

VAX

Access Control System ver. 2.10

XX274-30-08



Vicon Industries Inc. does not warrant that the functions contained in this equipment will meet your requirements or that the operation will be entirely error free or perform precisely as described in the documentation. This system has not been designed to be used in life-critical situations and must not be used for this purpose.

Document Number: 8009-8274-30-08 Product specifications subject to change without notice. Issued: 2/22 Copyright © 2022 Vicon Industries Inc. All rights reserved.

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

Copyright © 2022 Vicon Industries

Table of Contents

Introduction	x
Vicon Software - End User License Agreement	xi
Copyright	xiii
1. Getting Started	1
Overview	1
Server Prerequisites	1
Operating Systems Supported	1
Installation Procedures	2
New Installation Vicon Access Control	2
Upgrading Vicon Access Control	7
System Monitor	7
Frequently Asked Questions	8
Client Installation	9
Supported Browsers	9
Accessing the Server	10
Frequently Asked Questions	11
2. Upgrading Vicon Access Control	12
Download the Latest Version of VAX	12
Prerequisite Installation	12
Upgrade Installation	12
Panel Firmware Updates	12
Troubleshooting Firmware Update Problems	14
Frequently Asked Questions	15
3. Initial Configuration	16
Initial Software Configuration	16
Connection Configuration	17
Customer Configuration	17
Dealer Information	18
Initial Administrator	18
Email Settings	18
Logging Into Vicon Access Control Web Interface	19
Password Recovery in Vicon Access Control	19
Panel Initial Configuration	20
Navigating the Panel Interface	21
Communication Mode Configuration: Server IP	22
Communication Mode Configuration: Server Name (DNS)	24
Panel IP Settings: DHCP	25
Panel IP Settings: Static IP	27
Resetting a Panel	30
Testing Input/Outputs at the Door	31
Panel HTTP Configuration Interface	39
Adding a Panel to Vicon Access Control	40
Method 1: Adding a Panel via Unknown Panels Screen	41
Method 2: Adding a Panel Manually With MAC Address	42
Adding a Panel: Basic Configuration	42
Where to Go From Here	44
4. Software Licensing	45
Licensing Your Software	45
Supported Card Formats	47
FAQ for Software Licensing	47
5. System Manager UI	49
Accessing the System Manager UI	49
Changing System Manager UI Password	50
Backing up your Vicon Access Control Database	51
Restoring Your VAX Database	53

Service and System Management	54
Managing Services	54
Shutting Down or Restarting Your Server	54
Networking Settings in System Manager	55
Multi-Tenant	55
6. Planning an Access Control Deployment	56
Hardware	56
Hardware Specifications	57
Communication Topology	62
Cables, Standards and Best Practices	64
VAX-MDK Door Master Power Requirements	64
Identifying a Panel	65
Software	66
Order of Operations	66
Partitions	68
Sites	69
Door Time Zones	70
User Time Zones	72
Access Privilege Groups	73
Holidays	75
7. Setting up Your Panel	77
Advanced Panel Configuration	77
General Tab	77
Options	78
Input/Output Configuration	79
Updating Your Panel	85
Auto Panel Update	86
Panel Firmware Updates	87
Troubleshooting Firmware Update Problems	89
8. Setting Up a Door	90
Adding a Door	90
Advanced Door Configuration	92
General	92
Options	93
Reader Configuration	96
Areas	97
9. Door Time Zone Configuration	99
Adding a Door Time Zone	99
10. User Time Zones	102
11. Access Privilege Groups	104
12. User/Cardholder Configuration	106
Adding a User	106
User Privileges	107
User Card Holder Images	108
Custom Fields	108
User Credentials	109
Access Groups	110
Panel User Actions	110
User Templates	111
Enrolling Cardholders via Notification	112
Importing Users and Card Holders	113
Adding Custom Fields	115
13. Holiday Configuration	118
Holiday Order of Operations	118
User Holiday Time Zones	119
User Holiday Groups	120
Door Holiday Time Zones	121
Door Holiday Groups	122

Floor Holiday Time Zones	123
Floor Holiday Groups	124
Adding a Holiday	125
Holiday Example	126
14. One Time Run Zones	130
Adding a One Time Run Time Zone	130
15. Crisis Levels	132
Making Changes to Crisis Levels	132
Configuring User Security Levels	133
Applying Crisis Levels to Doors	133
Applying Crisis Levels in Vicon Access Control	133
Applying Crisis Levels With an Aux Input	134
16. Vicon Access Control Override Features	135
Override Doors	135
Override Floors	136
Override Outputs	137
17. Triple Swipe Features	139
User Requirements to Use Triple Swipe	139
List of Triple Swipe Options	139
Configuring Triple Swipe	141
Triple Swipe Examples	142
18. System Overview	144
19. Partition and Site Configuration	147
Adding Partitions	147
Adding Sites and Areas	148
Edit Sites and Areas: Areas	149
Edit Sites and Areas: Card Formats	149
20. Administrators and Privileges	151
Adding an Administrator Account	151
Administrator Examples	155
Example: Secretary	155
Service Account Administrators for Third-party Services	156
Generating API Key	156
IP Whitelist	158
Using an API Key	159
21. Areas and Anti-Passback	160
Hardware	160
APB Memory Module	160
Anti-passback Software Configuration	161
Adding Areas	161
Anti-Passback Configuration	162
Assigning Areas to Readers	163
APB Status and Violations	164
22. Mantrap Configuration	167
Mantrap Hardware Setup	167
23. Reporting	170
Administrative Log	170
User Activity	171
Door Activity	173
Floor Activity Report	175
Elevator Activity Report	177
User List	179
Notifications Report	181
Muster Report	183
Configuration Reports	186
Input Activity	188
Output Activity	190
Action Plan Activity	192

Time Tracking	194
Time Tracking Output	195
24. Notifications	197
Destinations	197
Real Time	197
Email	197
Web Push	197
Database	199
Notification Settings Page	199
Notification Rules	199
Types	199
Groups	199
Accessing the Notification Settings Screen	199
Rules List	200
Creating a Notification Rule	200
Notification Styles	201
Creating a Notification Style Rule	202
Live Camera Rules	203
Creating a Live Camera Rule	203
Notification Sidebar	203
Sidebar Controls	204
Monitoring Screen	205
Accessing the Monitoring Screen	205
Customizing Displayed Notifications	206
Monitoring Options	206
Selected Notification Options	207
25. Database	209
Purging Notifications	209
Purging the Administrator Log	210
Database Size Warning	210
26. System Settings	213
General Configuration	213
Server Address	213
Security	214
Enhanced Manual PIN Security	214
Email Configuration	214
Email Settings	214
Email Notifications	215
27. Elevator Hardware	216
Connecting the Elevator-Master Panel to the IO-Boards	217
Configuring IO-Board Addresses	218
IO-Board Input/Output Test	220
IO-Board Tamper Sensor	220
28. Elevator Software Components	221
Adding an Elevator Panel	222
Adding an Elevator	224
Button Sensing	226
Floor I/O Map	227
Floor Time Zones	227
Assigning User Access to Floors	229
29. Open Supervised Device Protocol (OSDP V2)	230
Benefits of using OSDP	230
Supported Door Controller Models	230
How to Check if Firmware Supports OSDP	230
Wiring Up an OSDP Reader	231
OSDP Connection Points	231
Termination Resistors	232
Setting up OSDP Communication	232

Setting OSDP Reader Address Through LCD Menu	233
OSDP Software Communication Settings	234
Setting OSDP Secure Channel Mode	235
Setting Encryption Keys	235
Enabling Secure Channel Mode on OSDP Readers	236
Software: Restricting OSDP Communication to Secure Channel Mode	237
30. Input/Output Boards	239
Introduction	239
IO Board Part Numbers	239
Hardware Setup	240
Connecting the IO-Master to the IO-Boards	240
Configuring IO-Board Addresses	242
IO Software Configuration	243
Adding the VAX-IO-STR-2 Master Panel to VAX	244
Configuring Inputs and Outputs	246
Input and Output Time Zones	251
Unmanaged and Monitored Doors with IO-Boards	255
Real World Applications For Inputs and Outputs	257
31. Camera System Integration	260
Supported Browsers	260
Enable the VMS Web/Mobile Server	261
Enable Web Server: Valerus Configuration	261
Enable Web Server: ViconNet	261
Enable Web Server: Milestone XProtect Mobile	262
Enable Web Server: Exacq exacqVision Web Services	262
Enable Web Server: Digital Watchdog DW Spectrum	263
Enable HTTPS: Hikvision NVR	263
Adding a Camera System	263
Manage Camera Systems	265
Purging Cameras	266
GPU Acceleration	267
WebSockets	267
Use Proxy	267
Viewing Synchronized Cameras	267
Viewing Live Video	268
Viewing Playback Video	270
Associating Cameras with Doors and Elevators	270
Camera Associations: Door	271
Camera Associations: Elevator	272
Camera Notifications	272
Configuring Live Camera Alerts	273
Adding Website Certificates for Camera Integration	274
Importing Certification in Internet Explorer	276
Importing Certification in Google Chrome.	277
Importing Certificates with the Certificate Import Wizard	279
Multi-vendor Camera Matrix	281
Viewing Cameras in Matrix	283
32. Active Directory Integration	284
Integration Overview	284
AD Integration Order of Operations	284
Planning: What AD Information will be Synchronized	285
AD Groups, Membership and Structure	286
User Credentials	286
Configuring Service Accounts	288
Create and Configure Service Accounts	288
Installing VAX in AD Domain Environment	289
LDAP Integration Settings in VAX	291
LDAP User Credentials	291

LDAP User Custom Fields	292
Create Associations Between AD Groups and Access Privilege Groups	293
Synchronize Users from AD	295
LDAP Administrator Authentication	295
Troubleshooting LDAP Integration	297
LDAP Conflicts	297
VAX Services Fail to Start	297
33. Action Control Engine	299
Introduction	299
ACE Use Cases	299
ACE Components	299
Action Plans	299
Action Triggers	304
Advanced Action Concepts	306
Variables in Action Plans	306
Expressions in Action Plans	308
If Action	309
Each Actions	309
HTTP Action	311
Exporting and Importing Action Plans	313
34. Interactive Maps	315
Adding a Map	315
Adjacent Maps	316
Adding Objects to Maps	317
Drawing an Area	319
Viewing and Monitoring With Maps	320
Map Objects Sidebar	321
Object Details Sidebar	322
35. Third Party Integration	324
CardPresso Photo Badging Software	324
Supported Fields	324
Creating an ODBC Connection for cardPresso	325
Configuring cardPresso Software to Access the Database View	327
Using the cardPresso Database Connection Wizard	327
Adding the CardHolder Picture	329
Taking Pictures with Vicon Access Control Web Interface	332
Assa Abloy® Aperio™ Lock Systems	332
Software/Hardware Requirements	332
Hardware Setup	333
Software Setup: Aperio Programming Application	334
Software Setup: Vicon Access Control Aperio Panels and Doors	337
36. Information for Domain and Network Administrators	339
Configuring Advanced Remote Access Through the Internet	339
How Panels Communicate	339
How Web Clients Communicate With Vicon Access Control	339
Remote Access: Network Requirements	339
Remote Access Examples	341
Performing Manual Back-up and Restore with MSSQL Command-Line	342
SQL Database Back-up	342
SQL Database Restore	343
Database Back-Up/Restore: Frequently Asked Questions	344
API integration	344
REST API	345
Real-time API	345
Accessing API documentation	345
Multi-Tenant Mode Configuration	345
Enabling Multi-Tenant Mode	346
Adding Tenants	346

Managing Tenants	347
SSL Certificate Information	349
Managing SSL Certificates	349
Performing Data Migration with Data Migrator	351
Exporting Partition Data	351
Importing Partition Data	352
Data Migrator Errors	354
Migration Example: Moving a Panel Between Partitions on the Same VAX System	354
37. Support	356
A.	357
Panel Model Reference	357
Visual Guides	357
Actions	368
WARRANTY AND SPECIAL PROVISIONS	380

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 section called "WARRANTY AND SPECIAL PROVISIONS" AND/OR OTHERWISE WITH THE SOFTWARE. SUCH LIMITED WARRANTIES, LIMITATION OF LIABILITY AND SPECIAL PROVISIONS ARE AN INTEGRAL PART OF THIS EULA.

Copyright

Copyright © 1998 - 2022 Vicon All rights reserved.

Information in this document is subject to change without notice. The software outlined in this document is provided under license agreement. The software may only be used in accordance with the terms expressed by Vicon.

No part of this documentation may be reproduced or transmitted in any form or by any means except for the User's benefit of operating the software without the express written permission of Vicon.

Vicon Industries Inc.

Phone: 800-645-9116

631-952-2288

Website: www.vicon-security.com

Chapter 1. Getting Started

Overview

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

- **Vicon Access Control Web Server:** The Web Server's responsibility is to host the web application and facilitate client access to managing your access control system.
- **Vicon Access Control System Monitor:** The System Monitor allows you to view the status and offers limited control over the web server and backup/restore utilities.
- **Microsoft SQL Server Database:** The Vicon Access Control software is designed to back onto a local or remote Microsoft SQL Database. You may opt to use the free (included) SQL Express 2012 or your own pre-installed instance of Microsoft SQL. Please note; we do not support non-Microsoft SQL Databases and a minimum version of 2008 is recommended.

Server Prerequisites

The Vicon Access Control application is designed to run on a modern PC running Microsoft Windows 7 or newer. Windows 10 or Windows Server 2012 is recommended for optimal performance.

Note

It is possible to install the Vicon Access Control 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 Vicon Access Control 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”.

- Intel Core I5 processor or higher.
- 4GB RAM.
- 5GB Free Hard Drive Space (Additional space required for database).
- Windows 7/8/10 Professional 32-bit or 64-bit; Windows 2008 or 2012 Server.

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 10 Professional (32 and 64 bit)	
Windows 10 Home (32 and 64 bit)	
Windows Server 2012 (Any Version)	
Windows 8 Professional (32 and 64 bit)	
Windows 8 Home (32 and 64 bit)	
Windows 7 Professional (32 and 64 bit)	
Windows 7 Home(32 and 64 bit)	
Windows Server 2008 R2	

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

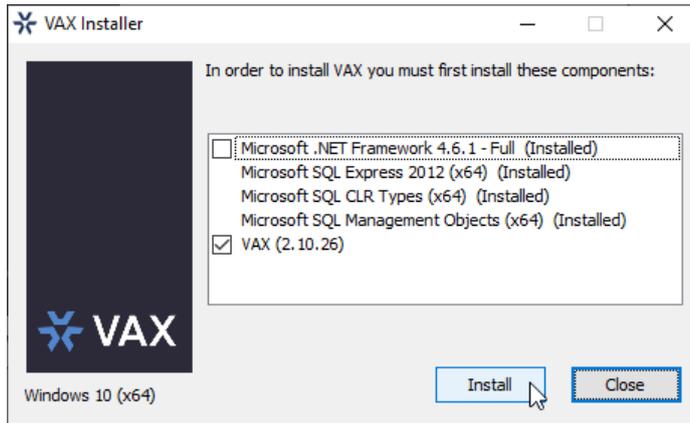
Installation Procedures

This section covers the installation of Vicon Access Control and some frequently asked questions.

New Installation Vicon Access Control

1. Locate and run the file called "VAX.exe" on your installation media or download and run the installer from our website.
2. Upon running the Installer for the first time, you will be presented with a screen outlining all the components required for installation. If a required component is not installed, it will be checked off automatically in the list of things to install. If you are unsure of which components to install, we recommend installing all checked components.

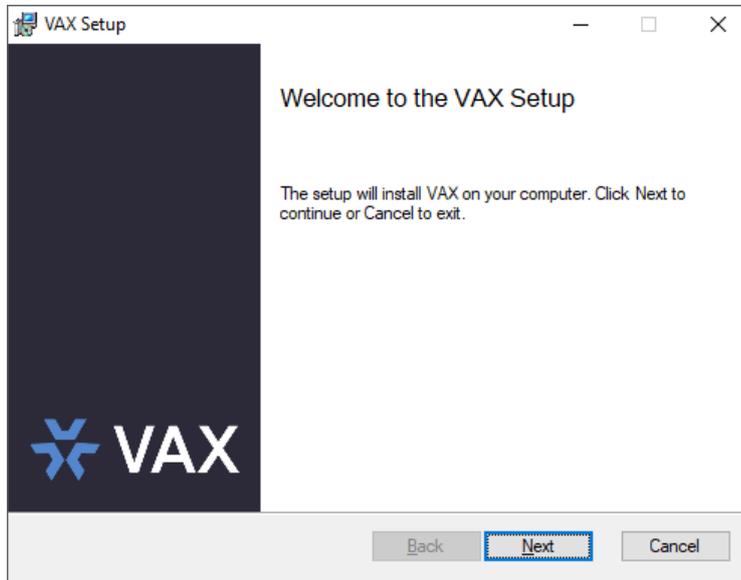
Figure 1.1. Vicon Access Control Initial Installation Screen



If you are installing from a USB Stick or DVD, the required components are often located directly on the installation media. In the event you are using a web installer, the required files will be downloaded from the internet.

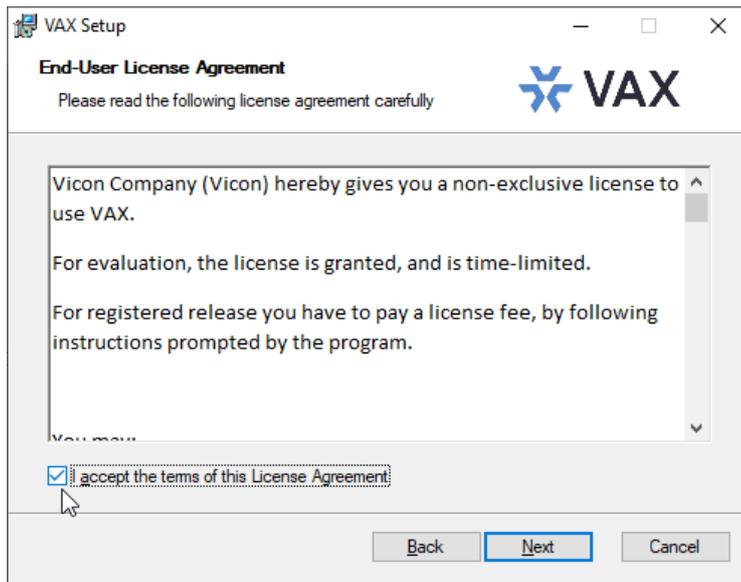
3. If prompted to start download for any components such as Microsoft SQL, click Start. This may take a while depending on the speed of your Internet connection.
4. If any components fail to install, restart the computer and try again. If they continue to fail, please see the relevant section within the master tech guide.
5. Once all prerequisites are installed, the installer will automatically launch the Vicon Access Control application installer.

Figure 1.2. Vicon Access Control Application Installer



After the Vicon Access Control Installer has loaded, click the **Next** button to continue.

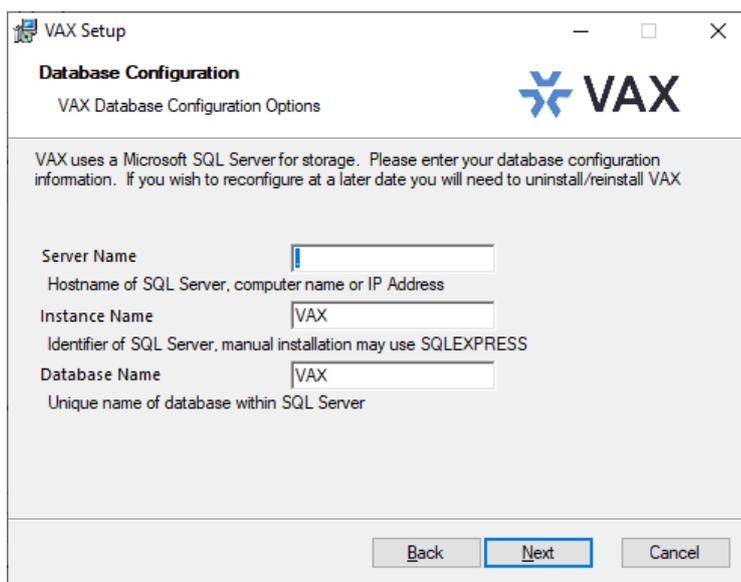
6. On the following screen, please read and accept the License Agreement. This agreement must be accepted in order to proceed with the Vicon Access Control installation. Click **Next**.

Figure 1.3. Vicon Access Control License Agreement

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

- **Typical installation** uses the default SQL Server and service configuration. This is recommended for Users who are not using an external SQL Server and don't have any custom requirements for service configuration.
- **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 Vicon Access Control configuration options.

8. **[Advanced Installation Only]** Database Configuration allows you to override the default SQL Server connection settings. This is commonly used if an external SQL database is being used.

Figure 1.4. Vicon Access Control SQL Configuration

- **Server Name:** The Server Name is host name of the SQL Server. Alternatively this can also be an IP address. In the case of an IP address, we recommend using a static IP address or DHCP reservation to ensure the address will not change.
 - **Instance Name:** The Instance Name is an optional identifier generally used with SQL Server Express products or in cases where there may be more than one SQL Server installation on a single machine (not databases).
 - **Database Name:** The Database Name is the unique name given to the database within the SQL Server.
9. **[Advanced Installation Only] Service Configuration** allows you to modify the User/password and ports used by the various Windows services.

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

Communication Server Service: The communication service is used to communicate with the **Panels** on **Port 9876**. This can be changed if port 9876 is being used by another service.

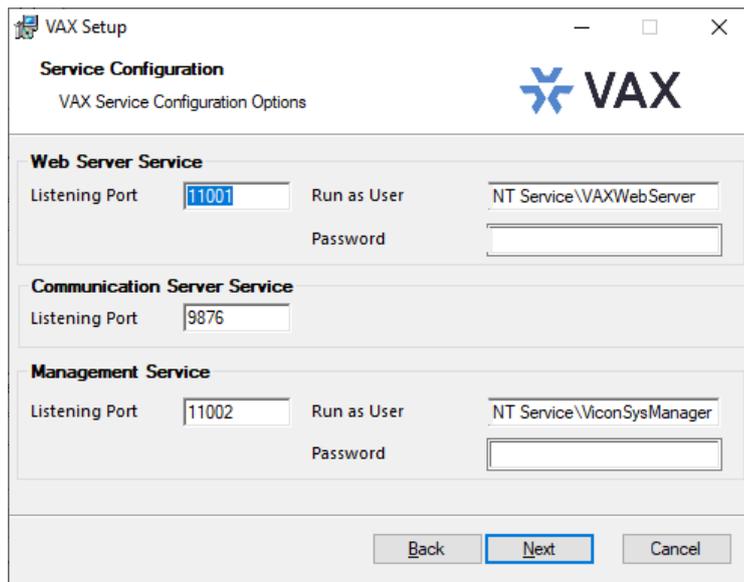
Management Service: The service the **System Manager UI** will run as. The **Listening Port** is the port the server will listen on for management communication, by default is **11002**.

"Run As User": The **Run As User** text box in each service above is the User the service will be run as. By default we use a **Service User** built into Windows.

Warning

In domain environments a **Domain Service User** or a **Local Administrator Account** may be needed to run the services.

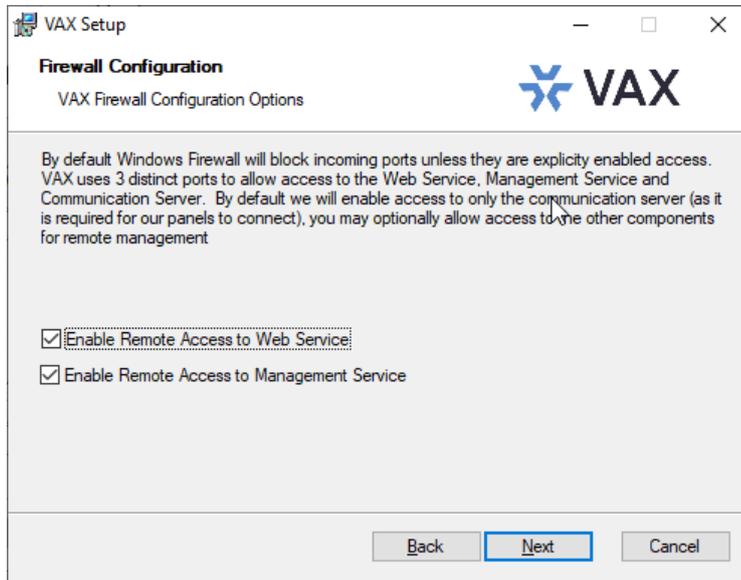
Figure 1.5. Vicon Access Control Service Configuration



10. The next step is to configure **Windows Firewall** to allow outside access. By default **Windows Firewall** will block incoming ports unless they are explicitly enabled access. Vicon Access Control uses 3 distinct ports to allow access to the Web Service and Management Service. Please note the installer will at your discretion allow access through the built in Microsoft Windows firewall, if

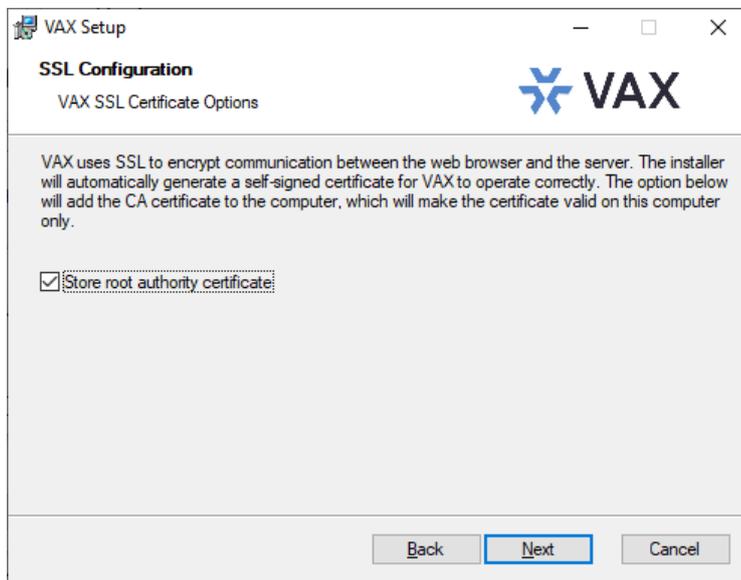
you are using a third party firewall; additional steps may be required to permit access. Please check your firewall documentation for additional clarification.

Figure 1.6. Vicon Access Control Firewall Configuration

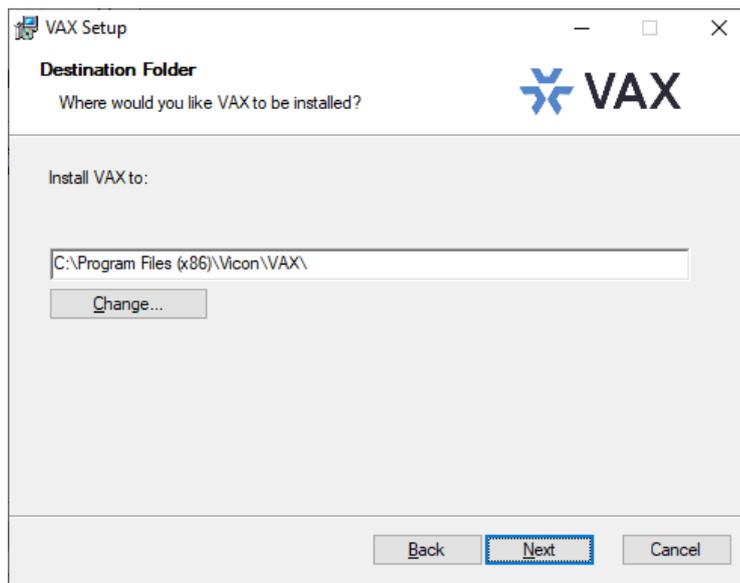


11. Next you can choose if we will store the SSL self signed certificate as a root authority. This can prevent self signed certificate errors on some web browsers when selected. For more information, please see the section called “SSL Certificate Information”.

Figure 1.7. Vicon Access Control Installation SSL Configuration



12. The next step is to select the installation directory where you would like the Vicon Access Control application to be installed.

Figure 1.8. Vicon Access Control Installation Directory Configuration

13. You have now completed the configuration portion of the installer. Click **Install** to perform Vicon Access Control installation and **Finish** when the installation completes.

Upgrading Vicon Access Control

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

Upgrade Installation

Depending on how you've installed Vicon Access Control, the procedure for upgrading the Vicon Access Control software may require some steps not covered in this section. Please see Chapter 2, *Upgrading Vicon Access Control* for more details on these extra steps. We recommend doing a backup of your Vicon Access Control database prior to upgrading. For more information about backing up your database, please see the section called “Backing up your Vicon Access Control Database”. We also recommend stopping the Vicon Access Control 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 upgrade.

Updating Firmware

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

System Monitor

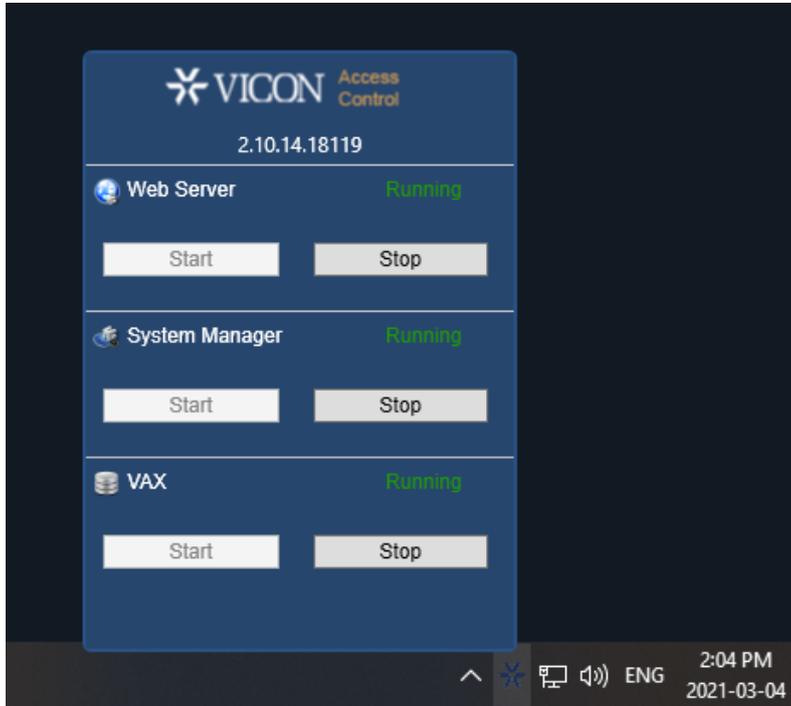
System Monitor is a tray application that shows you the status and offers limited control over the web server process. It can give you several useful shortcuts when the icon is right clicked. It will also show you the current version of your VAX software.

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).

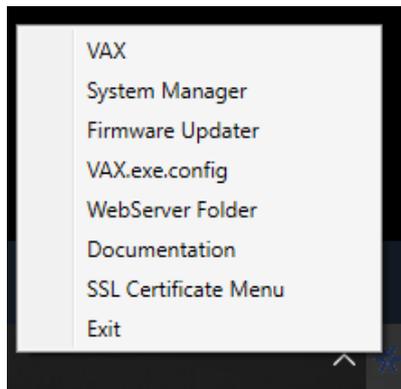
Figure 1.9. System Monitor Window



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 2012 or can I use my own database software?
- A:** We support any Microsoft SQL Server from 2008 to present, 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 your 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 7. We are committed to ensuring the software works with future versions of Microsoft Windows.

Q: I received an SQL error during Vicon Access Control installation. What should I do?

A: As part of the Vicon Access Control installation, you are required to provide the correct SQL information which the installer uses to configure a number of Vicon Access Control database and security options. If this information is incorrect, it will need to be corrected before you are able to successfully install the Vicon Access Control software. If you have chosen to install SQL Express as part of the Vicon Access Control 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: The maximum database size is a direct limitation of the version of SQL installed, not the Vicon Access Control software. If you have used the default SQL Express 2012 installation, the maximum database size is 10GB. Earlier versions of SQL Express prior to 2008 generally had a limitation of 2GB.

Q: Is Vicon Access Control 32-bit or 64-bit?

A: Vicon Access Control 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 Vicon Access Control software will not benefit from the increased addressing 64-bit provides.

Client Installation

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

Supported Browsers

The list of browsers supported is by no means a comprehensive list. These are browsers that receive testing by Vicon, 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. Vicon Access Control Browser Support

Browser	Version	Supported	Notes
Google Chrome	24.0+	Yes	No Silverlight support, limited integration with ViconNet
Mozilla Firefox	20.0+	Yes	
Microsoft Internet Explorer 11	10.0+	Yes	Note: IE10 in Metro UI (Windows 8) is not supported. The desktop version however is fully supported

Browser	Version	Supported	Notes
Microsoft Internet Explorer	6.0 to 9.0	No	No 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. No Silverlight support.
Apple Safari	5.0 (Mac/Windows)	Untested	
Apple Safari	6.0 (Mac)	Untested	
Blackberry Mobile	Any	Untested	
Epiphany (Linux)	Any	Untested	
Konquerer (Linux)	Any	Untested	
Opera (Any OS)	Any	Untested	Untested although newer webkit based version (11.0+) may work
Puffin (IOS/Android)	Any	Untested	Will work with some advanced manual setup, but poor end User experience

Accessing the Server

Once you have ensured you have a browser that supports the Vicon Access Control software, accessing the Vicon Access Control 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 Vicon Access Control From the PC the Server Software is Installed on:

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

Windows 8/8.1 Users

Windows 8/8.1 hides the shortcut by default within the Metro UI start screen. The shortcut can be located by typing 'Launch' within the start screen and selecting 'Launch VAX'. If you wish, you can pin this shortcut permanently to your start screen by right clicking and selecting 'Pin To Start.'

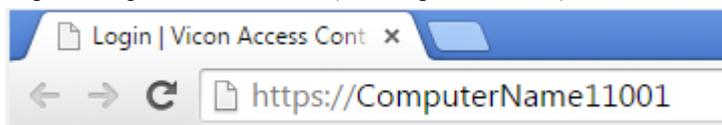
Accessing Vicon Access Control From a Remote PC:

Open your web browser and within the address bar enter the address of the Vicon Access Control 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 Vicon Access Control server remotely

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



Once you have entered the address, press Enter to navigate to the Vicon Access Control 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 Vicon Access Control 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 Vicon Access Control 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 Vicon Access Control 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 Vicon Access Control

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

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

Download the Latest Version of VAX

Visit our VAX downloads page at:

<http://www.vicon-security.com/software-downloads-library/vax-access-control-software>

You'll be prompted for information in order to download.

Prerequisite Installation

In order to upgrade Vicon Access Control, the following requirements will need to be met.

- Upgrade must be performed on the computer that Vicon Access Control is currently installed on.
- You must be logged in as the same Windows Login that installed Vicon Access Control (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 Vicon Access Control software is identical to that of a fresh install. (Please, see the section called “Installation Procedures”). We recommend doing a backup of your Vicon Access Control database prior to upgrading. For more information about backing up your database, please see the section called “Backing up your Vicon Access Control Database”. We also recommend stopping the Vicon Access Control web 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 Vicon Access Control, 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 Vicon Access Control 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 2.1. Firmware Out of Date Notification

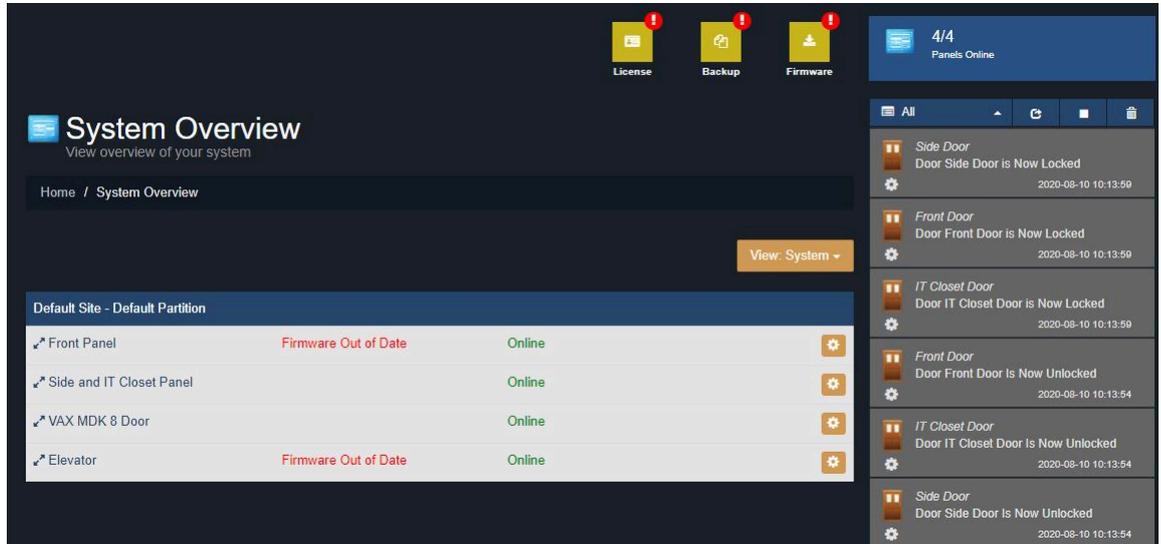


2. In order for a Panel to have its firmware updated we must place it into Firmware Update Mode. To do this we will navigate to the System Overview page in the software. Click on the "x/x Panels Online" box above the Notifications area or on the home page, scroll down to the section titled **System**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

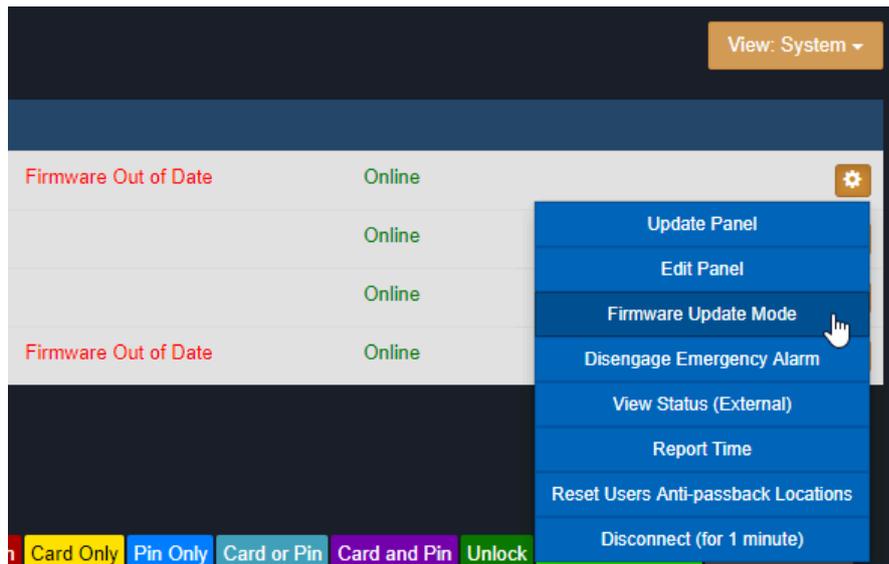


3. On the System Overview you will see a list of all Panels in your system. Any Panels that require a firmware update will have a message displayed next to its name.

Figure 2.2. 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 orange 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**

As of version 2.9.53, you can perform multiple firmware updates at the same time if needed.

5. The Vicon Access Control 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.

Frequently Asked Questions

Q: How can I check if my Windows login can upgrade Vicon Access Control?

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

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 Vicon Access Control.

Figure 2.3. Command Prompt: Backup

```

SQLCMD
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>SQLCMD -S .\VAX
1> USE VAX
2> GO
Changed database context to 'VAX'.
1>

```

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 Vicon Access Control.

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

A: Due to the manner that SQL database permissions work, when Vicon Access Control 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.

Chapter 3. Initial Configuration

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

Initial Software Configuration

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

Access the Vicon Access Control 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 Page. At this point you'll want to fill out the displayed form with the information required to setup your initial database. It is divided into 5 sections, Connection Configuration, Customer Configuration, Dealer Information, Initial Administrator and Email Settings. Email Settings and Dealer Information are optional.

VAX ACCESS CONTROL

Connection Configuration

Server Address* **How to Choose**

- If all panels are on the same network as the server, select **Ethernet Adapter** or **Computer Name**.
- If panels are connecting over the internet, select **Public IP Address**
- If you're using a domain name or dynamic DNS, select **DNS Name**

Type	Address
<input checked="" type="radio"/> Realtek PCIe GBE Family Controller	192.168.2.10

Warning Server is using DHCP to obtain an IP address. We recommend configuring the server with a static IP or DHCP reservation to prevent the IP from changing.

Public IP Address 178.210.133.102

Computer Name VAX

DNS Name 192.168.2.43

* Server Address field can be changed later under System Settings.

Customer Configuration

Name Required

Description Optional Description

Initial Site Time Zone (UTC-05:00) Eastern Time (US & Canada)

System Language English

Dealer Information

Dealer Information is optional but recommended

Dealer Name	<input type="text" value="Dealer Name"/>
Dealer Phone Number	<input type="text" value="XXXXXXXXXX"/>
Dealer Website	<input type="text" value="Website URL"/>
Dealer Email	<input type="text" value="Dealer@Email.Com"/>

Initial Administrator

Username (Email)	<input type="text" value="Required ex: user@domain.com"/>
First Name	<input type="text" value="Required"/>
Last Name	<input type="text" value="Required"/>
Password	<input type="text" value="Required"/>
Confirm Password	<input type="text" value="Required"/>

Email Settings

Email settings optional but recommended. They are used for email notifications and password resets.

SMTP Server	<input type="text" value="Required if using SMTP"/>
SMTP Server Port	<input type="text" value="25"/>
Requires SSL	<input type="checkbox"/>
Reply Address	<input type="text" value="user@email.com"/>
Username	<input type="text" value="Optional"/>
Password	<input type="text" value="SMTP Password"/>
Send Test Email	<input type="checkbox"/>

[Create Customer](#)

Connection Configuration

Table 3.1. Connection Configuration Fields

Field	Brief Description
Server Address	This selection is what is pushed to your VAX Panels and dictates how they communicate with the server. Local static IP recommended if controllers are communicating locally. Public static IP or DNS/domain name recommended if controllers are communicating over the internet.

Customer Configuration

Table 3.2. 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.
System Language	Software interface language. Choose from English, French, Spanish. Language of notifications is decided during software installation.

Dealer Information

Note

Dealer Information is optional, but recommended.

Table 3.3. 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: 18006459116)
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: http://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.

Initial Administrator

Table 3.4. Initial Administrator Fields

Field	Brief Description
Username (Email)	This is the email address/Username of the primary Vicon Access Control Administrator. This email address will be used to login to the site initially. You may create additional Administrator accounts after initial configuration, each with unique roles and system access.
First and Last Name	The first and last name of the primary Vicon Access Control Administrator.
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.

Email Settings

Note

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

Table 3.5. 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.

Field	Brief Description
Password	This is the password required for authenticating and sending email via SMTP.

Note

After initial configuration, you'll be able to test your email notifications to see if it is correct; please see the section called “Email Configuration”.

Once all required fields have been set, click **Create Customer** to continue. If everything entered was valid, Vicon Access Control will automatically create and setup your database for use.

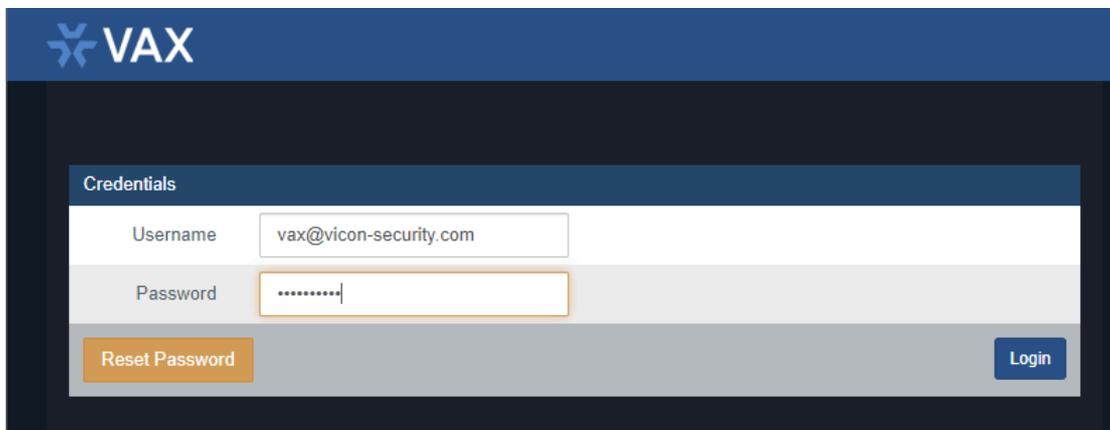
Congratulations! You are now ready to start configuring your access control system. We can now move on to configuring the Panels to communicate with the server.

Logging Into Vicon Access Control Web Interface

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

Figure 3.1. Vicon Access Control Login Screen



Password Recovery in Vicon Access Control

In the event that you are unable to remember or misplace your password to login to Vicon Access Control, you may go through the password recovery process by clicking the orange **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. 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 3.2. Password Reset Page

The screenshot shows the VAX web interface for password reset. It features a dark blue header with the VAX logo. Below the header, there are two main sections. The first section, titled 'Reset Password', contains a text input field for 'Username', a 'Return to login' button, and a 'Request Reset' button. The second section, titled 'Reset Password Confirmation', contains four text input fields: 'Username', 'Confirmation Code', 'Password' (with placeholder text 'Enter a Password'), and 'Confirm Password' (with placeholder text 'Confirm the Password'). This section also includes a 'Return to login' button and a 'Confirm Reset' button.

Panel Initial Configuration

This section will cover common initial configuration of Vicon VAX-1D-1/VAX-2D-1 PoE and VAX-MDK style door, elevator and input/output controllers. VAX-MDK style controllers are also utilized in Altronix TROVE kits such as the VAX-TROVE-2DR and VAX-TROVE-16DR. This section is focused on configuring communication information manually into the Panel so that it can connect to the Vicon Access Control 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 Vicon Access Control 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 **Vicon Access Control Server**. Note the IP address or name of the Vicon Access Control 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 Panel should either be mounted at its intended location or temporarily accessible physically near the Vicon Access Control server with a Cat5e/6 cable (non-crossover) connected directly to either a PoE Injector or powered network switch (Note: Maximum cable run from Vicon Access Control VAX-1D to injector or powered switch is 100 meters or 330 feet). In the case of a VAX-MDK Panel, 12-13.5 VDC power should be plugged in and the Cat5 should be connected to network that can reach the Vicon Access Control 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

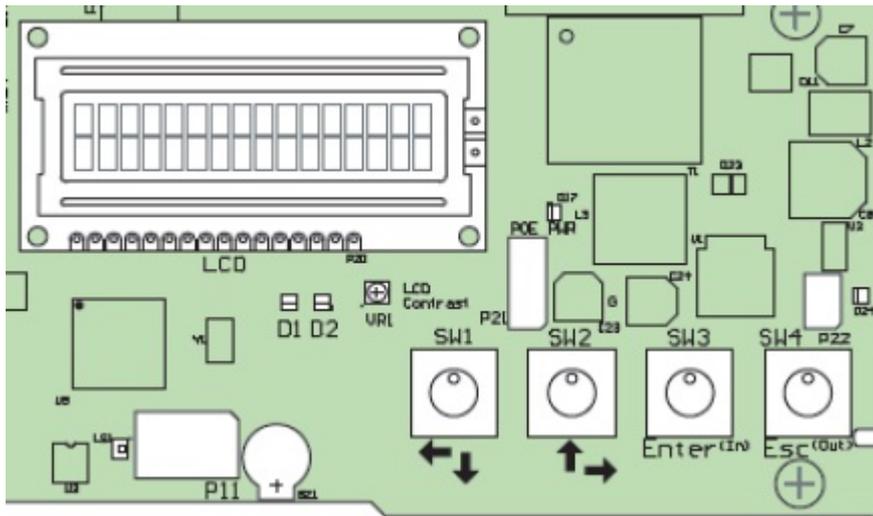
- The **Static IP** or **Server Name** of the Vicon Access Control server.

- 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 Vicon Access Control controller for accessing, viewing and configuring a Panel.

Figure 3.3. Panel Buttons (same button layout on VAX-1D-1/VAX-2D-1 PoE and VAX-MDK style 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. This may sound overwhelming but once you've configured a couple Panels it becomes second nature.

To quickly see how the Panel is currently configured (READ ONLY), hold the ESC (SW4) button for 4 seconds or until the Panel speaker 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 Vicon Access Control 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 communication 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.



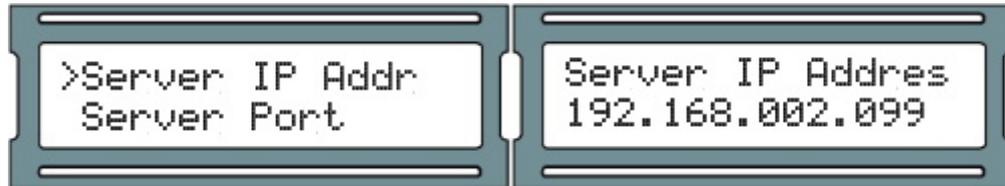
5. You will be presented with a message stating 'CHANGE CONFIRM?' and have two options: YES via pressing the ENTER button or NO via pressing the ESC button. If you wish to commit that setting to the Panel, press the ENTER button. You will now be presented with message indicating 'CHANGED'. Pressing the 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 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 '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 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 Vicon Access Control 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 communication 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.



- 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).



- 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.
- 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.)



- 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.

- 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 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 be 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.



- 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 (MDK Models)

This section includes detailed instructions on performing an Output test on 12VDC powered VAX-MDK door or IO controllers.

- 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'.



- 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.)



- 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.



- On VAX-MDK 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 3.8. 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-STR-2).
3: PRS_TDM	Select this option if the connected expander boards are two door expanders (VAX-MDK, VAX-EXP-2D).

Menu Option	Description
4: PRS_IO8_All	This option will allow you to test relays on multiple IO expanders at once (VAX-IO-STR-2).
5: PRS_TDM_All	This option will allow you to test relays on multiple two door expanders (VAX-MDK,VAX-EXP-2D).



- After selecting a Board Type, you will now choose a Board Address. Currently supported addresses are 1-4 for VAX-EXP-2D expanders and 1-8 for VAX-IO-STR-2 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.



- 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.



- 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)

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

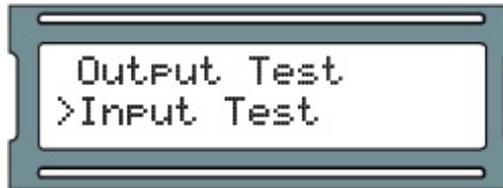
- Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.



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-MDK Models)

This section includes detailed instructions on performing an Input test on 12VDC powered VAX-MDK door or IO controllers.

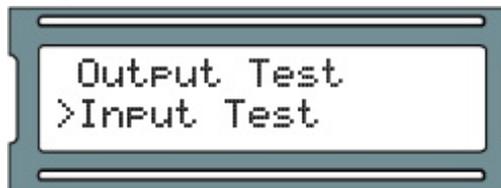
1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.



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 VAX-MDK 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.
2: PRS_IO8	Select this option if the connected expander boards are IO expanders (VAX-IO-STR-2).
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 addresses are 1-4 for VAX-EXP-2D expanders and 1-8 for VAX-IO-STR-2 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 Controllers)

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

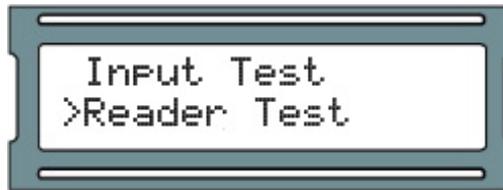
1. Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.



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.)



- 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.



- 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.



- 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.



- 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 Controllers)

This section includes detailed instructions on performing a Reader test on 12VDC powered VAX-MDK door controllers.

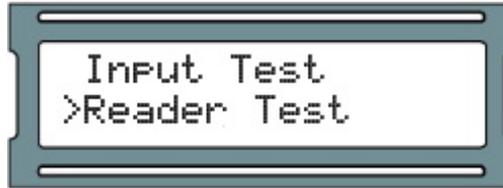
- Press and hold the ENTER (SW3) button on the Panel for approximately 3-4 seconds until you are presented with 'SETUP PASSWORD?' on the LCD screen and '0000'.



- 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 VAX-MDK 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 addresses are 1-4 for VAX-EXP-2D 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 VAX-ELV-STR-1 and VAX-IO-STR-2 style 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. Most Panels (not all) have a MAC address that starts with '001EXXXXXXXXXX'. 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 3.4. Panel HTTP Configuration Overview

ODM PANEL
PANEL6101

Door Access Panel
Overview

Overview

Panel Setup

Panel	
Name:	Front Panel
Area:	Default Site
Time:	2020,08,10 10:19:43
Firmware Version:	ODM V19083007 *
Run Mode:	Normal
Communication Mode:	DHCP Client
Connection Type:	Wired
Assigned IP:	192.168.002.128
MAC Address:	801F12A097D5

Server	
Name:	SERVER-PC
IP Address:	192.168.002.043
Port:	9876
Connection Mode:	Server IP

Door 1	
Mode:	Card
State:	Closed
Lock State:	Locked
Internal Motion:	Disabled
External Motion:	Disabled
Outside Reader:	Not exist
Inside Reader:	Reader 1

* Press F5 to update or click:

There are multiple 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 Vicon Access Control software. If changing communication methods in the interface, we advise making those same changes in the Vicon Access Control software. The **Panel Setup** screen should only be used for initial configuration or when the server information has changed.

Adding a Panel to Vicon Access Control

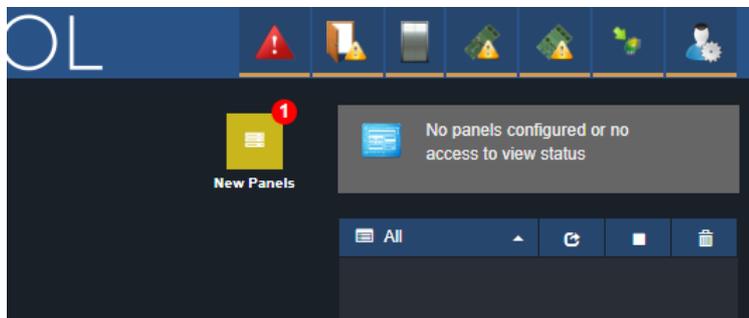
This section will cover the basic process of adding a Panel in Vicon Access Control. In most deployments it is a fairly easy process and can be done in two different ways.

Method 1: Adding a Panel via 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 Vicon Access Control server.)

1. Access your Vicon 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. On the **Home Screen** you will see an icon titled **New Panels** near the top of the screen. Click on this icon and you will be taken to the Unknown Panels screen. You can also access the Unknown Panels screen directly from the home screen in the Hardware section.



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.

 A screenshot of the 'Unknown Panels' screen. The title is 'Unknown Panels' with a subtitle 'View unknown panel list'. Below the title is a breadcrumb trail: 'Home / Panels / Unknown Panels'. The main content is a table with the following data:

Unknown Panels							
Name	MAC	IP Address	Type	Firmware	First Attempt	Last Attempt	
+ No Panel Name	5410ECD7DDA0	192.168.2.165	VAX-2D	08/30/2019	08/10/2020 10:41:50 AM	08/10/2020 11:11:54 AM	

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 Vicon 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 section called “Panel Model Reference”).
- 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 Vicon 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. On the **Home Screen**, scroll down to the section titled **Hardware**, click on the **Panels** icon (pictured below).



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

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

Figure 3.5. Add Panels Screen

Home / Panels / Add Panel

Panel

Panel Model: VAX-1D
Over The Door Module with POE Power

Name: Front Door

Description: Optional Description

Site: Default Site

Mac Address: 0004A3BE48F

Panel Password: 0000

Tamper Sensor:

Door Contacts:

Auto Add Doors:

TCP Connection

Connection Mode: Automatic (DHCP)

Undo Save

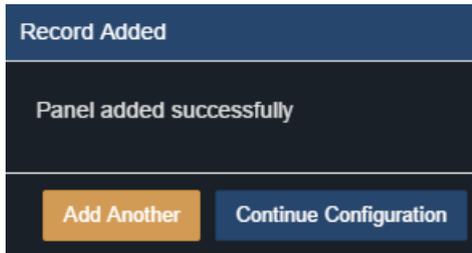
The following table describes the common fields.

Table 3.11. Add Panel

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'.
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.

Drop-down/Text Box/Checkbox	Description
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).

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 **Panel Added Successfully** with the options to **Add Another** (which will take you back to the **Add Panel Screen**) or **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").



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 Vicon Access Control 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 Vicon Access Control, please see Chapter 6, *Planning an Access Control Deployment*. It contains a lot of 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 Vicon Access Control, information about the licensing process, how card formats work with our product license, and frequently asked questions about licensing your software.

Vicon Access Control is a licensed product. Licensing helps us continue to develop and add new features to Vicon Access Control. 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 Vicon Access Control license, your system is also entitled to free core software updates.

Note

Vicon Access Control includes a 30 day trial license on first install.

Licensing Your Software

Activating the software license on your Vicon Access Control is designed to be a very straight forward and painless process.

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **System**, click on the **Licensing** icon (pictured below).



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. Vicon Access Control Licensing Screen

Licensing
Manage licensing

Home / Licensing

Licensing Info

Minimum Package	Small
Status	Trial
Account Number	<input type="text"/>
Expires On	09/05/2020
Package	Enterprise
Features	

License Options

Option	In Use	Active Package	Minimum Package
		Enterprise	Small
Max Doors	9	Unlimited	80
Max Cameras	0	Unlimited	80
Max Partitions	1	Unlimited	5
Supports Elevator Panels	Yes	Yes	Yes
Supports I/O Panels	No	Yes	Yes
Supports LDAP	No	Yes	Yes
Supports Monitored Doors	No	Yes	Yes

[Update My License](#)

- 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.
- 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.
- To generate a new license click the '**Update My License**' button at the bottom of the screen.
- You will be presented with your new **Request Key**. Contact your dealer, installer or Vicon (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.

Update License

Request Key
PQHFF-00030-8C690-RLBHI-348B7

Response Key

[Cancel](#) [Update](#)

9. Once you have entered the **Response Key** provided by Vicon, 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 42 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. 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 Vicon Access Control 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 if 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.

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 Time Zones
- Viewing Cameras
- Viewing Reports

Q: Why does Vicon Access Control 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 Vicon Access Control feature set are offered a price inline with what they need.
- To allow us to continue to upgrade and enhance the base Vicon Access Control 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: Contact Vicon for these details (please, see Chapter 37, *Support*).

Q: What does a Vicon Access Control license entitle me to?

A: An active Vicon Access Control license is always required to use the Vicon Access Control 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 Vicon Access Control software?

A: Upon restoring a Vicon Access Control 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 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 Vicon Access Control 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".

Windows 8/8.1 Users

Windows 8/8.1 hides the shortcut by default within the Modern UI start screen. The shortcut can be located by typing 'Launch' within the start screen and selecting '**Launch VAX System Manager**'. If you wish you can pin this shortcut permanently to your start screen by right clicking and selecting 'Pin To Start'.

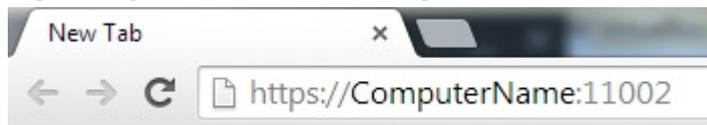
Accessing System Manager UI from a Remote PC

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 Vicon Access Control **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

Service Name	Status	Actions
VAX Web Server	Running	Restart Stop
SQL Server (VAX)	Running	Restart Stop

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 'viconaccess') followed by the new password twice.
4. Click '**Change**' to complete the password change procedure. This password only affects the System Manager UI, it is separate from your VAX login.

Backing up your Vicon Access Control 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 Vicon Access Control 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 than 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 section called "Installation Procedures" 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

File	Date	Size
vax_20170125142048.prbak	2017-01-25 02:20:48 PM	298.00 MiB
VAX_20160921105917.prbak	2016-09-21 10:59:17 AM	7.44 MiB

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

- 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 2015 would be called "Vax_20150325010349.prbak".

Restoring from Backup File

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

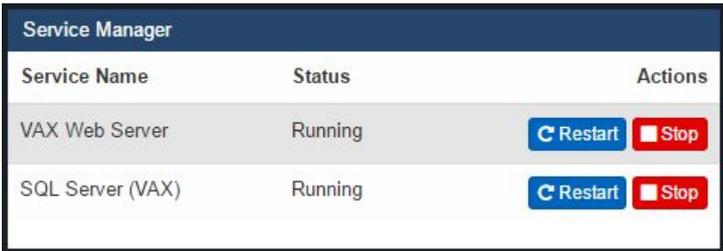
Service and System Management

The **System Manager UI** allows for control over the Vicon Access Control web server service and the SQL Server service being used by Vicon Access Control. 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

- Click on '**System**' in the top menu when logged into the system manager UI.
- You will see a Service Manager section for the VAX Web Server and SQL Server.

Figure 5.6. Managing Services



Service Name	Status	Actions
VAX Web Server	Running	 
SQL Server (VAX)	Running	 

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

Shutting Down or Restarting Your Server

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



- 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.

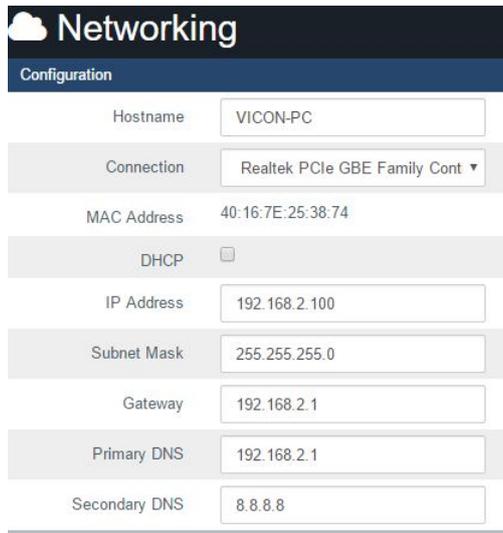
⚠ Caution

Changing network settings can cause a loss of connection to the System Manager and the Vicon Access Control 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



Networking	
Configuration	
Hostname	VICON-PC
Connection	Realtek PCIe GBE Family Cont ▾
MAC Address	40:16:7E:25:38:74
DHCP	<input type="checkbox"/>
IP Address	192.168.2.100
Subnet Mask	255.255.255.0
Gateway	192.168.2.1
Primary DNS	192.168.2.1
Secondary DNS	8.8.8.8

📄 Note

Changing your hostname will require a system restart.

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 Vicon Access Control 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. For more detailed visual guides to connect devices such as Door Strikes, Readers and other peripherals to our Panels, please see the section called “Visual Guides”.

Hardware

This section will go over hardware specifications, the communication topology of how our Panels interact with the Vicon Access Control 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 two-door expander board. Requires VAX-MDK-Master for communication and power distribution. Communicates on RS485 bus.
VAX-IO-EXP8-PCB	12VDC powered 8 I/O expander board. Requires VAX-MDK-Master for communication and power distribution. Communicates on RS485 bus.
VAX-MDK-Master (multi door kit)	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. VAX-MDK-Master is also utilized in TROVE multi door kits

Hardware Specifications

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

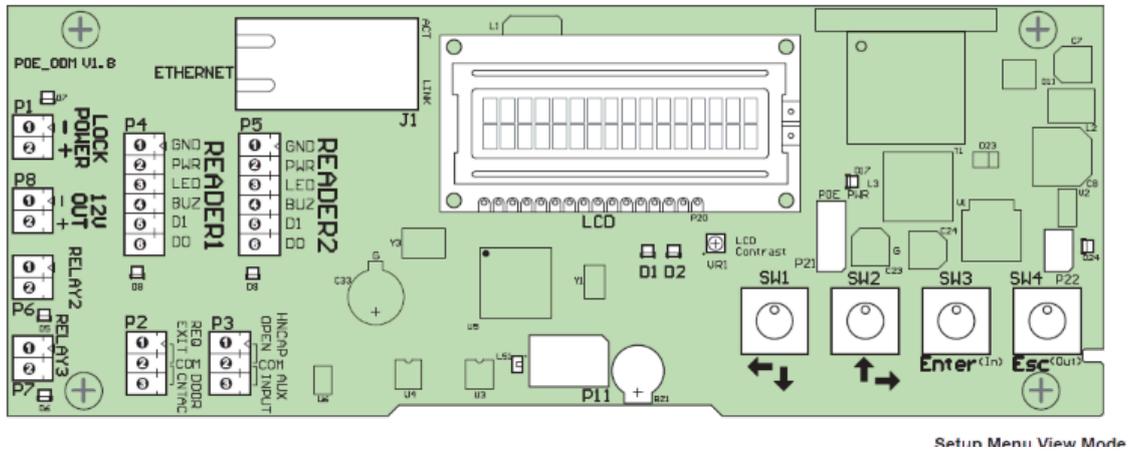


Table 6.2. Hardware Specifications VAX-1D-1/VAX-2D-1

Category	Item and Description
Power	
Supply	802.3af PoE (providing up to 15.4 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

Planning an Access
Control Deployment

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 Paintable
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 relay that can handle large loads such as maglocks
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

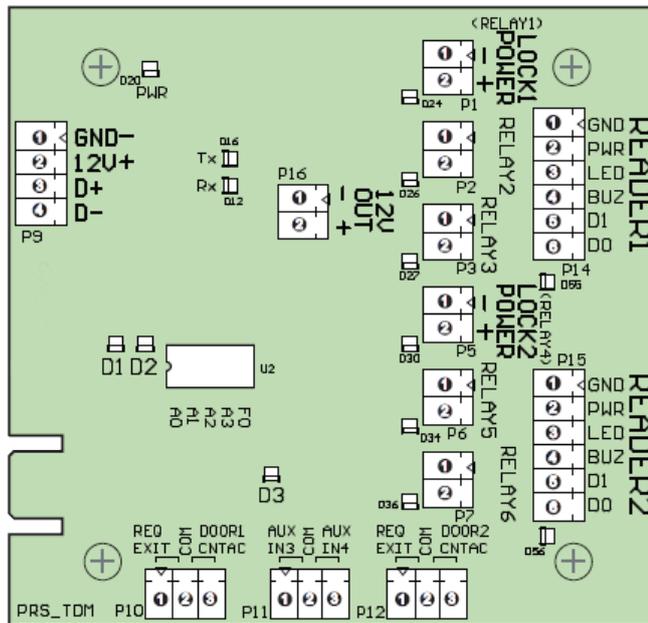


Table 6.3. Hardware Specifications VAX-EXP-2D

Category	Item and Description
Power	
Supply	1 x 12VDC power input provided by VAX-MDK-Master 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-Master. 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	

Category	Item and Description
12VDC input	In-Rush Current Limit and Overall Current Limit
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-STR-2

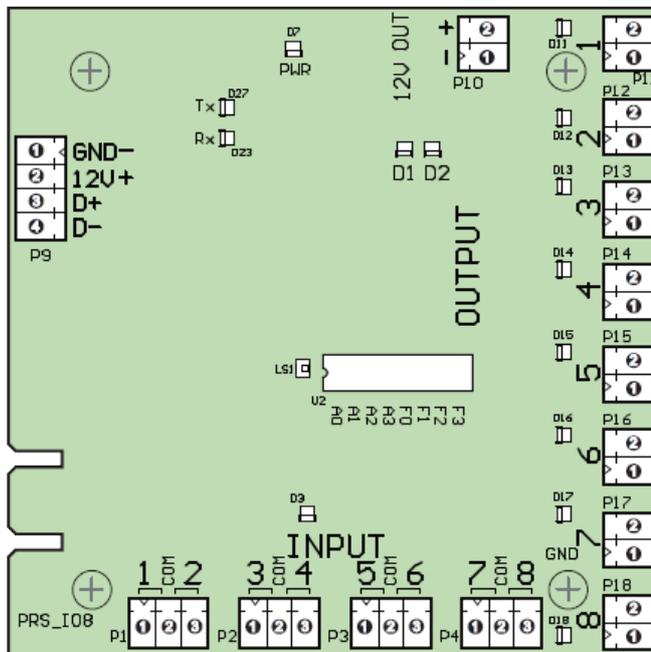


Table 6.4. Hardware Specifications VAX-IO-STR-2

Category	Item and Description
Power	
Supply	1 x 12VDC power input provided by VAX-MDK-Master 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-Master. 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

Category	Item and Description
User Interface	
LEDs	1 x Power Indicator 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-Master

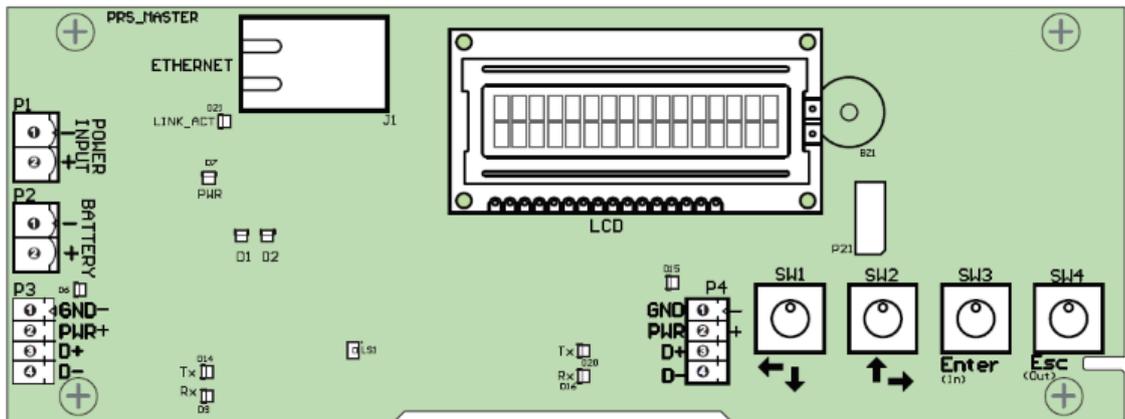


Table 6.5. Hardware Specifications VAX-MDK-Master

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-STR-2 or VAX-EXP-2D-modules. Up to 2.5A per output. 5A total.
Network	
Speed	10/100 Mbps
Modes	Static or DHCP
MAC	Unique

Category	Item and Description
Communication	2 x RS485 outputs for communication to up to 4 VAX-EXP-2D modules or 8 VAX-IO-EXP8-PCB modules.
User Interface	
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 Vicon Access Control deployment.

Vicon Door and Elevator 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.

VAX-MDK style controllers 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.

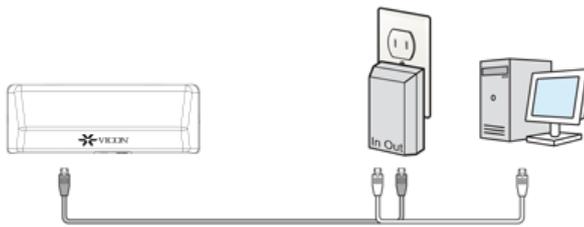
PoE Power. PoE Power may be supplied directly by switch or, alternatively, injected via single port injector between switch/router and the controller.

 : PoE Powered

 : Normal

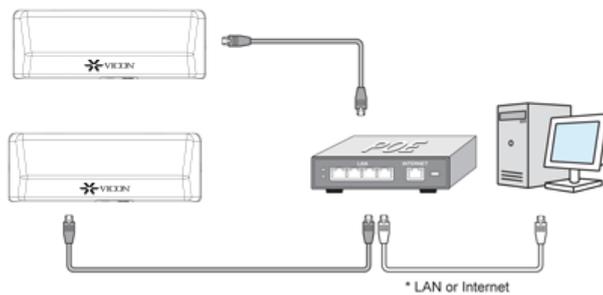
Controller - PoE Injector - PC (direct). In this scenario, the controller is being powered by a PoE injector which is connected right to the Vicon Access Control server. Scenarios like this happen a lot when there isn't very much network infrastructure to work with.

Controller-PoE Injector- VAX Server (direct)



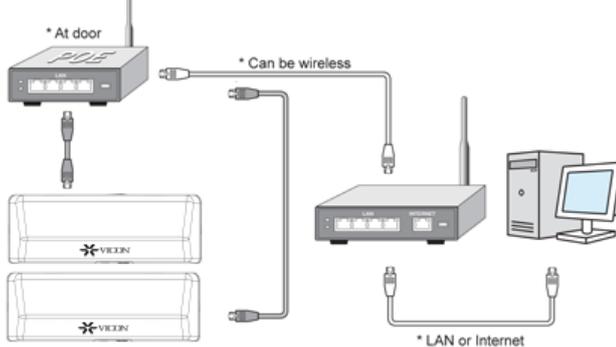
Controllers - PoE Switch/Router - PC. This is a more typical scenario and is seen quite often in the field. The controllers are powered by a PoE switch (located in a closet or electrical room), which connects to the on-site server using the site's existing network infrastructure, or an off-site server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

Controllers-PoE Switch-VAX Server



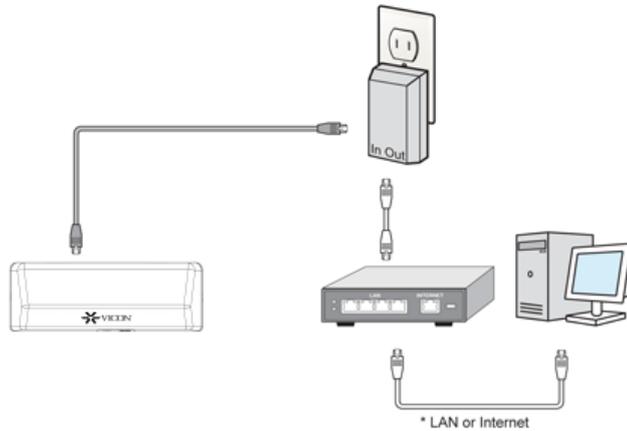
Controllers - PoE Switch (at Doors) - Router/Switch - PC. In this scenario the controllers are powered by a PoE switch (above/near the door), which connects (wireless or a single cable) to the site's existing network infrastructure, or an off-site server via an internet connection. This topology is used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

Controllers-PoE Switch-Wan/LAN-VAX Server



Controller - PoE Injector - Router/Switch - PC. In this scenario, the Vicon Controller is being powered by a PoE injector which 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.

Controller-PoE Injector-Switch/Router-Vax Server



As you can see, Vicon Door and Elevator controllers can be very flexible in how they are deployed to a site, and various Panels/Controllers 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 Access Control 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	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 Door Master Power Requirements

This section will go over power requirements of the VAX-MDK style panels.

The VAX-MDK Door Master 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-Master controller to connected VAX-EXP-2D expansion modules via the VAX-MDK-Master 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-Master 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-Master (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:

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

Example 6.1. VAX-MDK 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: $(2 \text{ VAX-EXP-2D} \times 10\text{mA}) + (4 \text{ readers} \times 80\text{mA}) + (4 \text{ strikes} \times 380\text{mA}) + (0 \text{ devices} \times 0\text{mA}) = 1860\text{mA} (1.86\text{A})$

Bank #2: $(2 \text{ VAX-EXP-2D} \times 10\text{mA}) + (4 \text{ readers} \times 80\text{mA}) + (4 \text{ strikes} \times 380\text{mA}) + (0 \text{ devices} \times 0\text{mA}) = 1860\text{mA} (1.86\text{A})$

With each bank consumption now determined, the minimum estimated UL Listed external power supply current availability for a VAX-MDK-Master is calculated as indicated below: $(\text{Bank \#1} + \text{Bank \#2}) + ((\text{Bank \#1} + \text{Bank \#2}) \times 10\%) + 10\text{mA}$

Minimum Power Supply Current Rating = $(1.86 + 1.86) + ((1.86 + 1.86) \times 10\%) = 4092\text{mA} (4.09\text{A})$

Identifying a Panel

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

Vicon carries 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-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
VAX-2D-1	2	2	No	Two-Door controller with PoE power
VAX-2D-REX	2	2	Yes	Two-Door controller with PoE Power and Integrated Motion
VAX-MDK-Door-Master (MD-K_MASTER)	8	8	No	1-8 door controller traditional style mounted in steel enclosure. Up to 8 doors with Appropriate amount of VAX-EXP-2D two door expansion boards. Powered via external 12VDC power supply.
VAX-MDK-Door-	8	8	No	1-8 door controller traditional style mounted in steel enclosure. Up to 8 doors with Appropriate

Model	Max Doors	Max Readers	Motion REX	Brief Explanation
Master-OSDP (MD-K_MASTER)				amount of VAX-EXP-2D-OSDP two door expansion boards. Powered via external 12VDC power supply. OSDP and wiegand readers supported.
VAX-EXP-2D	2	2	No	Two door expansion module. Connect up to 4 total to VAX-MDK-Door-Master style controllers. Wiegand readers supported.
VAX-EXP-2D-OSDP	2	2	No	Two door expansion module. Connect up to 4 total to VAX-MDK-Door-Master-OSDP style controllers. OSDP and wiegand readers supported.
VAX-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-ELV-STR	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. PoE power.
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-Master Panel with 8 IO-Boards. Powered via external 12VDC power supply.
VAX-IO-STR	N/A	0	N/A	Supports general Input/Output devices in various use cases and configurations. Up to 64 Inputs/Outputs per IO-Master Panel with 8 IO-Boards.
VAX-IO-EXP8PCB	N/A	0	N/A	Daughter-boards that increase the amount of Inputs/Outputs or Elevator floors when attached to VAX-ELV-STR, VAX-IO-STR-2 or VAX-ELV-STR systems.

All Vicon Panels are fully tested prior to shipping, and after the testing is successful the Panel receives the Vicon 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 Vicon Access Control. 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 Vicon Access Control is fairly flexible, however there is a general order of operations that should be adhered to.

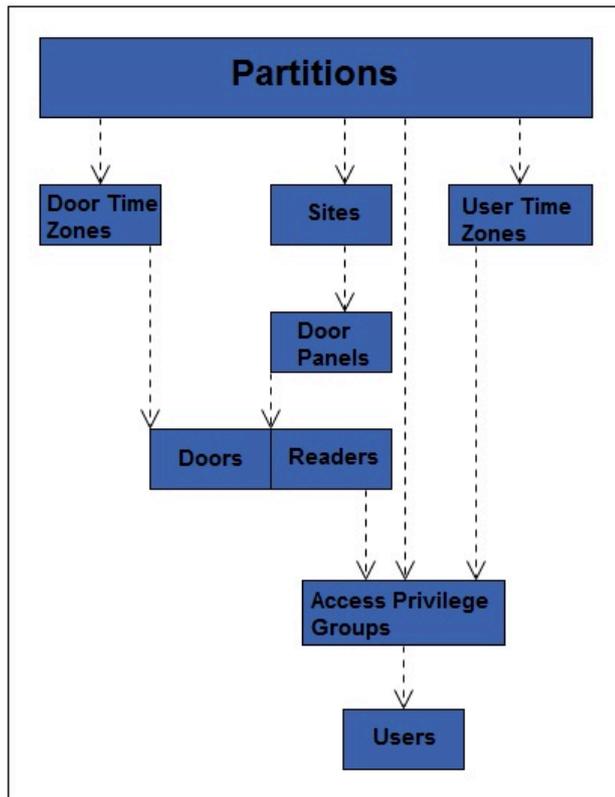
This table is meant as an overview and general guideline for the order of configuration. Each item will go into more detail later in this chapter.

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 Time Zones	Configure additional Door/Floor Time Zones if required; can be done before or after Doors and Elevators are added. We recommend doing it before.	Default Door Time Zones "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 Time Zones 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 Time Zones	User time zones must be configured after Partitions, and before Access Privilege Group.	Default User Time Zones "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 Time Zones, 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. Vicon Access Control Order of Configuration



Partitions

In this section we will cover the basic concepts of **Partitioning** within the Vicon Access Control. 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 Vicon Access Control, 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 Vicon Access Control 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 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 Vicon Access Control Panels configured in three different schools (A, B and C), with a single Vicon Access Control 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 Vicon Access Control 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 door controllers 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 Vicon Access Control.

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 time zones, it is recommended to separate those Panels into separate Sites; this will ensure the Panels always report events in the time zone 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 Vicon Door Panels. By utilizing Sites, each building can be its own Site and objects such as User Time Zones, Door Time Zones, 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 Time Zones and Access Privilege Groups.

Example 2: Municipal Government. A town government has chosen to use Vicon Access Control to manage their doors in offices and facilities. Using Sites, the building manager creates a Site for the0

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 Time Zones

In this section we'll cover the concepts of **Door Time Zones** within Vicon Access Control and a couple examples of Door Time Zones that are used in the field. For configuration of Door Time Zones, please see Chapter 9, *Door Time Zone Configuration*.

Concepts

Door time zones are how we can configure the Doors to behave, and when we want them to behave that way. Door time zones in Vicon Access Control 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 Time Zone 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 time zone schedule, the resultant action is that the Door using this time zone 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 time zone schedule, the resultant action is that the Door using this time zone 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 time zone schedule, the resultant action is that the Door using this time zone 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 time zone schedule, the resultant action is that the Door using this time zone 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 time zone schedule, the resultant action is that the Door using this time zone 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 time zone schedule, the resultant action is that the Door using this time zone 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 time zone schedule, the resultant action is that the Door using this time zone 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 time zone 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 time zone schedule, the resultant action is that the Door using this time zone is now in a secure state (locked). In order for access to be granted, two valid credentials must be 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 Time Zone Factors. Factors to keep in mind when planning your Door Time Zones 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 Time Zone?

Planning a Door Time Zone. 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 Time Zone, and can be applied to multiple Doors.

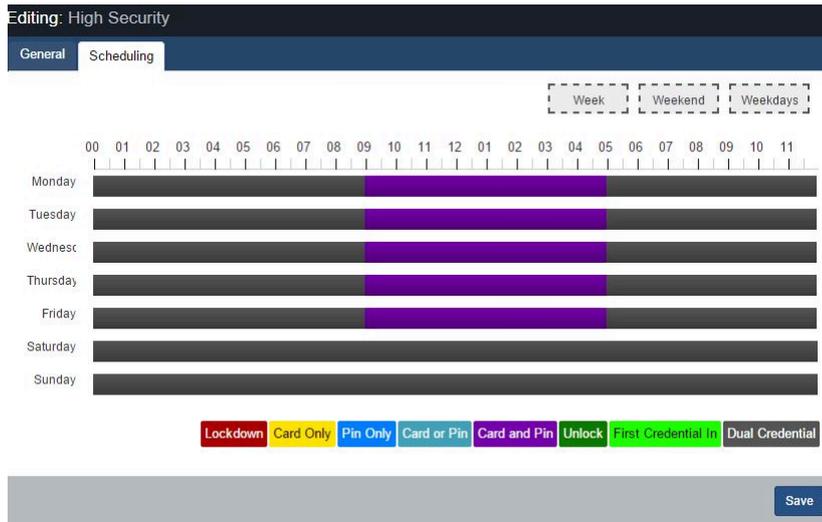
Examples

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

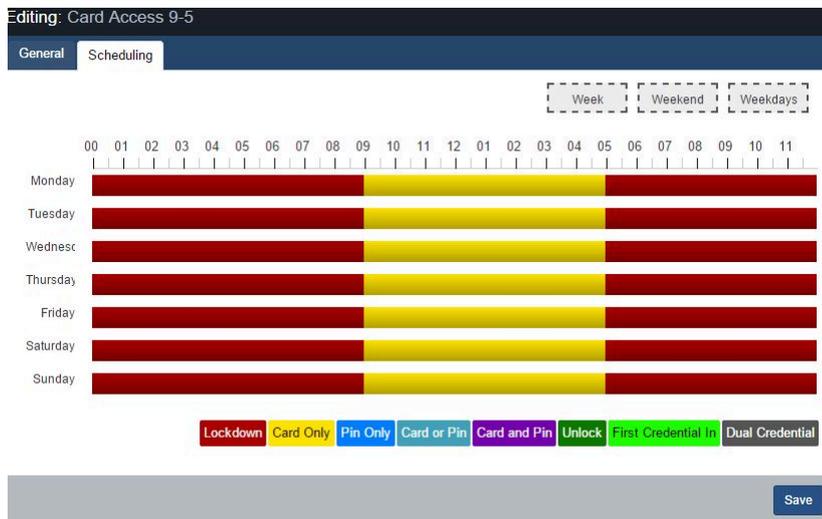
Example 1: Grocery Store Public Entrance. In this example, we have a Door Time Zone that will be assigned to the front public Door of a grocery store; it is set up to **Unlock** during store hours, and card only otherwise for staff.



Example 2: Data Center Door. In this example, we have a high security Door Time Zone that will be assigned to data center entrance; this time zone 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 Time Zone that will be assigned to the front Door of an office. This is one of the default Door Time Zones included in Vicon Access Control.



User Time Zones

In this section we'll cover the concepts of **User Time Zones** within Vicon Access Control and an example of a User Time Zone. For configuration of User Time Zones, please see Chapter 10, *User Time Zones*.

Concepts

Similar to Door Time Zones, User Time Zones 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 Time Zones** are applied to **Access Privilege Groups**, as opposed to **Door Time Zones**, which are applied to **Doors**.

Note

By default, Vicon Access Control comes with 3 default User Time Zones ('No Access', 'Always Access' and 'Access 9am to 5pm'). These User Time Zones 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 Time Zone "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 Vicon Access Control. For instructions on how to configure Access Privilege Groups, see Chapter 11, *Access Privilege Groups*.

Concepts

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

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

Planning Your Access Privilege Groups

An important concept that makes Vicon Access Control 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 Vicon Access Control, 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 Vicon Access Control. This section will cover concepts and some examples. For configuration of Holidays please see Chapter 13, *Holiday Configuration*.

Holidays within Vicon Access Control 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 time zones (User Time Zones and Door Time Zones), Holidays have 2 time zones called **Door Holiday Time Zones** and **User Holiday Time Zones**. In large deployments such as those spanning multiple countries, it can be very flexible.

Note

On the day of the Holiday, Door Holiday Time Zones and User Holiday Time Zones 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 Time Zones. Door Holiday Door Time Zones define the schedule a Door will follow on a Holiday. The schedule configuration is very similar to the regular Door Time Zone schedule configuration. All normal Door states are present and can change up to 4 time in a schedule. By default, Vicon Access Control comes installed with one Door Holiday time zone called '**Closed During Holiday**' with a schedule of lockdown 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, Vicon Access Control comes installed with two Door Holiday Groups: '**Standard Holidays**' and '**No Holidays**'.

User Holiday Time Zones. User Holiday Time Zones define a schedule a User account will follow on a Holiday. The schedule configuration is very similar to the regular User Time Zone schedule configuration. Available User modes include: '**Not Allowed**' and '**Allowed**'. By default, Vicon Access Control 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 Time Zone schedules Users will follow on a Holiday. This is assigned to Users via Access Privilege Group when created or edited. By default, Vicon Access Control 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 Time Zones (similar to Door Holiday Time Zones)

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 Time Zones). By default, Vicon Access Control 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 Time Zone** set as '**Closed During Holiday**'. As you can see, the default Door Groups and Time Zones 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.

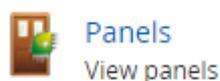
Chapter 7. Setting up Your Panel

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 Vicon 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. On the **Home Screen**, 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 six 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:

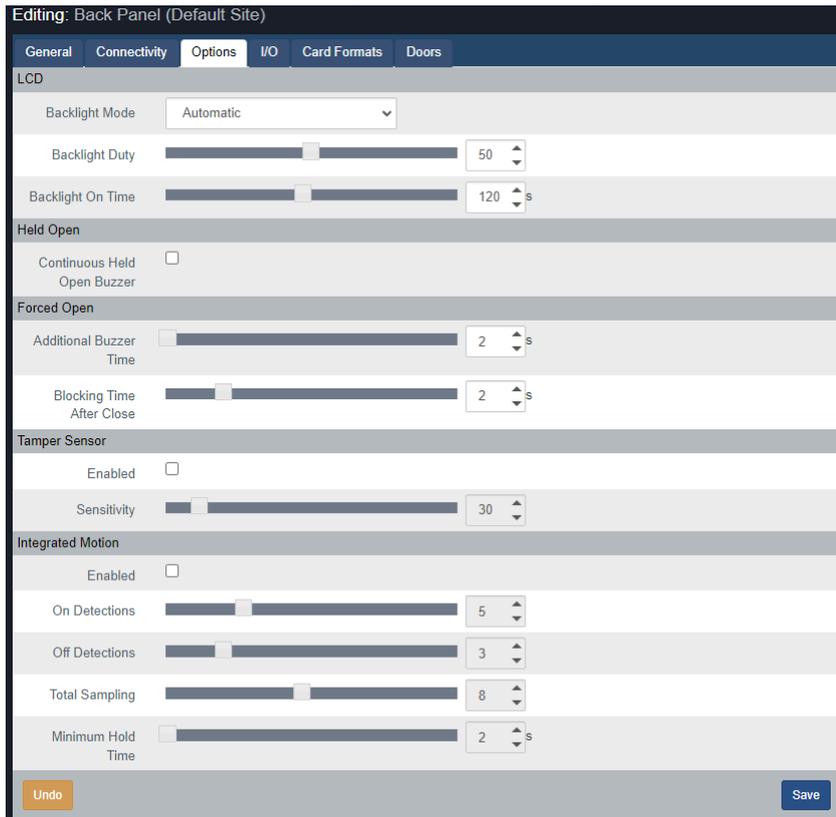
Table 7.1. Add Panel

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.
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).

Drop-down/Text Box/Check box	Description
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 5 sections: **LCD**, **Held Open**, **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 textbox next to the slider to manually enter a value.

Table 7.2. 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.
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	

Configuration Item	Description
Continuous Buzzer	Held Open 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.

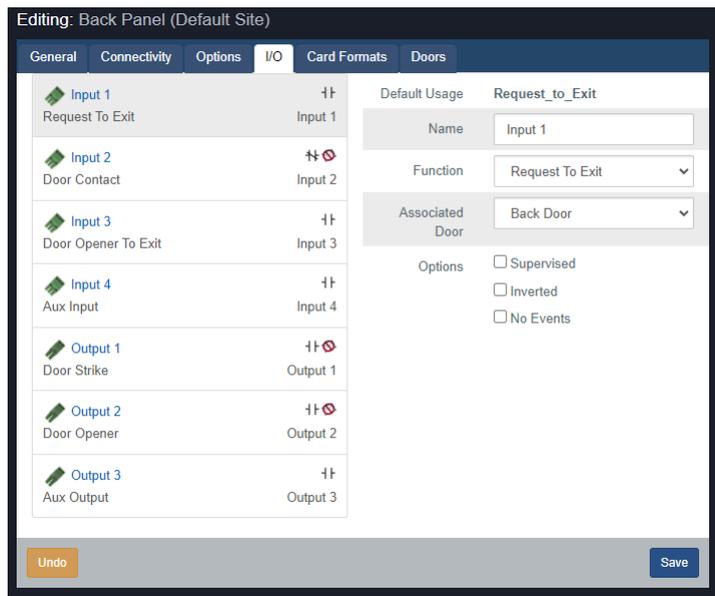
 **Note**

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; Output 1 and Output 2 will both be mapped as Door strikes. The I/O tab is unavailable on Elevator Panels. VAX-MDK panels and VAX-IO-STR-2 panels will have tabs

Figure 7.1. VAX-1D 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 with Two-Door Controllers)
- 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 VAX PoE controllers VAX-1D and VAX-2D

Table 7.3. Input/Output Functions VAX-1D-1/VAX-2D-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.
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.

Function	Description
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, <i>Triple Swipe Features</i> .
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 VAX-1D and VAX-2D panel models.

Table 7.4. 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 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.

Input Action	Description
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 Door Master

VAX-MDK Door controllers have some additional input/output features that will be noted in this section. Some specific differences include:

- Inputs can be assigned an Input Time Zone, 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 Time Zone. 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.
- 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.

The following table contains a list of Actions.

Table 7.5. 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.

Triple Swipe Actions	Brief Explanation
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 Time Zone 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.
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.

Triple Swipe Actions	Brief Explanation
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 7.6. 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 desirable.
Suppress invalid card format events	When checked, this panel will not report events related to invalid card formats.
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 Vicon Access Control 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>".

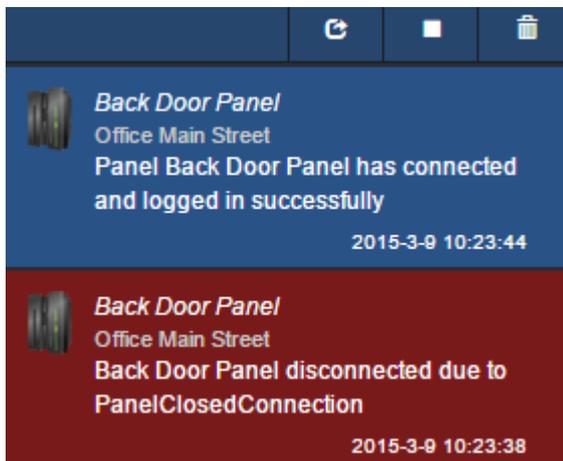
When you click on Update Panels, you'll be prompted by your browser if you are sure you'd like to do this action. Click Yes/Continue/OK. A window will appear in the middle of the screen that will show the status of the updates being sent to the Panel.

Figure 7.3. Panel Update Status Window



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

Figure 7.4. Typical Panel Update Notifications



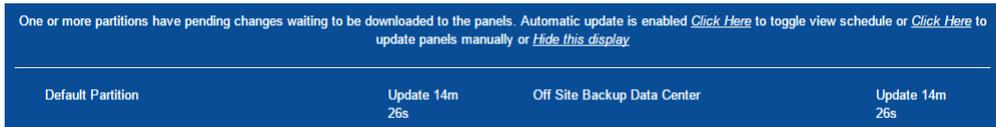
My Panel won't come back online after my first update. If your Panel doesn't come back online after its first update, check "Home>System Settings>Server Address". If it is a name, the Panel may be having trouble resolving the name into an IP through DNS. Consult IT staff; if a stable DNS server is not 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. It will be displayed on the bottom of 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:

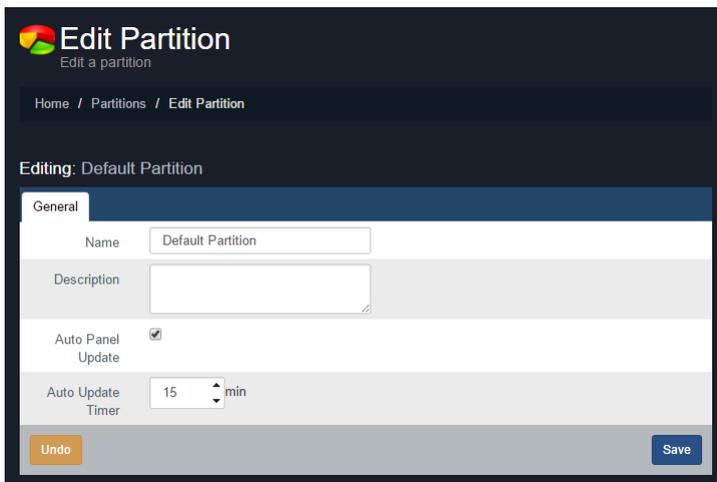
1. On the **Home Screen**, scroll down to the section titled **System**; click on the **Partitions** icon (pictured below).



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 Vicon Access Control, 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

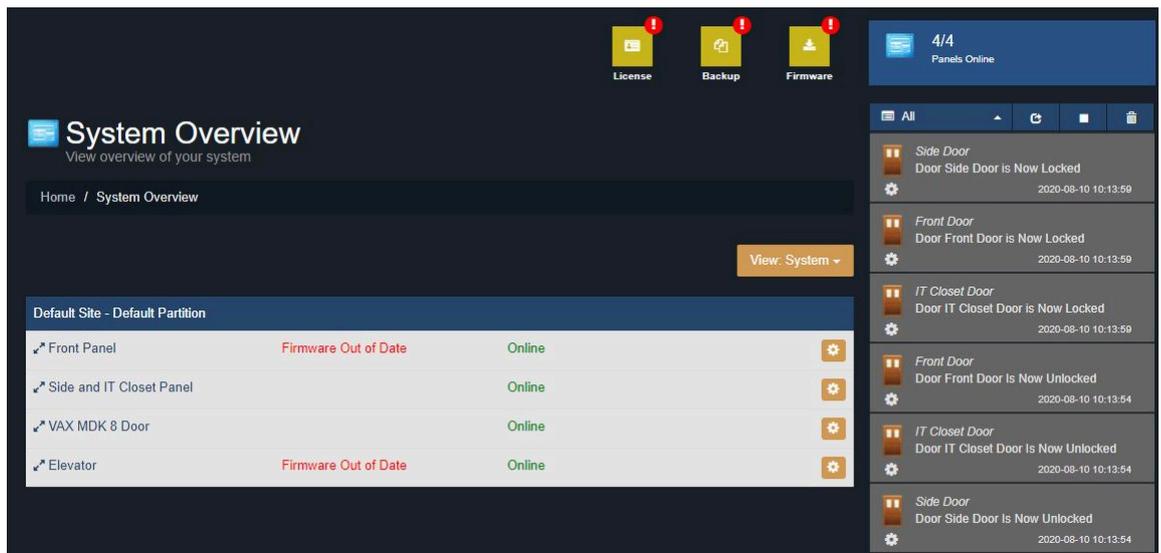


2. In order for a Panel to have its firmware updated we must place it into Firmware Update Mode. To do this we will navigate to the System Overview page in the software. Click on the "x/x Panels Online" box above the Notifications area **or** on the home page, scroll down to the section titled **System**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

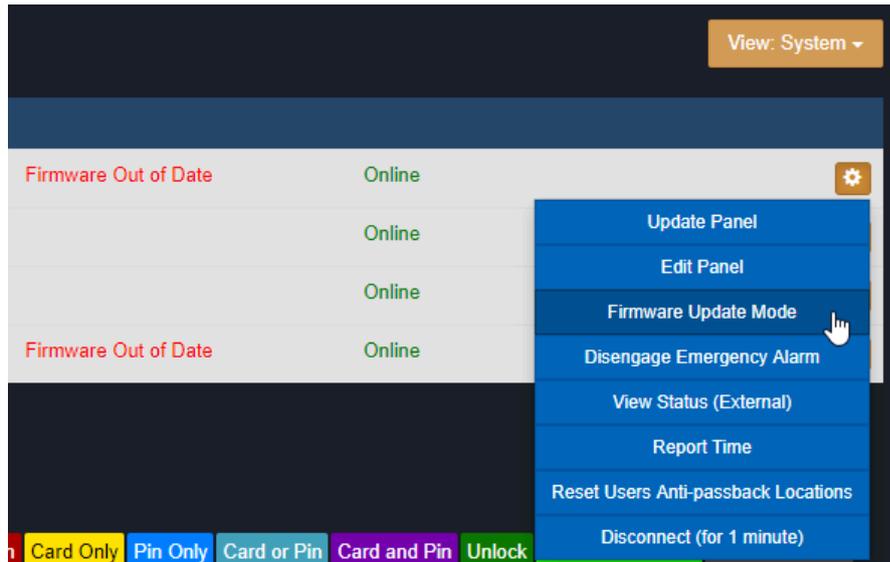


3. On the System Overview you will see a list of all Panels in your system. Any Panels that require a firmware update will have a message displayed next to its name.

Figure 7.8. 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 orange 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**

As of version 2.9.53, you can perform multiple firmware updates at the same time if needed.

5. The Vicon Access Control 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 Vicon Access Control 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 Time Zones, we recommend creating these before adding your Doors. Please see Chapter 9, *Door Time Zone 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 Vicon 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. On the **Home Screen**, 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

Add Door
Add a Door

Home / Doors / Add Door

Door

Door Type	Type	Supported Panels	Features
<input checked="" type="radio"/>	Managed	1D, 2D, MDK	Supports upto 2 readers, Automatic Opener, Anti-Passback, Cameras
<input type="radio"/>	Monitored	IO-STR, IO-STR-2	Only supports Door Contact and Cameras.
<input type="radio"/>	Unmanaged	IO-STR-2	Supports Door Contact, Door Strike and Cameras.

Name: Side Door

Description: Optional Description

Panel: Front and Side Panel (Default S)

Port on Panel: Port 1

Time Zone: Always Card Access

Holiday Group: No Holidays

Reader 1

Name: Side Door

Description: Optional Description

Port on Panel: Reader 1

Undo Save

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.
Description	Optional description of the Door. Accepts 4 to 255 characters.

Text Box/ Drop-down Menu	Description
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	If the Panel is a Single-Door Panel, one port will be available. If this is a Two-Door Panel, two will be available.
Time Zone	This is the most important configuration aspect of adding a Door. Select the desired Door Time Zone (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 **Home Screen**, 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.
Time Zone	This is the most important configuration aspect of a Door. Select the desired Door Time Zone (default or custom). You can also edit the selected Door Time Zone by clicking the "Edit Time Zone" 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 Time Zone 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, <i>Mantrap Configuration</i> .
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.

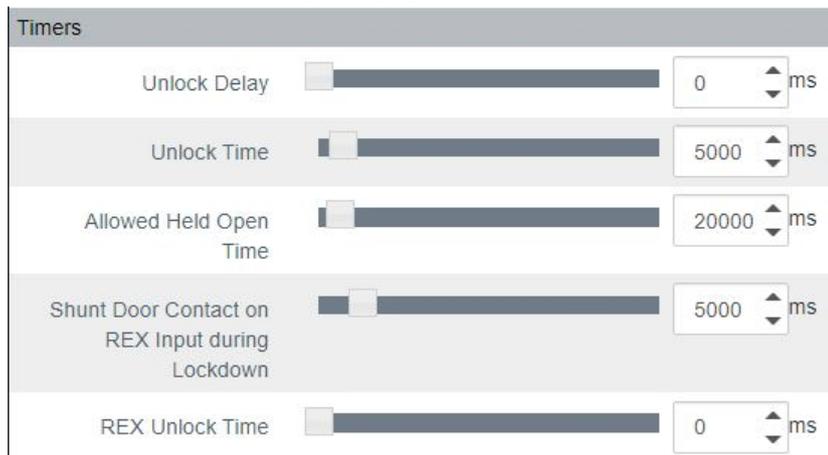


Table 8.4. Timers

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.

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.

Automatic Opener

Enabled

Disable Opened By Card/Pin

Opened With Motion

Opened With Rex

Opener Delay 100 ms

Opener On Time 500 ms

Table 8.5. 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.
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 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.

Disable

Disable Unlock on Emergency Alarm (Checked indicates unprotected door)

Forced Open

Forced Open Buzzer

Stop F/O Buzzer On Door Close

Held Open

Held Open Buzzer

Stop H/O Buzzer On Door Close

Lock After Door Open

Unlock By Motion

Table 8.6. Disable

Checkbox	Description
Unlock on Emergency Alarm	Prevent Door unlocking when emergency alarm is triggered.
Forced Open	Disable forced open alarm.

Checkbox	Description
Forced Open Buzzer	Disabled forced open buzzer.
Stop F/O Buzzer On Door Close	By default a forced open buzzer stops when the Door is closed; if disabled it continues until a valid credential is presented.
Held Open	Disable held open alarm.
Held Open Buzzer	Disable held open buzzer.
Stop H/O Buzzer On Door Close	By default a held open buzzer stops when the Door is closed; if disabled it continues until a valid credential is presented.
Lock After Door Open	Disable lock after Door opens (requires 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

The screenshot displays the 'Reader 1' configuration tab for a 'Front Door (Default Site)'. The interface includes the following elements:

- Enabled:** A checked checkbox.
- Name:** A text input field containing 'Front Reader'.
- Description:** A text input field containing 'Optional Description'.
- Reader Port:** A dropdown menu set to 'Reader 1'.
- Action:** A dropdown menu set to 'No Action'.
- Perform action only on Access Granted:** A checked checkbox.
- Enable Keypad:** An unchecked checkbox.
- Keypad Interval:** A slider and input field set to 5000 ms.
- Back To Back Filter Enabled:** An unchecked checkbox.
- Back To Back Filter Interval:** A slider and input field set to 2000 ms.
- Same Card Filter Interval:** A slider and input field set to 0 ms.
- Reader Input Interval:** A slider and input field set to 5000 ms.
- Sampling Mode:** A dropdown menu set to 'Default'.
- Triple Swipe:** An unchecked checkbox.
- Buttons:** 'Undo' (orange) and 'Save' (blue) buttons are located at the bottom.

Table 8.7. Reader Configuration Options

Configuration Item	Description
Action (MDK model only)	An optional Action is configurable upon a credential being presented to the reader. The available Actions are the same ones configurable for Triple Swipe. List of actions can be viewed in Chapter 17, <i>Triple Swipe Features</i> .
Perform action only on Access Granted (MDK model 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	Toggles if a keypad reader will be used on this reader port. If not enabled, a non-PIN credential could be used during card and pin schedules. This is not mandatory for PIN or Card or PIN 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 and out Reader 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.
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

Editing: Front Door (Default Site) Door Activity Report

General Options Reader 1 Reader 2 **Areas** Camera Association

Doors that will participate in anti-passback decisions require an optional memory module. Doors that will report user locations but not participate in anti-passback decisions do not require a memory module. A maximum of 32 site codes are supported by Anti-Passback.

Add Area To Default Site +

Reader 1 Grants Access to Area v

Reader 2 Grants Access to Area v

Track User Location (Without APB)

Enable Anti-passback

Override Sites APB Settings

Undo Save

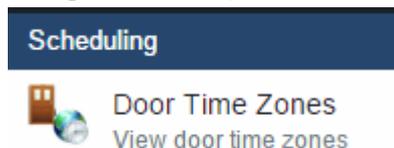
Chapter 9. Door Time Zone Configuration

This chapter covers the configuration of Door Time Zones in Vicon Access Control. For information about planning, concepts and examples of Door Time Zones, please see the section called “Door Time Zones”.

Adding a Door Time Zone

Adding a Door Time Zone in Vicon Access Control is a streamlined process that takes full advantage of HTML5. The default Door Time Zone 'Always Card Access' is the most commonly used time zone in the field, however there are hundreds of possible combinations of Door states that can fit many unique situations. Door Time Zones can support up to 20 time spans in a day. This section covers how to add a new Door Time Zone.

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **Scheduling**; click on the **Door Time Zones** icon (pictured below).



4. On the Door Time Zones screen, you'll notice the default time zones. In a lot of cases these time zones meet the needs of the system; however, if during your planning stage you (the installer or end-user) decided that additional Door Time Zones are needed, click the **Add** button on this screen.
5. On the **Add Door Time Zone** screen, you'll have a couple text boxes to populate.

Table 9.1. Add a Door Time Zone

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

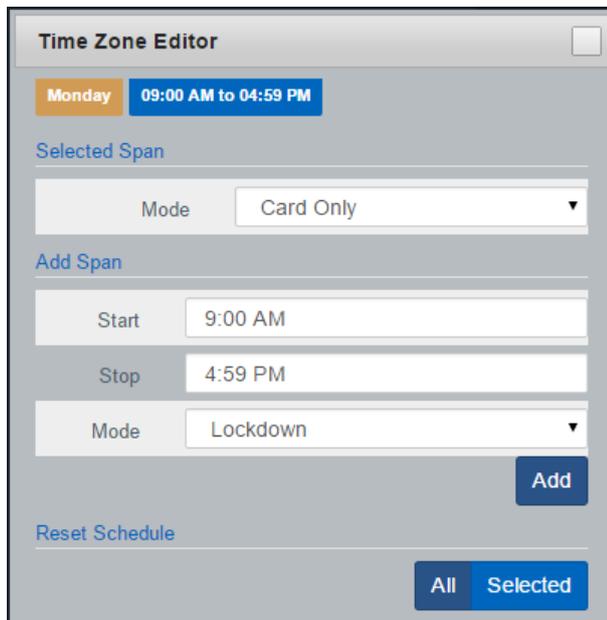
6. Creating the **Schedule** is the last step in creating a Door Time Zone. Below is what the schedule part of the add time zone page looks like.

Figure 9.1. Door Time Zone Schedule



7. Click on any of the horizontal bars in the time schedule to bring up the **Time Zone Editor Widget**. The time zone editor widget is a simple and powerful tool for creating time zones.

Figure 9.2. Time Zone Editor



8. Use the **Mode** drop-down menu to select the Door state for the **selected** time span. 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”.)
9. The **Add Span** section of the time zone editor has 3 fields used for adding a Door Time Zone 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 Door 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 time span you've added. Add additional time spans to that day if required.

If you'd like the time zone you've created to be used for several different days, you can click on the bar with your completed time zone, and drag it to the **Week**, **Weekend** or **Weekdays** boxes above the chart. The time zone will be replicated based on which box you drag your time zone into.



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

Chapter 10. User Time Zones

This chapter covers how to add additional User Time Zones to Vicon Access Control. For more information on what a User Time Zone is, please see the section called “Concepts”.

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

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **Scheduling**, click on the **User Time Zones** icon (pictured below).



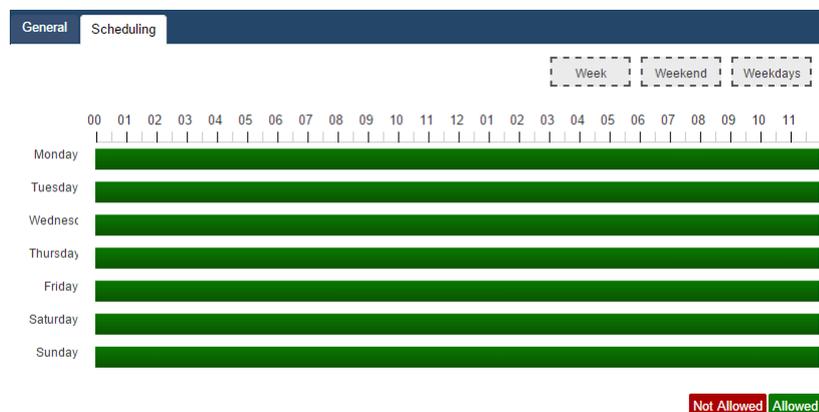
4. On the User Time Zones screen, you'll notice the default time zones. These Time Zones can be renamed and modified to fit the deployment needs. If during your planning stage you (the installer or end-user) decided that additional User Time Zones are needed, click the **Add** button on this screen.
5. On the **Add User Time Zone** screen, you'll have a few text boxes to populate.

Table 10.1. Add a User Time Zone

Text Box	Description
Name	Unique name of your User Time Zone. Accepts 2 to 60 characters. We recommend naming your time zones by the function of the time zone.
Description	Optional description of your User Time Zone. Accepts 4 to 255 characters.
Partitions	Select the Partitions you'd like to create this time zone 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 Time Zone. Below is what the schedule part of the Add Time Zone page looks like.

Figure 10.1. User Time Zone Schedule



- Click on any of the horizontal bars in the time schedule to bring up the **Time Zone Editor Widget**. The time zone editor widget is a simple and powerful tool for creating time zones.

Figure 10.2. Time Zone Editor

- Use the **Mode** drop-down menu to select the User access state for the selected span. Only **Allowed** and **Not Allowed** are available.
- The **Add Span** section of the time zone editor has 3 fields used for adding a User Time Zone 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 User access state the schedule will follow during the defined time span. Once you've completed these fields, click the **Add** Button.
- 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 time zone you've created to be used for several different days, you can click on the bar with your completed time zone, and drag it to the **Week**, **Weekend** or **Weekdays** boxes above the chart. The time zone will be replicated based on which box you drag your time zone into.



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

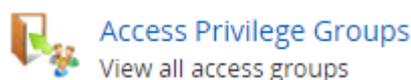
Chapter 11. Access Privilege Groups

This chapter will cover how to add an **Access Privilege Group** in Vicon Access Control. 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/Floors in the group, giving us additional control over which Doors/Floors Users can access.

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **Day To Day**, 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 Time Zone** 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 Time Zones match the access group requirements, you can create a new User Time Zone, please see Chapter 10, *User Time Zones*.

Readers

Search for a Reader By Name

Reader

Front Door (Default Site)

Access 9AM to 5PM ▼

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 Time Zone** 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).

Floors

Search for a Floor By Name

Floor 1

Cab 1 1-7 (Default Site)

Access 9AM to 5PM ▼

9. Once you've selected the Readers and User Time Zones 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 Vicon Access Control, 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 Vicon Access Control 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 Vicon Access Control, 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 Vicon Access Control. 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

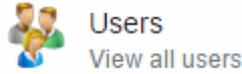
Adding a User in Vicon Access Control is a fairly simple process, however there are a variety of options that take advantage of various features of our software.

Prior to adding Users to Vicon Access Control, 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 a User to Vicon Access Control.

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **Day To Day**; 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 time zone 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, <i>Crisis Levels</i>
Master	Enable/Disable Master User privilege. Master Users have full access to all Doors and Floors, regardless of schedule or other privileges. 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 time zone.
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, <i>Triple Swipe Features</i> .
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

General	Custom	Images	Credentials	Partitions and Access Groups
First Name	<input type="text" value="Bob"/>			
Last Name	<input type="text" value="Joe"/>			
Starts On	<input type="text"/>			
Expires On	<input type="text"/>			
Crisis Level	Default: Follow Schedule ▼			
Master	<input type="checkbox"/>			
Supervisor	<input type="checkbox"/>			
First Card In	<input checked="" type="checkbox"/>			
Triple Swipe	<input checked="" type="checkbox"/>			
Disengage Alarm	<input checked="" type="checkbox"/>			
Auto Opener	<input type="checkbox"/>			

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 Vicon Access Control server in: "<Installation Directory>\Vicon Access Control\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

Images				
Card Holder		Or	<input type="button" value="Choose File"/>	No file chosen
Accessory 1		Or	<input type="button" value="Choose File"/>	No file chosen
Accessory 2		Or	<input type="button" value="Choose File"/>	No file chosen

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

Custom	
Employee Number	5861
Department	Information Technology
Hire Date	2012-06-19

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

Credentials

Select the type of credential to create on the left, once created credential will be moved to the right menu. Pin Numbers will not be generated/validated until the user is added.

Card with Pin Number
 Pin Only

Auto

Add Credential

Credentials for card and/or pin schedules		
Card Number	Pin Number	
033-06141	9999	Remove
033-32199	583237193	Remove

Credentials for pin schedules	
Pin Number	
85236	Remove

Depending on the Door Time Zone, 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 '033-0641'. The reader will expect the PIN '9999' 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 '85236'. PIN '9999' 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 '85326' 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*

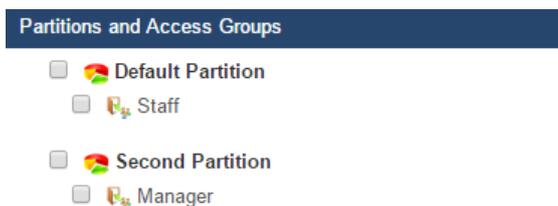
All Partitions you have permission to see will have their associated Access Privilege Groups displayed here. Select the Access Groups the User should belong to.

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".

Panel User Actions

After a user is added, a tab titled Panel Actions will be available. This section will outline what these actions do and some possible use cases.

User Panel Actions allow you to specify a specific action when a credential belonging to a specific user is granted access to a specific reader. This feature is only supported on readers connected to a VAX-MDK panel. The selectable actions are the same actions available for Aux Input Actions and Triple Swipe Actions. A full list of actions can be found in Chapter 17, *Triple Swipe Features*.

Figure 12.6. Action Example

Home / Users / Edit User

Alice Piece
Normal User

User Activity Report

General Custom Images Credentials Access Groups **Panel Actions** Anti-passback

Front Reader Action: Output - Pulse High

Output 1-2
Output 1-3
Output 1-5
Output 1-6

1/1

Delay (s): 0

Duration (s): 5

Save

Some possible use cases include:

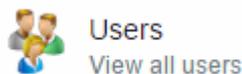
- **Duress PIN/Credential:** Connect an Aux Relay to an alarm system and set a specific user record that contains a special PIN which will use the Panel Action "Output - Pulse High". This will grant access but pulse a separate relay to an alarm system
- **Emergency Credential:** Set a specific user record that will override all doors on a VAX-MDK panel to Lockdown or initiate a local Crisis Level
- **Temporarily Disable Held Open:** Set a specific user record that will disable the Held Open for a specific duration.

User Templates

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

Adding and updating User Templates is simple:

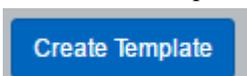
1. On the **Home Screen**, scroll down to the section titled **Day To Day**; click on the **Users** icon (pictured below).



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.

The screenshot shows a 'Template' configuration form. The 'Template' dropdown menu is open, displaying a list of options: 'Supervisors West', 'Select...', 'Employees', 'Supervisors West', and 'Required'. A mouse cursor is hovering over the 'Employees' option. The form also includes a 'General' section and a 'First Name*' field.

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 **Home Screen**, 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 Vicon Access Control.
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 Vicon Access Control. 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 text file that will need to be filled prior to importing.

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.

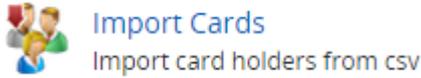
Warning

First name and last name must not contain any of the 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 Vicon 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. On the **Home Screen**, scroll down to the section titled **Day To Day**; 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. Vicon Access Control will now scan the file and proceed to step 2.

Figure 12.7. Import Options

Column #	Data Type	Record (1/11)
1	First Name	Alice
2	Last Name	Pierce
3	Credential #1 Site Code	33
4	Credential #1 Card Number	48503
5	Credential #1 PIN	1234

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

If the Users you are importing need separate sets of Access Privilege Groups, we advise using separate imports for each type of User.

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

- Click Validate on the bottom of the page once you've filled in all columns and Access Groups.
- 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 12.8. Import Preview

The screenshot shows the 'Import Preview' screen in a web application. At the top, there is a breadcrumb 'Home / Import Cards' and a progress indicator 'Step: 3 / 3'. Below this, there are two buttons: 'Clear Results' (orange) and 'Import File' (blue). The main content is a table with the following columns: 'Import' (checkbox), 'Record #', 'First Name', 'Last Name', 'Credential #1 Site Code', 'Credential #1 Card Number', and 'Credential #1 PIN'. There are four rows of data, all with checked checkboxes in the 'Import' column.

Import	Record #	First Name	Last Name	Credential #1 Site Code	Credential #1 Card Number	Credential #1 PIN
<input checked="" type="checkbox"/>	1	Alice	Pierce	33	48503	1234
<input checked="" type="checkbox"/>	2	Amanda	Harrison	33	48504	4569
<input checked="" type="checkbox"/>	3	Amy	Scott	33	48505	9876
<input checked="" type="checkbox"/>	4	Barbara	Pierce	33	48506	7894

- 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:

- On the **Home Screen**, scroll down to the section titled **Day To Day**; 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 12.9. 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 12.10. Add Custom Field

Home / Custom Fields / Add Custom Field

Custom Field

Name:

Field Type:

Mandatory:

Appears In Monitoring:

Format String:

Note: Format string is the format that you wish to show the DateTime in. By default, it will show in YYYY-MM-DD, however if you want to include the time, you can use YYYY-MM-DD hh:mm A. To find out more about the various format tokens and examples, see MomentJS's Reference.

Undo Save

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](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 (YYY-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.

Chapter 13. Holiday Configuration

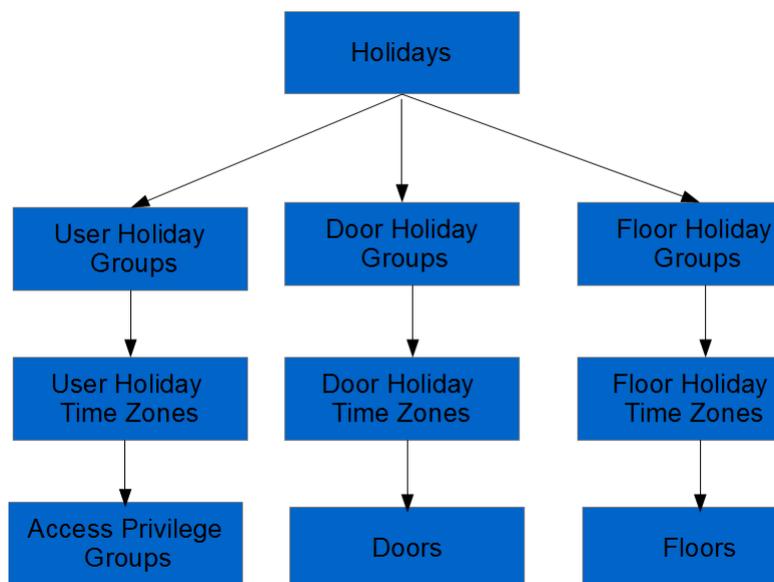
This chapter will cover the configuration of various Holiday components in Vicon Access Control. We recommend you read the section called “Holidays” prior to reading this chapter for planning how a Holiday should affect your system and an explanation of the components involved.

The 7 components of Holidays in Vicon Access Control are:

- User Holiday Time Zones
- User Holiday Groups
- Door Holiday Time Zones
- Door Holiday Groups
- Floor Holiday Time Zones
- 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 Time Zone:

After planning how Doors/Floors/Users should behave during a holiday, create these appropriate Holiday Time Zones 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 Time Zones 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 Time Zones

This section will cover the configuration of **User Holiday Time Zones**.

By default Vicon Access Control comes installed with 2 default User Holiday Time Zones:

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 Time Zones or to edit the default time zones.

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **Scheduling**; click on the **User Holiday Time Zones** icon (pictured below).



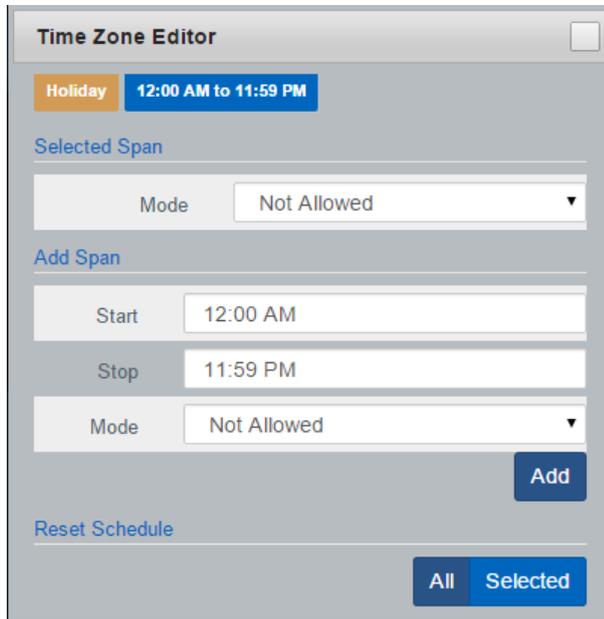
4. On the **User Holiday Time Zones Screen**, you'll see the default User Holiday Time Zones, if you require additional time zones; click the **Add** button.
5. On the **Add User Holiday Time Zone screen**, you'll see it looks almost exactly like other time zones you've added in the system. Populate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

Table 13.1. Add User Holiday Time Zone

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

- You may now configure the time zone based on what you want a User group to have access to during a Holiday. Click on the red bar next to **Holiday** in the **Schedule** half of the page. This will bring up the **Time Zone Editor Widget**.

Figure 13.2. Time Zone Editor



- On the **Time Zone Editor**, you can use the **Mode** drop-down menu to select a User mode for the entire day. If you need further customization, use the add span section to change the User schedule up to 4 times in a day.
- Once you've completed the schedule, click on the **Save** button. You have now added a User Holiday Time Zone.

User Holiday Groups

This section will cover the configuration of **User Holiday Groups**. By default Vicon Access Control 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.

- Access your Vicon Access Control system through your HTML5 browser of choice.
- Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
- On the **Home Screen**, scroll down to the section titled **Scheduling**, click on the **User Holiday Groups** icon (pictured below).



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

This section will cover the configuration of Door Holiday Time Zones. By default Vicon Access Control comes installed with 1 default Door Holiday Time Zone: 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 Time Zones or edit the default time zones.

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **Scheduling**; click on the **Door Holiday Time Zones** icon (pictured below).



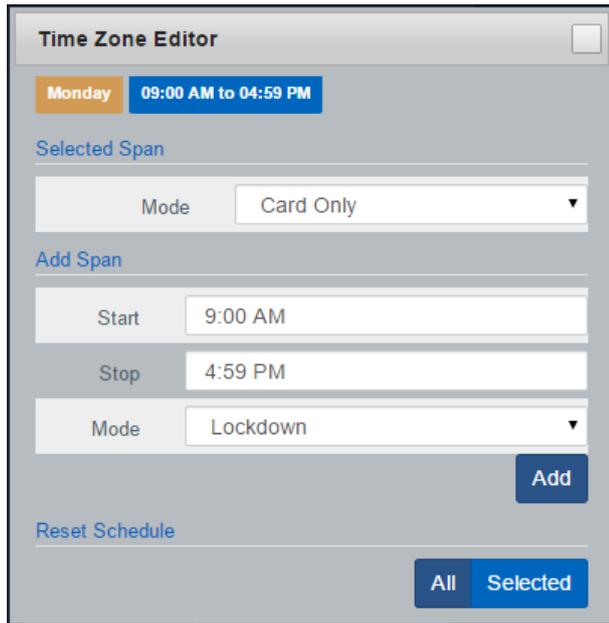
4. On the **Door Holiday Time Zones Screen**, you'll see the default Door Holiday Time Zone; if you require additional time zones, click the **Add** button.
5. On the **Add Door Holiday Time Zone screen**, you'll see it looks almost exactly like other time zones you've added in the system. Populate the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

Table 13.3. Add Door Holiday Time Zone

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

6. You may now configure the time zone based on what you want a Door to do during a Holiday. Click on the yellow bar next to **Holiday** in the **Schedule** half of the page. This will bring up the time zone editor.

Figure 13.3. Time Zone Editor



7. On the **Time Zone Editor**, you can use the **Mode** drop-down menu to select a Door mode for the entire day. 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 Time Zone.

Door Holiday Groups

This section will cover the configuration of Door Holiday Groups. By default Vicon Access Control 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 Vicon 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. On the **Home Screen**, scroll down to the section titled **Scheduling**; click on the **Door Holiday Groups** icon (pictured below).



4. On the **Door Holiday Groups Screen**, 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.
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 Time Zones

This section will cover the configuration of Floor Holiday Time Zones. By default Vicon Access Control comes installed with 1 default Floor Holiday Time Zone: 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 Time Zones or edit the default time zones.

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **Scheduling**; click on the **Floor Holiday Time Zones** icon (pictured below).



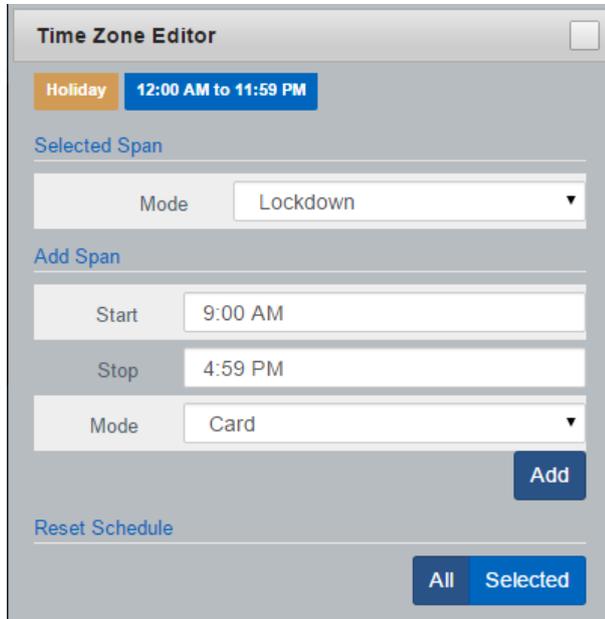
4. On the **Floor Holiday Time Zones Screen**, you'll see the default Floor Holiday Time Zone; if you require additional time zones, click the **Add** button.
5. On the **Add Floor Holiday Time Zone screen**, you'll see it looks almost exactly like other time zones you've added in the system. Populate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

Table 13.5. Add Door Holiday Time Zone

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

- You may now configure the time zone based on what you want a Floor to do during a Holiday. Click on the yellow bar next to **Holiday** in the **Schedule** half of the page. This will bring up the time zone editor.

Figure 13.4. Time Zone Editor



- On the **Time Zone Editor** you can use the **Mode** drop-down menu to select a Floor mode for the entire day. If you need further customization, use the add span section to change the Floor state up to 4 times in a day.
- Once you've completed the schedule, click on the **Save** button. You have now added a Floor Holiday Time Zone.

Floor Holiday Groups

This section will cover the configuration of Floor Holiday Groups. By default Although this often is enough for most Holiday configurations, it's fairly easy to add additional Floor Holiday Groups.

- Access your Vicon Access Control system through your HTML5 browser of choice.
- Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
- On the **Home Screen**, scroll down to the section titled **Scheduling**; click on the **Floor Holiday Groups** icon (pictured below).



- On the **Floor Holiday Groups Screen**, you'll see the default Floor Holiday Groups; if you require additional groups, click the **Add** button.
- 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 Vicon Access Control. 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 Vicon 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. On the **Home Screen**, scroll down to the section titled **Day to Day**; 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.
Partitions	Use this drop-down menu to change the Partition. Changing the Partition will change the User/Door/Floor groups displayed below.
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 Time Zone 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 Time Zone 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 Time Zone 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 Vicon Access Control.

In this example, we will use the default **Holiday Time Zones** 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 Independence Day

Add Holiday
Add a holiday

Home / Holidays / Add Holiday

Holiday

Name: Independence Day

Description: Optional Description

Initial Date: 1776-07-01

Occurs Annually:

Groups

Partition: Default Partition

User Groups

No Holidays: Holiday Access 9AM to 5PM

Standard Holidays - Default Group: Holiday No Access

Door Groups

No Holidays: Closed During Holiday

Standard Holidays: Closed During Holiday

Floor Groups

Default Holiday Group: Closed During Holiday

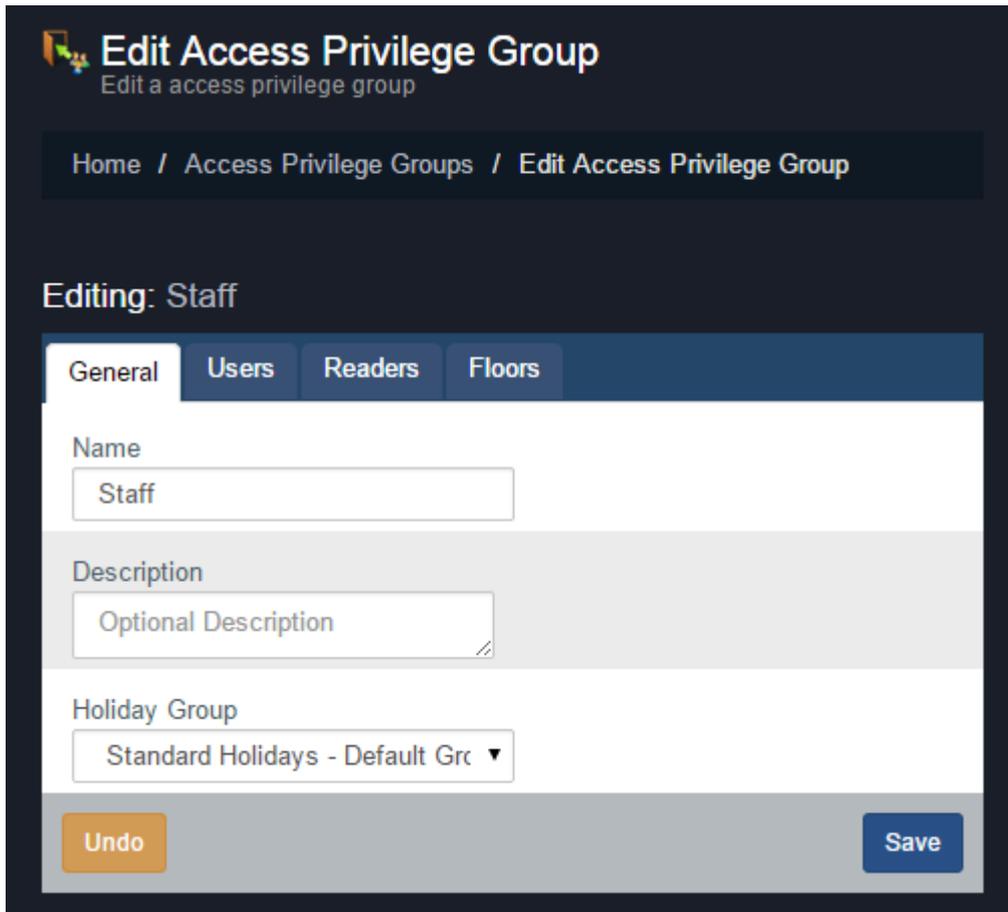
I/O Groups

No Records Found

Undo Save

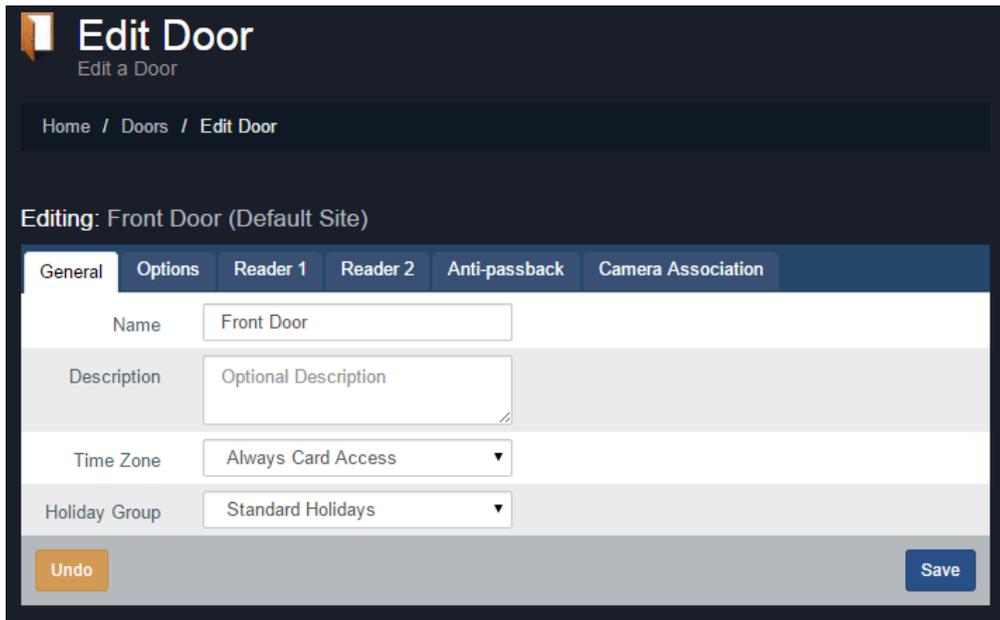
After the above Holiday has been added, we'll need to make sure the **Access Privilege Groups**, **Doors** and **Floors** that the Holiday should affect have the appropriate **Holiday Groups**.

Figure 13.6. Access Privilege Groups: Holiday Group



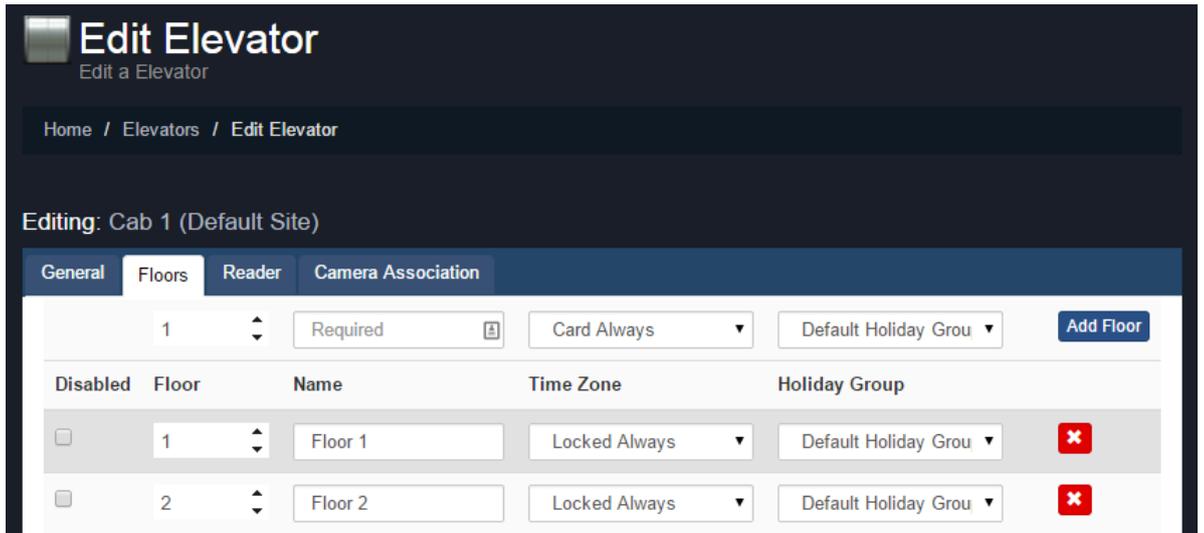
In the above screen shot, you see we've changed the **Holiday Group** drop-down menu to the **Standard Holidays User Holiday Group**, which is the User group we've added the Holiday to earlier.

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 Time Zone

This section covers the steps to adding a OTR on Vicon Access Control.

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **Scheduling**. For a Door OTR, click **Door OTR Time Zones**. For Floor OTR, click **Floor OTR Time Zones** (pictured below).



4. On the OTR screen, you'll see the previous OTRs that have been created click the **Add** button on this screen.
5. On the **Add OTR** screen, you'll have a couple text boxes to fill.

Table 14.1. Add a One Time Run Time Zone

Text Box	Description
Name	Unique name for your one time run time zone. 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 time zone 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.

6. 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

One Time Run Time Zone

Name: Secret Meeting

Start Time: 11/09/2015 6:00 AM

Stop Time:

Partition:

Affected Doors

- Data Center Entrance
- Main Entrance (Default)
- Server Cab MLX01 (C...

Calendar: November 2015

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Time: 06 : 00 AM

Tip

You can configure an OTR to span multiple days. This can be useful for holidays lasting more than a day.

Chapter 15. Crisis Levels

This chapter will cover how Crisis Levels work in Vicon Access Control, 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 Vicon 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. On the **Home Screen**, scroll down to the section titled **System**; 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

Disabled	Name	Level	Door State
	Default: Follow Schedule	1	
No	Code Yellow	2	Card Only
Yes	Level 3	3	Card Only
Yes	Level 4	4	Card Only
Yes	Level 5	5	Card Only
Yes	Level 6	6	Card Only
Yes	Level 7	7	Card Only
No	Code Orange	8	Card Only
Yes	Level 9	9	Card Only
Yes	Level 10	10	Card Only
Yes	Level 11	11	Card Only
Yes	Level 12	12	Card Only
Yes	Level 13	13	Card Only
Yes	Level 14	14	Card Only
Yes	Level 15	15	Card Only
No	Code Red	16	Card Only

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 **Home Screen**, scroll down to the section titled **Day To Day**; 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

The screenshot shows the 'Edit User' interface with the 'General' tab selected. The user's name is 'Bob Joe'. The 'Crisis Level' dropdown menu is open, showing options: 'Default: Follow Schedule' (selected), 'Code Yellow', 'Code Orange', and 'Code Red'. Other fields include 'Starts On', 'Expires On', and 'Supervisor'.

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 Vicon Access Control software, the second method is through the use of AUX Inputs on the Panels.

Applying Crisis Levels in Vicon Access Control

Applying a Crisis Level in Vicon Access Control can be done from any page in the Vicon Access Control 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 only way to resume to normal schedule is through the Vicon Access Control software interface, or by having an additional Input with an Aux Input trigger that places the Door into Default: Follow Schedule.

Chapter 16. Vicon Access Control Override Features

This chapter will cover the various Override features in Vicon Access Control, 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 Time Zones (with the exception of Override until next schedule).

Override Doors

This section covers how to Override a Door in Vicon Access Control using the **Override Doors** menu. Overriding a Door can be done from any page in the software by clicking on the Override Doors button on the top right 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 Vicon Access Control 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, **General**, **Override until resume** and **Override until next schedule**.

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. These Overrides behave slightly differently 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 Vicon Access Control using his smart phone and does 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 Floor in Vicon Access Control using the **Override Floors** 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 Floors icon to bring down the Override Floors menu. Here you will see all Sites in the system and the Elevators and Floors attached to each Site. Only Floors that are online and connected to Vicon Access Control 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

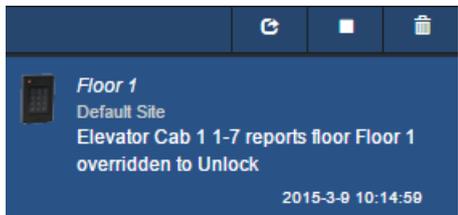
have selected the Floors, the buttons on the right side can be used to manipulate the state of the Floor instantaneously.

The Override Floors menu is divided into 3 sections, **General**, **Override until resume** and **Override until next schedule**.

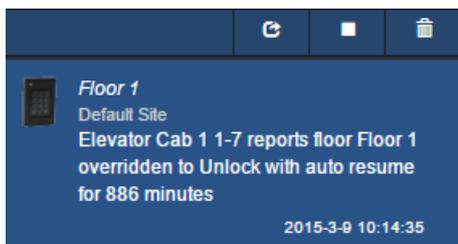
General. The **Resume** action can be used on any type of Floor Override to return the Floor to its normal schedule. When a Floor is resumed, you will see the Notification: **Floor Override Disabled**.



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. These Overrides behave slightly differently from an 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 Vicon Access Control. 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*

Chapter 17. Triple Swipe Features

Triple Swipe is a feature in Vicon Access Control where you can present a Credential to a Reader 3 times quickly and it will perform a pre-defined action. These actions include overriding the state of the Door, triggering Outputs on the Panel and activating Alarm Interfaces. This chapter will cover these 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 Time Zones 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. MDK 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 Time Zone 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 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 Overrides instruct the Door to Resume normal schedule when the Door Time Zone assigned to this Door is scheduled to change. Can

Triple Swipe Actions	Brief Explanation
	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
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 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 **Home Screen**, 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

The screenshot displays the 'Triple Swipe' configuration screen. At the top, there are two checked options: 'Enabled' and 'Enable Keypad'. Below these are nine rows, each representing an action for a specific keypress (0-9). Each row has a label on the left and a dropdown menu on the right. The dropdowns for keys 0-4 are set to 'No Action'. The dropdown for key 7 is set to 'Override the door into card mode'. The dropdown for key 8 is set to 'Resume an overridden door'. The dropdown for key 9 is set to 'Resume any overridden outputs'. At the bottom of the screen, there is an orange 'Undo' button on the left and a blue 'Save Reader 1' button on the right.

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 Figure A.1, "Alarm Panel Interface".

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.

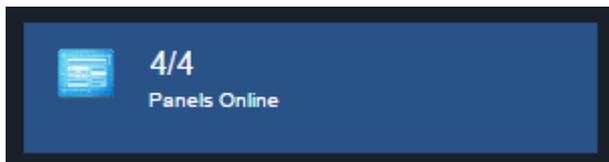
1. Go to "Home/Hardware/Door Panels".
2. Choose the Door you want to be able to lock early and click on the blue button (edit).
3. Click on either the **Reader 1** or **Reader 2** tab depending on which Reader you require this function to work.
4. Enable Triple Swipe by checking the check box.
5. From 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 Vicon Access Control 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 System Overview 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:

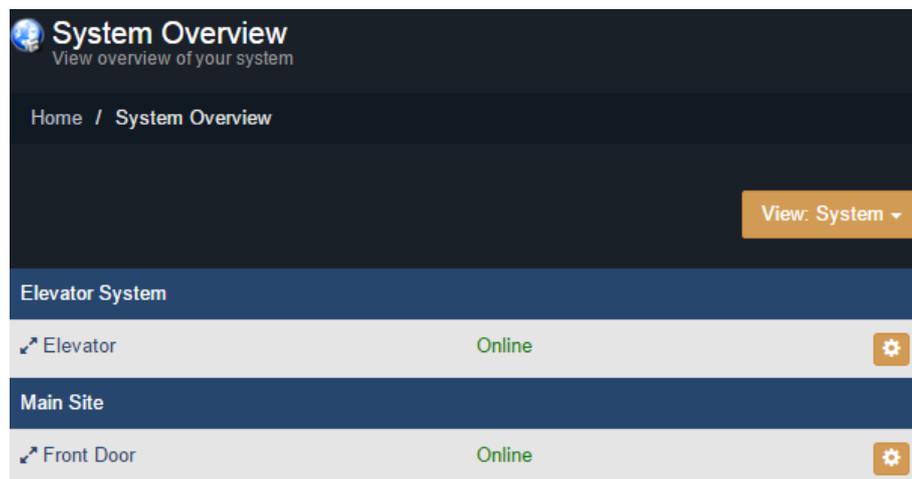
1. Access your Vicon Access Control system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Home Screen**, scroll down to the section titled **System**; click on the **System Overview** 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.

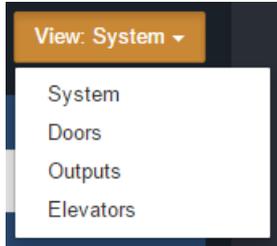
Figure 18.1. System Overview Screen: Default View



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 drop-down menu on the right side. 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	Will open the Edit Panel screen for the selected Panel.
Firmware Update Mode	Places the Panel into firmware update mode.
View External Status	Opens a new tab that will try to connect to the Panel http web interface. If a DNS server is not available or not aware of the Panel name, it may not resolve.
Report Time	The Panel will report what it thinks the current time is. 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.
Report Aperio Version	Menu item is specific to Doors connected to Aperio Panels. A Notification will be returned with the software version of the Aperio Panel.
Reset Aperio Device	Menu item is specific to Doors connected to Aperio Panels. Will reset the Aperio device (if applicable).
 Output Object Menu Items	

Menu Item	Description
Resume Output	Resumes the Output from an overridden state; works the same as the Resume action in the Output Overrides menu.
 Floor 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 Vicon Access Control. 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
Time Zones (Door, User, Holiday, etc)	Per Partition
One Time Run Time Zones	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 Vicon Access Control Partitions are complex, the configuration is relatively simple and straightforward.

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **System**; click on the **Partitions** icon (pictured below).



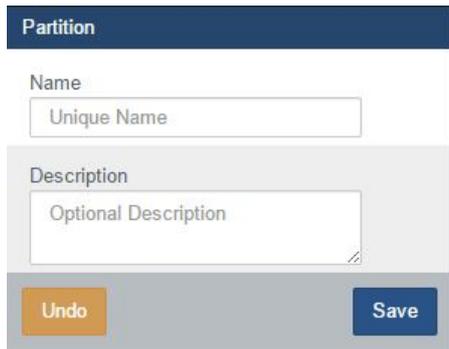
4. On the Partitions screen, you'll see the default Partition that is created by default. In a lot of cases a single Partition meets the needs of the system; however, if during your planning stage you (the installer or end User) decided that utilizing Partitions would benefit your deployment, click the **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 Vicon 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. On the **Home Screen**, 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 Vicon 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:

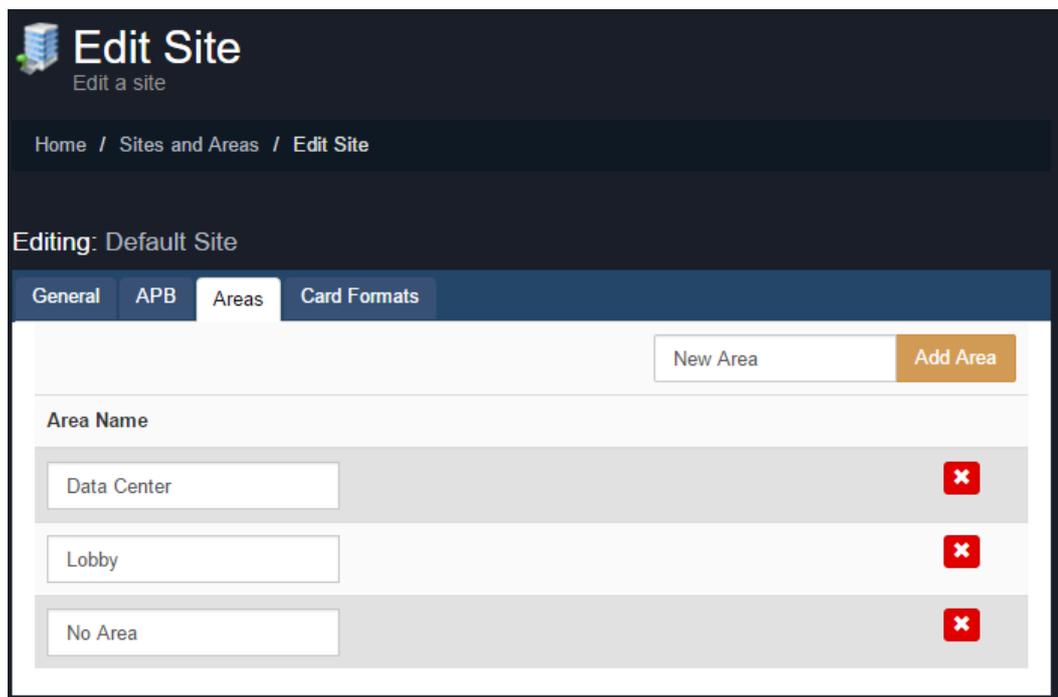
1. On the Edit Site screen, click on the **Areas** tab.
2. On the **Areas** tab, enter a name for your new area and click the **Add Area** button on the right side.

Note

The default area 'No Area' cannot be deleted.

You have now successfully added an Area to Vicon Access Control.

Figure 19.2. Adding an Area



For more information on Anti-passback, please see Chapter 21, *Areas and Anti-Passback*.

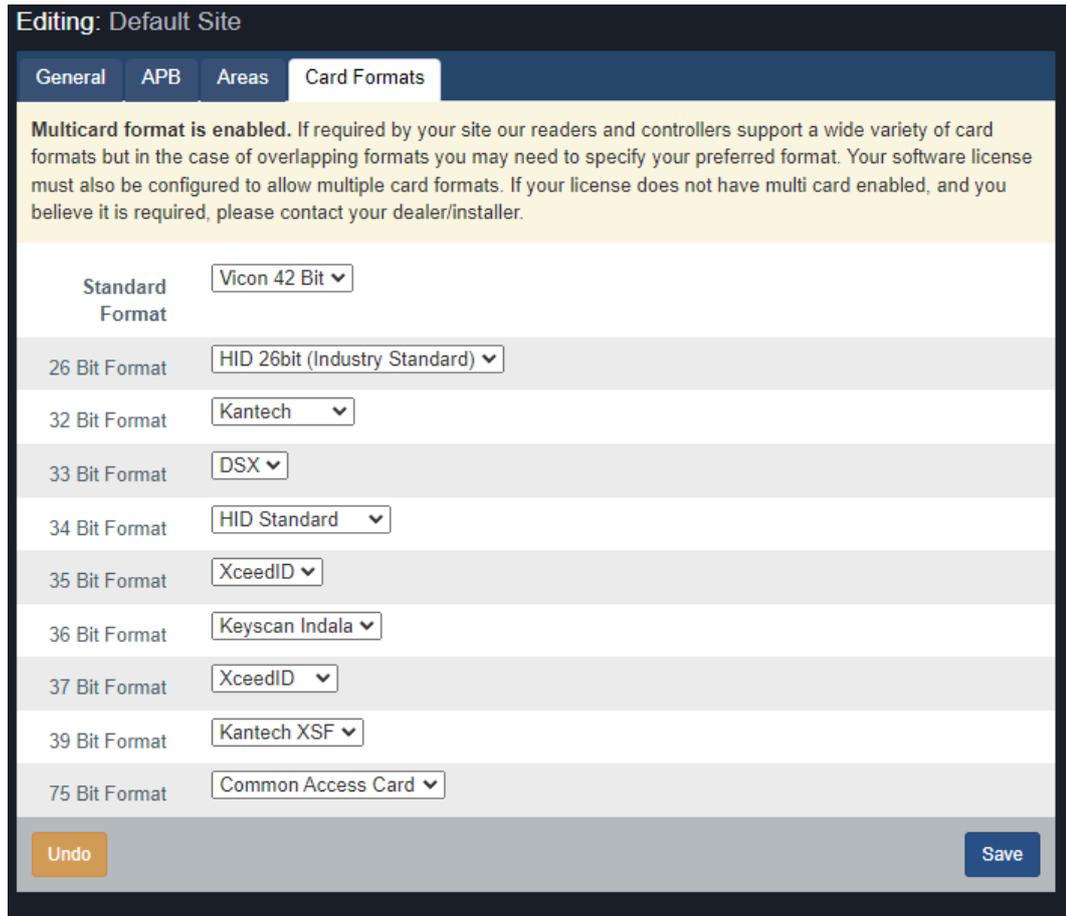
Edit Sites and Areas: Card Formats

Vicon Access Control supports a variety of card formats. The use of third party card formats (any format other than Vicon 42 bit) requires that the Multicard feature be enabled by your Vicon Access Control license. If you are in a trial period, Multicard will be enabled by default. If your license does not have multi card 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 you're 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

This chapter will cover how to add additional **Administrator Accounts**, the definitions of the privileges that can be assigned to these Administrators and a couple examples of how these accounts can be useful. 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*.

Adding an Administrator Account

1. Access your Vicon 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. On the **Home Screen**, scroll down to the section titled **System**; click on the **Administrators** icon (pictured below).



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.

You are presented with two sections to fill in. **Administrator Options** and **Partition Access and Privileges**. First lets go over the Administrator options and what they are.

Table 20.1. Add an Administrator: Options

Text Box/Drop-down Menu/Checkbox	Description
Authentication	The authentication of the Administrator account; options are Local, Service Account and LDAP (if LDAP is configured; see Chapter 32, <i>Active Directory Integration</i>).
Username	Unique Username (email address) 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	This checkbox dictates if the Administrator is a System Admin . Actions requiring System Admin are covered in the privileges section.
Password	Administrators password. Accepts 6 to 16 characters.
Confirm Password	Administrators password. Accepts 6 to 16 characters.

Privileges dictate what an Administrator may do within a Partition. 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. These are options that affect multiple Partitions or operate on a global scale.

 **Note**

Administrators with the **System Admin** checked are not bound by Partition permissions; they have unlimited access to all aspects of the system.

Table 20.2. Actions Requiring System Administrator

Action	Brief Explanation
Managing Administrators	Non-system Administrators may not create additional Administrator accounts; the initial Administrator is a System Admin.
Managing Crisis Levels	Non-system Administrators may initiate Crisis Levels within their Partition, however they cannot change the names/properties of Crisis Levels.
Managing Email Settings	Non-system Administrators cannot change Email/SMTP settings under Home/System Settings.
Managing Custom Fields	Non-system Administrators cannot add custom fields, however they can enter custom field values using with the Users they have access to through the administrative privilege "Manage Users".
Managing Licensing	Non-system Administrators cannot make modifications to the Vicon Access Control license.
Managing Partitions	Non-system Administrators cannot make modifications or add Partitions.
Notification/Administrator Activity Reporting	Non-system Administrators cannot run reports on Notifications or Administrator logs under Home/Reporting. Access to User and Door reports can be given to non-system Administrators through the administrative privilege "Reporting".

- The second part of adding an Administrator is assigning **Partition Access and Privileges**. Using the Partition drop-down menu you can give an Administrator permissions across multiple Partitions. These privileges only apply to non-system Administrators. The following table lists these permissions and a brief explanation.

Table 20.3. Assignable Administrator Permissions

Permission Name	Brief Explanation
Execute High Security Action Plans	Allows the Administrator to execute System type Action Plans with the High Security setting configured.
Execute Normal Security Action Plans	Allows the Administrator to execute System type Action Plans without the High Security setting configured.
Manage Access Privilege Groups	Allows the Administrator to manage/add Access Privilege Groups within the assigned Partitions.
Manage APB	Allows the Administrator to access APB Status page and reset APB per site/area or user.
Manage Cameras and Integration	Allows the Administrator to manage/add camera systems within the assigned Partitions and allows the administrator to add/edit associations between cameras and Doors/Elevators.
Manage Device Holiday Groups	Allows the Administrator to manage/add Device Holiday Groups within the assigned Partitions. These Groups are used for IO-Boards.

Permission Name	Brief Explanation
Manage Door Holiday Groups	Allows the Administrator to manage/add Door Holiday Groups within the assigned Partitions.
Manage Door Holiday TimeZones	Allows the Administrator to manage/add Door Holiday Time Zones within the assigned Partitions.
Manage Door TimeZones	Allows the Administrator to add/schedule Door Time Zones within the assigned Partitions.
Manage Doors	Allows the Administrator to add/edit all aspects of Doors and Readers within the assigned Partitions.
Manage Elevators	Allows the Administrator to add/edit all aspects of Elevators and Floors within the assigned Partitions.
Manage Floor Holiday Groups	Allows the Administrator to edit/add Floor Holiday Groups within the assigned Partitions.
Manage Floor Holiday TimeZones	Allows the Administrator to manage/add Floor Holiday Time Zones within the assigned Partitions.
Manage Floor TimeZones	Allows the Administrator to add/schedule Floor Time Zones within the assigned Partitions.
Manage Holidays	Allows the Administrator to add Holidays and assign them to User Holiday Groups and Door Holiday Groups within the assigned Partitions.
Manage Input Holiday TimeZones	Allows the Administrator to manage/add Input Holiday Time Zones within the assigned Partitions. Used with IO-Boards.
Manage Input TimeZones	Allows the Administrator to add/schedule Input Time Zones within the assigned Partitions. Used with IO-Boards.
Manage Maps	Allows the Administrator to add Active Maps.
Manage Notification Rules	Allows the Administrator to customize their notification settings and styling.
Manage OneTimeRun TimeZones	Allows the Administrator to add/edit One Time Run Time Zones and assign them to Doors within the assigned Partitions.
Manage Output Holiday TimeZones	Allows the Administrator to manage/add Output Holiday Time Zones within the assigned Partitions. Used with IO-Boards.
Manage Output TimeZones	Allows the Administrator to add/schedule Output Time Zones within the assigned Partitions. Used with IO-Boards.
Manage Panels	Allows the Administrator to edit all aspects of Door Panels within the assigned Partitions, and the ability to add new Door Panels.
Manage Sites	Allows the Administrator to add additional Sites and assign them to Partitions they have permission in.
Manage User Holiday Groups	Allows the Administrator to manage/add User Holiday Groups within the assigned Partitions.
Manage User Holiday TimeZones	Allows the Administrator to manage/add User Holiday Time Zones within the assigned Partitions.
Manage User TimeZones	Allows the Administrator to manage/add User Time Zones within the assigned Partitions.
Manage Users	Allows the Administrator to edit Users and add Users to Access Privilege Groups and/or assigned Partitions.

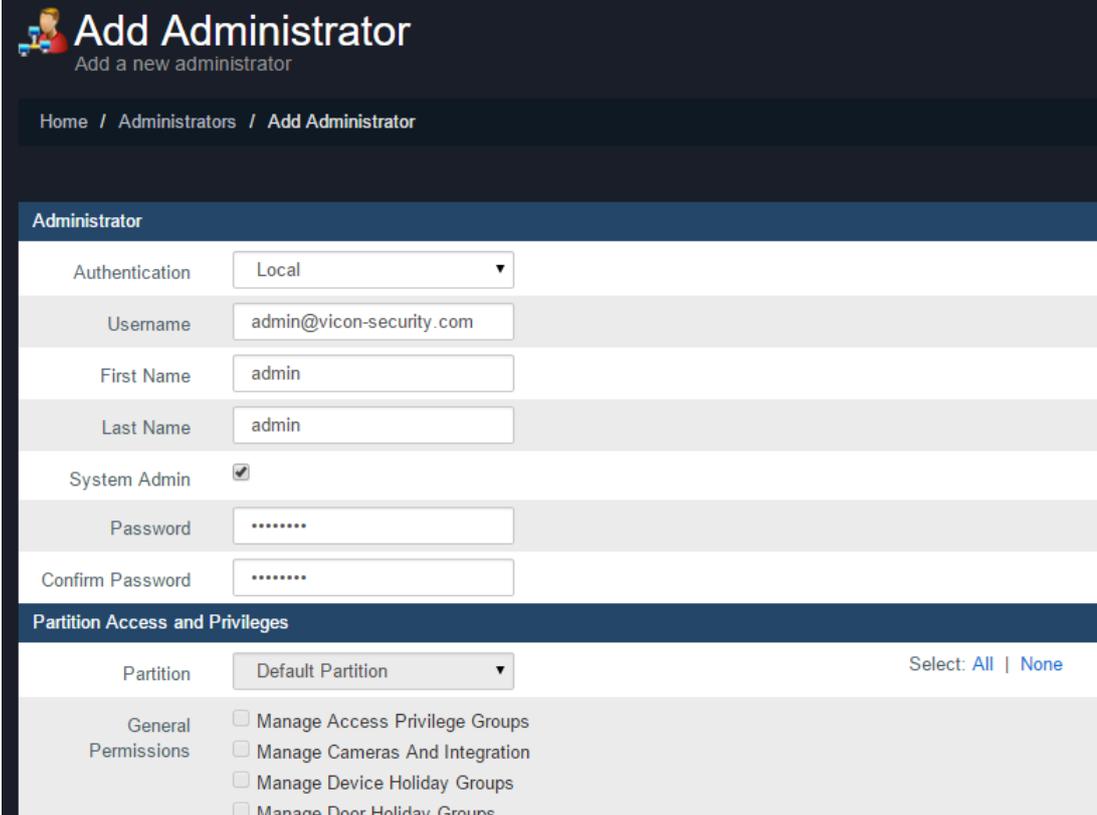
Permission Name	Brief Explanation
Reporting Action Plans	Allows the Administrator to run Action Plan reports within their Partitions.
Reporting APB	Allows the Administrator to run Muster reports within their Partitions.
Reporting Configuration	Allows the Administrator to run system configuration reports within their Partitions.
Reporting Door Activity	Allows the Administrator to run Door activity reports on Doors within their Partitions.
Reporting Elevator Activity	Allows the Administrator to run Floor activity reports on Elevators/Floors within their Partitions.
Reporting IO	Allows the Administrator to run Input and Output activity reports on IO-Board Inputs/Outputs within their Partitions.
Reporting Monitoring Module	Allows the Administrator to access the Monitoring screen.
Reporting UserActivity	Allows the Administrator to run User activity reports on Users associated with Access Privilege Groups within their Partitions.
Reporting User List	Allows the Administrator to generate and export a User list of the Users associated within their Partitions.
Reporting User Time Tracking	Allows the Administrator to generate User Tracking reports within their Partitions.
Disengage Emergency Alarm	Allows the Administrator to disengage the Emergency Alarm through system overview within their Partitions.
Special Permissions: Override Door	Allows the Administrator to override Doors in their assigned Partitions using the override Doors quick drop-down menu, or through system overview.
Special Permissions: Override Floor	Allows the Administrator to override Floors in their assigned Partitions using the override Floors quick drop-down menu, or through system overview.
Special Permissions: Override Input/Output	Allows the Administrator to override Inputs and Outputs in their Door and IO Panels within their assigned Partitions using the override Outputs quick drop-down menu.
Special Permissions: Pulse Door	Allows the Administrator to Pulse doors to unlock momentarily in their assigned Partitions using the override Doors quick drop-down menu, or through system overview.
Special Permissions: Update Panel	Allows the Administrator to update Door Panels within their Partitions using the update Panels button or through system overview.
Special Permissions: View Cameras	Allows the Administrator to view any live or historical camera views for any cameras assigned to their Partitions.
Special Permissions: View Maps	Allows the Administrator to view and edit Active Maps assigned to their Partitions.
Special Permissions: View Status	Allows the Administrator to see the system overview screen, including Panel and Door status on Panels and Doors assigned to their Partitions.

- 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.

Tip

There are **Select All** and **Select None** buttons on the top right of this screen for quickly assigning administrator permissions.

Figure 20.1. Add Administrator



Add Administrator
Add a new administrator

Home / Administrators / Add Administrator

Administrator

Authentication: Local

Username: admin@vicon-security.com

First Name: admin

Last Name: admin

System Admin:

Password:

Confirm Password:

Partition Access and Privileges

Partition: Default Partition Select: All | None

General Permissions:

- Manage Access Privilege Groups
- Manage Cameras And Integration
- Manage Device Holiday Groups
- Manage Door Holiday Groups

Administrator 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

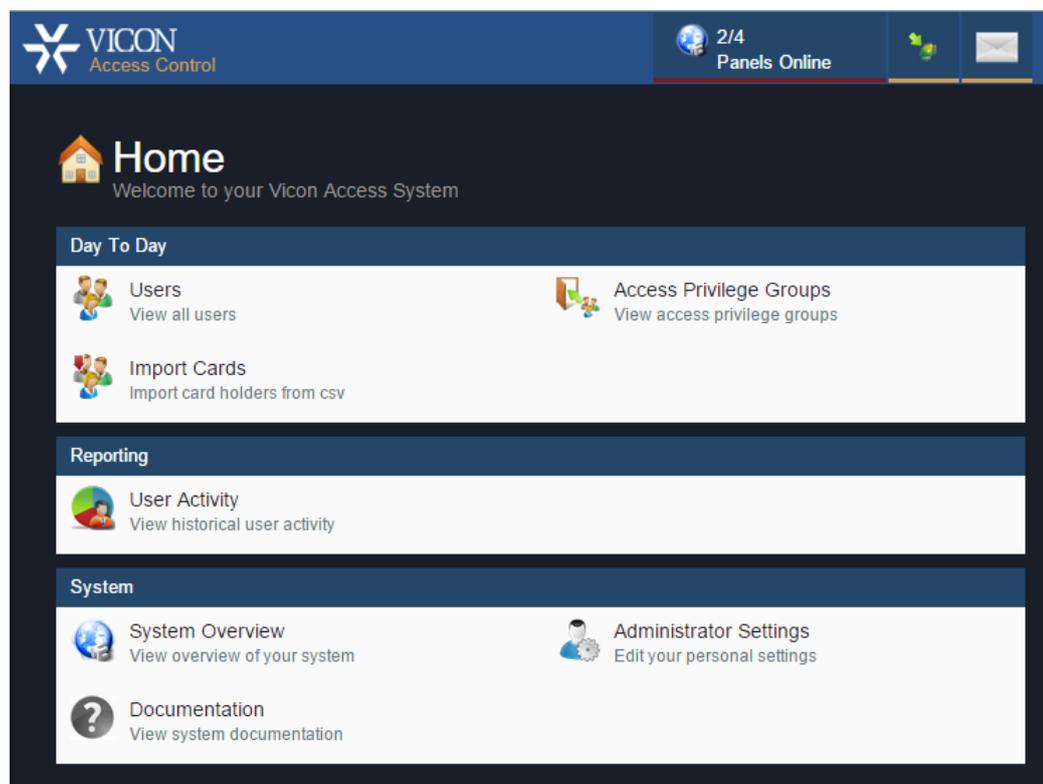
After the system is commissioned, the security integrator hands over an Administrator account to the organization that purchased the system. The security staff gives an Administrator Account to the secretary at the front desk with the following permissions:

- Manage Access Privilege Groups
- Manage Users
- 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 20.2. Administrator With Limited Permissions

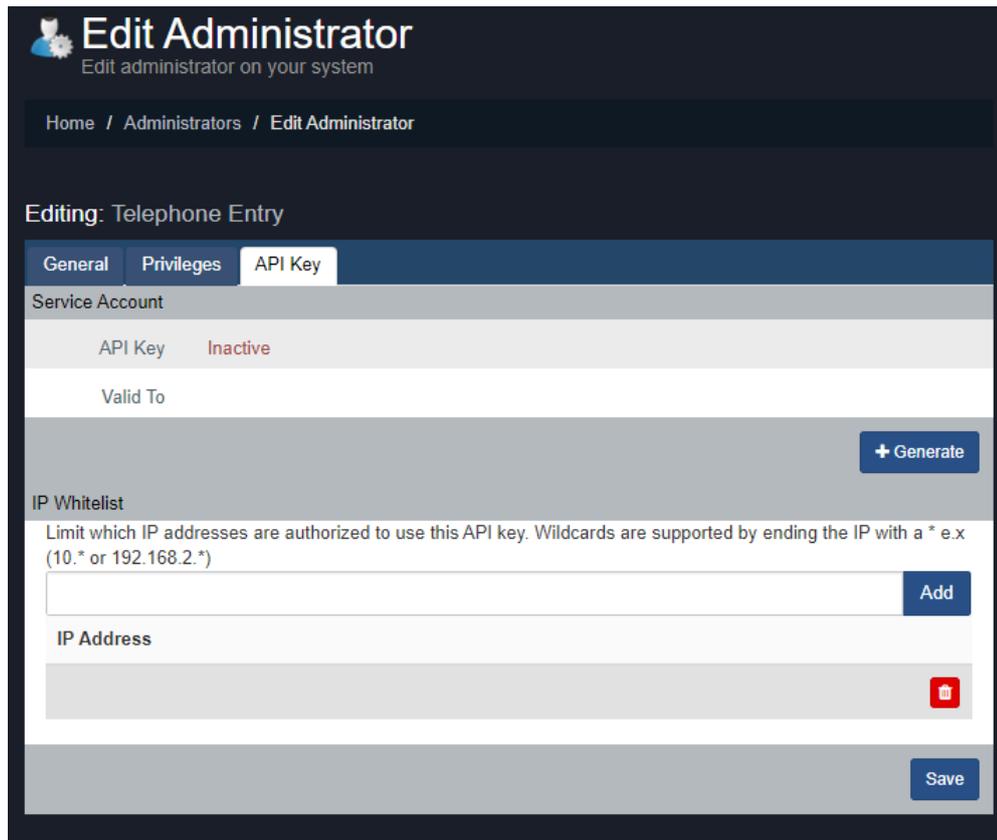


Service Account Administrators for Third-party Services

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

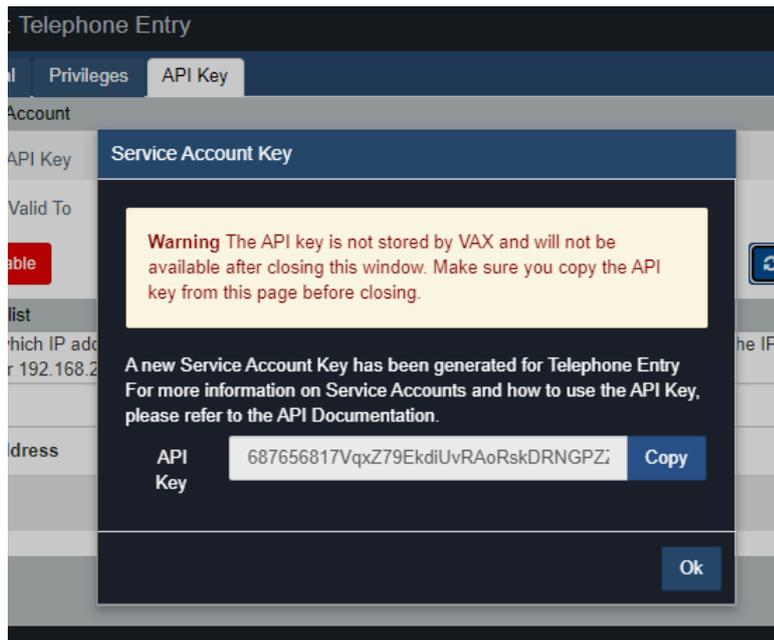
1. After you add the Administrator, navigate to the Edit Administrator screen for the Service Account Administrator.
2. Navigate to the API Key tab

Figure 20.3. 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 20.4. 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 20.5. IP Whitelist

Editing: Telephone Entry

General Privileges **API Key**

Service Account

API Key Active

Valid To August 13, 2021

✖ Disable **↻ Regenerate**

IP Whitelist

Limit which IP addresses are authorized to use this API key. Wildcards are supported by ending the IP with a * e.x (10.* or 192.168.2.*)

192.168.2.20 **Add**

IP Address

192.168.2.40	✖
192.168.1.*	✖

Save

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.

Chapter 21. Areas and Anti-Passback

This chapter covers the configuration of Anti-Passback in VAX. This feature is available in version 2.7 or above and is only supported on select Panel models.

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.

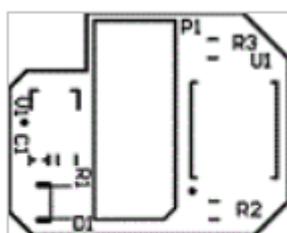
- Panel must be a Single-door Panel, no motion (VAX-1D) or Two Door Controller (VAX-2D) or Multi Door Kit (VAX-MDK). Other Panel models do not support this feature.
- If a Panel must make anti-passback decisions, it will require a **Memory Module**. Please see the following section on the APB Memory Module.
- VAX will need to be at least Version 2.1.50 for Local anti-passback. 2.7 for Global anti-passback.
- 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

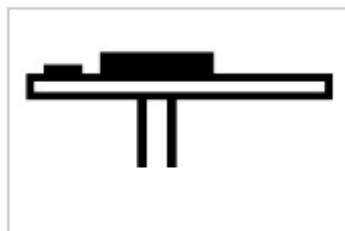
In order for a controller to make anti-passback decisions, it must have a Memory Module installed. Panels without a memory module will be unable to raise anti-passback violations but can report to the server when a User enters an Area, which can be forwarded to other Panels assigned to the same Areas.

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

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 Vicon 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. On the **Home Screen**, scroll down to the section titled **System**; click on the **Sites and Areas** icon (pictured below).



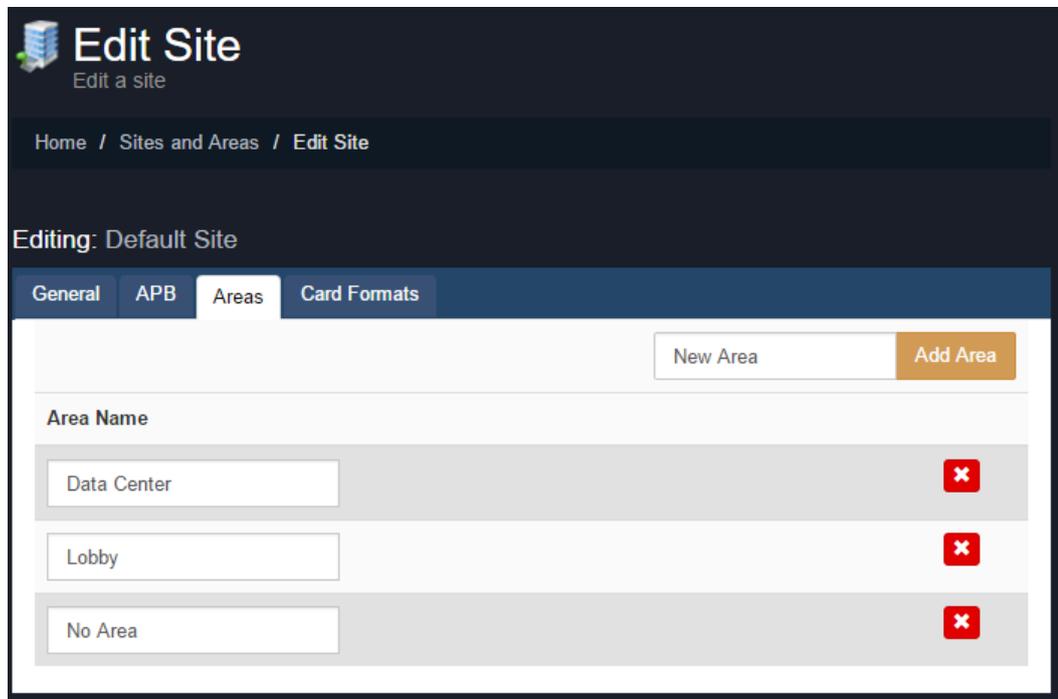
4. On the **Sites and Areas** screen, you'll see any sites you've created. Click the blue button (advanced settings) next to the Site you'll be using APB with.
5. On the Edit Site screen, click on the **Areas** tab.
6. On the **Areas** tab, enter a name for your new area and click the **Add Area** button 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 **Home Screen**, scroll down to the section titled **System**; click on the **Sites and Areas** icon (pictured below).



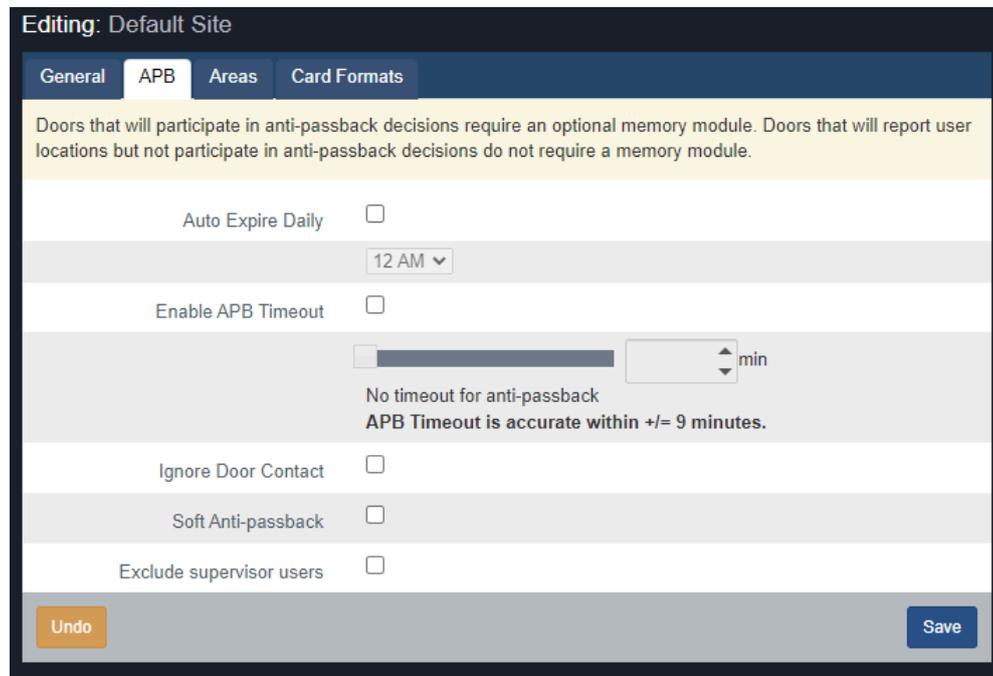
2. On the **Sites and Areas** screen, you'll see any sites you've created. Click the blue button (advanced settings) next to the Site you'll be using APB with.
3. On the Edit Site screen, click on the **APB** tab.

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 **Home Screen**, scroll down to the section titled **Hardware**; click on the **Doors** icon (pictured below).

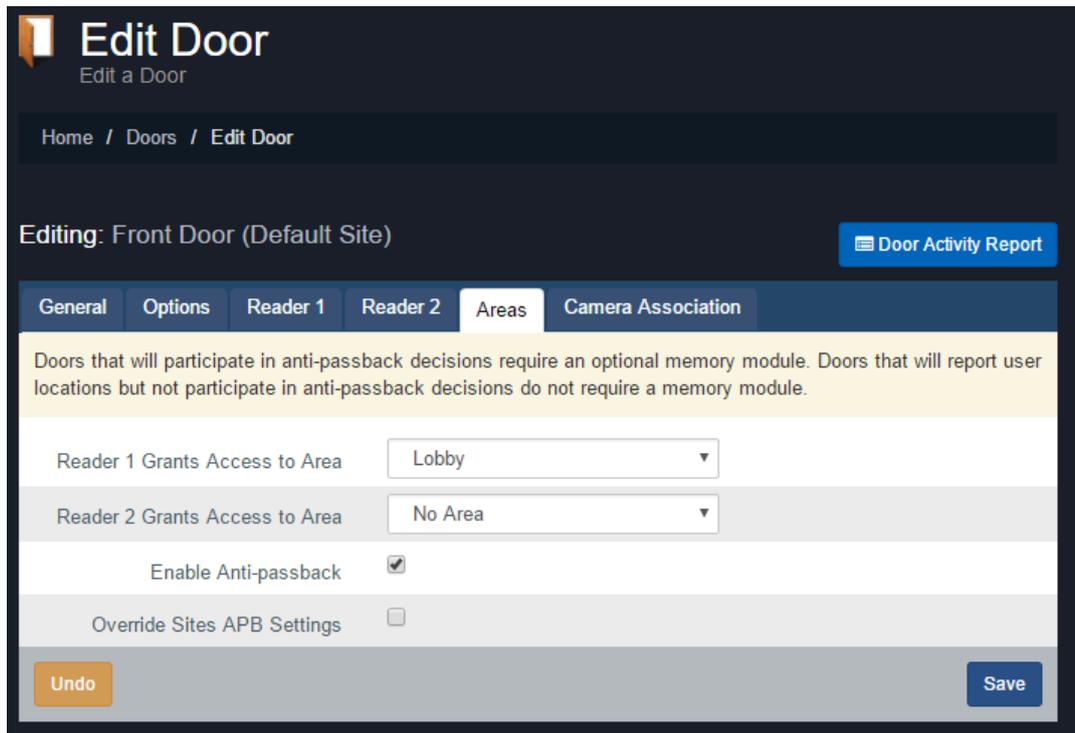


2. On the **Doors** screen, you'll see any Doors you've already configured listed here. Click the blue button next to the Door you'd like to configure APB on.
3. On the **Edit Door** screen, you'll see 5 tabs. Click on the **Areas** tab. The configuration items on this screen are explained below:

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.

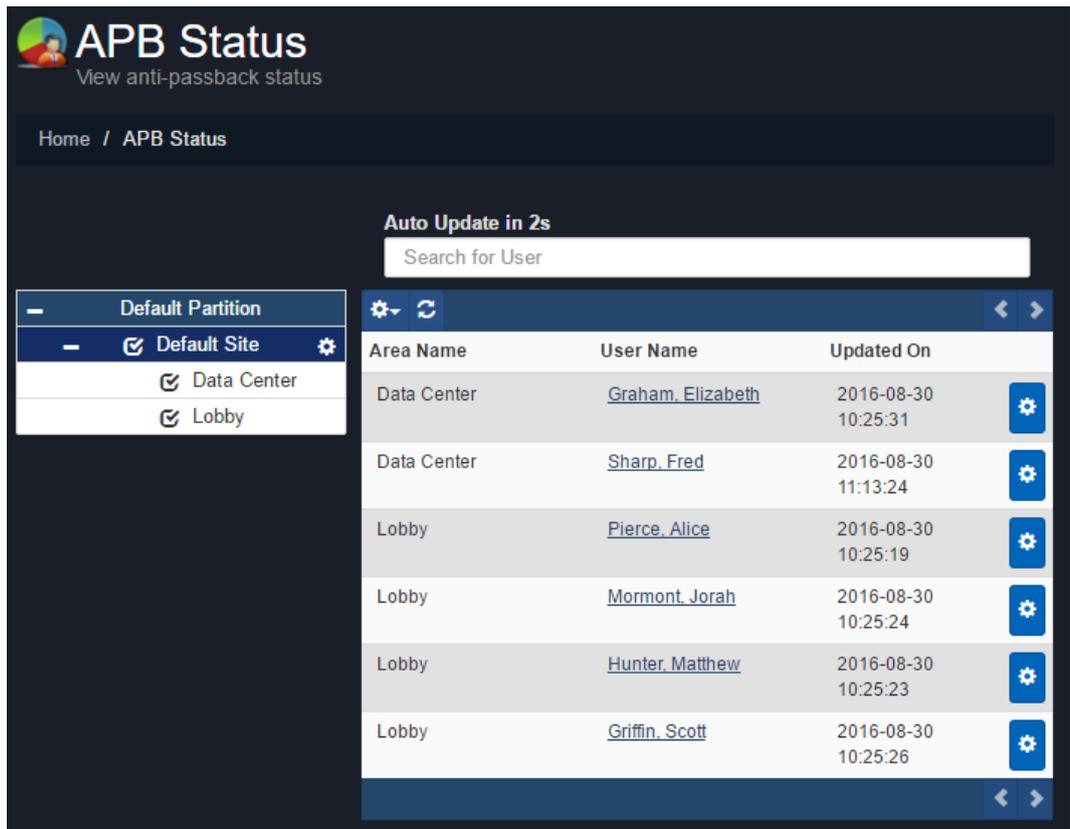
Most monitoring of APB can be done from the APB Status screen.

1. On the **Home Screen**, scroll down to the section titled **Day To Day**; 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



Chapter 22. Mantrap Configuration

This chapter covers the configuration of Mantraps in Vicon Access Control. This feature is available in version 2.3+ and is only supported on select Panel models and may require additional wiring in order to function.

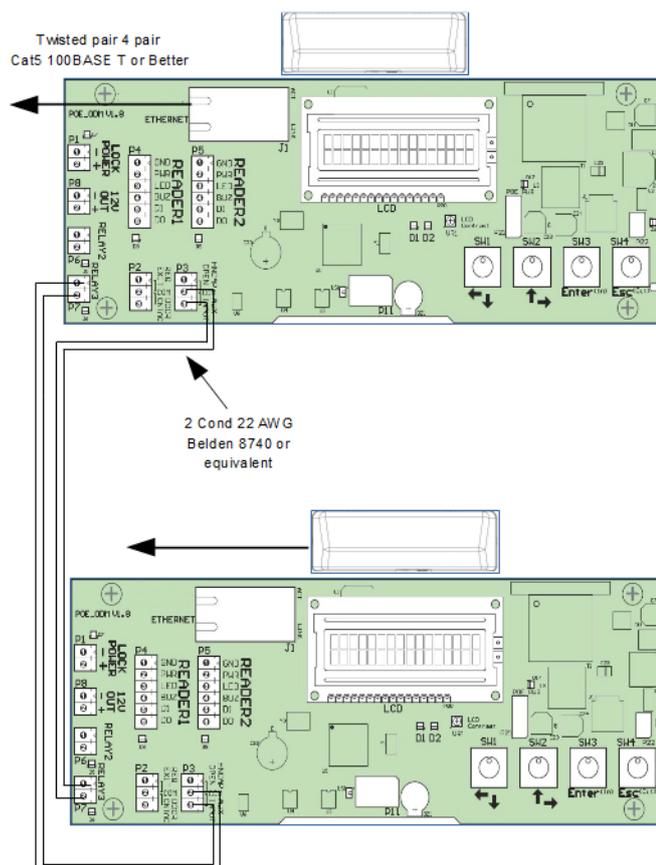
Mantrap (also called air lock or access control vestibule) is commonly used in high security areas where a cardholder enters an enclosed space between two (or more) doors. When the first door is opened or unlocked, the second door will receive a signal from the opened door instructing it not to open 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 Single-Door Panels (2 x VAX-1D) and Two-Door Panels (1 x VAX-2D).

VAX-1D Configuration: 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. VAX-1D Mantrap



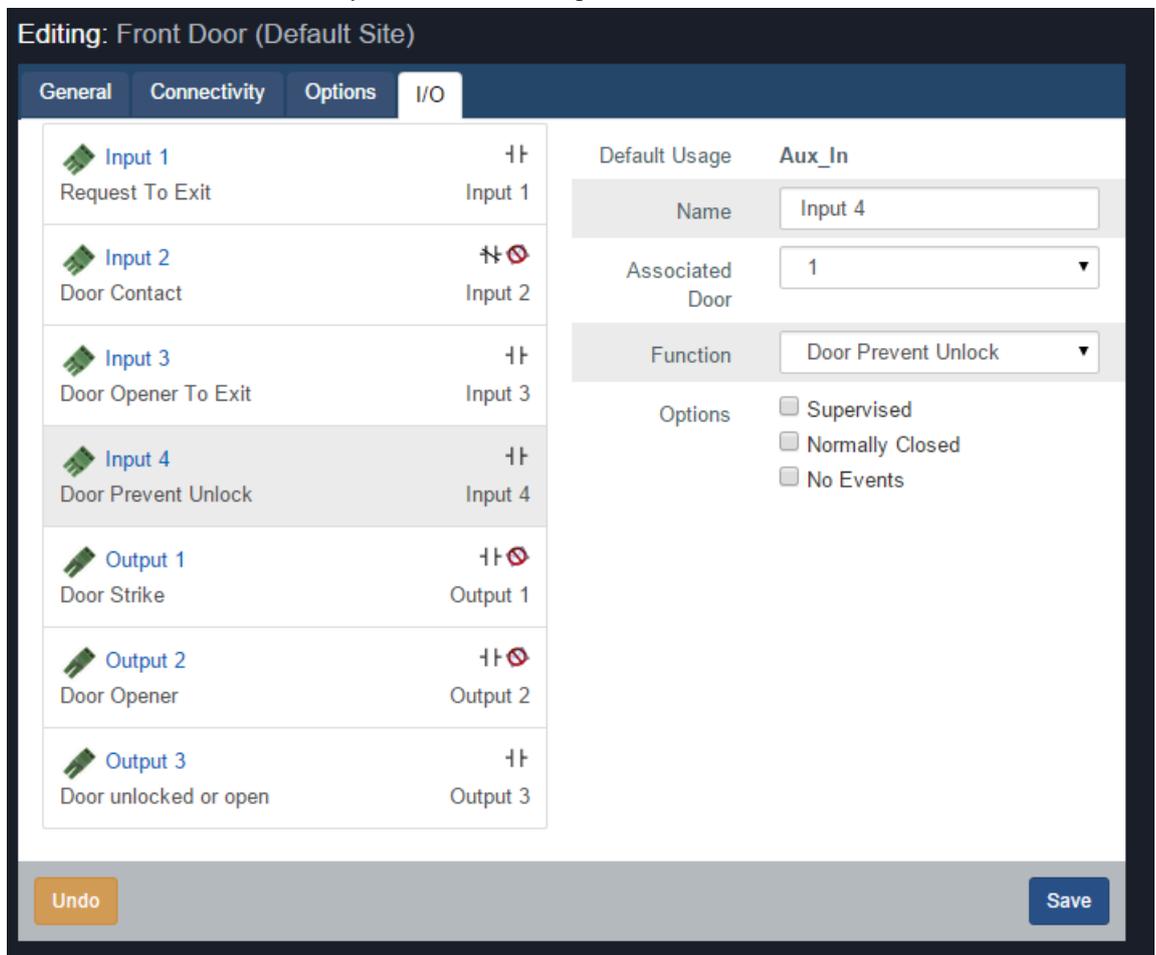
Once the above diagram has been implemented, use the following steps to configure the Input/Outputs.

1. Access your Vicon 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.

- On the **Home Screen**, scroll down to the section titled **Hardware**; click on the **Panels** icon (pictured below).



- Click the **blue** button (Advanced Settings) next to the Panel you'd like to configure.
- 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.
- 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".
- Select the Output the Panel that will be signaling the other Panel. Change the Function drop-down menu to "Door Unlocked or Open".
- Your I/O screen should look very similar to the example below:



- 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.

VAX-2D 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 **Home Screen**, 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.

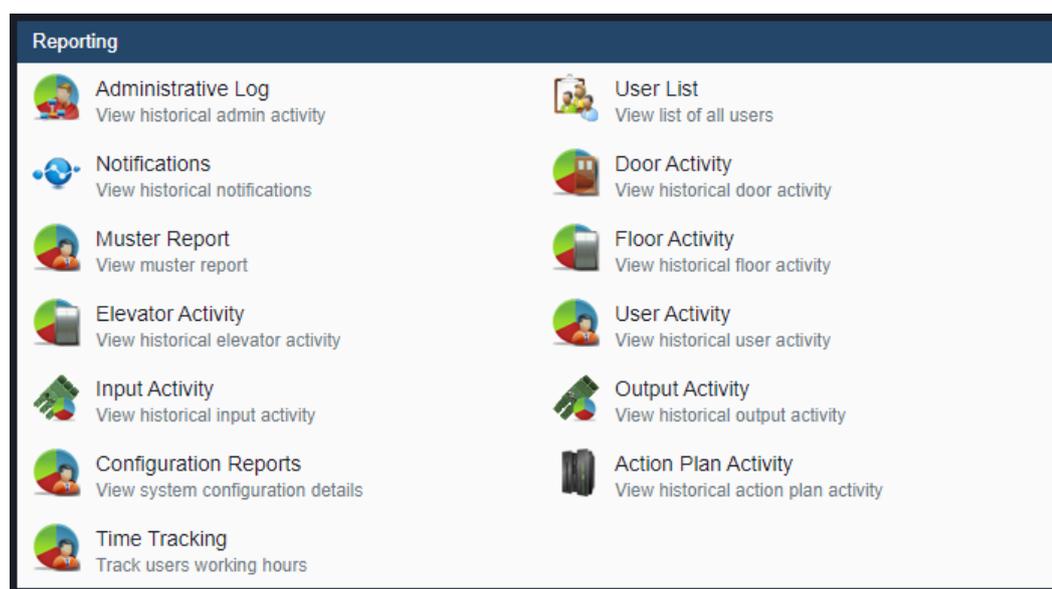
Chapter 23. Reporting

This chapter will be an overview of the various reporting features in Vicon Access Control. 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
Time Tracking Report	

Figure 23.1. Reporting Icons



Administrative Log

This section covers what the Administrative Log is and how to run it in Vicon Access Control.

The Administrative Log is a report used for tracking the activities of other Administrators in Vicon Access Control. 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:

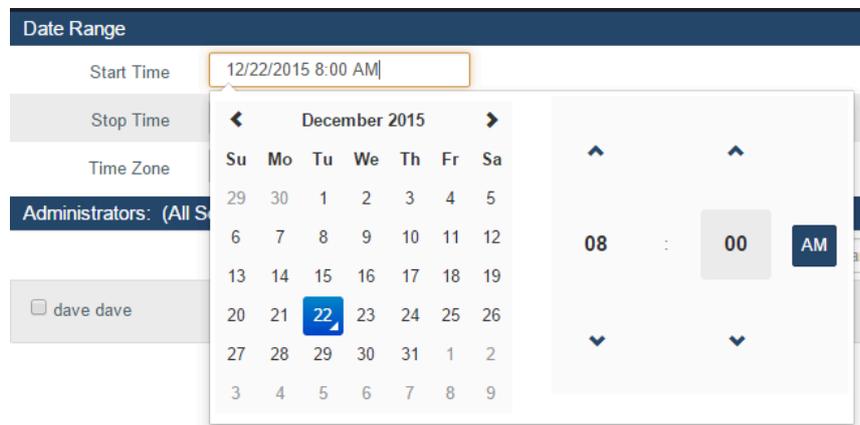
1. On the **Home Screen**, scroll down to the section titled **Reporting**; click on the **Administrative Log** icon (pictured below).



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 Vicon Access Control.

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 **Reporting 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:

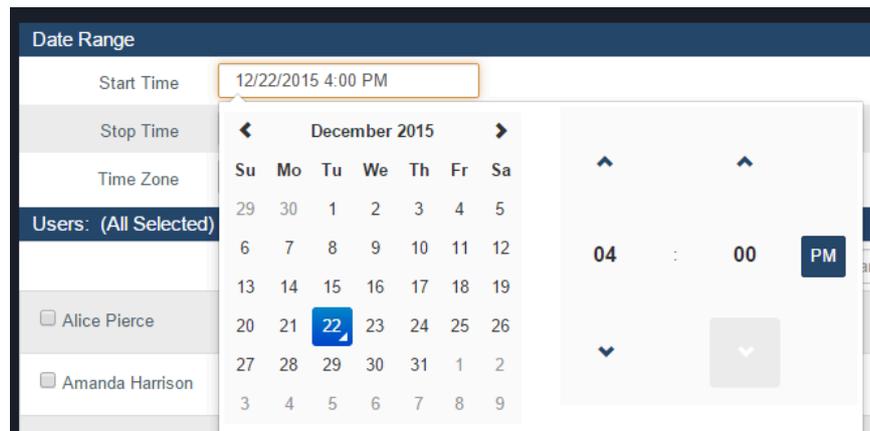
1. On the **Home Screen**, scroll down to the section titled **Reporting**; click on the **User Activity** icon (pictured below).



2. 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. 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.

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 Vicon Access Control.

The Door Activity Report is used for tracking the activities of Doors in Vicon Access Control. 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:

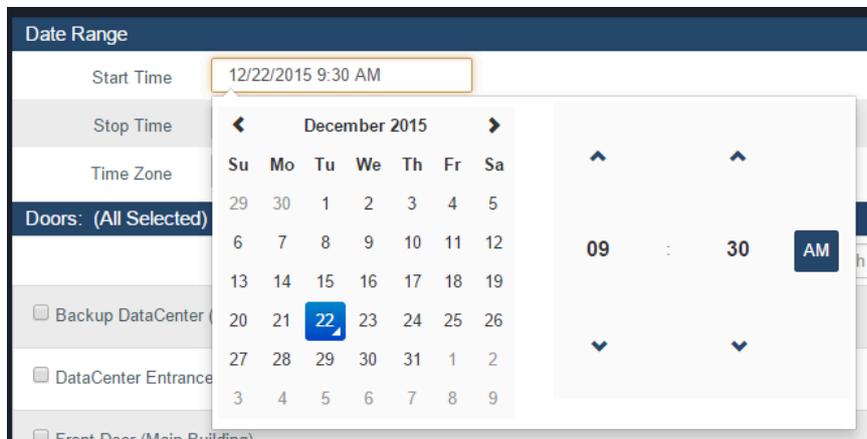
1. On the **Home Screen**, scroll down to the section titled **Reporting**; click on the **Door Activity** icon (pictured below).



2. 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 23.6. 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 23.7. 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 23.8. Sorting



- e. **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.

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 Vicon Access Control.

The Floor Activity Report is used for tracking the activities of Floors in Vicon Access Control. 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 report 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:

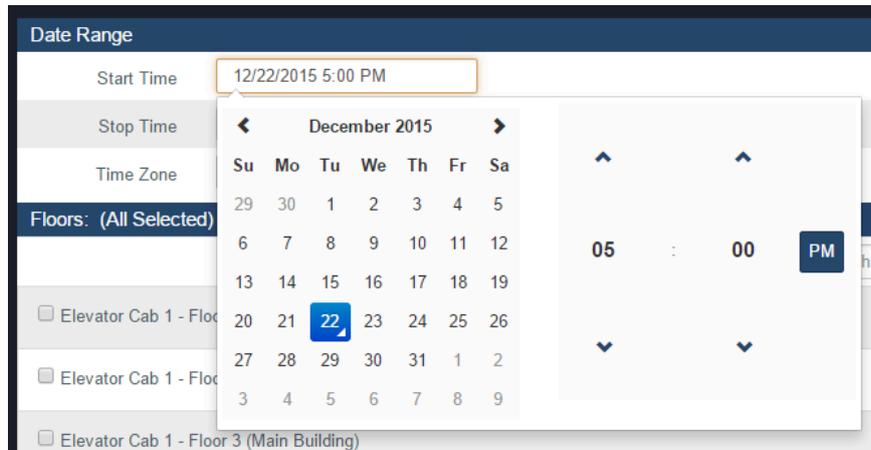
1. On the **Home Screen**, scroll down to the section titled **Reporting**; click on the **Floor Activity** icon (pictured below).



2. 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 23.9. 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 23.10. 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 23.11. Sorting



- e. **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.

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 Vicon Access Control.

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:

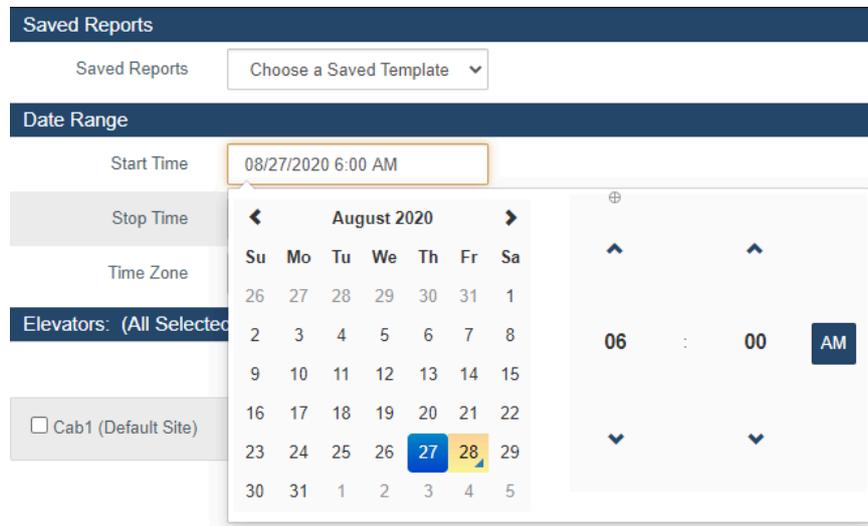
1. On the **Home Screen**, scroll down to the section titled **Reporting**; click on the **Elevator Activity** icon (pictured below).



2. 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 23.12. Date Picker Widget



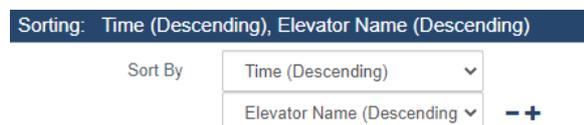
- b. **Elevators:** Select the Elevators you'd like to run the report against. You can select more than one at a time, or just an individual cab. The search bar can be used to find Elevators quickly.
- c. **Notification Types:** You can filter which notifications appear in the report in this section. All notification types are selected by default.

Figure 23.13. 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 23.14. Sorting



e. **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.

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 Vicon Access Control.

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 **Home Screen**, 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 Permissions	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.

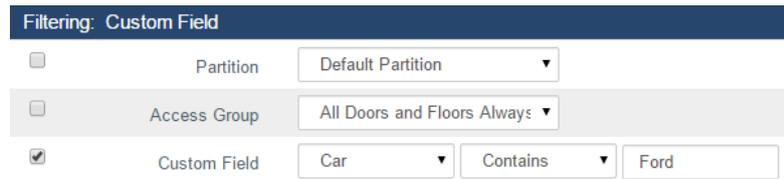
Figure 23.15. User List Options

- b. **Filtering:** You can further filter which Users appear in the report results here.

Table 23.3. Anti-Passback Configuration Items

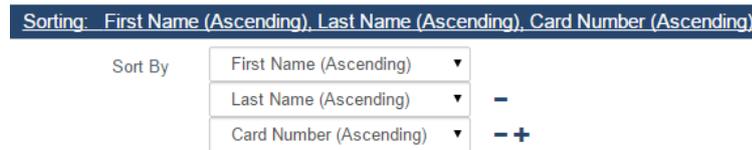
User List Filter	Description
Partition	Check and select a Partition to filter the report to only include users in the selected Partition.
Access Group	Check and select an Access Group to filter the report to only include users in the selected Access Group.
Custom Field	Check and select a custom field. You can set the filter to 'Starts With', 'Ends With', 'Contains' or 'Equals'. Fill in a custom field value to filter the report to only include Users that have the custom field based on your filter.

Figure 23.16. 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 23.17. Sorting



- d. **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.

Notifications Report

This section will cover what the Notifications Report is and how to run it in Vicon Access Control.

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:

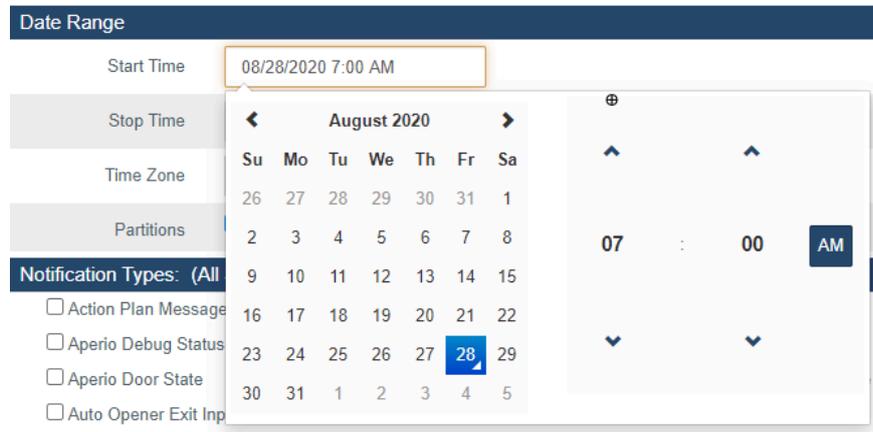
1. On the **Home Screen**, scroll down to the section titled **Reporting**; click on the **Notifications** icon (pictured below).



2. Once on the **Notifications** screen, you'll have 4 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 23.18. 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 23.19. 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 23.20. Sorting:

- d. **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.

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 Vicon Access Control.

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 **Home Screen**, scroll down to the section titled **System**; click on the **Sites and Areas** icon (pictured below).

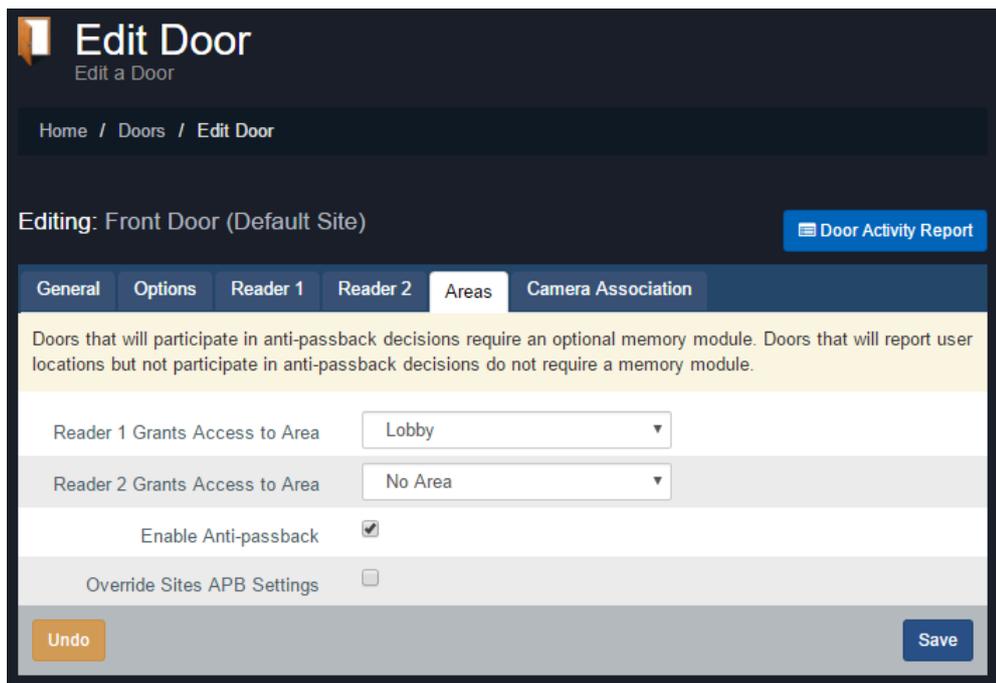


2. On the **Sites and Areas** screen, you'll see any sites you've created. Click the blue button (advanced settings) next to the Site you'd like to add Areas to.
3. On the Edit Site screen, click on the **Areas** tab.
4. On the **Areas** tab, enter a name for your new area and click the **Add Area** button on the right side. Add additional Areas as needed.
5. On the **Home Screen**, 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 23.21. Area Settings



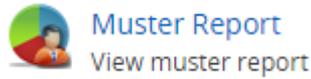
8. **Reader 1 Grants Access to Area:** The Area that Reader 1 grants access to. Select a custom Area or 'No Area'.

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 **Home Screen**, scroll down to the section titled **Reporting**; click on the **Muster Report** icon (pictured below).

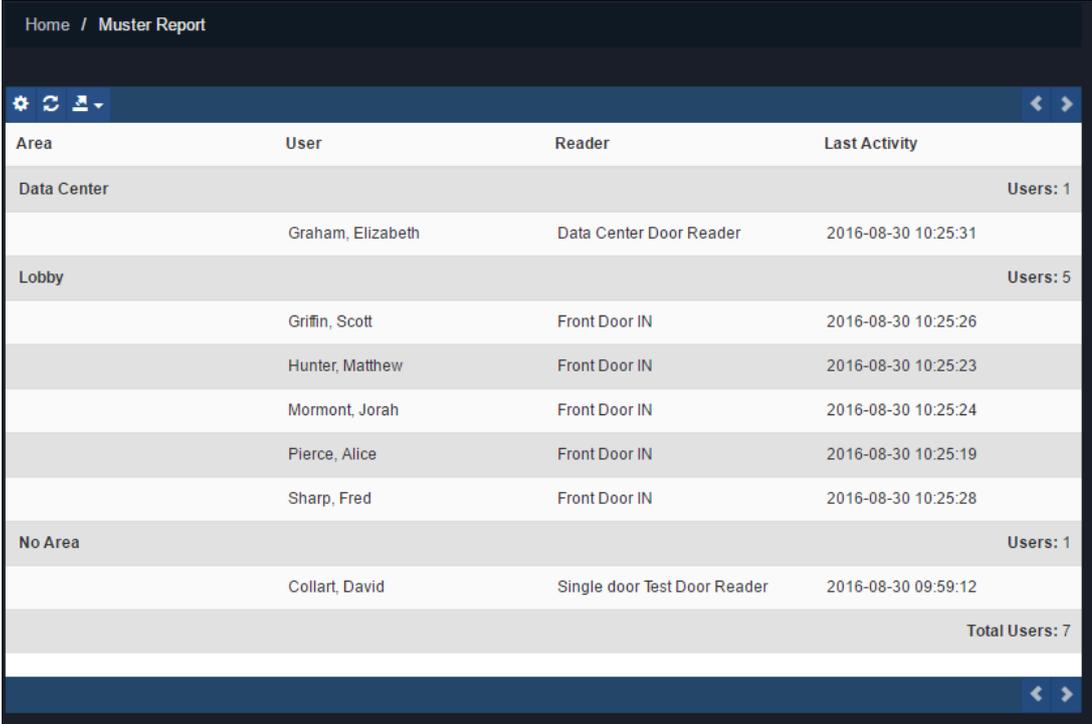


2. Once on the **Muster Report** screen, you'll have 3 sections to populate.
3. **Date Range:**
 - a. Select the **Start Time** you'd like to run the report against. The **Date Picker Widget** will appear. Use the calendar and time picker to select the date & time to start the report. The report will inquire for data between the Start Time and the current time.
 - b. Select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.
 - c. Select the **Partition** that the areas reside in that you want to run the report against.
 - d. Select the **Sites** that the areas reside in that you want to run the report against.

Figure 23.22. Date Picker Widget

The screenshot shows a 'Date Range' widget with a sidebar on the left and a date picker on the right. The sidebar includes fields for 'Start Time', 'Time Zone', 'Partition', 'Site', 'Areas: (All Selected)', 'Data Center', and 'Loby'. The date picker displays a calendar for November 2015, with the date 27 highlighted. The time is set to 12:00 AM.

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. Inline (results displayed in web browser) is the default. CSV and HTML can also be selected.
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.

Figure 23.23. Muster Report Results


Area	User	Reader	Last Activity
Data Center			Users: 1
	Graham, Elizabeth	Data Center Door Reader	2016-08-30 10:25:31
Lobby			Users: 5
	Griffin, Scott	Front Door IN	2016-08-30 10:25:26
	Hunter, Matthew	Front Door IN	2016-08-30 10:25:23
	Mormont, Jorah	Front Door IN	2016-08-30 10:25:24
	Pierce, Alice	Front Door IN	2016-08-30 10:25:19
	Sharp, Fred	Front Door IN	2016-08-30 10:25:28
No Area			Users: 1
	Collart, David	Single door Test Door Reader	2016-08-30 09:59:12
			Total Users: 7

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 Vicon Access Control that let you export system information. This can include network information for all your Panels, names and schedule for all your doors, how your timezones are configured and many more.

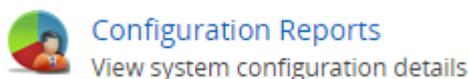
This section will cover where and how to run these reports and some information on each individual Configuration Report.

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 **Home Screen**, 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.

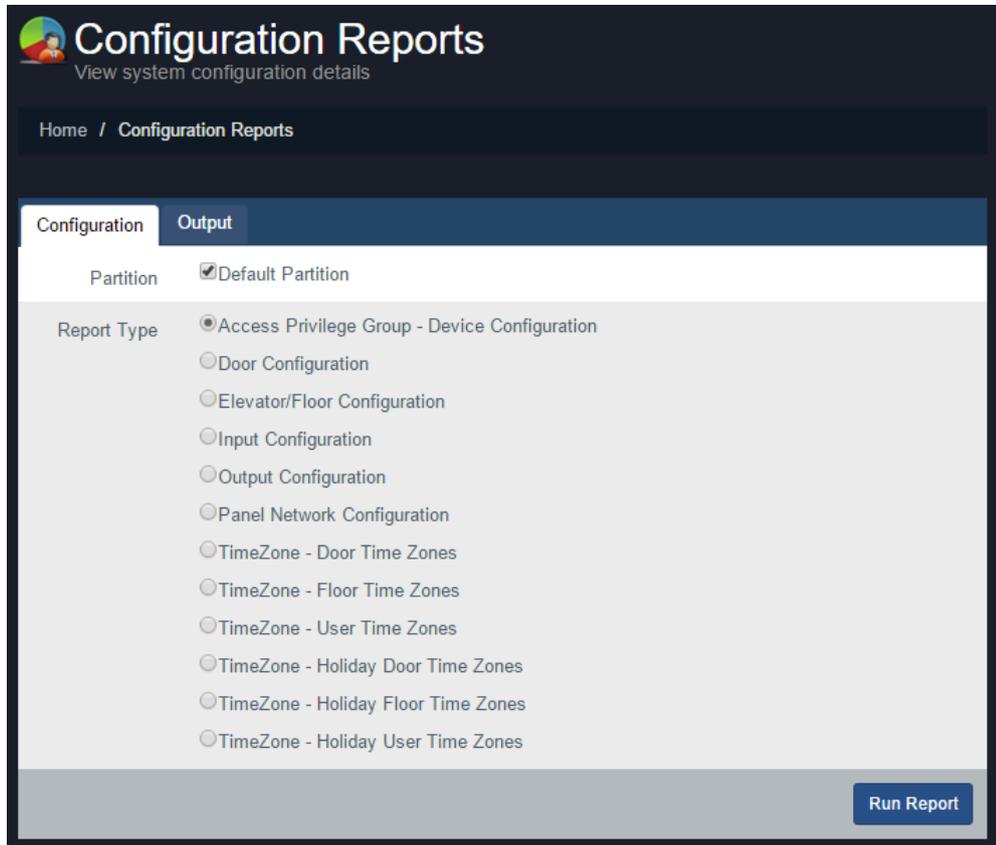
The following table outlines each of the configuration reports:

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 Time Zone 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 Time Zone 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 Time Zone 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 Time Zones, 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 Time Zone 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.
Time Zone - Door Time Zones	Will create an exportable list of all Door Time Zones in the selected Partitions along with the configured time spans and associated modes for each day of week.
Time Zone - Floor Time Zones	Will create an exportable list of all Floor Time Zones in the selected Partitions along with the configured time spans and associated modes for each day of week.
Time Zone - User Time Zones	Will create an exportable list of all User Time Zones in the selected Partitions along with the configured time spans and associated modes for each day of week.
Time Zone - Holiday Door Time Zones	Will create an exportable list of all Holiday Door Time Zones in the selected Partitions along with the configured time spans and associated modes for each day of week.
Time Zone - Holiday Floor Time Zones	Will create an exportable list of all Holiday Floor Time Zones in the selected Partitions along with the configured time spans and associated modes for each day of week.

Report	Description
Time Zone - Holiday User Time Zones	Will create an exportable list of all Holiday User Time Zones in the selected Partitions along with the configured time spans and associated modes for each day of week.

Figure 23.24. Configuration Reports Screen



- 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 **Output Tab** of the page where you can view the results of the report. If you'd like to change the parameters of the report, you can switch back to the **Parameters** to change report parameters.
- 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 Vicon Access Control.

The Input Activity Report is used for tracking the activities of Aux Inputs in Vicon Access Control. 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:

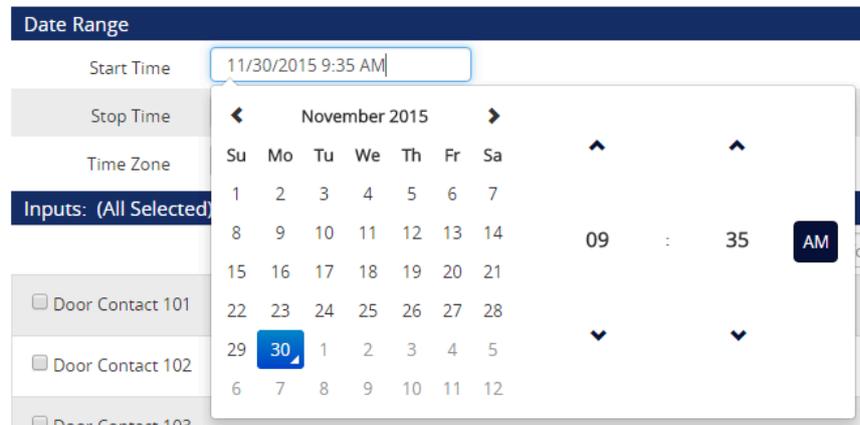
1. On the **Home Screen**, scroll down to the section titled **Reporting**; click on the **Input Activity** icon (pictured below).



2. 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 23.25. 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 23.26. 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 23.27. Sorting



- e. **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.

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 Vicon Access Control.

The Output Activity Report is used for tracking the activities of Aux Outputs in Vicon Access Control. 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:

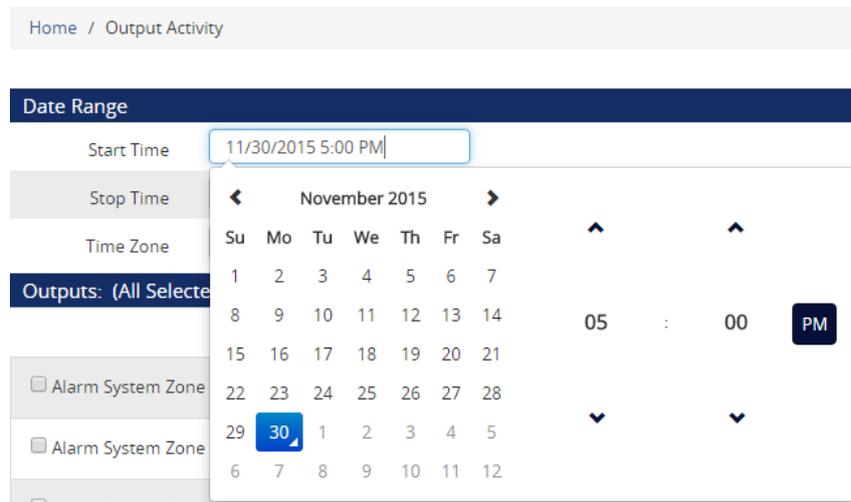
1. On the **Home Screen**, scroll down to the section titled **Reporting**; click on the **Output Activity** icon (pictured below).



2. 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 23.28. 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 Time Zone Changed and several other filters.

Figure 23.29. 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 23.30. Sorting



- e. **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.

Information that is presented on exported 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 Vicon Access Control.

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 **Home Screen**, scroll down to the section titled **Reporting**; click on the **Action Plan Activity** icon (pictured below).



2. 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 23.31. Date Picker Widget

The screenshot shows a 'Date Range' widget with a dark blue header. Below the header, there are input fields for 'Start Time' (01/03/2017 4:00 AM), 'Stop Time', and 'Time Zone'. A date picker calendar is open, showing January 2017. The date 03 is highlighted in blue. To the right of the calendar, there are time selection controls showing '04 : 00 AM'. Below the date picker, there are several filter sections: 'Action Plans: (All Selected)', 'Notification Types: (All Selected)' with checkboxes for 'Action Plan Error' and 'Action Plan Message', 'Sorting: Time (Descending)', and 'Output: Inline'.

- 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 23.32. Notification Types

The screenshot shows the 'Notification Types: (All Selected)' section. It features two checkboxes: 'Action Plan Message' and 'Action Plan State', both of which are currently checked.

- 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 23.33. Sorting

The screenshot shows the 'Sorting: Time (Descending)' section. It includes a 'Sort By' dropdown menu with 'Time (Descending)' selected, and a plus sign icon to the right.

- e. **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.

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 Vicon Access Control.

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 **Home Screen**, 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 5 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 23.34. Date Picker Widget

The screenshot shows a 'Date Range' section with two input fields: 'Start Date' (2017-04-17) and 'Stop Date' (2017-05-19). Below these is a section for 'In Readers: (1 Selected)' with two options: 'Front Door Out' (unchecked) and 'Front Door Reader' (checked). A calendar widget for April 2017 is displayed, showing dates from 26 to 6. The date 14 is highlighted with a mouse cursor.

- 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. 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 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.

Time Tracking Output

This contains examples of how the report will look once exported.

Figure 23.35. Report Results Inline

		Entry Time	Exit Time	Total
33 - 55998	Alice Pierce			
		2017-04-21 09:27:06	2017-04-21 13:11:33	3.73
		2017-04-25 10:28:35		0
				3.73
33 - 55990	Brandon Diaz			
		2017-04-21 09:27:08	2017-04-21 13:11:31	3.73
		2017-04-25 10:28:37		0
				3.73

Figure 23.36. Report Results HTML

VAX User Time Tracking Report

Run On: 5/17/2017 4:09:58 PM

	Entry Time	Exit Time	Total
33-55990	Brandon Diaz		
	4/21/2017 9:27:08 AM	4/21/2017 1:11:31 PM	3.73
	4/25/2017 10:28:37 AM		0
		Total	3.73
33-55891	Elizabeth Graham		
	4/21/2017 9:27:09 AM	4/21/2017 1:11:29 PM	3.73
	4/25/2017 10:28:39 AM		0
	5/5/2017 12:01:49 PM		0
		Total	3.73
33-55997	Frank Gibson		
	4/21/2017 9:27:11 AM	4/21/2017 1:11:27 PM	3.73
	4/25/2017 10:28:41 AM		0
	5/5/2017 12:01:48 PM		0
		Total	3.73
33-55994	Jacqueline Griffin		
	4/21/2017 9:27:12 AM	4/21/2017 1:11:26 PM	3.73
	4/25/2017 10:28:44 AM		0
	5/5/2017 12:01:42 PM		0
		Total	3.73

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.

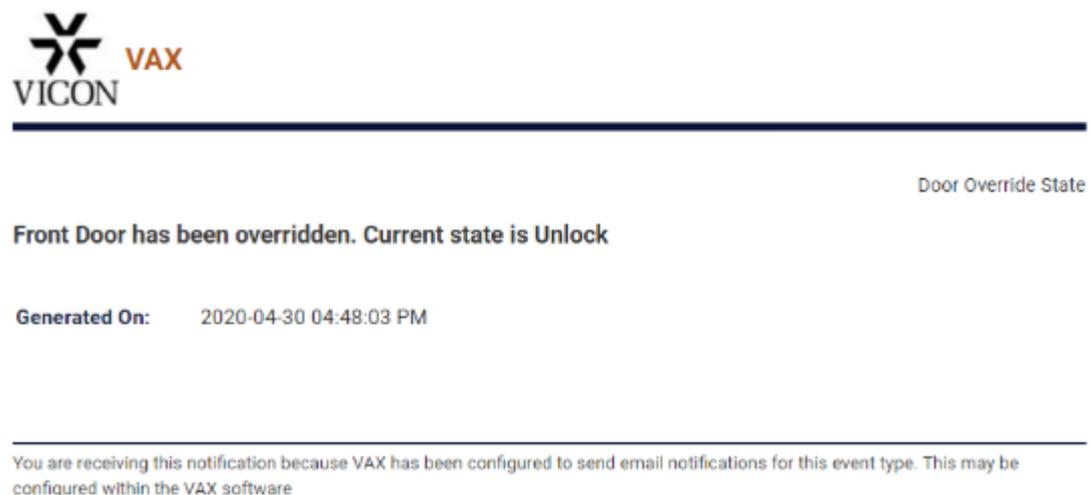
Real Time

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.

Figure 24.1. Email Example



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

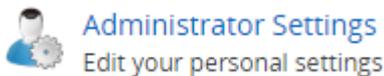
Browser	Minimum Version
Windows	
Chrome	Version 50 or higher
Firefox	Version 44 or higher
Edge	Version 17 or higher
Opera	Version 42 or higher
Mac/Linux	
Chrome	Version 50 or higher
Android	
Chrome	Version 81 or higher
Firefox	Version 68 or higher

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.



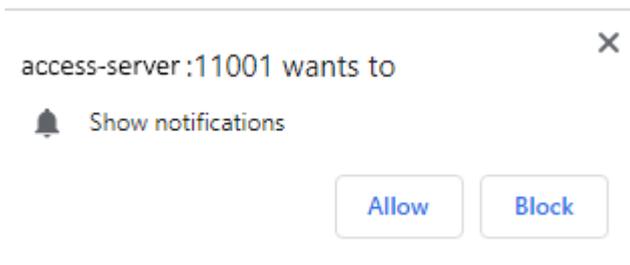
2. Open the **Web Push** tab at the top of the page.



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

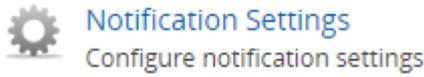
This does not apply to Database rules, which are always global.

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 **Home Screen**, 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.

Notification Rule

Partition	<input type="text" value="Default Partition"/>
Destination Sink	<input type="text" value="Realtime"/>
Type	<input type="radio"/> Global <input checked="" type="radio"/> Administrator
Group	<input type="text" value="Choose..."/> <input type="text" value="Group"/> +
Accept	<input checked="" type="checkbox"/>

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.

Filter

Notification Category	<input type="text" value="Door Contact State"/> x
Notification Types	<input type="text"/> Forced Open Held Open Open Closed v
📄 Panel	<input type="text" value="Panel"/> VAX MDK 8 Door v
🚪 Door	<input type="text" value="Door"/> Front Door v

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.

Time Restrictions

Start Time	<input type="text"/>
End Time	<input type="text"/>
Day Of Week	<input checked="" type="checkbox"/> S <input checked="" type="checkbox"/> M <input checked="" type="checkbox"/> T <input checked="" type="checkbox"/> W <input checked="" type="checkbox"/> T <input checked="" type="checkbox"/> F <input checked="" type="checkbox"/> S

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.

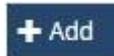
Notification Styles are either a Global-type or Administrator-type. This defines whether the style should be applied globally to all Administrators, or specific to the Administrator who created the style. Administrator Styles will always take priority over Global Styles. Global Styles can only be added/edited by System Administrators.

By default, there are 3 types of Notifications:

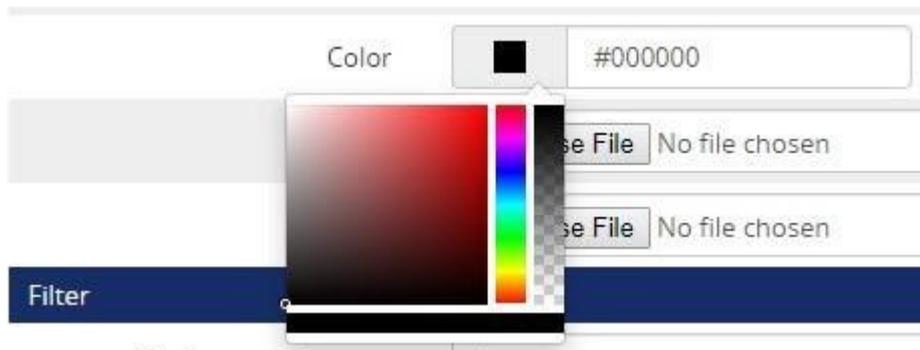
- Neutral (blue): Notifications that are not positive or negative. This includes Panel Logins, Inputs and Outputs changing state and more.
- Positive (green): Notifications that are positive. This includes Access Granted messages for Users.
- Alerts (red): Notifications that are negative. This includes 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 the 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

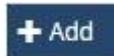
Live Camera Rules specify which notifications should cause a live camera feed to be shown on the Sidebar Notification pane and Alert Monitoring page. A live camera feed is shown only when a rule matches AND the device generating the notification has a camera associated to it.

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.

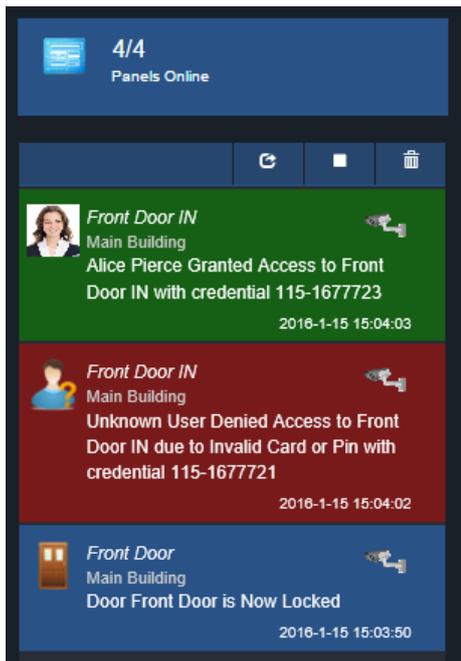


2. The **Partition** field will be pre-selected from the **Notification Settings** page. The **Type** field will be pre-selected depending on which Add button is pressed.
3. Live Camera rules can specify certain notifications or devices to match. By default, the rule will apply to all notifications unless 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 24.2. Notification Sidebar



Tip

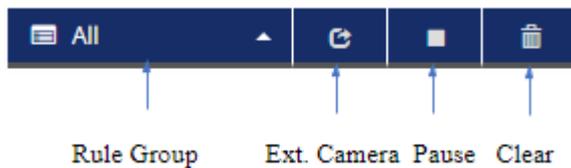
On smaller screen sizes, the Notification Sidebar will disappear. It can be accessed by clicking on the envelope icon on the top of the screen, pictured below.



Sidebar Controls

The Notification Sidebar has a row of buttons at the top that allow for easy control of the sidebar.

Figure 24.3. 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.

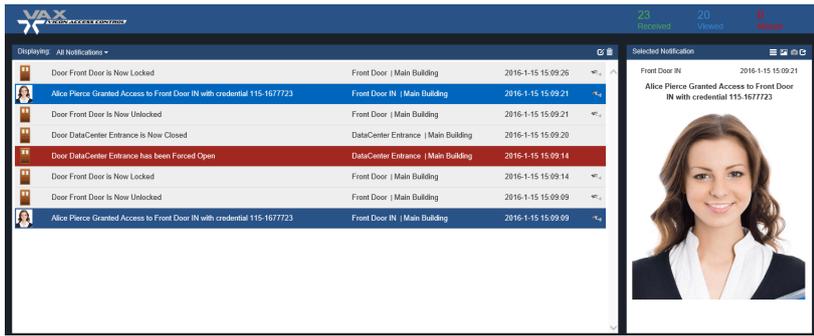
Accessing the Monitoring Screen

1. On the **Home Screen**, 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 24.4. Monitoring Screen



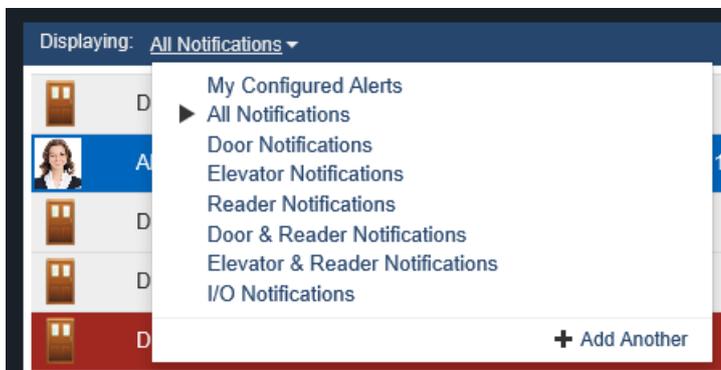
Customizing Displayed Notifications

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 24.5. 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 24.6. Monitoring Options

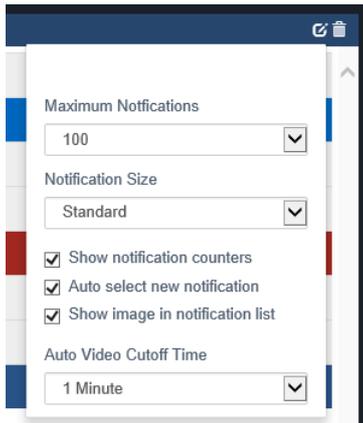


Table 24.2. Monitoring Options

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.

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 24.7. 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.

Configuration Item	Description
	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

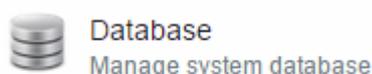
This chapter will cover the options available in the Database screen in Vicon Access Control, specifically the purging of Notifications and administrative log entries to reduce the size of the database and retain performance. Configurations are available for alerting administrators when the database 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.

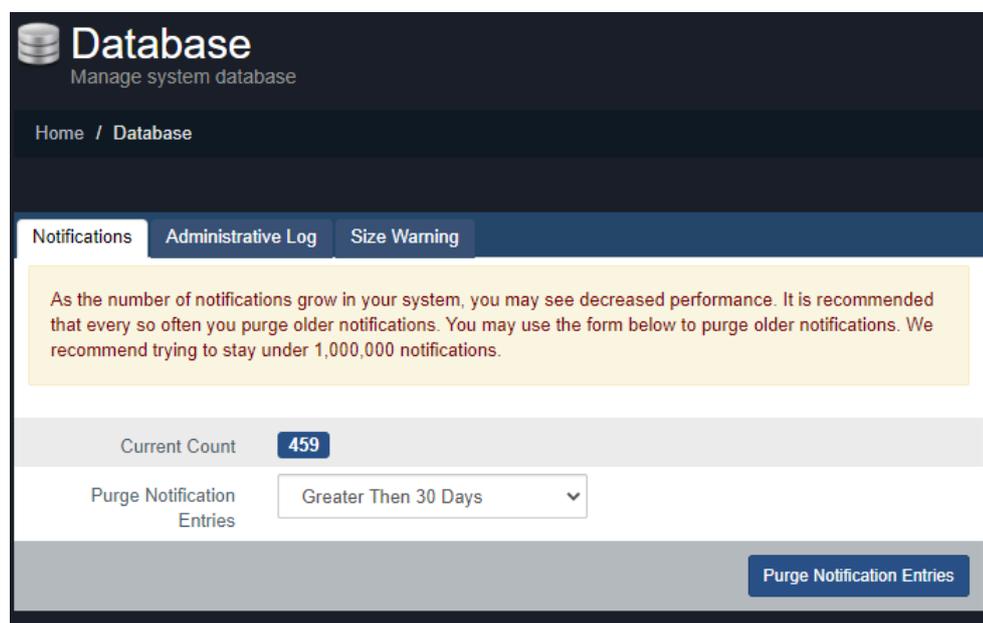
Use the following steps to access the database notification purging form in VAX Access Control:

1. On the **Home Screen**, scroll down to the section titled **System**; 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



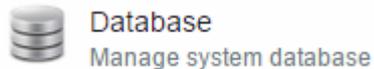
3. We recommend trying to stay under 1,000,000 Notifications. For smaller deployments this could take several years, but for larger ones it could be a few months.
4. To purge Notifications, use the **Purge Notifications** drop-down menu and change how old the Notifications need to be in order to be deleted. 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 Vicon 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.

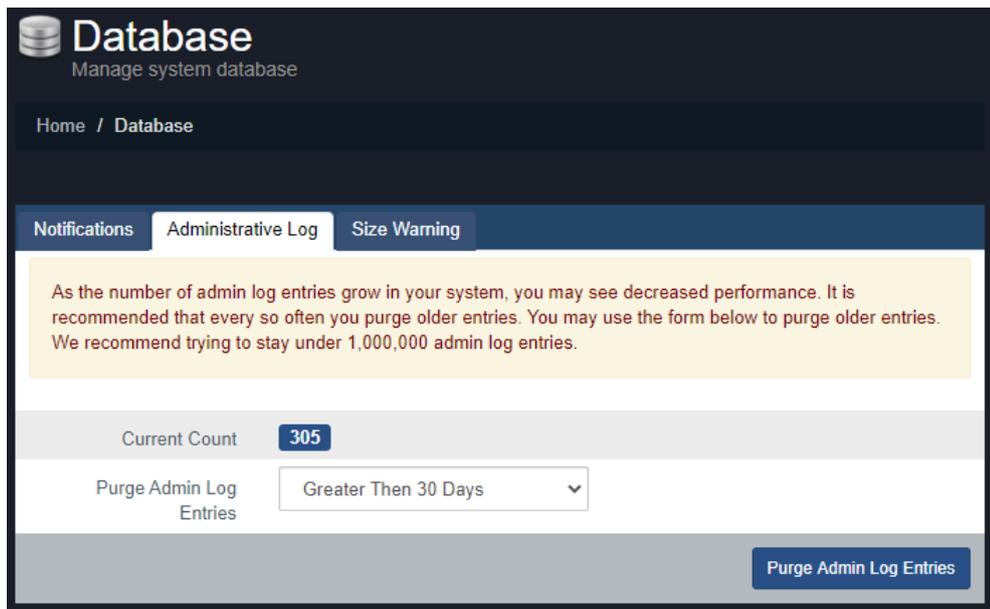
Use the following steps to access the database Administrative Log purging form in VAX Access Control:

1. On the **Home Screen**, scroll down to the section titled **System**; 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.

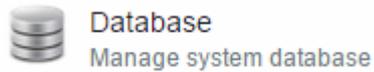
Database Size Warning

This section will cover how to configure a database size warning notification in VAX Access Control. Large amounts of Notifications and Admin Logs over time can hinder the performance of VAX Access

Control, 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 Access Control:

1. On the **Home Screen**, scroll down to the section titled **System**; click on the **Database** icon (pictured below).



2. Once on the **Database** screen, click on the **Size Warning** tab.

Figure 25.3. Size Warning Page

Database Info	
Version	SQL Server 2012 Express Edition (64-bit)
Space	13 MB / 10240 MB (0.13%)

Warning Settings	
Warning Percent	80 %
Show Banner	<input checked="" type="checkbox"/>
Notify System Admins	<input type="checkbox"/>
Notify Dealer	<input checked="" type="checkbox"/>
Notify Frequency	7 days
Last Notification	Never

3. Select the **Warning Percent** by either inputting the desired amount or use the up/down arrows provided within the text box.

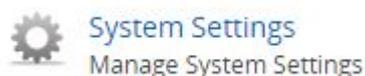
4. Select options including, but not limited to, Show Banner, Notify System Admins, Notify Dealer and the frequency of the notifications.
5. Once you've made your selection, click the **Save** button on the bottom right side.

Chapter 26. System Settings

This chapter covers the System Settings of Vicon Access Control. Most of these settings are the same fields that are configured during the Initial Configuration of Vicon Access Control. 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 Vicon 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. On the **Home Screen**, scroll to the section titled **System**; click on the **System Settings** icon. (pictured below)



On the System Settings screen, there will be three tabs of settings. They are **General Configuration**, **Security**, and **Email Configuration**.

General Configuration

This section will cover the General Configuration tab in Vicon Access Control 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 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 (eg: 8774110101).
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 Vicon Access Control server.

Table 26.2. Connection Config Fields

Field	Brief Description
Server Address	By default, the name of the PC that Vicon Access Control 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.

Once you made the desired changes to your settings, click on the **Save** button on the bottom right of the screen.

Security

This section will cover the Security Configuration tab in Vicon Access Control System Settings.

Enhanced Manual PIN Security

Enhanced manual PIN security is often enabled in deployments where **PIN Only** Door Time Zones 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 in the **Security** tab of **System Settings**.

Email Configuration

This section will cover Email Configuration in Vicon Access Control. 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 (eg: 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 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.

Field	Brief Description
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 Vicon Access Control 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 Vicon Access Control Email Configuration.

To setup email notifications, please see Chapter 24, *Notifications* for more information.

Chapter 27. Elevator Hardware

This chapter will cover the hardware components required to configure elevators in Vicon Access Control.

The Elevator Controller is used to incorporate elevator access into the access control system. Ideally there will be a reader in each cab and based on rules defined in the software; certain cardholders will only have access to specific elevator floors. The readers will connect to the Elevator-Master panel and will control the elevator floors through the IO-Boards attached to it.

The IO-Boards have the capability of switching its on-board solid state relays based on which floors are public or which floors the cardholder has access to. The IO-Boards are controlled and powered by the Elevator-Master Panel. **Each Elevator starter kit (VAX-ELV-STR) comes with an Elevator-Master Panel and an IO-Board.**

Tip

If you aren't planning on controlling any elevators with Vicon Access Control, you can safely skip this chapter.

Elevator-Master Panel: A Master controller, powered by PoE. Provides power and communication to up to 8 IO-Boards via RS-485 bus providing up to 64 floors per Elevator-Master Panel.

Figure 27.1. VAX-ELV-STR With Three VAX-IO-EXP8



IO-Board: Daughter boards that are powered and controlled by the Elevator-Master Panel. Each IO-Board can control up to 8 elevator floors connected to a single cab and is equipped with:

- 8 x Solid State Outputs:

- Solid State Relay Dry Contact, 60V, 500mA Limit, fully configurable, no mechanical parts. Other relay options available upon request.
- 8 x Dry Contact Inputs:
 - Can be triggered via buttons with button/floor sensing.

Table 27.1. Elevator Hardware

Part Number	Description
VAX-ELV-STR	Elevator Starter Kit. Comes with a Elevator-Master Panel and a single IO-Board. Pre-wired together for your convenience and mounted in a steel enclosure.
VAX-IO-EXP8	IO Expansion Kit. Comes with a single IO-Board in a steel enclosure. Can be used to expand the amount of floors on an VAX-ELV-STR starter kit. Can also be used to expand the amount of Inputs/Outputs on an VAX-IO-STR-2 starter kit.
VAX-IO-EXP16	IO Expansion Kit. Comes with a two IO-Boards in a steel enclosure. Can be used to expand the amount of floors on an VAX-ELV-STR starter kit. Can also be used to expand the amount of Inputs/Outputs on an VAX-IO-STR-2 starter kit.
VAX-IO-EXP8-PCB	IO Expansion Kit, no enclosure. Comes with a single IO-Board. Can be used to expand the amount of floors on an VAX-ELV-STR starter kit. Can also be used to expand the amount of Inputs/Outputs on an VAX-IO-STR-2 starter kit.

Connecting the Elevator-Master Panel to the IO-Boards

The **Elevator Master Panel** communicates with the **IO-Boards** through the **RS-485 Interface Plug-in Module**. We recommend using 2 pair twisted shielded.

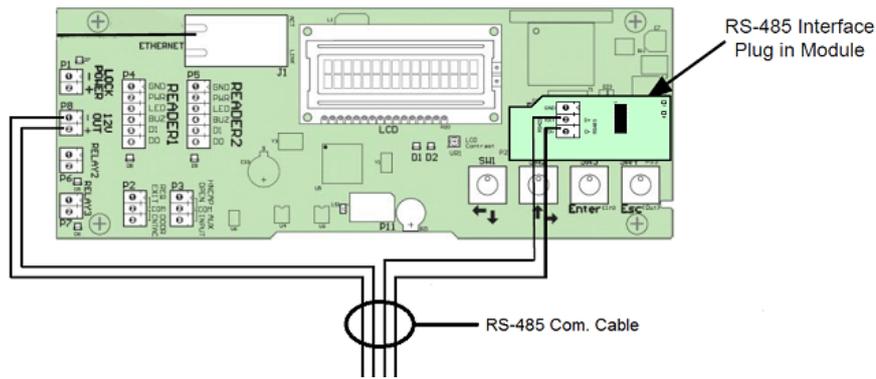
Note

When the Elevator-Master and IO-Boards are purchased in a kit (VAX-ELV-STR), the Elevator-Master will be pre-wired to the IO-Board. If you purchase Expansion kits you must run wire between the Starter kit and the Expansion kits to utilize additional floors.

1. Connect one of the two pairs of RS-485 cable to the '**12V OUT**' Output on the left side of the **Elevator-Master Panel**.
2. Connect the second pair of RS-485 cable to the '**D+**' and '**D-**' on the **RS-485 Interface Plug-in Module** on the right side of the Panel..

Your Panel should look exactly as follows:

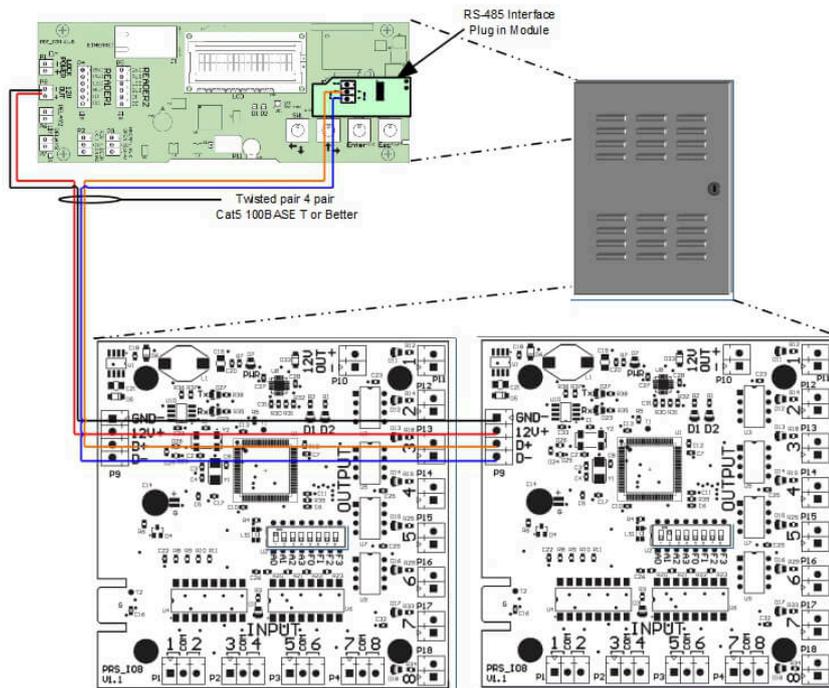
Figure 27.2. Elevator RS-485 Connection



On the first **IO-Board**:

1. Connect the other end of the '12V OUT' 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 **IO-Boards**.

Figure 27.3. Elevator-Master Panel with 2 IO-Boards

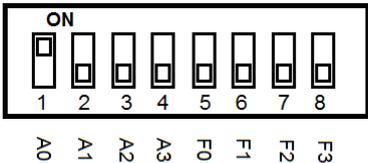
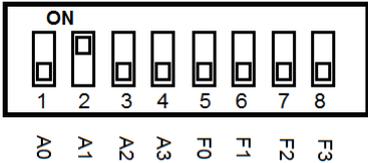
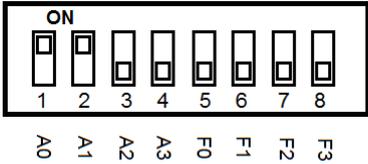
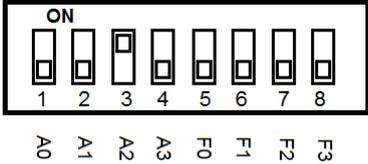
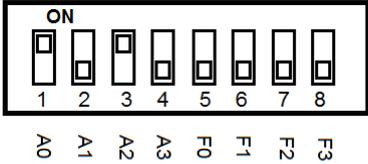
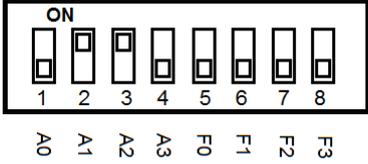
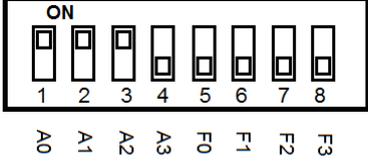
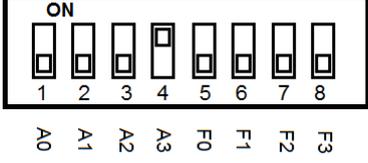


Configuring IO-Board Addresses

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 27.2. Expander Panel DIP Switch Address

DIP Switch Position	Resulting Panel Address
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 1 A3 ~ A0: 0001
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 2 A3 ~ A0: 0010
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 3 A3 ~ A0: 0011
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 4 A3 ~ A0: 0100
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 5 A3 ~ A0: 0101
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 6 A3 ~ A0: 0110
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 7 A3 ~ A0: 0111
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 8 A3 ~ A0: 1000

Once you've wired up your **IO-Boards** to the **Elevator-Master Panel** and configured the DIP switch **Panel Addresses**, you can now power up the **Elevator-Master Board** via a PoE power source such as an Injector or PoE switch.

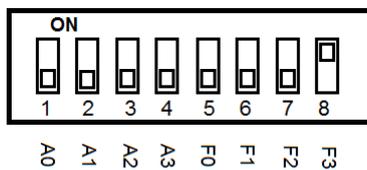
⚠ Warning

Prior to wiring the Inputs/Outputs on the IO-Board into your elevator system, we strongly recommend configuring the software prior to this. Please see Chapter 28, *Elevator Software Components*.

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. See Chapter 37, *Support*.

Figure 27.4. DIP Switch: Input/Output Test



IO-Board Tamper Sensor

The IO-Board has a built in Tamper Sensor. This sensor will send a Notification to Vicon Access Control if it detects a change in the light level. If the IO-Boards are located in the same container as the Elevator-Master Panel, you likely don't need the IO-Board tamper sensor enabled. If the IO-Boards are in a different location, at least one IO-Board should have it enabled. To Enabled the Tamper Sensor, simply turn F2 to ON. Keep A0 - A3 the same. See below.

Figure 27.5. DIP Switch: Tamper Sensor

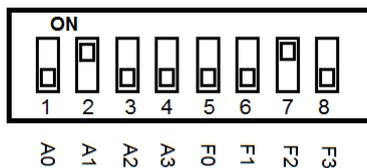


Figure 27.6. Tamper Sensor Notification



Chapter 28. Elevator Software Components

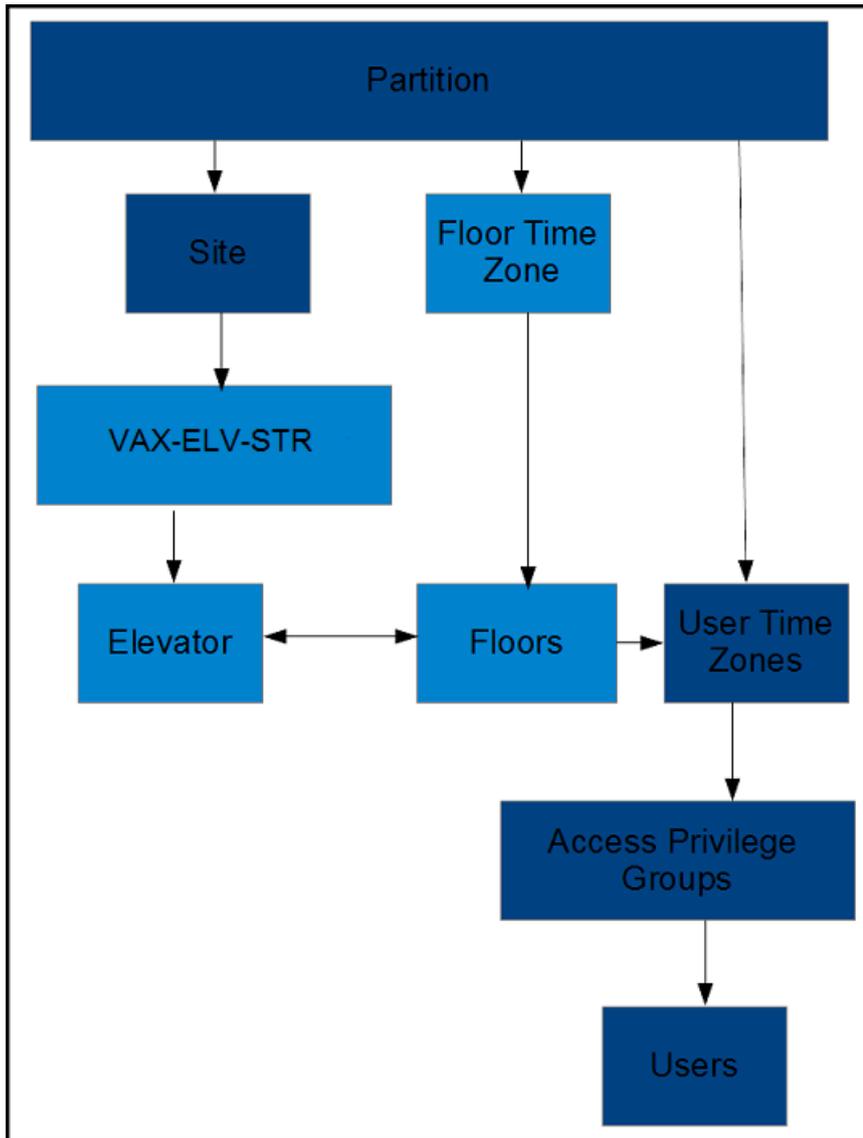
This chapter will be an overview of the various elevator components within Vicon Access Control.

The Elevator software components are as follows:

- Elevator-Master Panels
- Elevators
- Floors
- Floor Time Zones
- Floor One Time Run Zones (Floor OTR)
- Floor Holiday Groups
- Floor Holiday Time Zones

The following diagram demonstrates the primary components of elevators and how they interact with already existing software elements of Vicon Access Control.

Figure 28.1. Elevator Configuration Items



Adding an Elevator Panel

Adding an Elevator Panel to Vicon Access Control is very similar to adding a Door Panel. This section goes over this process.

1. Access your Vicon 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. On the **Home Screen**, 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**.

Figure 28.2. Add Panels Screen

The following table describes the fields to be filled in.

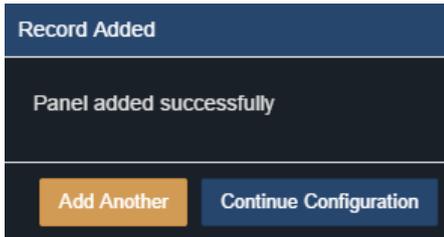
Table 28.1. Add Panel

Drop-down/Text Box/Check box	Description
Panel Model	Select VAX-ELV-STR.
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.

Drop-down/Text Box/Check box	Description
Expanders	The amount of IO-Boards attached to the Elevator 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.



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 Time Zones and Holiday Groups.

1. Access your Vicon 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. On the **Home Screen**, 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.

Drop-down/Text Box/Check box	Box/	Description
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

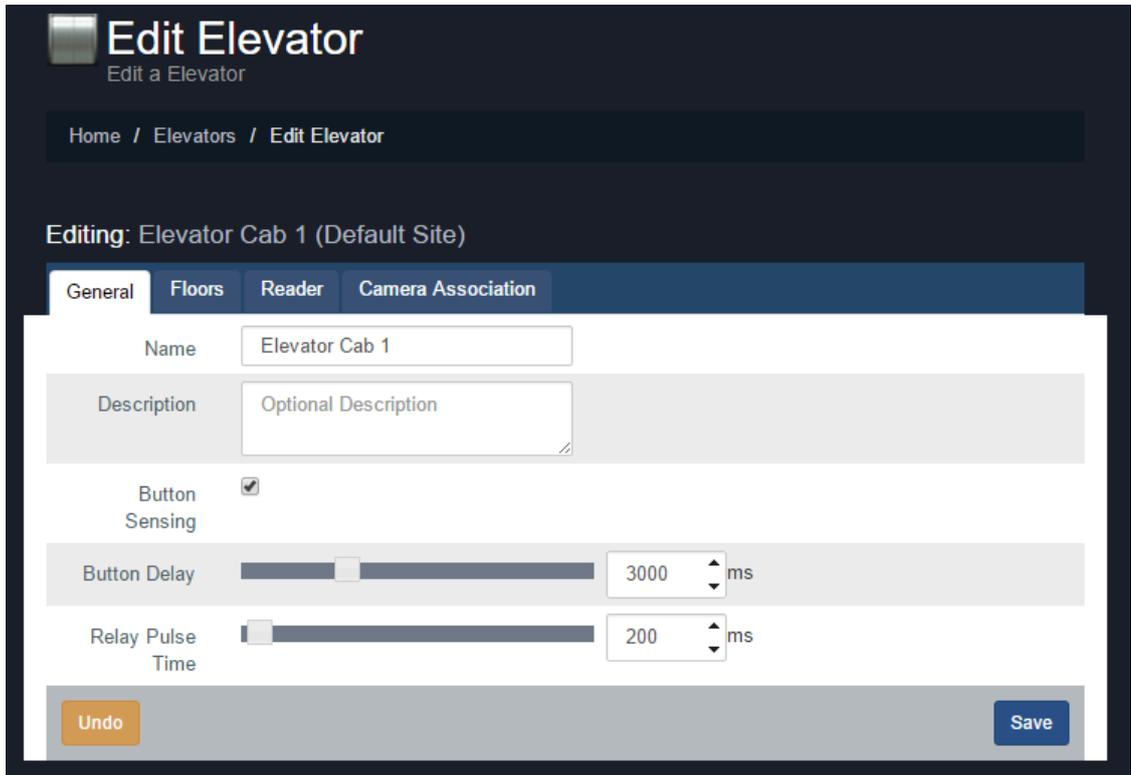


Table 28.3. General Tab

Drop-down/Text Box/Check box	Description
Button Delay	If using button sensing, how long in between presenting a credential and pushing a button and for how long 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 Time Zones** and the **Floor Holiday Group**.

Figure 28.4. Floors Tab

Disabled	Floor	Name	Time Zone	Holiday Group
<input type="checkbox"/>	1	Floor 1	Unlocked Always	Default Holiday Grou
<input type="checkbox"/>	2	Floor 2	Card Always	Default Holiday Grou
<input type="checkbox"/>	3	Floor 3	Card Always	Default Holiday Grou
<input type="checkbox"/>	4	Floor 4	Card Always	Default Holiday Grou

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 Time Zone** 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 Vicon Access Control 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 Vicon Access Control 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 in **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 Address- es 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

Editing: Elevator (Default Site)				
General Connectivity Options Floor I/O Map				
	Output	Status	Elevator	Floor
Expander 1 Elevator: Elevator Cab 1 Address: 1	1	Enabled	Elevator Cab 1	[1] Floor 1
	2	Enabled	Elevator Cab 1	[2] Floor 2
	3	Enabled	Elevator Cab 1	[3] Floor 3
	4	Enabled	Elevator Cab 1	[4] Floor 4
	5	Enabled	Elevator Cab 1	[5] Floor 5
	6	Enabled	Elevator Cab 1	[6] Floor 6
	7	Enabled	Elevator Cab 1	[7] Floor 7
	8	Enabled	Elevator Cab 1	[8] Floor 8
Expander 2 Elevator: None Address: 2	1	Not Used		
	2	Not Used		
	3	Not Used		
	4	Not Used		
	5	Not Used		

Floor Time Zones

This section covers adding additional **Floor Time Zones** to Vicon Access Control.

Floor Time Zones are applied to **Floors** in the **Floors Tab** of the **Edit Elevators Screen**. Unlike **Door Time Zones**, **Floor Time Zones** only have three possible states: **Card**, **Unlock** and **Lockdown**. By default, there are 3 default **Floor Time Zones**:

- Card Always
- Locked Always
- Unlocked Always

To add more Floor Time Zones:

1. Access your Vicon 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.

- On the **Home Screen**, scroll down to the section titled **Scheduling**; click on the **Floor Time Zones** icon (pictured below).



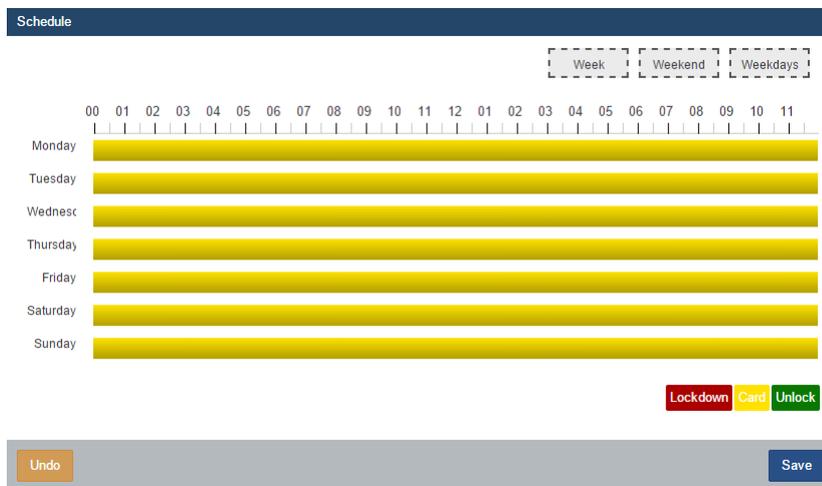
- On the Floor Time Zones screen, you'll see the default time zones. To add time zones, click the **Add** button on this screen.
- On the **Add Floor Time Zone** screen, you'll have a few text boxes to fill in.

Table 28.4. Add a Floor Time Zone

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

- Schedule: Creating the schedule is the last step in creating a **Floor Time Zone**.

Figure 28.7. Floor Time Zone Schedule



Note

In Floor Time Zones, you may have up to 8 time spans, meaning the state of the floor can change up to 8 times in a schedule.

- Click on any of the horizontal bars in the time schedule to bring up the **Time Zone Editor Widget**. The time zone editor widget is a simple and powerful tool for creating **Time Zones**.

Figure 28.8. Time Zone 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 time zone editor has 3 fields used for adding a Floor Time Zone 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 time zone you've created to be used for several different days, you can click on the bar with your completed time zone, and drag it to the **Week**, **Weekend** or **Weekdays** boxes above the chart. The time zone will be replicated based on which box you drag your time zone into.



11. Once your schedule for all 7 days is as desired, you may now press **Save** to create the Floor Time Zone 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 Vicon Access Control components you may already be familiar with.

Once you have added your Elevator(s) and assigned Floor Time Zones to each Floor, you can now assign Users permission to these Floors using Access Privilege Groups and User Time Zones 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 Controls 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 eavesdropping 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 (including TROVE multi door kits) 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 interoperability between OSDP hardware and non-OSDP hardware. Wiegand readers can still be used on OSDP panels.

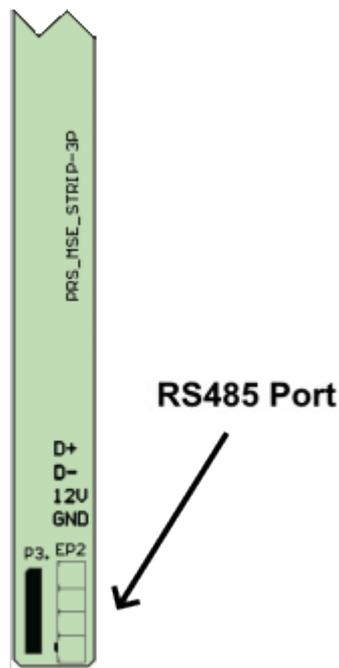
How to Check if Firmware Supports OSDP

VAX-MDK-Master: 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).



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 VAX-MDK 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 communication 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.



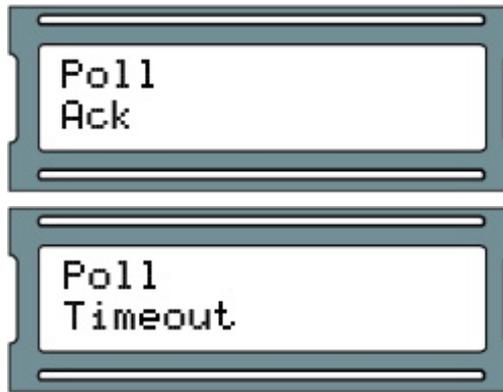
4. You will now choose an OSDP address to make changes or test. If you're not sure what the address is you should start with 00. Using the white up and down buttons on the Panel, locate the address you want to change or test and press the Enter button.



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.



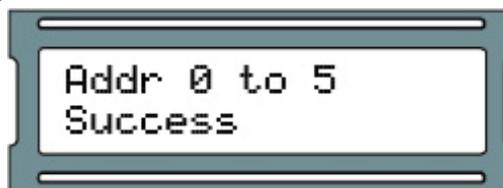
7. Press the ESC button to return to the previous menu.
8. If you need to change the address of the current device, use the white up and down buttons on the Panel to locate the menu option Change Address. Press the ENTER key to enter the change address menu.



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 Vicon 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.

Reader 1	
Name	Front Door
Description	Optional Description
Port on Panel	Reader 1
Interface	<input type="radio"/> Wiegand <input checked="" type="radio"/> OSDP
OSDP Address	8

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 recommended for maximum security. Encryption keys are set at the VAX software interface. OSDP MDK 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 communications.

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 Vicon 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 **Home Screen**, 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.

OSDP Encryption Code

255

OR

Use Panel Password

Undo Save

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 until 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 manufacturer 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 communication. 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 **Home Screen**, 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.

The screenshot shows a configuration interface for a device with several tabs: General, Options, Reader 1, Reader 2, Areas, and Camera Association. The 'Reader 1' tab is selected. The configuration is as follows:

Enabled	<input checked="" type="checkbox"/>
Name	Side Door
Description	Optional Description
Reader Port	Reader 1
Interface	<input type="radio"/> Wiegand <input checked="" type="radio"/> OSDP
OSDP Address	8
OSDP Encrypted Data Only	<input checked="" type="checkbox"/>

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 unmanaged doors (doors with locks, door contacts, inputs but no reader) or monitored doors (doors that only have door contacts).

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.

Figure 30.1. VAX-IO-STR With Three VAX-IO-EXP8-PCB



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-STR-2	Input/Output Starter Kit with VAX-MDK Master Controller with IO-8 expansion module. 12VDC powered with external power supply. Complete

Part Number	Description
	in steel vented and lockable enclosure. Add up to 7 more expanders to control up to 64 I/O's per Master.
VAX-IO-EXP8-PCB	IO Expansion Kit, no enclosure. Comes with a single IO-Board. Can be used to expand the amount of Inputs/Outputs on an VAX-IO-STR-2 starter kit. Can also be used to expand the amount of floors on an VAX-ELVSTR starter kit.

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:

POE-IO Master: A Master controller, powered by PoE. Provides power and communication to up to 8 IO-Boards via RS-485 bus providing up to 64 Inputs and 64 Outputs.

VAX-IO-STR-2 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. This model has a stronger feature set than the POE-IO master.

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 Panel.
- 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 Panel

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. Otherwise please use the following diagrams and charts for reference in the next section.

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 need to wire them together.

The **VAX-IO-STR-2 Master Panel** communicates with the **IO-Boards** through the RS-485 Interface Plug-in Module on the right hand side of the board. We Recommend using 2 pair twisted shielded.

The **VAX-IO-STR-2 Panel** does not require this module because it has 2 RS-485 ports built into the panel.

1. Connect one of the two pairs of RS-485 cable to the '**12V OUT**' Output on the left side of the **VAX-IO-STR-2 Master** or one of the 12v+ and GND- connectors on the **VAX-IO-STR-2 Master**.
2. Connect the second pair of RS-485 cable to the '**D+**' and '**D-**' on the **RS-485 Interface Plug-in Module** on the VAX-IO-STR-2 Master or the D+ and D- port on the VAX-IO-STR-2 Master.

Your Panel should look exactly as follows:

Figure 30.2. VAX-IO-STR-2 Master RS-485 Connection

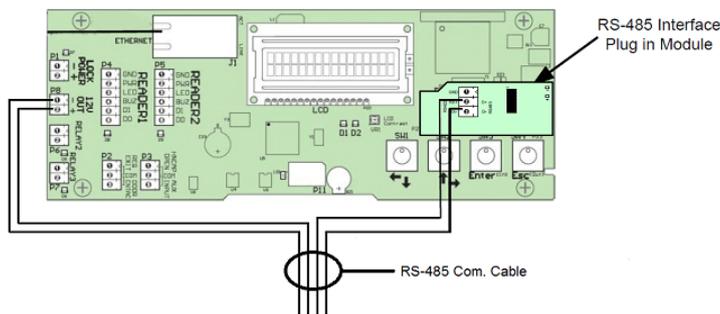
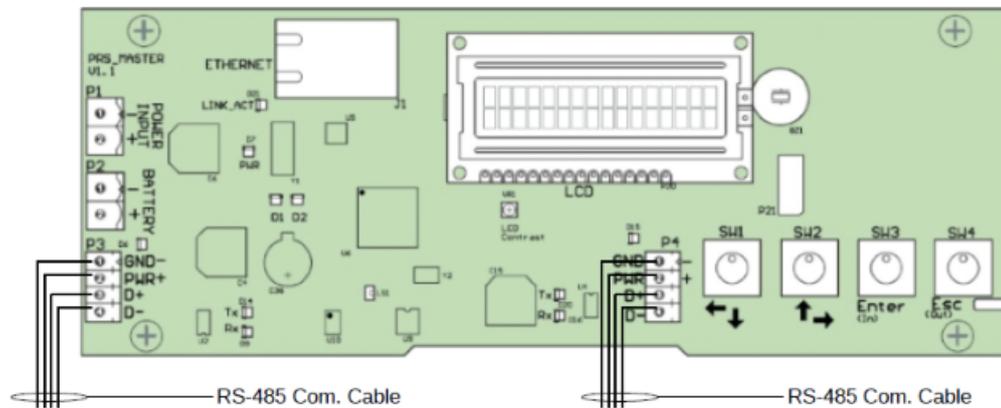


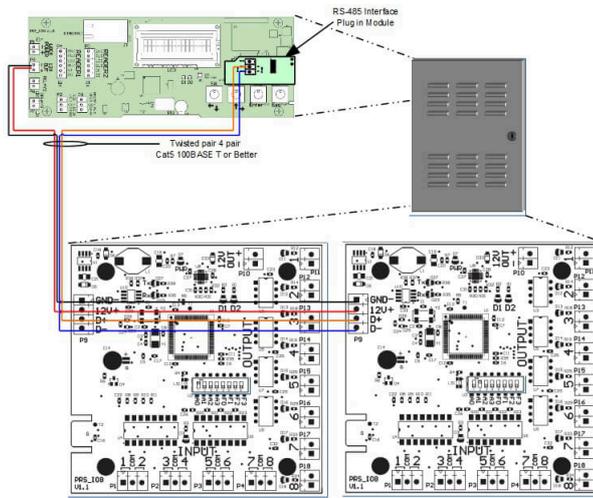
Figure 30.3. VAX-IO-STR-2 Master RS-485 Connection



On the first **IO-Board**:

1. Connect the other end of the '**12V OUT**' 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 **IO-Boards**.

Figure 30.4. VAX-IO-STR-2 Master Panel with 2 Expander Boards



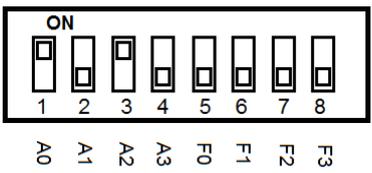
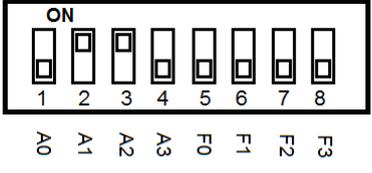
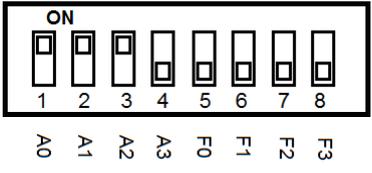
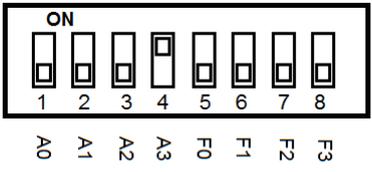
Configuring IO-Board Addresses

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
<p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	<p>Panel Address: 1</p> <p>A3 ~ A0: 0001</p>
<p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	<p>Panel Address: 2</p> <p>A3 ~ A0: 0010</p>
<p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	<p>Panel Address: 3</p> <p>A3 ~ A0: 0011</p>
<p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	<p>Panel Address: 4</p> <p>A3 ~ A0: 0100</p>

DIP Switch Position	Resulting Panel Address
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 5 A3 ~ A0: 0101
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 6 A3 ~ A0: 0110
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 7 A3 ~ A0: 0111
 <p>ON</p> <p>1 2 3 4 5 6 7 8</p> <p>A0 A1 A2 A3 F0 F1 F2 F3</p>	Panel Address: 8 A3 ~ A0: 1000

Once you've wired up your **IO-Boards** to the **IO-Master Panel** and configured the DIP switch **Panel Addresses**, you can now power up the **IO-Master Board** via a PoE power source such as an Injector or PoE switch.

Warning

Prior to wiring the Inputs/Outputs on the IO-Board into your external devices, we strongly recommend configuring the software prior to this.

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 support. See Chapter 37, *Support*.

Figure 30.5. 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:

- VAX-IO-STR-2
- IO-Boards/IO-Expanders
- Input Time Zones
- Input Holiday Time Zones
- Output Time Zones
- Output Holiday Time Zones
- IO Holiday Groups
- Unmanaged Doors

Adding the VAX-IO-STR-2 Master Panel to VAX

Adding an VAX-IO-STR-2 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 **Home Screen**, 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 the correct model, either **VAX-IO-STR** or **VAX-IO-STR-2**.

Figure 30.6. Add Panels Screen

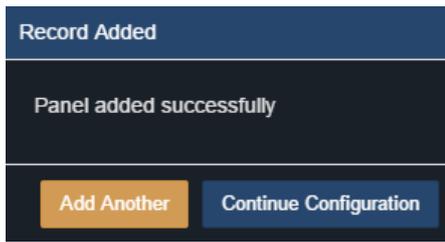
The following table describes the fields to be filled in.

Table 30.3. Add Panel

Drop-down/Text Box/Check box	Description
Panel Model	Select VAX-IO-STR or 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.



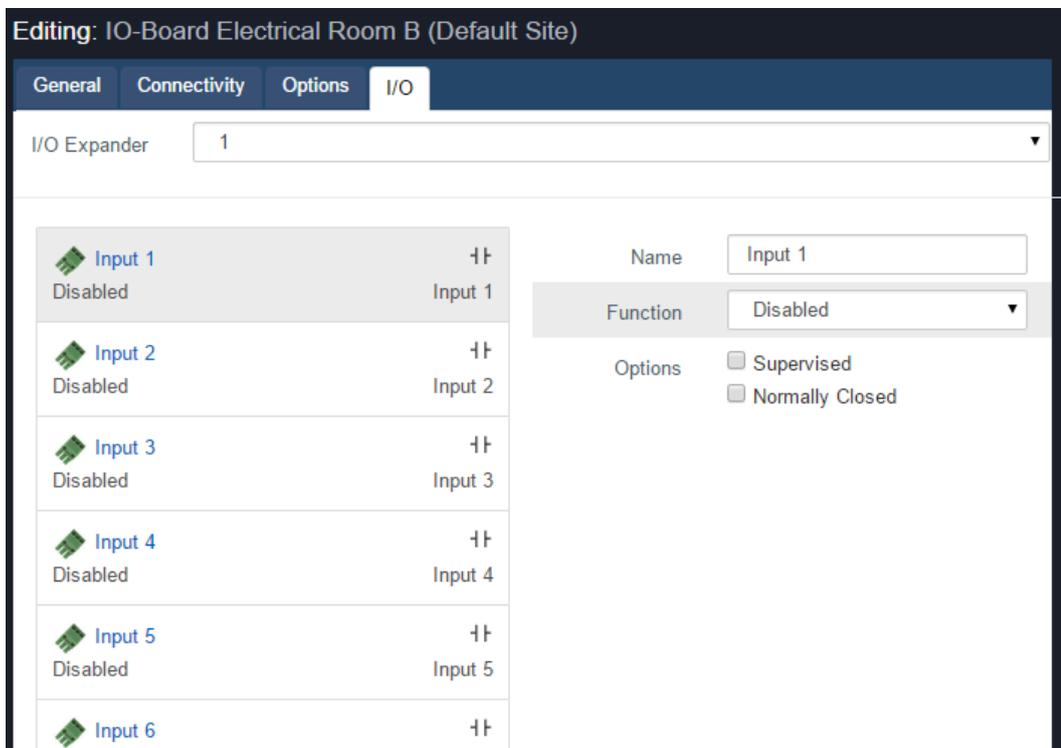
Configuring Inputs and Outputs

Once you've added the VAX-IO-STR-2 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 30.7. 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. POE-IO Master will allow Aux input and Door Contact. VAX-IO-STR-2 Master will allow additional input functions.
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.
Time Zone	Optional. Select an Input Time Zone 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-2 Input 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 VAX-IO-STR-2 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 on VAX-IO-STR-2 Master panels.

Table 30.6. VAX-IO Input Actions

Action	Description
Do Nothing	Actions are optional; an event will still be generated when input conditions are met.
Activate Selected Output	Activates an output, selectable via drop down list.
Toggle Selected Output	Toggle an output to the opposite state.
Deactivate Selected Output	Deactivate the selected Output, selectable via drop down list.
Pulse Selected Output (High)	Pulse an Output to close, configure a delay and the duration of the pulse.
Pulse Selected Output (Low)	Pulse an Output to open, configure a delay and the duration of the pulse.
Pulse Selected Output (Opposite)	Pulse an Output to the opposite of its current state, configure a delay and the duration of the pulse.
Activate Multiple Outputs	Activate multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Deactivate Multiple Outputs	Deactivate multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Toggle Multiple Outputs	Toggle multiple outputs from a single input. Up to 5 outputs can be selected. Use the CTRL key when clicking Outputs from the list.
Cancel Running Actions	Cancel any actions on an output based on affects from other outputs.

Table 30.7. 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.
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 Time Zone.
Unmanaged Door - Override Lock	Override a selected unmanaged door to a locked state. State will remain until resume command.

Action	Description
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 Time Zone.
Unmanaged Door - Override Unlock with Auto Resume	Override a selected unmanaged door to an unlocked state. State will resume its normal schedule at the next scheduled transition in the Output Time Zone.

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 30.8. Input Options

The screenshot shows a configuration form for an input board. The fields are as follows:

- Name: Input 1
- Function: Aux Input
- Detection Time: 0 s
- Time Zone: Always Allowed
- Holiday Group: -- No Holiday Group --
- Action: Do_Nothing
- Options:
 - Do_Nothing
 - Activate Selected Output
 - Deactivate Selected Output
 - Toggle Selected Output
 - Pulse Selected Output (High)
 - Pulse Selected Output (Low)
 - Pulse Selected Output (Opposite)
 - Activate Multiple Outputs
 - Deactivate Multiple Outputs
 - Toggle Multiple Outputs
 - Cancel Running Actions

The following table demonstrates each of the fields available when an Output is selected:

Table 30.8. 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.
Time Zone	Optional. Select an Output Time Zone from the drop-down list. This schedule will instruct the IO-Master to only monitor this input during a specific time.

Function	Description
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 Time Zone 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 Master 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 30.9. 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 Time Zone 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 Time Zone. Can change state based on overrides or input actions.

Figure 30.9. Output Options

The screenshot shows a configuration interface for an output board. It includes the following elements:

- Name:** A text input field containing "Output 1".
- Function:** A dropdown menu currently set to "Aux Output".
- Time Zone:** A dropdown menu currently set to "Always On".
- Holiday Group:** A dropdown menu currently set to "Inputs on holiday".
- Options:** A list of four checkboxes:
 - Normally Closed
 - No Events
 - Protected
 - Initially On (If No Time Zone Selected)

Input and Output Time Zones

This section will cover Input and Output schedules. Inputs and Outputs on IO-Boards can be placed on a schedule.

Input Time Zones

Input Time Zones 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 Time Zone:

1. On the **Home Screen**, scroll down to the section titled **Scheduling**; click on the **Input Time Zones** icon (pictured below).



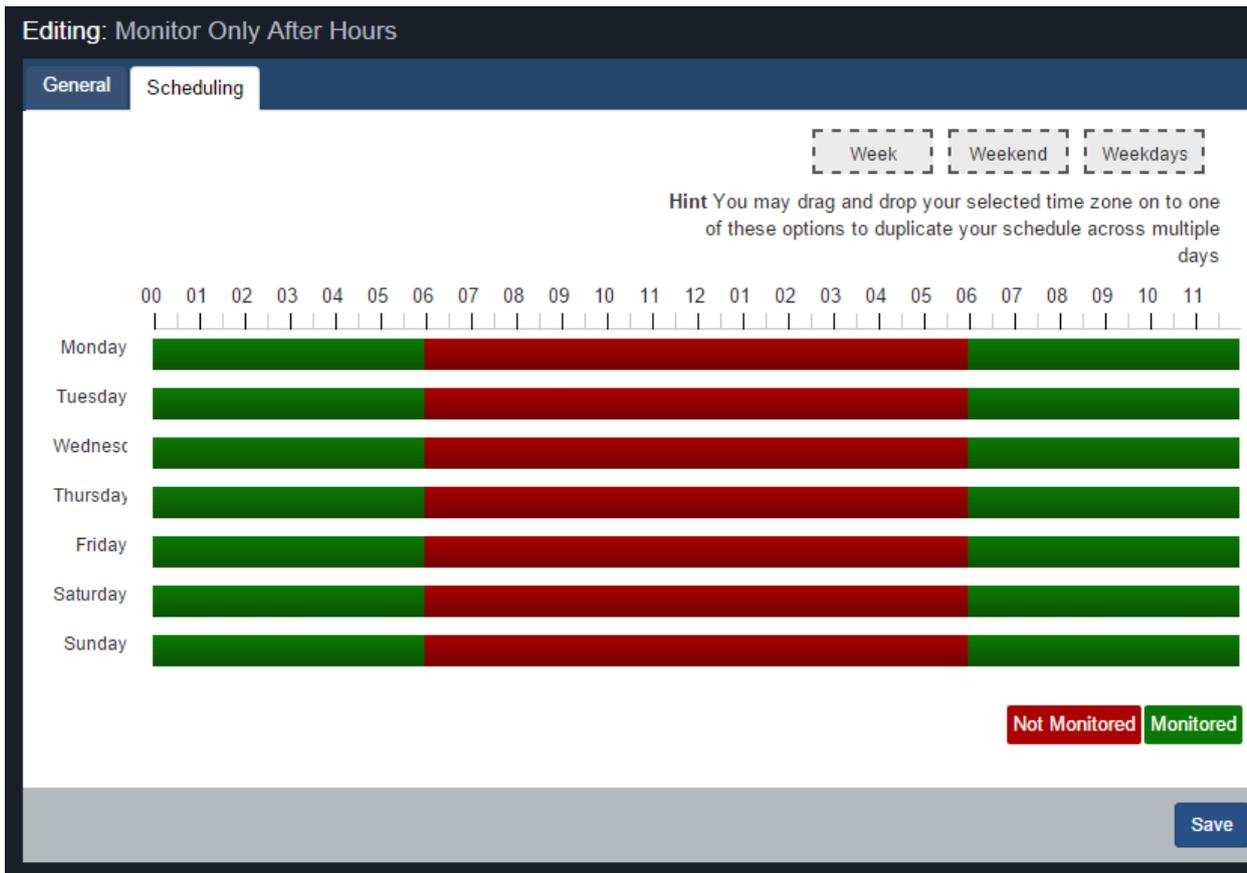
2. On the Input Time Zones screen, you'll see the default time zones. If additional Input Time Zones are needed, click the **Add** button on this screen.
3. On the **Add Input Time Zone** screen, you'll have a couple text boxes to populate.

Table 30.10. Add Input Time Zone

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

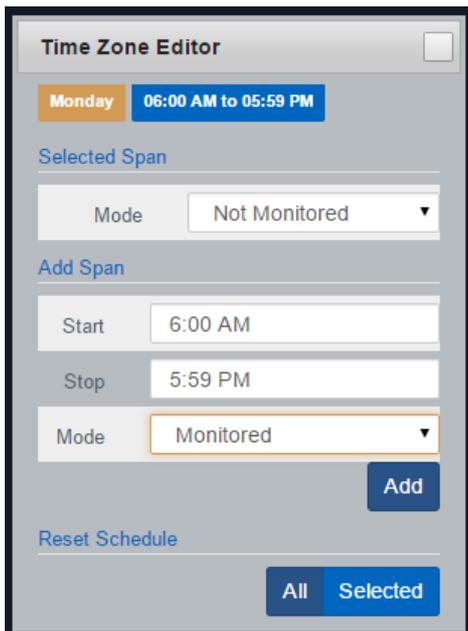
4. Creating the **Schedule** is the last step in creating a Input Time Zone. Below is what the schedule part of the add time zone page looks like.

Figure 30.10. Input Time Zone Schedule



5. Click on any of the horizontal bars in the time schedule to bring up the **Time Zone Editor Widget**. The time zone editor widget is a simple and powerful tool for creating time zones.

Figure 30.11. Time Zone 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 time zone editor has 3 fields used for adding a Input Time Zone 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 time zone you've created to be used for several different days, you can click on the bar with your completed time zone, and drag it to the **Week**, **Weekend** or **Weekdays** boxes above the chart. The time zone will be replicated based on which box you drag your time zone into.



9. Once your Input Time Zone for all 7 days is as desired, you may now press **Save** to create the Input Time Zone in the selected Partitions. The Input Time Zone can now be assigned to Inputs when adding or creating IO-Master Panels.

Output Time Zones

Output Time Zones 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 Time Zone:

1. On the **Home Screen**, scroll down to the section titled **Scheduling**; click on the **Output Time Zones** icon (pictured below).



2. On the Output Time Zones screen, you'll see the default time zones. If additional Output Time Zones are needed, click the **Add** button on this screen.
3. On the **Add Output Time Zone** screen, you'll have a couple text boxes to populate.

Table 30.11. Add Output Time Zone

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

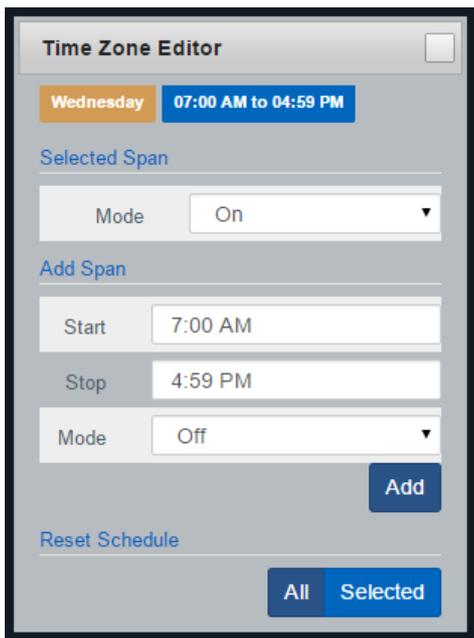
4. Creating the **Schedule** is the last step in creating a Input Time Zone. Below is what the schedule part of the add time zone page looks like.

Figure 30.12. Output Time Zone Schedule



5. Click on any of the horizontal bars in the time schedule to bring up the **Time Zone Editor Widget**. The time zone editor widget is a simple and powerful tool for creating time zones.

Figure 30.13. Time Zone 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 time zone editor has 3 fields used for adding a Output Time Zone 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 time zone you've created to be used for several different days, you can click on the bar with your completed time zone, and drag it to the **Week**, **Weekend** or **Weekdays** boxes above the chart. The time zone will be replicated based on which box you drag your time zone into.



9. Once your Output Time Zone for all 7 days is as desired, you may now press **Save** to create the Output Time Zone in the selected Partitions. The Output Time Zone 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 and/or 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 30.12. IO Door Types and Features

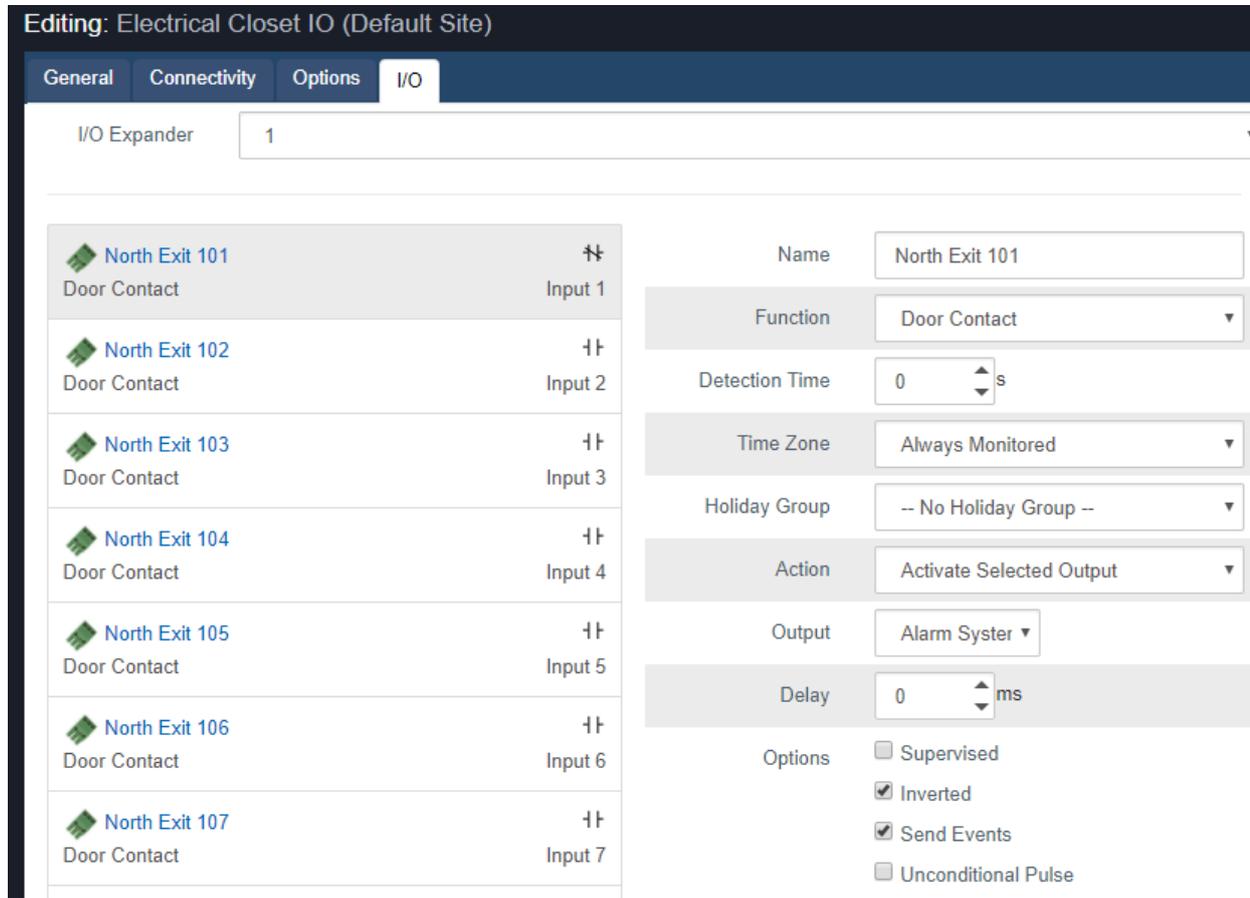
Door Type	Supported Panel Type	Features
Monitored	VAX-IO-STR, VAX-IO-STR-2	Only supports door contact and camera associations. Limited output functions. 64 Door limit per VAX-IO-STR-2 Master or POE-IO master.
Unmanaged	VAX-IO-STR-2	Supports door contact, door strike, REX, motion sensor, camera associations, remote override and additional output functions. 16 door limit per VAX-IO-STR-2 Master.

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.

- 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 30.14. IO Board Door Contact



- For VAX-IO-STR-2 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.
- After changing any required inputs to door contacts or other input and output functions, click Save on the bottom of the page.
- From the **Home Screen**, scroll down to the section titled **Hardware**, click on the **Doors** icon (pictured below).



- On the **Doors** screen, you'll notice any Doors you've already configured listed here. Click the **Add** button on this screen.
- On the **Add Door** screen, select Unmanaged or Monitored as the Door Type.
- Select the IO board your door contact is connected to on the Panel drop-down menu.
- Select the input your door contact is connected to on the Input drop-down menu.

Figure 30.15. Add Door Screen

Home / Doors / Add Door

Door

Door Type	Type	Supported Panels	Features
<input type="radio"/>	Managed	POE, PRS	Supports upto 2 readers, Automatic Opener, Anti-Passback, Cameras
<input checked="" type="radio"/>	Monitored	POE-IO, PRS-IO	Only supports Door Contact and Cameras.
<input type="radio"/>	Unmanaged	PRS-IO	Supports Door Contact, Door Strike and Cameras.

Name:

Description:

Panel:

Input:

Undo Save

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 (1D, 2D) 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:**

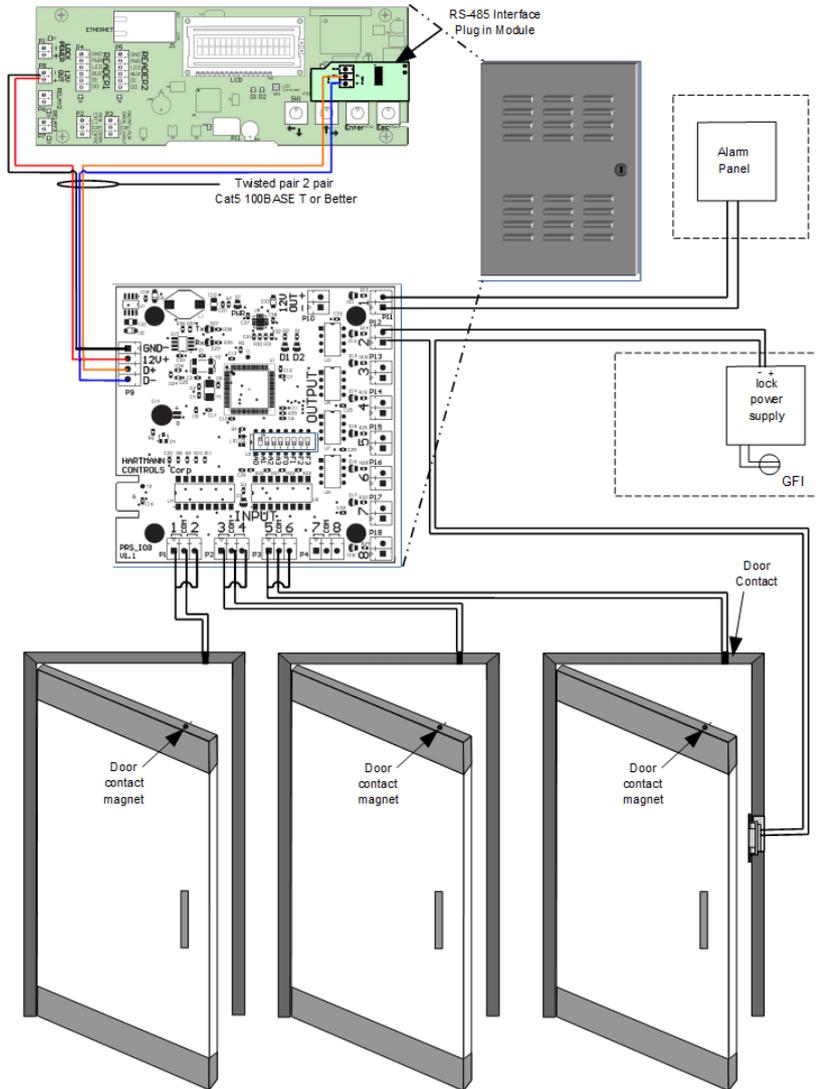
It is possible for other external systems and devices to interact with the IO-Boards, as long as they are able to provide the IO-Board a dry contact to close the Input to one of the common grounds on the IO-Board. This can include various inputs such as sensors, buttons, switches or Output devices such 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 30.13. 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 30.16. IO-Board Example



Chapter 31. Camera System Integration

VAX is capable of 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.
Hikvision NVR	Plug-in Version 3.0.6.1	HTTPS may need to be enabled. Requires a specific plug-in to work. Contact support to get a copy.

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	<ul style="list-style-type: none"> • Requires Valerus Plug-in. • Supports multiple cameras in matrix. • Good video quality and performance. • Very Low video latency. • No mobile support.
Vicon Vicon-Net	Internet Explorer 11	<ul style="list-style-type: none"> • Requires Silverlight Plug-in. • Supports multiple cameras in matrix. • Supports iris and focus adjustments.

System	Support Browsers	Notes
		<ul style="list-style-type: none"> • Good video quality and performance. • No mobile support.
Milestone xProtect	Internet Explorer 11 Opera 35.0 Google Chrome Mozilla Firefox Apple Safari	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.
Hikvision	Internet Explorer 11	<ul style="list-style-type: none"> • Requires Hikvision Web Components Plug-in. • Good video quality • No 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-Server: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”.

Enable HTTPS: Hikvision NVR

1. Hikvision Web Server should be enabled by default. We recommend enabling HTTPS on the NVR/DVR in order to securely view video.
2. Browse to the URL of the Hikvision NVR web interface.
3. Login to the web interface.
4. Navigate to the Configuration tab and select Advanced Settings.
5. Click the HTTPS tab. Check the Enable checkbox.
6. Select certificate installation method and click Save. In a few moments you should be able to access the HTTPS version of the web interface.
7. You should add the Self-Signed Hikvision SSL certificate; this process is outlined in the section called “Adding Website Certificates for Camera Integration”.
8. 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 **Home Screen**, 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 **Home Screen**, 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

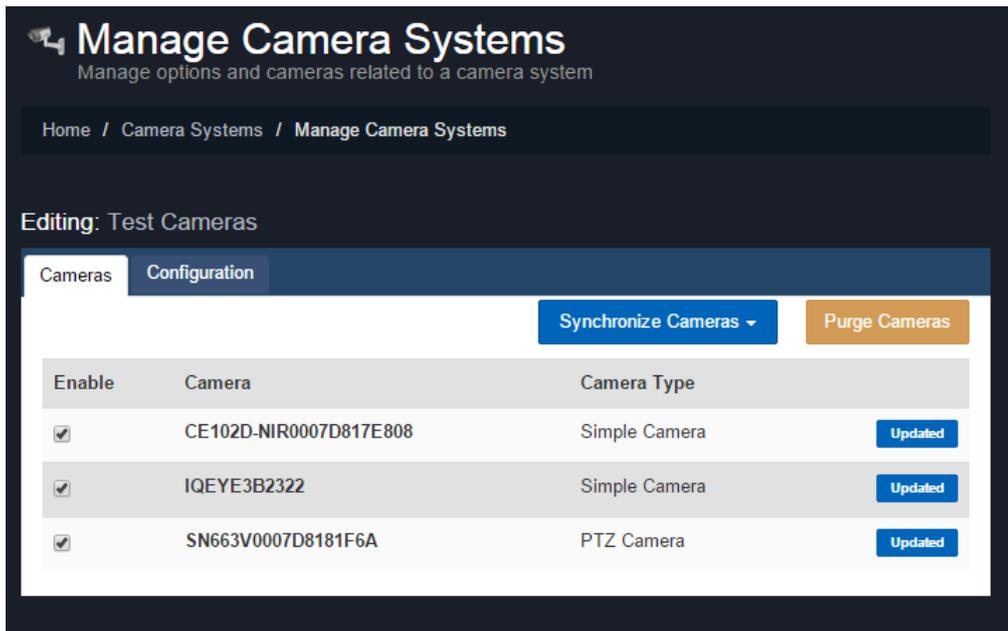
Depending on the number of cameras in the video management software, this process may take up to a few minutes. The process will also let you know if it fails to communicate with the server.

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

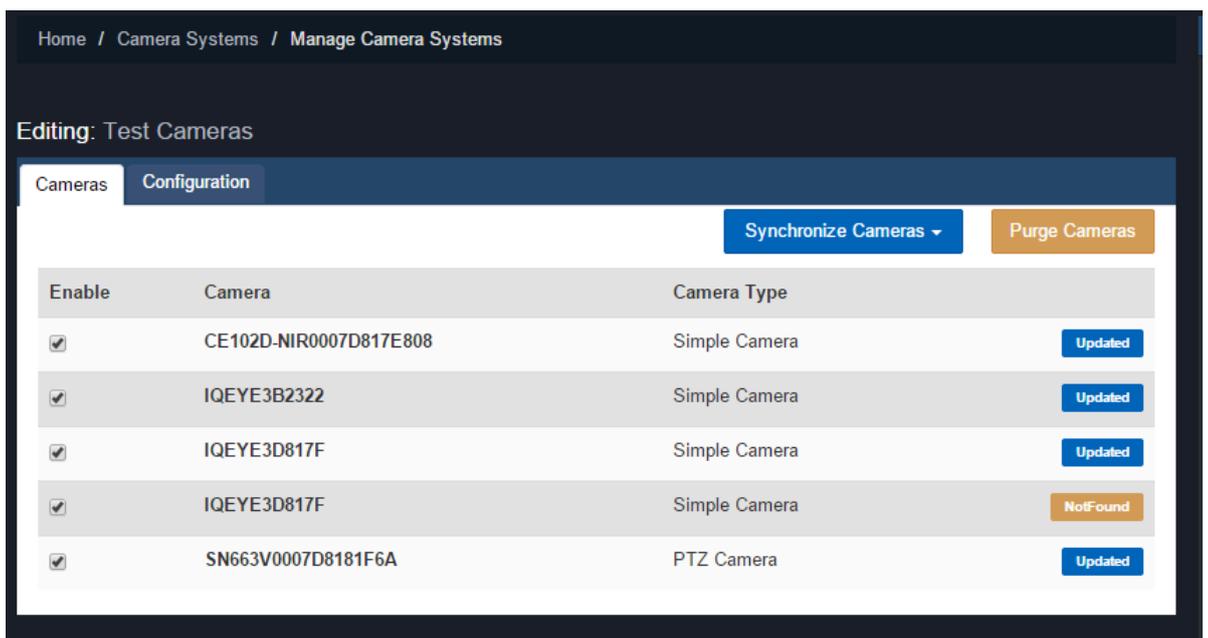


Purging Cameras

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 **Home Screen**, 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

Camera Viewer

Camera System: Test Cameras

Matrix Size: 1x1

Mode: Live Video Playback Video

Time: Time

Cameras:

- CE102D-NIR0007D817E808
- IQEYE3B2322
- SN663V0007D8181F6A

Hint: You can click the camera icon next to each camera for a quick view of a single camera

View Live Video

Tip

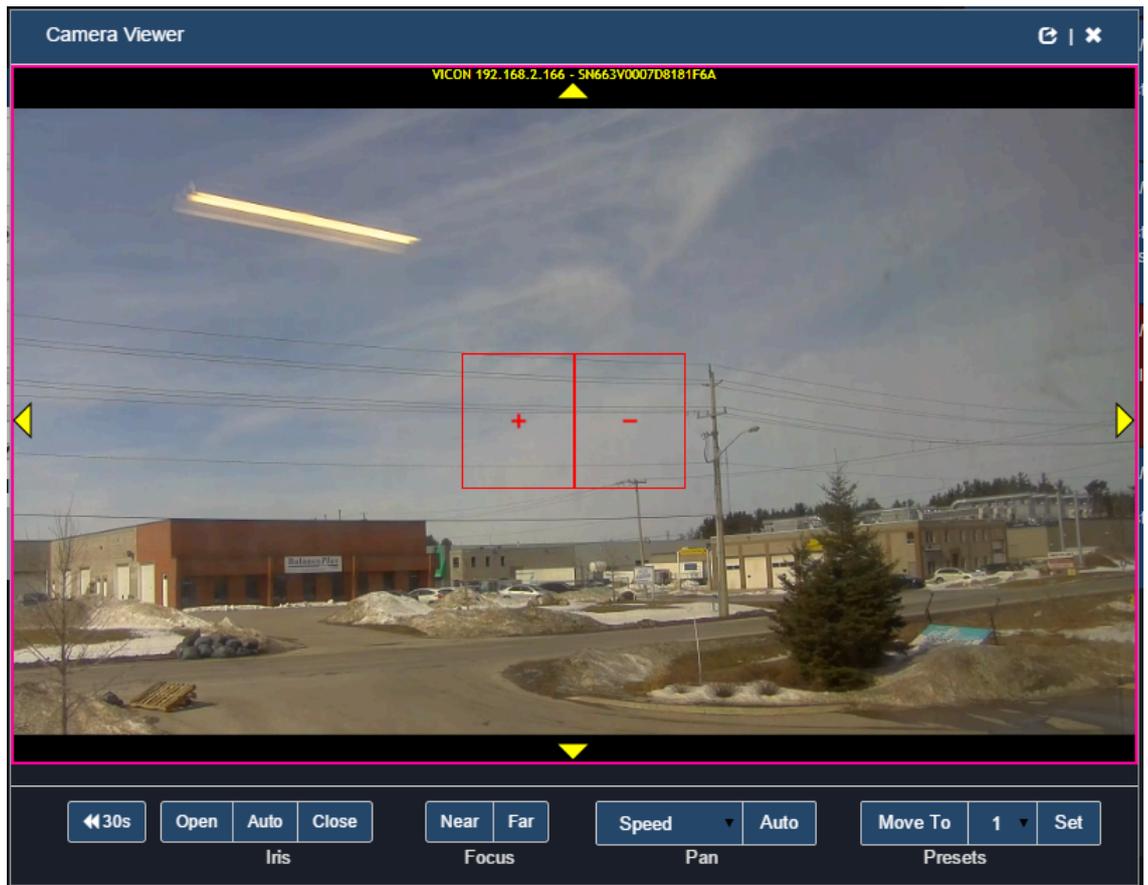
You can quickly view live feed of a single camera by clicking directly on the camera icon next to the name of each camera on this screen.

Viewing Live Video

To view live video on the View Cameras screen, input the following parameters:

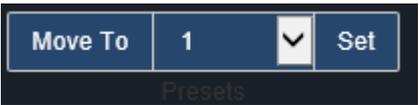
1. **Camera System:** Select the Camera System you would like to view.
2. **Matrix Size:** If the VMS supports a video matrix, you can select a matrix size. By default, the system will automatically choose the best size for the amount of cameras you are viewing.
3. **Mode:** Select **Live Video** as 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

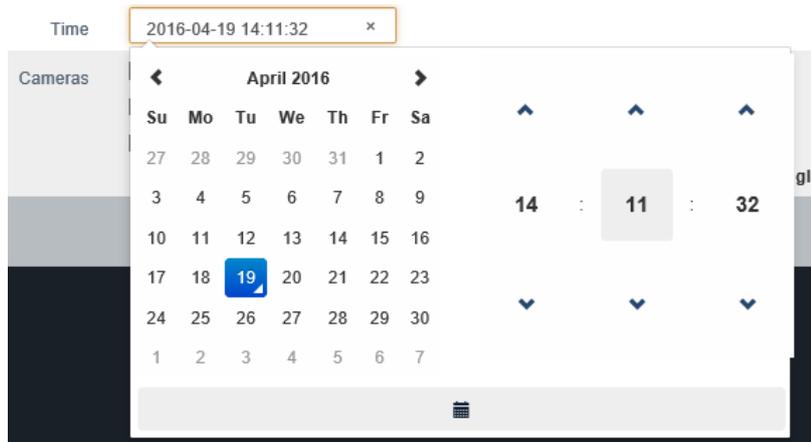
Option	Description
	This button will change the camera mode to playback. You can use the Up arrow to select where to start playback based on the current time or select a time with the date and time picker.
	PTZ Only. Pan Speed will influence how fast a PTZ camera will move when changing positions manually 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.
	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 relevant section within the master 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:

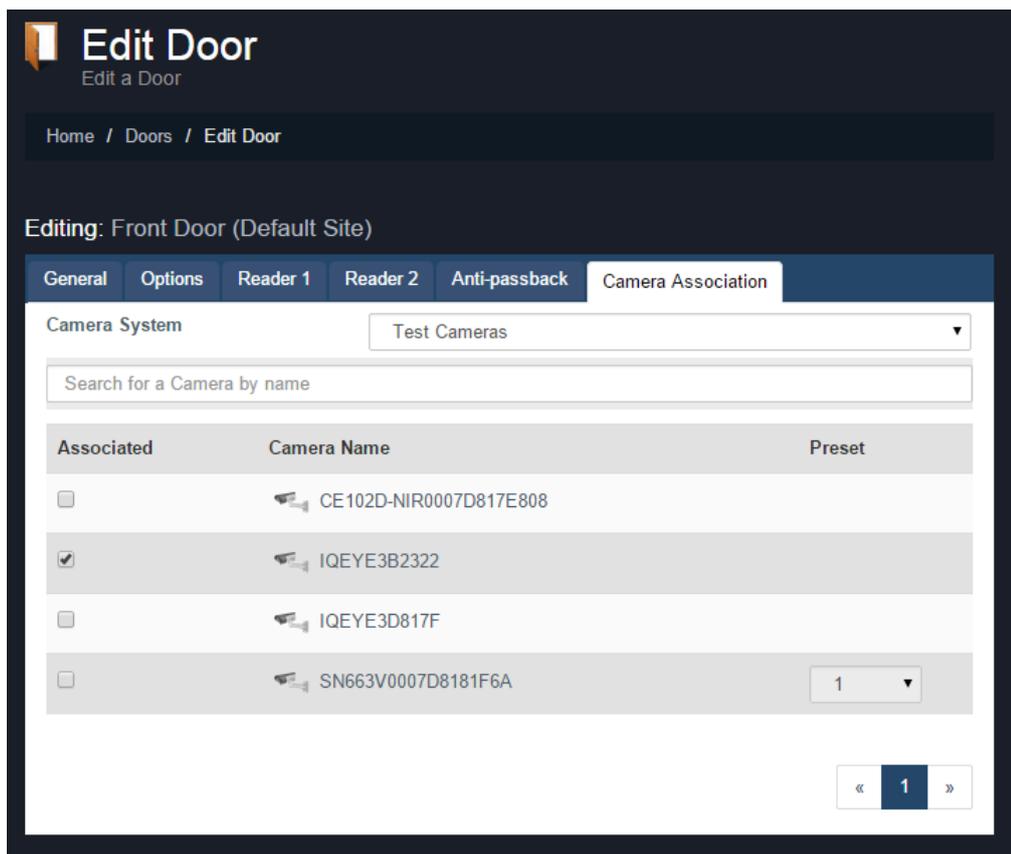
Camera Associations: Door

1. On the **Home Screen**, 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.

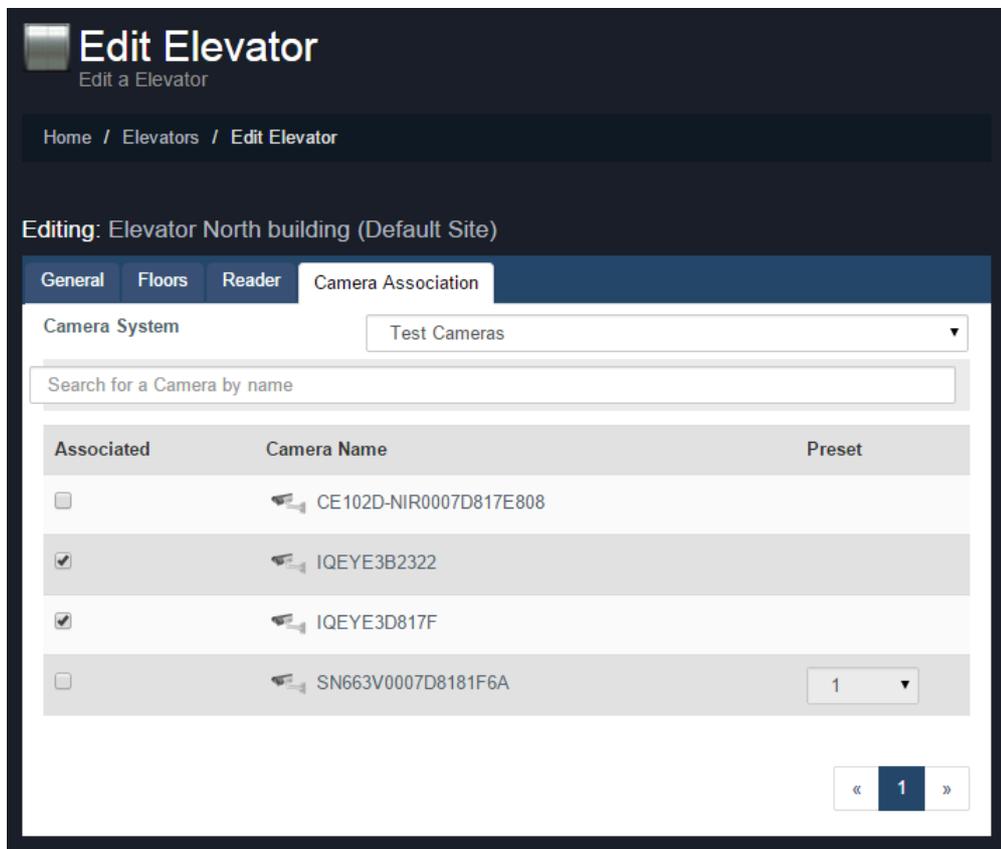
Camera Associations: Elevator

1. On the **Home Screen**, 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

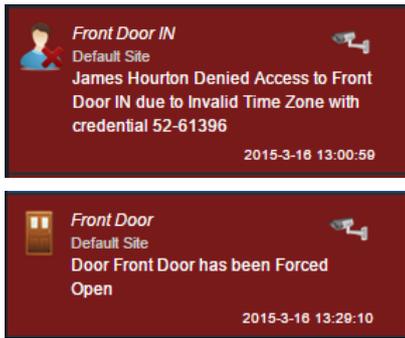


Figure 31.9. Elevator Notifications With Camera Link

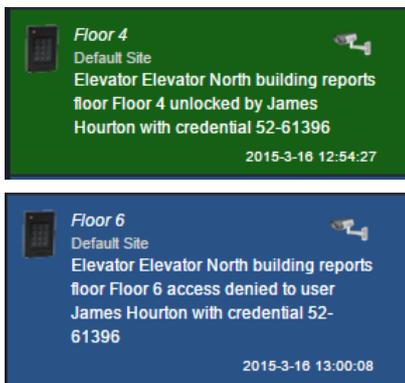


Figure 31.10. Door Activity Report With Camera Link

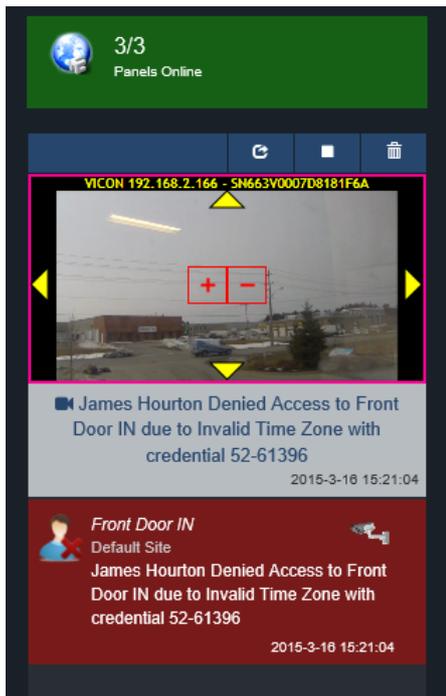
2015-3-16 13:02:24	Front Door		Door Front Door is Now Closed	
2015-3-16 13:00:59	Front Door Front Door IN	James Hourton 52-61396	James Hourton Denied Access to Front Door IN due to Invalid Time Zone with credential 52-61396	
2015-3-16 13:00:57	Front Door		Front Door has been overridden. Current state is Lockdown	
2015-3-16 12:58:42	Front Door		Front Door has resumed from an overridden state	

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.



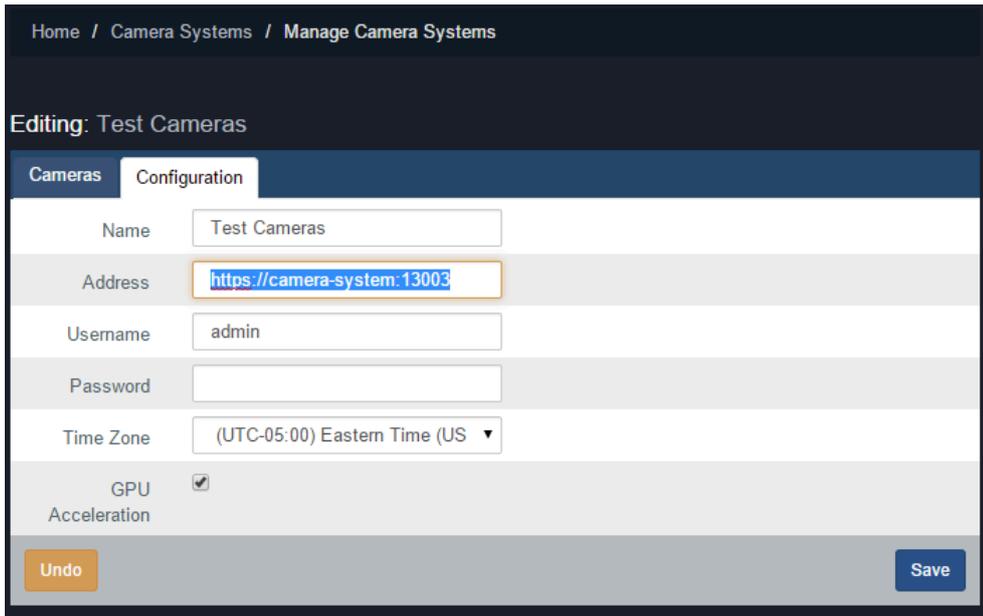
While this external display is open, notifications with the live video option will display in the new window, not the notification bar.

Adding Website Certificates for Camera Integration

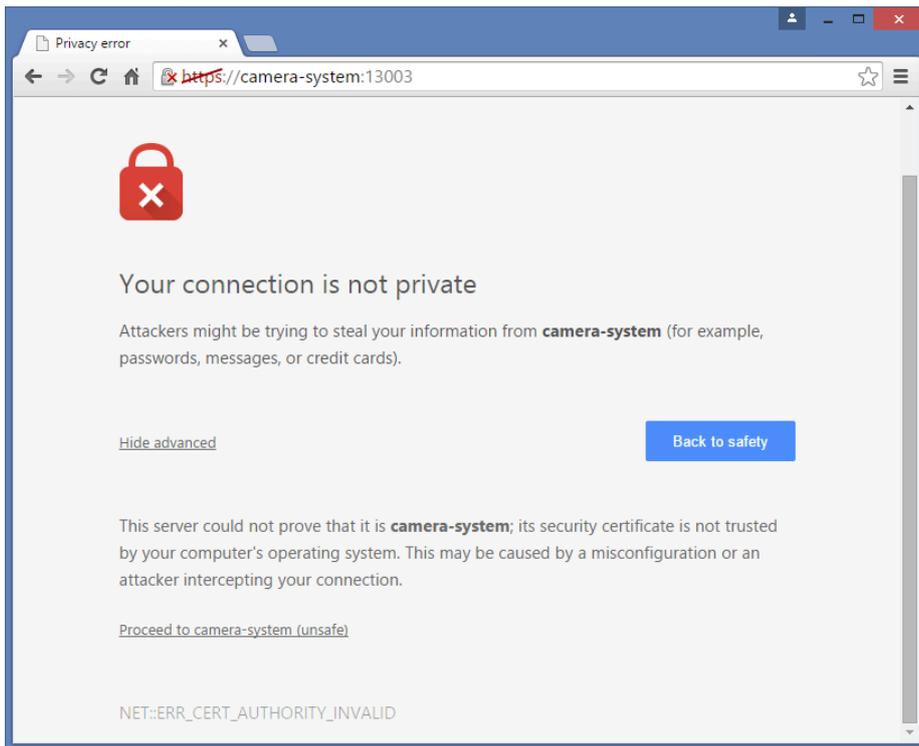
VAX uses secure HTTPS secure communication. If the VMS is using HTTPS as well, we must create a "trust" between the client PC and the VMS. If the VMS web server is using a self-signed certificate (as opposed to an official certificate purchased from a company, such as godaddy.com), you must add the self-signed certification generated by the VMS web server. This does not apply if you are using regular HTTP communication.

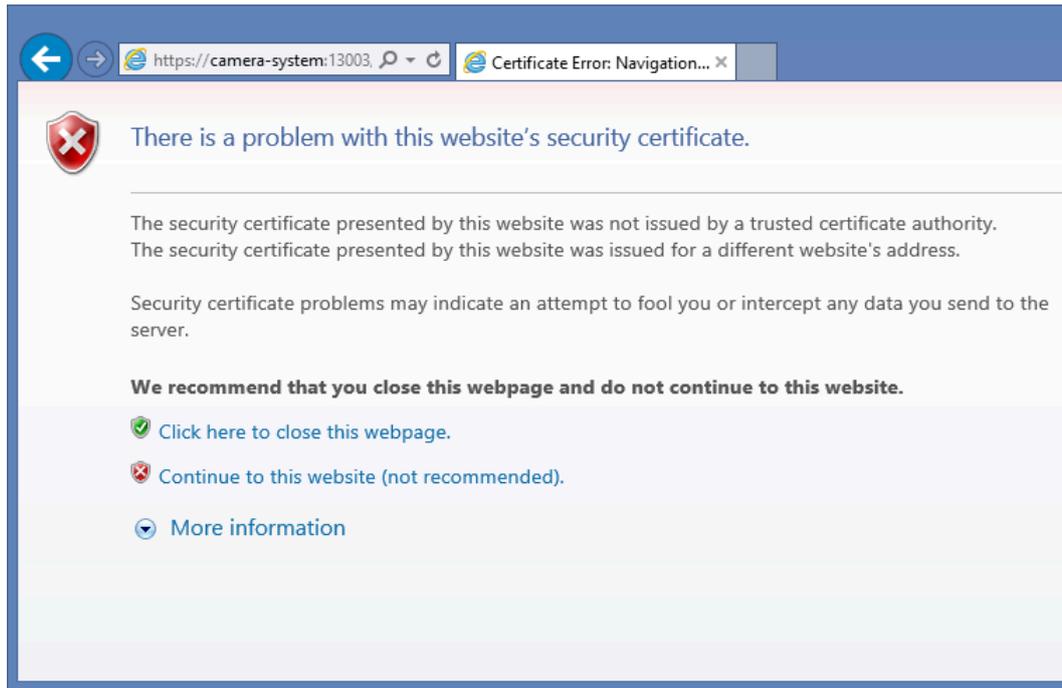
The following instructions will work on most operating systems and web browsers.

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).

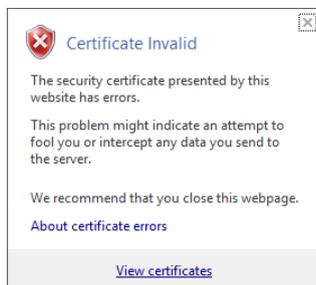




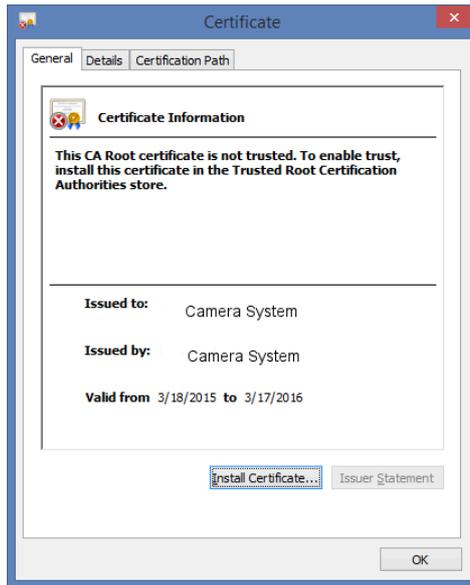
4. The next step is to extract the certification so that we can install it on our computer.

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".

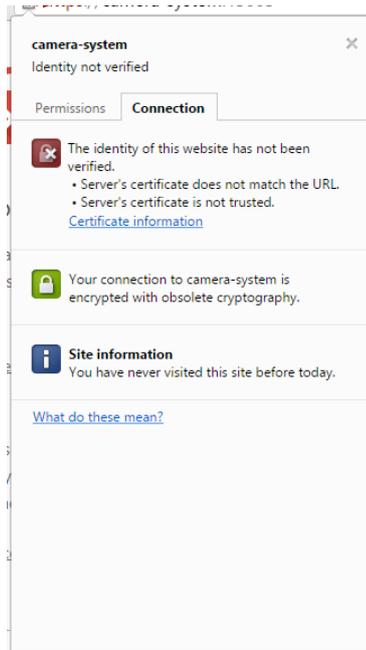


2. On the certificates window, click "install Certificate" on the bottom of the window. The certificate Import Wizard will now appear. Please proceed to the section called "Importing Certificates with the Certificate Import Wizard" to continue the certificate import process.

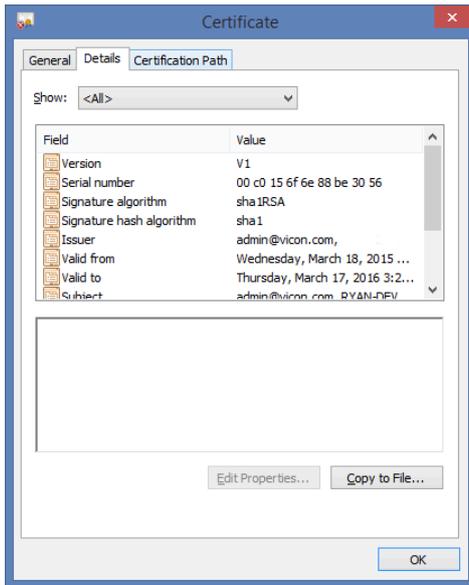


Importing Certification in Google Chrome.

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.

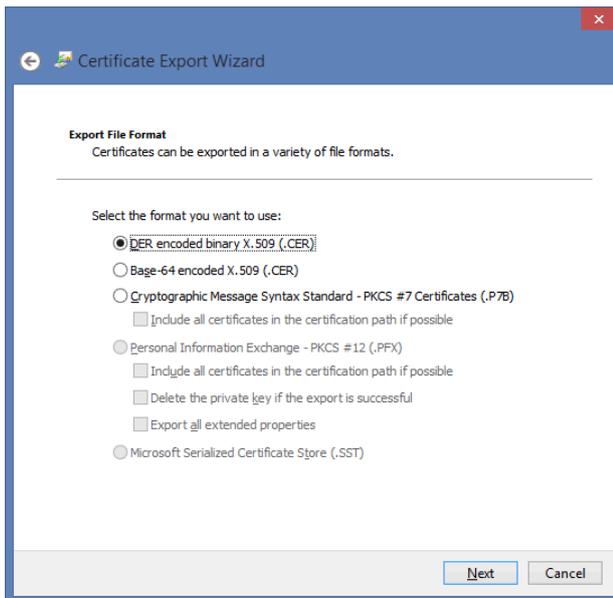


2. On this window, click the link titled "Certificate Information". A new window will appear. Click on the Details tab of this window.

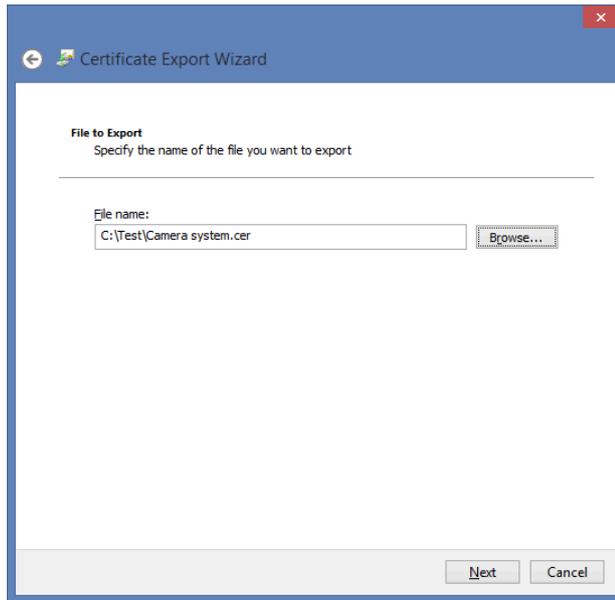


Click on the "Copy to File" button on this screen. This will launch the Certificate Export Wizard.

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 file will now be exported to the selected location.

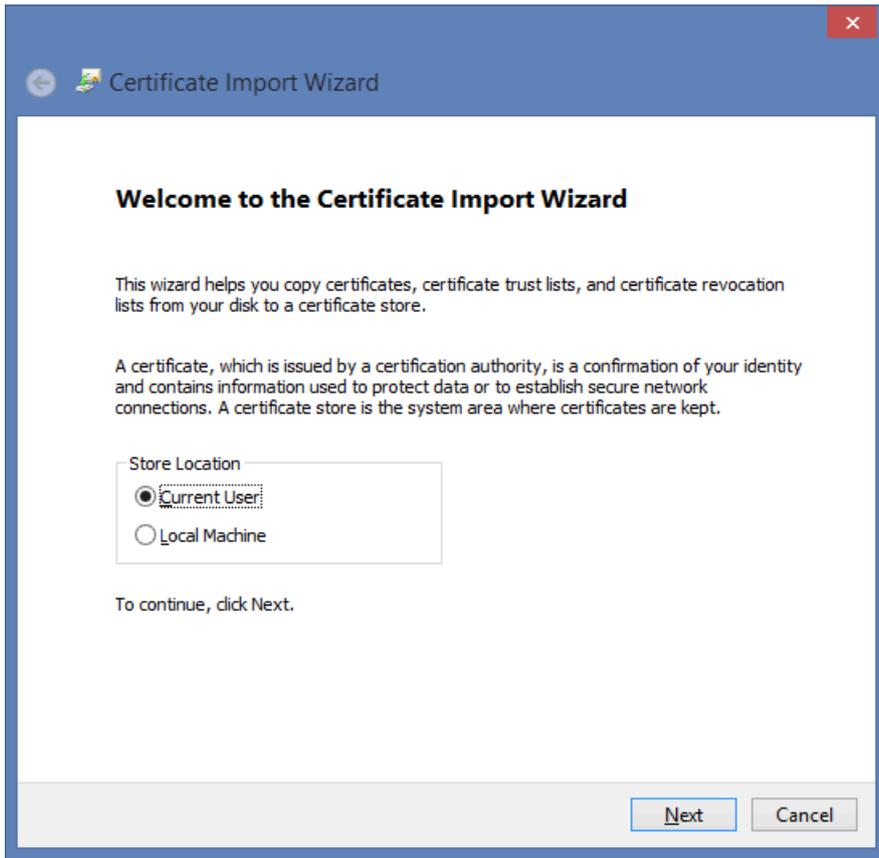


6. Browse to the location you exported the certification file. Right click on the file and select "Install Certificate". This will now launch the Certificate Import Wizard. Please proceed to the section called "Importing Certificates with the Certificate Import Wizard" for further instructions.

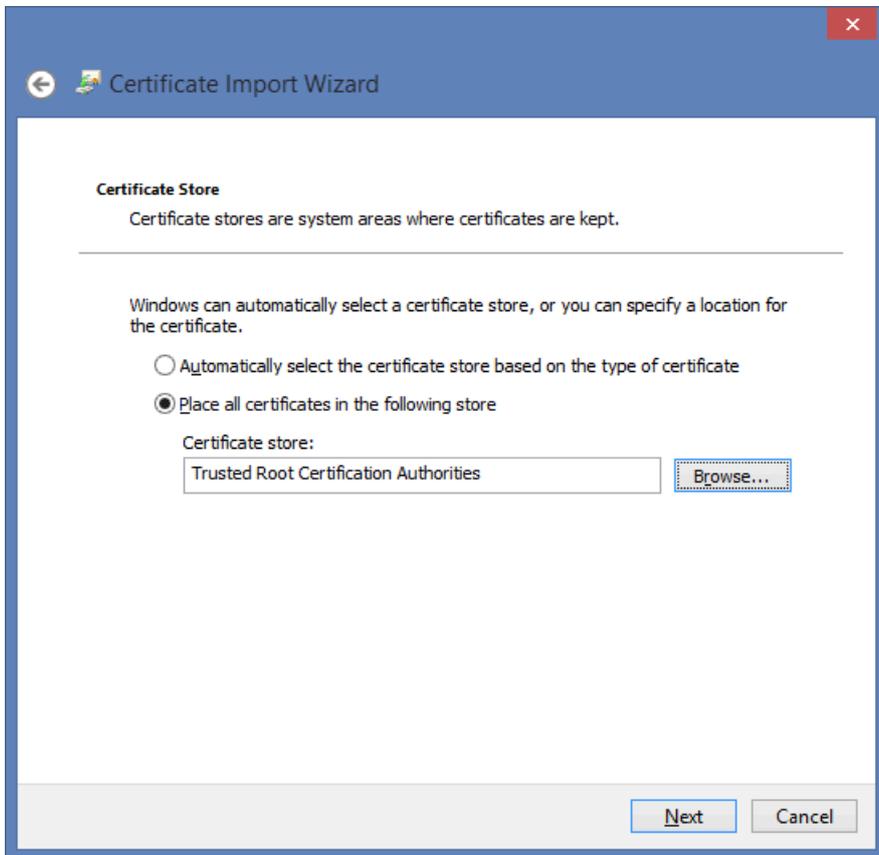
Importing Certificates with the Certificate Import Wizard

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.

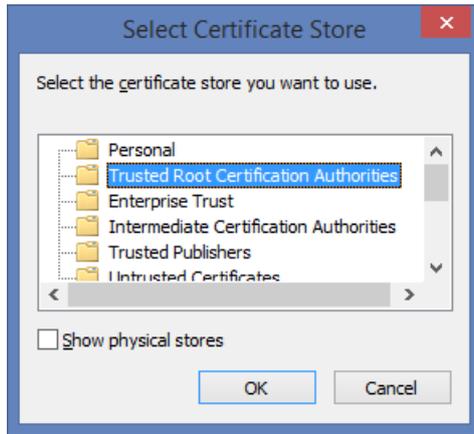
1. On the first screen of the import wizard, select "Current User" as the Store Location; if more than one Windows user will be utilizing the VAX web interface, select "Local Machine". Click Next.



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

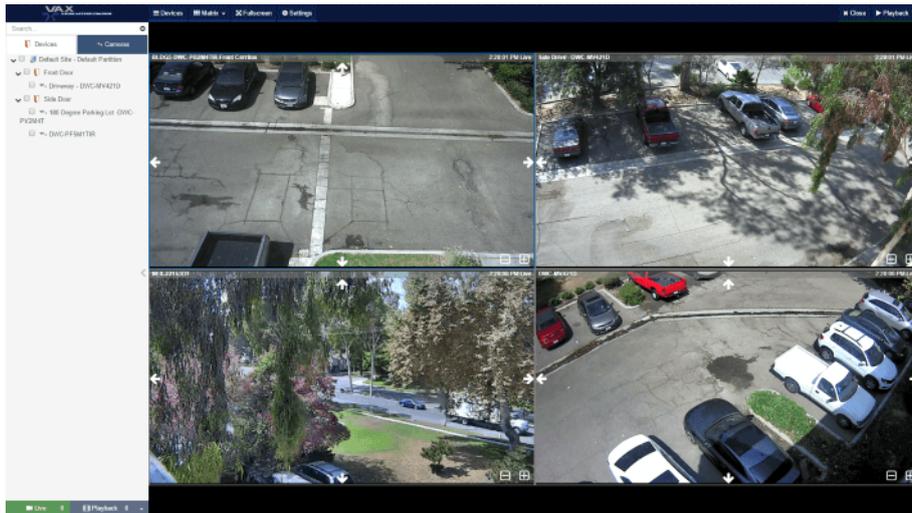
The Camera Matrix is a full screen in VAX dedicated to viewing cameras in a grid view. Cameras from multiple vendors can be viewed simultaneously. A maximum matrix size of 4 x 4 is supported.

On the **Home Screen**, scroll down to the section titled **Day To Day**; click on the **Camera Matrix** icon (pictured below).



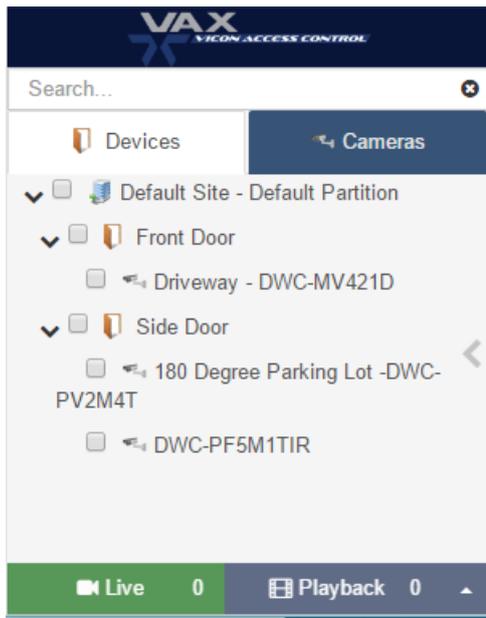
The Camera Matrix screen will open in another tab or external window.

Figure 31.12. Camera Matrix With Cameras



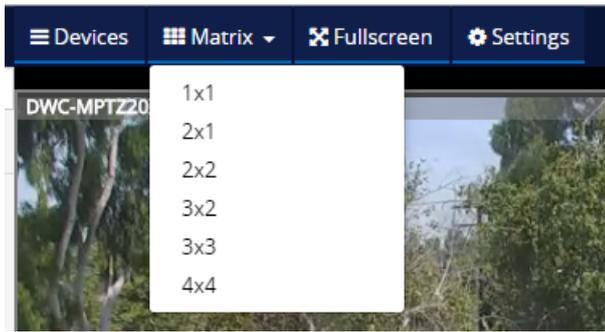
On the left side of the screen is your **Devices** list and **Camera** list.

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.

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, changed 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 be 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.

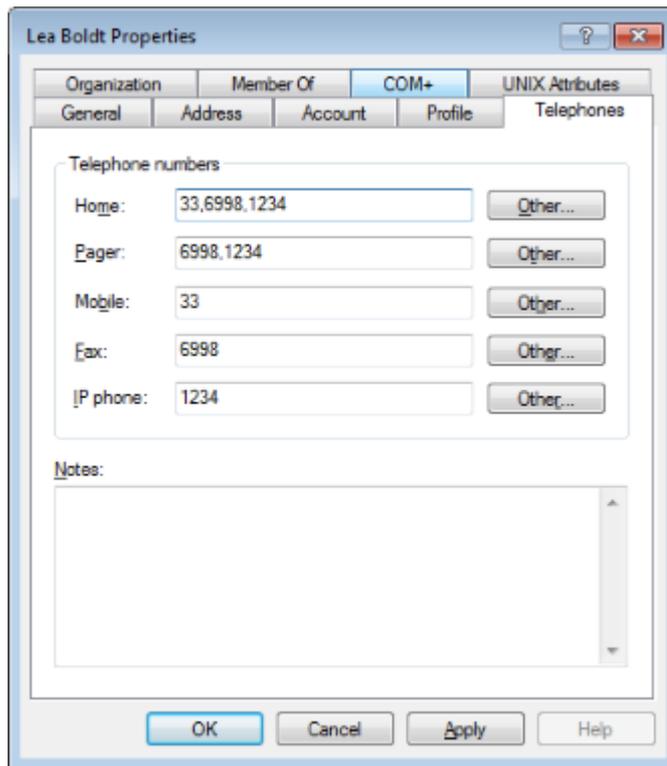
- Wiegand Credential from three Individual Fields:

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 will be in a single AD User Attribute field.

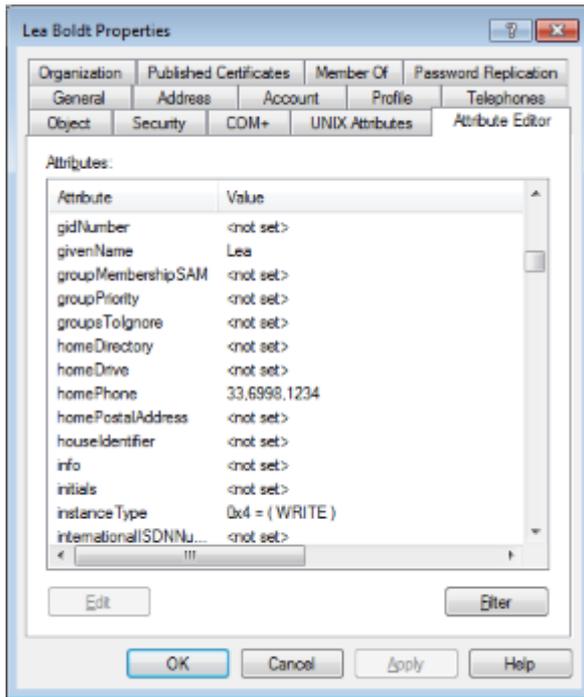
Example 32.1. Example of all types of credentials stored in AD User Attribute Fields



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 VAXWebService 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.

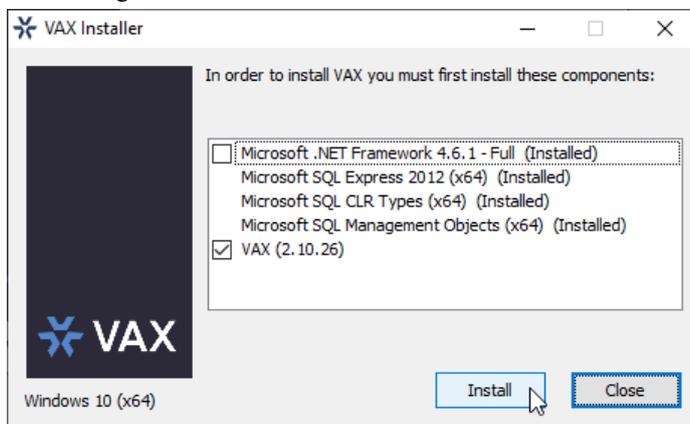
2. Open "Local Security Policy". You can also find it by searching or entering "secpol.msc" into a Run window.
3. In the Local Security Policy Window, expand the "Local Policies" from the left side and select "User Rights Assignment".
4. In the policy list, right click "Log on as a service" and select 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.

Installing VAX in AD Domain Environment

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.

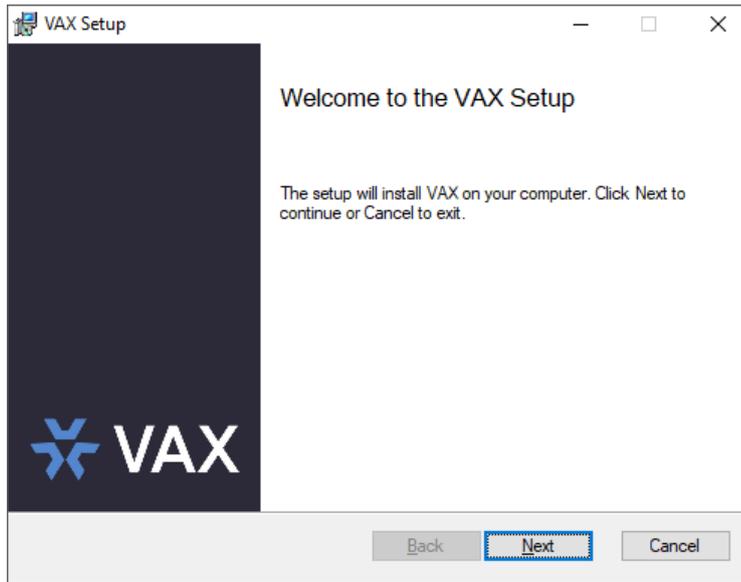


3. Click Install, any checked components will be installed. If you are installing from a VAX installation media; missing components will be installed locally. If installing from a web download, the installer will attempt to install those items from the internet.

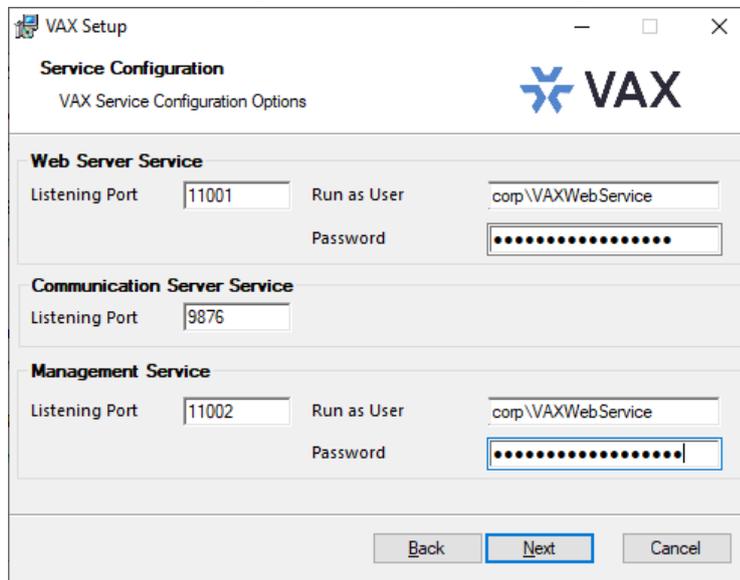
Note

If any components fail to install, try restarting the computer and run the installer again. If components continue to fail installation, contact Vicon 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\VAXWebService"). 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 **Home Screen**, 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.

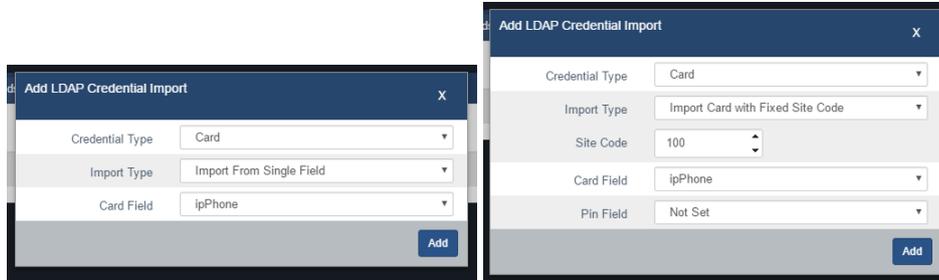
5. Click the **Save** button on the bottom of the screen.

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

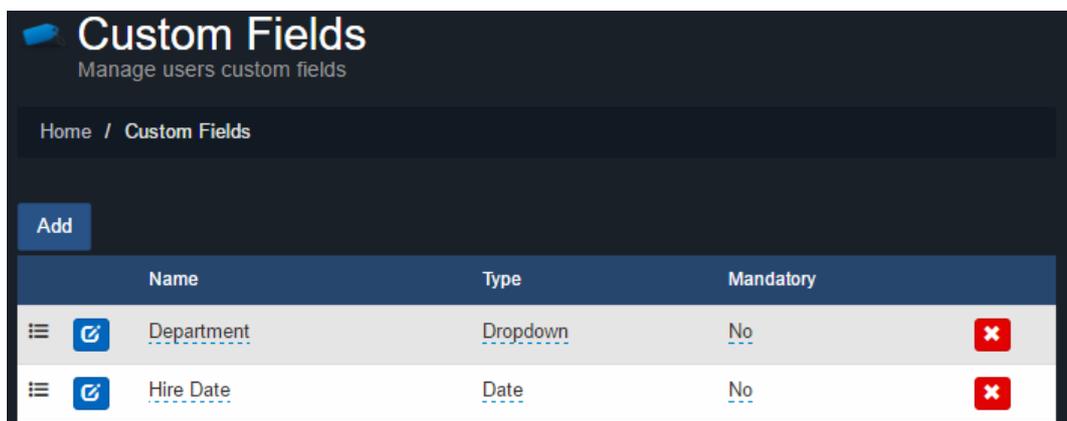
If it was decided during planning phases that one or more AD User Attributes should be synchronized to VAX from Active Directory, follow the rest of this section.

1. Custom Fields should be added in VAX before they are associated with AD Attributes.
2. On the **Home Screen**, 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

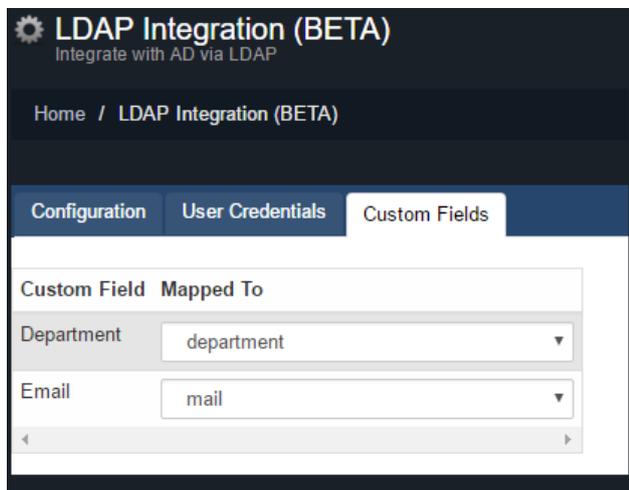


4. After you've added your Custom Fields, we must associate the VAX Custom fields to AD User Attributes.
5. On the **Home Screen**, scroll down to the section titled **Scheduling**; click on the **LDAP Integration** icon (pictured below).



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



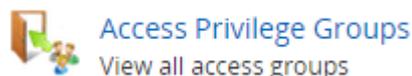
8. You can now move on to the next section for creating Access Privilege Group associations to AD Security Groups.

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 **Home Screen**, 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.

- 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.

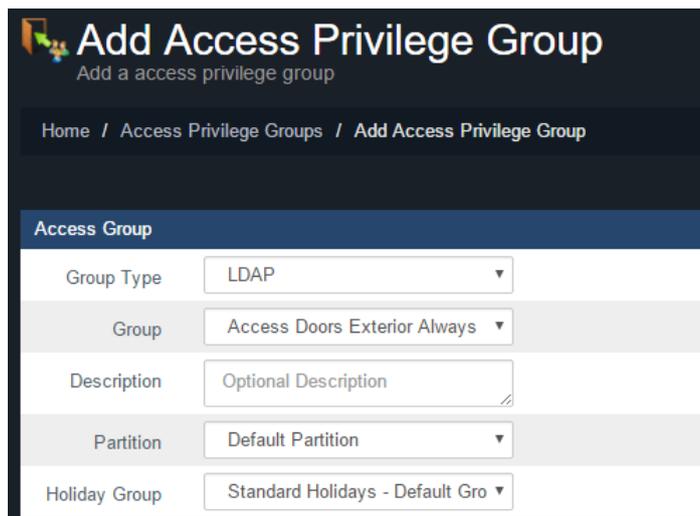
- (Optional) Fill in a description to help other administrators understand the role/purpose of this group.
- Select a Partition to create this Access Privilege Group in.

Note

You can associate the same AD Security Group to multiple Partitions by adding the group multiple times and changing which Partition is selected.

- 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.

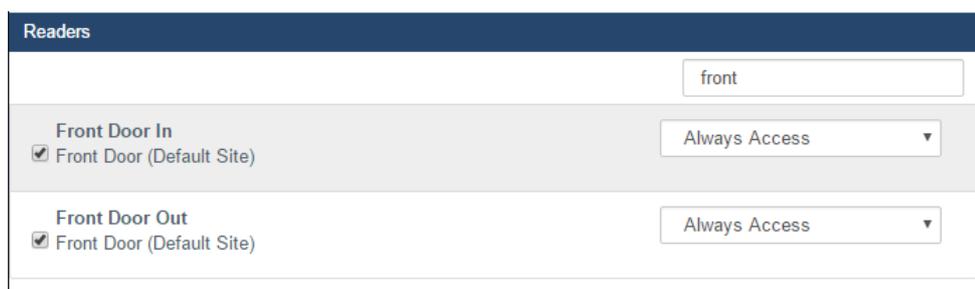
Figure 32.3. Adding a AD Security Group as a Access Privilege Group



- Readers/Floors:

If Panels, Doors, Elevators and Readers have been configured, you can optionally give access to Doors/Floors and select a Time Zone. AD Users that are synchronized will be given access to the specified Doors/Floors based on the User Time Zone 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 **Home Screen**, 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 **Home Screen**, 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 **Home Screen**, scroll down to the section titled **System**; click on the **Administrators** icon (pictured below).



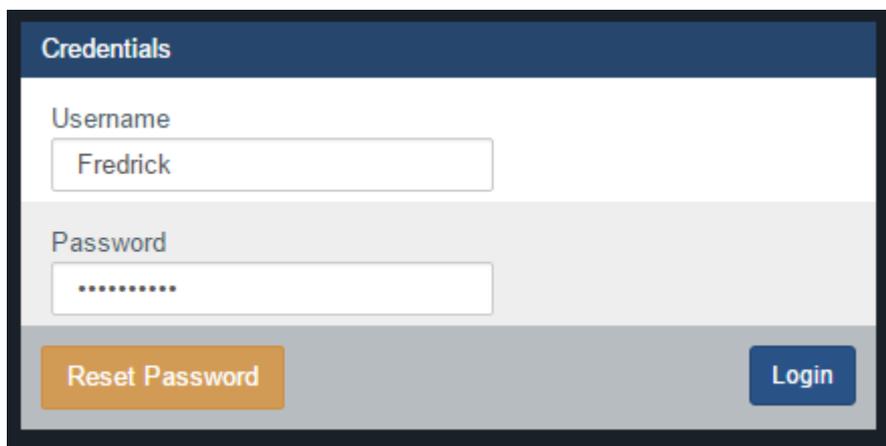
5. Click the "Add" button on this screen.
6. Select LDAP from the Authentication drop-down menu.
7. Fill in the Username with the 'User logon name' from the LDAP provider.

 **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.

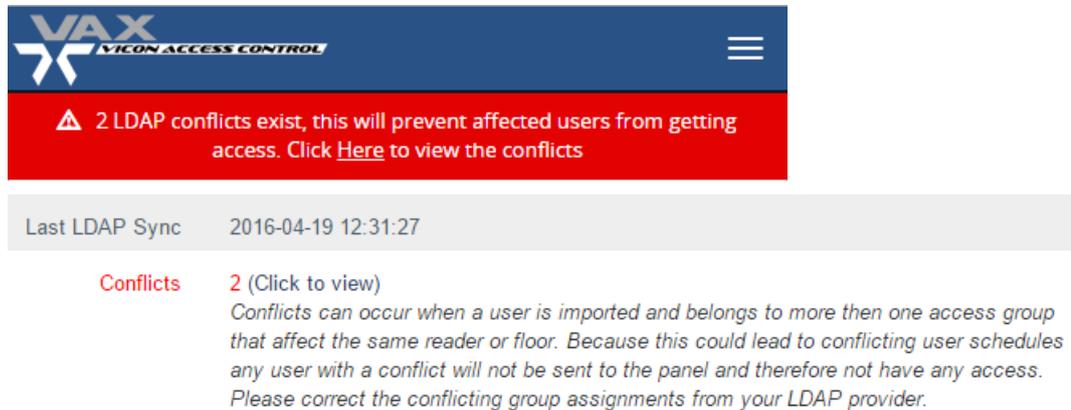
LDAP Conflicts

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.

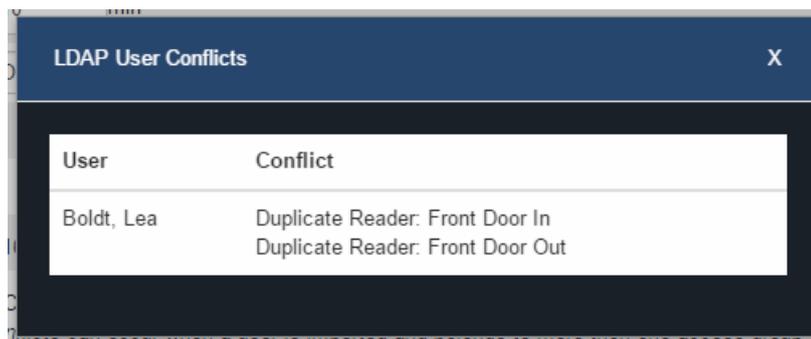
When a conflict occurs, you'll see a red banner on the top of the page and a section on the LDAP Integration screen.

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.

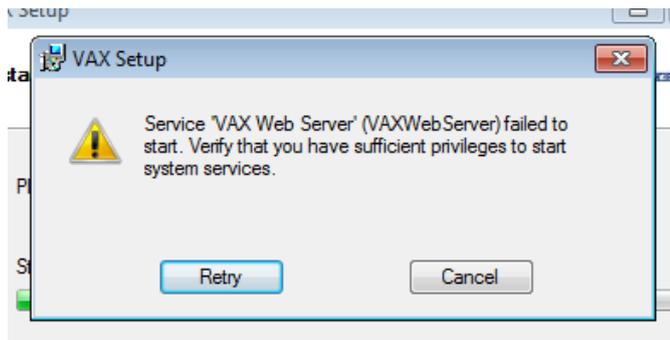
Figure 32.7. LDAP User Conflicts Example



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.

Figure 32.8. Installer Error

Checking Log Files

If the service that failed to start was VAXWebServer, we may be able to check log files for additional information.

1. Navigate to:

C:\Program Files(x86)\Vicon\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 WebServices.HCAuthProvider [(null)] - LDAP Authentication Error: Logon failure: unknown username 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 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 the relevant section within the master tech guide.

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.

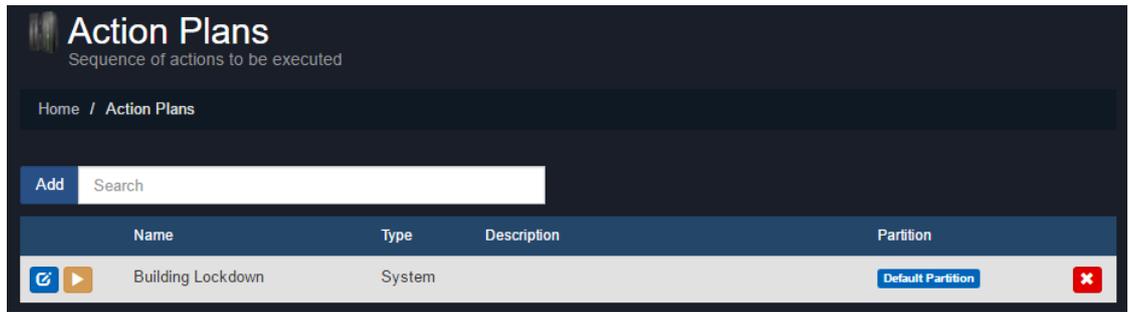
Action Plans

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 **Home Screen**, scroll down to the section titled **System**; click on the **Action Plans** icon (pictured below).



- 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.

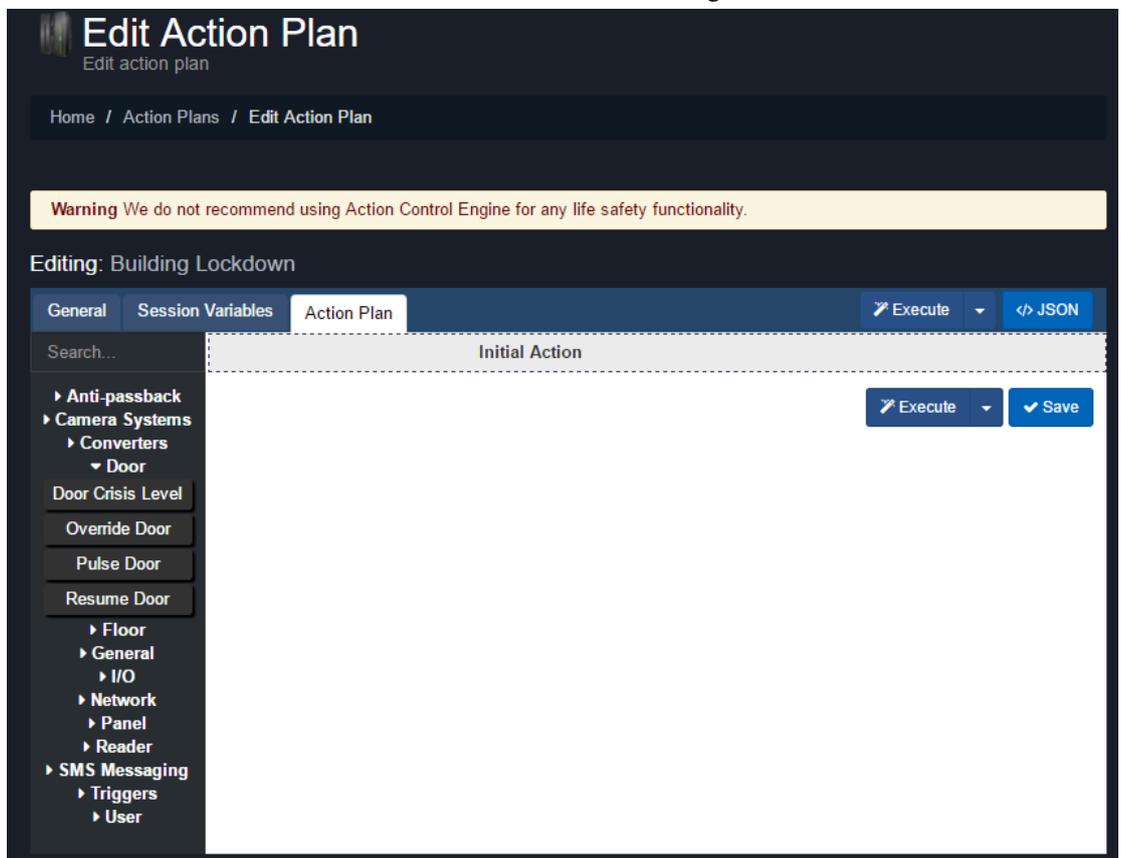


- On the Add Action Plan screen, fill in the name of the plan.

Tip

The name should represent what the action plan will do or its purpose. Description is optional.

- Select a Partition to place this plan into.
- 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.
- 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 section called “Actions” for full list of actions.

Table 33.1. Action Categories

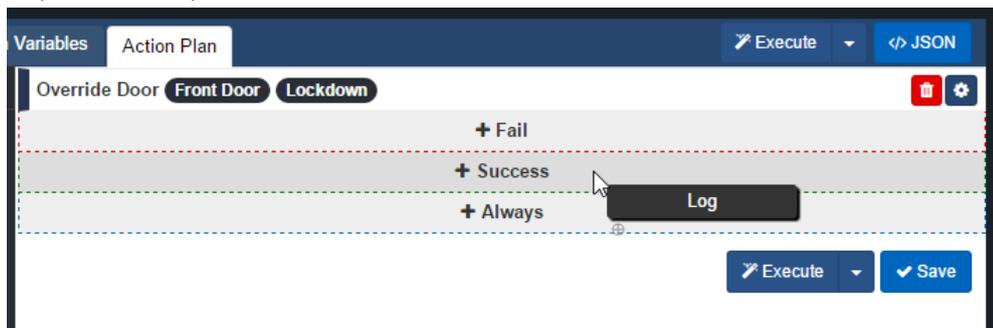
Action Category	Description
Anti-passback	Allows you to reset area and user locations in the system, commonly used to reset anti-passback locations
Camera Systems	Actions that are designed to interact with a VMS system
Converters	Actions that can convert numbers/strings to hashes such as MD5 or Base64. 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 blue Execute button on the Edit Action Plan screen.



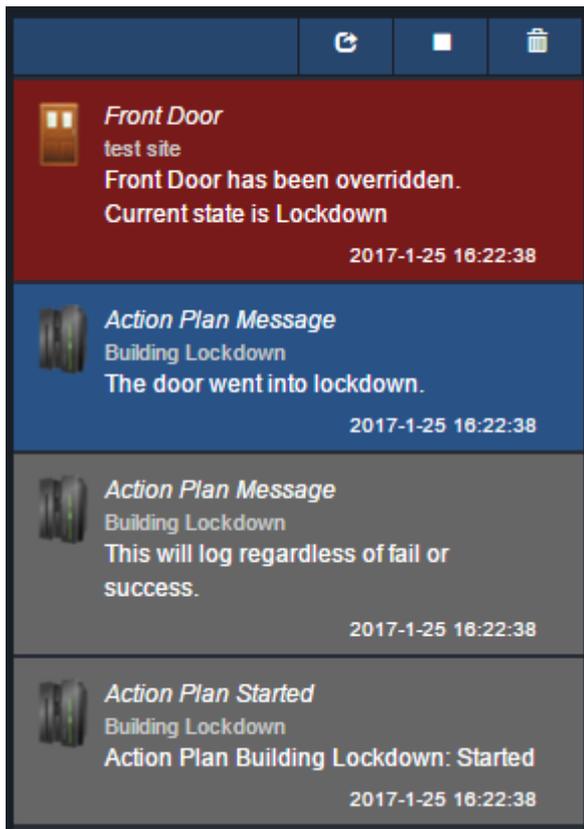
3. Execute the action via VAX Web API via HTTP POST request.

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.

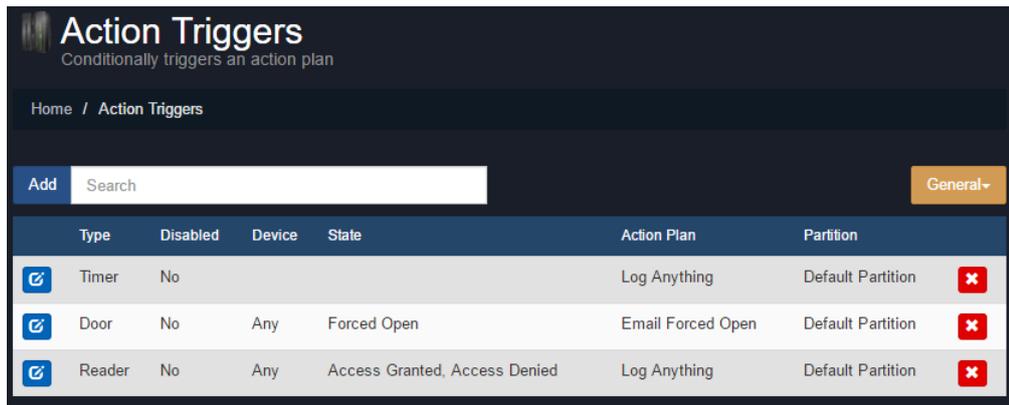
Steps to add an Action Trigger:

1. On the **Home Screen**, 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 the 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.

Trigger Location

Partition:

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.
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

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.

Trigger Conditions	
Type	Door
State	2/10 Forced Open, Held Open 
Door	Front Door

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.

Time Restrictions	
Note Device triggers will execute based on the devices local time.	
Day of Week	7/7 Any 
Start Time	9:00 AM
End Time	5:00 AM
Time Drift	10 Seconds

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.

Action	
Action Plan	Email Forced Open 
Log Level	Info

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 three types of variables available:

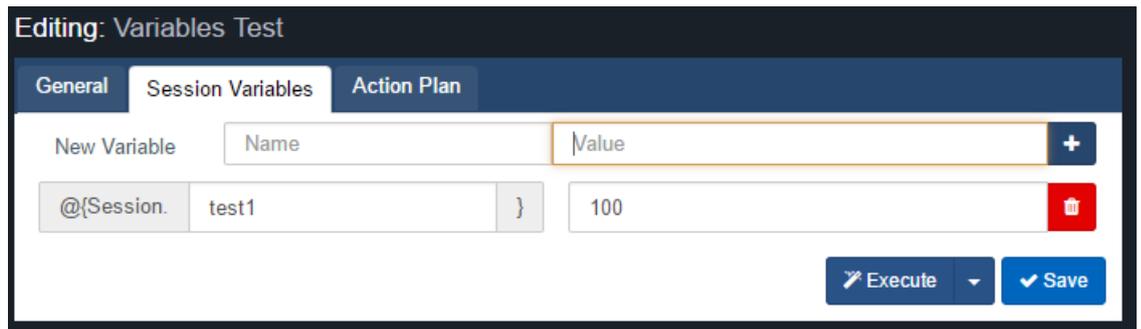
- **Session Variables:** Created during the action plan or as part of the action plan. Can contain numbers, strings, arrays, objects, other variables or the result of an expression.
- **Trigger Variables:** Variables that are available to be referenced or used in the action plan that are based on the 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'.

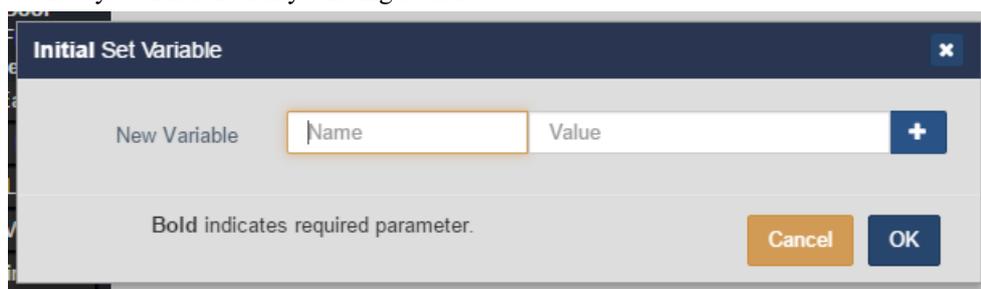
Creating a Variable

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.



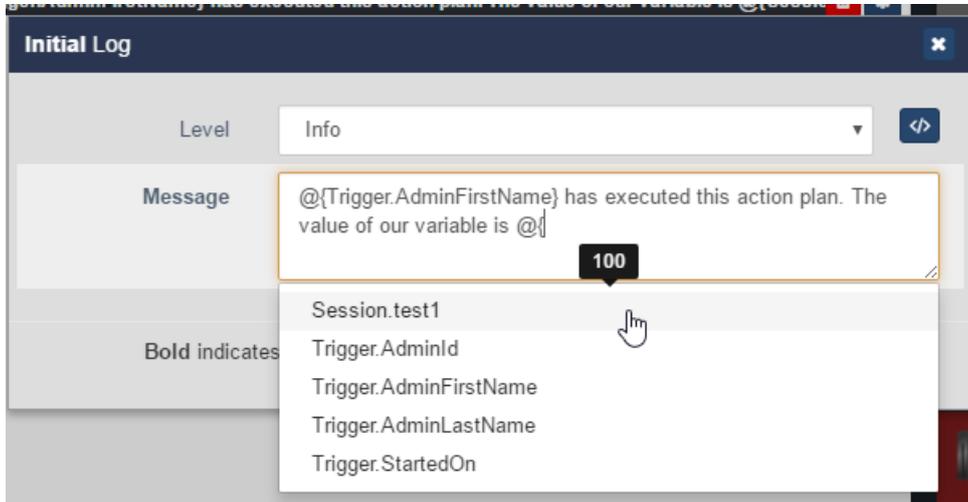
- d. Place a name and value next to the New Variable label. The value can contain an expression, another variable or a raw value.
- e. Click the '+' button to the right of the new variable value. You can add as many variables as you need during a set variable action. You can also edit existing session 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
@[@{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.

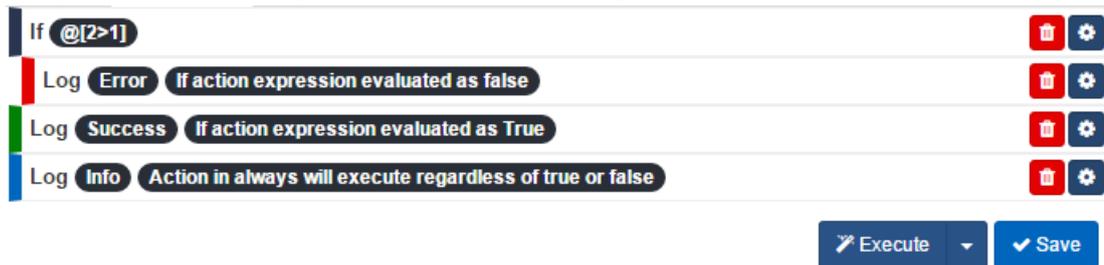
If Action

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:



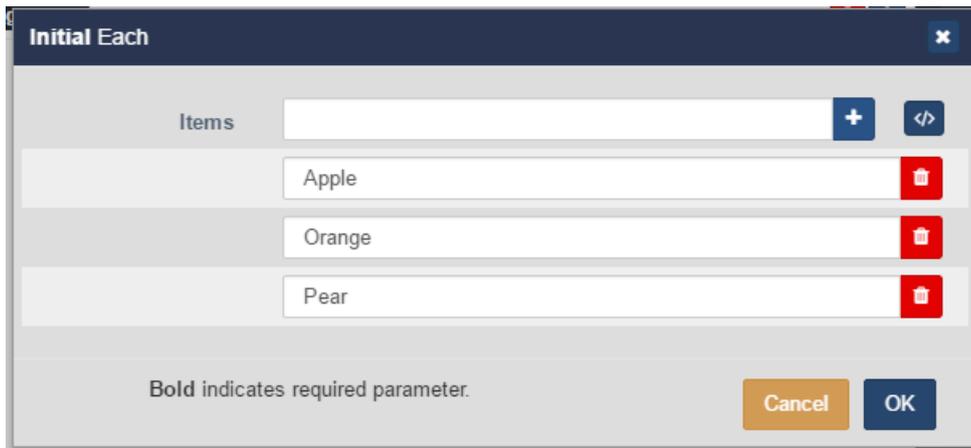
The If action is a powerful tool that can make action plans more customizable and more reactive to different circumstances.

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.

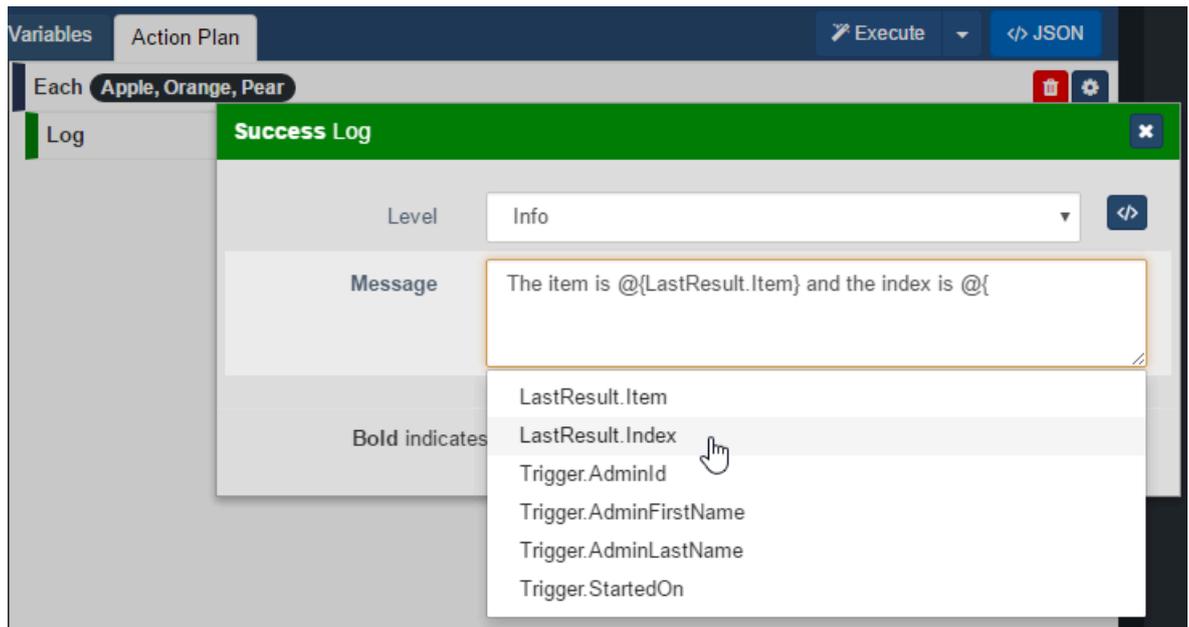
Figure 33.5. Each Action Example Items

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.

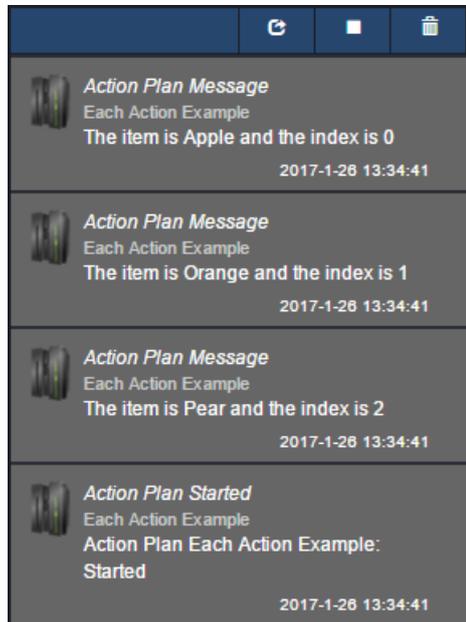
Figure 33.6. Each Action Example Variable

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.

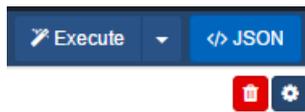
- '@{LastResult.StatusCode}': This variable will contain the HTTP status code returned by the destination address.
- '@{LastResult.Content}': This variable will contain the response returned by the destination address. You can save this variable as a session variable for later use or use this variable 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

The screenshot shows a software interface with a dark blue header. On the left, there are two tabs: "Variables" and "Action Plan", with "Action Plan" being the active tab. On the right side of the header, there are two buttons: "Execute" with a play icon and a dropdown arrow, and "List" with a list icon. The main area of the interface displays a JSON object in a light blue monospaced font. The JSON structure is as follows:

```
{
  "InitVar": {},
  "Action": {
    "_Type": "Each",
    "Parameters": {
      "Items": [
        "Apple",
        "Orange",
        "Pear"
      ]
    },
    "Fail": null,
    "Always": null,
    "Then": {
      "_Type": "Log",
      "Parameters": {
        "Level": 2,
        "Message": "The item is @{LastResult.Item} and the index is @{LastResult.Index}"
      }
    },
    "Fail": null,
    "..."
  }
}
```

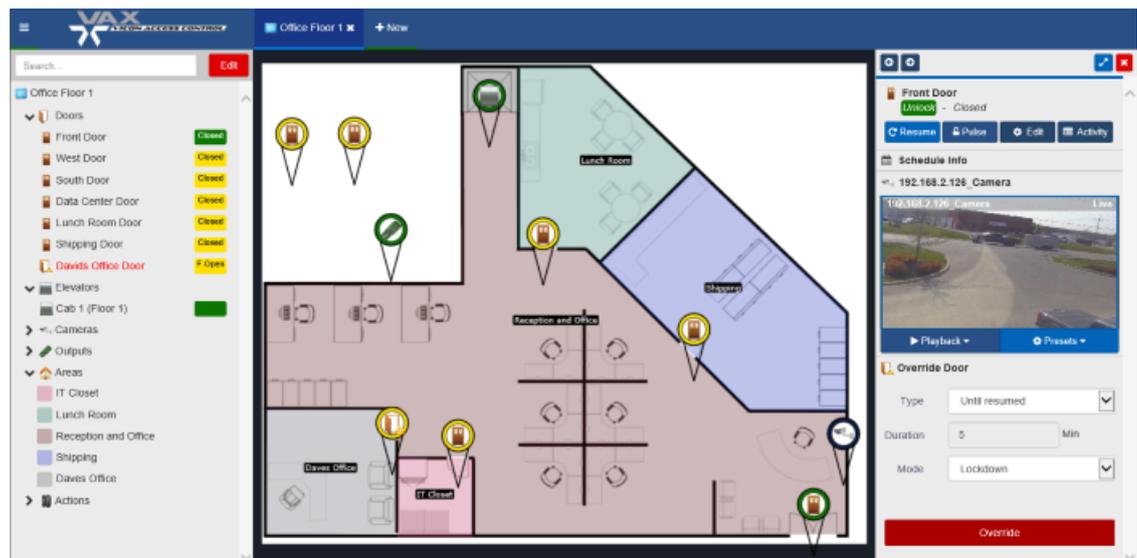
Chapter 34. Interactive Maps

This chapter will demonstrate how to setup and view interactive maps within VAX.

Interactive Maps is 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



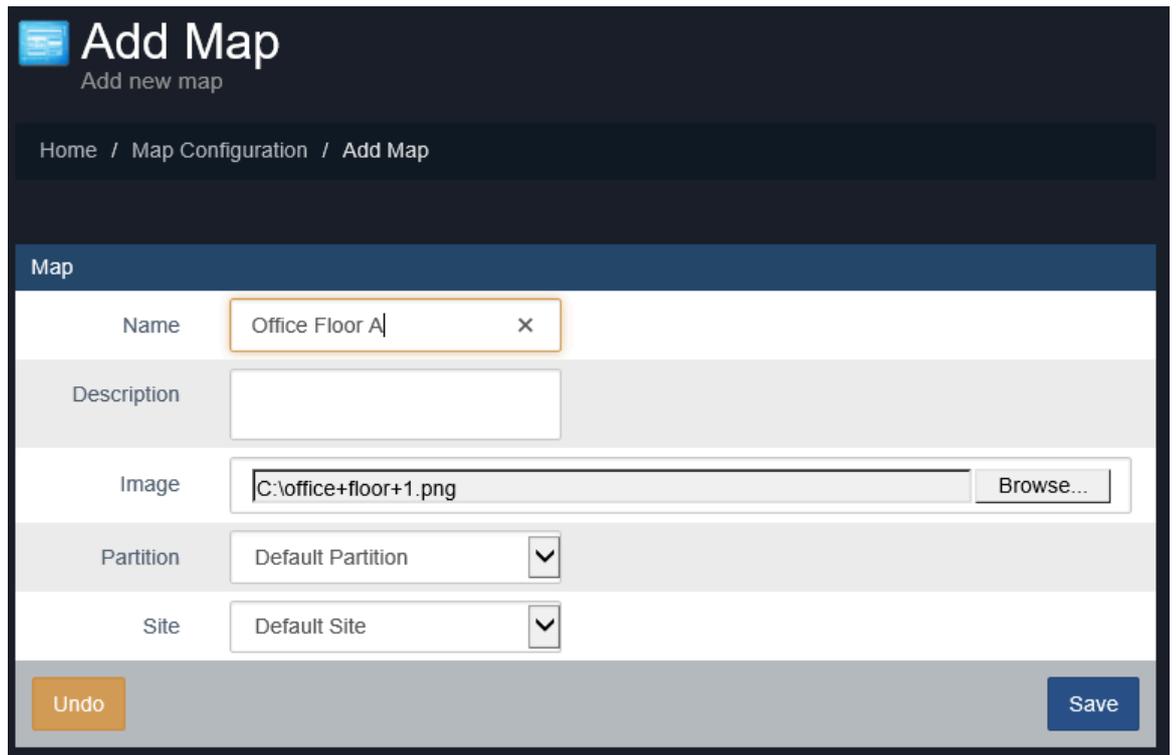
Adding a Map

Use these steps to add a map to VAX.

1. On the **Home Screen**, 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	Optionally choose a Site this map is associated to. This will influence which objects can be placed on the map based on site scope.

- 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

Editing: Office Floor A View Map

General Adjacent Maps Objects

Note
Adjacent Maps allow you to define maps that are immediately surrounding it. These links will appear as buttons on the right-side of the map viewer.

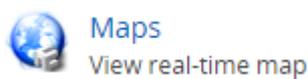
North Map	Warehouse	▼
East Map	Select Map...	▼
South Map	Select Map...	▼
West Map	Select Map...	▼
Above Map	Office Floor 2	▼
Below Map	Select Map...	▼

Undo Save

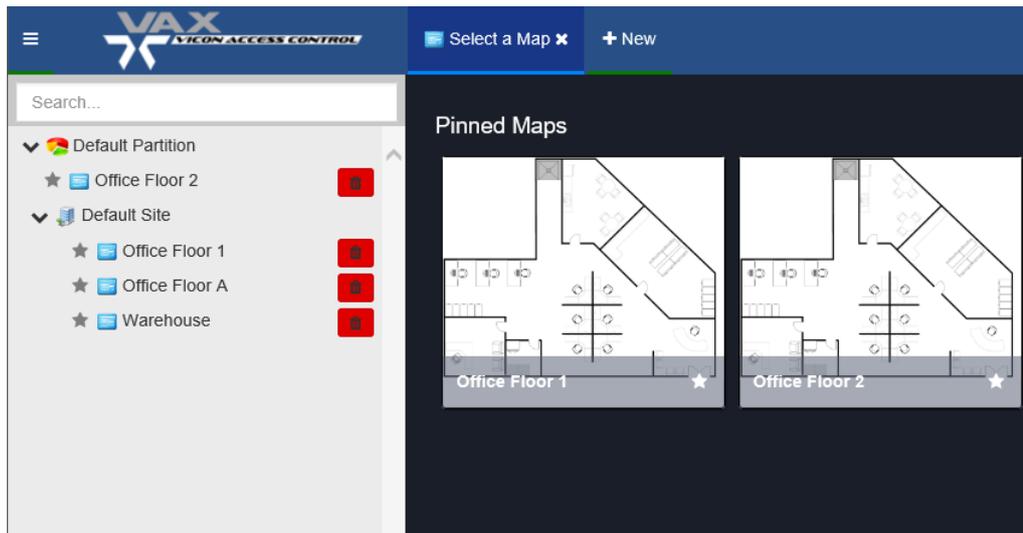
Adding Objects to Maps

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 **Home Screen**, 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

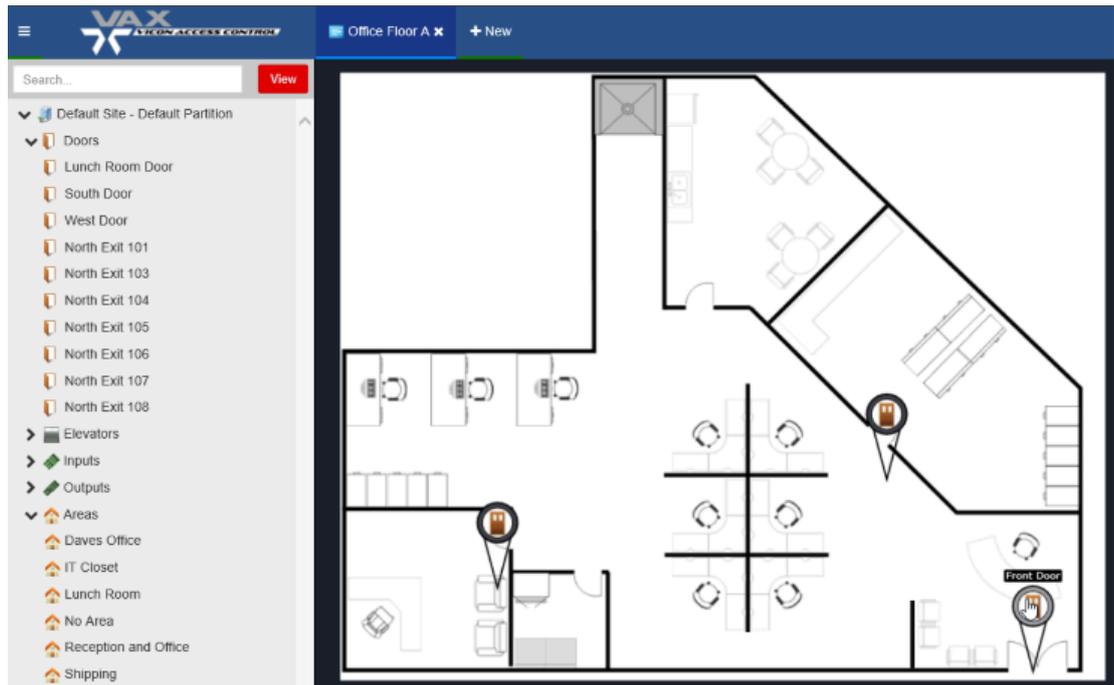
Clicking the star icon to the right of the map name on the map itself will pin the map to the front of the thumbnail list.

3. Select a map by clicking on it. The map will now be displayed in the map viewer.
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.

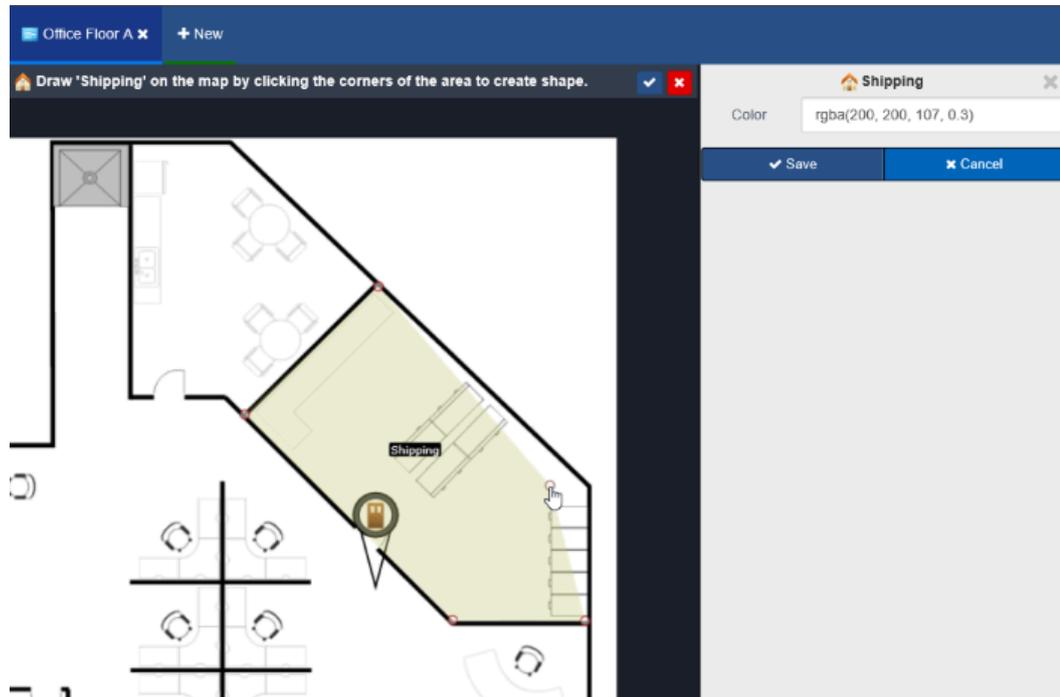
Tip

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.

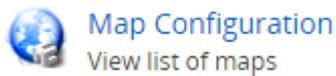
Figure 34.6. Drawing an Area



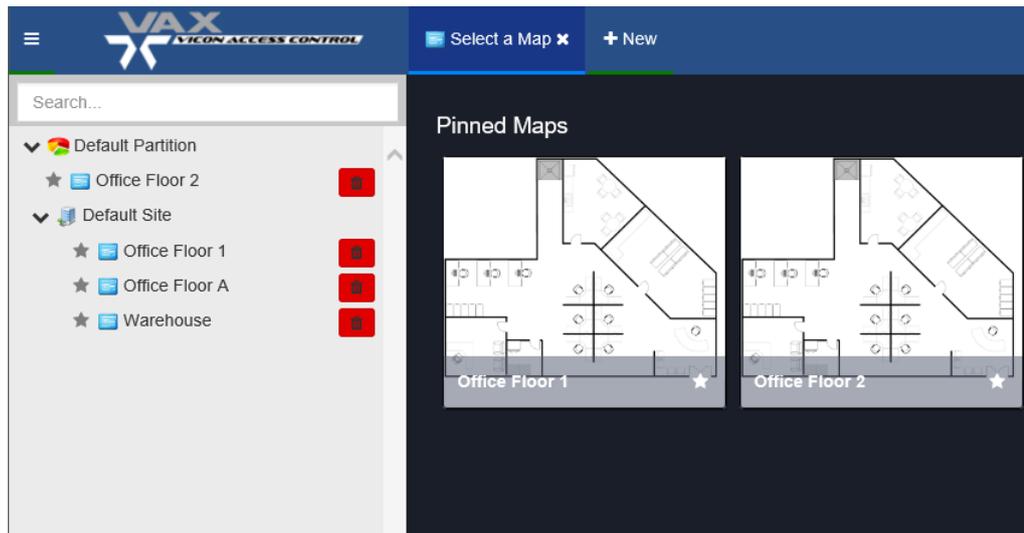
Viewing and Monitoring With Maps

This section will go over options available when viewing a map. Use the following steps to view a map.

1. On the **Home Screen**, 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.



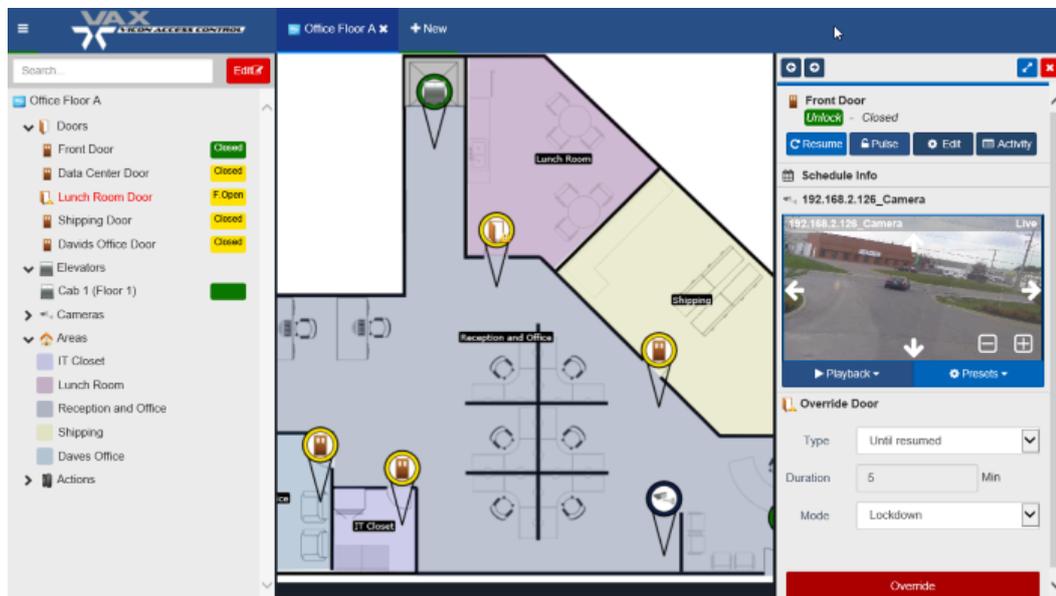
2. On the Map Viewer, you'll be shown the **Select a Map** tab; any maps you've already configured are listed here. A thumbnail of each map will appear with its title.

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.

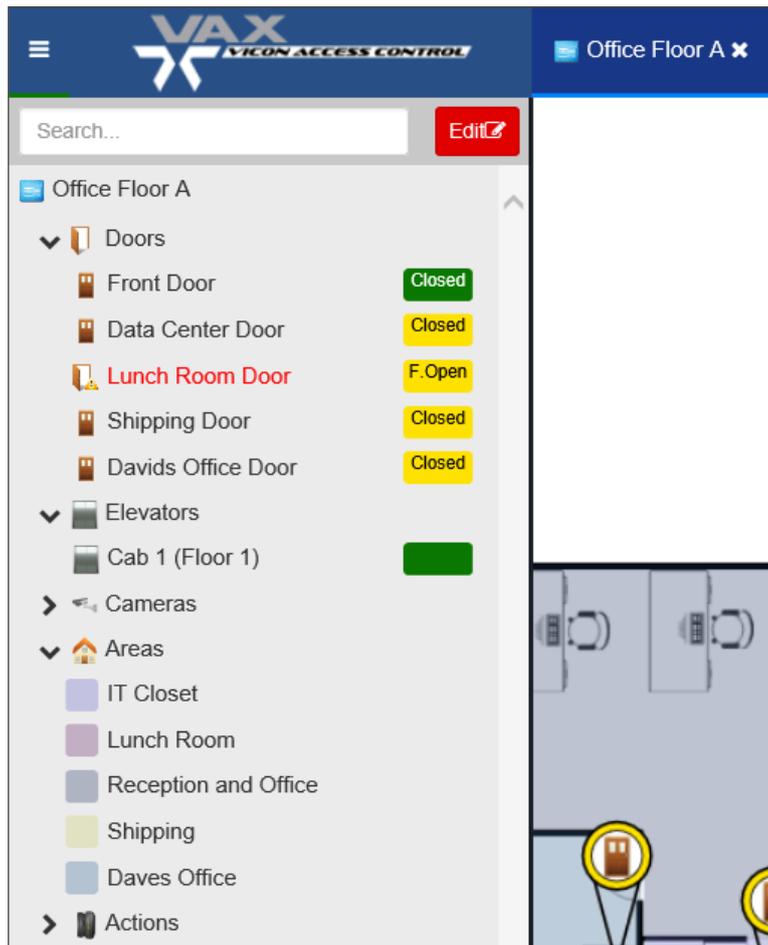
Tip

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.

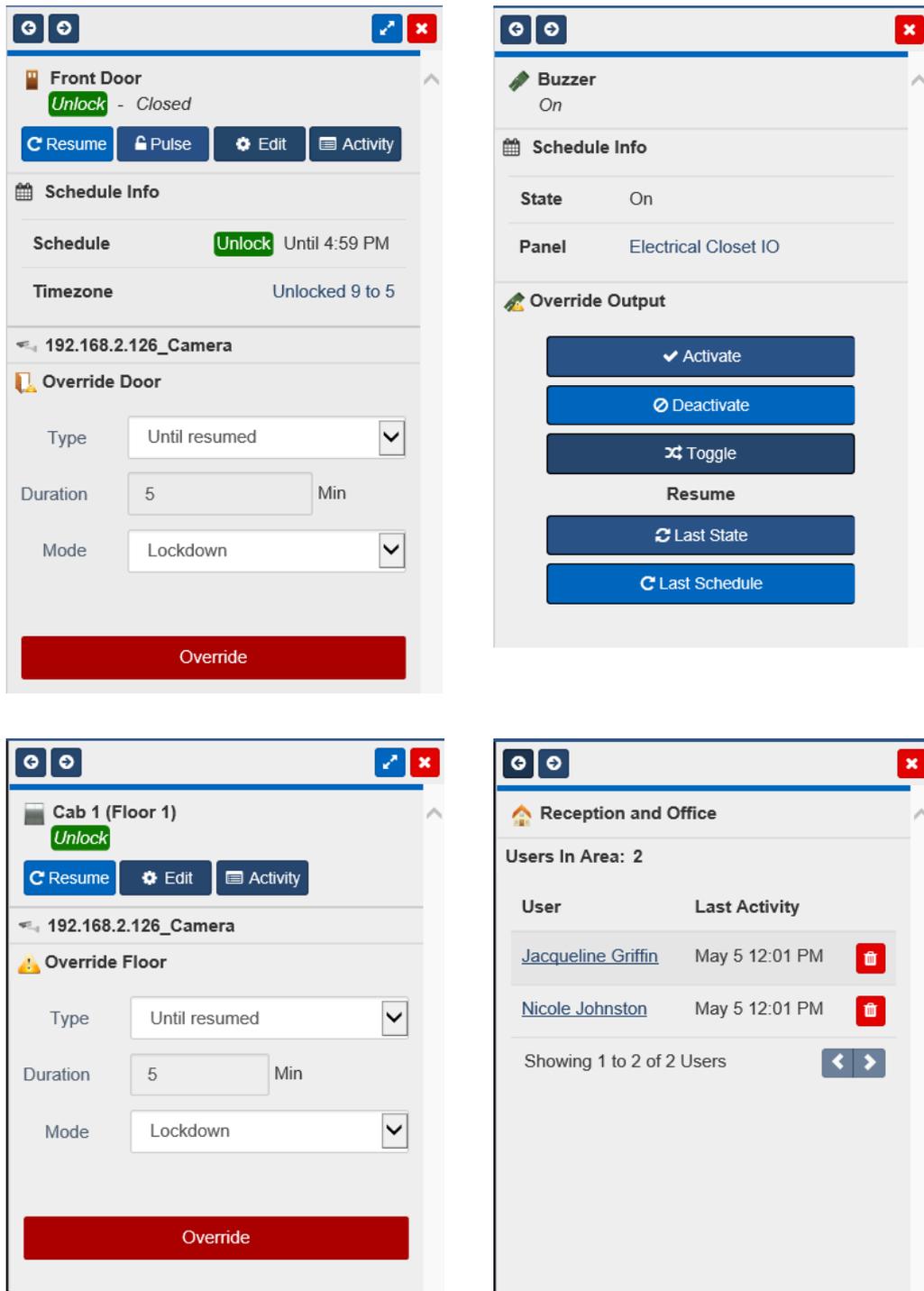
- Doors will show which mode they are in based on color code.
- Doors with door contacts will show if they are open or closed.
- Doors that are held open or forced open will have their name color changed to red and show the alert text right of the name.
- Objects that have been overridden will show their name as red.
- Objects connected to panels that are offline will appear gray.
- 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 Vicon Access Control integrates with third party software systems. This includes the cardPresso® photo badging software and ASSA ABLOY wireless lock systems.

CardPresso Photo Badging Software

This section covers the configuration of Vicon Access Control to interface with the photo badging software cardPresso.

By following these steps you will be able to utilize the User and Credential information contained within the Vicon Access Control database when you are creating badges with cardPresso.

Several of these steps require administrative rights to the Vicon Access Control server and basic IT knowledge. If you experience issues following this guide please contact your internal IT staff or Vicon.

This guide was written using Windows 7 64 bit computer with **Vicon Access Control 2.2+** and **card-Presso 1.4.137 XL version**.

Supported Fields

The following is a list of fields cardPresso can import from the Vicon Access Control database along with a brief description of what the field does.

Table 35.1. List of Fields

Field Name	Data Type	Brief Explanation
RecordId	string	A combination of the sitecode and card number formatted as <site code>-<card number>.
UserId	integer	A unique identifier for each User. User pictures are stored based on this field.
FirstName	string	The first name of the User.
LastName	string	The last name of the User.
StartedOn	datetime	The date that the User account becomes active and will be given access to secured locations.
ExpiresOn	datetime	The date that the User account becomes inactive and can no longer access secured locations.
Master	true/false	If a User account master field is set to true, that account will be granted access to any Door, regardless of lockdown state.
Supervisor	true/false	If the User account supervisor field is set to true, that account can be used for dual Credential Door Time Zones.
SiteCode	integer	A prefix for the card number, together with a card number, creates a User Credential.
CardNumber	integer	A unique number used in conjunction with sitecode to create a User Credential.
CanDisengageEmergency Alarm	true/false	If the User account CanDisengageEmergencyAlarm field is set to true, that account can disengage alarms using the triple swipe feature.
TripleSwipe	true/false	If the User account TripleSwipe field is set to true, that account can use triple swipe features at any Reader or keypad that triple swipe is configured.

Field Name	Data Type	Brief Explanation
FirstCardInEnabled	true/false	If the User account FirstCardInEnabled field is set to true, that account can be used in first card in Door Time Zones to change the Door into its public schedule.
AutoOpener	true/false	If the User account AutoOpener field is set to true, that account has permission to operate automatic Door operators after their Credential has been granted access.
Partitions	integer	This field is populated by the names of the Partitions that User account belongs to.
Custom 1-10	integer	cardPresso can import the first 10 custom fields assigned in the Vicon Access Control software. These fields can include job titles, phone numbers, rank, etc.

Creating an ODBC Connection for cardPresso

In this step we will create a data source reference so that cardPresso will interface with the Vicon Access Control database. These instructions are based upon the assumption that Cardpresso will be installed on the some computer the Vicon Access Control database is installed on.

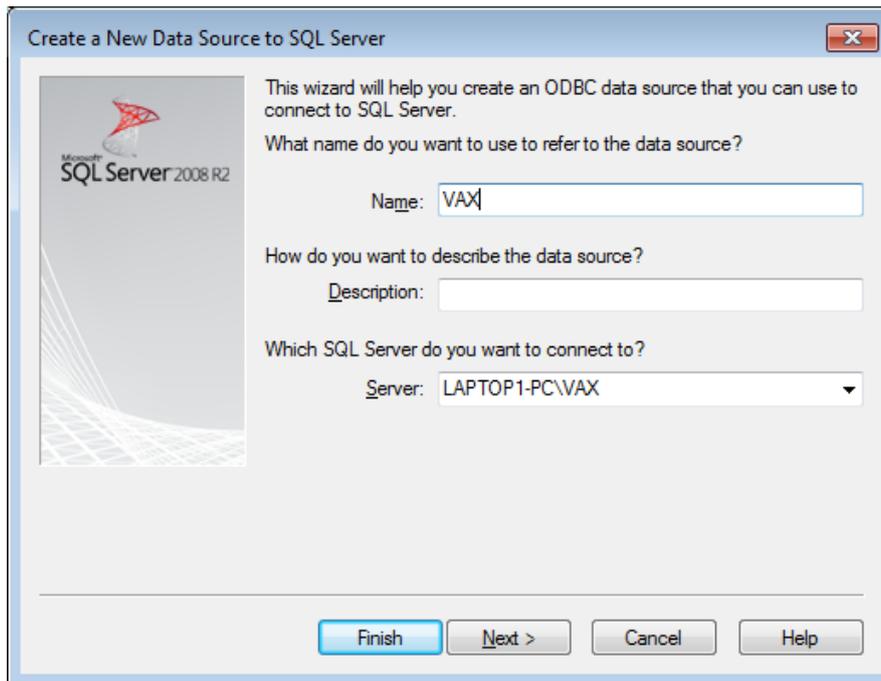
1. Open **Control Panel**; click on **Administrative Tools** or use the search bar to find **Administrative Tools**.
2. Open "Data Sources (ODBC)".

Note

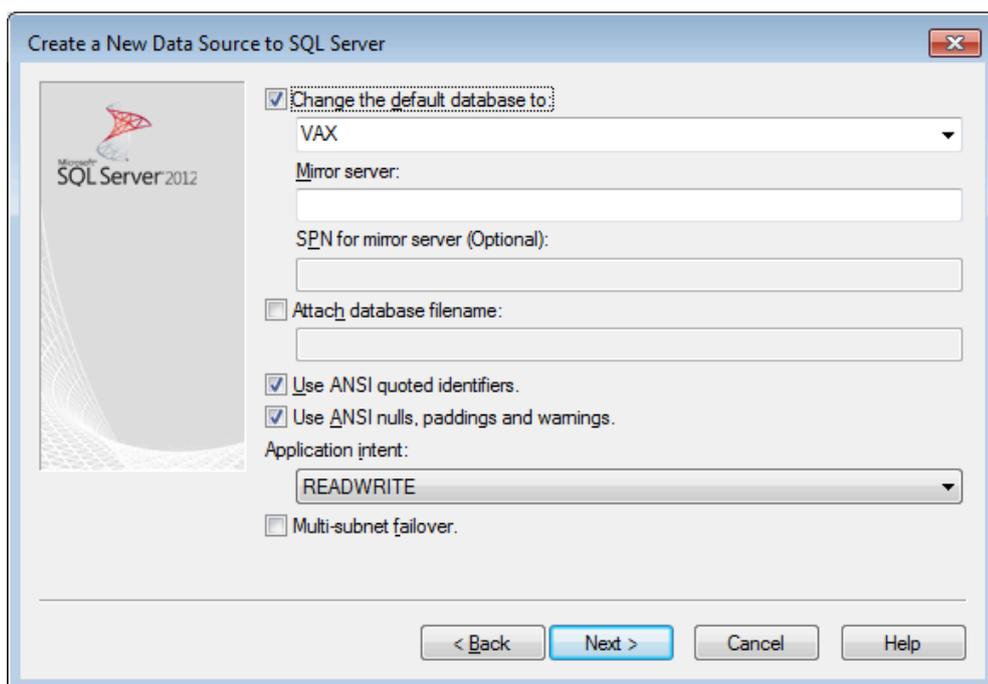
The name of this Panel may differ slightly depending on the version of Windows installed.

3. Once **Data Sources (ODBC)** is opened, click on the second tab named **System DSN**.
4. Click **Add**; a new window should appear. Select the latest version of **SQL server native client** and click **Finish**.
5. A new window will appear with 3 boxes to fill. The **Name** can be filled with "VAX", the **Description** can be blank, and the server will need to be in the format "servername\database instance".

For example "Vicon-PC\VAX"

Figure 35.1. Adding a New Data Source

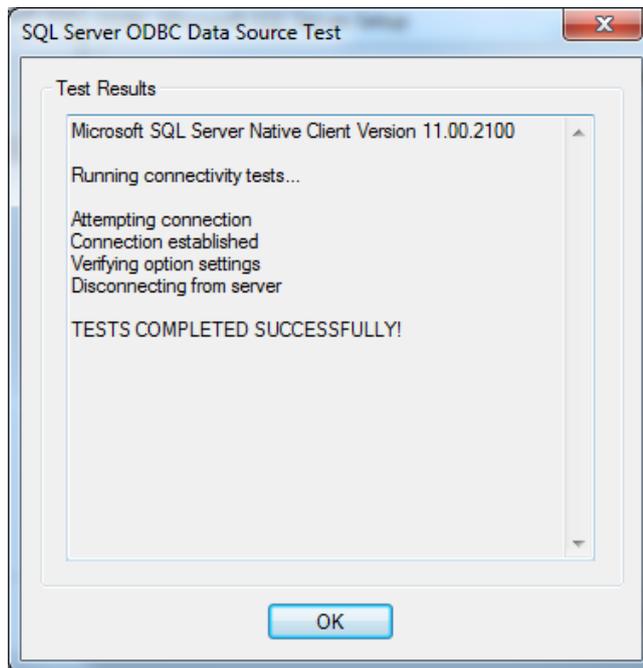
6. After clicking **Next**, two radio button options are presented; the first option **With Integrated Windows Authentication** will work in most circumstances unless using an external SQL server. **SPN** can be left blank. Press **Next**.
7. Select the check box **Change the Default databases to:** use the drop-down menu and select **VAX**. Click **Next**.

Figure 35.2. Default Database

8. The next window can be left as the default settings; click **Finish**.

- Click the **Test Data Source** button to ensure the settings are correct. You should see **TESTS COMPLETED SUCCESSFULLY!** Click **OK** and click **OK** again on the previous window.

Figure 35.3. Data Source Test Successful



- Click **OK** on the initial screen we started on to close the ODBC Data Source Tool.

We have now fully configured the reference to the Vicon Access Control database. We can now begin to configure the cardPresso software to obtain User information and pictures for printing purposes.

Configuring cardPresso Software to Access the Database View

In this section we will connect the cardPresso software to the custom database interface we have created in the section called “ Creating an ODBC Connection for cardPresso ”.

This chapter assumes the following:

- cardPresso Software is installed
- The reference to the custom database view has been created as outlined in the section called “ Creating an ODBC Connection for cardPresso ”
- In the cardPresso software you have selected a card template or have created one
- If you are having issues with installing or navigating cardPresso, please visit cardPresso.com and refer to their documentation

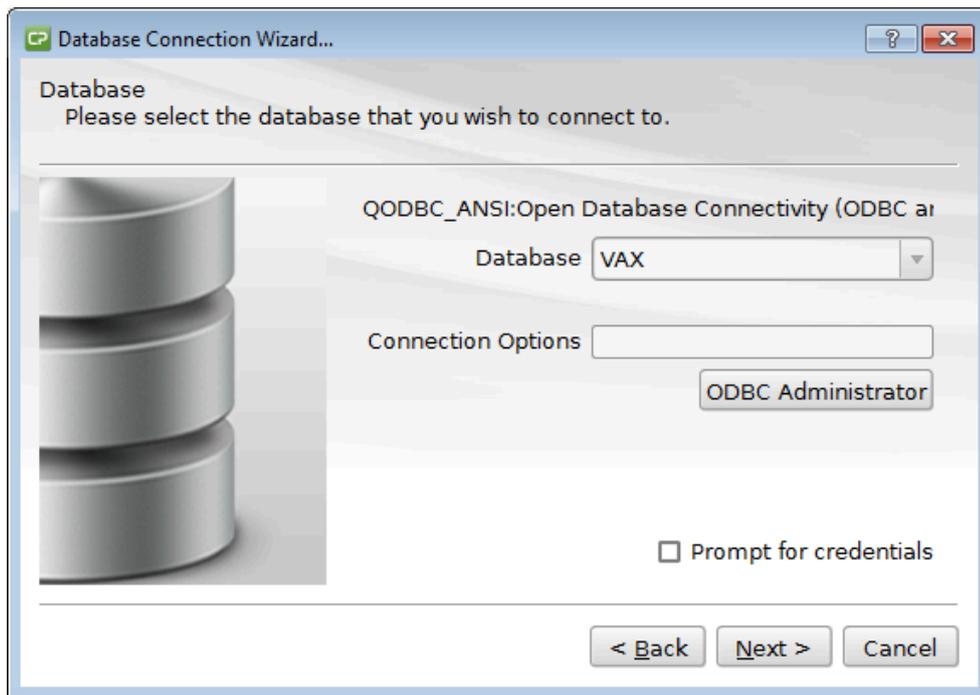
Using the cardPresso Database Connection Wizard

- Open the cardPresso software and select or create a template.
- On the top of the cardPresso software there is a button section for database operations.

Click the **Connect to Database** button, highlighted in the figure below:

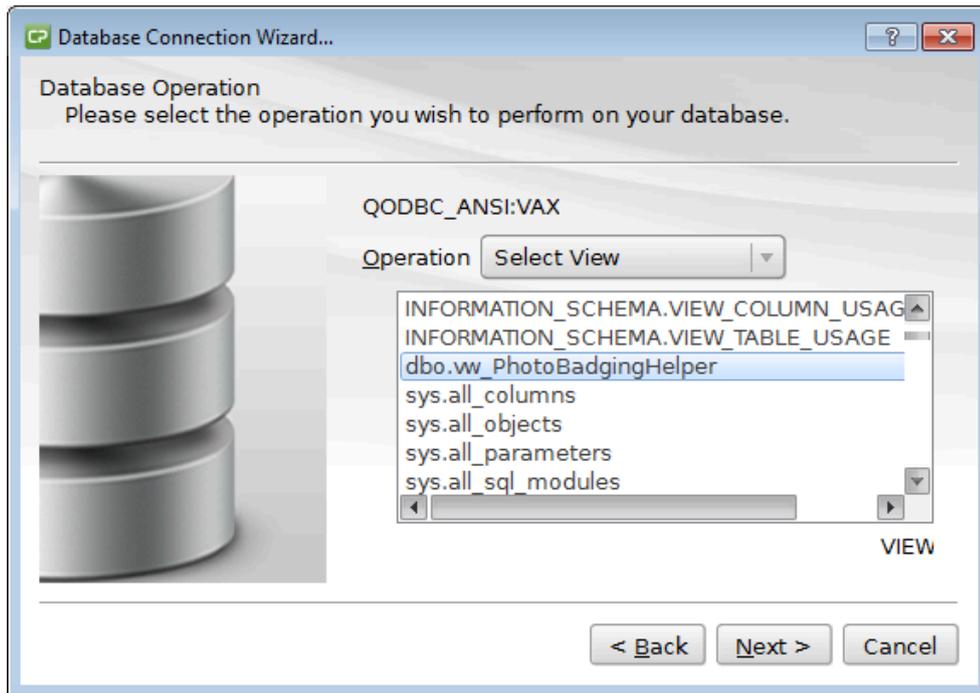
Figure 35.4. Database Connection Button

3. The cardPresso database connection wizard will now appear. Click **Open Database Connectivity (ODBC ANSI)** and click **N**ext.
4. Use the drop-down menu and select **VAX** (or the name of your database). Uncheck the **Prompt for Credentials** button and click **N**ext.

Figure 35.5. Database Connection Wizard

5. Change the drop-down menu beside **Operation** from **Select Table** to **Select View**.

Scroll to the view called **dbo.vw_photoBadgingHelper** (the view we created earlier). Select it and click **N**ext .

Figure 35.6. Database Connection Wizard: Select View

6. You should now see all the User fields. All are selected by default; de-select any you do not wish to import and click **Next**.
7. Click **Next** on the guide columns window.
8. In most cases the database filter text box can be left blank; click **Next**
9. This step will dictate how your Users are sorted; we recommend de-selecting **RecordID** and selecting the **UserID** checkbox.
10. Click **Finish** to complete the wizard. On the left hand side you'll see that the fields of the Users are now accessible and can be dragged and dropped into the card template.

You can also navigate through these records using the database navigation bar on the top, as pictured below:

Figure 35.7. cardPresso Record Navigation Bar

Adding the CardHolder Picture

This section will cover how to configure the cardPresso software to find the location of our stored pictures and reference them to the Users.

This section assumes the following:

- At least one User has a cardholder picture associated with their account within the Vicon Access Control web interface. For information about adding cardholder pictures, please see the section called “Taking Pictures with Vicon Access Control Web Interface”.
- cardPresso software has been configured and you are able to drag fields onto the card template and change records using the record navigator on the top of the page.

1. Open the cardPresso software; open your custom template or create a new one. Connect to the database as we did in the section called "Using the cardPresso Database Connection Wizard".
2. Ensure you are able to access the **Database Tab** on the right hand side of the software, including the various fields we have imported such as UserID, card number, etc.
3. Move your mouse over the **userid** field; click on the gray button with the 3 dots [...] (as pictured below). This will bring up the **userid Properties**.
4. Change the **Data Type** drop-down menu from **Integer Value** to **Indexed Image**. Click the rectangular "." button next to the drop-down menu to bring up the **Indexed Image Properties**.

Figure 35.8. cardPresso Index Image

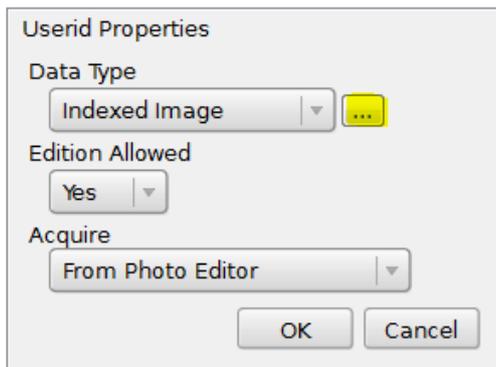
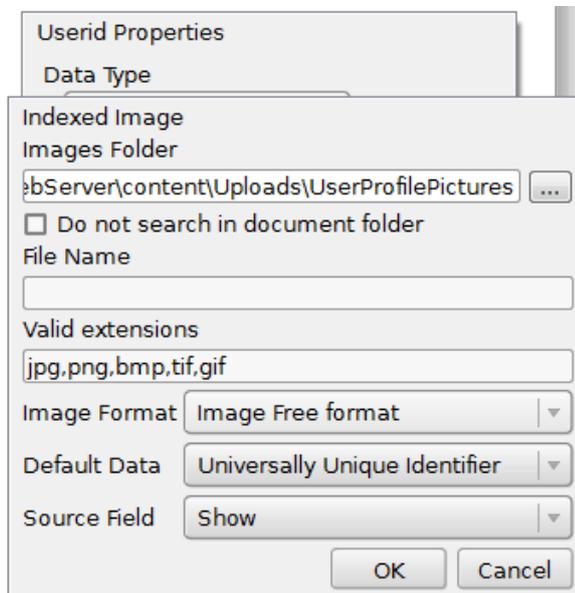


Figure 35.9. cardPresso Index Image Properties

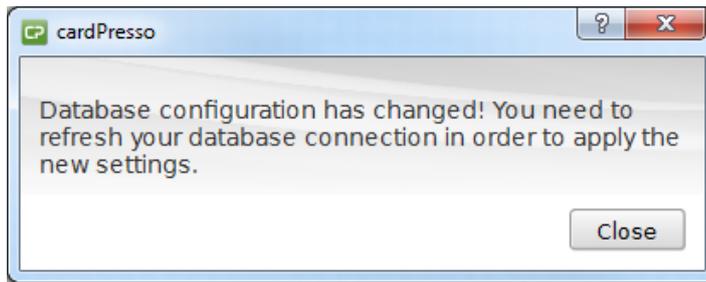


5. Change the **Images Folder** text box to "C:\Program Files (x86)\Vicon\VAX\WebServer\content\Uploads\UserProfilePictures".

Note

The installation directory may differ from the above example

6. Click **OK** to close that window; click **OK** again on the previous window. You will now be prompted that the database configuration has changed. Click the **Refresh Database** button on the database navigation bar.

Figure 35.10. Configuration Has Changed

7. After refreshing the database, we can now add the picturebox to the card template; on the left hand side is a button called **Database Image** pictured and highlighted below.

Figure 35.11. Add Image From Database

Click on the button and then again on the template to place the picture. Resize and move the picturebox as desired.

8. After clicking on the imagebox, you should see the source properties on the right hand side. It should look as follows:

Figure 35.12. Imagebox Source Properties

From Database ▼

Table
dbo.wv_PhotoBadgingHelper ▼

Column
@Userid ▼

Save with document
No ▼

Face Detection
No ▼

Open image editor
No ▼

We have finished configuring cardPresso, and successfully tested a template. Each time you reopen cardPresso you will need to reconnect to the database, however you won't need to redo any other steps mentioned in this guide. If you are having problems printing or working with card templates, please refer to cardPresso documentation. You can access the cardPresso help screen by pressing "F1" on any screen.

Taking Pictures with Vicon Access Control Web Interface

In this chapter we'll go through how to add images to a User through the Vicon Access Control Interface.

Note

A digital camera or equivalent device, such as a web-cam, will need to be connected to the computer to take pictures.

Warning

Google Chrome® is currently the only supported browser for the camera image capture feature; Chrome for Android is also supported.

1. Log into the Vicon Access Control web interface.
2. Navigate to the **Users** screen. Click the blue icon  (advanced settings) next to the User you'd like to add a picture to.
3. Click on the **Images** tab. Click the camera icon . Chrome browser will prompt you at the top of the page. You will need to click **Allow** to give Vicon Access Control access to your camera device.
4. You can also take the cardholder picture when creating new Users. After adding the User, refresh the database in the cardPresso software. You can use the **Last Record** button  to quickly select the last User added.

Assa Abloy® Aperio™ Lock Systems

This chapter covers the configuration and software/hardware requirements of using Assa Abloy Aperio Lock systems with Vicon 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.

Ensure you have the following items before proceeding to installation:

- Vicon 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

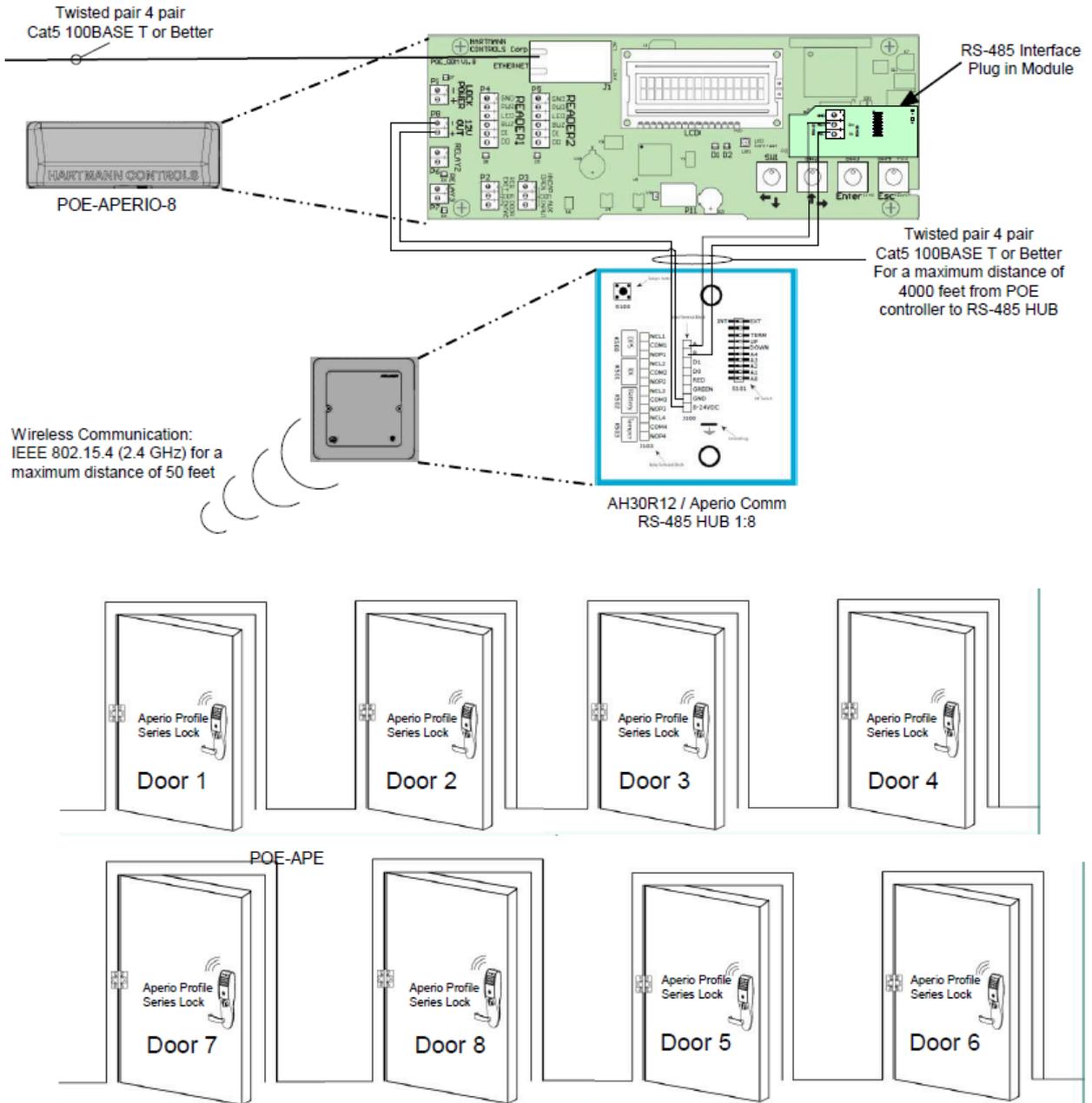
This section will cover the hardware aspect of connecting the Aperio Hub to the Vicon Aperio Panel. This section includes visual references and cable specifications.

The Vicon 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: Apero Programming Application

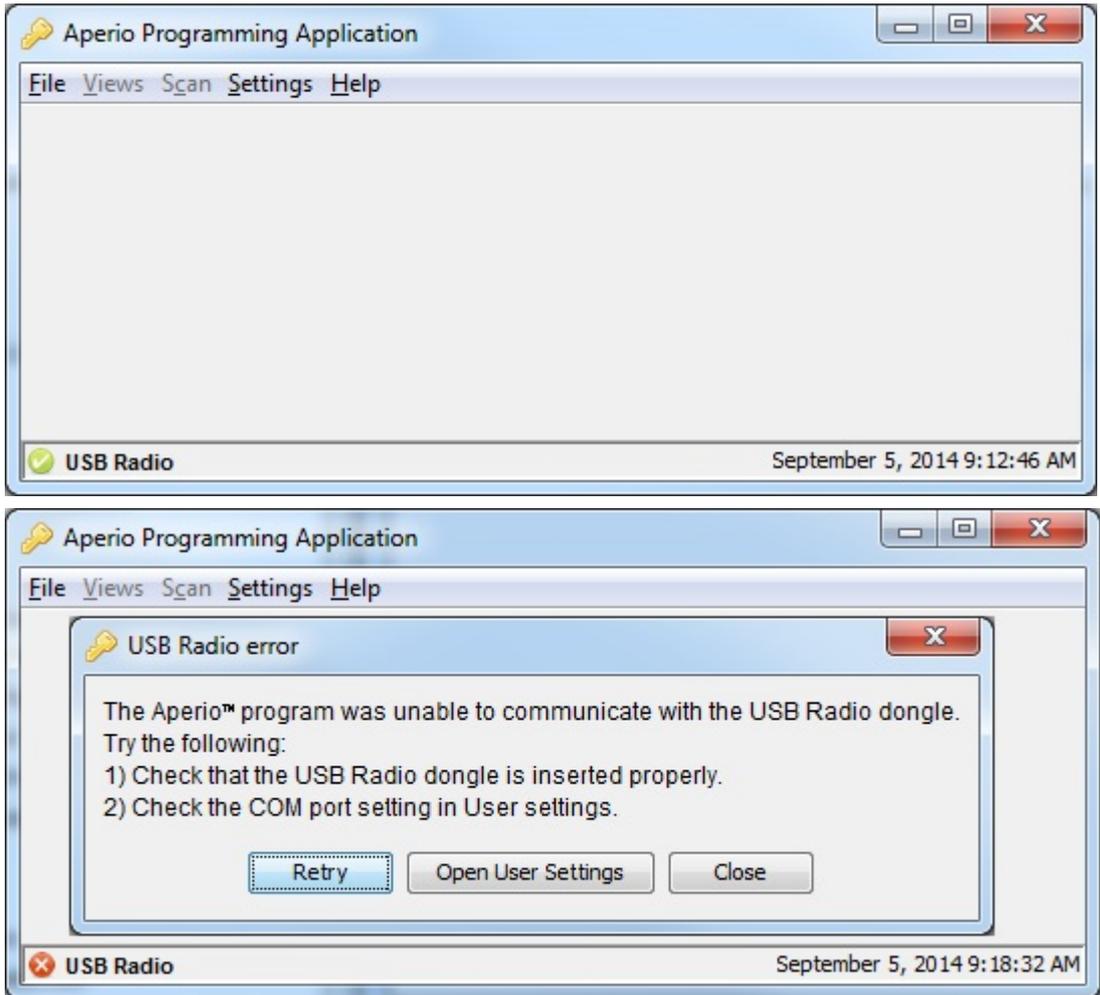
This section will cover the software aspects of setting up the Apero Hub to communicate with the Apero Locks via the Apero Programming Application. It is important to pair all of your locks with the Apero Hub prior to adding the Doors in Vicon Access Control.

1. On the laptop or PC you will be programming the Apero Hub, download the Apero Programming Application from your Apero kit or from http://www.assaabloyresources.com.au/downloads/eac/Apero_Common.zip
2. Unzip the Apero_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 Apero Programming Application).

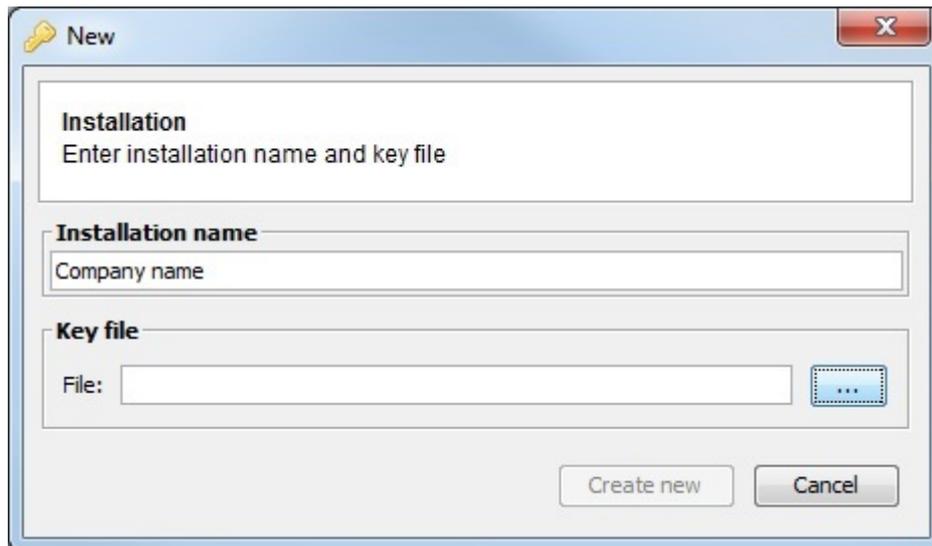
 **Note**

If you're having trouble installing the dongle driver or the Aperio programming Application, please contact your internal tech support or Assa Abloy support.

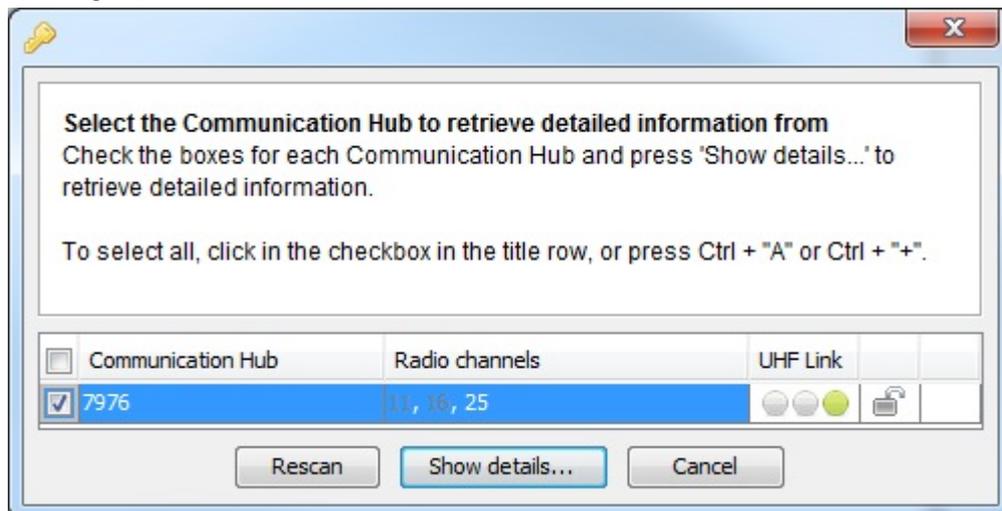
4. Ensure in Windows Device Manager that the "Tritech TriBee USB" is recognized and functioning.
5. Launch the Aperio Programming Application from your start menu. If the Tritech TriBee is installed correctly and plugged in, you'll see a green circle in the bottom left side of the application next to 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.

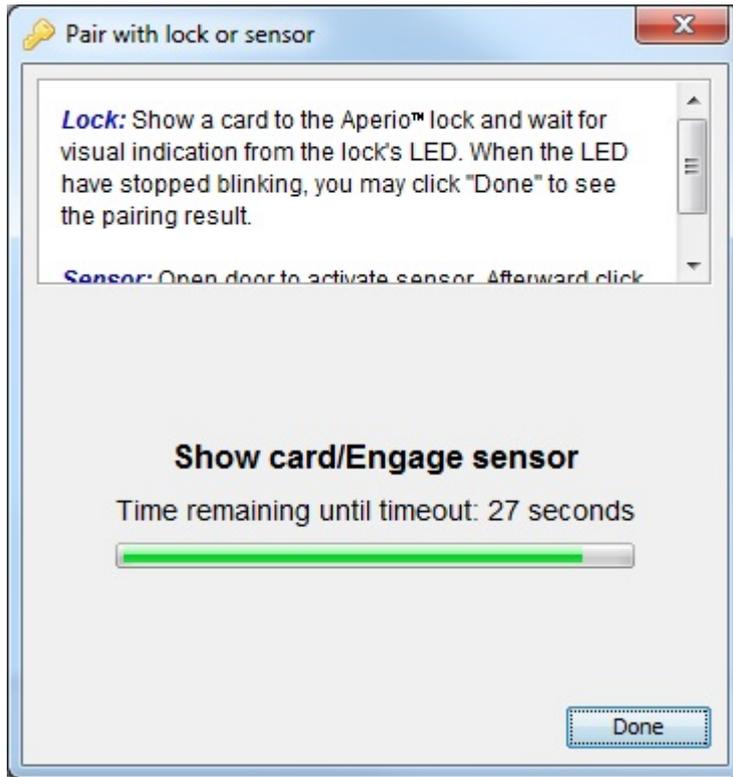


9. We can now begin pairing our locks with the communication hub. Right click on the communication hub you wish to configure. Click the communication hub sub menu on the hub you wish to pair locks with and click "pair with lock or sensor".

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".



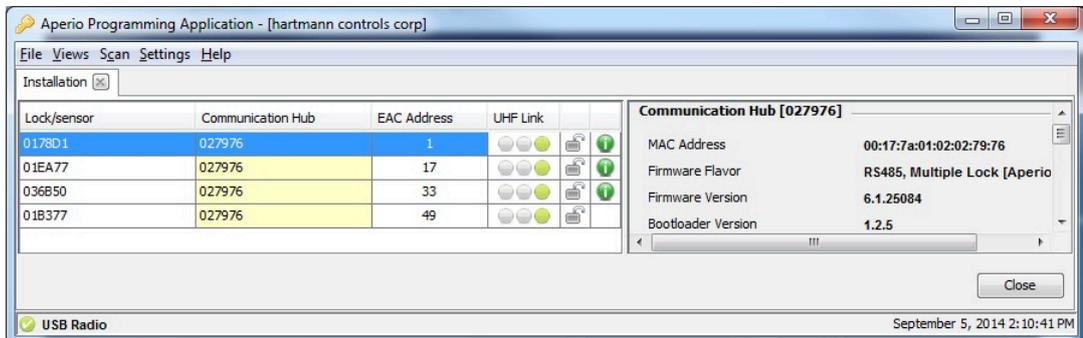
11. If the pairing is successful, you'll see "Communication Hub paired successfully to the following: XXXXXX" in the pair with lock or sensor window, where XXXXXX is the number printed on the back of the lock.

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 Vicon Access Control

Examples of 4 Locks synced within the Aperio Programming application



Software Setup: Vicon Access Control Aperio Panels and Doors

This section will cover the software aspect of adding Vicon Aperio Panels to Vicon Access Control and configuring Aperio Locks into Vicon Access Control 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 Vicon 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 Single-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 Vicon Access Control”.
 2. On the **Home Screen**, 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 Panel of any type to a Vicon Access Control server across the Internet. This section will also cover how to connect a web browsing client to the Vicon Access Control server across the Internet.

How Panels Communicate

The Vicon Access Control 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 Vicon Access Control 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 Vicon Access Control server. Once communication is established and the Panel is added in the Vicon Access Control 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.

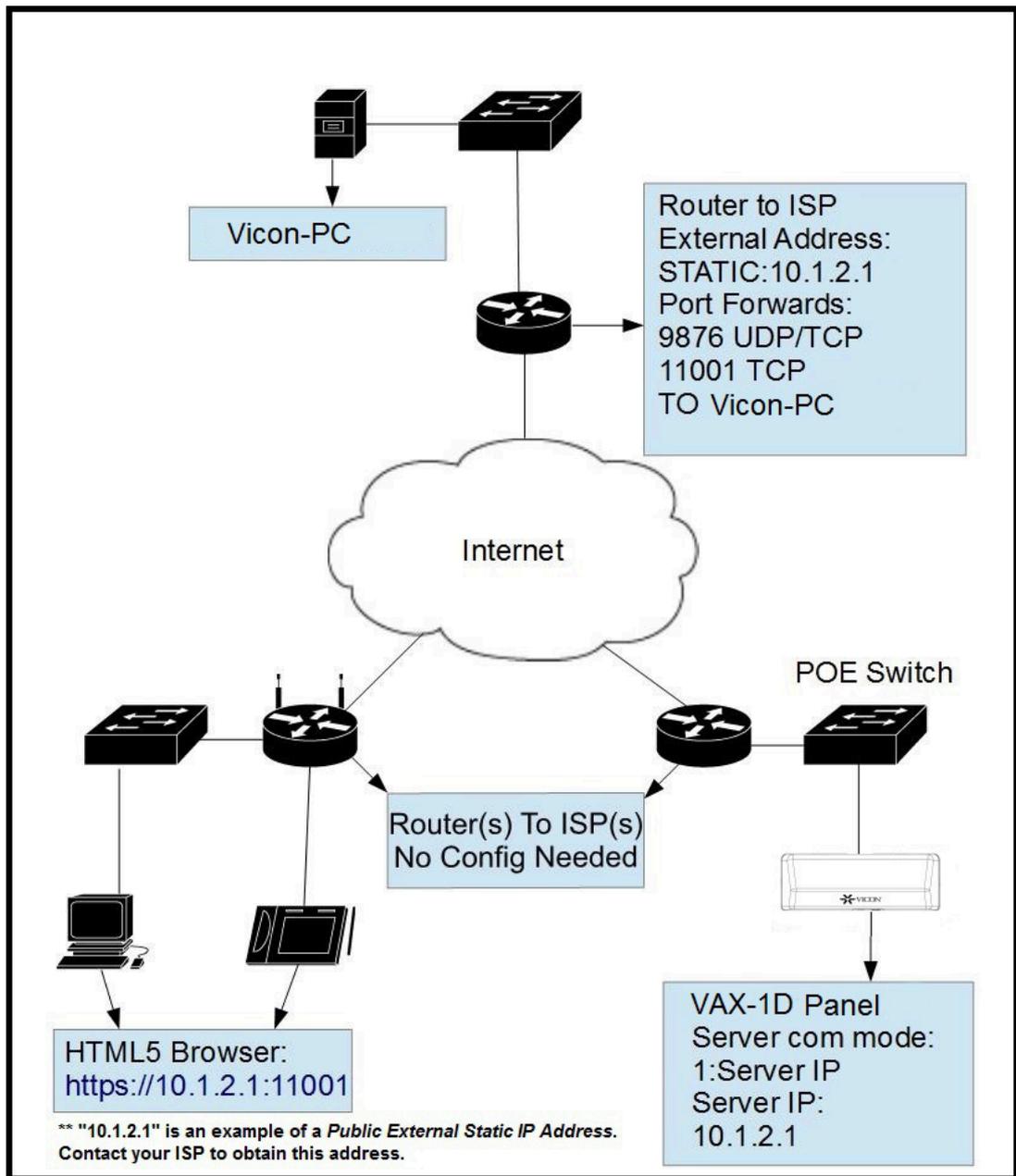
How Web Clients Communicate With Vicon Access Control

The Vicon Access Control 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 Vicon Access Control server will need to browse using the **Public Static IP Address** of the router connected to the private network the Vicon Access Control server resides on. The destination TCP port 11001 will need to be forwarded the internal address of the Vicon Access Control 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 Vicon Access Control 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.
- Vicon Access Control PC must have a static internal address.
- The main router on the site with the Vicon Access Control 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 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 that the clients and Panels reside on does 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 Vicon Access Control server needs 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 Vicon Access Control 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
Vicon Access Control Server	The computer (can also be a virtual machine) that the Vicon Access Control 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 Vicon Access Control server.

Example 1: Expansion Into Second Office. A business has expanded into a second office, and installs Vicon 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 Vicon Access Control server. They also make sure the Vicon Access Control 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 Vicon Access Control server.

Example 2: Dealer Hosted Vicon Access Control Server. A dealer/installer would like to host his clients Vicon Access Control 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 Vicon Access Control. This covers performing database back-ups and database restoration with SQL Command-Line.

Warning

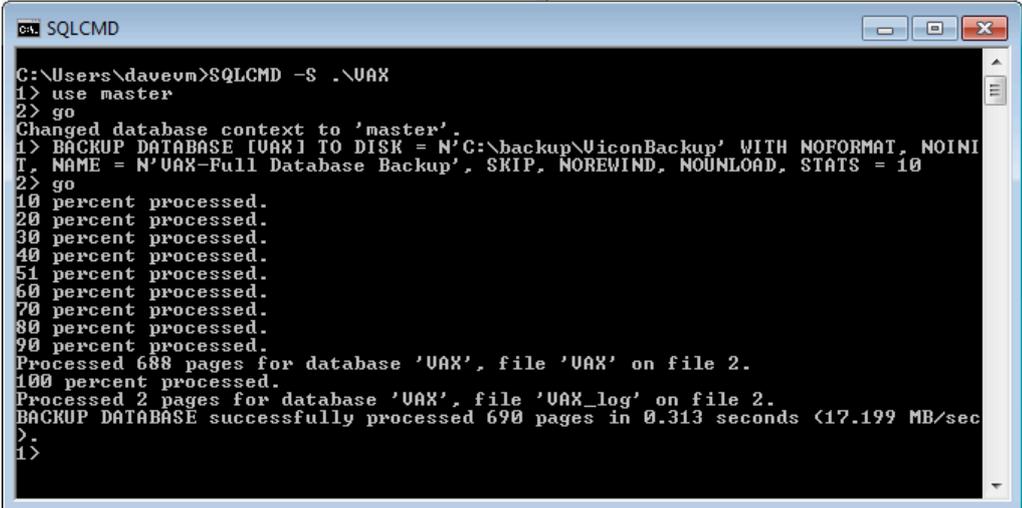
These instructions should only be performed by IT professionals and qualified Vicon installers. If you're having trouble performing Back-Ups and Restores with the System Manager UI, please give this document to your internal IT staff or contact Vicon. Please see Chapter 37, *Support*.

SQL Database Back-up

This section covers how to perform a database back-up via SQL Command-Line.

1. On the computer with Vicon Access Control 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\ViconBackup' 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



```
ca. SQLCMD
C:\Users\davevm>SQLCMD -S .\VAX
1> use master
2> go
Changed database context to 'master'.
1> BACKUP DATABASE [UAX] TO DISK = N'C:\backup\ViconBackup' WITH NOFORMAT, NOINI
T, NAME = N'UAX-Full Database Backup', SKIP, NOREWIND, NOUNLOAD, STATS = 10
2> go
10 percent processed.
20 percent processed.
30 percent processed.
40 percent processed.
51 percent processed.
60 percent processed.
70 percent processed.
80 percent processed.
90 percent processed.
Processed 688 pages for database 'UAX', file 'UAX' on file 2.
100 percent processed.
Processed 2 pages for database 'UAX', file 'UAX_log' on file 2.
BACKUP DATABASE successfully processed 690 pages in 0.313 seconds (17.199 MB/sec)
>
1>
```

SQL Database Restore

This section covers how to perform a database restore via SQL Command-Line.

1. Install Vicon Access Control on the computer that the database will be restored to. Ensure the version of Vicon Access Control 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:

"**Vicon Access Control_<dateofbackup>.prbak**" will need to be renamed to:

"**Vicon Access Control_<dateofbackup>.zip**".

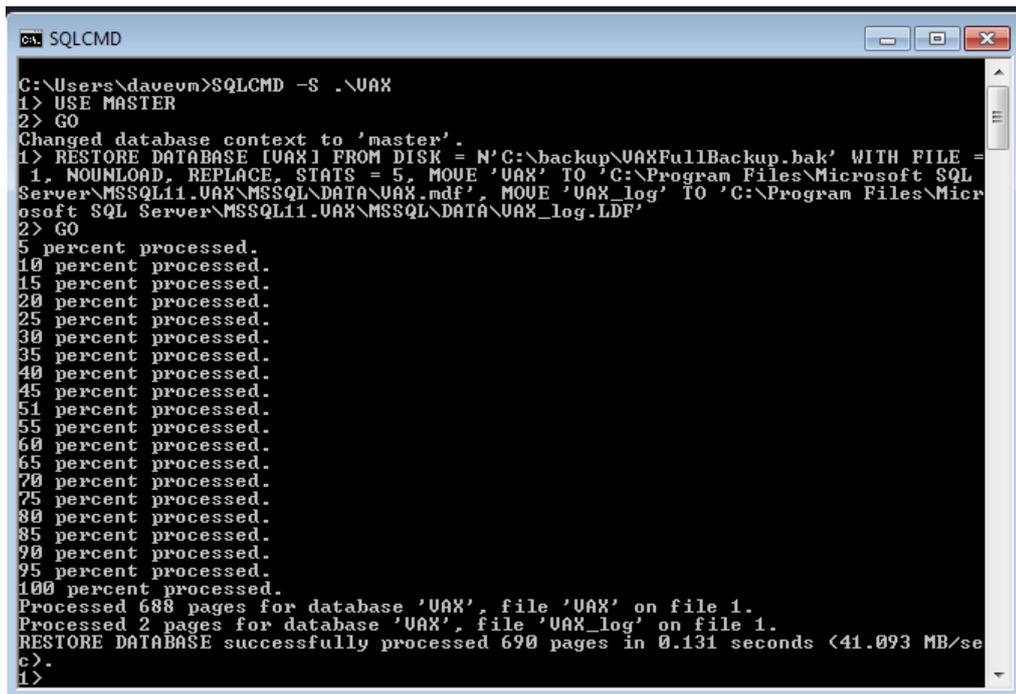
Extract the file and copy the file "**VAXFullBackup.bak**" to "**C:\backup**".

4. Stop the Vicon Access Control Web Service via System Monitor (see the section called "System Monitor"), or via System Management UI (see Chapter 5, *System Manager UI*).
5. On the computer with Vicon Access Control 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\VAXFullBackup.bak' WITH  
FILE = 1, NOUNLOAD, REPLACE, STATS = 5, MOVE 'VAX' TO 'C:\Program Files\Mi-  
crosoft 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 Vicon Access Control Web Service and login to confirm the backup was successful.

Figure 36.3. Command Prompt: Restore



```
C:\Users\daveum>SQLCMD -S .\UAX
1> USE MASTER
2> GO
Changed database context to 'master'.
1> RESTORE DATABASE [UAX] FROM DISK = N'C:\backup\UAXFullBackup.bak' WITH FILE =
1, NOUNLOAD, REPLACE, STATS = 5, MOVE 'UAX' TO 'C:\Program Files\Microsoft SQL
Server\MSSQL11.UAX\MSSQL\DATA\UAX.mdf', MOVE 'UAX_log' TO 'C:\Program Files\Micr
osoft SQL Server\MSSQL11.UAX\MSSQL\DATA\UAX_log.LDF'
2> GO
5 percent processed.
10 percent processed.
15 percent processed.
20 percent processed.
25 percent processed.
30 percent processed.
35 percent processed.
40 percent processed.
45 percent processed.
51 percent processed.
55 percent processed.
60 percent processed.
65 percent processed.
70 percent processed.
75 percent processed.
80 percent processed.
85 percent processed.
90 percent processed.
95 percent processed.
100 percent processed.
Processed 688 pages for database 'UAX', file 'UAX' on file 1.
Processed 2 pages for database 'UAX', file 'UAX_log' on file 1.
RESTORE DATABASE successfully processed 690 pages in 0.131 seconds <41.093 MB/se
c>.
1>
```

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 Vicon Access Control 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 Vicon Access Control installation using the following steps:

1. Browse to the WebServer folder of your Vicon Access Control installation directory (usually located in "C:\Program Files (x86)\Vicon\VAX\WebServer").
2. Open the file named "ProtectorNet.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 Vicon Access Control is currently using.

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 API's 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 provided 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 than the REST API and its 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 2.8 or newer.

If you have an existing system, you can access it with the following:

`https://NameOrIPOFServer: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.Vicon: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.

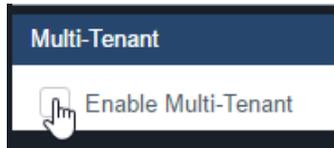
Warning

Enabling multi-tenant cannot be reversed. Carefully consider this before enabling this feature.

Enabling Multi-Tenant Mode

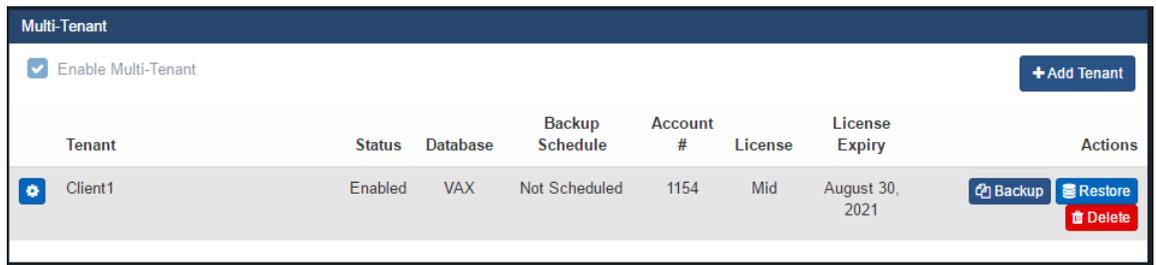
Multi-tenant mode is enabled from the system manager UI. DNS A records and pointers should be configured prior to enabling multi-tenant. Use the following steps to enable multi-tenant:

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. An informational prompt will appear. Read it and click OK. Multi-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 36.4. List of Tenants

A screenshot of a web interface titled "Multi-Tenant". At the top left, there is a checked checkbox labeled "Enable Multi-Tenant". At the top right, there is a blue button with a plus sign and the text "+ Add Tenant". Below this is a table with the following columns: Tenant, Status, Database, Backup Schedule, Account #, License, License Expiry, and Actions. The table contains one row for a tenant named "Client1".

Tenant	Status	Database	Backup Schedule	Account #	License	License Expiry	Actions
 Client1	Enabled	VAX	Not Scheduled	1154	Mid	August 30, 2021	 Backup  Restore  Delete

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.

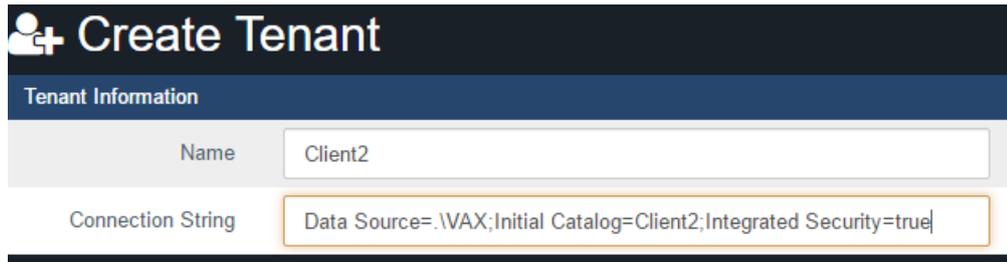
Example 36.1. Database Connection String:

```
Data Source=VAXServer\VAX; Initial Catalog=Client1;Integrated Security=true
```

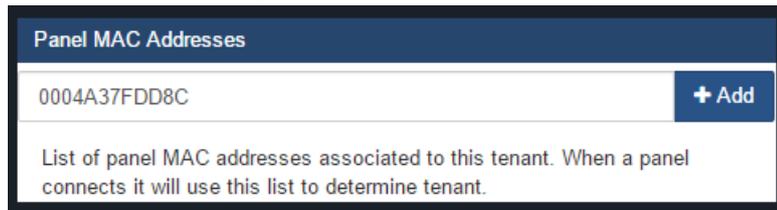
In the above example, **VAXServer** is the name of the computer the database will reside on. **VAX** is the name of the database instance the database will reside on. This can be the same for all tenants. **Client1** is the name of the database that will be created for the tenant. This must be unique.

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 Vicon Access Control 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 section called “Restoring Your VAX Database”.

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.vicon-security.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.

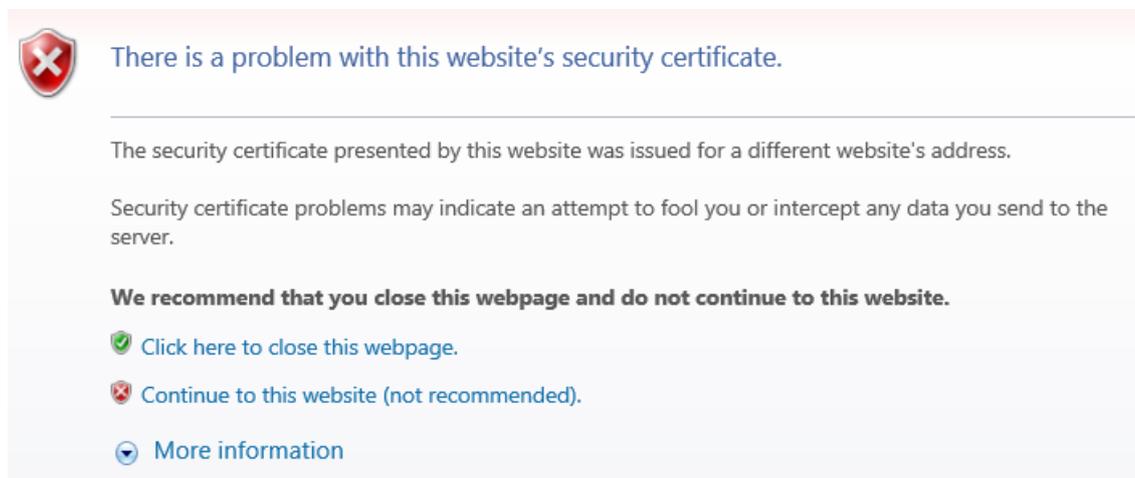
SSL Certificate Information

This section will cover information about SSL certificates in VAX.

SSL certificates are used by VAX to encrypt web traffic between the VAX server and any client connections (in most cases a web browser). This encryption is not optional.

By default, VAX will generate a self-signed SSL certificate using a sha256 signature algorithm with a 4096 RSA key. Because the certificate is self-signed (not verified by third-party), most web browsers will show an SSL error when browsing to the VAX web interface. It is possible to register a domain and obtain an SSL certificate from a third-party certificate authority.

Figure 36.5. Internet Explorer Self-signed Certificate Warning

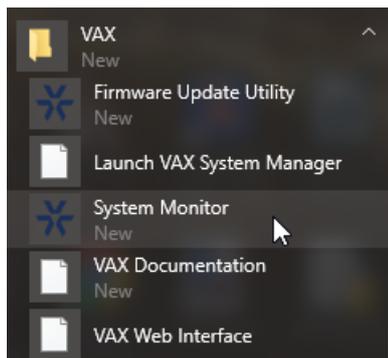


In most cases, administrators of VAX can be advised to click "Advanced" followed by Proceed to <computer name or localhost>". In Internet Explorer you would click "Continue to this website". You can also import the certificate into the Trusted Root Certification Authorities in order to permanently bypass the certificate error on any clients connecting to VAX. The URL will still be red but you will not need to bypass the certificate warnings.

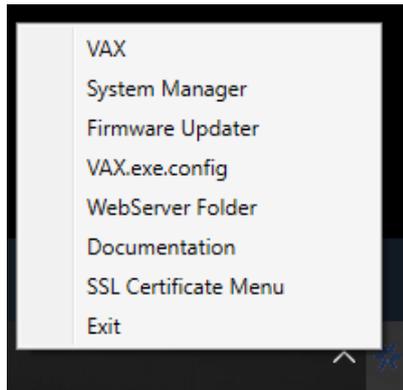
Managing SSL Certificates

This section will outline how to regenerate the self-signed SSL certificate and how to import your own SSL certificate obtained from a third-party.

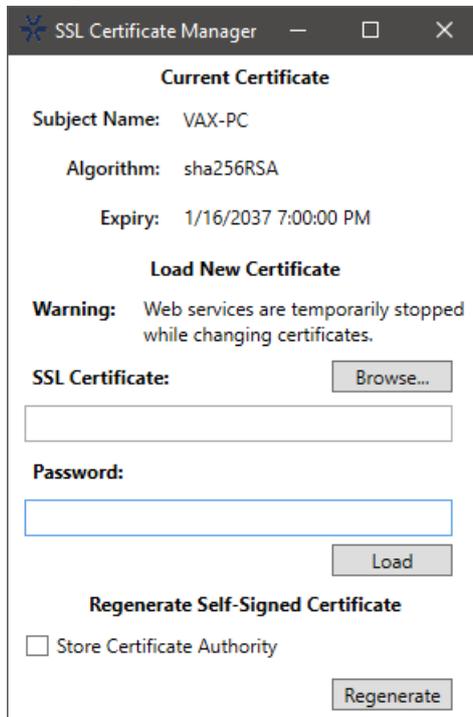
1. On the computer the VAX software is installed on, run the System Monitor from the VAX folder in the Windows Start menu.



2. The VAX System Monitor icon will appear in the system tray by the clock. Right click on the system monitor icon. If it does not appear, click the up arrow by the clock. This will reveal hidden icons.



3. Select SSL Certificate menu from the context menu. A small window will open (it will be minimized by default; select it from your task bar).
4. The SSL Certificate Manager will allow you to add an SSL certificate or regenerate the existing self-signed SSL certificate.



Regenerate Self-Signed Certificate

If the computer name changed or you wish to store the certificate authority, you can regenerate the self-signed certificate.

Tip

Storing the certificate authority will bypass certificate errors when browsing to the VAX interface from the same computer the server software is hosted on when accessed via computer name.



1. Access the SSL Certificate Manager as outlined in the above section.

2. If needed, check the Store Certificate Authority checkbox.
3. Click the Regenerate button. The VAX web services are temporarily stopped while the new SSL certificate is generated.

Importing Your Own SSL Certificate

If required or preferred, you can import your own SSL certificate generated by a Certificate Authority or purchased online through a company that issues SSL certificates. You will generally need a registered domain and proof of purchase to obtain an SSL certificate signed by a certificate authority. Most certificates will have a cost associated with them, usually on a yearly basis.

Use the following steps after you've obtained the SSL certificate files (*.pfx or *.cer):

1. The private key needs to be embedded within the certificate being loading via SSL Certificate Manager. When you view the certificate, it should say 'You have a private key corresponding to this certificate'.
2. Import the SSL certificate private key into the personal certificate directory using the Windows Certificates MMC snap-in.
3. Access the SSL Certificate Manager as outlined in the above section.
4. Click the Browse button. You will be prompted to select a file.
5. Select your certificate file (*.pfx or *.cer) and click Open.
6. If required, enter a password for the certificate.
7. Click the Load button. The selected certificate will now be loaded and bound to the appropriate ports. The VAX web services are temporarily stopped while the new SSL certificate is loaded.

Performing Data Migration with Data Migrator

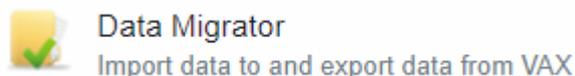
This section covers importing and exporting data in VAX between Partitions and/or systems.

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 **Home Screen**, scroll down to the section titled **System**; click on the **Data Migrator** icon (pictured below)

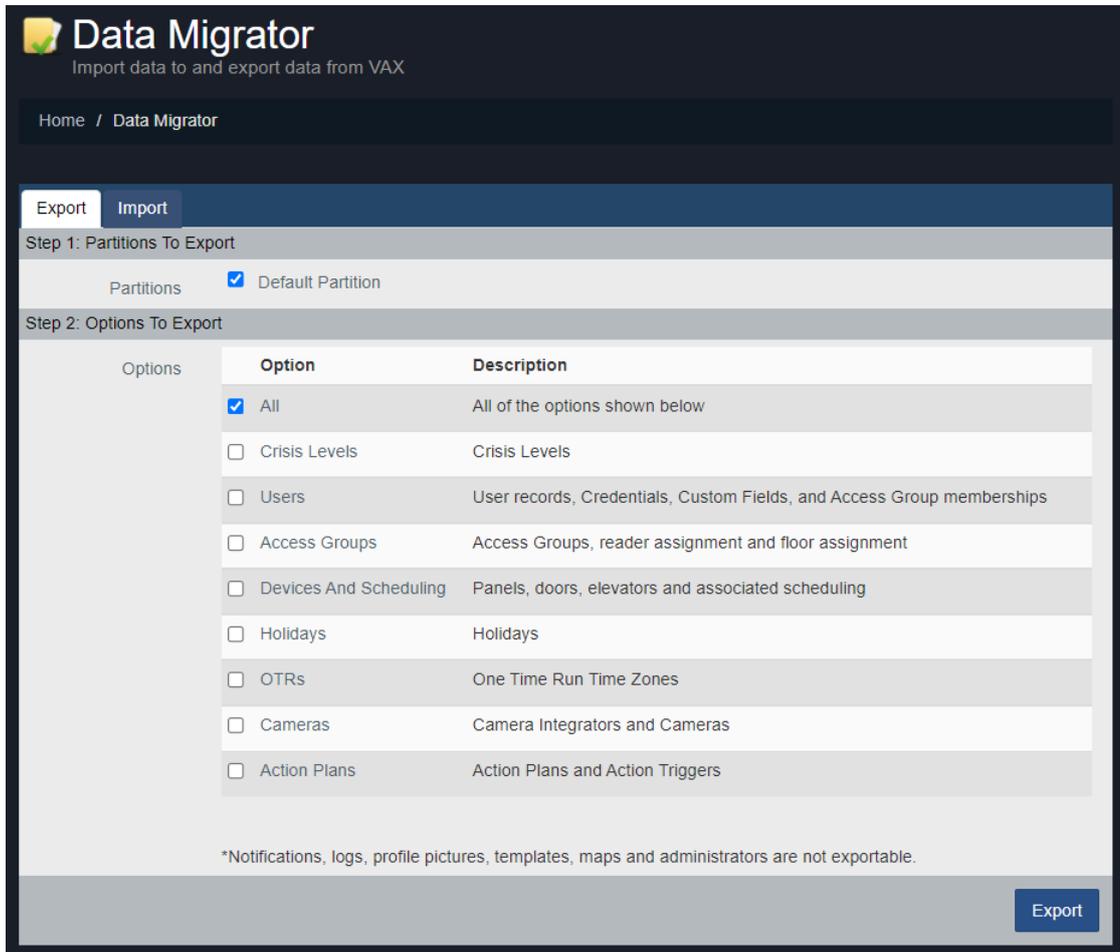
Figure 36.6. Data Migrator Icon



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 36.7. Data Migrator: Options To Export



Importing Partition Data

This section covers how to perform an *import* of Partition data via data migrator.

Warning

We recommend doing a backup of your Vicon Access Control database prior to importing data. For more information about backing up your database, please see the section called “Backing up your Vicon Access Control Database”.

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**, scroll down to the section titled **System**; click on the **Data Migrator** icon (pictured below)

Figure 36.8. 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 36.9. Data Migrator: Import

The screenshot shows the 'Import' tab of the Data Migrator interface. It is divided into four steps:

- Step 1: Select a File**: A file named 'VAX-Export-2022-03-03T16_01_51.prData' is selected. A 'Choose File' button and a 'Clear File' button are visible.
- Step 2: Verify Import Content**: A table displays file details:

File Name	VAX-Export-2022-03-03T16_01_51.prData
Customer	vax demo system
From Version	2.10.26.27388
Created On	2022-03-03 21:01:44
- Step 3: Setup Partition Mapping**: A table for mapping data from the source to the target:

Import	From	To
<input checked="" type="checkbox"/>	Default Partition	New Partition (dropdown) Demo System (text input)
- Step 4: Select Data To Import**: A list of data categories with checkboxes and radio buttons for selection:

Option	Description
<input checked="" type="checkbox"/> All	All of the options shown below
<input type="checkbox"/> Crisis Levels	Crisis Levels
<input type="checkbox"/> Users	User records, Credentials, Custom Fields, and Access Group memberships
Conflict Strategy: <input checked="" type="radio"/> Duplicate <input type="radio"/> Credentials <input type="radio"/> Name <input type="radio"/> Both	
Skip Unprivileged Users: <input type="checkbox"/>	
<input type="checkbox"/> Access Groups	Access Groups, reader assignment and floor assignment
Skip Empty APGs: <input type="checkbox"/>	
<input type="checkbox"/> Devices And Scheduling	Panels, doors, elevators and associated scheduling
<input type="checkbox"/> Holidays	Holidays
<input type="checkbox"/> OTRs	One Time Run Time Zones
<input type="checkbox"/> Cameras	Camera Integrators and Cameras
<input type="checkbox"/> Action Plans	Action Plans and Action Triggers

An 'Import' button is located at the bottom right of the interface.

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.

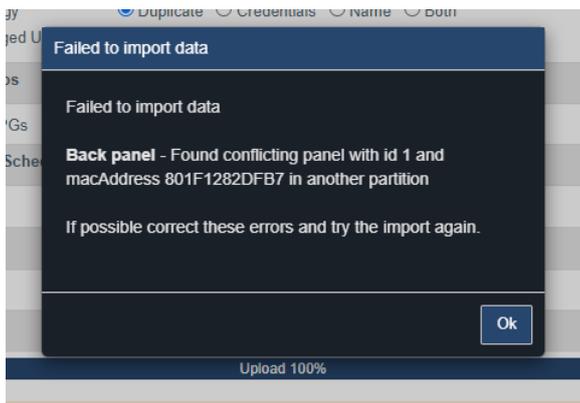
Strategy	Brief Explanation
Name	Use existing user if first name and last name match exactly
Both	Use existing user if all credentials and name match imported user.

Data Migrator Errors

This section covers some possible errors you may encounter when importing with the Data Migrator.

Because data migrator can be used to import large amounts of data and potentially complex relationships between data, you may encounter errors when doing imports.

Figure 36.10. Data Migrator: Error



When a critical error happens (such as a panel with the same mac address already existing in a system), the importer will skip that specific item and continue to other items in the import. Any errors will be displayed when the import is finished along with a reason for why the specific item wasn't imported. In most cases, you can make a corrective action and retry the import. You will see more errors than your first attempt because any items successfully imported will now create.

Migration Example: Moving a Panel Between Partitions on the Same VAX System

This section will cover a specific use case for the Data Migrator tool.

A building has 2 panels currently under the same Partition which covers a front and back entrance. The building owner no longer needs as much space and splits the building into 2 sections. The owner will want to keep using the existing front entrance panel but wants the back panel to be managed by a tenant moving into the back half of the building. Rather than delete the panel and readd the panel to a new Partition, the owner wants to move the panel to a new Partition so he does not have to reconfigure input/output settings and door settings. Here is how the owner can accomplish this goal:

1. Perform a database backup. For more information about backing up your database, please see the section called "Backing up your Vicon Access Control Database".
2. Access your VAX system through your HTML5 browser of choice.
3. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
4. On the Home Screen, scroll down to the section titled **System**; click on the Data Migrator icon.
5. On the Export tab of the Data Migrator screen, select the Partition containing the panels you wish to move.

6. Under the Options To Export section, select the checkbox next to Devices And Scheduling.
7. Click Export and save the .prData file somewhere safe and accessible.
8. Navigate within the VAX web interface to Panels under the Hardware section on the Home Screen.
9. Delete the panel you wish to migrate (we delete the panel we want to import, so that the import will recreate them)
10. Navigate within the VAX web interface back to Data Migrator under the System section on the Home Screen.
11. On the Import tab of the Data Migrator screen, click the Choose File button and select the .PRData file you exported earlier.
12. Click Parse.
13. In the Setup Partition Mapping section, select the Import checkbox and either keep the To dropdown menu as New Partition and fill in a name for the new Partition or select a specific Partition that already exists.
14. Under the Select Data To Import section, select the checkbox next to Devices And Scheduling.
15. Click Import. After a few moments, you will get an error because one or more of the panels in the export already exists, but the panel you deleted will be successfully imported into the new Partition along with all its settings and schedules.

Chapter 37. Support

Vicon world class technical support is available to assist with any installation related issues you may have.

Website

Vicon offers a number of technical guides and resources via our website: <http://www.vicon-security.com/>

Email

Email support is available through our website at <https://vicon-security.zendesk.com/hc/en-us/requests/new> . Please allow 24 - 48 business hours for responses.

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:

- **Within the US:** 1-800-348-4266
- **Outside the US and Europe:** 1-631-952-2288
- **UK:** +44 1489 566330

Customers requesting technical support are required to verify their status by providing a customer ID number in order to be passed through to the technical support queue. Requests for support from other sources will be directed to their dealer/integrator for technical support.

Appendix A.

Panel Model Reference

Table A.1. Panel Model Reference

Model	Max Doors	Max Readers	Motion REX	Brief Explanation
VAX-1D	1	2	No	Single-Door controller with PoE Power
VAX-1D-REX	1	1	Yes	Single-Door controller with PoE Power and Integrated Motion
VAX-2D	2	2	No	Two-Door controller with PoE power
VAX-2D-REX	2	2	Yes	Two-Door controller with PoE Power and Integrated Motion
VAX-MDK	1-8*	1-8*	No	1-8 door controller, Traditional style 12VDC powered mounted in steel enclosure. Uses master controller and VAX-EXP-2D two door expansion modules. *Can also be configured to communicate to up to 8 EXP8 for general purpose input/output.
VAX-APERIO-8	8	8	No	ASSA ABLOY Aperio master controller capable of controlling up to 8 Aperio devices via 1 - 8 Aperio Hubs
VAX-ELV-STR	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.
EXP8	N/A	0	N/A	Daughter-boards that increase the amount of Inputs/Outputs or Elevator floors when attached to VAX-IO or VAX-ELV systems.
VAX-EXP-2D	2	2	N/A	Daughter-boards that increase the amount of Inputs/Outputs and reader ports when attached to VAX-MDK systems.

* Requires appropriate quantity of EXP8 or VAX-EXP-2D modules

Visual Guides

This chapter contains examples of wiring diagrams and visual hardware information. For additional wiring diagrams for systems such as mag-locks, Fire Panels, or interacting with other external systems, please check the 'Technical Diagrams' folder on your Vicon Access Control installation media, or contact Vicon.

Figure A.1. Alarm Panel Interface

Interfacing with a Security Panel (DSC) Single Door



Programming of VAX

1. Go to Home – Hardware – Door Panels. Locate the panel the alarm is connected to and click the blue button (advanced settings).
2. Select the I/O tab. Click on input 4 and change the function drop down menu to "External Alarm Status". Click Save.
3. On the same screen, click on Relay 3 and change the function drop-down menu to "Alarm Interface". Click Save.
4. Go to Home – Hardware - Doors. Locate the door attached to the alarm panel and click the blue button.
5. Click the Reader 1 Tab. 6. Scroll down to "Triple Swipe " and click on the "Enabled" checkbox and choose from the "Triple Swipe Action" dropdown "Toggle Alarm Interface". Click "Save Reader 1".
7. Go to Home - Users. Click the blue button on the user that will have the ability to arm and disarm the security system. 8. Enable both check boxes for "Triple swipe" and "Disengage Alarm" on the user. 9. Update panels and test.

Programming of Alarm Panel

1. Program input as momentary Arm/Disarm
2. Program programmable output as system status

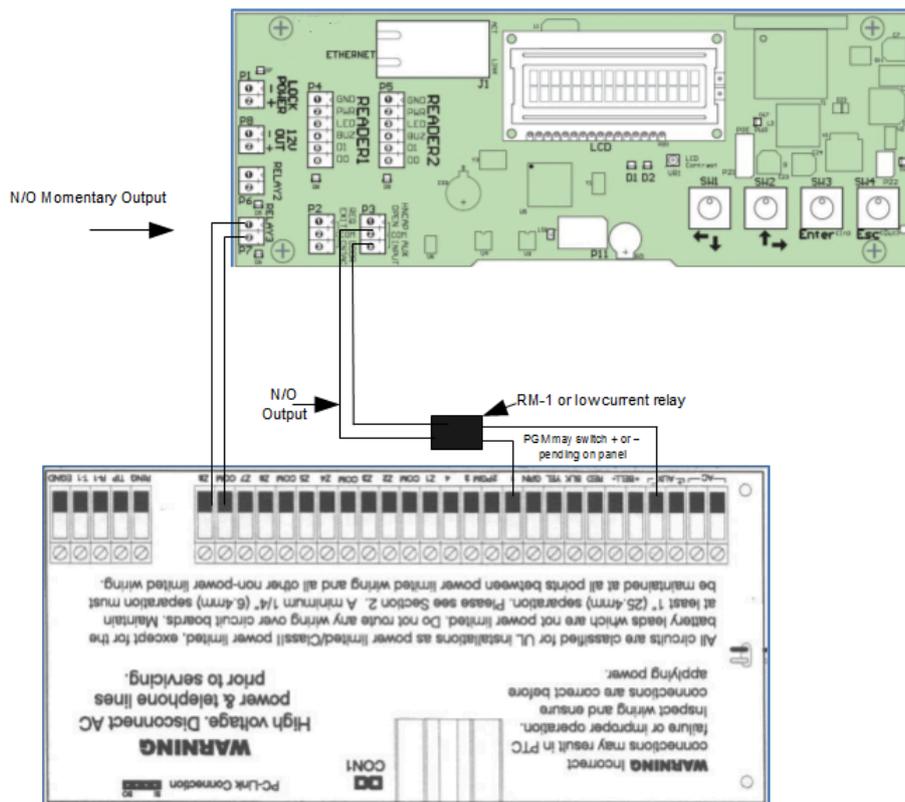


Figure A.2. VAX-1D Door Strike Typical

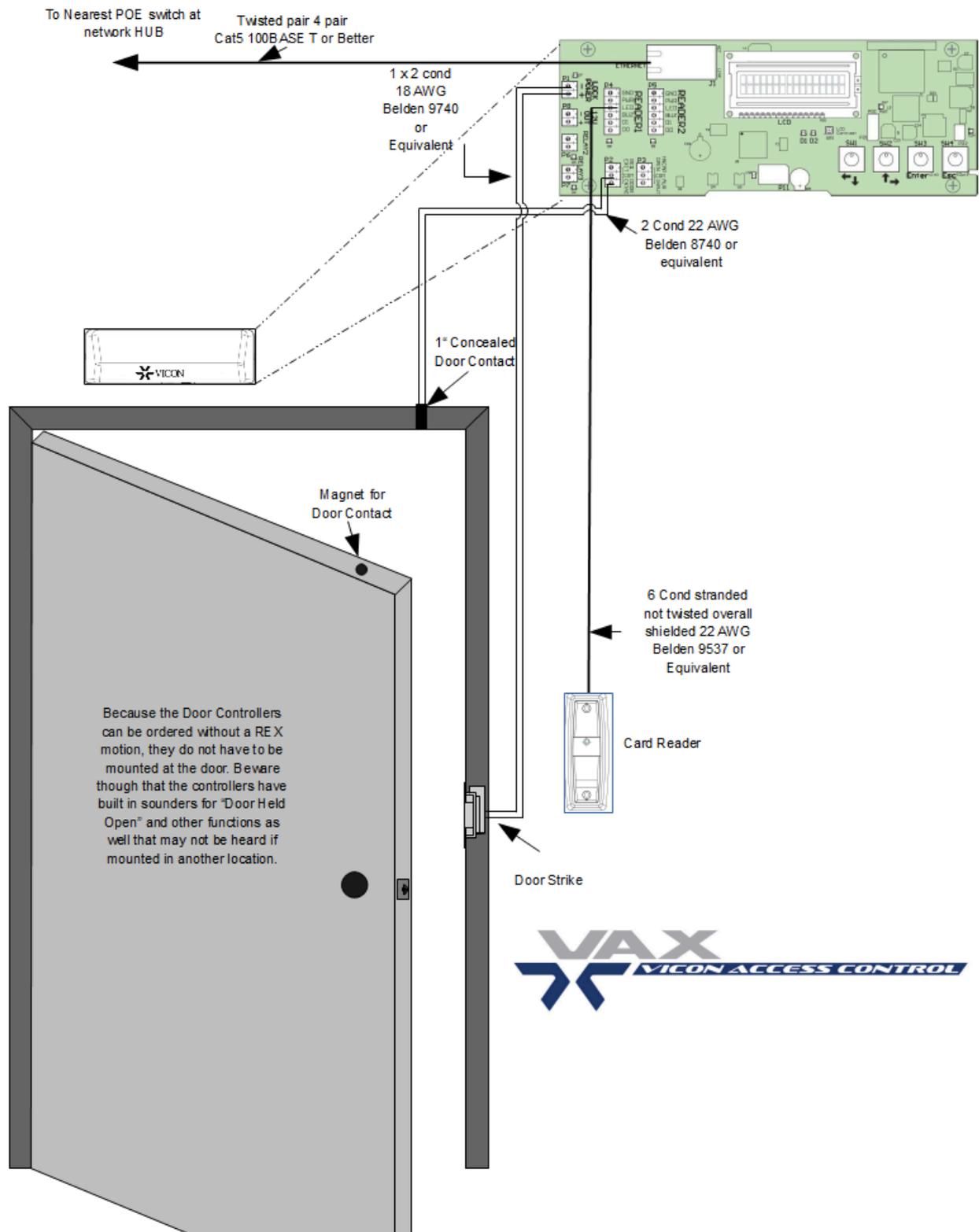


Figure A.3. VAX-1D with Handicap Operator

Programming instructions:

1. Go to Home – Hardware – Door Panels.
2. Find the panel that the door operator will be interfaced with and click on the blue button (advanced settings).
3. Go to the "I/O" tab and insure input 3 function drop-down menu is set to "Door Opener to Exit".
4. On the same page, insure input 4 function drop-down menu is set to "Door Opener Require Card" and click "save".
5. On the same page, insure output 2 function drop down menu is set to "Door Opener" and click "save".
6. Go to Home – Hardware – Doors. Choose the door that the door operator will be interfaced with and click on the blue button. Click on the options tab. Ensure under "Automatic Opener" the check-box "enabled" is checked and click "save".
7. Go to Home/Users. Other options are also configurable.
8. Click on the "Update Panels" Icon at the top right.

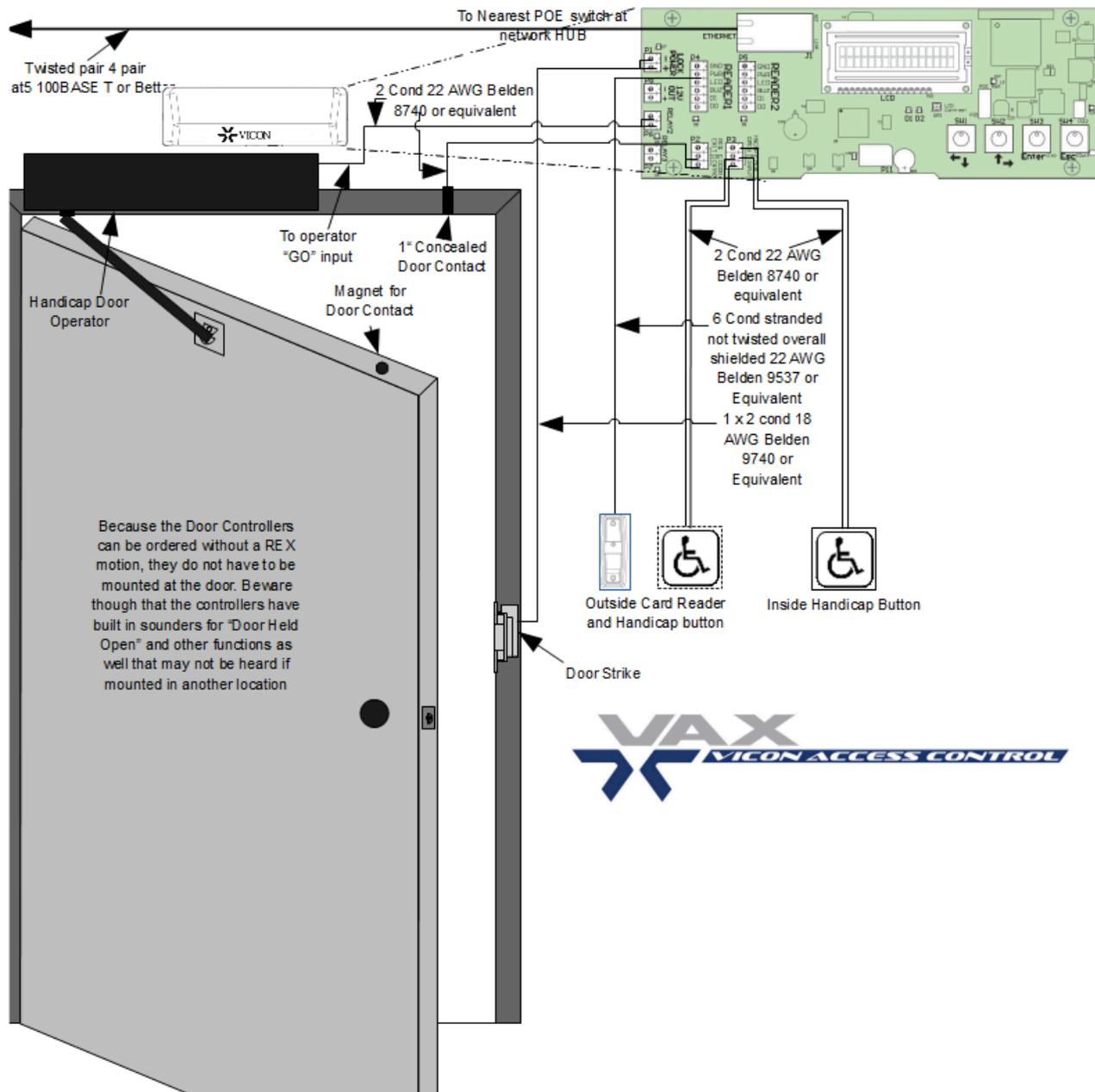


Figure A.4. Installation Example

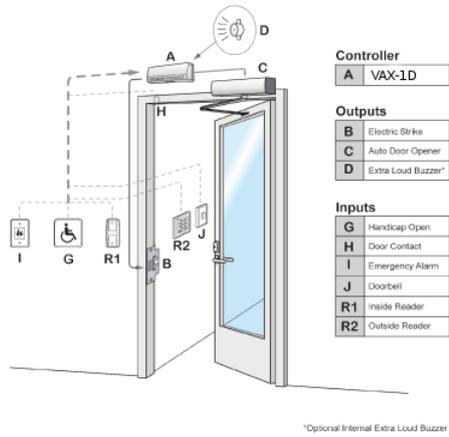


Figure A.5. Single-Door Typical Installation (with motion, single Reader, Door contact and auto opener)

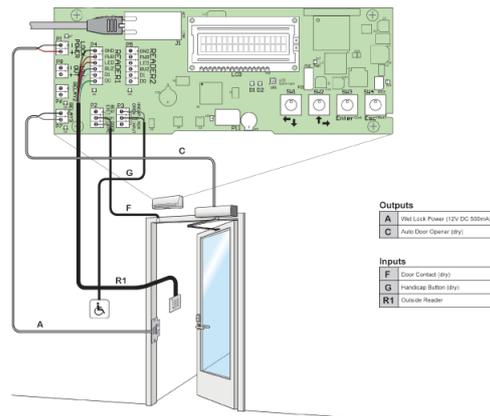
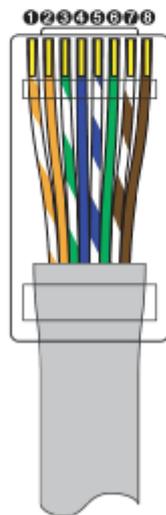


Figure A.6. Cable Requirements

Name	Maximum Distance	Cable Type	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, 100% 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*

* Unless otherwise specified by manufacturer.
 ** Recommended the following T568B wiring for both ends.

T568B (TIA/EIA568B) Wiring



- ❶ White/Orange
- ❷ Orange
- ❸ White/Green
- ❹ Blue
- ❺ White/Blue
- ❻ Green
- ❼ White/Brown
- ❽ Brown

Figure A.7. Package Contents

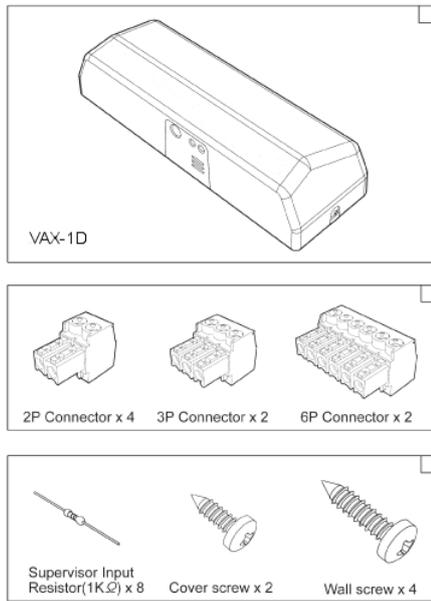


Figure A.8. Panel Layout

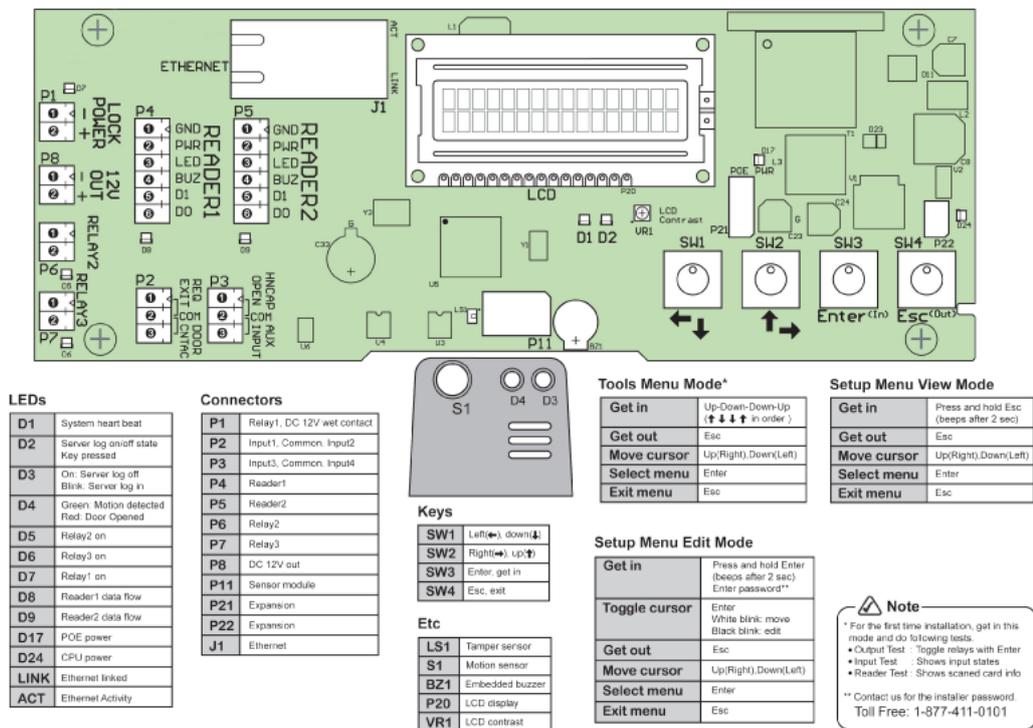


Figure A.9. Panel Dimensions

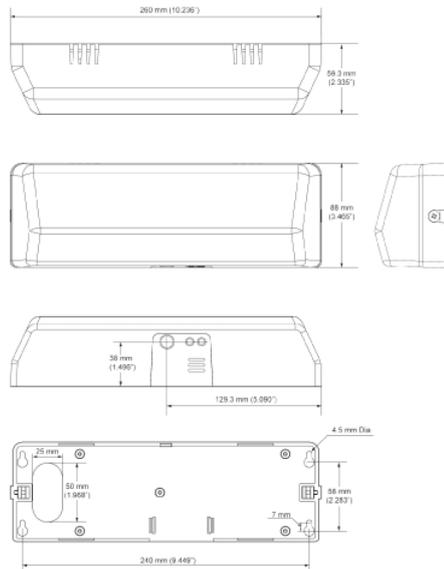


Figure A.10. Input Types

Specification

Digital*	Off, On
Supervised*	Off, On, Short, No connection

* Software selectable

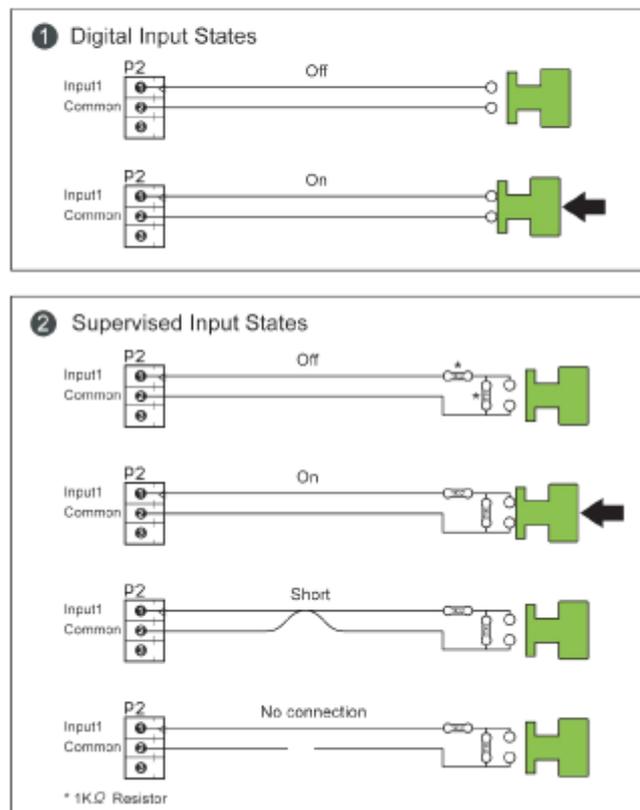
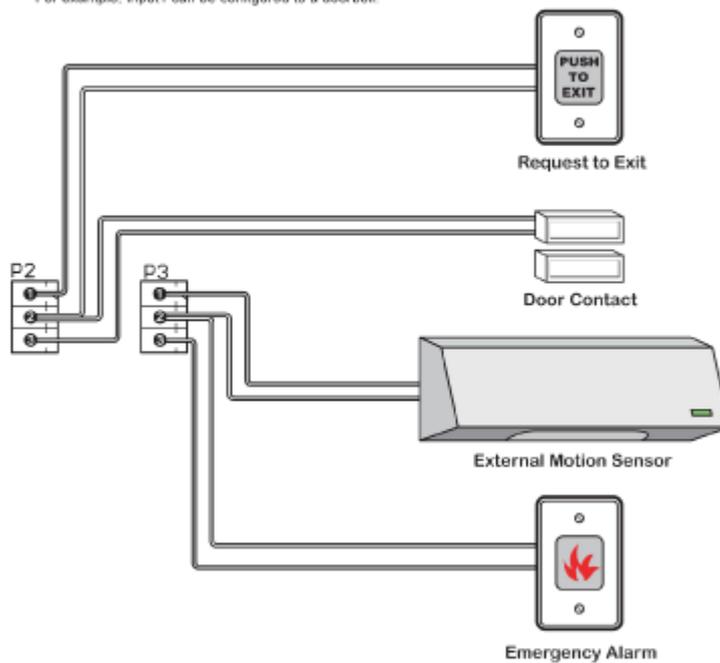


Figure A.11. Input Example

Specification

P2 1-2 Pin (Input1)	① Input	② Common (GND)
P2 2-3 Pin (Input2)	② Common (GND)	③ Input
P3 1-2 Pin (Input3)	① Input	② Common (GND)
P3 2-3 Pin (Input4)	② Common (GND)	③ Input

* All the inputs are configurable.
For example, Input1 can be configured to a doorbell.



Note : Input Test

- Get in Tools Menu Mode by pressing ↑↓↑ keys in order.
- Select Input Test menu. (↑↓ Enter keys)
- LCD displays current input states. (0 = Off, 1 = On, 2 = Short, 3 = Disconnected)

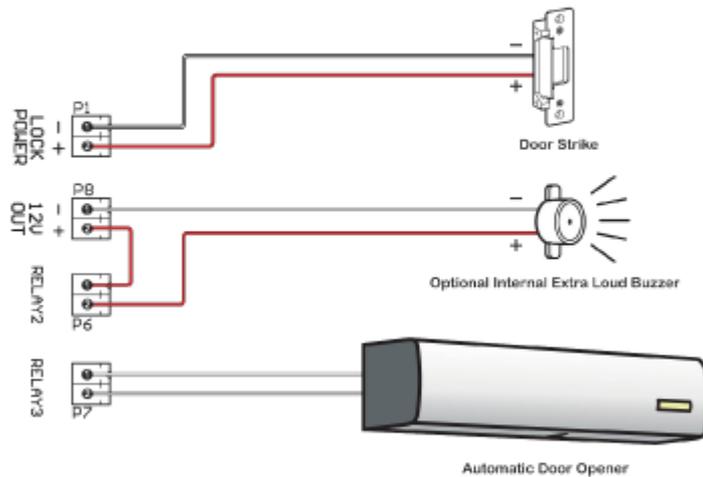
I1	I2	I3	I4
1	0	2	3

Figure A.12. Relay Example

Specification

P1 (Relay1, Lock power)	Lock power relay. ① GND, ② 12V DC 500mA
P8 (12V DC out)	12V DC output. ① GND, ② 12V DC 200mA
P6 (Relay2)	24V DC 500mA limit
P7 (Relay3)	24V DC 500mA limit

* All the relay outputs are configurable.
For example, Relay2 can be configured to a door strike.



Note : Output Test

- ① Get in Tools Menu Mode by pressing ↑↓↓↑ keys in order.
- ② Select Output Test menu. (↑↓Enter keys)
- ③ Toggle selected relay by pressing Enter. (Select change ←→ keys. 0 = Off, 1 = On.)

The screenshots show the menu flow: first, the physical buttons; then a screen with 'Output Test' and 'Input Test' options; finally, a screen displaying the status of three relays: R1 (1), R2 (0), and R3 (0).

Figure A.13. Reader Example

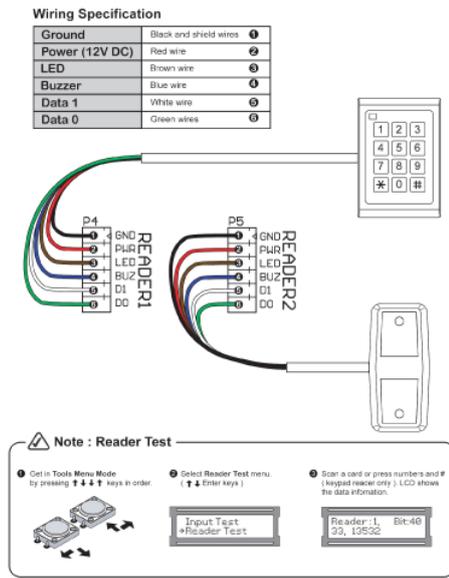
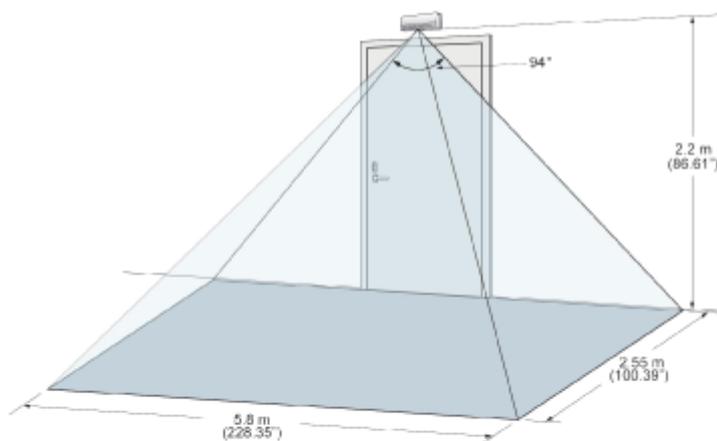


Figure A.14. Motion Sensor

Specification

Sensor Type	PIR
Detection Range	5 m
Detection Angle	H: 94°, V: 82°
Detection Zone	04 zones



Actions

This section will give you a list of available actions, a brief description of what they do and the required parameters.

Action Name:ResetSitesAPB

Description:Reset user's apb locations on all panels within the specified site state

Parameters:

SiteId
Description: Site to reset

Action Name:ResetUsersAPB

Description:Reset user's apb locations state

Parameters:

UserId
Description: User to reset

Action Name:SetUsersAPB

Description:Set a user's anti-passback location to an area state

Parameters:

UserId
Description: User to set
AreaId
Description: Area to set

Action Name:DWAuth

Description:Authenticate against Digital WatchDog state

Parameters:

Address
Description: Address of the Digital WatchDog server
Username
Description: Digital WatchDog Username
Password
Description: Digital_WatchDog_Password

Action Name:ConvertFromBase64

Description:Convert the provided base64 string to a plain text of the specified encoding state

Parameters:

Input
Description: Input string in Base64 format
Encoding
Description: Type of encoding to convert string to

Action Name:ConvertToBase64

Description:Convert the specified string to Base64 format state

Parameters:

Input
Description: String to convert
Encoding
Description: Encoding of the input string

Action Name:ConvertToMD5Hash

Description:Convert the specified string to a md5 hash state

Parameters:

Input
Description: String to convert

Action Name:DoorCrisisLevel

Description:Put a door into crisis mode or resume from crisis mode state

Parameters:

CrisisLevelId
Description: Crisis level to place door into
DoorId
Description: Door to affect

Action Name:OverrideDoor

Description:Override a door's scheduled state state

Parameters:

DoorId
Description: Door to affect
TimeZoneMode
Description: Mode to override the door to
ResumeOnNextTZ
Description: Automatically resume the door to it's natural state on the next scheduled change in its time zone

Action Name:PulseDoor

Description:Pulse unlock the specified door state

Parameters:

DoorId
Description: Door to affect

Action Name:ResumeDoor

Description:Resume a door from an overridden state state

Parameters:

DoorId
Description: Door to affect

Action Name:OverrideFloor

Description:Override a floor's scheduled state state

Parameters:

FloorId
Description: Floor to affect
TimeZoneMode
Description: Mode to override the floor to
ResumeOnNextTZ
Description: Automatically resume the floor to it's natural state on the next scheduled change in its time zone

Action Name:ResumeFloor

Description:Resume a floor from an overridden state state

Parameters:

FloorId
Description: Floor to affect

Action Name:Each

Description:Iterate over a set of items state

Parameters:

Items
Description: Collection of items to iterate over

Action Name:If

Description:Perform a conditional operation state

Parameters:

Expression
Description: Expression to evaluate. Will be considered successful if the result of the expression is 'true'

Action Name:Log

Description:Log message to notification display and action plan history state

Parameters:

Level
Description: Determines the severity of the log message
Message
Description: Message to log

Action Name:SetVariable

Description:Set's one or more session variables for later use within the action plan state

Action Name:Timer

Description:Delay execution of the next action within the action plan by the specified interval state

Parameters:

Delay
Description: Duration to delay execution of subsequent actions

Action Name:OverrideInput

Description:Override a input's scheduled state state

Parameters:

InputId
Description: Input to affect
Mode
Description: Mode to override the input to

Action Name:OverrideOutput

Description:Override a output's scheduled state state

Parameters:

OutputId
Description: Output to affect
Mode

Description: Mode to override the output to

Action Name:Email

Description:Send an email state

Parameters:

To
Description: Email Address to send to
From
Description: Email Address to send from
CC
Description: Optional Carbon Copy
BCC
Description: Optional Blind Carbon Copy
Subject
Description: The subject of the email message
Body
Description: The body or content of the email message
AllowHTML
Description: Determines whether the body is rendered as html
Attachment1
Description: Email_Attachment1_Description
Attachment2
Description: Email_Attachment2_Description
Attachment3
Description: Email_Attachment3_Description

Action Name:HttpRequest

Description:Perform a HTTP request against an external resource state

Parameters:

Address
Description: Url of the server to send the request to
Method
Description: HTTP Method associated with the request. GET/PUT/POST/DELETE/OPTIONS
Body
Description: Contents of the HTTP Request. Not supported with GET requests
ContentType
Description: Content type of the body of the HTTP request
Headers
Description: Set any additional headers to be sent with the request
BypassCertificateValidation

Description: Bypass SSL certificate validation. Required for hosts using self signed certificates
UseCookieContainer
Description: Use the common cookie container within this action plan. Useful for cookie based authentication

Action Name:NotifyAdministrator

Description:Send a notification to a administrator who is currently logged in state

Parameters:

Title
Description: Title of the message
Message
Description: Message to send
AdministratorId
Description: Administrator to send message too
CameraId
Description: Camera to be displayed in the popup
Closeable
Description: Determines if the popup can be closed via user by clicking on the X in the top right
CloseButtonActionPlanId
Description: Action to perform when popup is closed via close button
CloseButtonPersistSessionVariables
Description: Determines whether session variables for the current action plan are persisted to the newly executed action
Button1Enabled
Description: Determines if the first button will be visible
Button1Label
Description: Label for the first button
Button1CloseOnClick
Description: Determines if clicking the first button will cause the popup to close
Button1ActionPlanId
Description: Action Plan to execute when the first button is clicked
Button1PersistSessionVariables
Description: Determines whether session variables for the current action plan are persisted to the newly executed action
Button2Enabled
Description: Determines if the second button will be visible
Button2Label
Description: Label for the second button
Button2CloseOnClick
Description: Determines if clicking the second button will cause the popup to close
Button2ActionPlanId
Description: Action Plan to execute when the second button is clicked

Button2PersistSessionVariables

Description: Determines whether session variables for the current action plan are persisted to the newly executed action

Action Name:Ping

Description:Ping a specified network host state

Parameters:

Address

Description: IP Address or Host Name to ping

Action Name:WakeOnLan

Description:Send a wake on lan magic packet to specified device state

Parameters:

MacAddress

Description: The mac address of physical address of the device to wake

BroadcastAddress

Description: Broadcast address to send to, in most cases the default value will work

BroadcastPort

Description: Port to send on, in most cases the default value will work

Action Name:ActivateChangeTracker

Description:Set pending change tracking for current partition state

Action Name:CancelChangeTracker

Description:Cancel pending change tracking on partition state

Action Name:DisconnectPanel

Description:Force a panel to disconnect from the server state

Parameters:

PanelId

Description: DisconnectPanel_PanelId_Description

DisconnectionTime

Description: Amount of time in minutes to disconnect panel for

Action Name:PlaySound

Description:Start playing the specified sound on the specified panel state

Parameters:

PanelId

Description: The panel to affect
PanelSound
Description: Sound to play

Action Name:StartEmergencyAlarm

Description:Send start emergency alarm command to panel state

Parameters:

PanelId
Description: Panel to send to
ActionCode
Description: Action to perform

Action Name:StopEmergencyAlarm

Description:Send stop emergency alarm command to panel state

Parameters:

PanelId
Description: Panel to send to

Action Name:StopSound

Description:Stops a currently playing panel sound state

Parameters:

PanelId
Description: The panel to affect

Action Name:UpdatePanels

Description:Request a panel update of all panels within the same partition as the action plan state

Action Name:ExecuteReader

Description:Execution an action on the specified reader state

Parameters:

ReaderId
Description: Reader to execute the action on
Action
Description: Action to execute

Action Name:StopReader

Description:Stop a currently executing reader action state

Parameters:

ReaderId
Description: Reader to stop the action on

Action Name:SMSClickatell

Description:Send a SMS message using the third party Clickatell.com website. state

Parameters:

Username
Description: Username provided by Clickatell
Password
Description: Password provided by Clickatell
APIKey
Description: APIKey provided by Clickatell
To
Description: Phone number to send the SMS to
Message
Description: Message to send

Action Name:SMSTwilio

Description:Send a SMS message using the third party Twilio.com website state

Parameters:

AccountSid
Description: SMSTwilio_AccountSid_Description
AuthToken
Description: Auth Token provided by Twilio
To
Description: Phone number to send the SMS to
From
Description: Twilio phone number to send from
Message
Description: Message to send
TwilioBaseURI
Description: Base URL of the Twilio service. In most cases the default will work

Action Name:WaitForDoor

Description:Wait for the specified door to meet the specified state within the provided interval state

Parameters:

SiteId

Description: The site containing the device to watch for
DoorId
Description: Door to wait for
State
Description: One or more door states to watch for
WaitFor
Description: The amount of time to wait for this trigger to occur
AllowedDrift
Description: The maximum allowed drift between the event time and the server time. Any notifications raised outside this boundry will not be treated as valid triggers

Action Name:WaitForFloor

Description:Wait for the specified floor to meet the specified state within the provided interval state

Parameters:

SiteId
Description: The site containing the device to watch for
FloorId
Description: Floor to wait for
State
Description: One or more floor states to watch for
WaitFor
Description: The amount of time to wait for this trigger to occur
AllowedDrift
Description: The maximum allowed drift between the event time and the server time. Any notifications raised outside this boundry will not be treated as valid triggers

Action Name:WaitForInput

Description:Wait for the specified input to meet the specified state within the provided interval state

Parameters:

SiteId
Description: The site containing the device to watch for
InputId
Description: Input to wait for
State
Description: One or more input states to watch for
WaitFor
Description: The amount of time to wait for this trigger to occur
AllowedDrift
Description: The maximum allowed drift between the event time and the server time. Any notifications raised outside this boundry will not be treated as valid triggers

Action Name:WaitForOutput

Description:Wait for the specified output to meet the specified state within the provided interval state

Parameters:

SiteId
Description: The site containing the device to watch for
OutputId
Description: Output to wait for
State
Description: One or more output states to watch for
WaitFor
Description: The amount of time to wait for this trigger to occur
AllowedDrift
Description: The maximum allowed drift between the event time and the server time. Any notifications raised outside this boundry will not be treated as valid triggers

Action Name:WaitForReader

Description:Wait for the specified reader to meet the specified state within the provided interval state

Parameters:

SiteId
Description: The site containing the device to watch for
ReaderId
Description: Reader to wait for
UserId
Description: Optional user to wait for
State
Description: One or more reader states to watch for
WaitFor
Description: The amount of time to wait for this trigger to occur
AllowedDrift
Description: The maximum allowed drift between the event time and the server time. Any notifications raised outside this boundry will not be treated as valid triggers

Action Name:WaitForReaderWithAPG

Description:Wait for the specified reader to meet the specified state involving a user within the specified access group state

Parameters:

SiteId
Description: The site containing the device to watch for
AccessPrivilegeGroupId
Description: Access privilege group to watch for

ReaderId
Description: Reader to wait for
State
Description: One or more reader states to watch for
WaitFor
Description: The amount of time to wait for this trigger to occur
AllowedDrift
Description: The maximum allowed drift between the event time and the server time. Any notifications raised outside this boundary will not be treated as valid triggers

Action Name:AddUserToGroup

Description:Add specified user to an access group state

Parameters:

UserId
Description: AddUserToGroup_UserId_Description
AccessPrivilegeGroupId
Description: AddUserToGroup_AccessPrivilegeGroupId_Description

Action Name:DisableUser

Description:Immediately disable a user's access to all doors state

Parameters:

UserId
Description: User to disable
PanelId
Description: Optionally Limit Disable to a single panel
Temporary
Description: If temporary the disable will be cleared upon panel update. Only applies if a panel is selected

Action Name:RemoveUserFromGroup

Description:Remove specified user from an access group state

Parameters:

UserId
Description: RemoveUserFromGroup_UserId_Description
AccessPrivilegeGroupId
Description: RemoveUserFromGroup_AccessPrivilegeGroupId_Description

Action Name:SetCustomField

Description:Set value for a users custom field state

Parameters:

UserId
Description: User to set value on
CustomFieldId
Description: SetCustomField_CustomFieldId_Description
Value
Description: SetCustomField_Value_Description

Action Name:UserInGroup

Description:Determines if the specified user has membership to the specified group state

Parameters:

UserId
Description: User to evaluate
AccessPrivilegeGroupId
Description: Access Group to evaluate

WARRANTY AND SPECIAL PROVISIONS

WARRANTY AND SPECIAL PROVISIONS FOR THE UNITED STATES OF AMERICA, CANADA ANY OTHER COUNTRY . LIMITED WARRANTY: Vicon warrants that the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of (2) years from the date of receipt. Any implied warranties or conditions on the SOFTWARE are limited to (2) years. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

NO OTHER WARRANTIES: To the maximum extent permitted by applicable law, Vicon disclaim all other warranties, either express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose, with regard to the SOFTWARE, the accompanying written materials, and any accompanying hardware. This limited warranty gives you specific legal rights. You may have others which vary from province/state/jurisdiction to province/state/jurisdiction.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES: To the maximum extent permitted by applicable law, in no event shall Vicon be liable for any damages whatsoever (including without limitation, direct or indirect damages for personal injury, loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if Vicon has been advised of the possibility of such damages. In any case, Vicon entire liability under any provision of this agreement shall be limited to the amount actually paid by you for the SOFTWARE. Because some province/state/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

This Software License Agreement is governed by the laws of the Province of Ontario, Canada. Each of the parties hereto irrevocably agrees to the jurisdiction of the courts of the Province of Ontario and further agrees to commence any litigation which may arise hereunder in the courts located in the Judicial District of York, Province of Ontario.

Copyright © 1998 - 2022 Vicon All rights reserved.

Information in this document is subject to change without notice. The software outlined in this document is provided under license agreement. The software may only be used in accordance with the terms expressed by Vicon No part of this documentation may be reproduced or transmitted in any form

or by any means except for the User's benefit of operating the software without the express written permission of Vicon.

Vicon.

- **Within the US:** 1-800-348-4266
- **Outside the US and Europe:** 1-631-952-2288
- **UK:** +44 1489 566330

Customers requesting technical support are required to verify their status by providing a customer ID number in order to be passed through to the technical support queue. Requests for support from other sources will be directed to their dealer/integrator for technical support

Web site: www.vicon-security.com/