To resize an element, the element must first be unselected. The Administrator may then hover over the element to resize it.

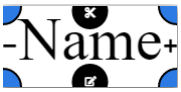
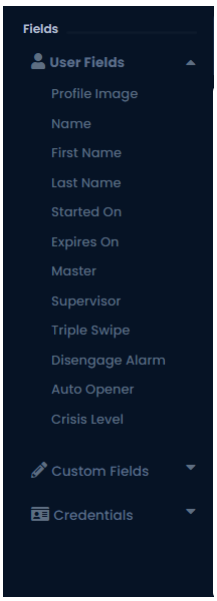


Figure 40.1. Card Holder Fields



On the left hand side (Figure 40.1), there is a menu that can be hidden or shown via the top left corner menu button. User information, Custom Fields, and Credential information can automatically be pulled from the software and printed on the card by dragging the corresponding element onto the card on screen. Examples include a card holder's profile image, name, card number, and any custom fields that may have been created and associated with the user.

Table 40.1. User Fields Options

User Field	Description
Profile Image	Grabs the profile picture of the card holder if applicable.
Name	Takes the full name of the card holder (both first and last name combined).
First Name	Takes only the first name of the card holder
Last Name	Takes only the last name of the card holder
Started On	Pulls the starts on property of the card holder.
Expires On	Pulls the expires on property of the card holder.
Master	Display if the card holder is a Master user.
Supervisor	Display if the card holder is a Supervisor.
Triple Swipe	Display if the card holder has the triple swipe permission enabled.
Disengage Alarm	Display if the card holder has permission to bypass and disengage alarms.
Auto Opener	Display if the card holder has permission to automatically fire the door opener on card swipe.
Crisis Level	Display the crisis level permission of the user.

Table 40.2. Custom Fields

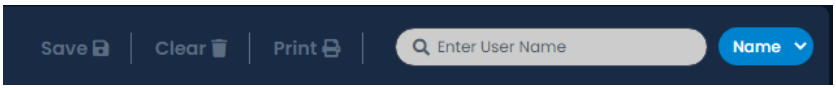
Custom Field	Description
Text Custom Fields	Display the text values of the selected custom field for a card holder.
Checkbox Custom Fields	Display the text value of the checkbox (true or false) for a card holder.
Dropdown Custom Fields	Display the text value of the selected dropdown element for a card holder.
Date Custom Fields	Displays the date custom field of a card holder, in the format specified. By default, it will display as *mm/dd/yyyy H:MM:SS AM*.

Table 40.3. Credential Fields

Credential Field	Description
Card Number	Display the card number of the card holder's credential.
Site Code	Display the Site code/Facility code of the card holder's credential.
Card Name	Display the name of the credential on the card.

Across the **top of the editor** are the various tabs, as VAX gives the Administrator the ability to have multiple cards open in different tabs to be edited or printed at the same time.

Just below that very top bar is the name of the template, along with buttons to save the template, clear it and start from scratch, print the card, or search users.



Searching can be done by *name* (first or last name) or *card number/pin credential*. After searching a user and selecting from the dropdown, the card template will update with their respective information so the Administrator may see a preview of how the card would look, as well as print the individual card immediately from the editor with the user information.

To the right of the card canvas is the Card, Tools, and Shapes menu. The Card options change the orientation of the card as well as which side of the card is currently selected to edit. The tools and shapes menus provide the following options:

Table 40.4. Tools Menu

Tools	Description
Image	Upload an image onto the card that may be moved and resized.
Background Image	Upload a static image to be used as the background of the card. Image will be stretched to fill the entire card.
Text Box	Places an editable text box to contain any text.
Color Fill	Fills the background with a specific color of choice, or using one of the preset background images.
Card Preview	Displays the card by itself. Click "Exit Card Preview" to edit the card further.
Download Canvas	Downloads the current card canvas and side as a single JPEG image.
QR Code	Generate a QR code to be placed onto the card with information containing the card holder's *User Fields, Custom Fields, or Credential* information. Only 1 field may be selected and generated per QR code.
Barcode	Generate a Bar code to be placed onto the card with information containing the card holder's *User Fields, Custom Fields, or Credential* information. Only 1 field may be selected and generated per Bar code.

Table 40.5. Shapes Menu

Shapes	Description
Line	Place a single a solid line on the card.
Square	Places a solid fill square onto the card.
Circle	Places a solid fill circle onto the card.
Star	Places a solid fill star onto the card.

Shapes	Description
Rectangle	Places a solid fill rectangle onto the card that may be resized in varying degrees.
Heart	Places a solid fill heart shaped object onto the card.
Diamond	Places a solid fill diamond object onto the card.
Triangle	Places a solid fill triangle object onto the card.
Infinity Symbol	Places an infinity symbol object onto the card.
Plus Symbol	Places a plus symbol object onto the card.
Certificate	Places a certificate object onto the card.
Chat Bubble	Places a solid fill chat bubble shape onto the card

Each element has a set of properties that are very similar across similar elements. Below is a table of the various properties for each element.

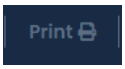
Table 40.6. Field Properties Table

Property Type	Description
Image Properties	• **Blur** - Adjust the slider/text box to increase the overall blur of the image. Values between 0 - 5 for intensity of the blur. • **Brightness** - Adjust the slider/text box to increase or decrease the brightness of the image. Values between 0 - 200. • **Contrast** - Adjust the slider/text box to increase or decrease the contrast of the image. Values between 0 - 200. • **GrayScale** - Adjust the slider/text box to decrease the amount of color in the image. Values between 0 - 100. • **Invert** - Adjust the slider/text box to invert the colors of the image. Values between 0 - 100. • **Opacity** - Adjust the slider/text box to change the transparency of the image. Values between 0 - 100. • **Saturate** - Adjust the slider/text box to increase or decrease the saturation of the colors of the image. Values between 0 - 200. • **Sepia** - Adjust the slider/text box to increase the sepia filter and make the picture warmer. Values between 0 - 100. • **Default Properties** - Reset all values to their defaults.
Text Properties	• **Bold** - Checkbox to make the entire name bold. • **Italics** - Checkbox to set name in italics. • **Underline** - Checkbox to underline the entire name field.

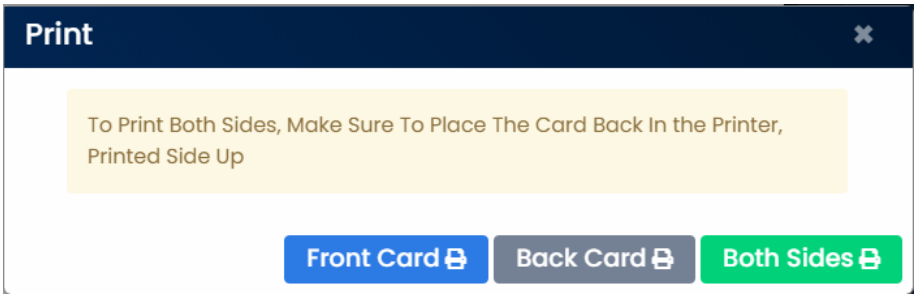
Property Type	Description
	• **Strike Through** - Checkbox to apply a line from left to right across the entire name field. • **Text Size** - Adjustable slider/text box to increase or decrease the size of the text. Values between 0 - 300. • **Text Color** - Change the color of the text, using RGB values or selecting from the configurable palette. • **Opacity** - Adjust the slider/text box to change the transparency of the image. Values between 0 - 100. • **Shadow** - Add a shadow effect on the card.
Shape Properties	• **Blur** - Adjust the slider/text box to increase the overall blur of the image. Values between 0 - 5 for intensity of the blur. • **Brightness** - Adjust the slider/text box to increase or decrease the brightness of the image. Values between 0 - 200. • **Contrast** - Adjust the slider/text box to increase or decrease the contrast of the image. Values between 0 - 200. • **GrayScale** - Adjust the slider/text box to decrease the amount of color in the image. Values between 0 - 100. • **Invert** - Adjust the slider/text box to invert the colors of the image. Values between 0 - 100. • **Opacity** - Adjust the slider/text box to change the transparency of the image. Values between 0 - 100. • **Saturate** - Adjust the slider/text box to increase or decrease the saturation of the colors of the image. Values between 0 - 200. • **Sepia** - Adjust the slider/text box to increase the sepia filter and make the picture warmer. Values between 0 - 100. • **Default Properties** - Reset all values to their defaults.

Printing a Card

Printing to card printers within VAX can be done through the New Card editor or the individual Edit User pages. Navigate to the edit user page and click on the Credentials tab. Beside the credential will be a printer icon. Click on this icon to open the Card Templates pop up, where the available saved templates will now appear. Select the template to use for front or back. The printer options will now appear.



Printing from the card editor will display a pop up where the Administrator can select to print the front, back, or both sides of the card. A printer can then be selected as the destination.



Chapter 41. Schlage Integration

Allegion Schlage wireless locksets can be integrated with VAX. After the initial setup, there will be very little difference between the functionality of a Schlage lockset when compared to a typical managed door in the VAX software.

Note

The Schlage Server for VAX to communicate with the gateway will need to be added on install. If VAX is already installed without the Schlage Server added, VAX will need to be uninstalled and reinstalled. *Uninstalling and Reinstalling will not wipe the database and is safe to perform to add the additional Schlage service.*

Note

Lockset add-on must be purchased on the license from **Obsidian** for the locks to link to the system.

Schlage Overview

VAX is able to integrate with Schlage wireless locksets through the ENGAGE Gateway.

- View status of Alarm Partitions and Alarm Zones
- Arm (Stay Arm, Away Arm, Night Arm) and disarm through the VAX web interface, Mobile app, Action Plans or through the VAX API
- Bypass zones, contact emergency services, silence trouble beeping

There are 3 external components to integrate Schlage Locksets with VAX:

- ENGAGE Gateway - acts as a "Panel" within VAX
- Schlage Lockset - acts as a "Door" within VAX
- Allegion ENGAGE - to register app and devices to a Schlage System

Allegion ENGAGE App

The Allegion ENGAGE phone application is used to connect Schlage locksets to a Schlage gateway. An Allegion account is required to begin adding locksets and gateways to a site.

1. The **Allegion ENGAGE** app can be downloaded from the Google Play Store for Android devices or the Apple App Store for Apple devices.

Adding an ENGAGE Site

1. In the left sidebar menu, locate and click on Engage Sites found under the HARDWARE section.
2. Click Add to create a new Engage site.
3. Provide a name to the Engage site. Select the Partition and Site in VAX which the Engage site will reside in.

Note

Any future devices added to this Engage Site will be added to the Partition and Site selected in VAX.

4. Enter the email and password credentials for an Engage account, then click Create New Engage Site. If proper credentials were entered, the Engage Site will be added successfully. Otherwise, re-enter the credentials and click the Create button again.

5. Verify the site exists by opening the Allegion ENGAGE app on a mobile device and view sites.

Connecting an ENGAGE Gateway to the App

1. Power on the Gateway.

2. Take note of the Gateway Serial Number. This can be found on the bottom side of the Gateway.

3. Factory Reset the Gateway. Refer to the Gateway manual for instructions on how to reset (typically a button on the backside).

4. Within the Allegion ENGAGE Mobile app, select the Engage site created previously and tap "Select". This will open the Devices page.

5. Tap the + button located on the bottom right of the screen to add a device.

6. From the list, select Gateway to add the ENGAGE Gateway. The following page will then show a list of all nearby gateways ready to connect, differentiated by serial numbers.

7. Select the Gateway with the serial number as noted earlier to add it.

8. Give the Gateway a name and select Next.

9. Select IP as the Gateway Communication Mode and click Next.

10. Toggle "IP Behind Firewall" to ON and select DHCP for the IP settings. Click Next.

11. The Server address will now look for your Schlage server settings configured during initial install (Advanced). Set the following parameters:

Table 41.1. Gateway Parameters

Server URL	https://<*your server address*>:7111/engage_wss
CA Server URL	http://<*Your server address*>:7110/engage/newCA/current
Keep Alive (in seconds)	300

The device will then begin connecting and will notify once completed.

12. There are 2 methods to adding the Gateway into VAX once it has been added to the ENGAGE site.

    - Under Unknown Panels, the Gateway will appear with its serial number as the MAC address.

    - When in the Engage Sites edit page, navigate to the Gateways tab and click the Sync button.

13. The Gateway will now appear under Panels and the Administrator can now edit it from the Panels page or Edit Engage Sites page.

Adding a Schlage Lockset to VAX

1. The Lockset will require batteries. Makes sure that new or fully charged batteries are installed in the Lockset. A credential presentation to the Lockset reader will respond if there is sufficient power provided.

Note

Typically AA batteries are used in Locksets. Please refer to the Lockset Manual for recommended battery type.

2. On the **Allegion ENGAGE** app, select the ENGAGE site in use and select the + button.
3. On the Device Type selection screen, select ND if the Lockset is the NDE Series or select LE if the Lockset is the LE Series.
4. Complete adding the Lockset device to the ENGAGE site by following the remaining instructions on the app. The wifi section can be skipped.
5. From VAX, Under the **Hardware** section on the side bar, select **Engage Sites**. Select the Engage site that the device was added to. Select the **Devices** tab and select the Sync button. The new Lockset should be seen in the **Locks** tab.

Adding Lockset to a Door

1. From VAX, under the **Hardware** section on the side bar, select **Engage Sites**.
2. Edit the Engage site where the Lockset was added. Select the **Gateway** tab and select the edit Gateway button.
3. Select the **Doors** tab and select the **+ Add New Doors** button. This will cause the Gateway to scan for all available Locksets nearby.

Note

The scan can take up to 30 seconds, also might take a few attempts. If the lock is too far from the selected Gateway, a closer gateway may have to be selected from previous steps.

4. After the scan, select the **Add** button on the required Lockset.
5. The Schlage Lockset is now added as a door in the VAX System

Note

If a lock needs to be changed to a different gateway in the same Engage site, the Door can be Unlinked from the Gateway on the Edit Gateway page under the Linked Locks tab on the Locks tab.

Caution

If a lock needs to change Engage Sites, then the lock must be deleted from the Engage Site, factory reset and then added to a different Engage Site.

Schlage Override and Monitoring

Schlage wireless locksets can be treated as a Door within VAX. Refer to the Doors Overrides and Monitoring section for information on how to override or monitor the status of the locksets.

Troubleshooting Schlage

A total of 10 ENGAGE enabled devices allowed per gateway.

Gateway communication range to locks is from 30' to 50' in ideal location

Make sure to not link devices in the app. The app is just for adding the lockset and gateway.

App showing no devices found. Hold the reset button until the device turns green.

Power cycle the gateway if issues continue to persist with connecting in the app.

Chapter 42. Health Monitoring in VAX

This chapter will cover the fundamentals of **Health Monitoring Systems** in VAX, and explain how to use the tools available to maintain the health of the VAX system.

Introduction to Health Monitoring

It is important to understand how to maintain an VAX system. The VAX Reporting tools allow Administrators to look back at events the VAX system has handled and the history of the system. The health of the VAX system can be monitored using the tools in **Health History** and maintained using the different **Health Settings** selections. Settings allow Administrators to set notifications or logs to appear when an event occurs, notifying them in real time.

Health History is a reporting tool that allows the Administrator to view events related to the health and upkeep of the system. **Health Settings** is a settings section that contains a list of events related to the health of the VAX system that can be monitored and set to notify Administrators on occurrence. The **Health History** tool gathers logs on the Health Status of the VAX system between a start time and end time. These logs may be further filtered by Health Issues and the severity or nature of the log such as Healthy, Warning, and Critical levels. Below **Health Settings** are options to display Icons, Logs, and Notifications when an event related to the health of the VAX system activates an action, including new software versions, uninstalled panels, low battery on devices, and more. The next section will go over the **Health History** tools of VAX.

Health History

The Health History section of Reporting contains options to run reports on the health and status of the VAX system. As a type of Report this tool runs a report to compile a list of events the VAX system has handled. This chapter will explain its features and tools and how to use these tools to narrow the reports search for customizable results.

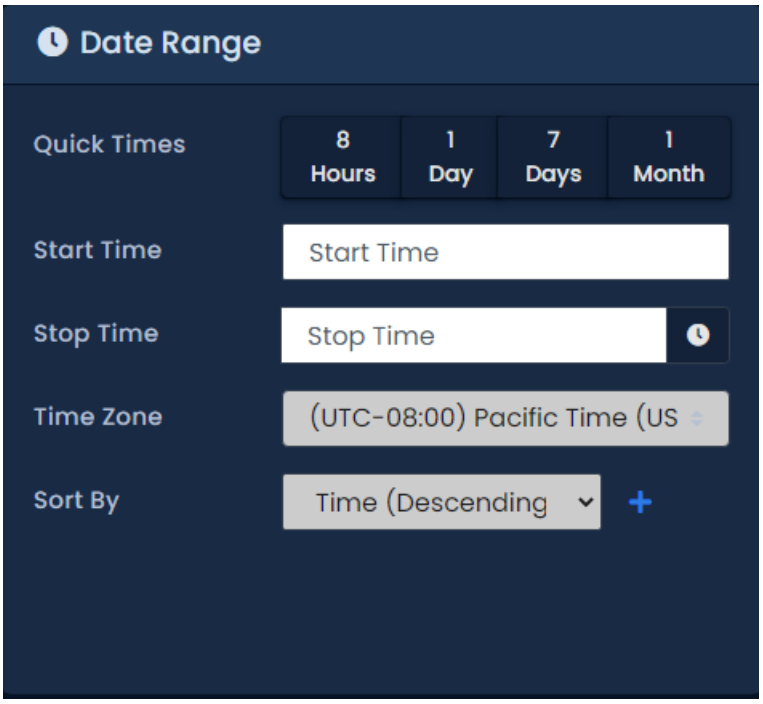
Figure 42.1. Health History Icon

Health History Tools

Health History: Date Range

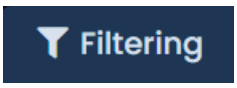
Health History, found under the Reporting section of the toolbar, displays reports on the health of the VAX system. This feature allows Administrators to pick a start time and date and end time and date to filter notifications. The times are set by using the calendar tool to help set these quickly. The system will then compile all logs created between the times set that match a list of filter specifications selected. There are Quick Time options that allow for selection of 8 hours, 1 Day, 7 Days, and 1 Month without manual setup. Administrators can choose a Sort By method which orders the logs by Ascending or Descending, by occurrence. There is a Time Zone selector that can calibrate the timestamps to different time zones.

Figure 42.2. Health History Icon



Filtering

Figure 42.3. Filtering Icon



There are filter selections by Health Issues and the Status of the issue. These Health Issues are tracked automatically by VAX and filter Health Issues to narrow the selection and eliminate unselected issues from the report list. If no issues are selected VAX will include all Issues by default. Filter options for Health Issues include:

1. Low Disk Space
2. Low Memory
3. New Version
4. License Expiry
5. Database Backup
6. Database Size
7. LDAP Conflicts
8. Uninstalled Panels
9. Device Disconnected
10. New Device Firmware
11. Device Tampered

12.Device Low Battery

Some of these issues are as simple as logging if software updated to a new version, while others, like Low Memory or Device Low Battery, are monitored and will report on their changes.

Low Disk Space

The Low Disk Space option toggles selection of the log of the value monitored by the **Health History** reporting system. Selecting the Low Disk Space option will narrow the report list to include Low Disk Space logs. The system will show a Low Disk Space Log when the disk the VAX system is installed on reaches a threshold percent of remaining disk space. This threshold value can be set and changed in Health Settings. A threshold can be set for Warning and Critical Levels and the VAX will display the appropriate Level and the percent disk space remaining. The default disk space remaining for Warning Level is 70% and for Critical is 90%.

Low Memory

The Low Memory option toggles selection of the log of the value monitored by the **Health History** reporting system. When the system is using a high percentage of the Memory available to the system a logs is created. By default the Warning Level will notify when 70% or more of Memory is used and Critical Level is 90% or more. These values can be changed in Health Settings.

New Version

The New Version option toggles selection of the logs monitoring the availability of a New Version of software. The system will create a log based on number of days since release. The default for Warning Level is 0 days. These values can be changed in Health Settings.

License Expiry

The License Expiry option toggles selection of the logs monitoring the expiration of the license of the VAX system. The system will log a Warning Level when there is a number of days remaining until Expiry. The default number of days is 0. These values can be changed in Health Settings.

Database Backup

The Database Backup option toggles selection of the logs monitoring the days since a backup was performed. By default, the system will log a Warning Level when the days since a Backup has reached 75 days. The Critical Level is 80 days since Backup. These values can be changed in Health Settings.

Database Size

The Database Size option toggles selection of the logs monitoring the size of the database of the VAX system. By default, the Warning Level will log a Warning when the Database reaches 1% and will continue notifying weekly on the growth of the system. By default, the Critical Level is set to 90% of database size. These values can be changed in Health Settings.

LDAP Conflicts

LDAP Conflicts option toggles selection of the logs monitoring system LDAP Conflicts. VAX will create a log after a number of hours since the last conflict occurred. By default, the Warning Level is set to 0 hours after a conflict. Critical Level is set to 0 hours by default. These values can be changed in Health Settings.

Uninstalled Panels

Uninstalled Panels option toggles selection of the logs monitoring the status of panels. The VAX system will create a log after a number of panels is uninstalled. By default, the Warning Level will create a log if more than 0 panels become uninstalled. These values can be changed in Health Settings.

Device Disconnected

Device Disconnected option toggles selection of the logs monitoring the amount of devices that become disconnected. The VAX system will create a log after greater than 1% of devices have been disconnected.

New Device Firmware

New Device Firmware option toggles selection of the logs monitoring the release of a new firmware for the devices connected to the VAX system. By default the system will create a log if greater than 0% of devices have an available firmware update. These values can be changed in Health Settings.

Device Tampered

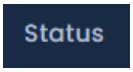
Device Tampered option toggles selection of the logs monitoring the tampering of devices. By default, if greater than 0% of devices have been tampered the Warning Level will create a log. These values can be changed in Health Settings.

Device Low Battery

Device Low Battery option toggles selection of the logs monitoring the battery level of wireless devices. By default, the system creates a log if greater than 0% of batteries reaches 0%. These values can be changed in Health Settings.

Status

Figure 42.4. Status Icon

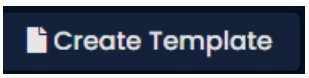


Next are different options to filter the logs by Status and severity. These Status types can filter by positive health changes and negative changes by the following selections:

1. Any
2. Healthy
3. Warning
4. Critical

Use a combination of the Filters, Statuses, and date range options to narrow the search to specific issue(s), type of status, and time or dates of occurrence. There is also a button to save these filtered searches as a template that can be called on for repeated use, altered and resaved in the future or saved as a new template. Formatting options include CSV and HTML. After running a **Health History** Report there is a Back to Configuration button, a Refresh Report button, and an Export button. The Export button will provide two options, CSV or HTML. CSV file can be downloaded and opened in spreadsheet and text editor programs like Microsoft Excel or Notepad. The HTML files can be downloaded and opened in an HTML browser to view in a new window. Arrows on the top and bottom of the results can be used to progress to the next page to view more logs.

Figure 42.5. Template Icon



Health Settings

Figure 42.6. Health Settings Icon

The **Health Settings** in the Administration section is a tool to turn notifications on for events related to the health of the system. The different Health Settings and their uses will be discussed in this chapter.

Introduction to Health Settings

Health Settings can be found by navigating to the Administration section on the task bar. This tool allows the user to select an Action to take in the event that there is a change to the value the **Health Settings** is monitoring.

Actions

Figure 42.7. Actions Icon

Any number of the actions can be selected to occur for each event that the **Health Settings** can monitor. After selecting a Health Setting to work under, multiple actions can be selected for each Health Setting by selecting each action's checkbox . These actions can be deselected by unchecking the box. These Actions include:

1. Show Icon
2. Log Issue
3. Notify System Admins via Email
4. Notify Dealer via Email
5. Notify System Admins via Web Push

Notify Frequency

The Notify Frequency format allows an input number equaling a selection of Hours, Days, Weeks, or Months between notifications. The user can dictate an increase or decrease in Warning Level based upon a value Administrators can set for each **Health Settings** type. The Administrator can also change the Notify Frequency value to increase or decrease the time between notifications sent during the active Warning Level for a **Health Setting**. For example, "1" days after a New Version release set Warning Level to 1. During this period Administrators can perform the actions "Log Issue" every "12" hours until the warning level changes. After "7" days after release the Warning Level increases to Warning Level 2/Critical Level, changing Action types to "Show Icon", and/or "Notify Dealer via Email", and changing the Notify Frequency to every "2" hours based on the settings made under Warning Level 2/Critical Level section for that **Health Setting**.

Warning Levels

Figure 42.8. Warning Level Icon

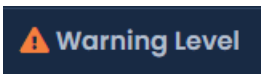
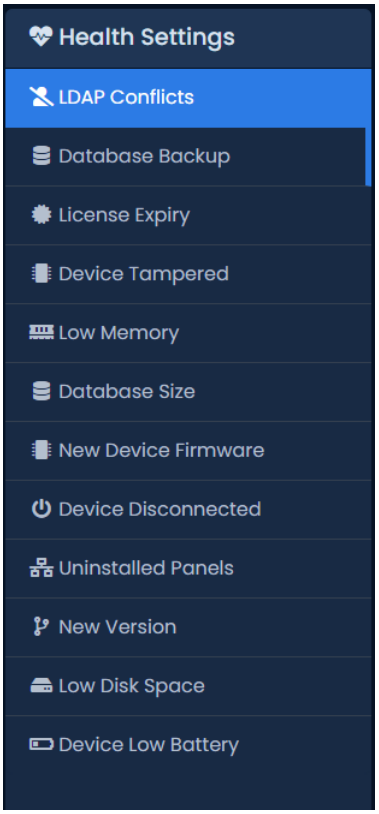


Figure 42.9. Critical Level Icon

Each of these **Health Settings** can be Enabled by selecting the Enable checkbox at the top of each **Health Settings** page. By default these settings are Enabled. Each **Health Settings** has a different event observed and a threshold value that will trigger a change in Warning Level if reached. For each Warning Level any number of Actions and the frequency of the notifications can be assigned and changed. Setting this threshold value will determine when the action(s) will be taken. Actions can be assigned to activate if the Warning Level changes. During the time the Warning Level is active the actions will activate as frequently as designated by the Notify Frequency selection. Up to two Warning Levels can be assigned for each **Health Settings**. If the second threshold is reached, the Warning Level changes and the second set of Actions and Notify Frequency settings override the previous Warning Level. The Critical Level can be set with increasing, decreasing, or equal Action and Notification Frequency parameters.

Health Settings: Options

Figure 42.10. Health Settings



This section will go over the different types of health settings and what each of the settings monitors. The **Health Settings** that can be set to trigger actions include:

1. Device Tampered
2. License Expiry
3. Device Disconnected
4. Uninstalled Panels
5. Database Size

6. New Version
7. New Device Firmware
8. Device Low Battery
9. Database Backup
10. Low Memory
11. Low Disk Space
12. LDAP Conflicts

Low Disk Space

When the disk the VAX system is installed on reaches a threshold percent of remaining disk space. This threshold value can be set and changed in **Health Settings**. The default disk space remaining for Warning Level is 70% and for Critical is 90%.

Low Memory

When the system is using a high percentage of the Memory available to the system a log is created. By default the Warning Level will notify when 70% or more of Memory is used and Critical Level is 90% or more.

New Version

The system will create a log based on number of days since release. The default for Warning Level is 0 days. These values can be changed in Health Settings.

License Expiry

The system will log a Warning Level when there is a number of days remaining until Expiry. The default amount of days is 0. These values can be changed in Health Settings.

Database Backup

Database Backup logs the days since a backup was performed. By default, the system will log a Warning Level when the days since a Backup has reached 75 days. The Critical Level is 80 days since Backup. These values can be changed in Health Settings.

Database Size

Database Size logs the size of the database of the VAX system. By default, the Warning Level will log a Warning when the Database reaches 1% and will continue notifying weekly on the growth of the system. By default, the Critical Level is set to 90% of database size.

LDAP Conflicts

LDAP Conflicts logs the system's LDAP Conflicts. VAX will create a log after an number of hours since the last conflict occurred.

Uninstalled Panels

Uninstalled Panels monitors the connection status of panels. The VAX system will create a log after a number of panels is uninstalled.

Device Disconnected

Device Disconnected monitors the number of devices that become disconnected.

New Device Firmware

New Device Firmware monitors the release of a new firmware for the devices connected to the VAX system. These values can be changed in Health Settings.

Device Tampered

Device Tampered monitors the tampering of devices.

Device Low Battery

Device Low Battery option monitors the battery level of wireless devices.

Conclusion

The health of the VAX system is important to understand and maintain; knowing that your system is updated, backed up, has sufficient storage space, and battery power can all be vital things to monitor when maintaining and troubleshooting the VAX system. Combine using the **Health Settings** and **Health History** tools to stay informed about the history and current health of the VAX system. This allows Administrators to look back to troubleshoot problems and view the status updates of the system as it happen in real time.

Chapter 43. Troubleshooting in VAX

Sometimes an installation goes wrong, or files are missing or corrupted. Communications are not connecting, Inputs and Outputs are not responding correctly, and cards return Access Denied when they shouldn't. This chapter will cover how to troubleshoot common problems to find a solution.

Common Tools: Panel LED Menus

Some important information about panel troubleshooting: Using the LED on the panel we can access an Edit menu and a Read Only menu. Below are instructions how to use these menus.

To access the Edit menu on the panel LED:

1. Press and hold the [Enter] button
2. Enter the panel password;, by default it is 0000
3. Press [ESC] to enter the password
4. Scroll up and down using the white buttons (SW1, SW2)
5. Press [Enter] to select a mode to change/view
6. Use the white buttons to scroll between options
7. Press [ESC] to exit Edit Mode

The Read Only menu on the panel LED:

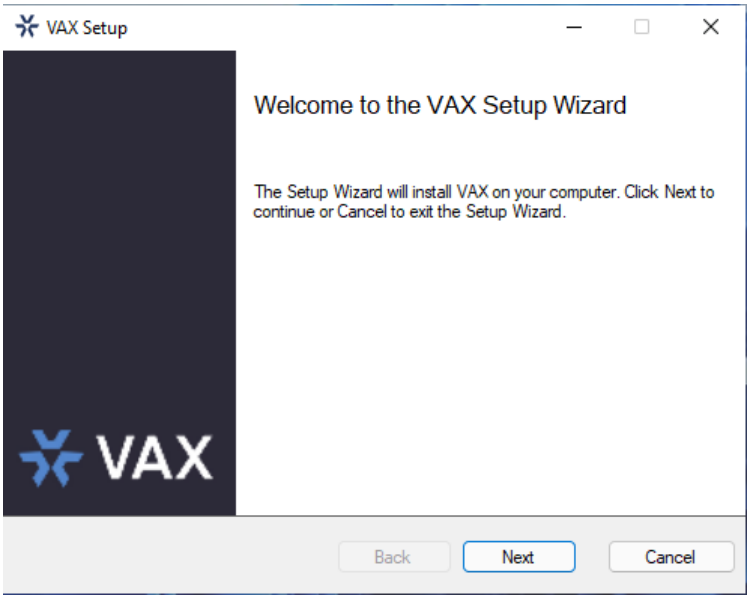
1. Press and hold the [ESC] button
2. Scroll up and down using the white buttons to view (SW1, SW2)
3. Press [ESC] to exit Read Only

These menus are useful for troubleshooting panels, connectivity, and finding information about your panel. Please refer to Chapter 3, *Initial Configuration* for more information and images.

Troubleshooting the Installer

The Install process can take a few steps to complete, and in each step something can go wrong. This section will cover common issues with installation and how to troubleshoot to find the problem and resolve it.

Figure 43.1. VAX Application Installer



Important Note

When upgrading or migrating to a new server please be sure to read the notes of the installer carefully. In some instances installing the newest version can cause damage if the versions are incompatible. Please remember to check if the version of VAX installed on the server and the upgrade or migration version of VAX are compatible. There are also cases where SQL server versions are incompatible with another SQL version. Remember to carefully read the notes of the installer for information on this, refer to the User Guide, or call our Support line for help when upgrading or migrating.

Unsupported Opperating Systems and Prerequisites

The VAX system requires a modern PC running at minimum Microsoft Windows 10, Microsoft Windows Server 2016. Windows 10/11 or Windows Server 2019 is recommended for optimal performance. Please see Chapter 1:
<Getting_started>Getting Started</Getting_started>
and Chapter 3:
<Initial_config>Initial Config</Initial_config>
for a list of system requirements and supported operating systems.

Unsupported operating systems or devices that do not have all the system requirements may be incompatible with VAX; consider upgrading to a supported device. Use the "About Your PC" tool in Windows Settings to find a device's specifications.

Setup Tool

Running the VAX Setup tool allows for changes to be made to the system, to remove a system and repair a system. If an error message displays stating there are missing or lost files, running a repair can find and replace some of the lost files. In some cases removing and reinstalling VAX will solve the issue. It is important to run a backup before repairing or reinstalling so there is a copy of the SQL database. When reinstalling/upgrading, 'test' the default path for the SQL server or the custom pathway to the SQL server before reinstalling or upgrading.

SQL Server Troubleshooting

Multiple instances of SQL can run on a single machine. SQL server 2008, 2012, and 2019 can all run concurrently on the same machine. When installing VAX a prompt to install a SQL server will

appear if one is not already present. The default name and placement of this folder is recommended. If regular backups are set up after install, and there is a lost database, a backup can be restored using the System Manager tool. Additionally, when reinstalling or upgrading, there is an option to test for the SQL server pathway to find an existing SQL server.

Cannot Install/Uninstall VAX - Error 1316 The Specified Account Already Exists

Cause: This is typically caused by corrupt registry keys.

Solution: Remove VAX within Regedit, then install 3.1 and choose "Repair".

1. Open the Registry Editor.
2. Navigate to Computer > HKEY_LOCAL_MACHINE > SOFTWARE > WOW6432Node.
3. Search for Vicon.
4. Right click on "Vicon" and Delete.
5. Download the VAX installation file (same version is recommended).
6. Run the installer.
7. Follow the prompts. *May only give the repair option. Select Repair if there is no option for a new install*

Windows 11 SQL Install Guide for NVME Drives

When installing SQL of any version on a Windows 11 machine, there is a chance the installation will not work under normal circumstances. This is due to Microsoft no longer emulating the hard drive sector setting “PhysicalBytesPerSectorForAtomicity” as 4096(4kb).

It is a known issue with NVME drives that it will no longer emulate this and instead set it to whatever the manufacturer has on board, in some cases 16kb-32kb. There are two ways to handle this:

1. Downgrade to Windows 10
2. Run the following commands in an elevated Command Prompt window to force an emulation registry level of 4kb
   - REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\stornvme\Parameters\Device" /v "ForcedPhysicalSectorSizeInBytes" /t REG_MULTI_SZ /d "* 4095" /f
   - REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\stornvme\Parameters\Device" /v "ForcedPhysicalSectorSizeInBytes" /t REG_MULTI_SZ /d "* 4095" /f

Run this command as well in Command prompt to check what it is currently running;, a restart is required for this to take effect visually and functionally.

- “fsutil fsinfo sectorinfo C:”

The response should be 4096 or lower after running those commands.

Source:

<Source> https://docs.microsoft.com/en-us/troubleshoot/sql/admin/troubleshoot-os-4kb-disk-sector-size</Source>

Moving VAX to a New Computer

Moving VAX to a new computer can be very simple. The important steps to take note of are as follows:

- Method of Database migrations
- Network Location
- Connection Mode
- License Re-Arming

Method of Database Migration refers to how the database information will be moved. Moving between local deployments can be done through the Data Migration utility or the System Manager Backup/Restore Option.

1. The Data Migrator tool grabs partition(s) data and exports it as a YAML file. This file can then be imported into another instance of VAX.
    - **Data Migrator does not export Notifications, Logs, Profile Pictures, Templates, Maps, Administrators, Site and Areas
2. System Manager Backup/Restore performs an entire system database. This can then be restored on a new VAX system.
3. **Sounds and System Logs are not transferred
4. **Hosted solutions can only be transferred using the Data Migrator utility.

Network Location refers to if the new server is on the same network as the old server. These are important factors, as the Panels may not be able to connect if it is on a different network, or Administrators will not be able to access from their devices.

Connection Mode is how users and Panels connect to the server. If the server uses an IP address, it can be as simple as setting the new server to the old IP address (make sure no IP conflict results from this). Server name will be different, as this could be a matter of changing the DNS server's name resolution.

License Re-Arming. The license will need to be re-armed to be associated with the new computer.

Toggle I-Frames on VAX

In some cases the I-Frame security of VAX may need to be improved. Please refer to the following guide to toggle an I-Frame setting improvement. In versions 3.0.1.26 and newer this setting is already enabled. To toggle this setting follow these steps to edit the Appsettings file. Keep in mind changing the following setting to false will enable the setting; changing to true will disable the I-Frame setting.

1. Start by opening the C: drive in File Explorer
2. Navigate to Program Files (x86)
3. Navigate to folders VAX
4. Navigate to WebServer folder
5. Find the file named appsettings and open it in Notepad (Run Notepad as an Administrator;, this may require you to open Notepad as an Administrator first, then use File > Open File and open the Appsettings file)

6. Scroll down to the bottom of the code where you see the code block Authentication at the bottom of the main block of Authentication; look for: "CookieSameSitePolicy": "Lax"

7. Create a new line and add this line: "AllowIFrames": false

8. Additionally you would need to add a comma at the end of the line above: "CookieSameSitePolicy": "Lax",

The bottom of the appsettings file (from the Authentication section and down) should look like this:

"Authentication": {

"MaxPasswordAttemptLockoutTime": 10,

"MaxPasswordAttempts": 5,

"UniquePINByPartition": false,

"MobileCredentialSiteCode": 61000,

"SlidingSessionExpiryInMinutes": 600,

"CrossOriginURLs": [],

"CookieSameSitePolicy": "Lax",

"AllowIFrames": false

},

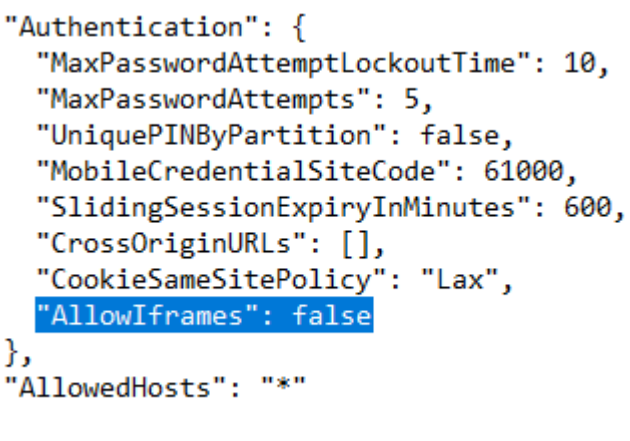
"AllowedHosts": "*"

}

Note:

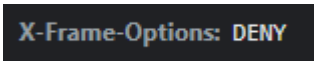
You may need to run Notepad as an Administrator before opening Appsettings. To do this you need to open Notepad by typing Notepad in the Windows search or finding its icon in the Start Menu and right click to Run as Administrator. Then use the File > Open File in Notepad to navigate to the Appsettings file. Once you are inside the correct folder you may need to change the type of file being displayed to All Files instead of just .txt . Click on the file appsettings to open. At this point refer to the section above to make the necessary changes.

Figure 43.2.



This setting should be set to false if you wish to protect from vulnerabilities. If you wish to disable this security feature please replace "AllowIFrames": false with "AllowIFrames": true. By default this setting is set to false and can be observed in the developer tools of VAX. To view the status enter developer tools on a page with VAX open and navigate to the Network tab and Header tab. Under Response Header observe I-Frame-Options: DENY. This indicates the software is protecting against I-Frame vulnerabilities.

Figure 43.3.



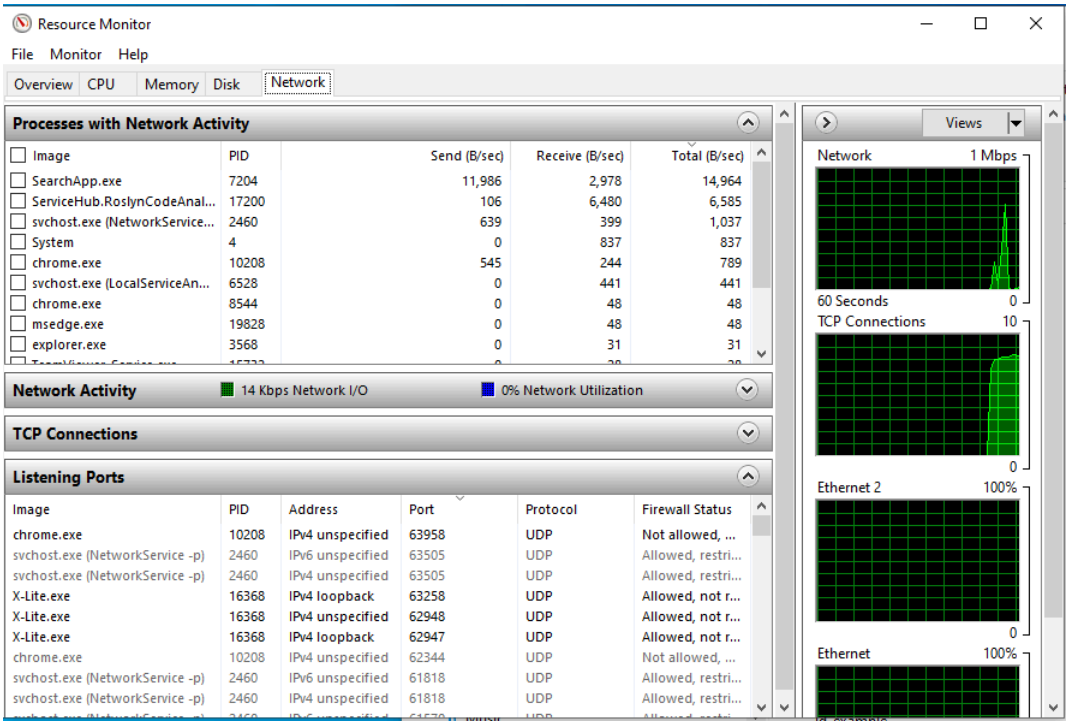
Troubleshooting Communication

A panel may disconnect and stay disconnected for a wide variety of reasons, from server side to panel side and everything in between. This guide will help provide insight on where to begin troubleshooting for connectivity.

Server Diagnostics

1. Check if the Server IP address is correct. Within VAX, check to see if the Server Address field (found under System Settings) is consistent with the Server's actual IP address. Panels initiate the communication to the Server and so will be looking for a defined Server Address, which should resolve to the machine where VAX is hosted.

2. Check if ports are unblocked or used (Firewall Status and Resource Monitor). Firewalls such as McAfee are common culprits where it is required to unblock the ports manually through their interface. As well, another process may be using the ports used by VAX. Resource Monitor is a useful tool to quickly check if the ports are occupied or blocked.



Panel Diagnostics

1. Start by checking if the Panel has obtained an IP Address. By default, the panels seek to acquire a DHCP address, and this address can be seen on the LCD of each panel on the scrolling menu.

To change the Panel to have a Static IP address, refer to the "Set Panel IP Information" in FAQ. It may also be seen in the Read Only menu:

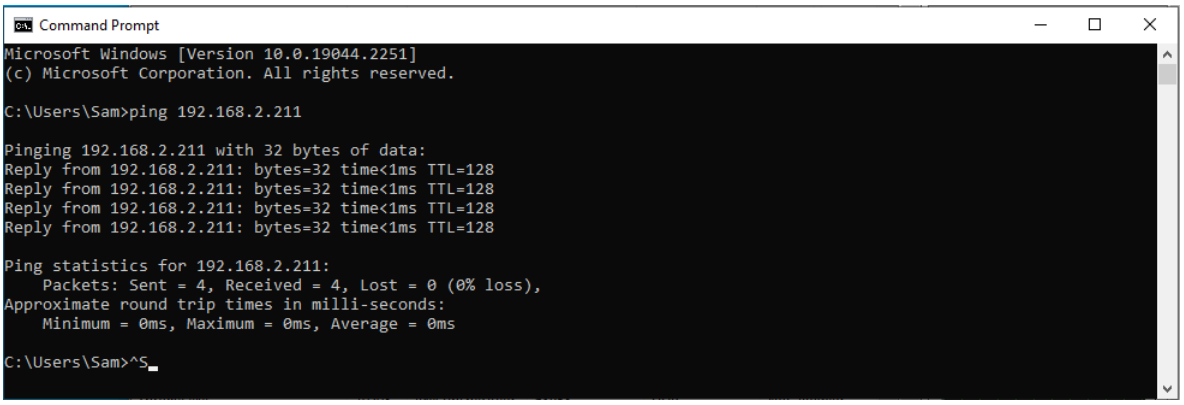
a. Press and hold the ESC button on the Panel (SW4)

b. Once in the Read Only menu, navigate to Option 6: Actual IP Address using the SW1 and SW2 buttons

2. From the Server or a local machine, check if the IP Address from the previous step is reachable by ping or web browser. All panels except the POE Elevator have a web interface that can be accessed by web browser.

3. If unreachable, verify the integrity of the network cables and devices. This can be tested by using another device such as a laptop or other device, or swapping out the components with other network cables or devices (i.e., swap from POE switch to POE injector).

4. Check if the switch or device the Panel is plugged into is a managed or unmanaged switch. Vicon Panels will not accept VLAN tagging information.



Cannot Connect To VAX

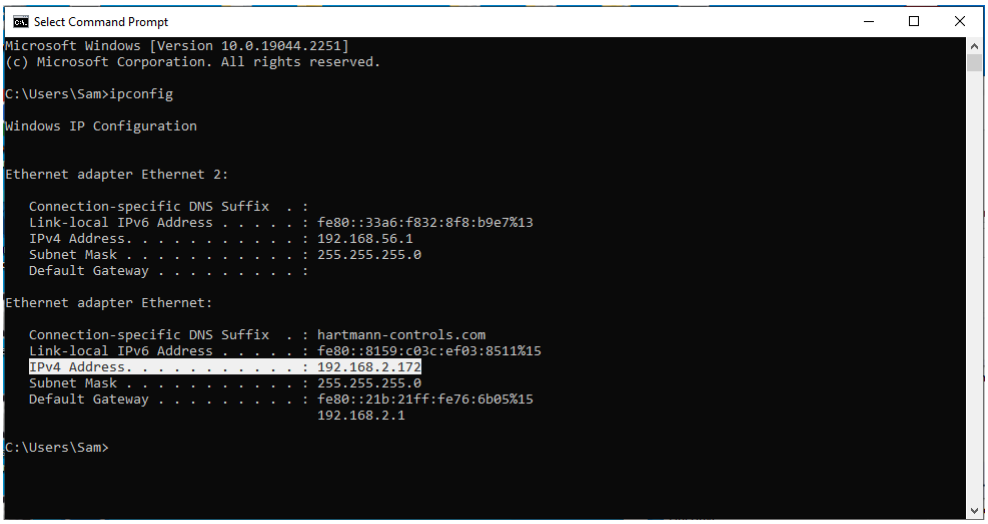
VAX requires HTTPS:// to connect to the Server. Next step is to see how the user is connecting.

- Are they using an IP Address?
- Computer/DNS Name?
- * It should match the method done upon initial configuration *

If the Administrator is using the correct browsing method (IP or Server name) to connect, check the Server settings to ensure that the IP Address configured under “Server Address” matches the IP address of the computer. This can be cross referenced by opening a CMD prompt and entering 'ipconfig' to compare IPv4 Addresses.

If the Server address and computer address match and the browser is still experiencing issues, this can be due to a network error. Verify connectivity by pinging the remote Server from the computer. A ping failure can determine if the Server is reachable from the host. To ping, open a CMD prompt and enter 'ping ' and the Server's IPv4 address or Server name (ie., ping 192.168.2.172). If the ping request Times Out, the Server is unreachable. If the ping is returned there is a connection.

*** IMPORTANT *** Ping failure does not always determine connectivity errors, as a firewall configuration on the Server machine may reject ICMP (ping) requests. Try pinging from the Server to the host computer, or try pinging the router from the Server and host computer.

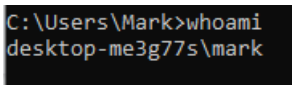


VAX Refuses to Connect

One of the most common reasons this occurs is due to a data migration fail. The error can be observed in the Application Logs. Usually System Manager and the SQL server will still run correctly. However, the VAX web server is unable to locate the SQL Server and because it cannot reach it, the web server will not run. It may stay up and keep running for a few minutes but will ultimately stop.

To remedy this problem, perform the following actions.

Figure 43.4. whoami



1. Open CMD and type “whoami”
2. Next within the CMD, attempt to access the server by entering the following commands:
   a. sqlcmd -S .\VAX
   b. Use VAX
   c. Go
3. Once access is confirmed, check the appsettings.json/VAX.exe.conf file. Change the following line to reflect below:
   a. ...Data Source=.\\VAX;...
4. Next check the Registry to check the installer registry, and if filled, clear it.

VAX Gets Connection Timeout to Database (3.0+)

1. Open appsettings.json
2. Modify the database connection string and add a new item at the end so it looks like this:

   "MainDatabaseContext": "Data Source=.\\VAX;Initial Catalog=VAX;Integrated Security=True;Connection Timeout=600"

3. Save and restart service

If using multi tenant, connection timeout needs to be added to connection string of each tenant.

Triple Swipe not Working on Card Readers

Triple swipe is a useful feature that enables programmability with card readers to perform specific functions. Common reasons why triple swipe does not work are as follows:

- Configuration: Triple swipe must be enabled on the card reader and the user account.
- To use triple swipe with a card reader ONLY, tap 3 times with the card reader.
- For keypads, tap 3 times OR enter PIN and then hit # 3 times to simulate tapping 3 times (i.e., 1 2 3 4 # # #).
    - Keypads have more options, after triple “swiping”, immediately press the desired key then hit #. There is a timeout.

Input, Output and Output Peripherals

Output Peripherals can include but are not limited to:

- Door Strikes
- Maglocks
- Gate Openers
- Turnstyles
- External Relays
- Sirens
- Strobes
- Automatic Openers
- Intrusion/Alarm Systems
- Elevator PLC
- Generic PLC Input
- Dry Contact Input on another Panel or Third-Party Panel

Inputs and Outputs can fail to work as intended. In some cases Inputs and Outputs control a function of the door. An alarm system that is supposed to go off doesn't. In this situation troubleshooting the input and outputs can resolve the issue. When troubleshooting, often the conclusion is one of the following:

- Wiring is incorrect or has become damaged (points of failure also include wire terminations, splices/B connectors)
- The device itself is damaged
- Output device requires more power or voltage than Panel specifications allow
- Input/Output is not configured to the correct function (Output 1-1, Output 1-2)
- Input/Output is incorrectly set (normally open/normally closed)

- Faulty input or output

Identifying the problem of the input/output will require a process of elimination. To divide the problem into multiple pieces and verify functionality of individual parts of the system to eventually discover what part is the problem. These pieces can usually be divided into these parts:

- The door/IO controller itself
- The cabling to/from the device
- The input/output device (door strike, door contact, exit button, etc.)
- The software configuration

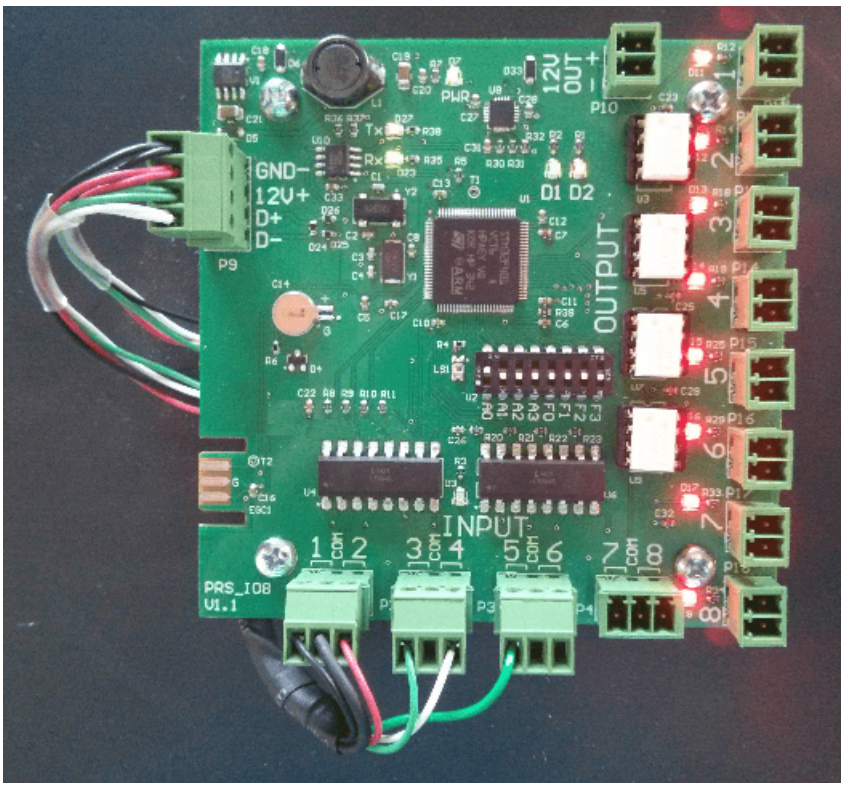
Input, Output, and Peripheral Troubleshooting

1. It is important to know which Outputs on the panels require an external power source. Please see Chapter 7
   <Output_troubleshooting>Panel Setup</Output_troubleshooting>
   In some cases the output requires an external power supply; the Panel will not provide power. It is important to know how much power the output uses and if the POE can supply enough power.
   - VAX-EXP-2D and VAX-1D-1Wet Relays (lockpower 1, lockpower 2) are limited to 550mA @ 12VDC
   - VAX-EXP-2D and VAX-1D-1 Solid State Relays (Output 2,3,5,6) are limited to switching 24VDC 1A
   - VAX-IO-EXP8-PCB relays are limited to switching 30VDC 500mA
2. Inputs on all controllers are dry contact. When the Panel sees a ground closure from the signal pin it considers the input active.
3. If an output is not working, first check the physical hardware of the output. If the door strike is being powered from lockpower, use a multi-meter at the Panel to check if the strike is receiving voltage and to check the state of the amber LED. If there is a short on the door strike or the cable, the amber LED will turn off. Measure the voltage at the lockpower output while the lock is connected (override it to unlocked from the software or use an Output test on the panel LCD) and while the header block is disconnected.
4. If the door strike is externally powered, take the header block off the relay and change the multi-meter to resistance or conductivity mode and measure the relay while on and off. If there is no conductivity;, the relay is damaged. If there is conductivity;, the next step would be to take the wires out of the header block and short them together (to simulate the relay). If the strike fires, it implies the relay is the issue (verify specs of the strike as this implies the strike damaged the relay with too much voltage or too much current). If it seems fine, try a spare relay (if available) or switch to an external relay.
5. Taking the wires off the Panel's relay and shorting them together will verify if relays are no working. If the device (strike, maglock, auto opener) doesn't work after doing a short;, then it's the wiring, the Peripheral device itself, or the power supply.
6. To measure the voltage (or conductivity) at the device itself or rule out the wiring, unmount the door strike or maglock and bring the device directly to the Panel with a short cable. If it works directly connected to the Panel but not with the longer cable;, then it's likely the cable. A technician should be able to verify this with a cable tester or by twisting one end of the cabling together, making a short, and then do a conductivity test with a mutli-meter.
7. Verify that the hardware itself is working and the Panel itself is functioning before logging into the software to verify the relay settings, which door is associated, timers on the doors, etc. If the door overrides work but card reads do not;, check the timers on the door in case a 200ms unlock timer

is set. Check if the Input/Output is overridden in the System Overview, disabled, or on the wrong input/output in the IO settings of the panel.

8. Similarily, with an input;, if the input test (via panel LCD) does work but the action (such as unlocking the door) doesn't work;, this indicates attention should shift to the input configuration on the software. If the Panel input is functional, then it is time to rule out the device or the cabling.

Figure 43.5.

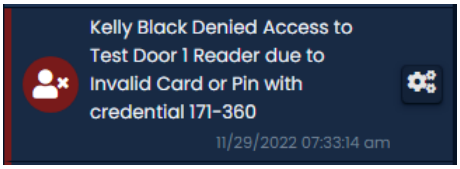


Access Denied Troubleshooting

When cards and PIN are configured incorrectly there is typically one component missing. Some of these common causes are:

- Access Groups: Users may be placed in a different Access Privilege Group.
- Partition: The Panel for the door may have been added to a different partition.
- Schedules: The Schedules configured on the door or access group may be denying access at the specified times. (User Schedules apply to specific readers within an access group) .
- Door Schedules: Door Schedules apply to the actual door. A common issue can be using a PIN on a door with Card Only Access.
- The door/floor or connected inputs/outputs may be override. Check System Overview for door/floor/input/output status.

Figure 43.6. Access Denied



Will my Existing Cards Work with VAX?

Cards can vary from all sorts of bit formats. For example, the ProxyII cards can be programmed with anything up to 85 bits. Some things to check to see if it is compatible:

1. Can the readers “read” the card? Is there a beep?
2. What does VAX see on the card? Does the output show as expected?
3. Some of the above issues can also be due to incorrect wiring of the card reader, so make sure the reader is able to scan an existing card that is known to work with the system.
4. Do a reader test and make note of the Bit Format and card number. Compare this to a reader test of the same credential at another reader.

Keypad Not Sending PINs

VAX requires 8 bit burst mode to be able to read the PINs correctly.

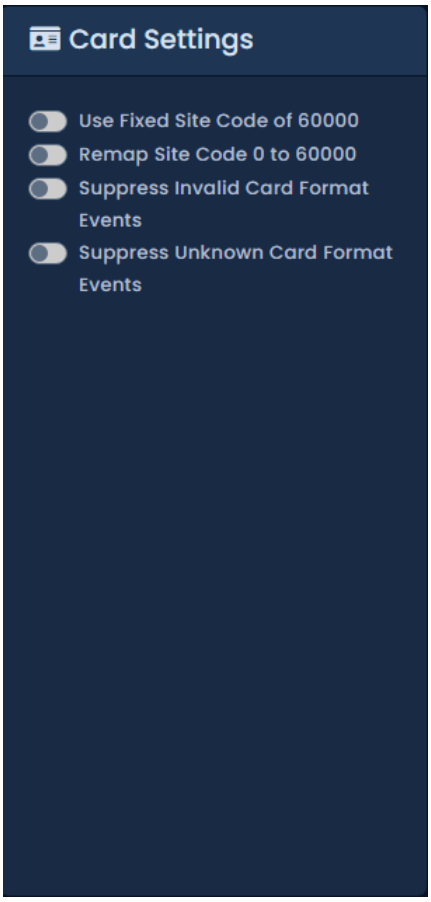
- On a Rosslare (AYC-Q65), perform the following actions:
  - Enter programming mode (# # # #) (sometimes holding # for 4 seconds works)
  - Enter programming code (1 2 3 4)
  - Enter menu 1 (1)
  - Select Option 3 (3), which is the Wiegand 8-bit Nibbles Complemented

List of Possible Reasons for Denied Access

- An Update to Panels
- Wrong Timezone
- No Privilege
- Card Invalid
- Invalid Start Work Date
- Invalid End Work Date
- PIN Expected
- Incorrect PIN
- Invalid Security Level
- Invalid Card Format
- Not in Access Privilege Group
- Authentication Levels
- Override
- One Time Run Event
- Holiday

- Door Timezone
- User Timezone
- Crisis Mode Enabled
- Timezone set to card mode when entering a pin
- Rosslare keypads don't support PINs higher than 50999
- If you are seeing an error with 1 bit navigate to the Card Formats under Edit Panel and toggle Suppress Invalid Card Format and Suppress Unknown Card Format Events.
- If site codes are not working override site code under Card Formats under Edit Panel and toggle Use Fixed Site Code of 60000. Then change each user's credential to site code 60000.

Figure 43.7. Card Formats



Access Denied Types

Table 43.1. Access Denied Types

Image	Error	Description
Invalid Credential		Access denied to door because Credential type is Invalid for Reader.
Invalid Card or PIN		Access denied to door because PIN or Card Credential is Invalid.

Image	Error	Description
Invalid Timezone		Access denied to door because APG or Credential Invalid for the currently set TimeZone.
Invalid Crisis Level		Access denied to door because Crisis Level Access is below the currently set Crisis Level.
Invalid Start Date		Access denied to door because current date is not within Credential Start Date and End Date.
Invalid End Date		Access denied to door because current date is not within Credential Start Date and End Date.
Invalid APB		Access denied to door because Anti-Passback settings show user already inside area.
Invalid Access: Mantrap		Access denied to door because Mantrap settings show door 1 is still open before opening door 2.

Reader Troubleshooting

Summary of possible issues

- Reader does not respond (beep, blink) to a credential
- Reader does not power up
- Reader keeps beeping
- Card number doesn't match what is expected
- Presenting credential displays Unknown Card Format within the software
- Reader responds to credential but no notification in the software
- Some credentials unlock the door but others do not

Troubleshooting Methodology

Troubleshooting reader can be a similar process to troubleshooting inputs/outputs; divide the issue into easily testable pieces to narrow down the issue. Depending on the issue it may or may not be easily divisible.

Reader Does Not Respond to Credential

Symptom(s)

- Person presents RFID credentials to a reader but the reader does not beep or blink or respond. Nothing shows up in the software

Possible Causes

- Mismatch between the frequency of the reader and the frequency of the card (such as trying a 125khz card on a smartcard reader)
- Reader does not have sufficient voltage/current (not common)

- (Smartcard only) Encryption keys missing
- (Smartcard only) Reader not configured to support specific technology (reader may respond to DESfire EV2 but not MIFARE Classic)

Additional Information

- Try to find the model of the reader, usually located on the back, to check what RFID technology it supports
- Try to find the box the card came from to identify the frequency

Typical frequencies and types include:

- HID 125KHz
- AWID 125KHz
- EM 125KHz
- INDALA 125KHz
- IOPROX 125KHz
- 433MHZ UHF (WRR22, WRR44, etc)
- 902 to 928 MHz (UHF readers like Specre, LR-3000)
- 13.56MHz (ICLASS, ICLASS SEOS, MIFARE CLASSIC, MIFARE Desfire EV1/EV2/EV3

Reader Does Not Power Up

Symptoms:

- Reader does not show any LED or startup beeps
- Reader may be power cycling which would make it do start up beeps every few moments

Possible Causes:

- Insufficient voltage or current
- Short across GND and POWER
- Power not connected (damaged cable, miswired, bad B connector, etc)
- Damaged reader

Additional information:

- Get the model of the reader to lookup the current requirements. VAX-1D-1 has 500mA available for readers. VAX-EXP-2D has up to 700mA available for readers.
- Measure the voltage coming off the reader port on the panel side. There will be no voltage if there is a short or over current. Unplug the reader(s) and see if voltage comes back.
- Measure the voltage at the reader itself (involves having to take the reader partially off the wall).
- If over current is suspected, connect the reader to alternate 12V power source such as the bottom header block connection on the interconnect strips, external 12VDC power supply or even a 12VDC battery.

- Connect the reader directly to the Panel to rule out the wiring if a multimeter isn’t available.

Reader is Beeping Erroneously

Symptom(s):

- Reader is continuously beeping (ie., 'beeeeee...')
- Reader is doing multiple beeps in a row (ie., 'beep beep beep...')
- Reader is continuously beeps but only when the door is unlocked

Possible Causes:

- Continuous beep can be caused when Buzz line is shorted to ground or if only beeping when door is unlocked; Buzz and LED line are likely mixed up
- Door is Forced Open or Held Open

Additional Information:

- To rule out the reader itself deciding to beep, disconnect the Buzz wire from the Panel side to rule out the Panel as being the one telling the reader to beep

Card Number Doesn't Match Expected Number

Symptom(s):

- User presents their credential to the reader but the number shown on the LCD or the Panel doesn't match the expected card number
- Credential shows a card number correctly on one reader, incorrectly on another

Possible Causes:

- Data lines (D1, D0) are backwards (26 bit Wiegand backwards will show 0-0; other bit lengths will just show the wrong card number)
- Card Format settings don’t match the format of the credential. Perform a Reader Test to check the bit length and try changing the applicable bit length setting on the Card Formats tab of Edit Panel or Edit Site
- If bit length is 32 bits, this may indicate that a smartcard reader was unable to access to encrypted card number and read the CSN of the credential instead

Additional Information:

- When smartcard readers read the CSN of a card, the reader itself (HID or STid) may be programmed to output the CSN in a different way. So one reader may read it as expected while the other doesn’t.

Software Shows Unknown Card Format Upon Credential Presentation

Symptom(s):

- User presents their credential to the reader but the software shows one or more Unknown Card Format, number of bits x

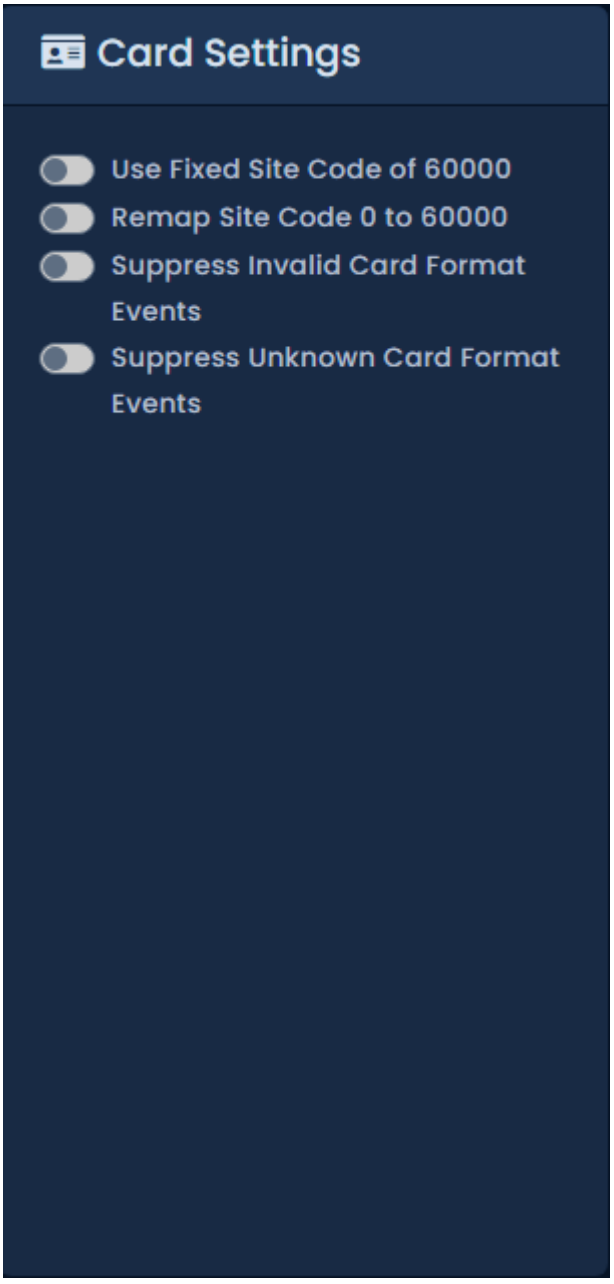
- Without presenting a credential, software shows Unknown Card Format, number of bits 1 or 2

Possible Causes:

- One of the data lines is not connected (D1 or D0 disconnected will return several unknown card format notifications of various lengths)
- EMF/EMI is causing bad data to get sent to the panel or could potentially be affecting the signal
- Incorrect cable used (no shield or no grounding of the shield)
- Reader tamper (some readers like STid will spit out a bunch of single bits of the tamper is active)

Additional Information:

- There may be an incorrect cable; use the Reader Sampling settings either directly on the LCD or on the Reader tab of the Edit Door screen (LCD sampling mode is a temporary change, try all settings; once a setting works set that type in the software)



Reader Responds to Credential But No Notification in Software

Symptom(s):

- User presents their credential to the reader and the reader responds, but the software or the LCD do not display any card number or related messages

Possible Causes:

- Data lines both completely disconnected
- VAX-EXP-2D not communicating to VAX-MDK (could be DIP switches or software not configured with correct amount of expanders
- No door has been added to the controller (can be ruled out with Reader Test on LCD)
- Notification Settings have a real time rule set to not display reader events (can be ruled out with Reader Test on LCD)

Additional Information:

- If a reader is in Reader Test mode there will be no notification or logs for card reads until it is returned to normal state

Readers and Configuation

ForHID Reader configuration please refer to the following resources:
<configure>https://configure.hidglobal.com/configure</configure>

Wiegand Keypad - 8-bit {Dorado}
<figures>

</figures>

Card Reading Incorrectly

Some common issues for why cards read but appear in our software incorrectly:

- Incorrect bit format in VAX. Can be changed within software or some sample cards can be sent and we will try to crack them.
- Data lines are backwards. Swapping them may fix it.
- Older versions of software did not support long card numbers. Version 2.10.18 added support.

Card Readers Turning Off Intermittently on a VAX-MDK Panel

A VAX-MDK Panel with 3 modules, 6 doors and 6 readers attached. Some readers turn off intermittently and when they are on, transmit garbled ID’s to the server. Wiring is correct, 22 gauge running 75ft at most. Power is transmitted, voltage readings are correct.

Issue was with interference on the line. Changing the Sampling mode on the readers fixed the issue.

Wiring Issues

Bursts of denied access with short bit numbers is typical of interference or grounding issues.

The reader is reading the card but coming back with a 0-0 or a different odd card format is typical of a incorrect order of white and green reader cables.

Some Cat6/Cat5e cable will work but in some cases twisted pair cables are not shielded from each other. Also, do not use twisted pair (green and white/green for data lines (D1 D0). Distance from panel to reader should be a maximum 500ft from panel to reader when installed correctly with the correct wire.

Power Specifications

Readers:

- VAX-1D-1 Readers - 500mA/per port
- VAX-2D-1 readers 350mA/per port (700mA/per VAX-EXP-2D)
- 26 bit standard / 125 khz frequency
- 8 bit burst for keypad

Outputs:

- VAX-2D-1 12V out 500mA @ 12VDC (shared with Reader ports)
- VAX-EXP-2D 12V out 350mA @ 12VDC (shared with Reader ports)
- VAX-EXP-2D / VAX-1D-1 wet relays (lockpower 1,4) = 500mA @ 12VDC
- VAX-EXP-2D / VAX-1D-1 Solid State Relays (output 2,3,5,6) switching 1A @ 24VDC
- VAX-IO-EXP8-PCB relays Switching 500mA @ 30VDC