Protector.Net Tech Guide

Protector.Net Tech Guide

Table of Contents

Introduction

Hartmann Controls is proud to present our Protector.Net Access Control software. 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 Hartmann Controls Protector.Net access system. Thank You for your business.

Warranty

Hartmann Controls Access Control System: 2-Year Full Warranty . Hartmann Controls warrants all Controllers manufactured by Hartmann Controls Corp. and are free from defects in material and workmanship for the period of (2) years. This warranty also covers some non-manufactured peripheral products sold by Hartmann Controls such as Readers, proximity cards/key tags. All other peripheral products are covered by a 30-day manufacturer's warranty. The warranty period for the Hartmann Controllers is 2 years from date of purchase. Hartmann Controls Corp will repair or replace defective equipment upon return to its facility. If it is identified that the warranty was breached in any way, Hartmann Controls Corp. will not warrant any damage that occurred during shipping or handling, or damage caused by a repair or an attempt to repair by any person other than those authorized by Hartmann Controls. This warranty covers normal industrial use and does not cover defects or damage to any product which, in the sole opinion of Hartmann Controls Corp. has been subject to improper installation, unauthorized modification, misuse, neglect, abuse, or abnormal operating conditions, improper storage, or which has been attributable to acts of God such as lightning and flooding.. Installation, which is not in accordance with the installation instructions, published by Hartmann Controls, will void the warranty. This warranty does not cover defects or damage caused by a product, which is not approved by Hartmann Controls Corp. and is connected to its system.

The said warranty only applies to the original purchaser and is and shall be in lieu of any and all other warranties.

Note

Please note this does not include shipping, which will be the responsibility of the customer.

Claim Procedure. In order to obtain warranty performance, the purchaser must contact Hartmann Controls Corp. to obtain an RMA number. Unauthorized returns will be refused and returned to the sender at the sender's expense. **Do not ship any defective product back before receiving an RMA number**. Upon receiving goods, Hartmann Controls Corp. will assess the condition of the returned defective merchandise and, if found to be defective, will be repaired/replaced and shipped back. If the merchandise is found to be non-defective, the merchandise will be returned to the sender and subject to applicable return freight charges.

Note

If a replacement product is required for the functionality of the system, Hartmann Controls Corp. will overnight the replacement item at the purchasers expense and the purchaser will be invoiced for items being replaced. Once the defective merchandise is received and if found to be defective and if within the limits of warranty, Hartmann Controls Corp. will credit the replacement item invoice. If the product is found to be non-defective, Hartmann Controls will ship the merchandise back at the expense of the purchaser.

Information Required For RMA.

- Product Type
- Model of the Panel
- Problem Reported
- Geological location

Note

The proof of date of purchase may be required before warranty service is rendered.

Hartmann Controls Software - End User Licence 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 Hartmann Controls Corp. with which you acquired the Hartmann Controls Corp. software product(s) identified above ("SOFTWARE"). The SOFTWARE includes Hartmann Controls Corp 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 Hartmann Controls Corp. for instructions on return of the unused product(s) in accordance with Hartmann Controls 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

   Hartmann Controls Corp. 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 Hartmann Controls Corp.

   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 Hartmann Controls Corp. 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: Hartmann Controls Corp. reserve 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 Hartmann Controls Corp. 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. Hartmann Controls Corp. may use this information solely to improve

their products or to provide customized services or technologies to you. Hartmann Controls Corp. 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 Hartmann Controls licensed SOFTWARE. Any attempts to access the database information via unlicensed and/or unauthorized access will terminate this license agreement. Hartmann Controls Corp. provides no direct access to the database information.

Additional Software/Services: The terms of this EULA apply to Hartmann Controls updates, supplements, and add-on components of the SOFTWARE that Hartmann Controls Corp. 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, Hartmann Controls Corp. 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 Hartmann Controls Corp. or its suppliers.

4. UPGRADES

   If the SOFTWARE is labeled as an upgrade, you must be properly licensed to use a product identified by Hartmann Controls Corp. 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 Hartmann Controls 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 Hartmann Controls Corp. 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

Hartmann Controls Corp.

Phone: 1-877-411-0101 (Toll Free Canada/USA)

Fax: + 705-792-5632

Website: www.hartmann-controls.com

Chapter 1. Getting Started

Overview

Protector.Net 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 Protector.Net server software consists of:

- **Protector.Net Web Server**: The Web Server's responsibility is to host the web application and facilitate client access to managing your access control system.
- **Protector.Net 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 Protector.Net 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 Protector.Net application server is designed to run on a modern PC running Microsoft Windows 7 or newer.

Note

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

- 2Ghz or faster 32-bit (x86) or 64-bit (x64) processor. Two or more cores recommended.
- 4GB RAM for 32-bit and 4GB RAM for 64-bit .
- 1GB Free Hard Drive Space (Additional space required for database).
- Windows 7 Home or Higher (Windows 7 Starter Not Supported).
- Microsoft .Net Framework 4.5 Full.
- Microsoft SQL Server 2008 or SQL Server 2008 Express or Higher (SQL Express installation available from the Protector.Net Installer).

Installation Procedures

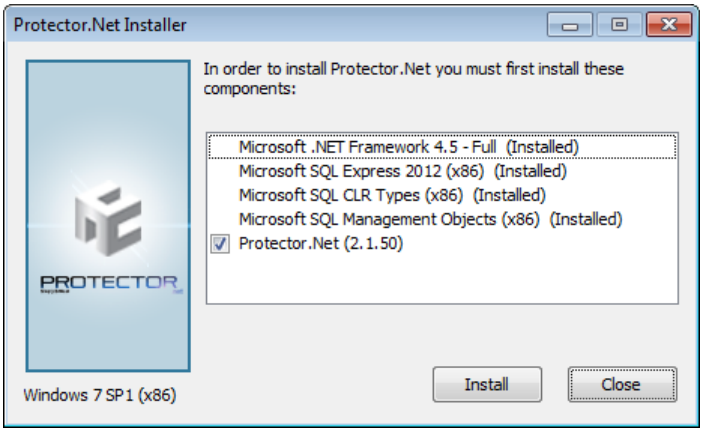
This section covers the installation of Protector.Net and some frequently asked questions.

New Installation Protector.Net

1. Locate and run the file called "ProtectorNet.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. Protector.Net 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.

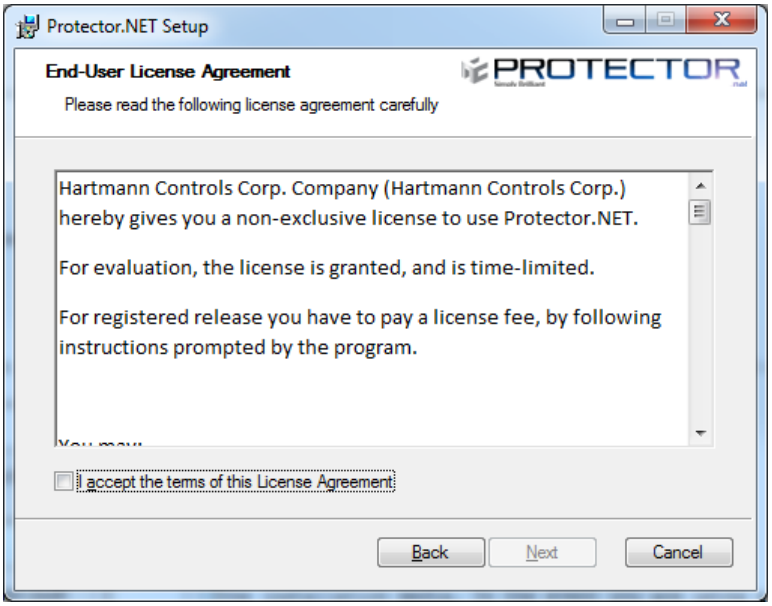
3. Once all prerequisites are installed, the installer will automatically launch the Protector.Net application installer.

Figure 1.2. Protector.Net Application Installer

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

4. On the following screen, please read an accept the License Agreement. This agreement must be accepted in order to proceed with the Protector.Net installation. Click **Next**.

Figure 1.3. Protector.NET License Agreement



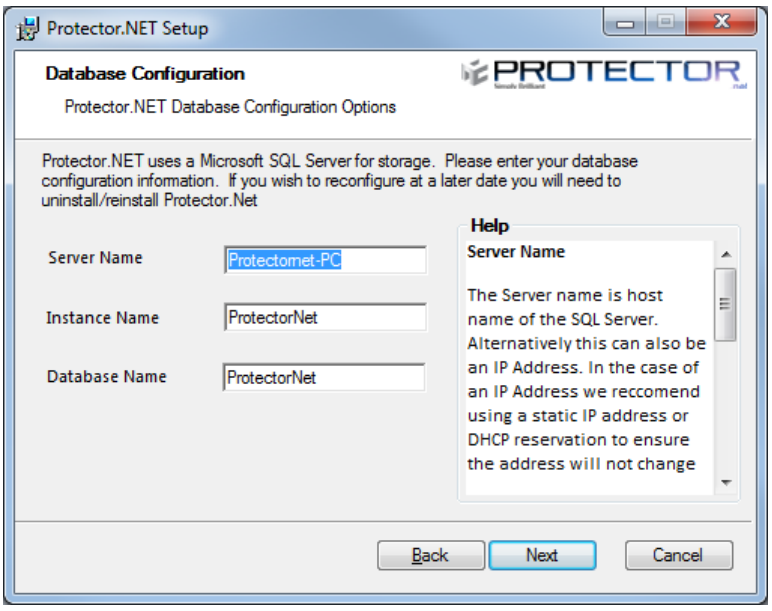
5. The next step is to choose the installation type:

   - **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 Protector.Net configuration options.

6. **[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. Protector.Net 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 then 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.

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

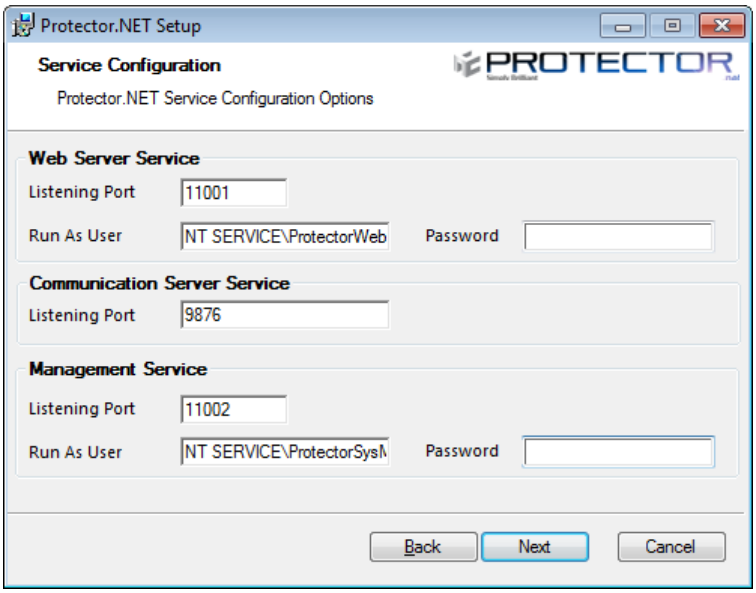
   Management Service: The service the **System Manager UI** will run as. The **Listening Port** is the port the server will listen on for management communication, by default is **11002**.

   "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 enviroments a **Domain Service User** or a **Local Administrator Account** may be needed to run the services.

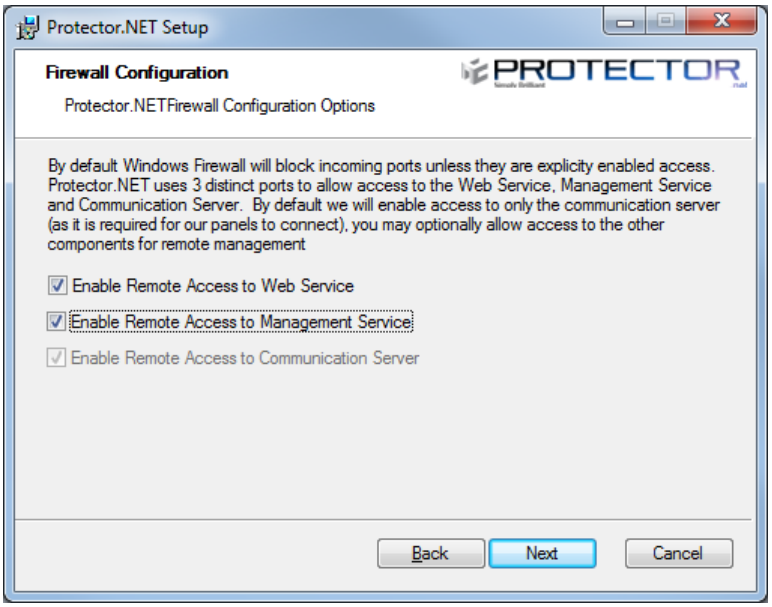
Figure 1.5. Protector.Net Service Configuration



8. 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, Protector.Net 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

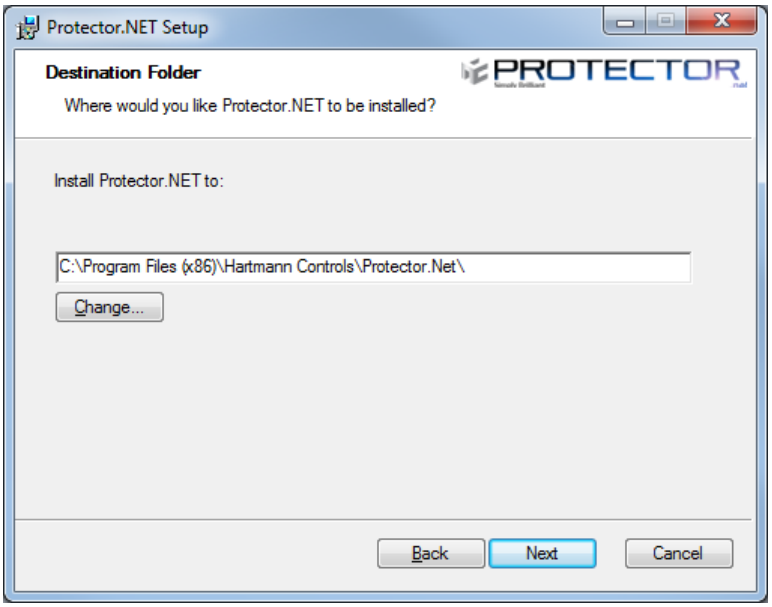
using a third party firewall, additional steps may be required to permit access. Please check your firewall documentation for additional clarification.

Figure 1.6. Protector.Net Firewall Configuration



9. The next step is to select the installation directory where you would like the Protector.Net application to be installed.

Figure 1.7. Protector.Net Installation Directory Configuration



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

Upgrading Protector.Net

Periodically updates are released to Protector.Net to enhance features, fix bugs or improve compatibility. Protector.Net does not offer separate upgrade packages. Our standalone installer is

capable of installing a new software instance or upgrading an existing instance of the Protector.Net software.

Upgrade Installation

Depending on how you've installed Protector.Net, the procedure for upgrading the Protector.Net software is sometimes a few extra steps fresh install. Please see Chapter 2, *Upgrading Protector.Net* for more details on these extra steps. We recommend doing a backup of your Protector.Net database prior to upgrading. For more information about backing up your database, please see the section called “Backing up your Protector.Net Database”. We also recommend stopping the Protector.Net service via **System Monitor** prior to installation. Please note, if the installer does not contain a newer version then the currently installed version, you will not be given the option to perform upgrade. You will instead be prompted to 'Repair' or 'Remove' the current installation.

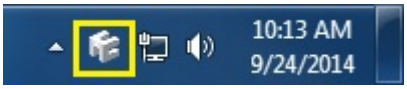
Updating Firmware

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

System Monitor

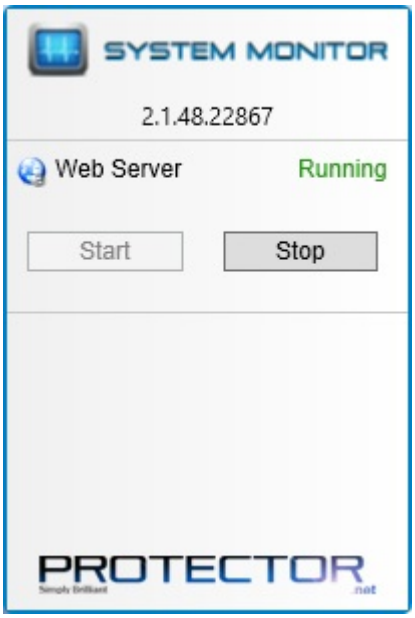
System Monitor is a tray application that shows you the status and offers limited control over the web server process. It will also show you the current version of your Protector.Net software.

Once Protector.Net is installed on the server, the system monitor icon will sit in the system tray (by the clock, highlighted below).



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

Figure 1.8. System Monitor Window



Once the System Monitor window is open, you can use the **Start** and **Stop** buttons to start and stop the service. This can be useful when performing software upgrades as you can safely turn the service off. You can also see the version of Protector.Net you are using.

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 you own database server instance, you will need to ensure the correct privileges and protocols are available for connection. This is something we generally only recommend for technicians or network Administrators who are well versed in the installation and configuration of SQL Server. Also please note different versions of SQL have different operating system and PC requirements. If you choose to use a different version, please ensure your PC meets the requirements for that version.

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

A: At this time there is no plan to support operating systems earlier than Microsoft Windows 7. We are committed to ensuring the software works with future versions of Microsoft Windows.

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

A: As part of the Protector.Net installation, you are required to provide the correct SQL information which the installer uses to configure a number of Protector.Net database and security options. If this information is incorrect, it will need to be corrected before you are able to successfully install the Protector.Net software. If you have chosen to install SQL Express as part of the Protector.Net 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 Protector.Net 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 Protector.Net 32-bit or 64-bit?

A: Protector.Net 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 Protector.Net software will not benefit from the increased addressing 64-bit provides.

Client Installation

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

Supported Browsers

The list of browsers supported is by no means a comprehensive list. These are browsers that receive testing by Hartmann Controls, 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 1.1. Protector.Net Browser Support

Browser	Version	Supported	Notes
Google Chrome	24.0+	Yes	Hartmann Control's browser of choice
Mozilla Firefox	20.0+	Yes	
Microsoft Internet Explorer	6.0 or earlier	No	No HTML5 Support
Microsoft Internet Explorer	7.0	No	No HTML5 Support
Microsoft Internet Explorer	8.0	No	No HTML5 Support
Microsoft Internet Explorer	9.0	No	Insufficient HTML5 Support
Microsoft Internet Explorer	10.0	Yes	Note: IE10 in Modern UI (Windows 8) is not supported. The desktop version however is fully supported
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 Protector.Net software, accessing the Protector.Net 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 Protector.Net From the PC the Server Software is Installed on:

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

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 Protector.Net'**. If you wish, you can pin this shortcut permanently to your start screen by right clicking and selecting **'Pin To Start'** .

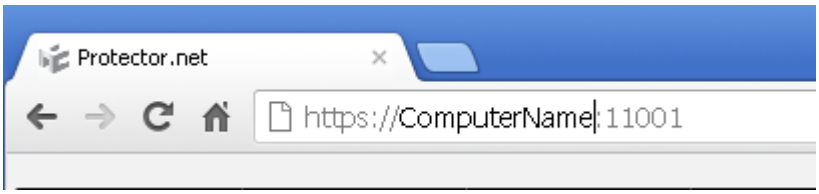
Accessing Protector.Net From a Remote PC:

Open your web browser and within the address bar enter the address of the Protector.Net 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 Protector.Net server remotely

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



Once you have entered the address, press Enter to navigate to the Protector.Net 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 required Windows 7 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 Protector.Net 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 Protector.Net 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 Protector.Net 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)

Chapter 2. Upgrading Protector.Net

This chapter covers the process of upgrading Protector.Net, the pre-requisites for upgrading, and how to update the firmware on the Panels.

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

Download the Latest Version of Protector.Net

Visit our Protector.Net downloads page at:

http://www.hartmann-controls.com/Support/ProtectorNetDownloads

You'll be promoted for credentials to download, please contact Hartmann Controls for these details.

Prerequisite Installation

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

- Upgrade must be performed on the computer that Protector.Net is currently installed.
- You must be logged in as the same Windows Login that installed Protector.Net (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 Protector.Net software is identical to that of a fresh install. (Please, see the section called “Installation Procedures”).We recommend doing a backup of your Protector.Net database prior to upgrading. For more information about backing up your database, please see the section called “Backing up your Protector.Net Database”. We also recommend stopping the Protector.Net service via **System Monitor** prior to installation.

Note

During installation, its advised you click "advanced" and ensure information such as the database connection look correct.

Panel Firmware Updates

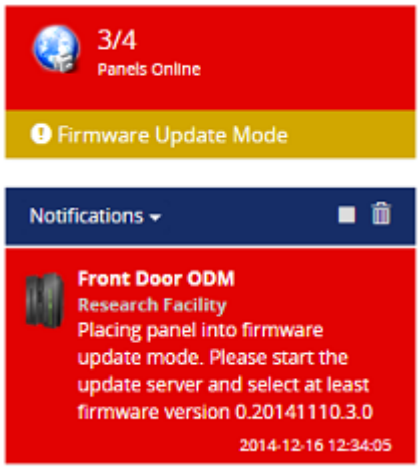
Periodically when we enhance Protector.Net, firmware upgrades to your Panels will be required with the software updates. Updating a Panels firmware is a relatively straight forward process.

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 only update one Panel at a time.

1. When a Panel attempts to connect to the Protector.Net application and the firmware is found to be out of date, you will see a Notification within the Notification window, along with a indicator that a panel is in Update mode above the notification window.

Figure 2.1. Firmware Out of Date Notification



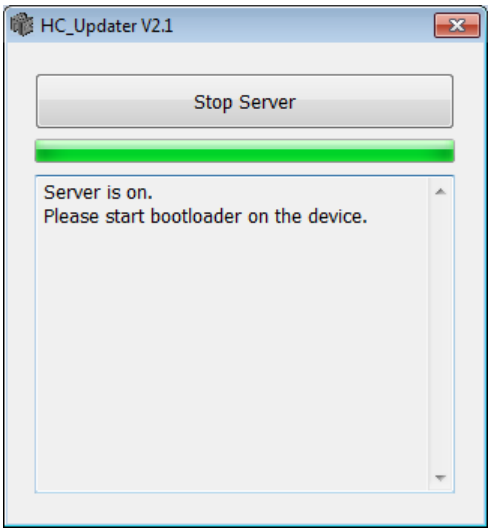
2. If no other Panels are currently in firmware update mode the Panel will be automatically placed into firmware update mode. If another Panel is currently updating the Panel will be disconnected from the server (but still fully functional) until the currently updating Panel is complete.

3. In order to update your Panel you will need to launch the Firmware Update Utility located within your start menu. The link for the firmware update utility can be located by clicking Start -> All Programs -> Protector.Net and finally clicking on **"Firmware Update Utility"**.

Windows 8/8.1 Users

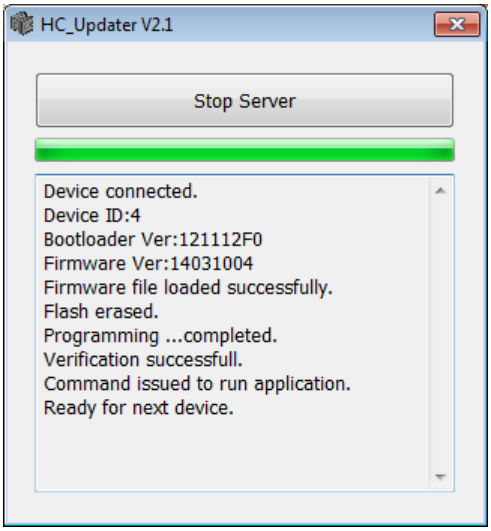
Windows 8/8.1 hides the shortcut by default within the Modern UI start screen. The shortcut can be located by typing 'Firmware Update' within the start screen and selecting 'Firmware Update Utility'. If you wish you can pin this shortcut permanently to your start screen by right clicking and selecting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

Figure 2.2. HCUpdater Utility



4. The HCUpdater application 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 firmware update utility will instruct the Panel to disconnect, at which point the Panel will resume normal operation and the firmware update utility will begin listening for the next Panel.

Figure 2.3. HCUpdater Utility Successful Update



5. Once all of your Panels are online within the Protector.Net application and you are no longer seeing 'Firmware Out of Date Notifications', you may close the firmware update utility.

6. After Panels firmware have been 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 Doesn't Connect to HCupdater. If the Panel does not connect to the firmware update utility after being placed into update mode by our software, 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. If these obsoletes appear clear but there is still no connection to the Firmware Updater:

1. Open HCUpdater from the start menu.

2. You will need physical access to the Panel. Unplug the Cat5 cable to the Panel, press and HOLD SW3 (enter). While holding SW3, plug the Cat5 back into the Panel. Once it powers up and you see the LCD change from 'SW3: Stored IP' to 'Panel IP', release SW3. You have now manually placed the Panel into firmware update mode.

3. Check the HCUpdater utility for activity. When the update is successful you may resume normal operation.

If none of the above results in the Panel successfully updating, please contact Hartmann Controls support. See Chapter 29, *Support*.

Frequently Asked Questions

Q: How can i check if my Windows login can upgrade Protector.Net?

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

1. Open a command line with administrator privileges (right click cmd.exe, 'Run as Administrator'.)

2. At the command line, type: 'SQLCMD -S .\PROTECTORNET' (your instance name may be different). Click 'ENTER'.

3. At the '1>', type 'USE PROTECTORNET' and press 'ENTER'.

4. At the '2>', type 'GO' and press 'ENTER'.

If you see the message "Changed database context to 'ProtectorNet'." Your Windows account has permission to upgrade Protector.Net.

Figure 2.4. Command Prompt: Backup

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

Q: My Windows login doesn't have permission to upgrade Protector.Net, how do i find out which account does?

A: Due to the manner that SQL database permissions work, when Protector.Net 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 Hartmann Controls.

Q: How can i test if UDP port 9876 is unblocked for a firmware update?

A: Prior to performing an upgrade, you can remotely place a Panel into 'Firmware Update Mode'. This will flash the firmware on the Panel to the same version it currently has. On larger multi-site systems, its advised you perform this test to at least one Panel on each site. To perform this test:

1. You will need to be logged into the computer with Protector.Net server software installed.

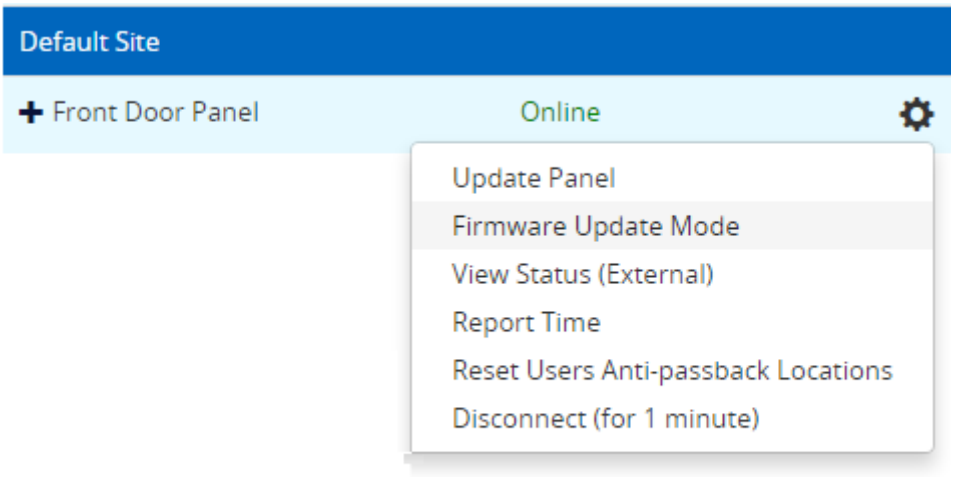
2. Open the Firmware Updater from the start menu, located in the Protector.Net sub folder. Or in Windows 8 search for "Firmware Updater".

3. Browse to the System Overview page in Protector.Net. From here, click on the gear icon next to a Panel you'd like to test. A drop-down menu will appear.

4. From the drop-down menu, select "Firmware Update Mode". The Panel will now disconnect and be placed into firmware update mode.

5. Switch over to the Firmware Update Utility. Monitor the window for activity. If the Panel fails to connect to the updater, please contact Hartmann Controls or your System Administrator.

Figure 2.5. System Overview: Firmware Update Command



Chapter 3. Initial Configuration

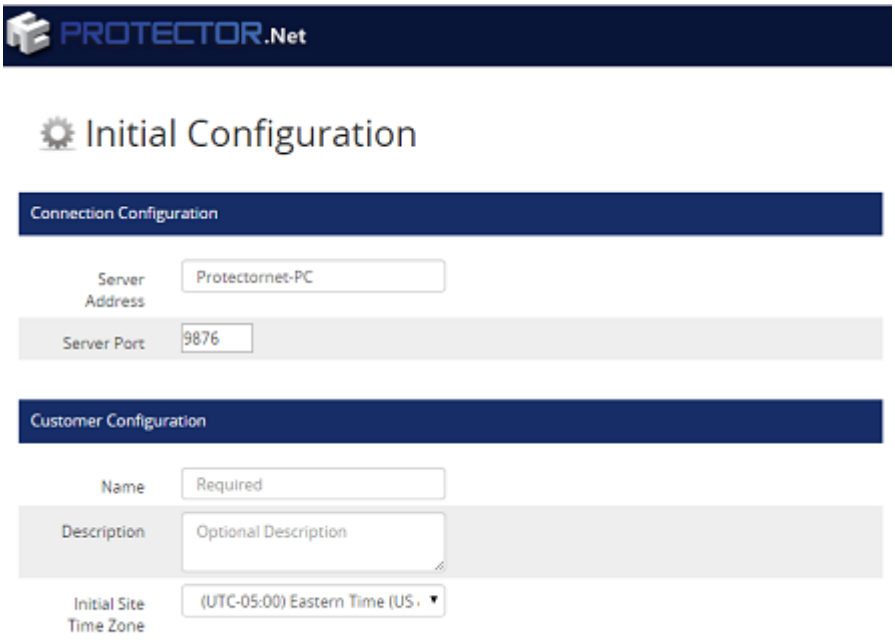
This chapter will cover the initial configuration of the software and hardware elements of Protector.Net. This includes the initial setup of the software, the initial setup of the Panels and how to associate a Panel with Protector.Net

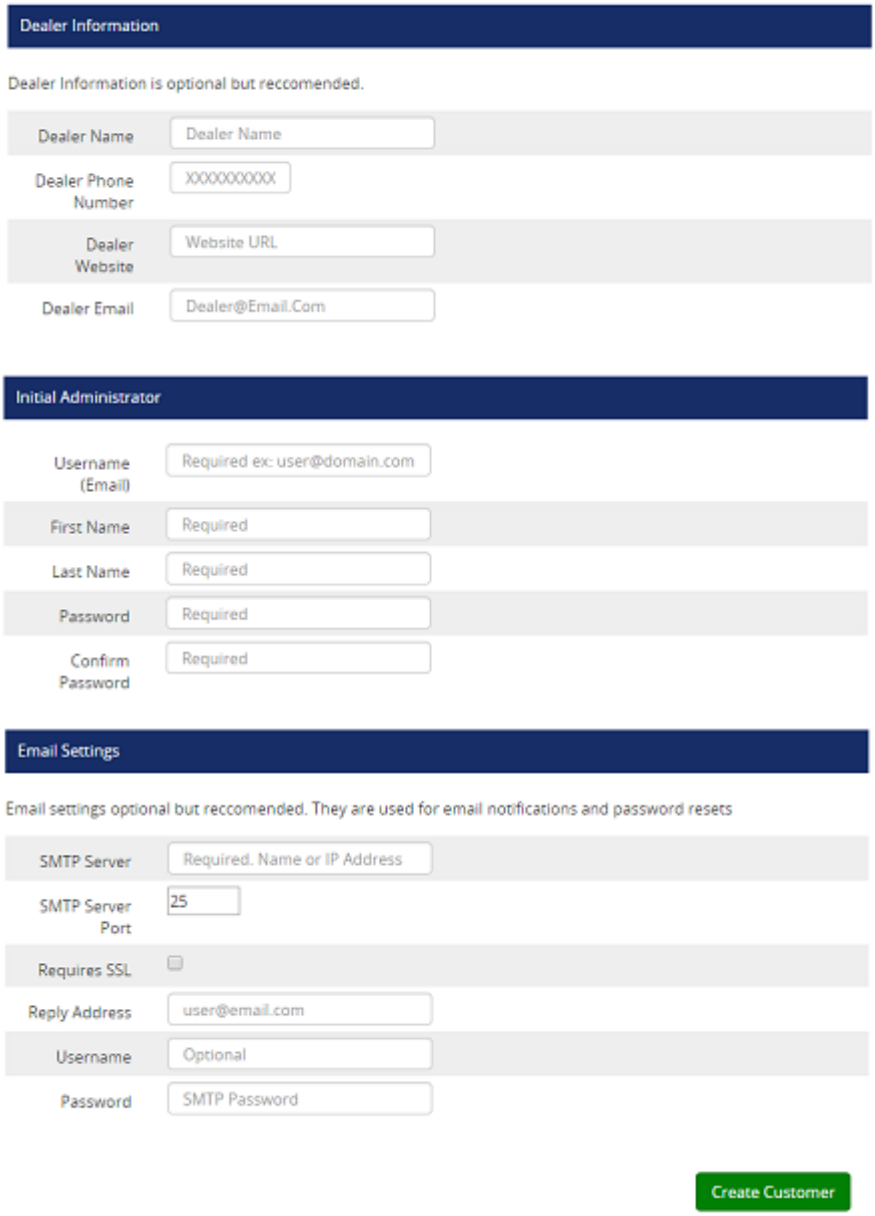
Protector.Net Initial Software Configuration

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

Access the Protector.Net 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, 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.





Connection Configuration

Table 3.1. Connection Configuration Fields

Field	Brief Description
Server Address	By default, the name of the PC Protector.Net was installed on. This field is what is pushed to your Panels and dictates 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.
Server Port	By default; 9876. This field is dictates what port the Panels will use to communicate with the server. Can be changed if the default port is being used by another service or proccess.

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.

Dealer Information

Note

Dealer Information is optional, but recommended.

Table 3.3. Dealer Information

Field	Breif 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: 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. Enter the full URL of the dealer website. Example: http://www.hartmann-controls.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 Protector.Net 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 User roles and system access.
First and Last Name	The first and last name of the primary Protector.Net 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. 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 send emails via SMTP (port 25 is common however your settings may vary).
Requires SSL	Check the Secure Socket Layer checkbox if your email client requires and uses SSL for encrypting email messages.
Reply Address	This is the email address email 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.

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, Protector.Net 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.

Panel Initial Configuration

This section will cover common initial configuration of Hartmann Controls PoE Over the Door Module (ODM), specifically; what communication method to use to reach the Protector.Net server. This section is focused on configuring communication information manually into the Panel. 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 Protector.Net software installed onto a PC or server with the Initial Configuration completed with a assigned email account name and valid password. We will refer to the PC with Protector.Net installed as the **Protector.Net Server**. Note the IP address or name of the Protector.Net server; as this is required during Panel Configuration.

From a hardware perspective, the Panel should either be mounted at its intended location or temporarily accessible physically near the Protector.Net server with a Cat5e/6 cable (non-crossover) connected directly to either a PoE Injector or powered network switch (Note: Maximum cable run from Protector.Net ODM to injector or powered switch is 100 metres or 330 feet).

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

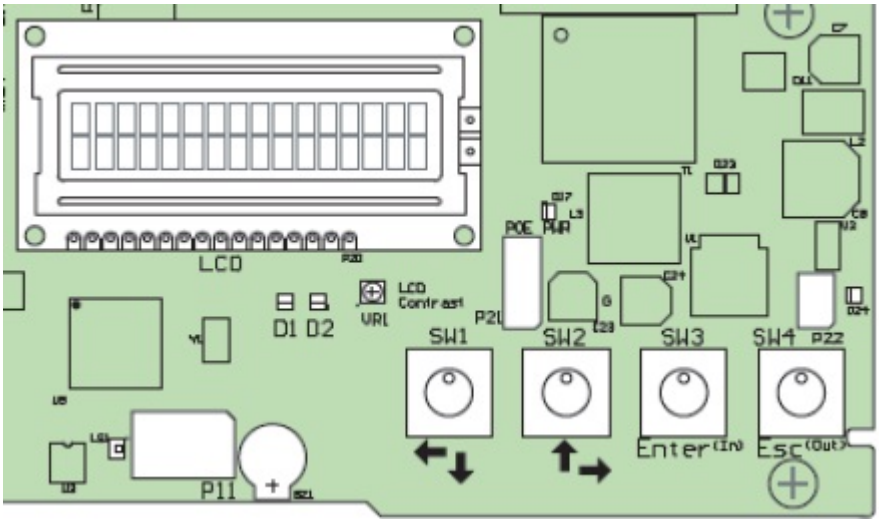
- The **Static IP** or **Server Name** of the Protector.Net server.
- Will this Panel be using **DHCP** or a **Static Address**?

- 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 Protector.Net controller for accessing, viewing and configuring a Panel.

Figure 3.1. Panel Buttons



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	18 WiFi Network Type
19 WiFi Security Mode	20 WiFi SSID Hidden
21 WiFi SSID	

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 Protector.Net or if the IT staff need 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 Protector.Net 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).

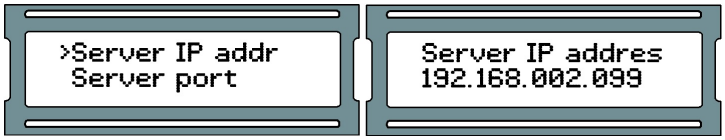
3. Using the white up and down buttons on the Panel, locate and set the indicating arrow on the LCD screen to 'SERVER CONN MODE' and then press the ENTER button.

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 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 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 Protector.Net 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 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 are 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.

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

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

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

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

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

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

Panel IP Settings: DHCP

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

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

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

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

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

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

6. Press ESC once more to save the configuration to flash memory. You'll 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 have already designated an IP for the Panel.

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

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

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 presented with 'setupsaved'

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 was 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.

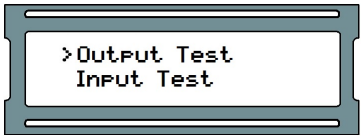
Output Test

This section includes detailed instructions on performing a Output test.

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 Input you'd like to test. Press ENTER and the highlighted zero will change to a 1, and the Output will be triggered. Press ENTER again to disengage the Output. When you are done testing, press the ESC button.

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

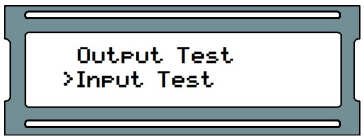
Input Test

This section includes detailed instructions on performing a Input test.

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

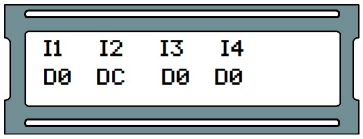
2. Press the ESC button. You should then be presented with a message on the LCD screen stating 'ACCESS GRANTED'. (Note: If there is no configuration activity for 60 seconds, the Panel will perform a forced logout).

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



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

5. If you have any Input devices such as Door contacts, REX; the Panel will beep and show you which Inputs are active. Inactive Inputs are D0 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 be see a message saying "Canceled'. You'll be returned to the option menu. You can now proceed with additional tests.

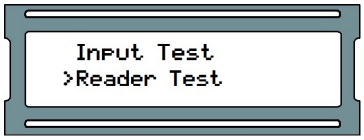
Reader Test

This section includes detailed instructions on performing a Reader test.

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

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

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



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

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

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

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 in the PoE Elevator Panel.

Each Panel has a configuration web interface that can be accessed through a web browser, as long as the client connecting to ths 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 '001EXXXXXXXXX'. 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 promoted 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 3.2. Panel HTTP Configuration Overview

There are three 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 Panel communication settings. **Wireless Setup** is where you can configure/ change wireless data for wireless Panel models.

Overview. On the overview page you can see Panel status and configuration. Some of the note worthy 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 Protector.Net software. If changing communication methods in the interface, we advise making those same changes in the Protector.Net software. The **Panel Setup** screen should only be used for initial configuration or when the server information has changed.

Adding a Panel to Protector.Net

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

Method 1: Adding a Panel Via Notification

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

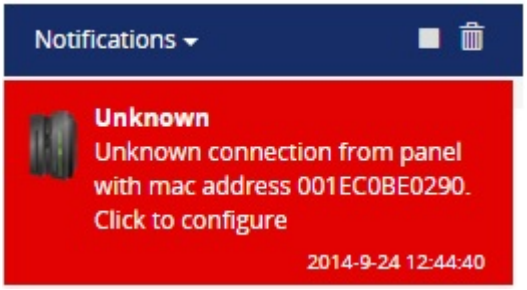
The Panel is configured to find the server by **Name** or **IP Address**. (Please see the section called “Panel IP Settings: Static IP” and the section called “Communication Mode Configuration: Server Name (DNS)” for details on configuring a Panel to find a Protector.Net server)

1. Access your Protector.Net 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**, pay attention to the **Notifications** section on the right side of the page.

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



5. This Notification indicates that the server was contacted by a Panel that the server is not aware of. The Notification will show the Mac address of the Panel trying to connect. If this address matches a Panel you'd like to configure, click on the Notification.
6. Once you click on the unknown Panel Notification, you'll be taken to the **Add Panel** screen with the **Mac Address** field pre-populated with the Mac address displayed in the Notification.
7. Please proceed to the section called “Adding a Panel: Basic Configuration” for continued instructions on adding a Panel.

Method 2: Adding a Panel Manually With Mac Address

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

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

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

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

Note

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

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

Adding a Panel: Basic Configuration

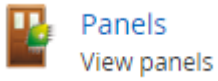
This section will cover the various fields that need to be populated in order to add a Panel in Protector.Net. It is advised to fill them in the order they are shown on the screen, the exception being the Mac address if it is pre-populated.

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

1. Access your Protector.Net 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.

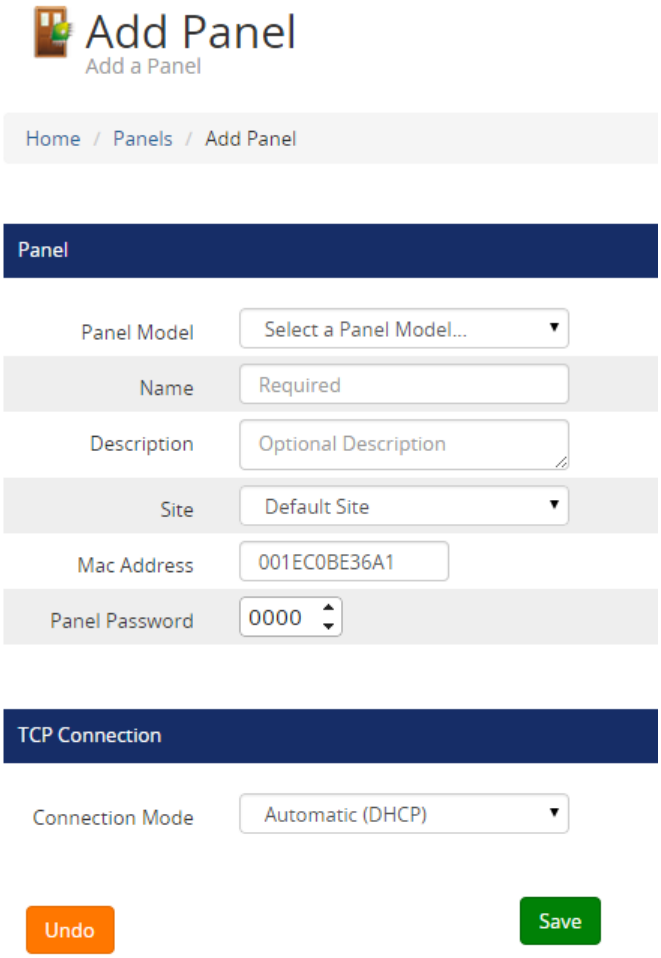
3. On the **Home Screen**, scroll down to the section titled **Hardware**, click on the **Panels** icon (pictured below).



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

On the **Add Panels** screen you'll be presented several drop-down menus, text fields and checkboxes to populate.

Figure 3.3. Add Panels Screen



The following table describes the common fields.

Table 3.8. Add Panel

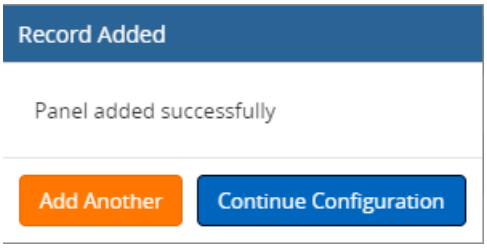
Drop-down/Text Box/Check box	Description
Panel Model	Select the Panel model using this drop-down menu, depending on the model you choose; additional options may be displayed.

Drop-down/Text Box/Check box	Description
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. The default value is '0000'.
TCP Connection: Connection Mode	The method in which the Panel receives its IP address, DHCP or Static. Selecting static will bring up additional fields to fill.

Note

If you've already configured the Panel with a static IP address, you'll need to enter this information after changing **Connection Mode** to **Static IP**.

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 Protector.Net licence 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 Protector.Net, 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 29, *Support*

Chapter 4. Software Licensing

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

The Protector.Net application is a end-user licensed software solution. This means in order to use the software you will at all times require a valid software license.

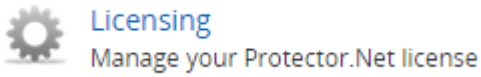
Note

Protector.Net includes a 1 year trial license on first install.

Licensing Your Software

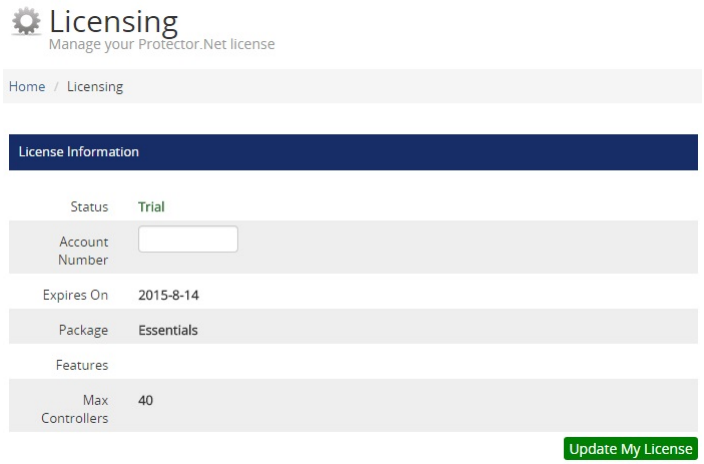
Activating the software license on your Protector.Net is designed to be a very straight forward and painless process.

1. Access your Protector.Net 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 #**' field. If not, this can be obtained by contacting Hartmann Controls (Please, see Chapter 29, *Support*).

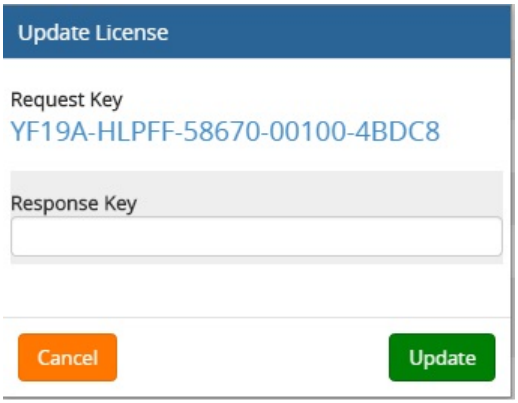
Figure 4.1. Protector.Net Licensing Screen



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

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

8. You will be presented with your new **Request Key**. Contact Hartmann Controls (Please, see Chapter 29, *Support*) with this request key. We will help determine with you the best license length and software package for your needs and in turn we will provide you with a response key, that will activate your software.



9. Once you have entered the **Response Key** provided by Hartmann Controls, click '**Update**' to activate your software.

Note

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

Supported Card Formats

Note

Protector.Net supports a variety of card bit formats, however for simplicity and added security, we recommend using our 40 bit high-security credentials. For more more information about other card formats and enabling them in your software licence (free of charge) please contact Hartmann Controls. See Chapter 29, *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 Protector.Net software will advise the software is about to expire and provide the exact expiry date.

Q: **What happens if my software expires?**

A: When the software expiry lapses, Protector.Net will automatically prevent any changes from being made to the system. Upon login you will be automatically presented with the licensing screen and this screen will prevent further access to the software until the licensing is updated. However during this period all Panels will retain their instruction set and continue to operate as previously configured.

Q: **Why does Protector.Net 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 Protector.Net feature set are offered a price inline with what they need.
- To allow us to continue to upgrade and enhance the base Protector.Net 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: We provide software licenses that are valid for 1 year, 5 years or Perpetual term licence. In addition, we also provide 4 levels of software packages which are Essentials, Small Business, Mid Business and Enterprise. Please contact Hartmann Controls for more information on these packages. (Please, see Chapter 29, *Support*)

Q: What does a Protector.Net license entitle me too?

A: An active Protector.Net license is always required to use the Protector.Net 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 Protector.Net software?

A: Upon restoring a Protector.Net database to a different computer it will automatically invalidate your license. You are however not charged a fee to license the new computer. Contact Hartmann Controls 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

Accessing the System Manager UI

Accessing the System Manager UI is a very similar procedure to accessing the Protector.Net application, 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 -> Protector.Net and finally clicking on **"Launch Protector.Net 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 Protector.Net System Manager'**. If you wish you can pin this shortcut permanently to your start screen by right clicking and selecting 'Pin To Start'

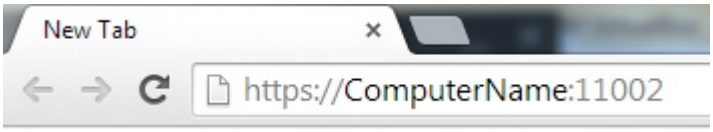
   Accessing System Manager UI from a Remote PC

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

   Alterntivly, you can also access the 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 Protector.Net **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

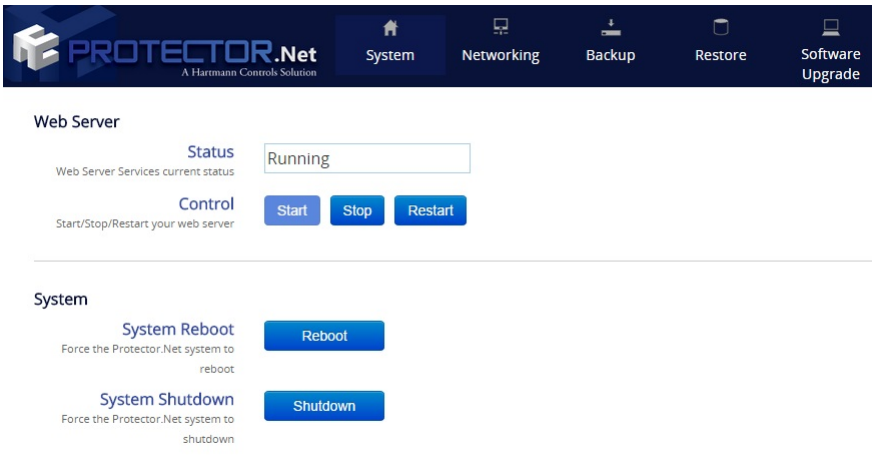
The default User-name is 'hc' and the default password is 'hcaccess' (case sensitive and without the quotes).

Caution

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

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

Figure 5.2. System Manager UI System Screen



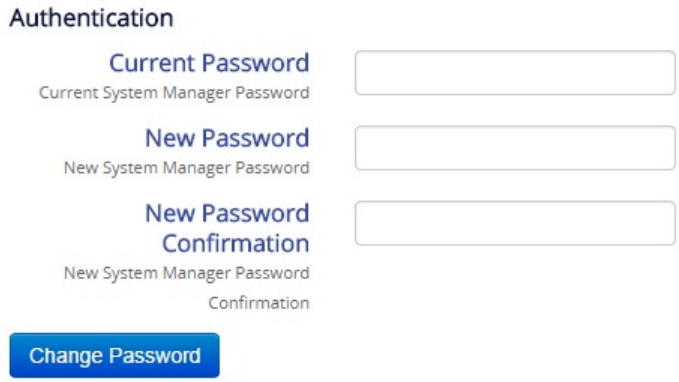
Changing Your Password

1. Access the **System Manager UI** (Please, see the section called “Accessing the System Manager UI”).

2. Click on '**System**' in the top menu.

3. On the **System Screen**, scroll down until you see '**Authentication**'.

Figure 5.3. Authentication Section



4. Enter your current password (default is 'hcaccess') followed by the new password twice.

5. Click **'Change Password'** to complete the password change procedure.

Service and System Management

The **System Manager UI** allows for control over the Protector.Net web server service. 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 service or to check if it is running.

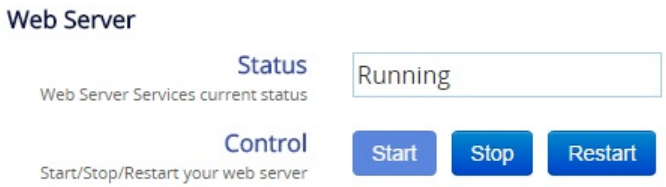
Managing Services

1. Access the **System Manager UI**. (Please, see the section called “Accessing the System Manager UI”)

2. Click on **'System'** in the top menu.

3. You will see a control section for the web server.

Figure 5.4. Managing Services



4. From here you may Start/Stop/Restart and see the status of the web service

Shutting Down or Restarting Your Server

1. Access the **System Manager UI**. (Please, see the section called “Accessing the System Manager UI”)

2. Click on **'System'** in the top menu.

3. Scroll down until you see the section labeled **'System'.**

Figure 5.5. Shutting down or Restarting your server.

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

Networking

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 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 Protector.Net 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.

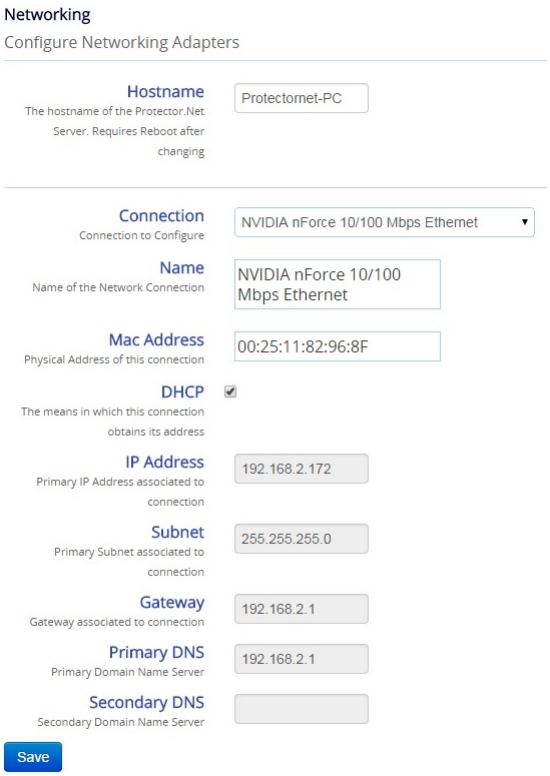
Configuring Your Network

1. Access the **System Manager UI** (Please, see the section called “Accessing the System Manager UI”) .

2. Click on '**Networking**' in the top menu.

3. You will now be presented with the network configuration page.

Figure 5.6. Network Configuration Page



Note

Changing your host-name will require a system restart.

Backing up your Protector.Net 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.
   - **Database**

     The Protector.Net database (recommended).
   - **Profile Pictures**

     Images associated with your Users (cardholders) (recommended).
4. Select your backup options.
   - **Compress Backup**

     Determines whether the backup file is compressed upon successful backup (recommended).
   - **Remove Files Older then X Days**

     Automatically removes .prbak files from the backup location if the age exceeds the number of days specified.

- **Encrypt Backup with password**

  Should a password be placed on the backup. The password will be required to restore the backup.

5. Determine your backup user. This is generally used when the host computer belongs to a domain and the backup is being written to a network share. In the case of backing up to USB, this is not required and should be left blank.

6. Determine where you backup will be backed up to. We offer support for either a local USB drive or a network share.

Backup to USB Drive

- Select **'USB Drive'** in the **'Output To'** drop-down list.

- The drop-down on the right will refresh and show a list of detected system drives. Select the appropriate drive.

Note

If you don't see the drive listed refresh your browser (F5) to force the System Manager to re-detect your drives.

Backup to Network Share

Caution

Network share is only supported when the computer is a member of a domain and a backup user with appropriate privileges to write to the network share is specified. Alternatively you can use a network share with public read/write privileges but this is not recommended.

- Select **'Network Share'** in the **'Output To'** drop-down list.

- Enter the path of your network share without the proceeding '\\' .

Example 5.2. Network Share Example

Servername\PathToMyBackupShare

7. Select a Backup Schedule.

   - **Disabled:** No automatic schedule. Backup is invoked by hitting the **'Save and Run Now'** button.

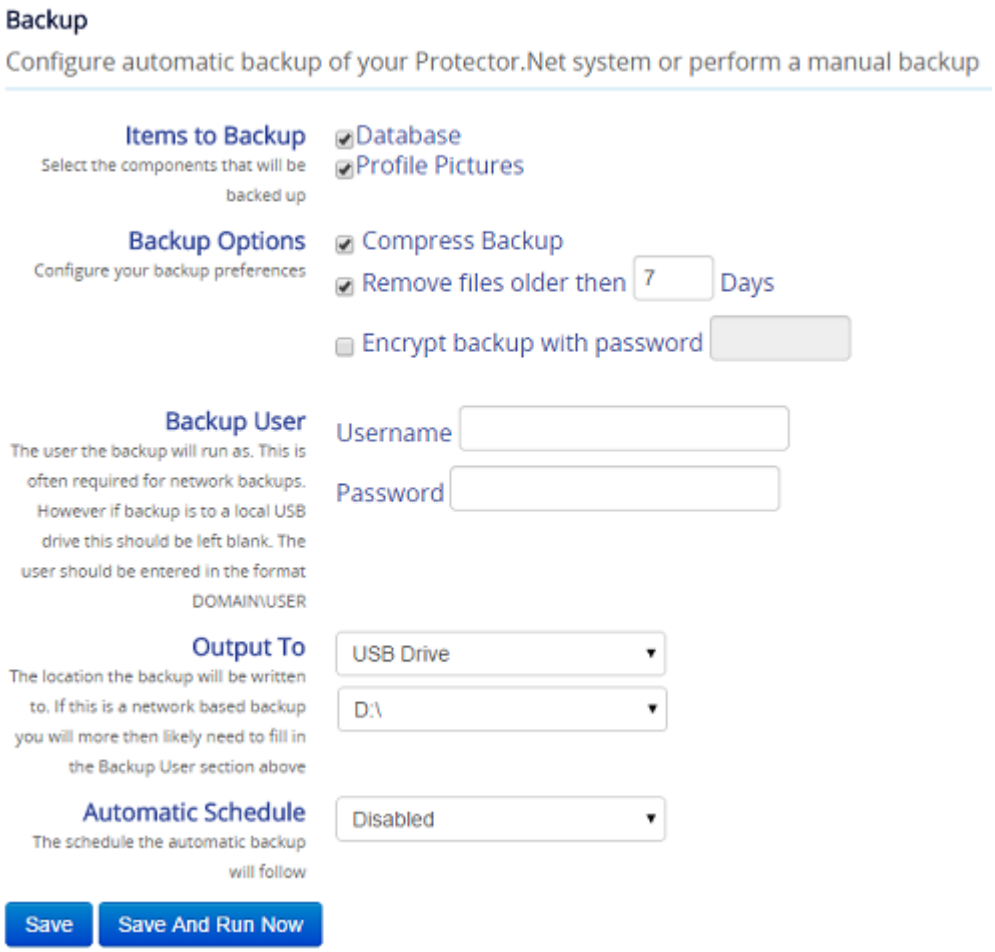
   - **Daily:** Backup occurs once a day at the time specified.

   - **Weekly:** Backup occurs once a week on the day of week and time specified.

   - **Monthly:** Backup occurs once a month on the day and time specified.

8. 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).

Figure 5.7. 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 Protector.Net Database

Warning

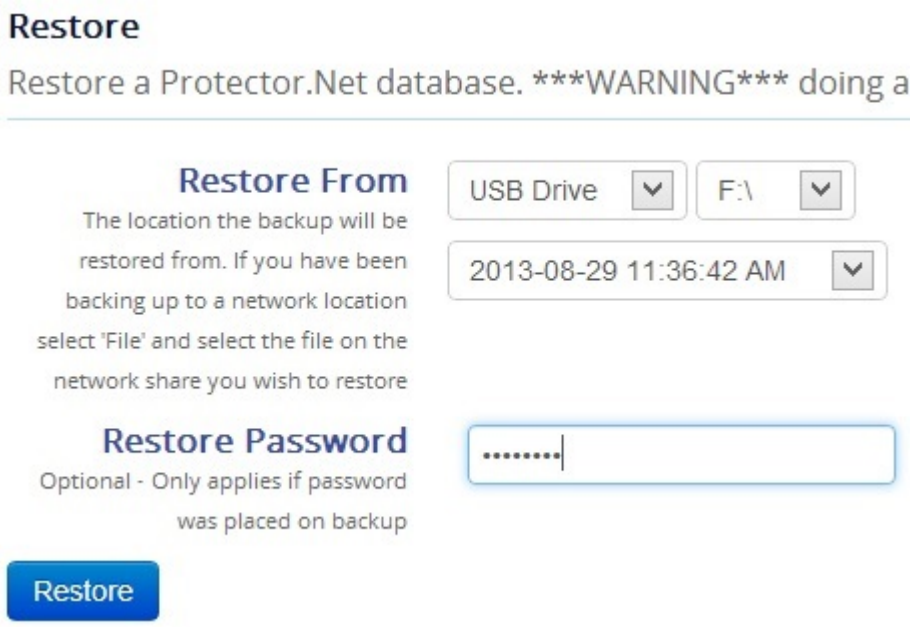
Ensure you stop your Web Server service before attempting a restore. Failure to do so may cause errors during restore and/or data loss. For instructions on stopping the Protector.Net service, please see the section called “Service and System Management”.

1. Access the System Manager UI (Please, see the section called “Accessing the System Manager UI”).

2. Click on '**Restore**' in the top menu.

3. You may restore from either a USB Drive or by manually selecting the .prbak file on your local PC.

Restoring from USB Drive

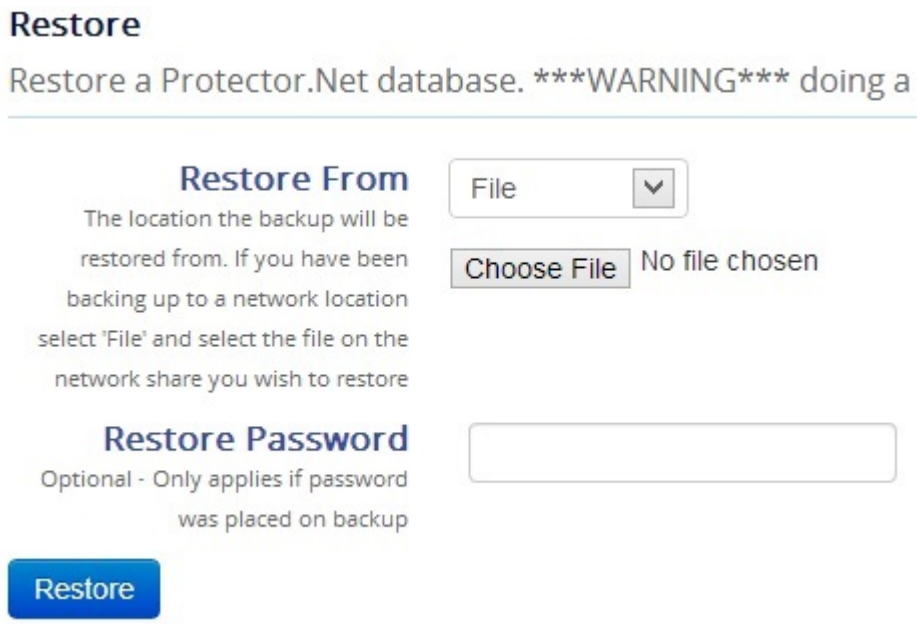


- Select **'USB Drive'** in the first drop-down list.
- The drop-down on the right will refresh and show a list of detected system drives. Select the appropriate drive.

> **Note**
>
> If you don't see the drive listed refresh your browser (F5) to force the System Manager to re-detect your drives.

- Select the File to restore from the bottom drop-down box (if more than one backup is detected on the USB drive).
- Optionally enter the password if a password was used during backup.
- Click the **'Restore'** button.

Restoring from Local Drive



- Select '**File**' in the first drop-down list.
- Click '**Choose File**', browse and select the appropriate file to restore.
- Optionally enter the password if a password was used during backup.
- Click the '**Restore**' button.

Note

If you are having trouble restoring database backups 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”.

Chapter 6. Planning an Access Control Deployment

This chapter is meant to help technicians in their planning stages of Protector.Net 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 Chapter 30, *Visual Guides*.

Hardware

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

Hardware Specifications - Protector.Net POE ODM

Table 6.1. Hardware Specifications

Category	Item and Description
Power	
Supply	802.3af PoE / PoE+ (providing up to 20 W)
Lock Power	Solid State 12VDC 500mA / 24 VDC 250 mA (with opt. converter)
Auxiliary Output	12 VDC 200mA
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 500mA limit)
Inputs	4 x Supervisor or Digital (REX, Door Contact, HDCP Opener, Auxiliary)
Reader	
Reader Port	2 x Wiegand (D0, D1, BUZ, LED, VCC, GND)
User Interface	
LED's	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

Category	Item and Description
Push Buttons	4 x Tactile Switch
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-Colour 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, Off-White 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
Expansion Boards	Extra Memory, Elevator Expander Panels, I/O’s(for future expandability)
RS-485 Plug-In Module	Used for communicating with Assa Abloy Aperio products and the Elevator Expander Boards.

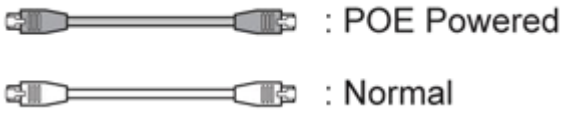
Communication Topology

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

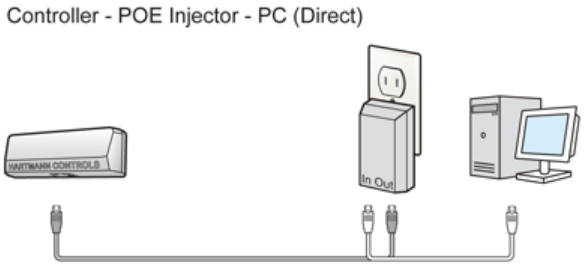
Hartmann Controls Over The Door (ODM) are powered by Power Over Ethernet (PoE). This power is provided via either a PoE network switch or a PoE injector. The ODM communicates by TCP/IP over Cat5e/Cat6 cable, often through the same cable it receives power from.

Below we have several configuration examples of how the ODM communicates over a variety of network infrastructures.

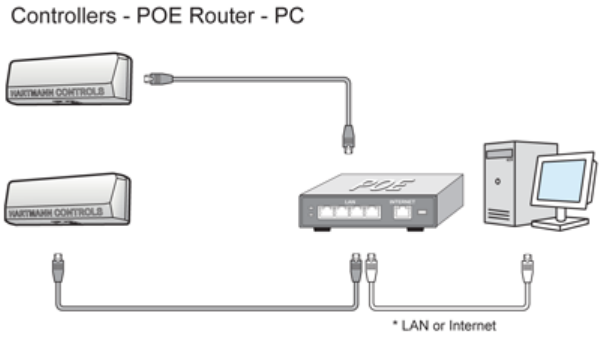
PoE Power. PoE Power may be supplied directly by switch or alternatively injected via single port injector between switch/router and ODM Panel.



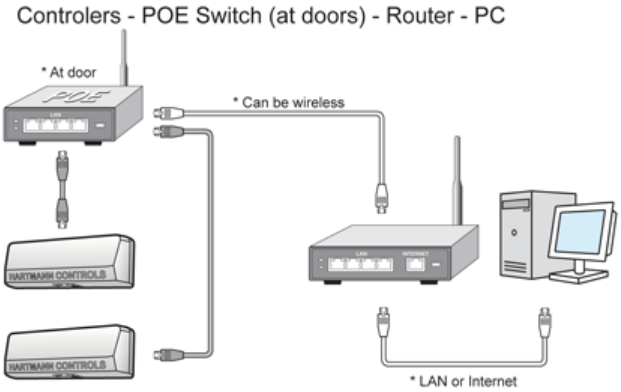
Controller - PoE Injector - PC (direct). In this scenario, the ODM is being powered by a PoE injector which is connected right to the Protector.Net server. Scenarios like this happen a lot when there isn't very much network infrastructure to work with.



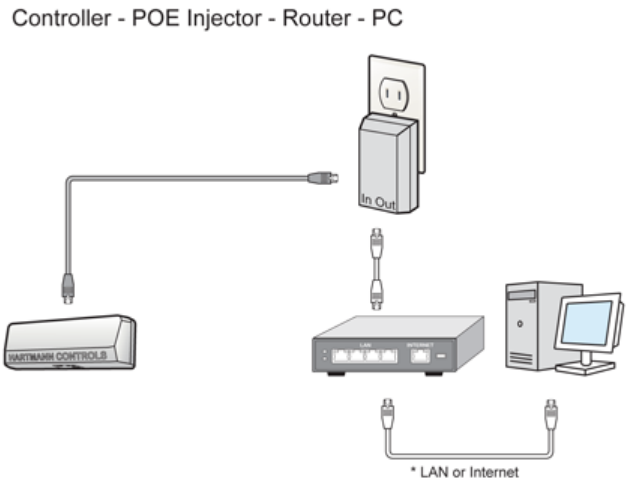
Controllers - PoE Switch/Router - PC. This is a more typical scenario and is seen quite often in the field. The ODM Panels are powered by a PoE switch (located in a closet or electrical room), which connects to the on site server using the site's existing network infrastructure, or an off-site server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



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



Controller - PoE Injector - Router/Switch - PC. In this scenario, the ODM 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 its not cost-effective to buy a PoE switch.



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

Cables, Standards and Best Practices

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

Cable Specifications and Standards

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

Table 6.2. 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

Identifying a Panel

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

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

Table 6.3. Panel Model Reference

Model	Max Doors	Max Readers	Motion REX	Brief Explanation
POE-ODM-X	1	2	No	Over The Door Module with PoE Power

Model	Max Doors	Max Readers	Motion REX	Brief Explanation
POE-ODM-M	1	1	Yes	Over The Door Module with PoE Power and Integrated Motion
POE-TDM	2	2	No	Two Door Module with PoE Power
POE-TDM-M	2	2	Yes	Two Door Module with PoE Power and Integrated Motion
POE-APERIO-2	2	2	No	ASSA ABLOY Aperio master controller capable of controlling up to 2 Aperio devices via 1 - 2 Aperio Hubs
POE-APERIO-4	4	4	No	ASSA ABLOY Aperio master controller capable of controlling up to 4 Aperio devices via 1 - 4 Aperio Hubs
POE-APERIO-8	8	8	No	ASSA ABLOY Aperio master controller capable of controlling up to 8 Aperio devices via 1 - 8 Aperio Hubs
POE-Elevator-64	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.

All Hartmann Controls Panels are fully tested prior to shipping, and after the testing is successful the Panel receives the Hartmann Controls seal of approval in the form of a sticker on the Panel to the right of the LCD screen. This sticker contains the model number and the date of the Panel batch.

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 Protector.Net. 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 Protector.Net 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.

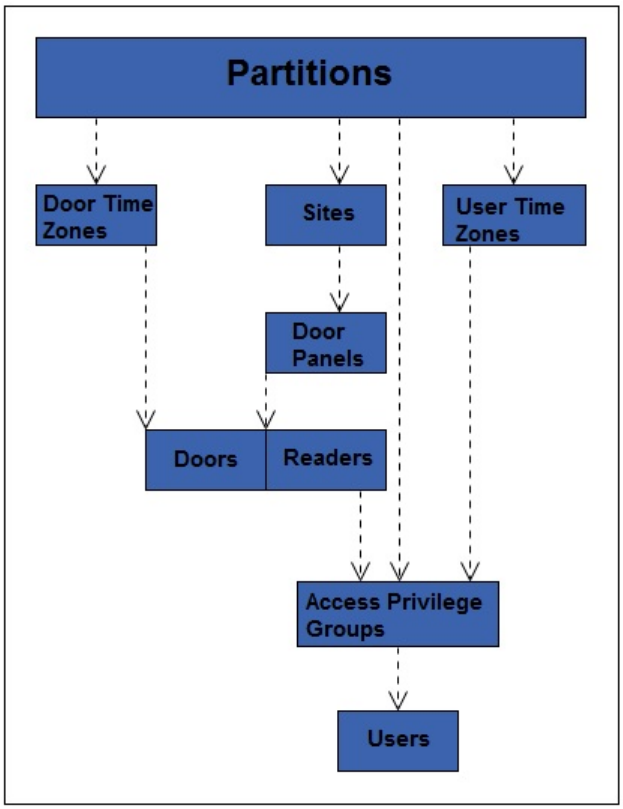
Table 6.4. Order of Operations: Software Configuration

#	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.

#	Configuration Item	Configuration Order	Additional Notes
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 massaged 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, User access 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 6.1. Protector.Net Order of Configuration



Partitions

In this section we will cover the basic concepts of **Partitioning** within the Protector.Net. 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 Protector.Net; 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 Protector.Net 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 Hartmann Controls 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 Protector.Net Panels configured in three different schools (A, B and C), with a single Protector.Net 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 Protector.Net 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 Hartmann Controls ODM Panels 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 Protector.Net.

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 Hartmann Controls 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 choose to use Protector.Net to manage their doors in offices and facilities. Using Sites; the building manager creates a Site for the town hall, water management buildings, fire stations and even community centers. Sites and Partitions can be used in this scenario to simplify management and create logical separators. For example, the community center would likely be its own Partition, and could be managed by on site staff while still maintaining a central authority at city hall.

Door Time Zones

In this section we'll cover the concepts of **Door Time Zones** within Protector.Net 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 Protector.Net 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 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 grey 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 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:

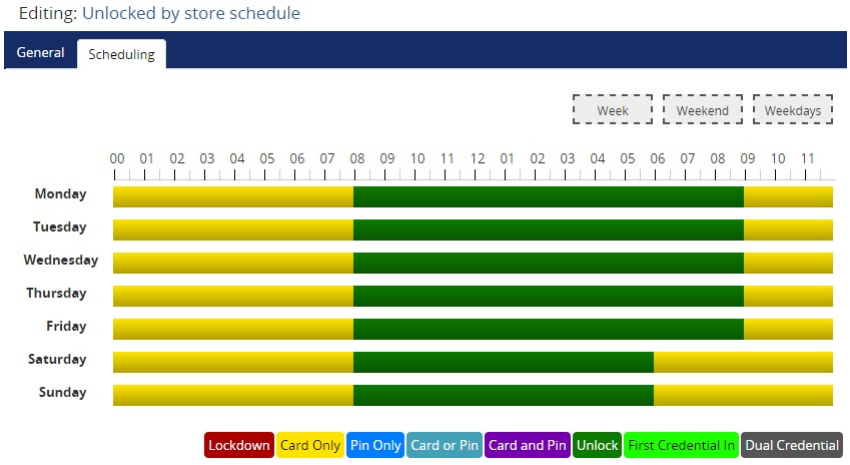
- Will the deployment have a public Door? If so when should that Door change to a locked state? Should that Door use **First Card In**?
- Is the deployment using combination prox/keypads? Do any of these Doors require **Card AND Pin/ Card OR Pin/Pin Only**?
- Is there any ultra secure locations within 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.

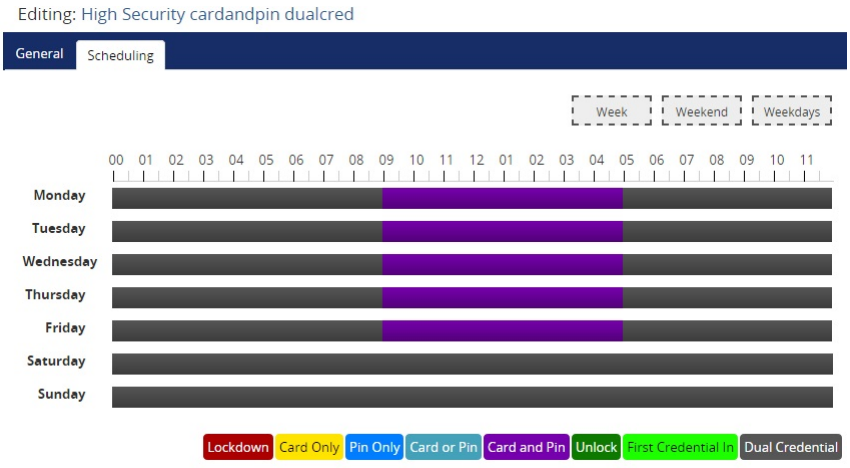
Examples

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.

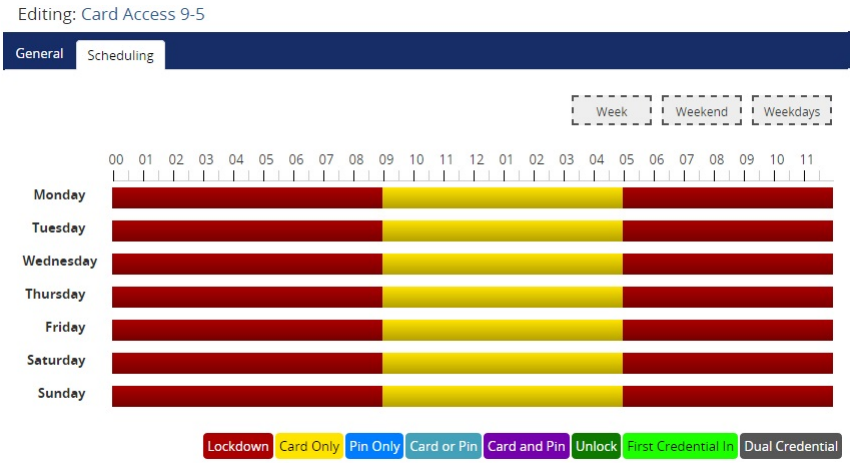
Example 1: Grocery Store Public Entrance. In this example, we have a Door Time Zoned that will be assigned to the front public Door of a grocery store, it is set up to **Unlock** during store hours, and card only otherwise for staff.



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 Protector.Net.



User Time Zones

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

Concepts

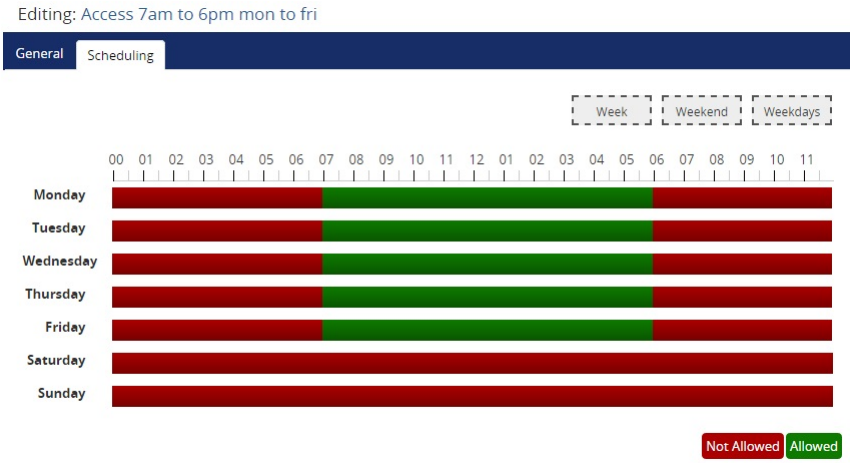
Similar to Door Time Zones; User Time Zones are the method in which Users are validated if they have access to a specific Reader.**(Access** or **No Access**.) The only exception that would affect an Allowed access and prevent the cardholder from being granted access is when the particular Door is currently 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; Protector.Net 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** (APG's), and what their role is in Protector.Net. For instructions on how to configure Access privilege Groups, see Chapter 11, *Access Privilege Groups*.

Concepts

Access Privilege Groups in Protector.Net 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 Protector.Net unique from other systems; is that Users can be part of more than one Access Group. This gives us the flexibility to create APG's based on similar Doors and assign an individual User to multiple APG's 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, ect..)
- 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). These style of groups are based on the type of Users in the group. Such as:

Table 6.5. 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 Protector.Net; 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 6.6. 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, 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 APG's as User based. The important part is to communicate to your client about their needs, and build effective APG's 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 Protector.Net. This section will cover concepts and some examples. For configuration of Holidays please see Chapter 13, *Holiday Configuration*.

Holidays within Protector.Net 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 Timezones 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, Protector.Net 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, Protector.Net 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, Protector.Net 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, Protector.Net 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, Protector.Net 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 effected by this Holiday? (For example, Sites in other countries where the Holiday may not be present)
- Should this Holiday effect 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

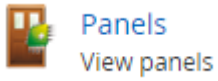
This section covers configuration aspects of Panels after the Panel has been added to the software. Once the Panel is added, additional configuration options are available such as the Input/Output configuration.

To get to the Panel advanced settings:

1. Access your Protector.Net 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.

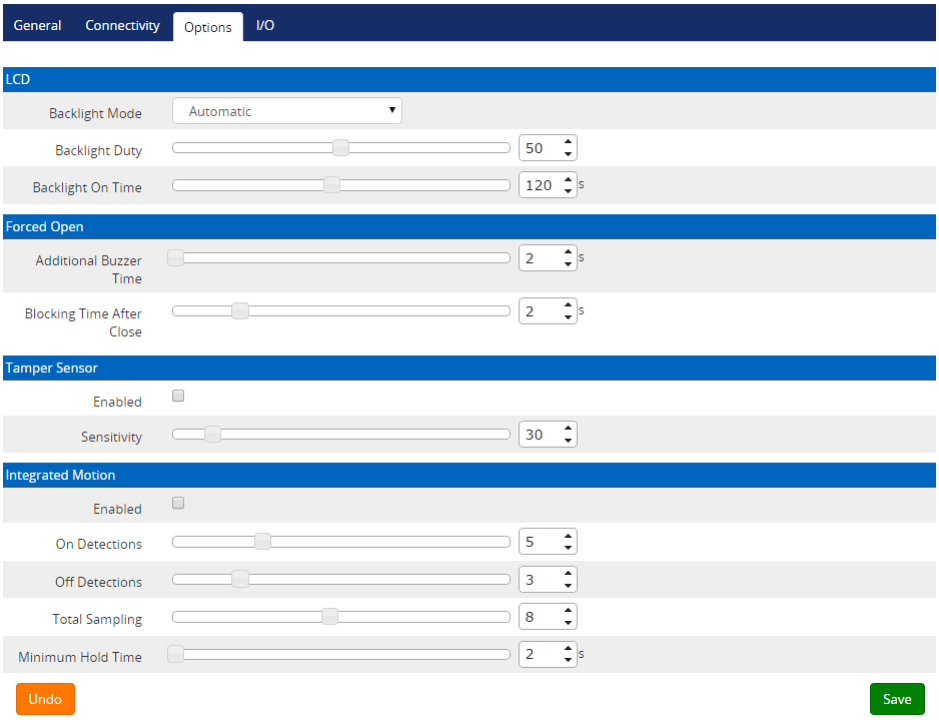
5. On the **Edit Panel** screen, there are four tabs. The **General** and **Connectivity** tabs are what we configured when adding the Panel. Most of these options can be modified as needed. The **Options** and **I/O** tabs are automatically filled based on which Panel model you selected when adding the Panel. These settings will be covered in the next section.

Note

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

Options

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



The **Options** tab is divided into 4 sections: **LCD**, **Forced Open**, **Tamper Sensor** and **Integrated Motion**. Each section has several slider bars that are used to easily change the settings. You can also use the textbox next to the slider to manually enter a value.

Table 7.1. Options Tab

Configuration Item	Description
LCD	
Backlight Mode	The operating mode of the Panel integrated LCD. Values are Automatic, Always On, Always Off.
Backlight Duty	The light level of the Panels integrated LCD. Increments by 1. Valid values are 0 to 100.
Backlight On Time	The time the Panels integrated LCD backlight will stay active after receiving User Input. Increments by 1 s. Valid values are 0 s to 254 s.
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.

Configuration Item	Description
Integrated Motion	
Enabled	Enable/Disable the integrated Motion Sensor (if applicable).
On Detections	Motion On Detections. Increments by 1 . Valid values are 1 to 16 .
Off Detections	Motion Off Detections. Increments by 1 .Valid values are 0 to 15 .
Motion Total Sampling	Motion Total Sampling. Increments by 1 . Valid values are 1 to 16 .
Minimum Hold Time	Motion Minimum Hold Time. Increments by 1 s. Valid values are 0 s to 255 s.
Anti-passback	
Reset Anti-passback At Midnight	If enabled, Local Anti-passback will be reset at midnight.

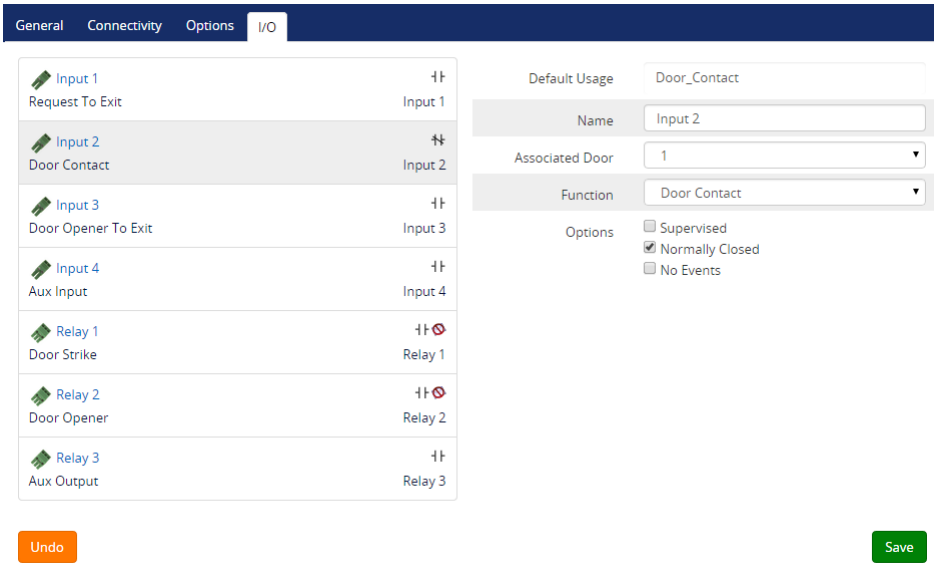
Note

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

Input/Output Configuration

This section covers configuration options in the **Input/Output(I/O)** tab. Depending on the Panel model selected when adding the Panel, the software will change what the default values are. For example: If you add a POE-TDM; Output 1 and Output 2 will both be mapped as Door strikes. The I/O tab is unavailable on Elevator Panels.

Figure 7.1. ODM 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 grey) 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 TDM Door Controllers)
- Function, see below

- If the Output/Input is Normally Closed/Open
- Disable/enabled Events for this Output/Input

The following chart will go over the 10 different Input functions and the 8 different Output functions.

Table 7.2. Input/Output Functions

Function	Description
Input Functions	
Disabled	The Input is disabled and will not react to any Input state changes on the selected Input.
Request To Exit	This function allows the Input to be used as a REX. This will allow a push button or other Input to unlock the Door.
Door Contact	This Input function is used for Inputs that track if the Door is open or closed. Should be disabled if not in use.
Door Opener To Exit	This type if Input is generally used for handicap 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. Integrated Motion must be disabled in Panel Configuration Options tab.
Aux Input	This Input function has the most configurable options. Including Input actions such as pulsing Outputs, overriding Doors, activating alarms. Aux Input actions are covered in more detail in the section called “Aux Input Configuration”.
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 if Input is generally used for handicap operators for activating auto Door openers. Automatic Opener must be enabled in Door Configuration Options.
Does Not Exist	Used to disable an Input, also placed by default on Inputs that are not usable on specific Panel models.
Output Functions	
Disabled	The Output is disabled and will not fire, even if instructed to by override.
Door Strike	Used to define an Input 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.
Alarm Interface	This Output is connected to an Input on the Panel capable of arming the alarm system, the alarm can now be armed using a triple swipe command. For more information on triple swipe scenarios please see Chapter 17, *Triple Swipe Features*.
Aux Output	An Output that can be triggered from Input changes or through triple swipe commands.

Function	Description
Secondary Door Strike	Setting a 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.
Does Not Exist	Used to disable an Output, also placed by default on Outputs that are not usable on specific Panel models.

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 Configuration

This section covers additional actions that can be programmed into an **Aux Input** in Protector.Net.

Table 7.3. Aux Input Actions

Input Action	Description
Activate Selected Output	Allows the Input to activate a 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 a Output (selectable from drop-down menu).
Toggle Selected Output	Allows the Input to toggle a 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 a 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 a Output (selectable from drop-down menu) with a 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 a Output (selectable from drop-down menu) with a audible alert that the Output was deactivated.
Toggle Selected Output with Sound	Allows the Input to toggle a Output (selectable from drop-down menu) with a 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 a 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 a Output (selectable from drop-down menu) for 1.5 seconds with a 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 a 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 a Output that is assigned as an alarm interface.
Toggle Alarm Interface	Allows an Input (such as a button) to activate a Output that is assigned as an alarm interface. The circuit changes to a closed state for 1.5

Input Action	Description
	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 a Output that is assigned as an alarm interface with a 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 a Output that is assigned as an alarm interface with a audible alert.
Toggle Alarm Interface with Sound	Allows an Input (such as a button) to activate a Output that is assigned as an alarm interface with a 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.
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”.

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 Protector.Net software. Simply click the update Panels button on the top right of the page (pictured below).

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.

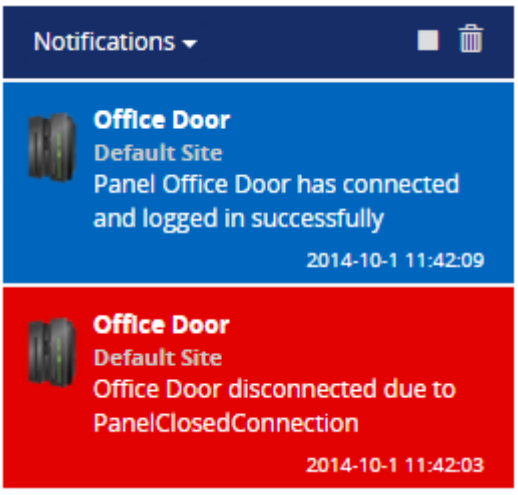
- Is the correct server address or name in Home>System Settings>Server Address:
- Are your Panels using Door contacts? If not, have they been disabled in the Panel configuration I/O tab?
- If you're doing additional work on the physical Panel, it may be helpful to temporarily disable the Tamper Sensor,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

When you click on Update Panels, you'll be promoted 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 7.2. Panel Update Status Window

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

Figure 7.3. 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.

Panel Firmware Updates

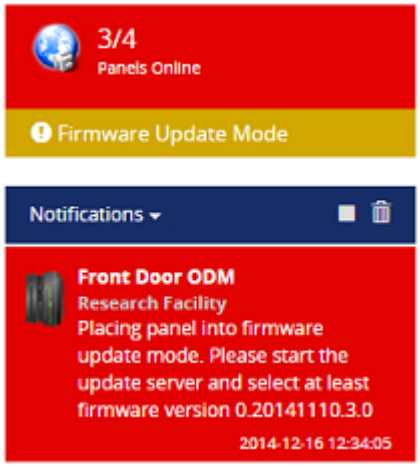
Periodically we enhance the Protector.Net, and often firmware upgrades to your Panels will be required with the software updates. Updating a Panels firmware is a relatively straight forward process.

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 only update one Panel at a time.

1. When a Panel attempts to connect to the Protector.Net application and the firmware is found to be out of date, you will see a Notification within the Notification window, along with a indicator that a panel is in Update mode above the notification window.

Figure 7.4. Firmware Out of Date Notification



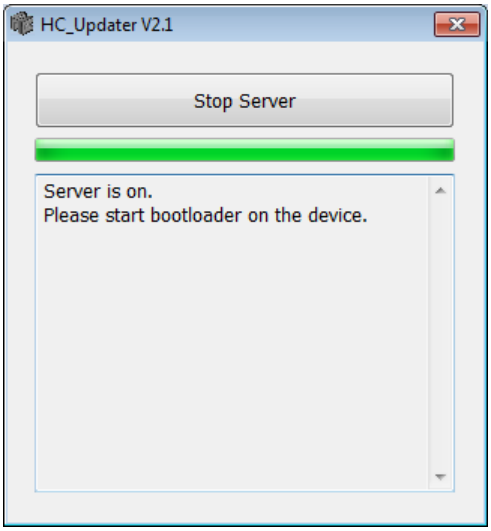
2. If no other Panels are currently in firmware update mode the Panel will be automatically placed into firmware update mode. If another Panel is currently updating the Panel will be disconnected from the server (but still fully functional) until the currently updating Panel is complete.

3. In order to update your Panel you will need to launch the Firmware Update Utility located within your start menu. The link for the firmware update utility can be located by clicking Start -> All Programs -> Protector.Net and finally clicking on **"Firmware Update Utility"**.

Windows 8/8.1 Users

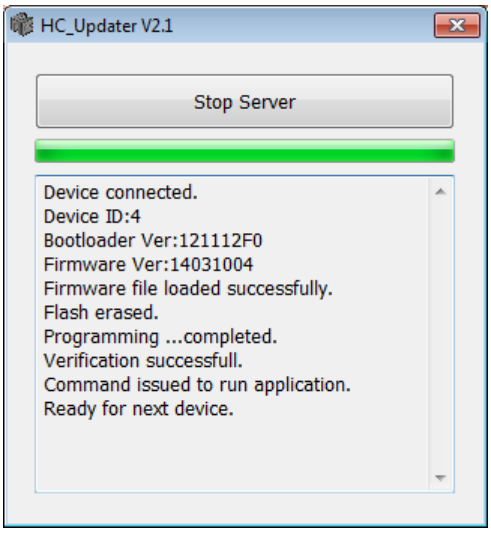
Windows 8/8.1 hides the shortcut by default within the Modern UI start screen. The shortcut can be located by typing 'Firmware Update' within the start screen and selecting 'Firmware Update Utility'. If you wish you can pin this shortcut permanently to your start screen by right clicking and selecting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

Figure 7.5. HCUpdater Utility



4. The HCUpdater application 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 firmware update utility will instruct the Panel to disconnect, at which point the Panel will resume normal operation and the firmware update utility will begin listening for the next Panel.

Figure 7.6. HCUpdater Utility Successful Update



5. Once all of your Panels are online within the Protector.Net application and you are no longer seeing 'Firmware Out of Date Notifications', you may close the firmware update utility.

6. After Panels firmware have been 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 Doesn't Connect to HCupdater. If the Panel does not connect to the firmware update utility after being placed into update mode by our software, 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. If these obsoletes appear clear but there is still no connection to the Firmware Updater:

1. Open HCUpdater from the start menu.

2. You will need physical access to the Panel. Unplug the Cat5 cable to the Panel, press and HOLD SW3 (enter). While holding SW3, plug the Cat5 back into the Panel. Once it powers up and you see the LCD change from 'SW3: Stored IP' to 'Panel IP', release SW3. You have now manually placed the Panel into firmware update mode.

3. Check the HCUpdater utility for activity. When the update is successful you may resume normal operation.

If none of the above results in the Panel successfully updating, please contact Hartmann Controls support. See Chapter 29, *Support*.

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*.

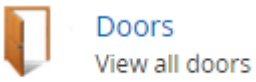
Adding a Door

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 Protector.Net 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.

Table 8.1. Add a Door

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.
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 ODM, one port will be available. If this is a TDM 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 its 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

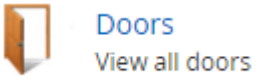
Text Box/ Drop-down Menu	Description
	motion on the Panel advanced settings. Once disabled fill in the Reader 2 fields.

6. Once all the required fields are filled, click the **Save** button to add the Door. You'll be promoted 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 as been added. For information about adding a Door, please see the section called “Adding a 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 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. On the **General** tab, are the main settings we configured when adding the Door. All of these can be changed if required.

Options

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

The first two checkboxes are miscellaneous options:

Play Sound on Open.

If checked, the Panel will play an audible indicator when the Door opens (requires Door contact).

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.

Timers

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

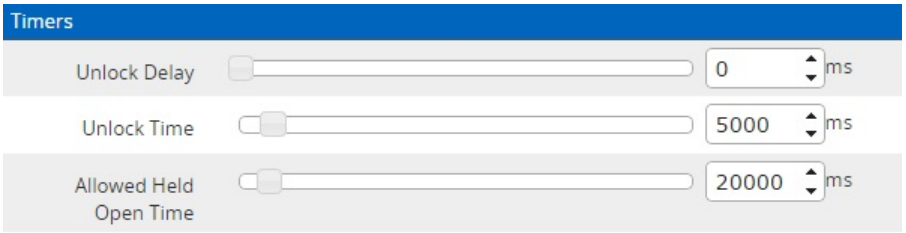


Table 8.2. Timers

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.

Automatic Opener

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

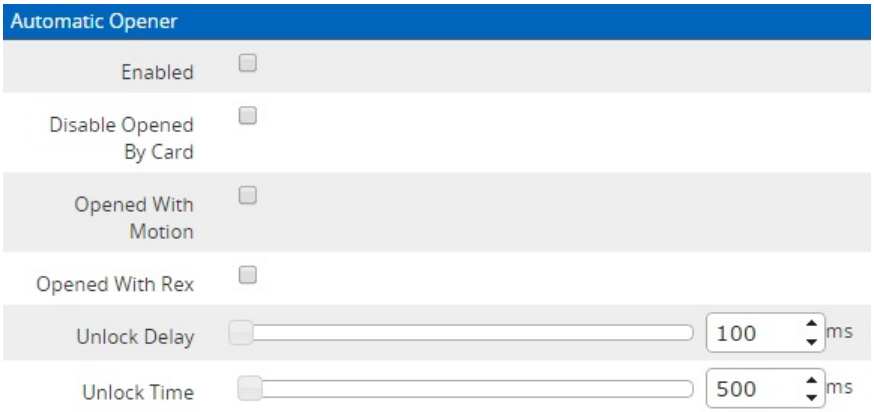


Table 8.3. Automatic Opener

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.
Unlock Delay	Automatic Opener Unlock Delay. Increments by 100 ms. Valid values are 100 ms to 1000 ms.
Unlock Time	Automatic Opener Unlock Time. Increments by 100 ms. Valid values are 100 ms to 20000 ms.

Disable

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

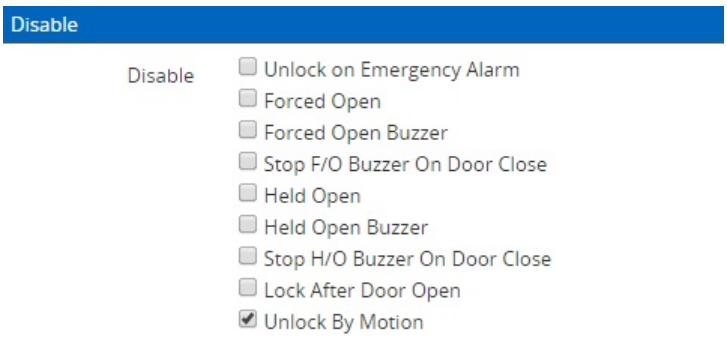


Table 8.4. Disable

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

Table 8.5. Reader Configuration Options

Configuration Item	Description
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.

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

This section covers the basics configuring the triple swipe feature. 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. For more information on User configuration, please see the section called “User Privileges ”.

Local Anti-passback

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

Chapter 9. Door Time Zone Configuration

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

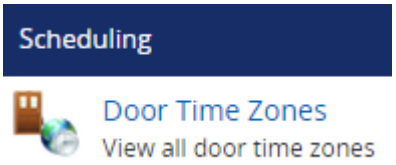
Adding a Door Time Zone

Adding a Door Time Zone in Protector.Net 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. This section covers how to add a new Door Time Zone

1. Access your Protector.Net 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.

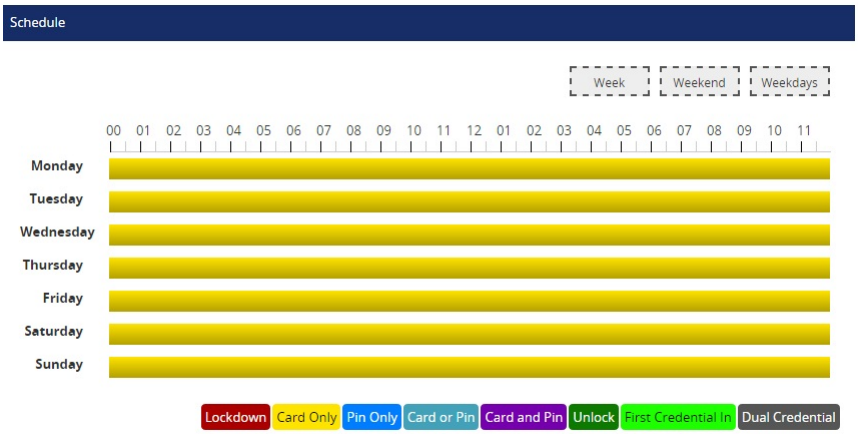
5. On the **Add Door Time Zone** screen, you'll have a couple text boxes to populate.

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.

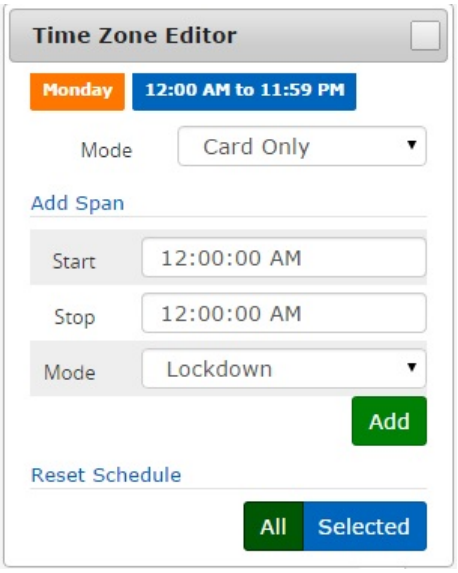
6. Creating the **Schedule** is the last step in creating a Door Time Zone. Below is what the schedule part of the add time zone page looks like.

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** 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 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 colour 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

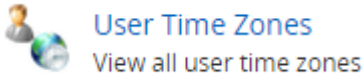
This chapter covers how to add additional User Time Zones to Protector.Net. For more information on what a User Time Zone is, please see the section called “Concepts”.

Adding a **User Time Zone** in Protector.Net closely resembles how we add other time zones in the software such as **Door Time Zones** and **Floor Time Zones**. The main differences being that these time zones are applied to Users through **Access Privilege Groups** and only have two possible states. **Allowed** and **Not Allowed**.

1. Access your Protector.Net 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 timezones can be renamed and massaged 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.

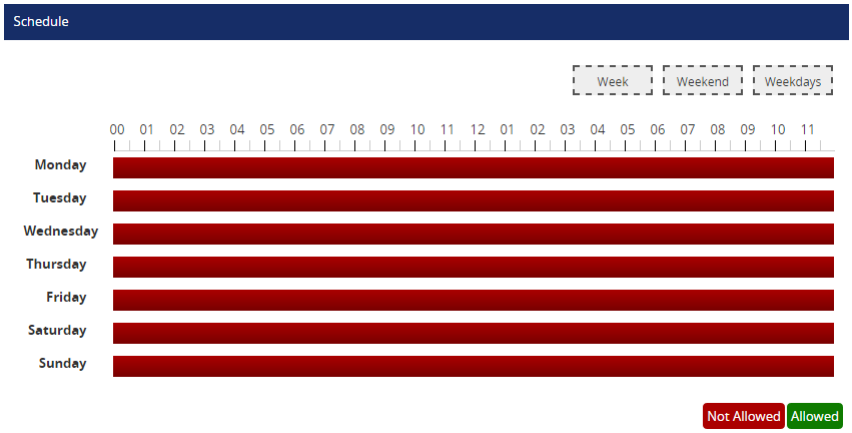
5. On the **Add User Time Zone** screen, You'll have a few text boxes to populate.

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.

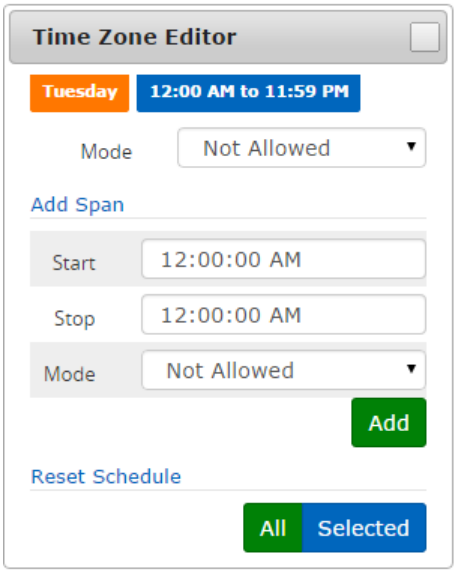
6. Schedule: Creating the schedule is the last step in creating a User Time Zone. Below is what the schedule part of the Add Time Zone page looks like.

Figure 10.1. User Time Zone Schedule



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 10.2. Time Zone Editor



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

9. The **Add Span** section of the time zone editor has 3 fields used for adding a User 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 User 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 colour 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 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 Protector.Net. If you'd like more information about planning an Access Privilege Group and example scenarios, please see the section called “Concepts”.

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

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

1. Access your Protector.Net 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.

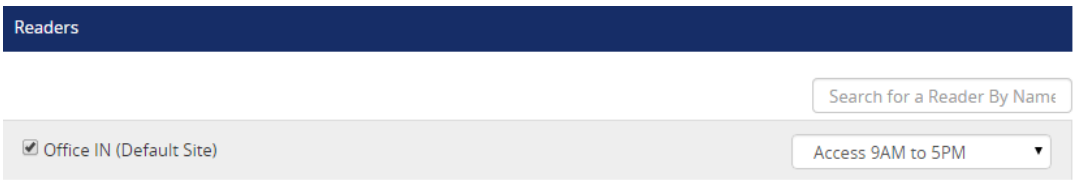
Note

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*.



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).

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 Configuration

This chapter will cover adding **Users** in Protector.Net, 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

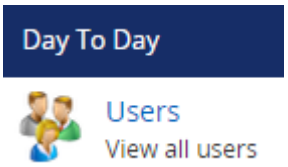
Adding a User in Protector.Net is a fairly simple proccess, however there is a variety of options that take advantage of various features of our software.

Prior to adding Users to Protector.Net, 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 privilges the User may need such as use of auto-door openers or triple swipe access; these privieleges 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 Privielege Groups** this User will belong to.

Once this information has been gathered, we can now begin adding a User to Protector.Net.

1. Access your Protector.Net 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 notice 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 checkboxes 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.

Table 12.1. Add User: General Settings

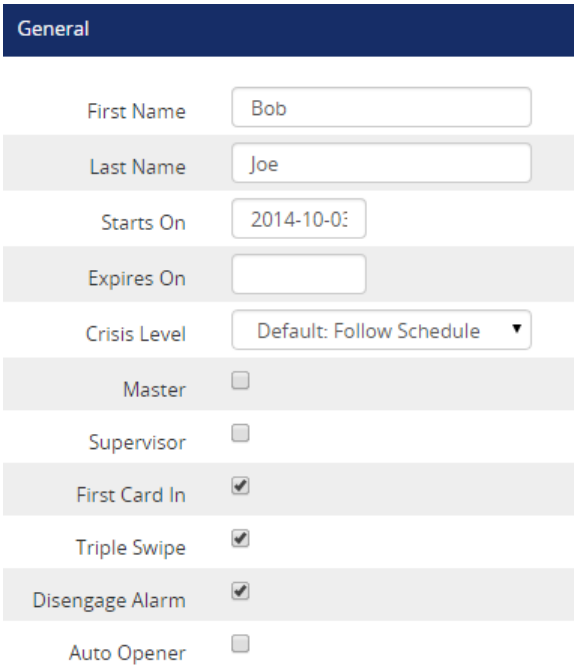
Text Box/Check box	Description
First Name	The Users first name. Accepts 1 to 60 characters.
Last Name	The Users last name. Accepts 1 to 60 characters.
Starts On	The date the User becomes active. Prior to this date the User will be denied access regardless of timezone or privilege (optional).

Text Box/Check box	Description
Expires On	The date the Users access will automatically be revoked. Useful for contractors and temporary workers (optional).
Crisis Level	The Security Level the User is granted when Crisis Mode is initialized. If the security level is equal or greater then the Crisis Level, the User will be granted access. For more information about Crisis Levels, please see Chapter 15, *Crisis Levels*
Master	Enable/Disable Master User privilege. Master Users have full access to all Doors and Floors, regardless of schedule or other privileges. Useful for security staff or emergency personnel.
Supervisor	Enable/Disable Supervisor User privilege. Supervisor Users can be used to grant other Users access in Door Time Zones where Dual Credential is the Door state and supervisor is required.
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 Users privilege to trigger any pre-configured triple swipe actions at the Door. For more information about triple swipe options, please see Chapter 17, *Triple Swipe Features*
Disengage Alarm	Enable/Disable the Users privilege to Disengage Emergency Alarm via double swipe.
Auto Opener	Does this User required an automatic opener to be triggered (if available).

Note

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

Figure 12.1. General Settings example



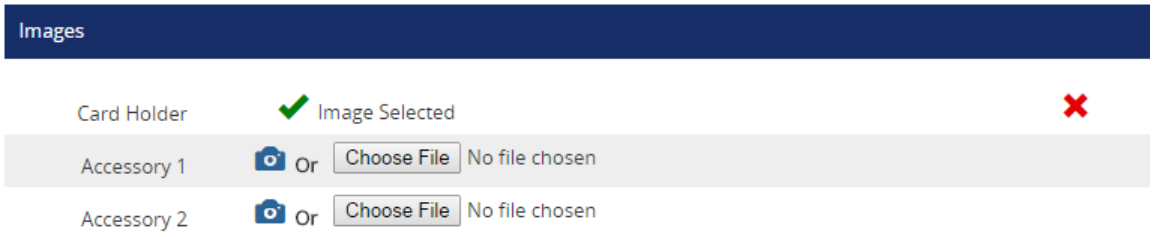
User Card Holder Images

The next section is **Images**. You can upload up to 3 images per User. The Card Holder image is the main image that will appear in the notifications for that User. Accessory 1 and 2 are 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 Protector.Net server in: "<Installation Directory>\Protector.Net\WebServer \content\Uploads\UserProfilePictures".

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

Figure 12.2. Images example

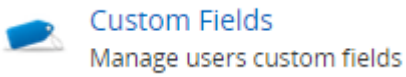


Custom Fields

The next section is **Custom Fields**. If you've created any previously, here is where you can populate them for each User.

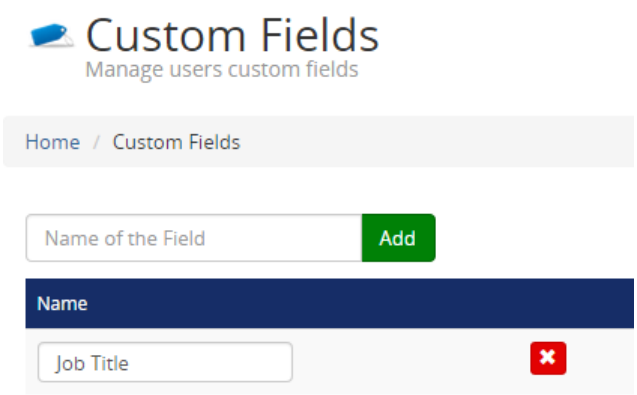
To create additional custom fields, please follow these steps:

1. 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 notice any custom fields you've already created. To add an additional field, fill the textbox titled **Name of the Field** and click the **Add** button.

Figure 12.3. Custom Fields: Example



3. After you've added your custom fields, they will be available when adding new Users or editing Users under the tab or section titled **Custom.**

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.

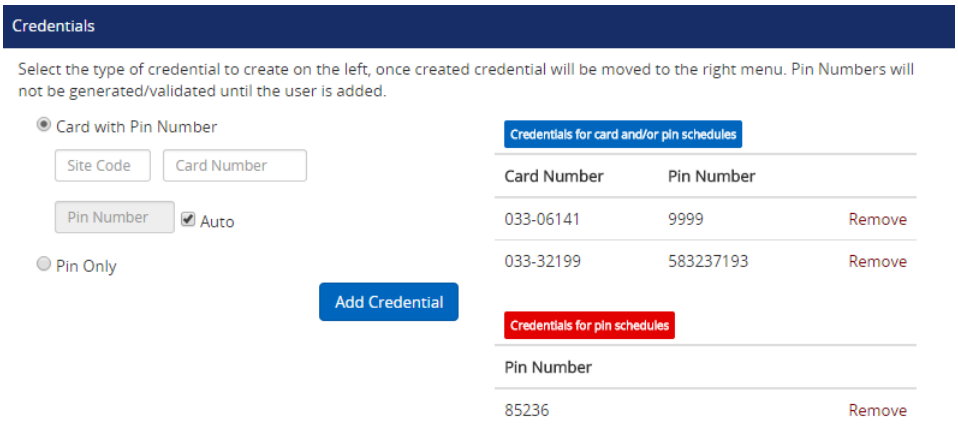
1. Enter the site code (also refereed to as facility code) and card number of the Credential into the **Site Code** and **Card Number** text boxes. A pin number associated with the Credential will be auto generated for Card and Pin schedules unless the Auto checkbox is unchecked.

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

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

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

Figure 12.4. Credentials: Example



Depending on the Door 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'

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.

Pin Only Schedules. The reader will only expect Pins in this schedule. In the example above,Pin '9999' 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*

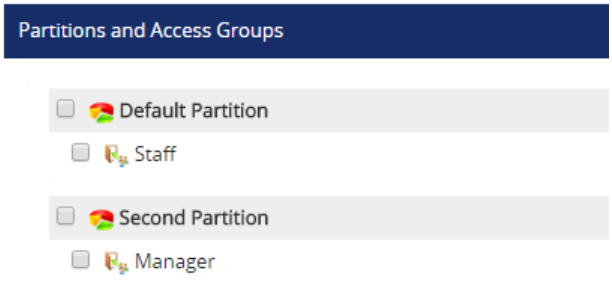
All Partitions you have permission to see will have their associated Access Privilege Groups displayed here. Select the Access Groups the User should belong to.

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



Importing Users and Card holders

This section covers how to import large amounts of Users and Credentials into Protector.Net. This is often used when there are 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

Warning

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

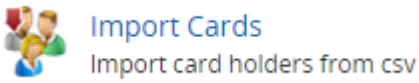
Save the file as **Import.CSV**. You can also use a spreadsheet program, as long as the Users are separated by line and the file is saved as a CSV file.

To import the file, follow these steps:

1. Access your Protector.Net 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.

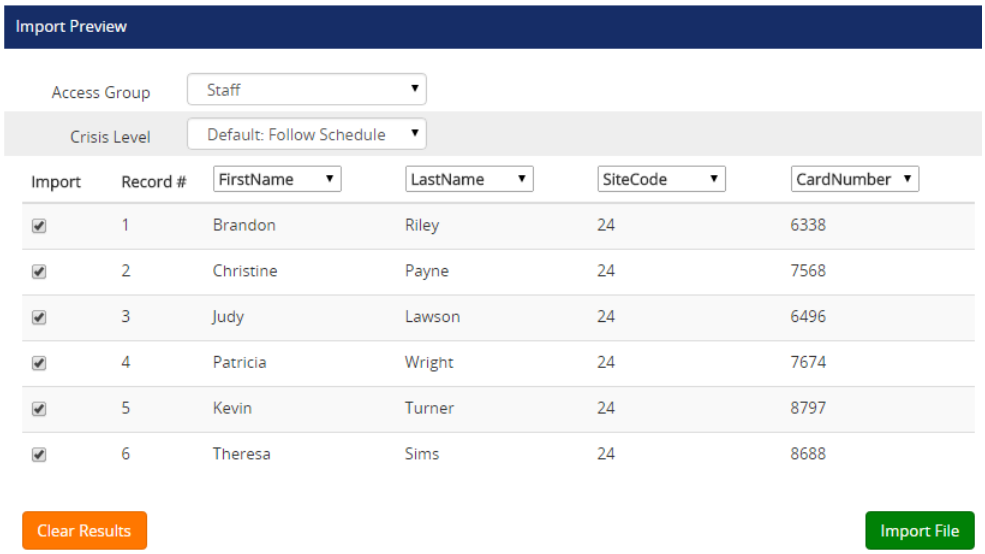
3. On the **Home Screen**, scroll down to the section titled **Day To Day**, click on the **Import Cards** icon (pictured below).



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. Protector.Net will now scan the file and show you the import preview.

Figure 12.6. Import Preview



6. Use the drop-down menu **Access Group** and select the **Access Privilege Group** these Users will be placed in.

> **Note**
>
> If the Users you are importing are going to be in separate Access Privilege Groups, we advise using separate imports for each Access Privilege Group. Only one access group can be imported at a time.

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

8. Above each User data column is a drop-down menu that lets you select the type of information in that column. The selections are: FirstName, LastName, SiteCode, CardNumber, Don't Import. Fill in these selections for each coumn.

   If the data in the column does not match with the data type, the entries with invalid data will change to red. If the errors are in the file such as invalid characters or data in the wrong place, clear the results with the **Clear Results** button. Correct the file, and import it again.

9. Once you've filled the required fields, click on **Import File** to import the Users. Any Users that change 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.

Chapter 13. Holiday Configuration

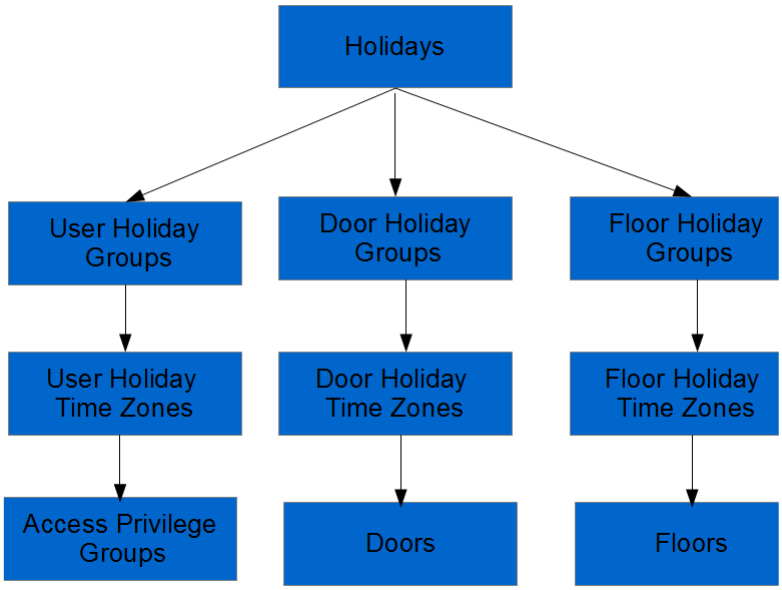
This chapter will cover the configuration of various Holiday components in Protector.Net. We recommend you read the section called “Holidays” prior to reading this chapter for planning how a Holiday should affect your system and an explanation of the components involved.

The 7 components of Holidays in Protector.Net 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 eachother.

Figure 13.1. Holiday Configuration Diagram



Holiday Order of Operations

Although these Holiday componants can be configured 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 Protector.Net 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.

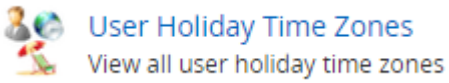
Holiday No Access: with a schedule of 'Not Allowed' all day.

Although this often is enough for most Holiday configurations, its fairly easy to add additional User Holiday Time Zones or to edit the default time zones.

1. Access your Protector.Net 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 notice the default User Holiday Time Zones, if you require additional time zones, click the **Add** button.

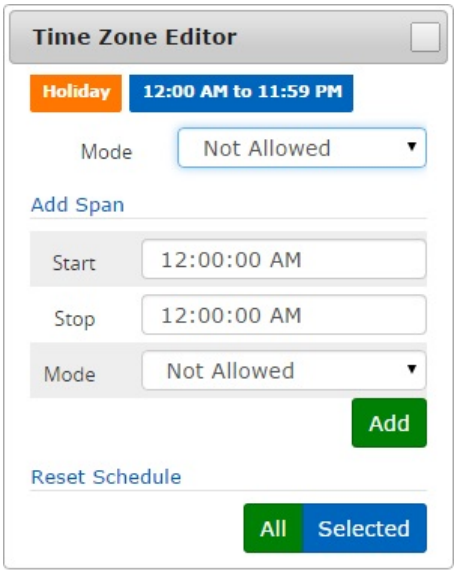
5. On the **Add User Holiday Time Zone screen**, you'll notice it looks almost exactly like other time zones you've added in the system. Populate the textboxes and checkboxes with the appropriate values.

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 then 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 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



7. 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.

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

User Holiday Groups

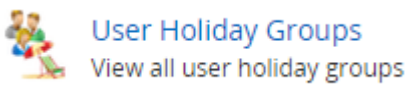
This section will cover the configuration of **User Holiday Groups**. By default Protector.Net comes installed with 2 default User Holiday Groups:

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

1. Access your Protector.Net 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 Groups** icon (pictured below).



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

5. On the **Add User Holiday Groups** page. Populate the textboxes and checkboxes with the appropriate values.

Table 13.2. Add User Holiday Group

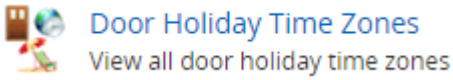
Text Box/Check box	Description
Name	Unique name for your Holiday User Holiday Group. Accepts 2 to 60 characters. We recommend naming the group as the type of Holidays it will contain or the User group for easier readability.
Description	Optional description of your User Holiday Group. Accepts 4 to 255 characters.
Partitions	Select the Partitions you want to create this group in, if more then 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 Protector.Net 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, its fairly easy to add additional Door Holiday Time Zones or edit the default time zones.

1. Access your Protector.Net 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).



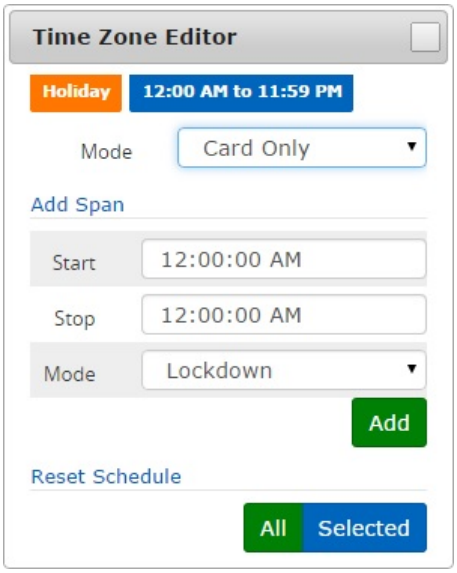
4. On the **Door Holiday Time Zones Screen**, you'll notice the default Door Holiday Time Zone, if you require additional time zones, click the **Add** button.
5. On the **Add Door Holiday Time Zone screen**, you'll notice it looks almost exactly like other time zones you've added in the system. Populate the textboxes and checkboxes 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 then 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.

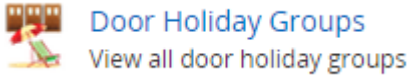
Door Holiday Groups

This section will cover the configuration of Door Holiday Groups. By default Protector.Net comes installed with 2 default Door Holiday Groups: Closed During Holidays, and No Holidays. Although this often is enough for most Holiday configurations, its fairly easy to add additional Door Holiday Groups.

1. Access your Protector.Net 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 notice the default Door Holiday Groups, if you require additional groups, click the **Add** button.

5. On the **Add Door Holiday Groups** page. Populate the textboxes and checkboxes with the appropriate values.

Table 13.4. Add Door Holiday Group

Text Box/Check box	Description
Name	Unique name for your Holiday 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 then 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**.

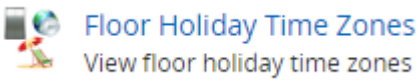
Floor Holiday Time Zones

This section will cover the configuration of Floor Holiday Time Zones. By default Protector.Net 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 Holidays configurations, its fairly easy to add additional Floor Holiday Time Zones or edit the default time zones.

1. Access your Protector.Net 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 notice the default Floor Holiday Time Zone, if you require additional time zones, click the **Add** button.

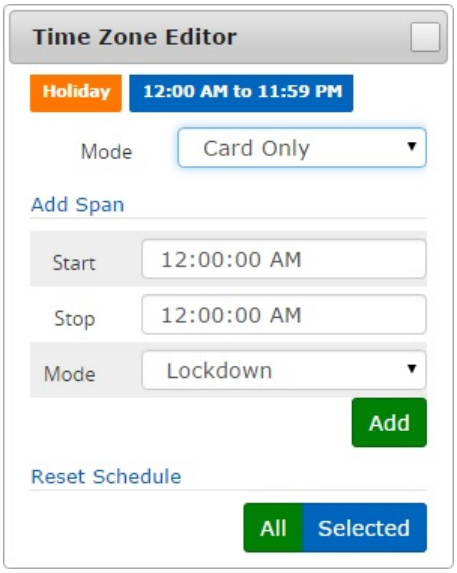
5. On the **Add Floor Holiday Time Zone screen**, you'll notice it looks almost exactly like other time zones you've added in the system. Populate the textboxes and checkboxes with the appropriate values.

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 then 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 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



7. 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.

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

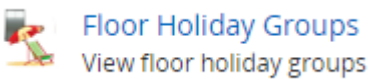
Floor Holiday Groups

This section will cover the configuration of Floor Holiday Groups. By default Protector.Net comes installed with 1 default Floor Holiday Groups: Default Holiday Group. Although this often is enough for most Holiday configurations, its fairly easy to add additional Floor Holiday Groups.

1. Access your Protector.Net 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 Groups** icon (pictured below).



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

5. On the **Add Floor Holiday Groups** page. Populate the textboxes and checkboxes 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 then 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**.

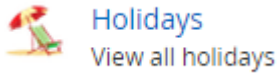
Adding a Holiday

This section will go over how to add additional Holidays to Protector.Net. 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 Protector.Net 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 notice the Holidays (Christmas and New Years). If you require additional Holidays, click the **Add** button.

5. On the **Add Holiday** page. Populate the textboxes and checkboxes 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 checkbox 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 checkbox 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 checkbox 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

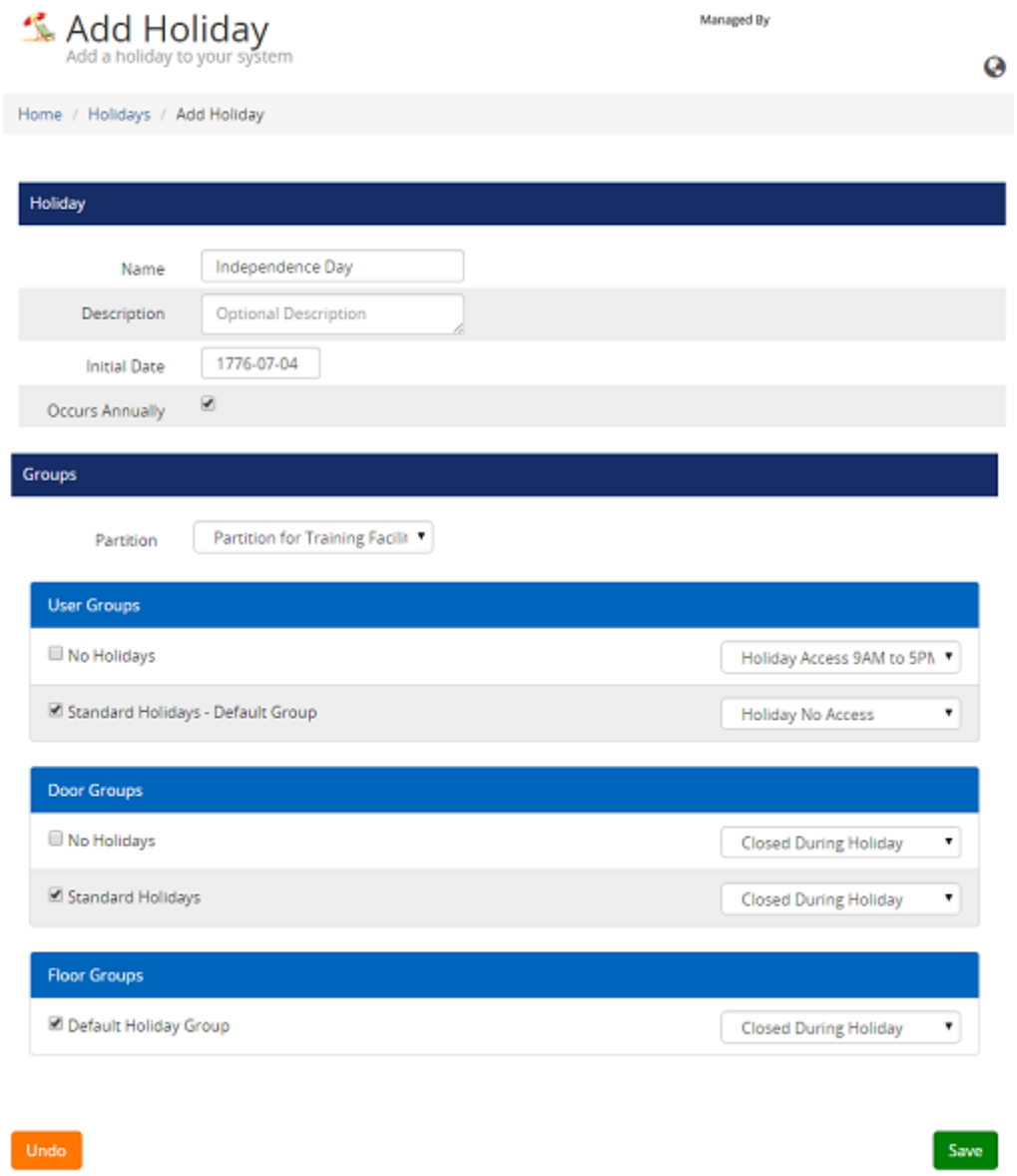
Remeber to perform an Update to your Panels in order for them to be aware of the new Holiday.

Holiday Example

This section contains the example of Independence Day being added as a Holiday in Protector.Net.

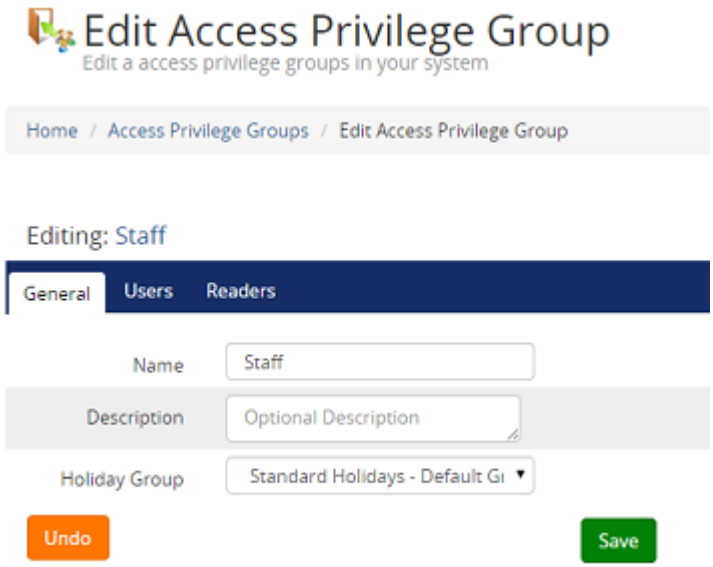
In this example, we will use the default **Holiday Time Zones** and **Holiday Groups**. We simply add the Holiday and make sure **Doors** have the **Door Holiday Group** applied to them, the **Access Privilege Groups** have the **User Holiday Group** applied to them, and the **Floors** have the **Floor Holiday Group** applied to them

Figure 13.5. Adding Independence Day



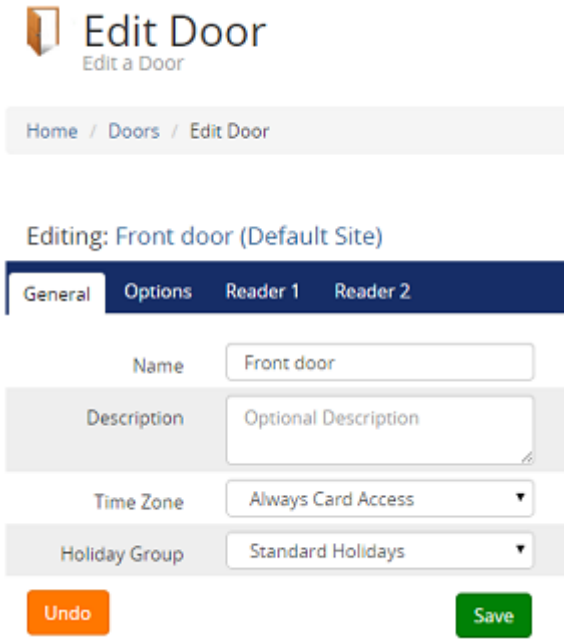
After the above Holiday has been added, we'll need to make sure the **Access Privilege Groups** , **Doors** and **Floors** that the Holiday should affect have the appropriate **Holiday Groups**.

Figure 13.6. Access Privilege Groups: Holiday Group



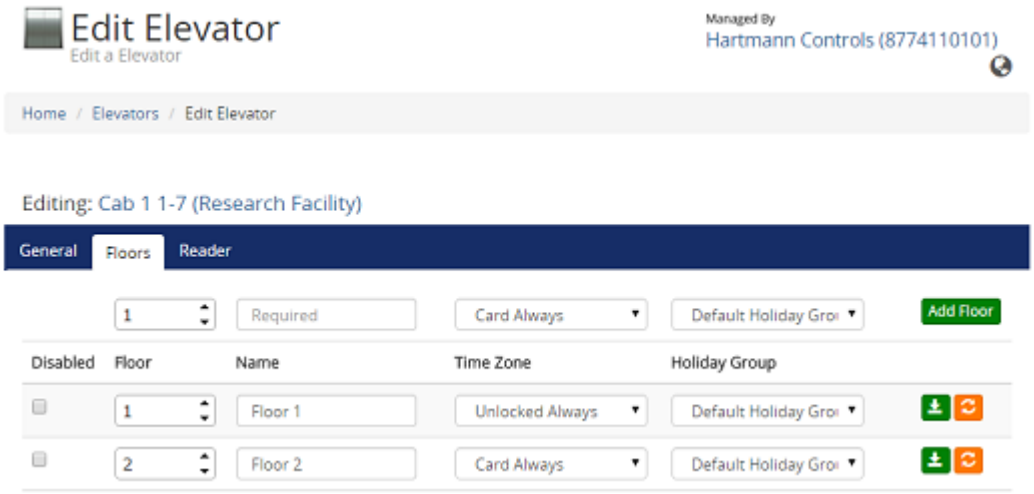
In the above screen shot, we see we've changed the **Holiday Group** drop-down menu to the **Standard Holidays User Holiday Group**, which is the User group we've added the Holiday to earlier.

Figure 13.7. Door: Holiday Group



In the above screen shot, we 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, we 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

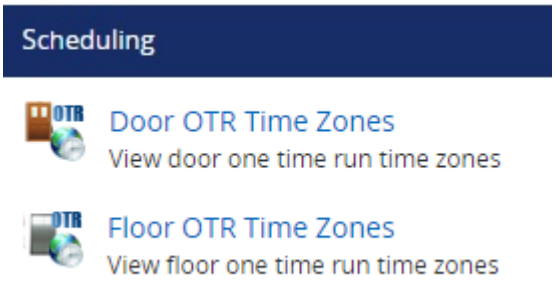
One Time Run Zones (OTR) are used to create one time events where a Door or Floor state changes on a specific day for a predetermined amount of time.

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 Protector.Net.

1. Access your Protector.Net 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).



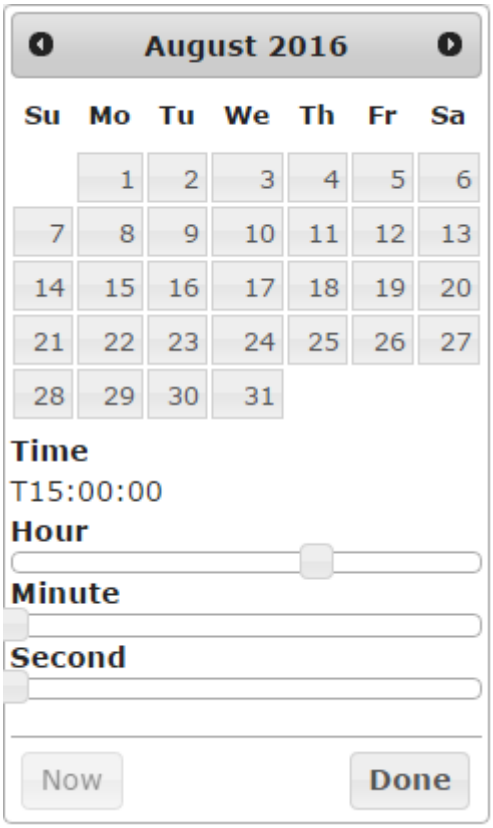
4. On the OTR screen, you'll notice the previous OTR's that have been created, click the **Add** button on this screen.
5. On the **Add OTR** screen, You'll have a couple text boxes to fill.

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, birthday party.
Start Time	The date and time the time zone begins, upon clicking the date picker widget will appear. Use the sliders to pick the start time.
Stop Time	The date and time the time zone ends, upon clicking the date picker widget will appear. Use the sliders to pick the stop time.
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



Chapter 15. Crisis Levels

This chapter will cover how Crisis Levels work in Protector.Net, along with how to customize them and use them effectively.

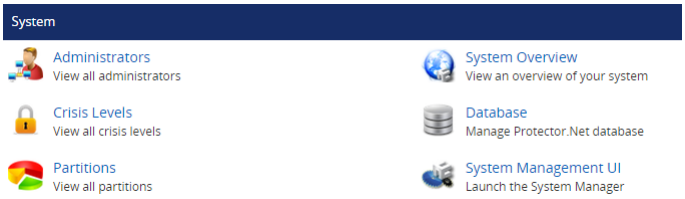
Crisis Levels give Administrators the ability to change the behaviour of Doors quickly during emergency situations with a verity of configurable severity levels. Up to 16 Crisis Levels can be configured, by default only 4 are active.

Making Changes to Crisis Levels

This section will cover how to make adjustments to the names and behaviour of Crisis Levels.

To view and make changes to how each Crisis Level behaves, use the following steps:

1. Access your Protector.Net 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 Level screen, you'll notice all 16 available levels.

Figure 15.1. Crisis Levels Screen

Disabled	Name	Level	Door State
1 = lowest security; 16 = highest security			
	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.

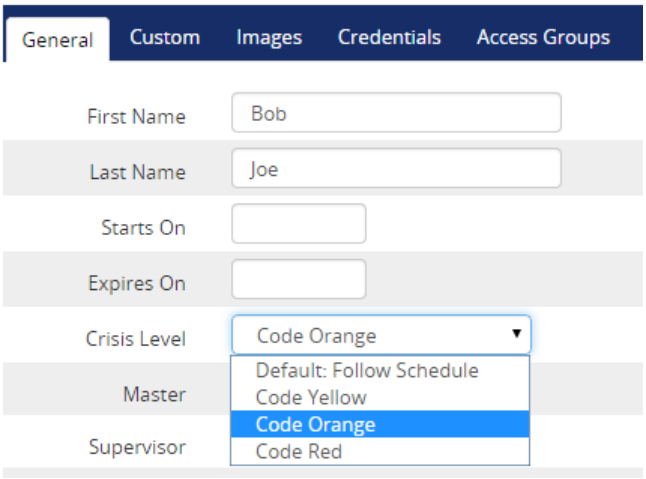
Configuring User Security Levels

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 the Credential unless the User security level is equal 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



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 Protector.Net software, the second method is through the use of AUX Inputs on the Panels.

Applying Crisis levels in Protector.Net

Applying a Crisis Level in Protector.Net can be done from any page in the Protector.Net 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 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.

Warning

Once an Aux Input triggers a Crisis Mode, the only way to resume to normal schedule is through the Protector.Net software interface, or by by having an additional Input with an Aux Input trigger that places the Door into Default: Follow Schedule.

Chapter 16. Protector.Net Override Feature

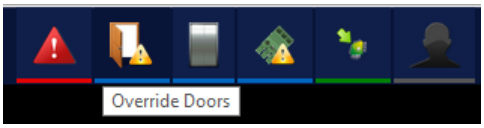
This chapter will cover the various Override features in Protector.Net, including how to Override a Door, an Output or a Elevator Floor through the software in real time.

Warning

Overrides are the highest level of state a Door, Output or Floor will obey. Overrides supersede Holidays, OTR's, 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 Protector.Net 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 Protector.Net will be shown, Doors that are offline will be greyed 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 dived into 3 sections, **General**, **Momentary Override** and **Override until next schedule**.

General. The most common Override is the **Pulse Unlock** action, which will unlock a Door and return its normal schedule immediately after. 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 Overriden.

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.

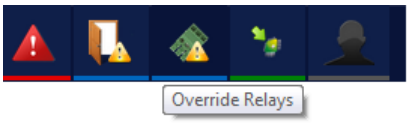
Example: A company has a public Door that is unlocked 9-5, and card only after hours. Its a slow day and the manager decides to close up early. He browses to Protector.Net using his smart phone and does an Override until next schedule, with a Door state of Lockdown. The Door will stay in this state until 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 verity of situations, such as locking up early. For more information on triple swipe options, please see Chapter 17, *Triple Swipe Features*

Override Outputs

This section covers how to Override Outputs in Protector.Net. 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).

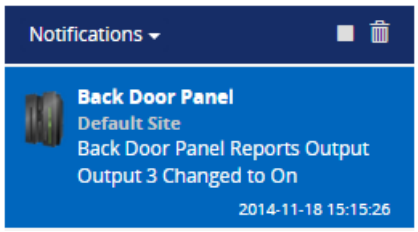


Click on the Override Outputs icon to bring down the Override Outputs Menu. Here you will see all Sites in the system and available Outputs attached to each Site, Outputs connected to Panels that are offline will be greyed out.

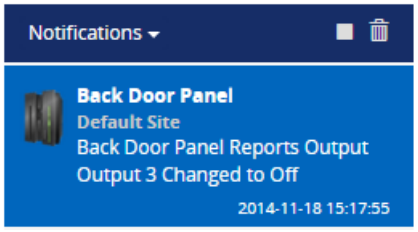
Figure 16.2. Override Outputs Menu

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.



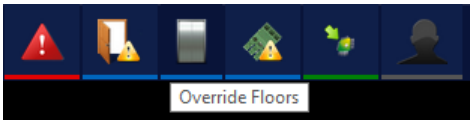
Resume. Resumes a Output to its natural state. (defined in Panel I/O configuration as normally closed or normally open).

Note

Output Overrides can also be performed by configuring Triple Swipe Actions. This can be useful for a verity 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 a Elevator Floor in Protector.Net 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 Foors icon to bring down the Override Foors menu. Here you will see all Sites in the system and the Elevartors and Floors attached to each Site. Only Foors that are online and connected to Protector.Net will be shown, Floors that are offline will be greyed out.

Figure 16.3. Override Floors Menu

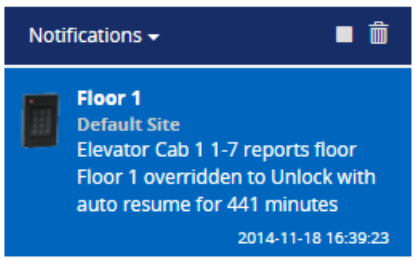
Clicking the checkbox next to a Site will select all Floors in that Site. Clicking on an Elevator will select all Floors attached to that Elevator. Alternatively, you can select individual Foors. Once you have selected the Foors, the buttons on the right side can be used to manipulate the state of the Foor instantaneously.

The Override Floors menu is dived 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 Foor to its normal schedule. When a Foor is resumed, you will see the Notification: **Foor 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 Overriden.

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.



Chapter 17. Triple Swipe Features

Triple Swipe is a feature in Protector.Net where you can present a Credential to a Reader 3 times quickly, 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.

List of Triple Swipe Options

This list contains the currently configurable Triple Swipe Actions.

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 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 "Cancel Override". 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

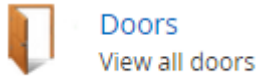
If you are using a keypad, you can configure up to 7 Triple Swipe Actions based on a key press after a Triple Swipe.

Configuring Triple Swipe

As you may have read earlier in this guide, Triple Swipe Actions are configured on the Reader tab of the Edit Door Screen.

To get to this screen:

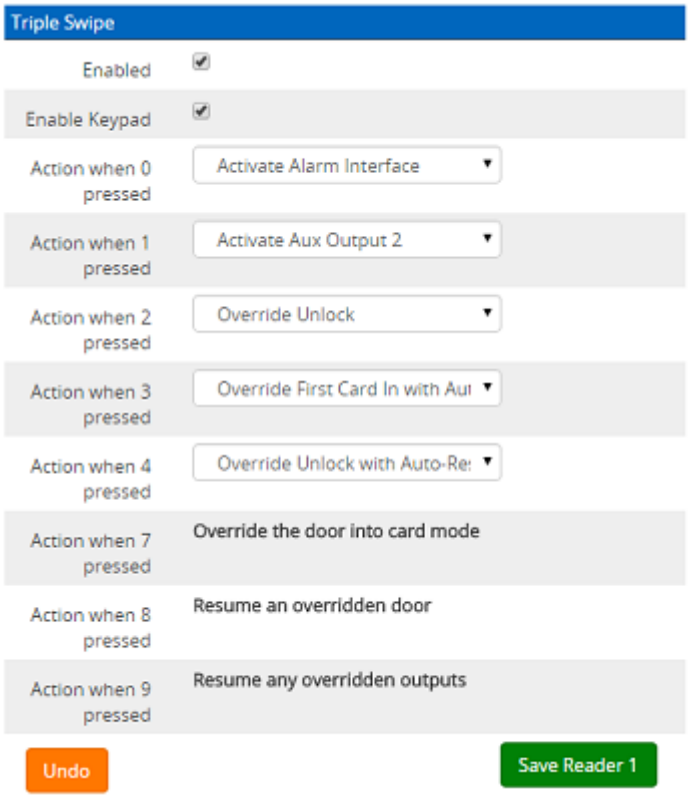
1. On the **Home Screen**, scroll down to the section titled **Hardware**, click on the **Doors** icon (pictured below).



2. On the **Doors** screen, your configured Doors will be listed here. 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, you'll see the options for Triple Swipe Actions.

Figure 17.1. Reader Tab: Triple Swipe



Triple Swipe Examples

This section contains real world examples of how Triple Swipe is being used by our dealers/end Users.

Arm/Disarm Alarm System. Many Users of our product use our system to Arm/Disarm their alarm systems. Its 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 30.1, “Alarm Panel Interface”

Close a Public Door Early. Several customers 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.

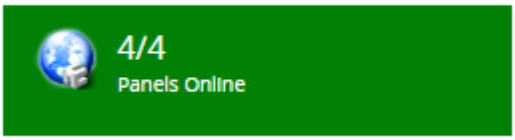
We can also accomplish the above via a Triple Swipe Action. Below are instructions for locking the Door early, but also to tell the Door to **Resume** normal schedule the next day when its scheduled to unlock.

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

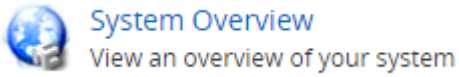
This chapter will cover the System Overview screen in Protector.Net and how it can be used to simplify actions, including updating Panels individually, viewing all Doors and Outputs in the system and viewing the status of Elevators and Floors.

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.



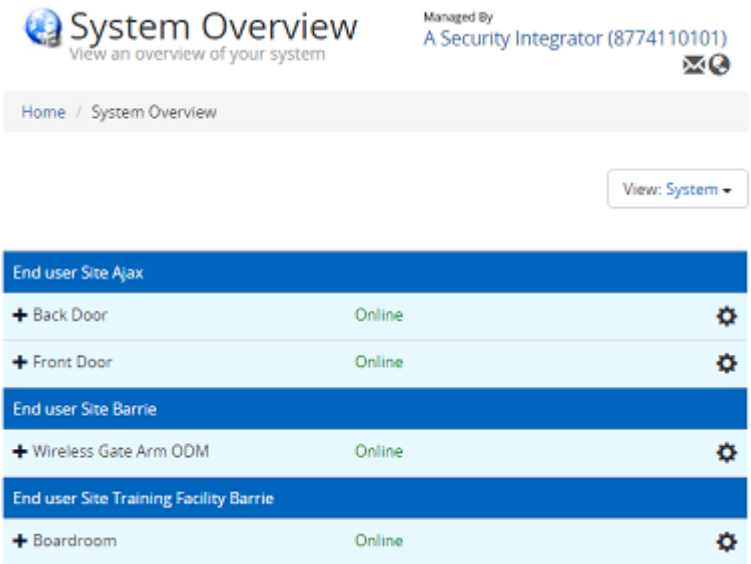
Alternatively, you can navigate to System Manager using the following steps:

1. Access your Protector.Net 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).



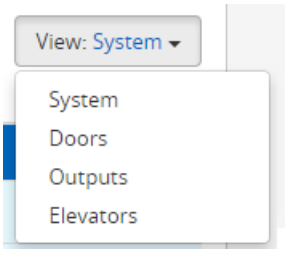
Once on the **System Overview** screen, you'll notice all the Sites created in your system and each of the Panels connected to them, along with if they're online or offline.

Figure 18.1. System Overview Screen: Default View



You can use the + button to expand each Panel to reveal the Doors associated with your Panels. This will show if the Door is in an overridden state or following schedule. If the Door is open or closed (If a Door contact is available). The Doors are colour 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 **Outputs** to view only Outputs in your system. Select **Elevarors** 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.
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.
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 a 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
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 Protector.Net. 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 a 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.

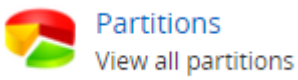
Table 19.1. How Objects Interact With Partitions

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 Protector.Net Partitions are complex, the configuration is relatively simple and straight forward.

1. Access your Protector.Net 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).



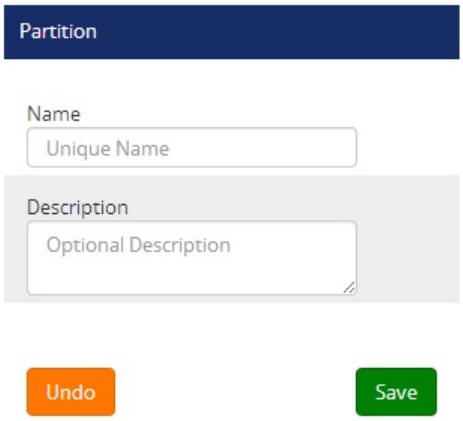
4. On the Partitions screen, you'll notice the default Partition that is created my default. In a lot of cases a single Partition meets the needs of the system, however if during your planning stage you (the installer or end User) decided that utilizing Partitions would benefit your deployment, click 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 Partion 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 creates Sites associated with those Partitions.

Adding Sites

Adding Sites in Protector.Net is similar to adding Partitions, and goes hand in hand with each other. If your not entirely sure what a "Site" is please see the section called "Sites".

1. Access your Protector.Net 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 notice the default Site named **Default Site**, as with Partitions; small deployments generally only use one Site.
5. If your deployment requires more then 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.

Text Box/Option	Description
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 you'll likely want to add your **Panels**, please see the section called "Adding a Panel to Protector.Net". If you're using multiple Partitions and plan on having several Administrator accounts, please see Chapter 20, *Administrators and Privileges* .

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 Protector.Net 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 notice 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. **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/ Check Box	**Description**
Authentication	The authentication of the Administrator account, options are Local and LDAP (if LDAP is configured, see the section called “LDAP”.
Username	Unique User name (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 are what dictates 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 at 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 Protector.Net licence.
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".

5. 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
Manage Access Privilege Groups	Allows the Administrator to manage/add Access Privilege Groups within the assigned Partitions.
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.

Permission Name	Brief Explanation
Manage Door Holiday TimeZones	Allows the Administrator to manage/add Floor Holiday 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 OneTimeRun TimeZones	Allows the Administrator to add/edit one time run time zone's and assign them to Doors within the assigned Partitions.
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.
Reporting DoorActivity	Allows the Administrator to run Door activity reports on Doors within their Partitions.
Reporting FloorActivity	Allows the Administrator to run Floor activity reports on Elevators/Floors within their Partitions.
Reporting UserActivity	Allows the Administrator to run User activity reports on Users associated with Access Privilege Groups within their Partitions.
Reporting UserList	Allows the Administrator to generate and export a Userlist of the Users associated with
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 Output	Allows the Administrator to override Outputs in their Door Panels within their assigned Partitions using the override Outputs quick drop-down menu.
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 Status	Allows the Administrator to see the system overview screen, including Panel and Door status on Panels and Doors assigned to their Partitions.

6. 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.

Chapter 21. Local Anti-passback

This chapter covers the configuration of Local Anti-passback in Protector.Net. This feature is available in 2.1.5 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 through a Door (in some cases a gate) without exiting the monitored Door first.

Note

In this chapter, Local Anti-passback will be refereed to as APB.

Hardware

Before you can enable APB; your Door Panel must meet the hardware requirements:

- Panel must be a ODM (no motion) or TDM. Other Panel models do not support this feature.
- Panel will require Memory Module. Please contact Hartmann Controls for more details Chapter 29, *Support*.
- If using an ODM, two readers will be required, one on each side of the door in order to use local Anti-passback.
- Protector.Net will need to be at least 2.1.50.

Local APB Software

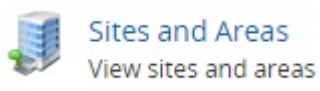
There are three main components for configuring APB.

- **Areas:** Configured on the Edit Sites screen
- **APB Settings:** Configured on the Edit Door screen
- **Reset Anti-passback At Midnight:** Configured on the Options tab of the Edit Panel screen

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 Protector.Net 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 notice and sites you've created. Click the blue button (advanced settings) next to the Site you'll be using Local 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.

You have now successfully added an Area to Protector.Net, and can continue configuring Local APB.

Anti-passback Configuration

Most configuration items for APB are configured on the Edit Door screen. To reach 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, you'll notice 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 **Anti-passback** tab. The configuration items on this screen are explained below:

Table 21.1. Anti-passback Configuration Items

Configuration Item	Description
Enable Anti-passback	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.
Area From	The Area that a User is coming from. On an ODM, the Area From represents Reader 1 on the Door. We recommend selecting 'No Area' in an ODM configuration. In a TDM configuration, the Area From field will depend on if the Door is providing entry or exit.
Area To	The Area that a User is going to. On an ODM, the Area From represents Reader 2 on the Door. Select your custom Area as Area To in an ODM configuration. In a TDM configuration, the Area To field will depend on if the Door is providing entry or exit.
Time Out	The amount of time (in minutes) after a credential is presented that the credential will be allowed through the Door/Gate without raising a APB violation.
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 result in the User being denied access.
Exclude Supervisor Users	Users with the User Privilege "Supervisor" will be exempted from APB violations.

Figure 21.1. APB Settings

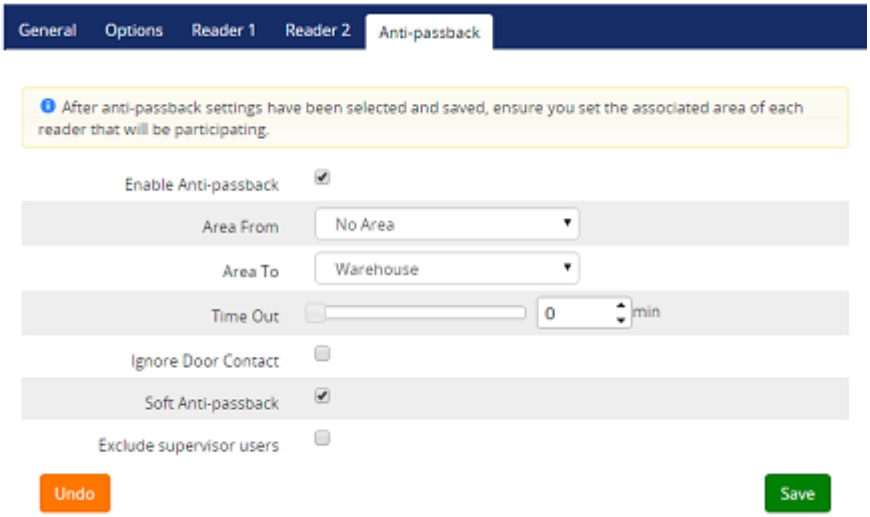
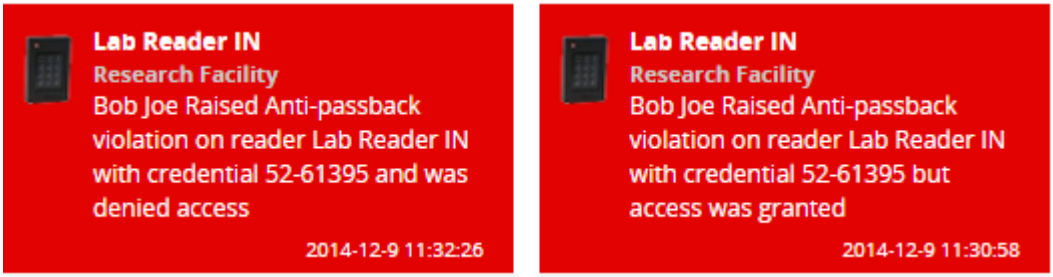


Figure 21.2. APB Violations



Local Anti-passback Examples

This section contains some examples of how APB is used in the field.

ODM Anti-passback. A Pharmaceuticals company requires strict access to a research lab in their building. The Door has an IN and an OUT reader connected to an ODM. In this case APB configuration is fairly simple. The administrator creates an Area called "Laboratory". Enables APB on the Edit Doors screen and selects 'No Area' for the Area From and selects "Laboratory" as the Area To.

TDM Anti-passback: Parking Garage. A parking garage is experiencing a problem with drivers handing their credential to other drivers and drivers tailgating into the garage. The property owner installs a TDM to control the Gate In and Gate Out. After configuring the usual aspects of Protector.Net, the Administrator configures APB:

Gate IN: On the 'Door' Gate IN, APB is enabled. Area From is set to: 'No Area' and Area To is set to the custom Area: 'PkGarage'. Ignore Door Contact is checked since the gate does not have a monitoring device.

Gate OUT: On the 'Door' Gate OUT, APB is enabled. Area From is set to: 'PkGarage' and Area To is set to: 'No Area'. Ignore Door Contact is checked since the gate does not have a monitoring device. The Administrator may choose to enable Soft Anti-passback for the Gate Out, to prevent violators and tail-gators from being stuck in the garage. APB violations will still be reported and can be emailed to the Administrator.

Chapter 22. Elevator Hardware

This chapter will cover the hardware components required to configure elevators in Protector.Net.

The following items are required:

Table 22.1. Elevator Hardware

Part Number	Description
POE-Elevator-64	The Elevator Master Panel. A ODM with special firmware to interact with Hartmann Controls Elevator Expanders through an RS-485 connection.
Elevator Expander Board	Daughter-boards with 8 Inputs and 8 Outputs. Controlled from the Elevator Master Panel through an RS-485 connection.
RS-485 Interface Plug in Module	Field replaceable RS-485 adapter that connects the Elevator Master Panel to the Expander Boards. Can daisy chain up to 8 expanders using the RS-485 bus.

Connecting the Elevator Master Panel to the Expander Boards

The **Elevator Master Panel** communicates with the **Expander Boards** through the **RS-485 Interface Plug-in Module**. We Recommend using (cable name or standard).

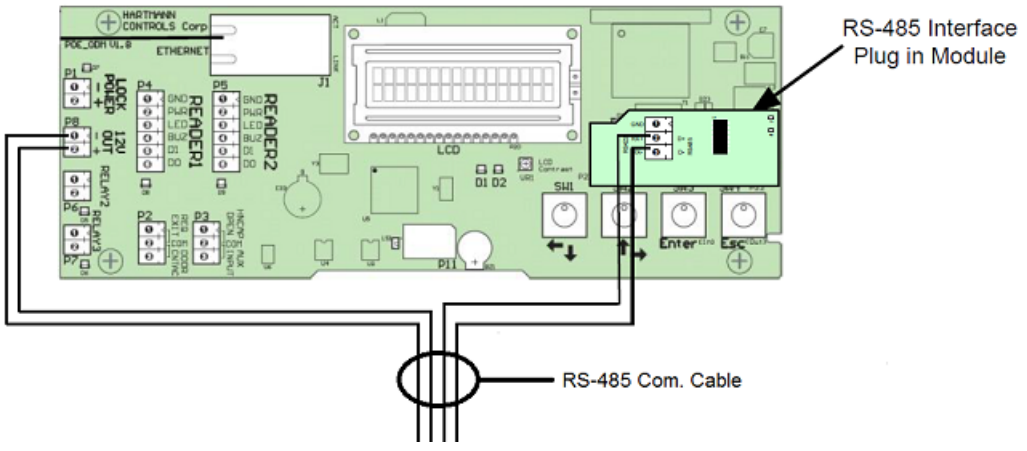
1. Connect one of the two pairs of RS-485 cable to the **'12V OUT'** Output on the left side of the **Elevator Master Panel**.

2. Connect the **RS-485 Interface Plug-in Module** into the **Module Port** on the right side of the **Elevator Master Panel,** ensuring the side of the module with 10 pins is on the left and the side with 6 pins is on the right.

3. Connect the second pair of RS-485 cable to the **'D+'** and **'D-'** on the **RS-485 Interface Plug-in Module** we plugged into the Panel.

Your Panel should look exactly as follows:

Figure 22.1. Elevator RS-485 Connection

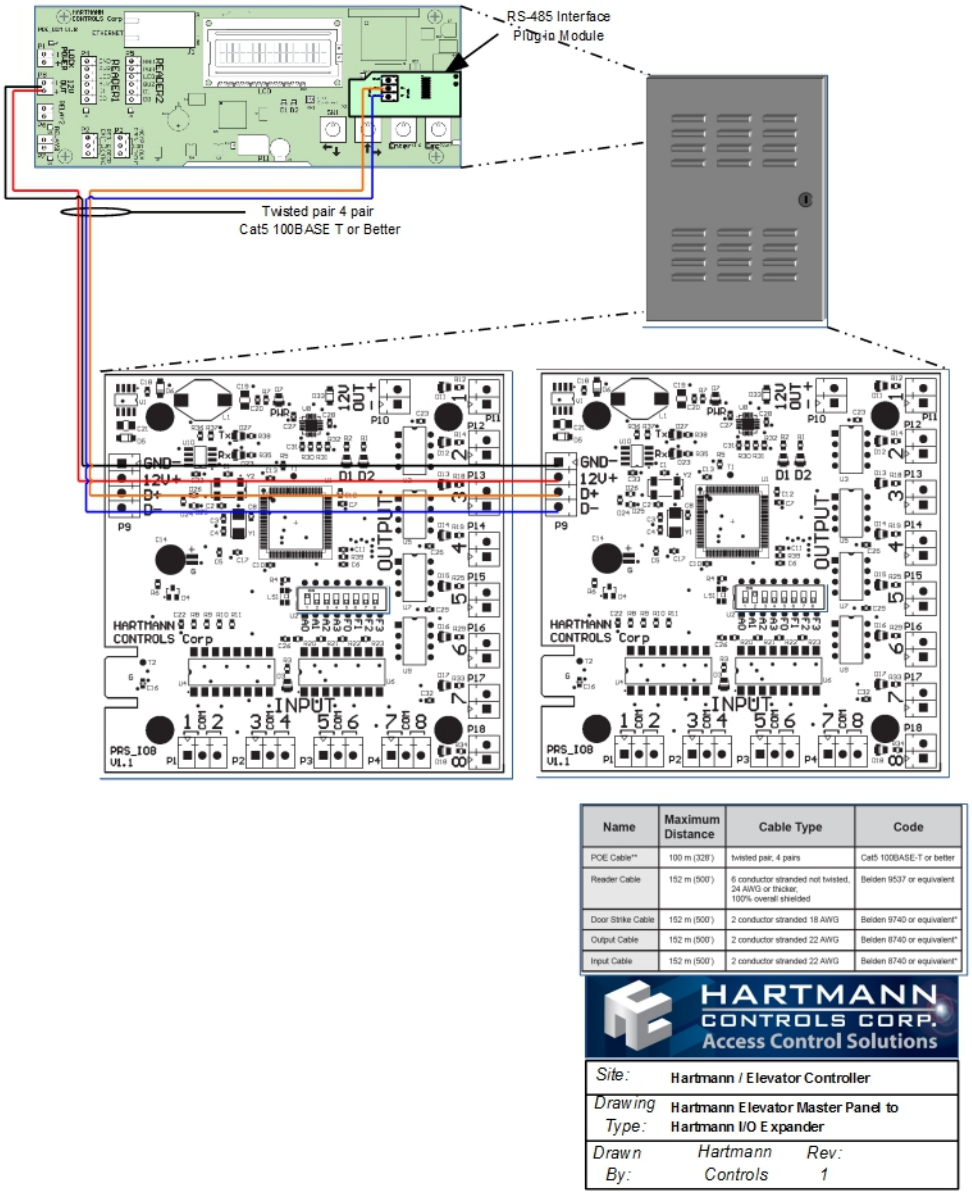


On the first **Expander Board**:

1. Connect the other end of the '**12V OUT**' pair to the '**GND-**' and '**12V+**' on the 4pin header on the left side of the **Expander Board**. Ensure polarity matches.

2. If more than 1 **Expander Board** is being used, an additional RS-485 cable will be run from the first **Expander Board** to the second using the same header block. Ensure polarity matches. Continue this chain for all additional **Expander Boards**.

Figure 22.2. Elevator Master Panel with 2 Expander Boards



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*

HARTMANN CONTROLS CORP.
Access Control Solutions

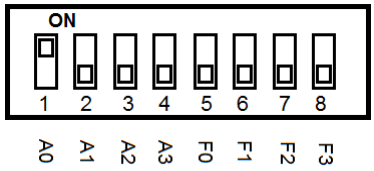
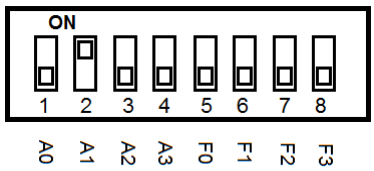
Site:	Hartmann / Elevator Controller
Drawing Type:	Hartmann Elevator Master Panel to Hartmann I/O Expander
Drawn By:	Hartmann Controls — Rev: 1

Configuring Expander Board Addresses

Each **Expander Board** on the RS-485 bus requires a sequential **Panel Address**. The address is configured using the first 4 dip switches on the **Expander Board**. The first **Expander Board** needs an address of '1', the second an address of '2' and so on.

The following chart will demonstrate the DIP switch positions and the corresponding Expander Board Address:

Table 22.2. Expander Panel Dip Switch Address

Dip Switch Position	Resulting Panel Address
	Panel Address: 1 A3 ~ A0: 0001
	Panel Address: 2 A3 ~ A0: 0010
	Panel Address: 3 A3 ~ A0: 0011
	Panel Address: 4 A3 ~ A0: 0100
	Panel Address: 5 A3 ~ A0: 0101
	Panel Address: 6 A3 ~ A0: 0110
	Panel Address: 7 A3 ~ A0: 0111
	Panel Address: 8 A3 ~ A0: 1000

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

Warning

Prior to wireing the Inputs/Outputs on the Expander Board into your elevator system, we strongly reccomend configuring the software prior to this. Please see Chapter 23, *Elevator Software Components* .

Expander Board Input/Output Test

The Expander 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 Expander Board will sequentially activate its 8 Outputs. After all 8 Outputs have been tested, they will turn off and Inputs will be available for testing. To test an Input, simply short the Input and the corresponding Output will be activated. If any of these tests fail, please contact Hartmann Controls. See Chapter 29, *Support*.

Figure 22.3. Dip Switch: Input/Output Test

Expander Board Tamper Sensor

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

Figure 22.4. Dip Switch: Tamper Sensor

Figure 22.5. Tamper Sensor Notification

Chapter 23. Elevator Software Components

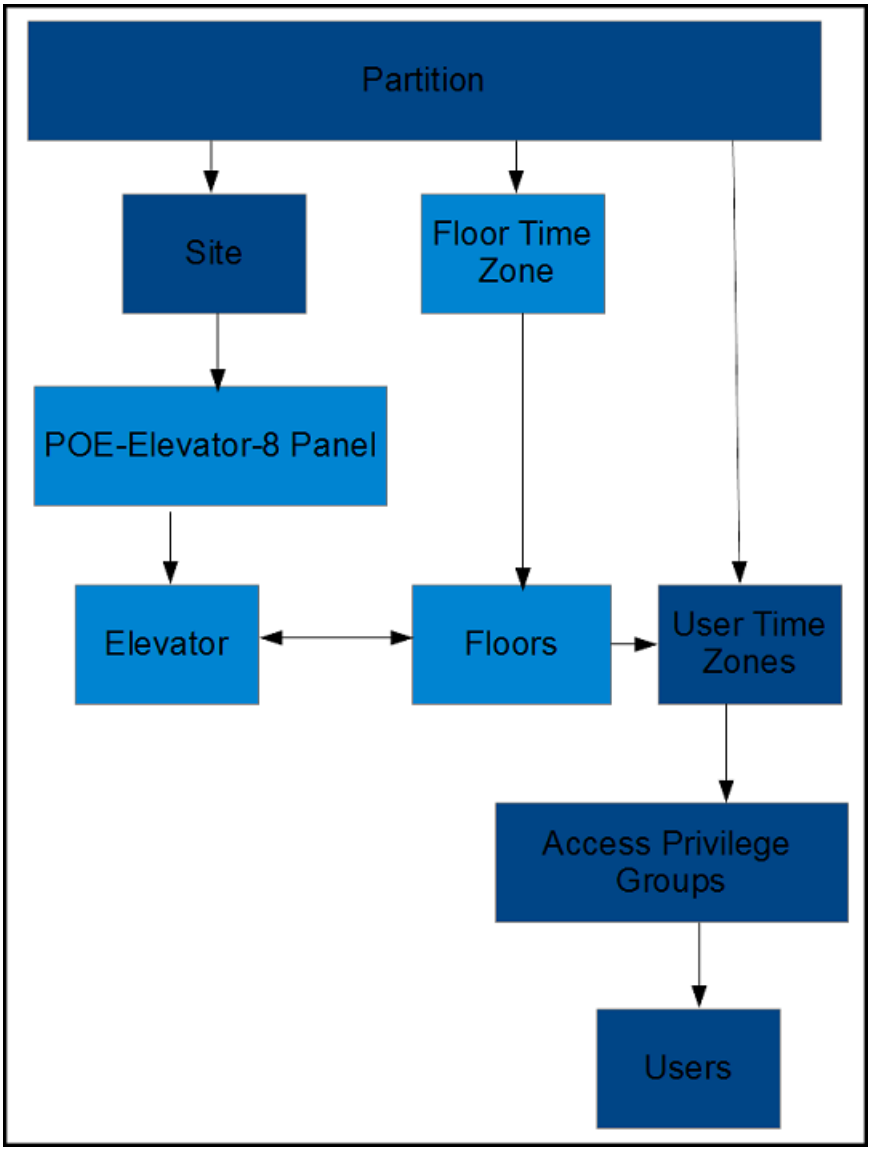
This chapter will will be an overview of the various elevator components within Protector.Net 2.1.0+.

The Elevator software componants are as follows:

- Elevator Panels (the POE-Elevator-64)
- 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 Protector.Net.

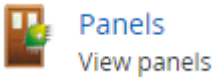
Figure 23.1. Elevator Configuration Items



Adding an Elevator Panel

Adding an Elevator Panel to Protector.Net is very comparable to adding a Door Panel. This section goes over this process.

1. Access your Protector.Net 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).

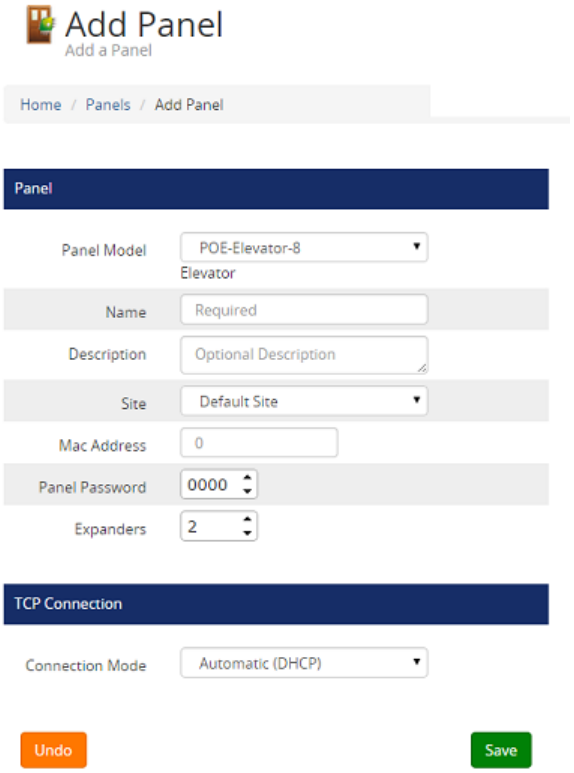


4. On the**View Panels screen**, click the **Add** button.

On the **Add Panels** screen you'll be presented several drop-down menus, text fields and checkboxes to populate.

Ensure the **Panel Model** drop-down menu is set to: **POE-Elevator-8**.

Figure 23.2. Add Door Panels Screen



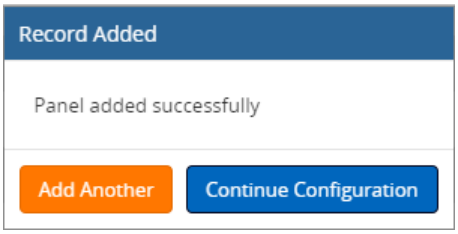
The following table describes the fields to be filled.

Table 23.1. Add Panel

Drop-down/Text Box/Check box	**Description**
Panel Model	Select POE-Elevator-8.
Name	The name of the Panel, we recommend naming the Panel based on its location on the site. Accepts 4 to 60 characters.
Description	Optional description of the Panel. Accepts 0 to 255 characters.
Site	Select the site the Panel will reside on. This cannot be changed once the Panel is added.
Mac Address	The unique network address built into every Panel. May be pre-populated if you're adding the Panel through a Unknown Connection From Panel Notification. Must be 12 characters.
Panel Password	The password required for access to the administration menu built into the Panel. Valid values are 0 to 9999.
Expanders	The amount of Expander Boards attached to the Elevator Panel. Valid values are 1 to 8.
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.

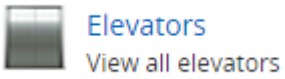
If successful you'll be shown the message: '**Panel added successfully**' with the options to add an additional Panel, or to continue to the edit Panel screen of the Panel we just added.



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, Holiday Groups.

1. Access your Protector.Net 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 several drop-down menus, text fields and checkboxes to populate.

The following table describes the fields to be filled.

Table 23.2. Add Elevator

Drop-down/Text Box/Check box	Description
Panel Model	A unique name for your Elevator. Accepts 2 to 60 characters.
Description	A optional description for your Elevator. Accepts 0 to 255 characters.
Panel	Select the Elevator Panel this Elevator will be attached to.
Button Sensing	Disable/Enable if button sensing is available. For more information on button sensing please see the section called “Button Sensing”
Starting Floor Number	Starting Floor Number. Valid values are -55 to 200 .
Number Of Floors	Number of Floors. Valid values are 0 to 255. If there are more than 8 Floors, more than one Expander Boards will be required. If no ports are available, you will be notified upon saving.

Once you've filled in the required fields, click the **Save** button on the bottom of the screen.

If successful you'll be shown the message: '**Elevator added successfully**' with the options to add an additional Panel, 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”.)

Floors. The **Floors Tab** is where you can edit, add or delete Floors. Its where you assign the **Floor Time Zones**, and the **Floor Holiday Group**.

Reader. The **Reader Tab** is where you can enable the Reader, name/re-name the Reader and assign which Reader port the read is attached to. A ready is required for proper Floor control.

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 crating 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 Protector.Net 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 its 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.

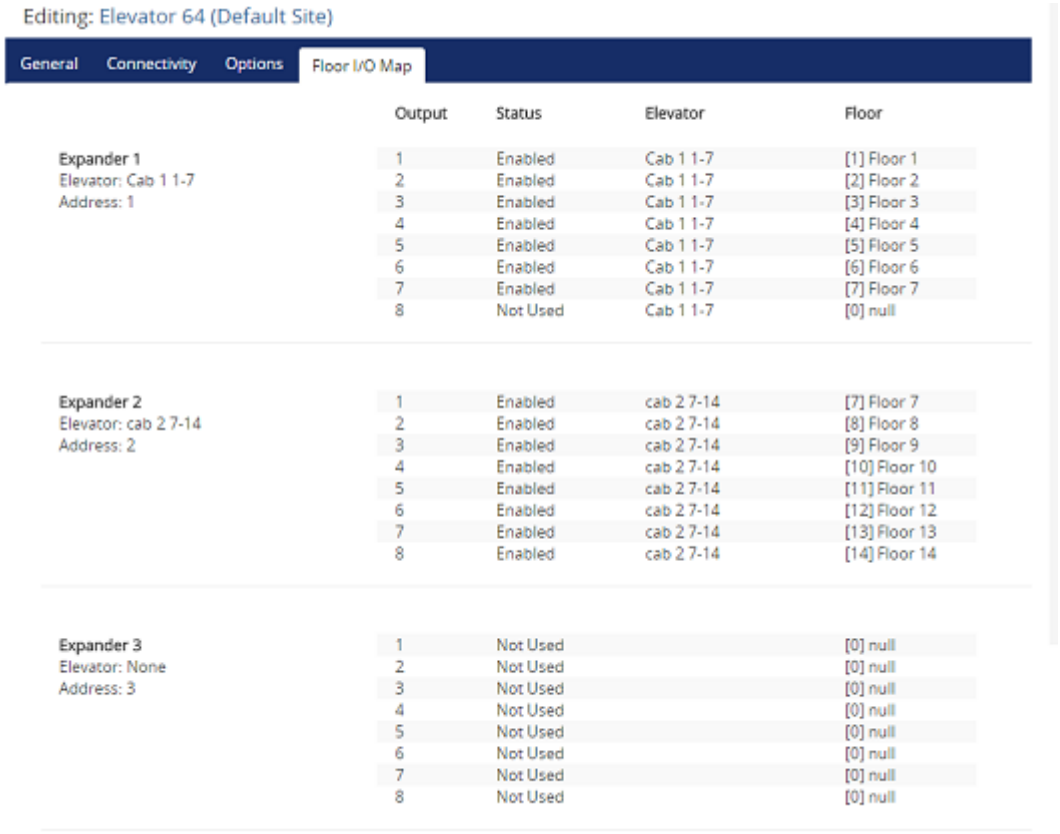
Since the **Expander Board** can't interpret which Floor the User wants to select, when an authorized Credential has been presented (the User has an An**Access Privilege Group** that gives them access to specific Floors), all **Outputs** associated with **Floors** the **User** has access to will become 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 Protector.Net wont be able to see which **Floor** the **User** selected. A record of the **User** presenting his/her Credential to the **Reader** in the cab will be visible **Floor Activity/ User Activity Reports**.

Floor I/O Map

The Floor I/O Map is a tab in the Edit Panel screen that shows a map of all the Outputs on the Expander Board and the corrosponding Floors and Elevators based on the current configuration. The Floor I/O map is extremely useful for a wireing reference. This scren will display the Expander Board Addresss of each Expander, which Elevator the Expander is associated with, and the Output each Floor is associated with.

Figure 23.3. Floor I/O Map



Floor Time Zones

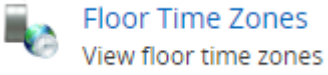
This section covers adding additional **Floor Time Zones** to Protector.Net.

Floor Time Zones are applied to **Floors** in the **Floors Tab** of the **Edit Elevators Screen**. Unlike **Doors 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 additional Floor Time Zones:

1. Access your Protector.Net 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 Time Zones** icon (pictured below).



4. On the Floor Time Zones screen, you'll notice the default time zones. To add additional time zones, click the **Add** button on this screen.

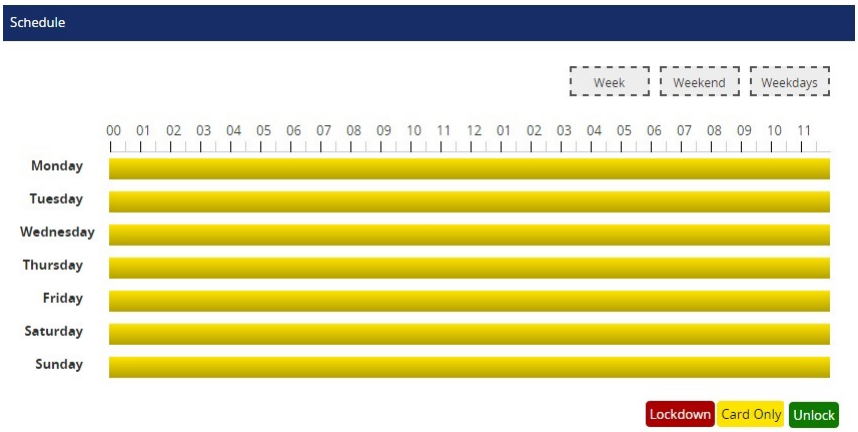
5. On the **Add Floor Time Zone** screen, you'll have a few text boxes to fill.

Table 23.3. 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 are selected, a copy will be created for each Partition.

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

Figure 23.4. Floor Time Zone Schedule

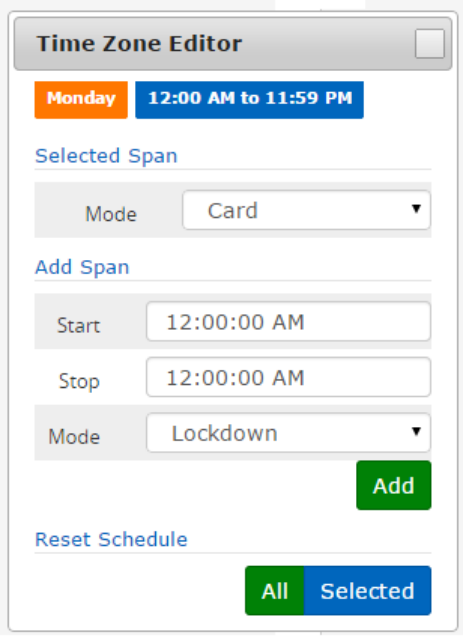


Note

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.

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 23.5. 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 colour coded to the 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 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 Protector.Net 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 User permissions 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 24. Reporting

This chapter will over the various reporting features in Protector.Net. 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.

- Administrative Log
- User Activity
- Door Activity
- Door Activity
- User List
- Notifications

Administrative Log

This section covers what the Administrative Log is, and how to run it in Protector.Net.

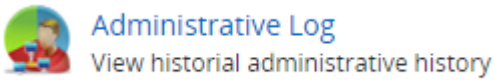
The Administrative Log is a report used for tracking the activities of other Administrators in Protector.Net. This report allows you see what settings other Administrators have changed, and when the Administrator made that change. Options for exporting the report are also available.

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).

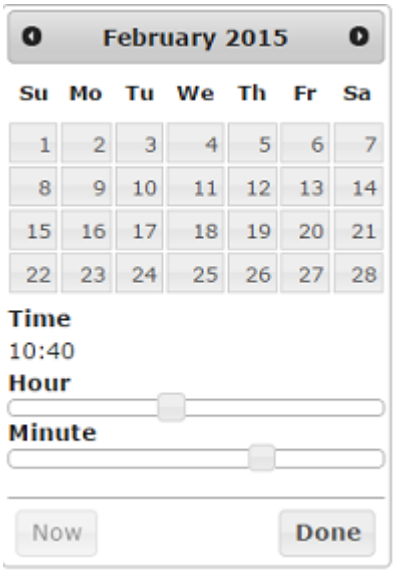


2. Once on the **Administrative Log** screen, you'll have 2 sections to populate.

3. **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 sliders 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.

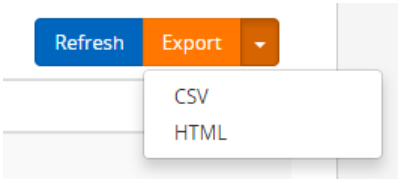
Figure 24.1. Date Picker Widget



4. **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.

5. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the **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.

User Activity

This section covers what the User Activity Report is, and how to run it in Protector.Net.

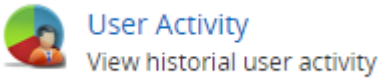
This report allows you see what Doors, Floors and Readers a User account has been in contact with; including access granted and access denied. Options for exporting the report are also available.

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).

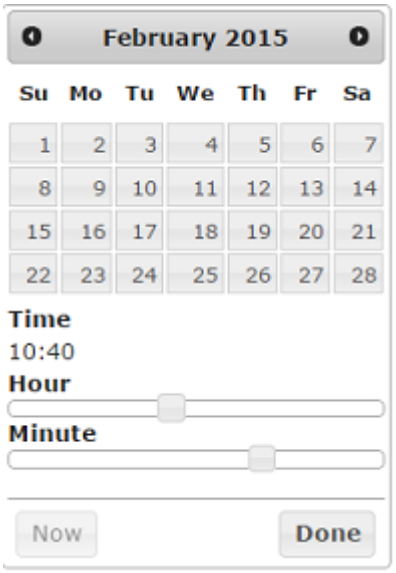


2. Once on the **User Activity** screen, you'll have 2 sections to populate.

3. **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 sliders 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.

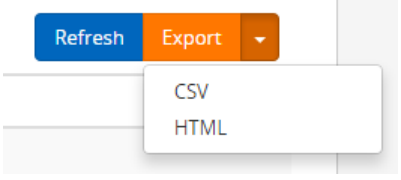
Figure 24.2. Date Picker Widget



4. **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.

5. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the **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.



Information that is presented on exported User Activity Reports include 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, Floor

Door Activity

This section covers what the Door Activity Report is, and how to run it in Protector.Net.

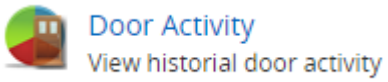
The Door Activity Report is used for tracking the activities of Doors in Protector.Net. This report allows you see what Doors have been doing; when they were opened, when they were unlocked and what Users were granted access or denied to these Doors. Options for exporting the report are also available.

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:

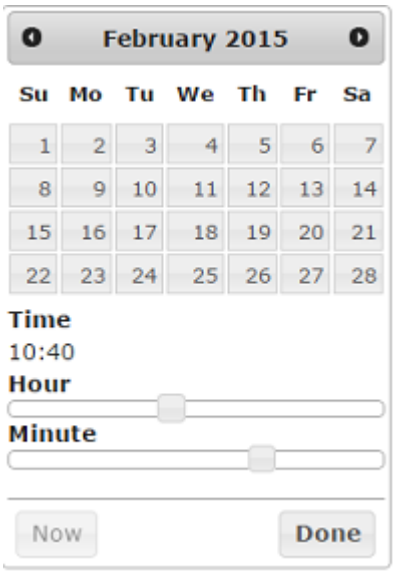
1. On the **Home Screen**, scroll down to the section titled **Reporting**, click on the **Door Activity** icon (pictured below).



2. Once on the **Door Activity** screen, you'll have 2 sections to populate.
3. **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 sliders 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.

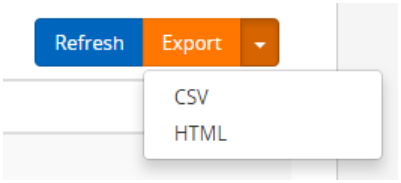
Figure 24.3. Date Picker Widget



4. **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.

5. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the **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 Tab** 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.



Information that is presented on exported Door Activity Reports include 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. on.
- **Card Number** If a Credential was involved with the event, it will be displayed here. 1.
- **Message:** Additional information about the event, such as Access Granted/Access Denied, the User, Credential, Reader, Floor

Note

Overrides, exit buttons, OTR's 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 Protector.Net.

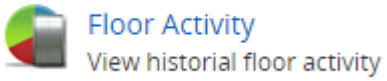
The Floor Activity Report is used for tracking the activities of Floors in Protector.Net. This report allows you see what Floors have been doing; when they were accessed, and what Users were granted access or denied to these Floors. Options for exporting the report are also available.

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).

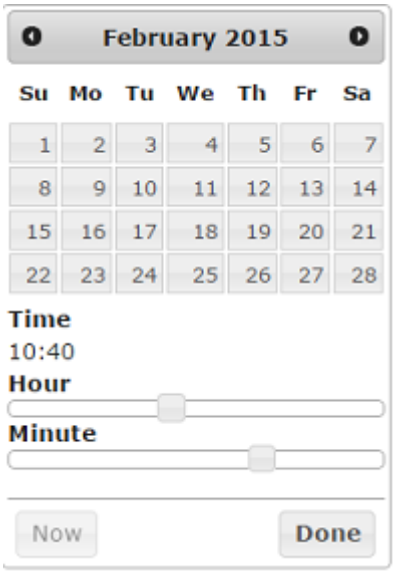


2. Once on the **Floor Activity** screen, you'll have 2 sections to populate.

3. **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 sliders 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 24.4. Date Picker Widget

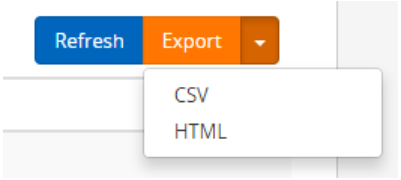


4. **Floors.** Select the Floors you'd like to run the report against. You can select more than one at a time, or just an individual Floor. The search bar can be used to find Floors quickly.

5. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the **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 Tab** 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.



Information that is presented on exported Floor Activity Reports include 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. on.
- **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, Floor.

Note

Overrides, and OTR's 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 Protector.Net.

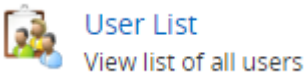
The User List Report is used to view all Users in the system (that you have permission to view), and information, Credentials permissions for each User account. Options for exporting the report are also available.

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).

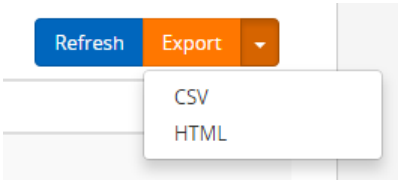


2. Once on the User List screen, the list will automatically begin generating. Depending on the amount of Users in your system, this may take a few moments.

3. Once generated, the Users will be listed along with various User account information including: Name, Classification, Card Number, Pin Number, Groups (Access privilege groups), Crisis Level, Start Date, Expires On, Triple Swipe, Auto Opener, First Card In.

You can sort the Users by any of the displayed properties using the **Sort By** button on the left side.

Just like the other reports in Protector.Net, you can Output the User List Report to a CSV or HTML file using the **Export** button drop-down menu on the right side of the Output tab.



Information that is presented on exported Floor Activity Reports include 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. on.
- **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, Floor.

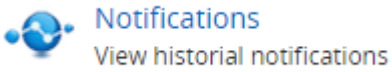
Notifications Report

This section will cover what the Notifications Report is and how to run it in Protector.Net.

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:

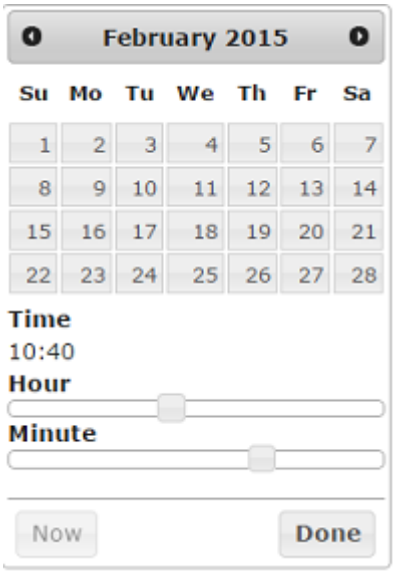
1. On the home screen, scroll down to the section titled **Reporting**, click on the **Notifications** icon (pictured below).



2. Once on the **Notifications** screen, you'll have a few fields to populate.
3. **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 sliders to select the date & time to start/stop the report.

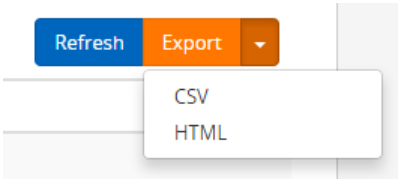
You can also select which **Time Zone** the exported report will be converted to. This is useful when parts of your deployment are in different time zones.

Figure 24.5. Date Picker Widget



4. Once you've filled the required fields, you can now click **Run Report** on the bottom of the page. You'll be taken to the **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 Tab** to change report parameters.

Just like the other reports in Protector.Net, you can Output the Notifications Report to a CSV or HTML file using the **Export** button drop-down menu on the right side of the Output tab.



Information that is presented on exported Notifications Reports include the following:

- **Time:** The date & time of the Notification.
- **Event:**Event type of the Notification.
- **Message:**Event type of the Notification.

Chapter 25. Database

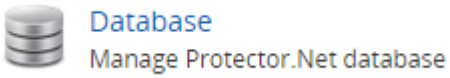
This chapter will cover the options available in the Database screen in Protector.Net, specifically; the purging of Notifications to reduce the size of the database and retain performance.

Purging Notifications

This section will cover how to purge Notifications in Protector.Net. Large amounts of Notifications over time can hurt the performance of Protector.Net, especially with deployments with hundreds of active Panels and thousands of Users.

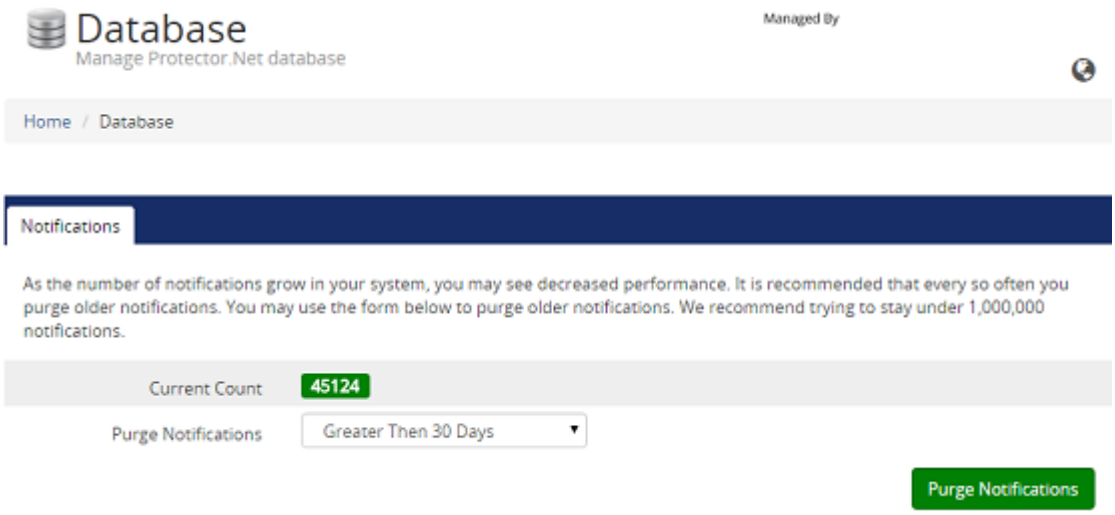
Use the following steps to access the database purging form in Protector.Net:

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 notice the amount of Notifications currently in the database, highlighted in green.

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.

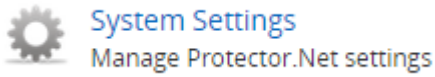
5. Once you've made your selection, click the **Purge Notifications** button on the bottom right side. The Notifications that match the date parameter will now be deleted. Refresh your page to see the new Notification count.

Chapter 26. System Settings

This chapter covers the System Settings of Protector.Net. Most of these settings are the same fields that are configured during the Initial Configuration of Protector.Net. 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 Protector.Net 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** and 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 Protector.Net 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 Hartmann Controls account number. This is provided by Hartmann Controls 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 and Server Port

The server address and server port are configured at the bottom of the General tab, these fields are pushed to the Panel during a Panel update and dictates how the Panels communicate with the Protector.Net server.

Table 26.2. Connection Config Fields

Field	Brief Description
Server Address	By default, the name of the PC Protector.Net was installed on. This field is what is pushed to your Panels and dictates 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 Protector.Net System Settings.

LDAP

LDAP (Lightweight Directory Access Protocol) is a vender neutral standard for sharing directory information services across multiple applications. In Protector.Net this is often used to enable single sign on for system Administrators with active directory.

The benefits of using LDAP with Protector.Net include:

- Single sign in allows Administrators to use their active directory or domain Credentials to access Protector.Net.
- Passwords are authenticated with active directory. In the event that the password changes in active directory; Protector.Net will require the new password for the Administrator to log in.

Some of the disadvantages of using LDAP with Protector.Net include:

- If the LDAP server is offline, Administrators cannot log in to make changes to the system.
- If the LDAP Credentials are compromised, Protector.Net can be as well.

To enable LDAP in Protector.Net:

1. Check the Enable LDAP checkbox on the **Security** tab of **System Settings**.
2. In the **LDAP Address** text box, enter the connection string of the LDAP server. Formatted as: LDAP://[Domain]/OU=MyOu, DC=my, DC=domain, DC=ext
3. Click **Save** to enable LDAP.
4. Once LDAP is enabled and configured, create an Administrator account in Protector.Net. You'll notice the **Auth Method** drop-down menu in the **Add Administrator** screen, change this to LDAP. Use an email address of a active directory/domain account.

For more information on adding Administrators to Protector.Net, please see Chapter 20, *Administrators and Privileges*

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 reduces 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 Protector.Net. 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 email alerts and email recovery will be sent from. It can be the same as the sender email address.
Username	This is the Username required for authenticating and sending email via SMTP.
Password	This is the password required for authenticating and sending email via SMTP.
Send Test on Save	If checked, a test email will be sent from the reply address to itself to verify that the settings are correct.

Once all required fields have been set, click Save. If the checkbox Send Test on Save was checked, a test email will be sent to the reply address from the reply address.

Email Notifications

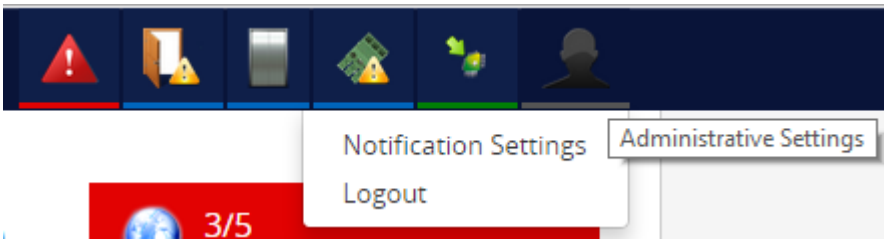
Email Notifications is a feature in Protector.Net that allows you to receive emails when certain events happen in your access control system. For example; If someone was denied access to a reader, you may want to receive an email alert about it.

Note

In order for email notifications to function, you must proporly setup Protector.Net Email Configuration.

To setup email notifications, please follow these steps:

1. Access your Protector.Net system through your HTML5 browser of choice.
2. Log in using the Administrator account you created during the initial setup or provided to you by your dealer/installer.
3. On the **Home Screen**, click on the **Administrative Settings** icon on the top of the screen. A drop-down menu will appear. Select **Administrative Settings**.



4. On the Notifications Settings Screen, you'll notice 16 sections and 3 columns. Each section contains a header about the type of notification beneith it.

5. Each notification has an Alert and Email button on the left side. When the Email button next to a notification is set to On, an email will be sent to the logged in administrator when this notification happens, along with information about the notification such as the involved user/door/reader/time.

Chapter 27. Third Party Integration

This chapter includes information about how Protector.Net intergrates with third party software systems. This includes the cardPresso® photobadging software and ASSA ABLOY wireless lock systems.

CardPresso Photo Badging Software

This section covers the configuration of Protector.Net 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 Protector.Net database when you are creating badges with cardPresso®.

Several of these steps require administrative rights to Protector.Net server, and basic IT knowledge. If you experience issues following this guide please contact your internal IT staff or Hartmann Controls.

This guide was written using Windows 7 64 bit computer with **Protector.Net 2.0.xx** and **cardPresso® 1.3.47 XL version.**

Supported Fields

The following is a list of fields cardPresso® can import from the Protector.Net database along with a brief description of what the field does.

Table 27.1. 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.

Field Name	Data Type	Brief explanation
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.
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 Protector.Net software. These fields can include job titles, phone numbers, rank, ect.

Preparing the Protector.Net Database

In this step, we'll need to execute an SQL script that will create the database view for the cardPresso® software.

1. Navigate to the Protector.Net installation directory for example: "C:\Program Files (x86)\Hartmann Controls\Protector.Net\WebServer\SQLHelpers"

   ### Note

   Your installation directory may differ from the example above.

   Copy the URL address in the navigation bar.

2. Open a command prompt with administrative privileges. Navigate to the sqlhelpers folder in the command prompt using the "cd" command followed by a paste of the URL you copied previously.

   Example: type "CD C:\Program Files (x86)\Hartmann Controls\Protector.Net\WebServer \SQLHelpers"

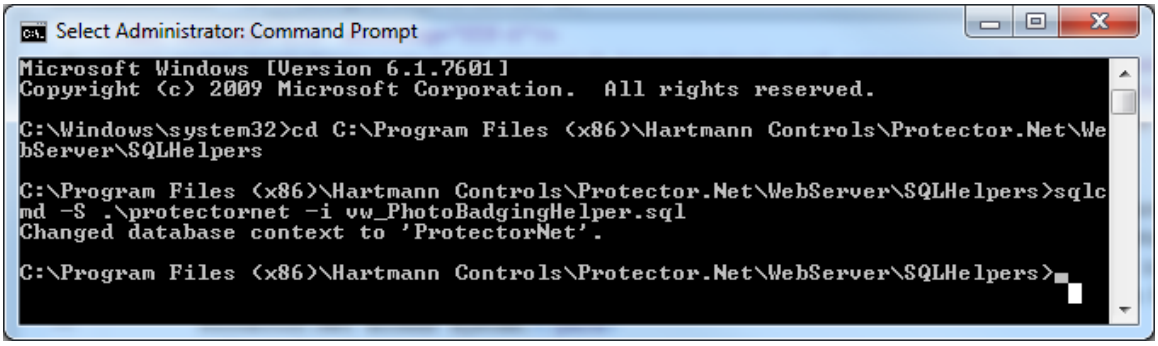
3. Execute the script using SQL command line:

   "sqlcmd -S .\protectornet -i vw_PhotoBadgingHelper.sql"

   ### Note

   ".\protectornet" is a reference to the database instance, your instance may differ if using an external database server.

Figure 27.1. Command Line Example



The database view has now been created, next we will create a reference to this view that cardPresso® can use.

Creating an ODBC Connection for cardPresso®

In this step we will create a data source reference to the view we created in the section called “Preparing the Protector.Net Database” so that cardPresso® will interface with the Protector.Net database.

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.

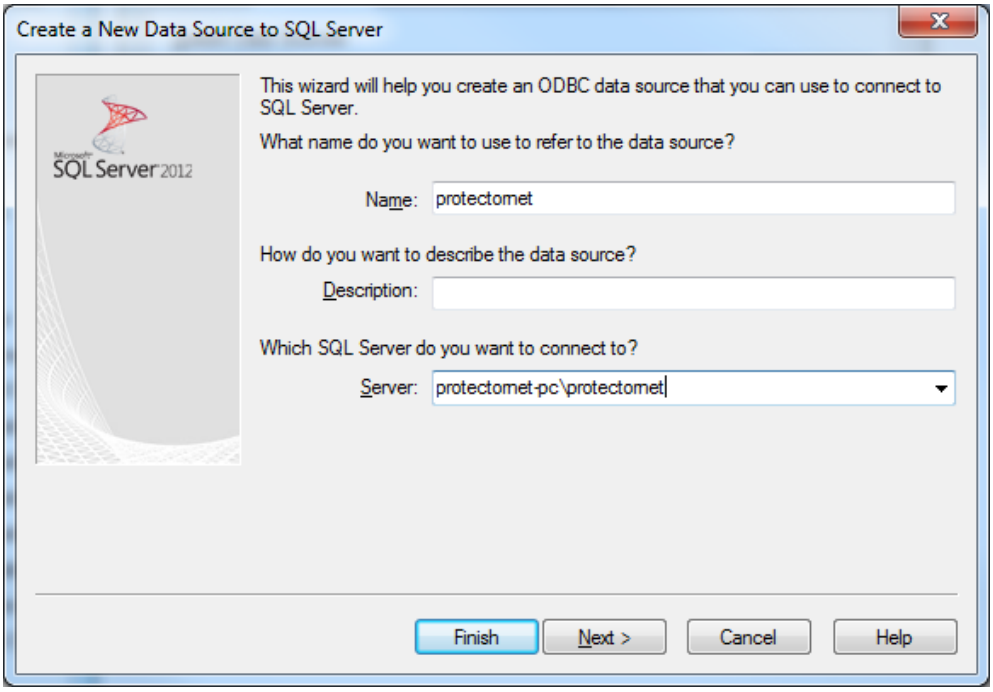
3. Once **Data Sources (ODBC)** is opened, click on the second tab named **System DSN**.

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 "protectornet", the **Ddescription** can be blank, the server will need to be in this format "servername\database instance".

   For example "protectornet\protectornet"

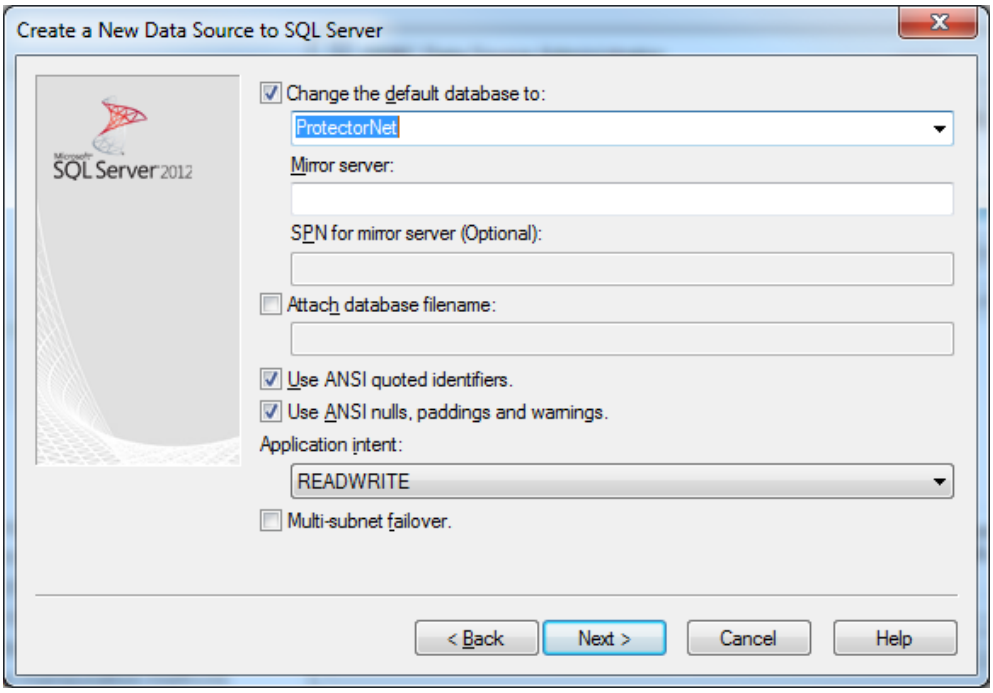
Figure 27.2. Adding a New Data Source



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 **ProtectorNet.** Click **Next**.

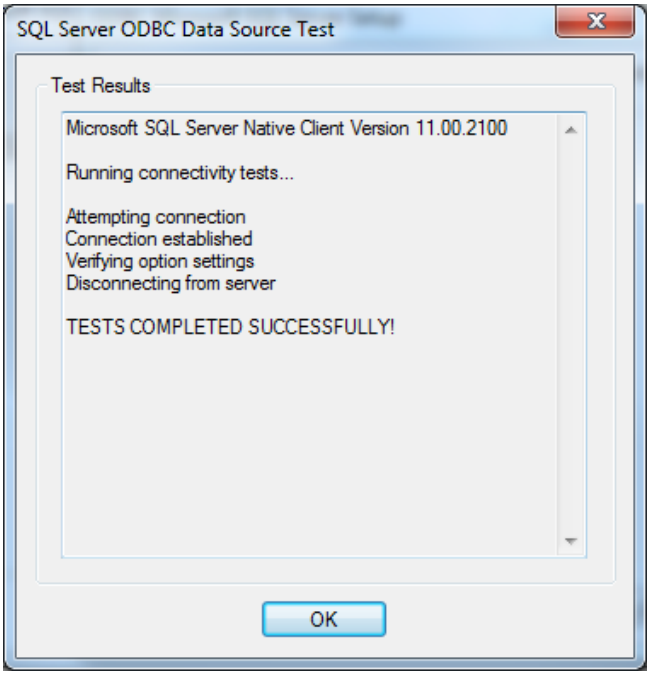
Figure 27.3. Default Database



8. This window can be left as the default settings, click **Finish**.

9. 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 27.4. Data Source Text Successful



10. 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 Protector.Net database, we may 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 “Preparing the Protector.Net Database” and the section called “ Creating an ODBC Connection for cardPresso® ”.

This chapter assumes the following:

- cardPresso® Software is installed
- Photo-badge helper sql script has been executed as outlined in the section called “Preparing the Protector.Net Database”
- 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 www.cardPresso.com and refer to their documentation

Using the cardPresso® Database Connection Wizard

1. Open the cardPresso® software and select or create a template.

2. On the top of the cardPresso® software there is a button section for database operations

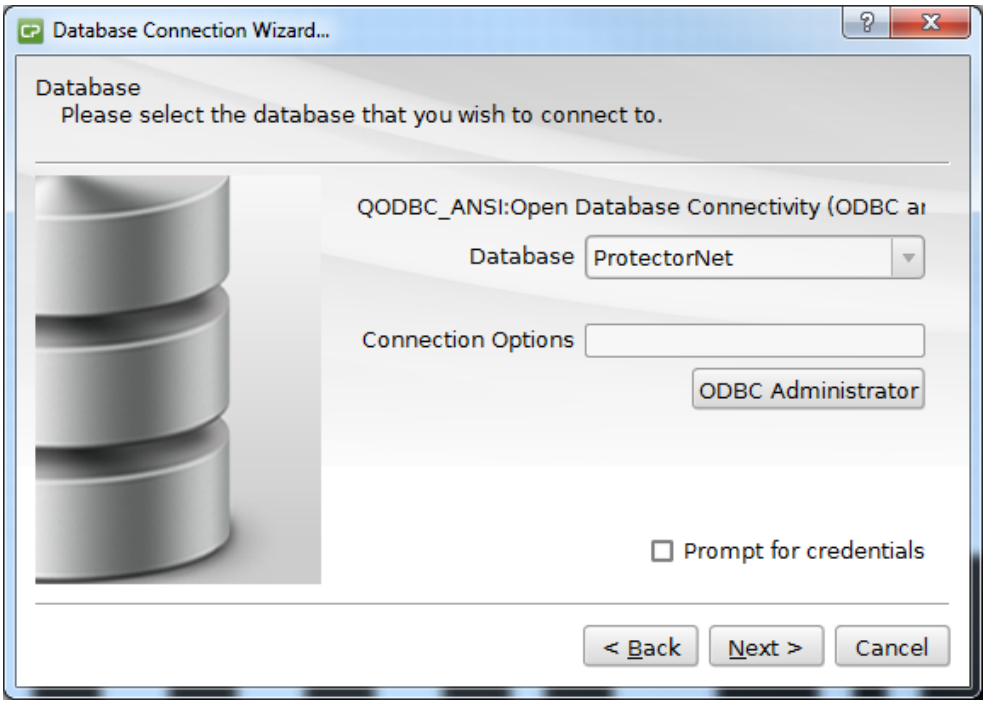
   Click the **Connect to Database** button, highlighted in the figure below:

Figure 27.5. Database Connection Button

3. The cardPresso® database connection wizard will now appear. Click **Open Database Connectivity (ODBC ansi)** and click **Next**.

4. Use the drop-down menu and select **ProtectorNet** (or the name of your database). Uncheck the **Prompt for Credentials** button and click **Next**.

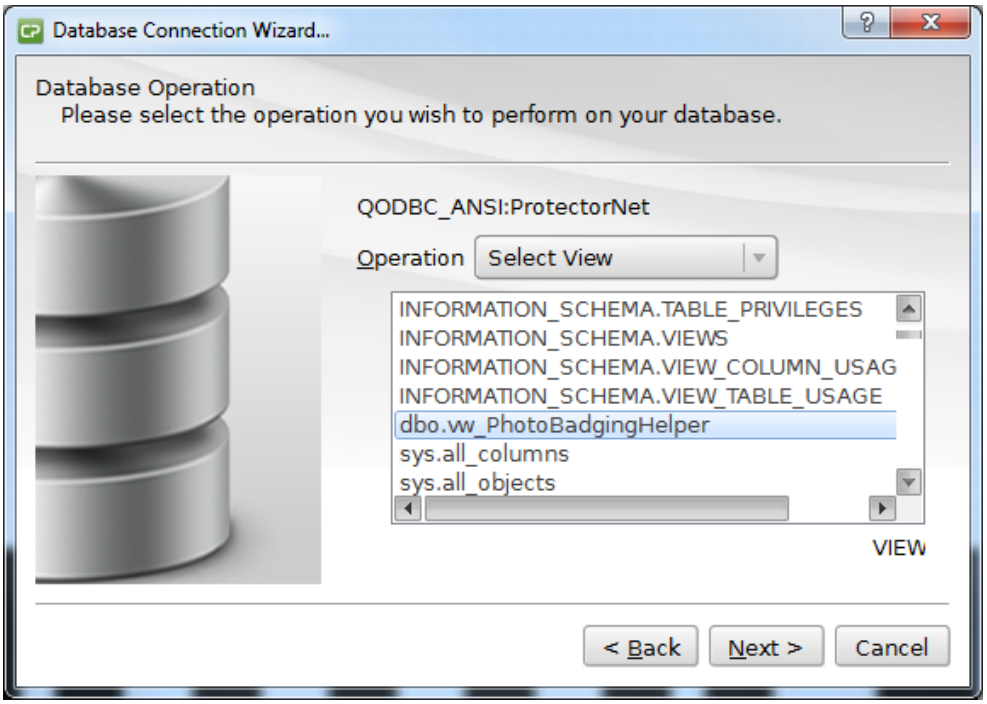
Figure 27.6. Database Connection Wizard



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 **Next** .

Figure 27.7. 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 select the **Userid** checkbox.
10. Click **Finish** to complete the wizard. On the left hand side you'll notice 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 27.8. 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 Protector.Net web interface. For information about adding card holder pictures, please see the section called “ Taking Pictures with Protector.Net 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, cardnumber, etc...

3. Move your mouse over the **Userid** field, click on the grey 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 27.9. cardPresso® Index Image

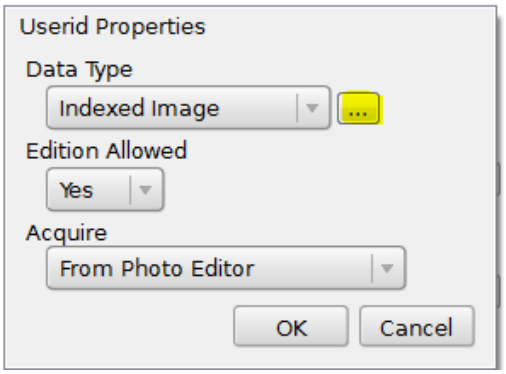
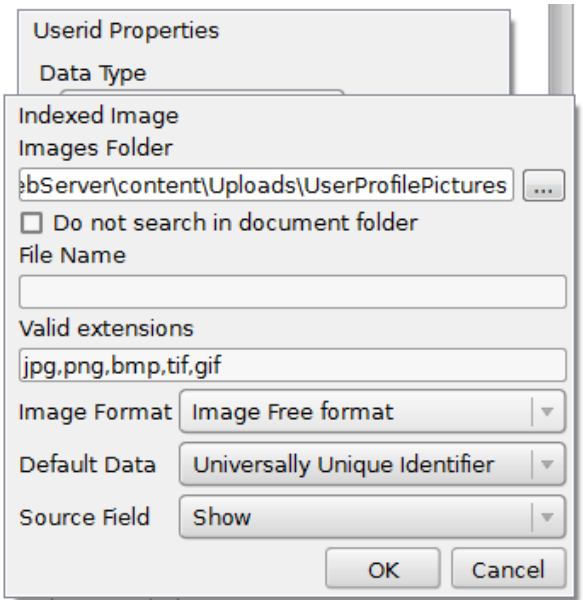


Figure 27.10. cardPresso® Index Image Properties



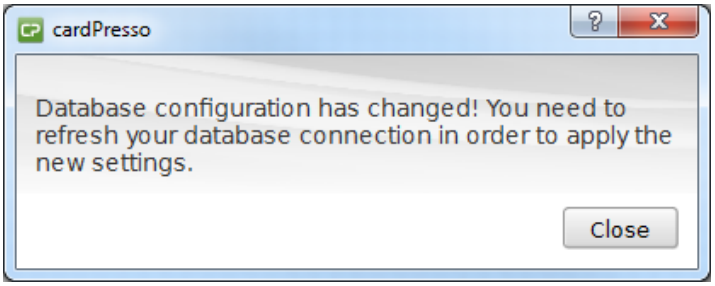
5. Change the **Images Folder** text box to "C:\Program Files (x86)\Hartmann Controls\Protector.Net \WebServer\content\Uploads\UserProfilePictures".

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 promoted that the database configuration has changed. Click the **Refresh Database** button on the database navigation bar.

Figure 27.11. Configuration Has Changed



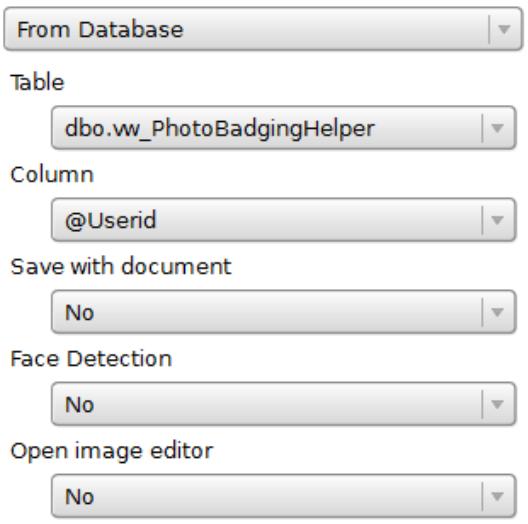
7. After refreshing the database, we can now add the picturebox to the card template, on the left hand side is a button called **Database Image** pictured and highlighted below.

Figure 27.12. 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 27.13. Imagebox Source Properties



We have finished configuring cardPresso®, and successfully tested a template. Each time you re-open cardPresso® you will need to re-connect 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 Protector.Net Web Interface

In this chapter we'll go through how to add images to a User through the Protector.Net 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 Protector.Net 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 on the top of the page. You will need to click **Allow** to give Protector.Net access to your camera device.
4. You can also take the card holder 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 Hartmann Controls 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 re-sellerr to order Assa Abloy products from Hartmann-Controls. Hartmann Controls is a certified reseller of Assa Abloy products.

Ensure you have the following items before proceeding to installation:

- Hartmann-Controls 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 Licence Key file*
- Aperio Wireless Locks

* Included in Aperio Kit

Hardware Setup

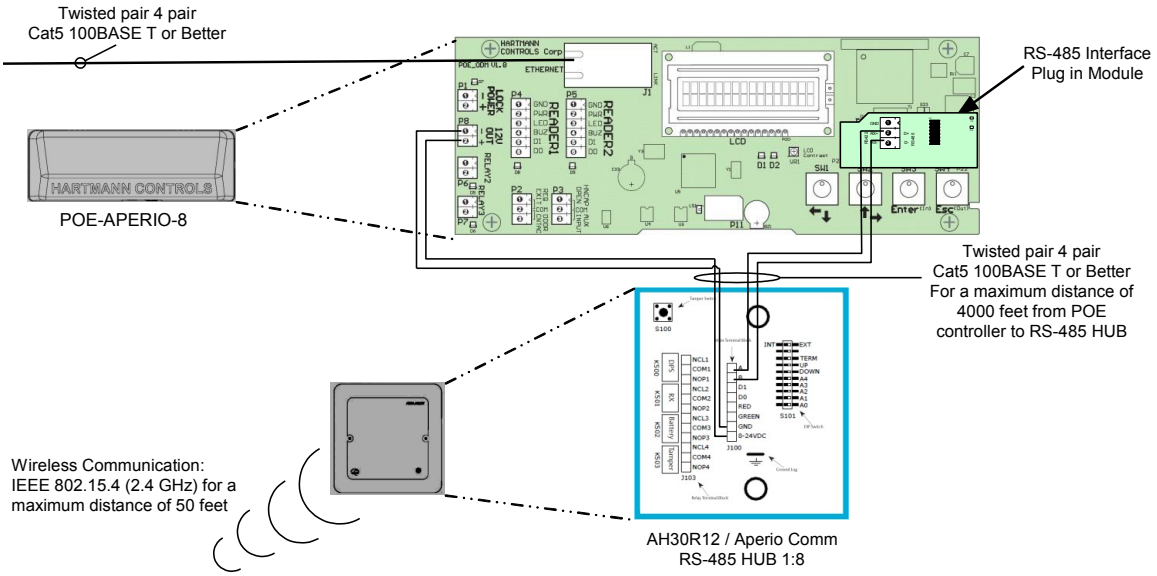
This section will cover the hardware aspect of connecting the Aperio Hub to the Hartmann-Controls Aperio Panel. This section includes visual references and cable specifications.

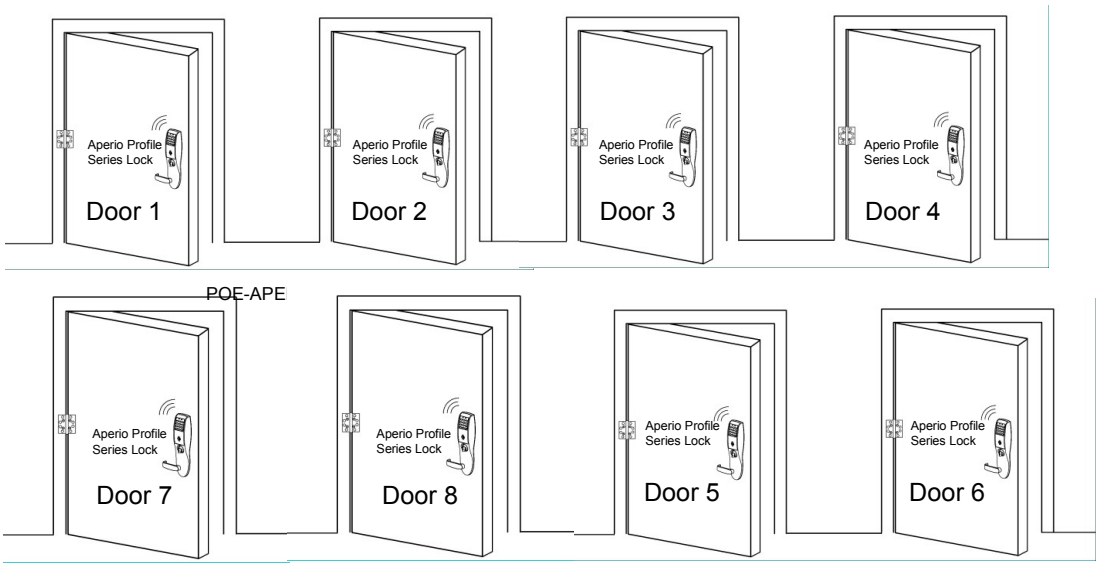
The Protector.Net PoE Aperio Panel communicates with the Aperio Hub via a RS-485 connection. A RS-485 Plug in module is included and installed in all Aperio Panels.

To connect the Aperio Panel to the Aperio Hub, please follow these steps:

1. Designate a pair of the RS-435 cable wires that will be providing power to the Aperio Hub from the Aperio Panel.
2. On the Panel side of the RS-435, connect the genitive 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-435 cable wires that will be providing communication to the Aperio Hub from the Aperio Panel.
5. On the Panel side of the RS-435 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.





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*
RS-485 Com. Cable	1300 m(4000')	Twisted Pair, 2 pairs	Cat5 100BASE-T or better

HARTMANN CONTROLS CORP.
Access Control Solutions

Site:	**Hartmann / Aperio Door Typical**
Drawing Type:	**Aperio Wireless locks to a Hartmann Controls Protector.Net ODM Interface # 1**
Drawn By:	*Joe Dineley* *May 9, 2014* *Rev:* *B*

Software Setup: Aperio Programming Application

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

1. On the laptop or PC you will be programming the Aperio Hub, download the Aperio Programming Application from your Aperio kit or from http://www.assaabloyresources.com.au/downloads/eac/Aperio_Common.zip

2. Unzip the Aperio_Common.zip to your computer and install the application.

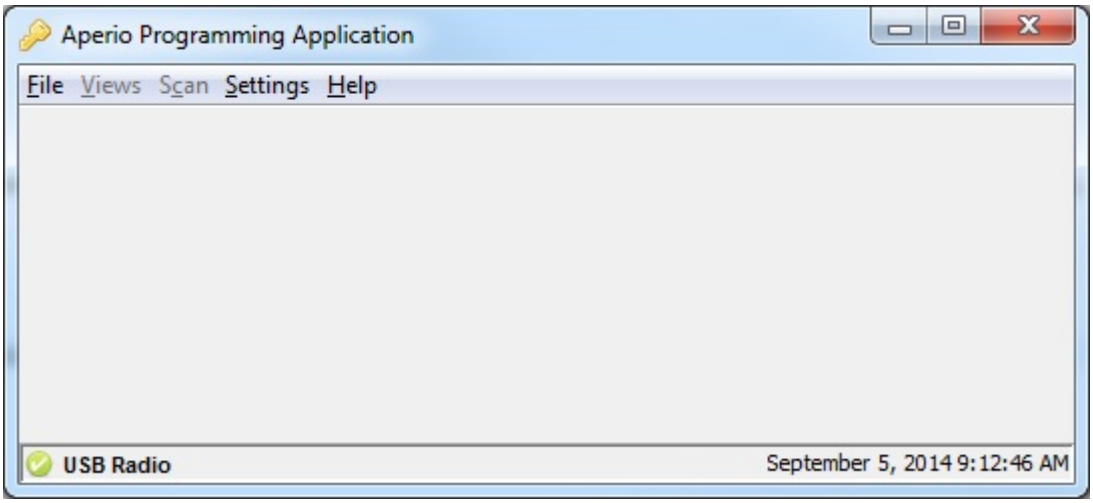
3. Plug in your Assa Abloy USB Radio Dongle and install the driver (located in the installation directory of the Aperio Programming Application).

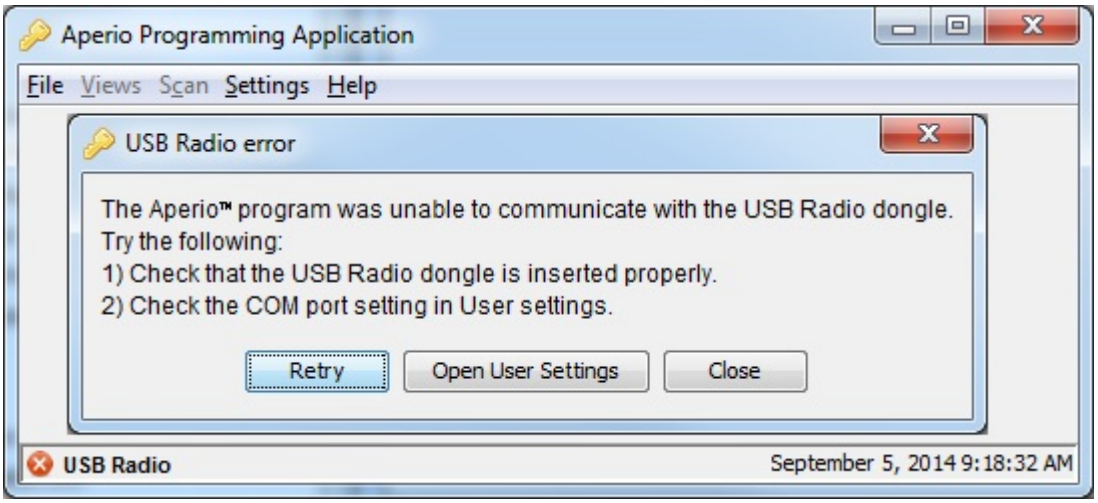
   ### Note

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

4. Ensure in Windows Device Manager that the "Tritech TriBee USB" is recognized and functioning.

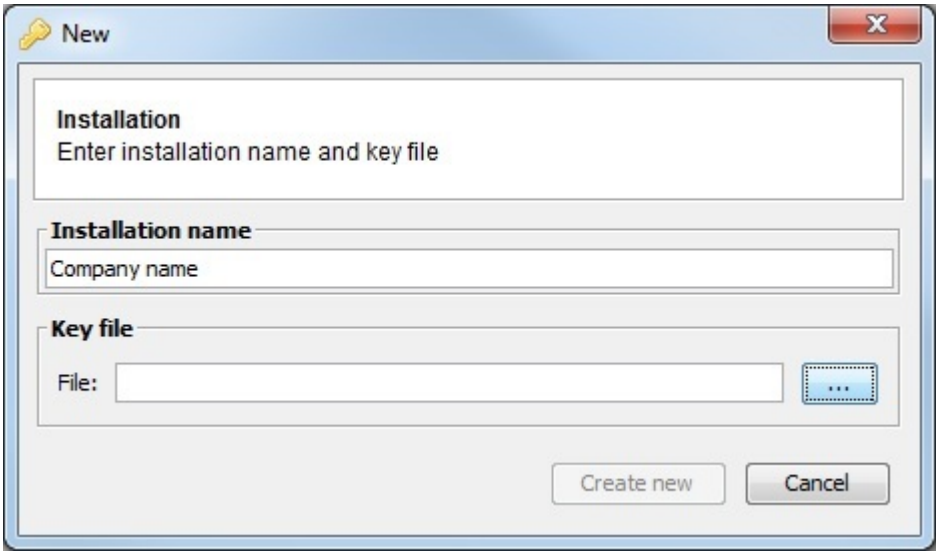
5. Launch the Aperio Programming Application from your start menu. If the Tritech Tribee is installed correctly and plugged in, you'll see a green circle in the bottom right side of the application next to USB Radio. If the USB dongle is not installed correctly or not connected to the PC/Laptop you'll receive an error.



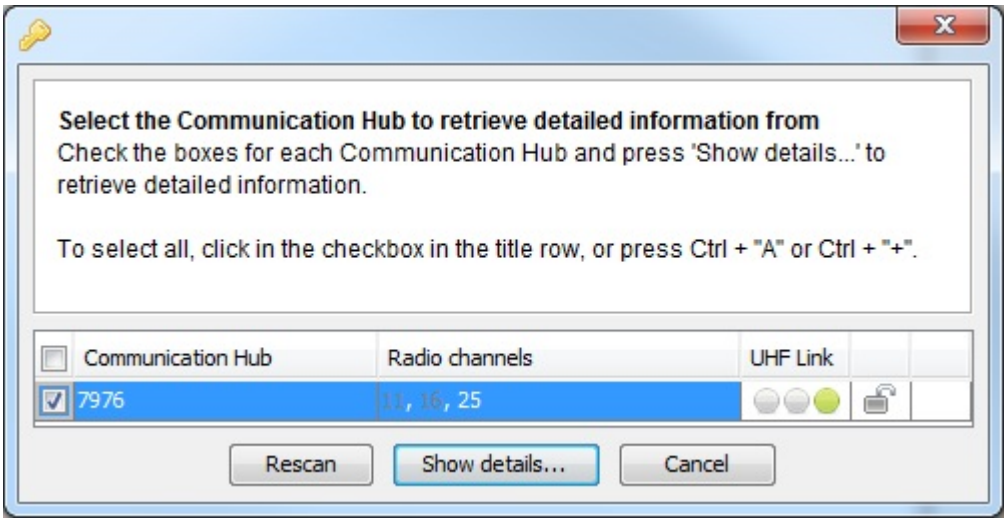


6. Once the Aperio Programming Application has detected your USB Radio, click File and then New on the top menu.

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 promoted 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...

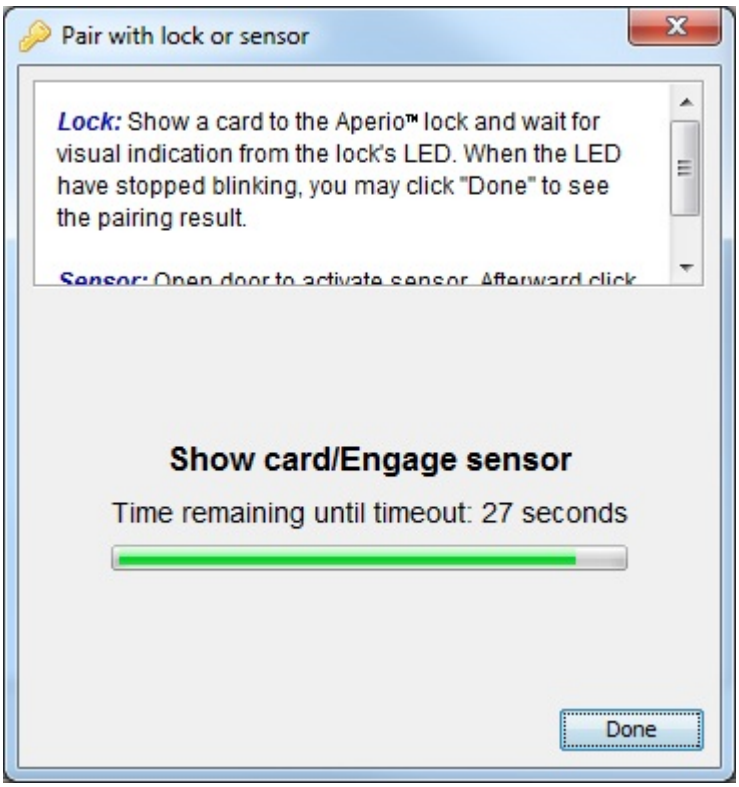


9. We can now begin paring our locks with the communication hub. Right click on the communication hub you wish to configure. Click the communication hub sub menu on the hub you wish to pair locks with, click "pair with lock or sensor".

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".



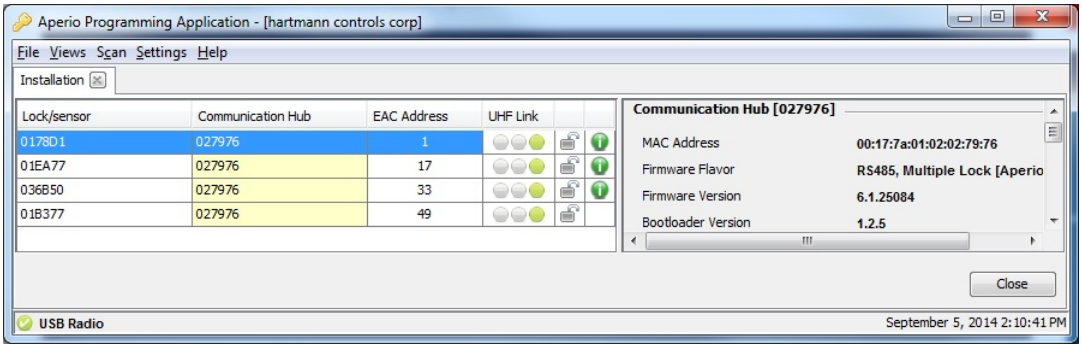
11. If the pairing is successful, you'll see "Communication Hub paired successfully to the following: XXXXXX" in the pair with lock or sensor window, where XXXXXX is the number printed on the back of the lock.

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 Protector.Net

Examples of 4 Locks synced within the Aperio Programming application



Software Setup: Protector.Net Aperio Panels and Doors

This section will cover the software aspect of adding Hartmann-Controls Aperio Panels to Protector.Net and configuring Aperio Locks into Protector.Net 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 Hartmann-Controls 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 ID's 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 ODM 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 Protector.Net”
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 like you would 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 28. Information for Network Administrators

Configuring Advanced Remote Access through the internet

This section will cover how to connect a Hartmann Controls Panel of any type to a Protector.Net server across the internet. This section will also cover how to connect a web browsing client to the Protector.Net server across the internet.

How Panels Communicate

The Protector.Net server is a listening device, it listens on **TCP Port 9876** for Panel connections. The Panels reach out to the server by either DNS name or IP.

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 reached the public IP address of the network where the Protector.Net 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 Protector.Net server. Once communication is established and the Panel is added in the Protector.Net 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.

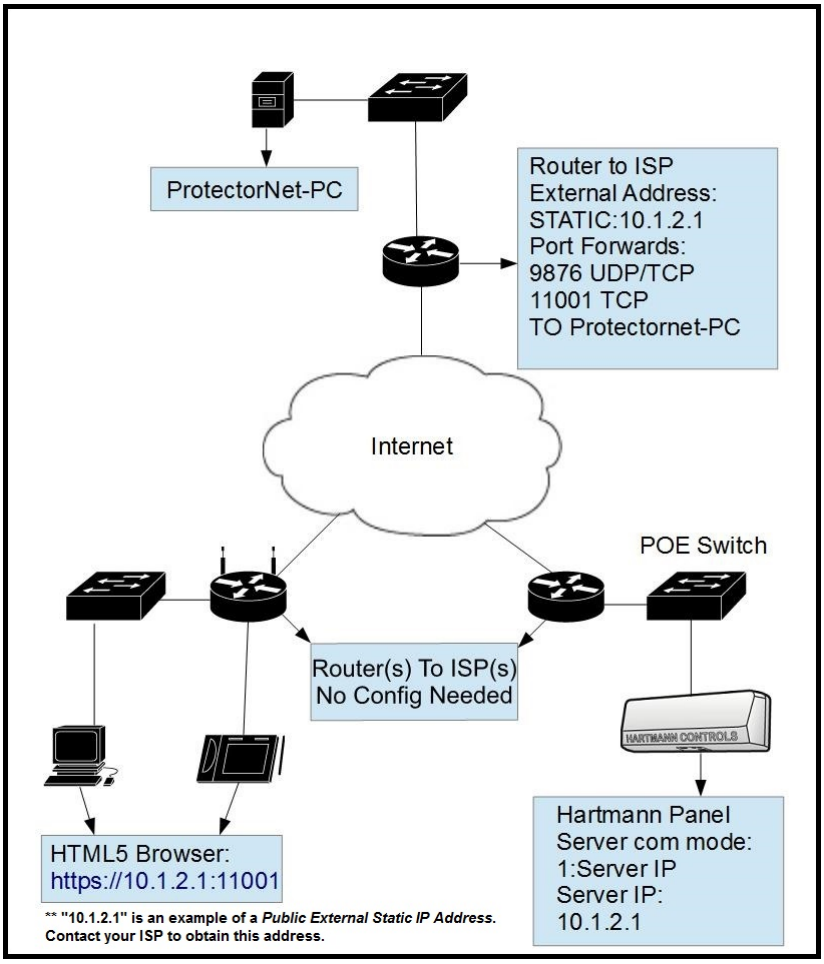
How Web Clients Communicate With Protector.Net

The Protector.Net 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 Protector.Net server will need to browse using the **Public Static IP Address** of the router connected to the private network the Protector.Net server resides on. The destination TCP port 11001 will need to be forwarded the internal address of the Protector.Net 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 28.1. Network Topology: Remote clients and Panels



Network Requirements

- The site with the Protector.Net 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.
- Protector.Net PC must have a static internal address.
- The main router on the site with the Protector.Net 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 be several internet companies (for a charge, or sometimes free). 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. Hartmann Controls 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 do not need any Port forwards or static addresses (In most cases) because they are calling out to the server using dynamic source ports. Only the site with the Protector.Net 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 Protector.Net 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 28.1. Terminology Reference

Term	Description
Protector.Net server	The computer (can also be a virtual machine) that the Protector.Net web service is running. This computer can be browsed to over the network or internet 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 examples scenarios of remote access, including scenarios where dealers/ installers will host the Protector.Net server

Example 1: Expansion Into Second Office. A business has expanded into a second office, and installs Hartmann Controls Door Panels in its second location. Instead of purchasing a second server and licence 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 obtain 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 Protector.Net server. They also make sure the Protector.Net 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 Protector.Net server.

Example 2: Dealer hosted Protector.Net server. A dealer/installer would like to host his clients Protector.Net servers at his office in order to provide maintenance, 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 clients, 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 Protector.Net. 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 Hartmann Controls 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 Hartmann Controls. Chapter 29, *Support*

SQL Database Back-up

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

1. On the computer with Protector.Net 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 .\ProtectorNet**' and press **Enter**. (ProtectorNet 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”)

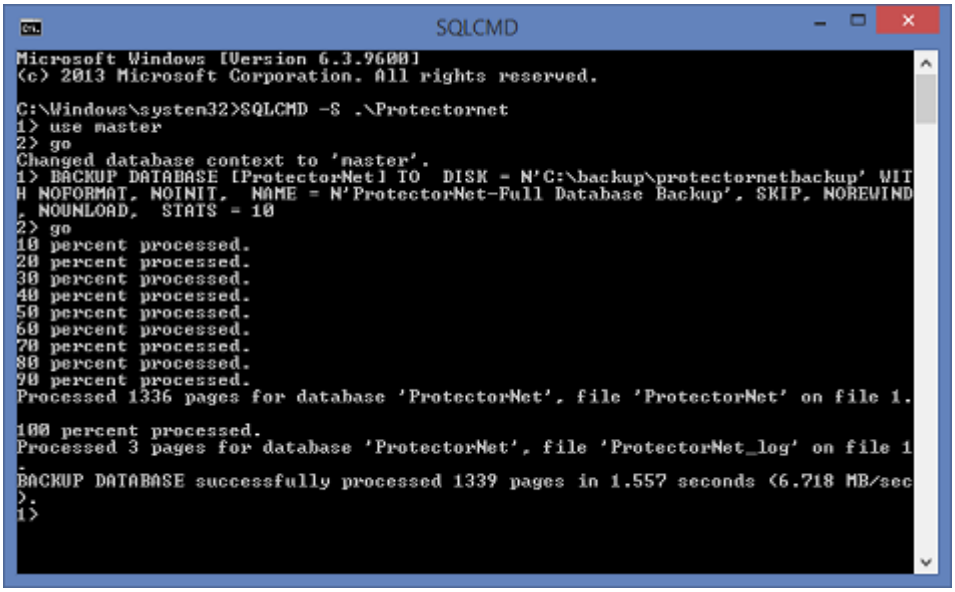
3. Type '**use [master]**' and press **Enter**. Type '**Go**' and press **Enter**.

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 [ProtectorNet] TO DISK = N'C:\backup\protectornetbackup' WITH NOFORMAT, NOINIT, NAME = N'ProtectorNet-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 28.2. Command Prompt: Backup



SQL Database Restore

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

1. Install Protector.Net on the computer that the database will be restored to. Ensure the version of Protector.Net installed is the same version or newer then 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:

   "**protector.Net_<dateofbackup>.prbak**" will need to be renamed to:

   "**protector.Net_<dateofbackup>.zip**".

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

4. Stop the Protector.Net 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 Protector.Net 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 .\ProtectorNet**' and press **Enter**. (ProtectorNet 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**.

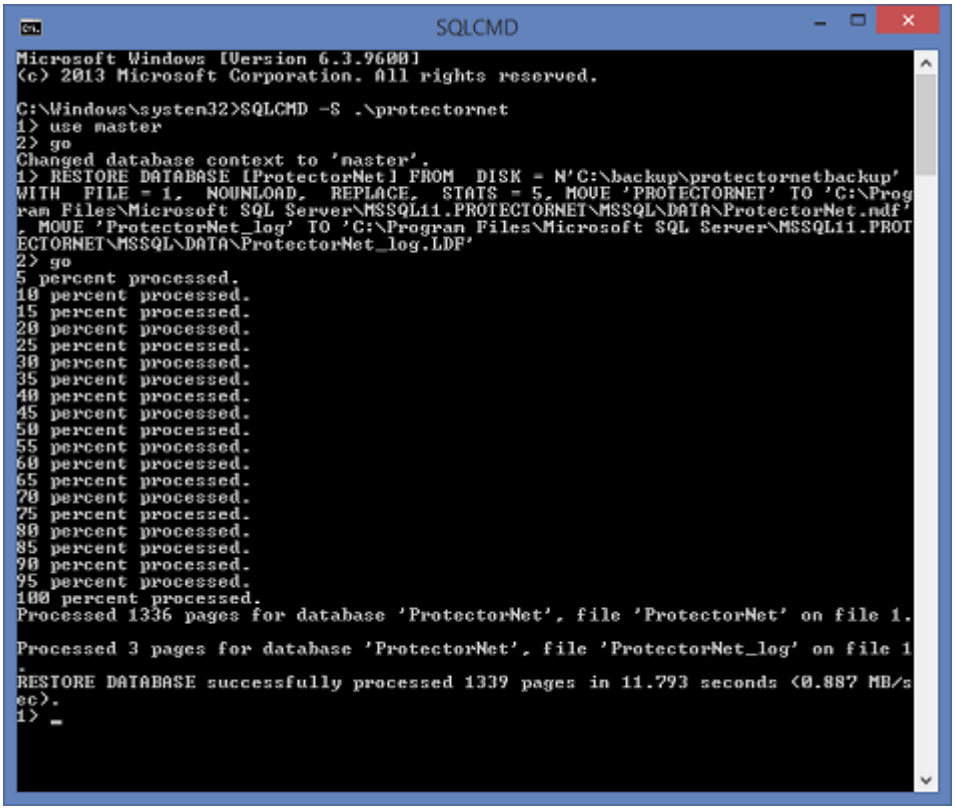
8. Type:

   '**RESTORE DATABASE [ProtectorNet] FROM DISK = N'C:\backup\protectornetbackup' WITH FILE = 1, NOUNLOAD, REPLACE, STATS = 5, MOVE 'PROTECTORNET' TO 'C:\Program Files\Microsoft SQL Server\MSSQL11.PROTECTORNET\MSSQL\DATA \ProtectorNet.mdf', MOVE 'ProtectorNet_log' TO 'C:\Program Files\Microsoft SQL Server \MSSQL11.PROTECTORNET\MSSQL\DATA\ProtectorNet_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 Protector.Net Web Service and login to confirm the backup was successful.

Figure 28.3. Command Prompt: Backup



Database Back-Up/Restore: Frequently Asked Questions

Q: Why didn't the built in Restore utility work?

A: Microsoft SQL Server is a fairly sophisticated piece of software, however the locations and behaviours 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 Protector.Net 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 Protector.Net installation using the following steps:

1. Browse to the WebServer folder of your Protector.Net installation directory (usually located in "C:\Program Files (x86)\Hartmann Controls\Protector.Net\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\ProtectorNet;' where 'pcname' is the name of your computer/server. The name after the PC is the name of the database instance Protector.Net is currently using.

Chapter 29. Support

Hartmann Controls world class support is available Monday to Friday between 9AM and 5PM est to assist with any installation related issues you may have.

Website

Hartmann Controls offers a number of technical guides and resources via our website: http://www.hartmann-controls.com

Email

Email support is available through our website at http://www.hartmann-controls.com/Company/Contact. 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:

- **Toll Free (North America only):** (877) 411-0101
- **Local Support:** (705) 719-6705
- **Fax:** (705) 792-5632

Chapter 30. 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 Protector.Net installation media, or contact Hartmann Controls.

Figure 30.1. Alarm Panel Interface

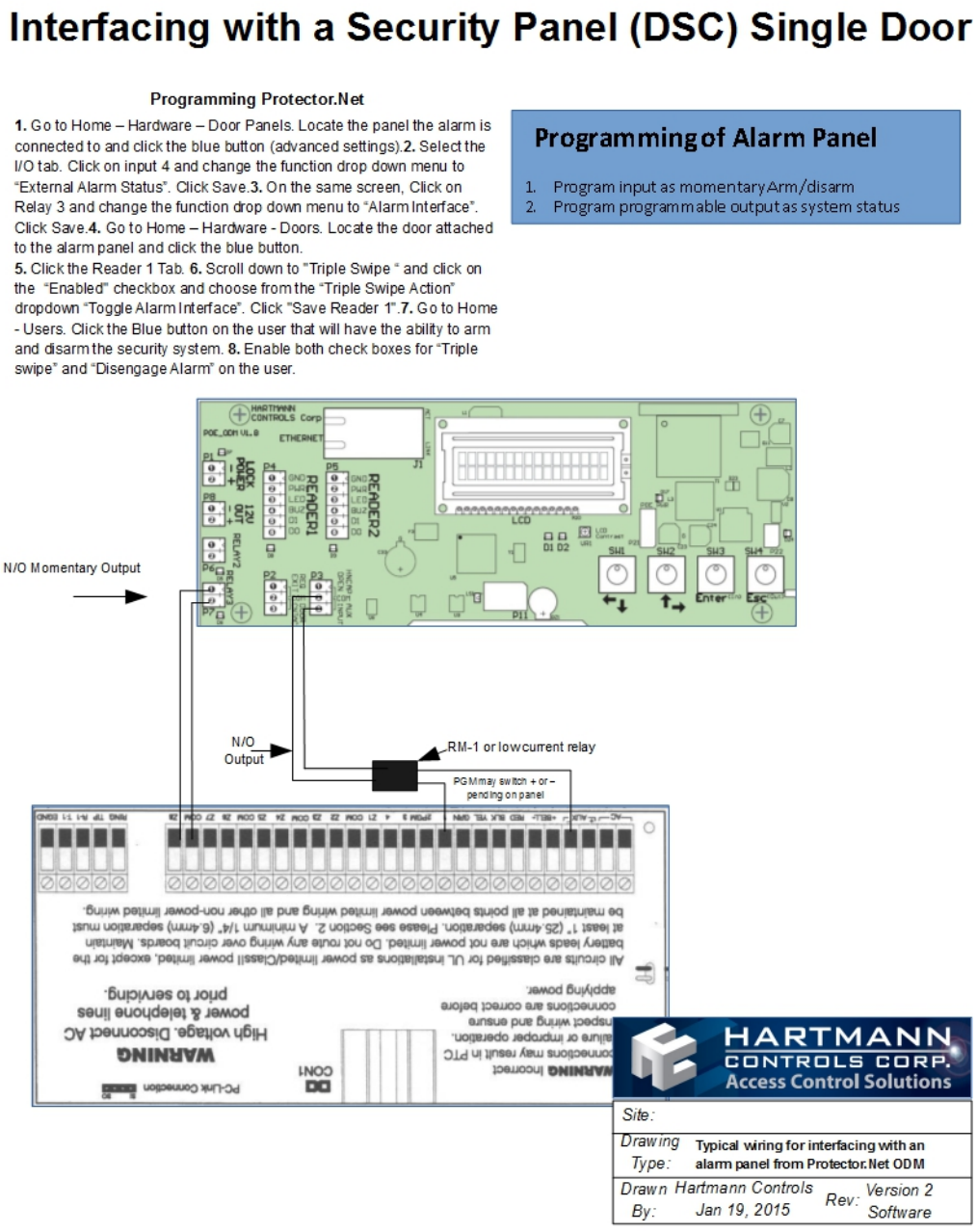


Figure 30.2. ODM Door Strike Typical

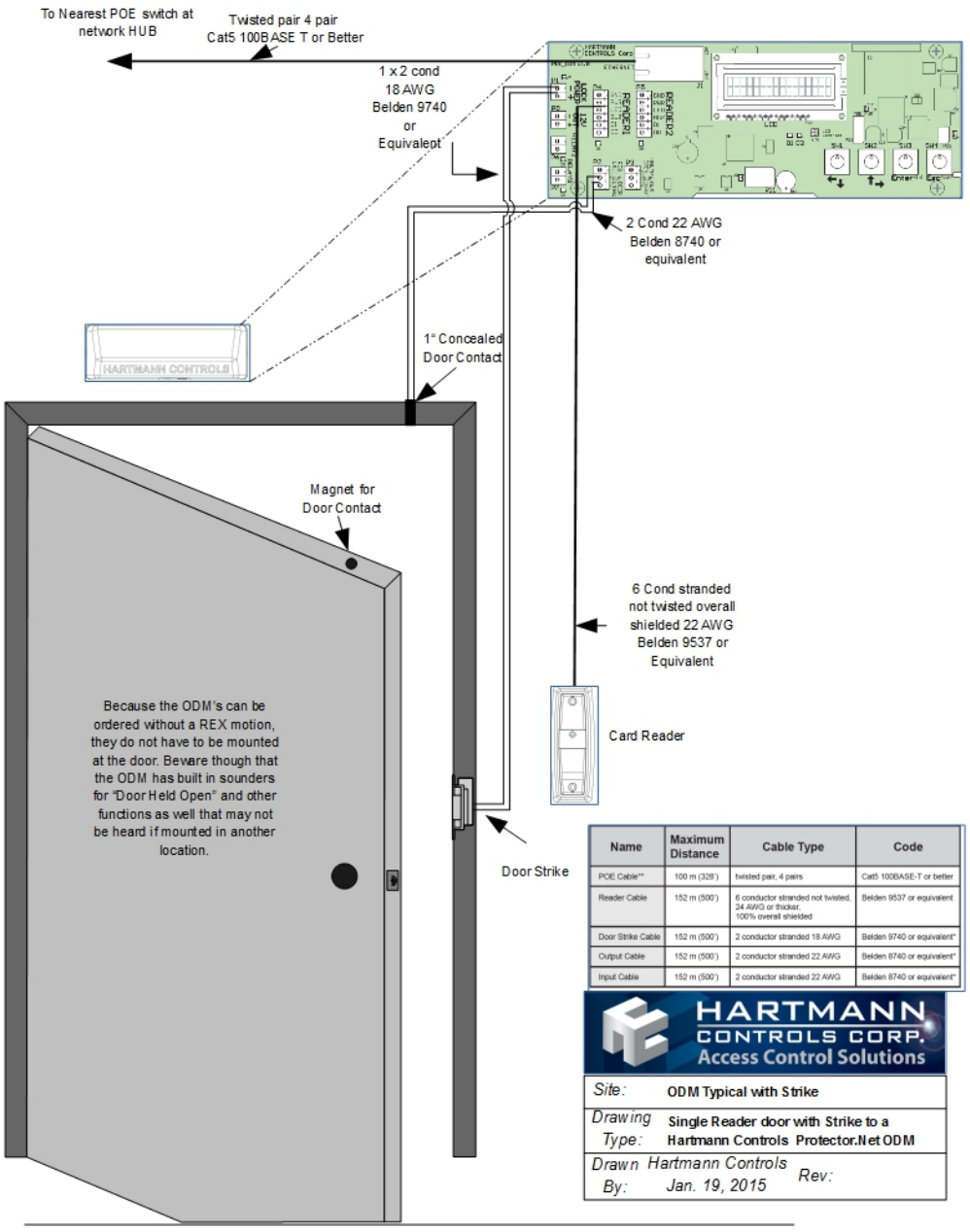


Figure 30.3. Hartmann ODM with Handicap Operator

Figure 30.4. Installation Example

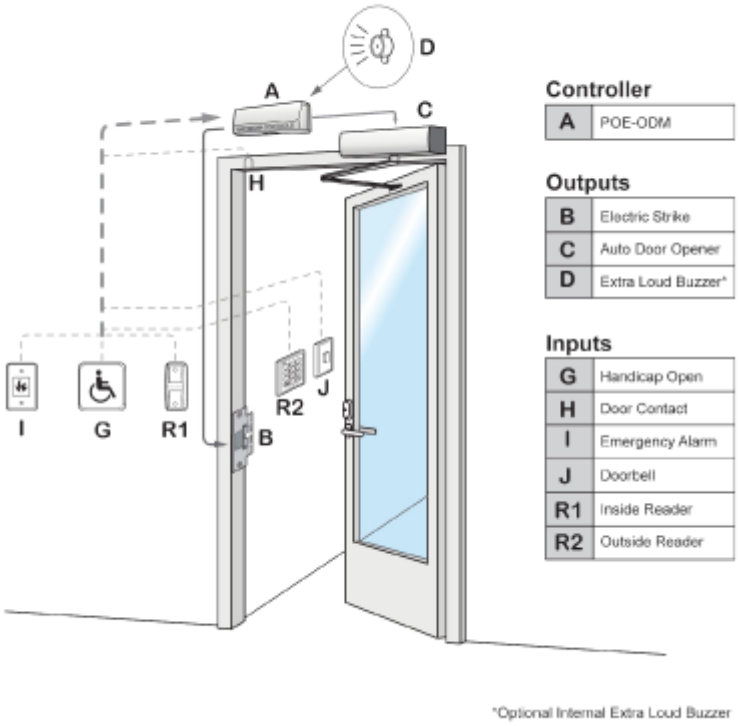


Figure 30.5. Single Door Typical Installation (with motion, single Reader, Door contact and auto opener)

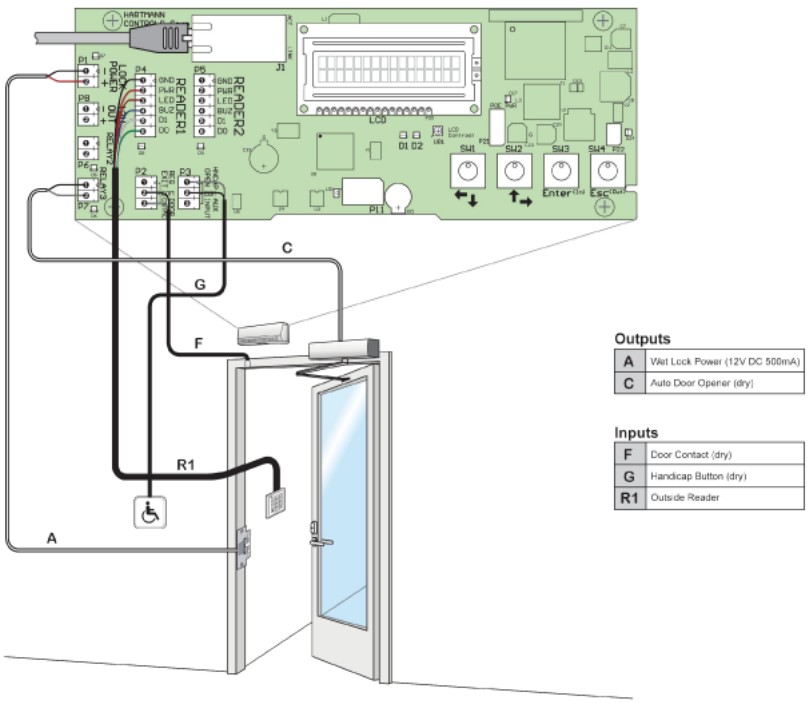


Figure 30.6. Cable Requirements

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.
** Recommanded the follownq T568B wiring for both ends.

T568B (TIA/EIA568B) Wiring

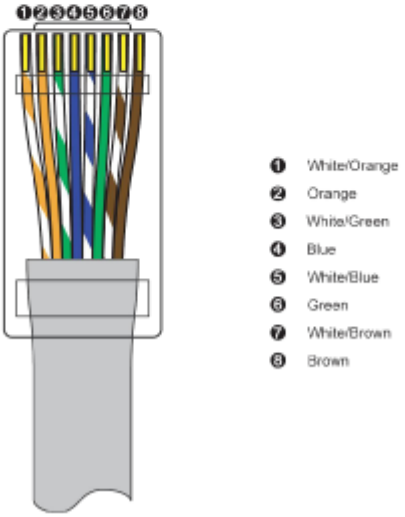


Figure 30.7. Package Contents

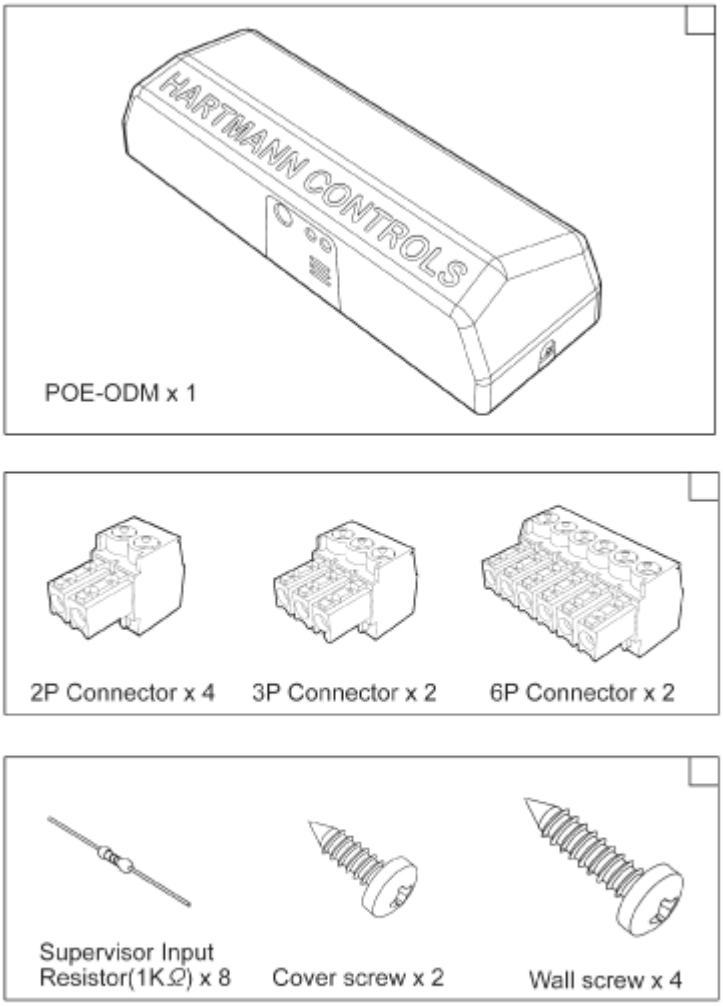


Figure 30.8. Network Examples

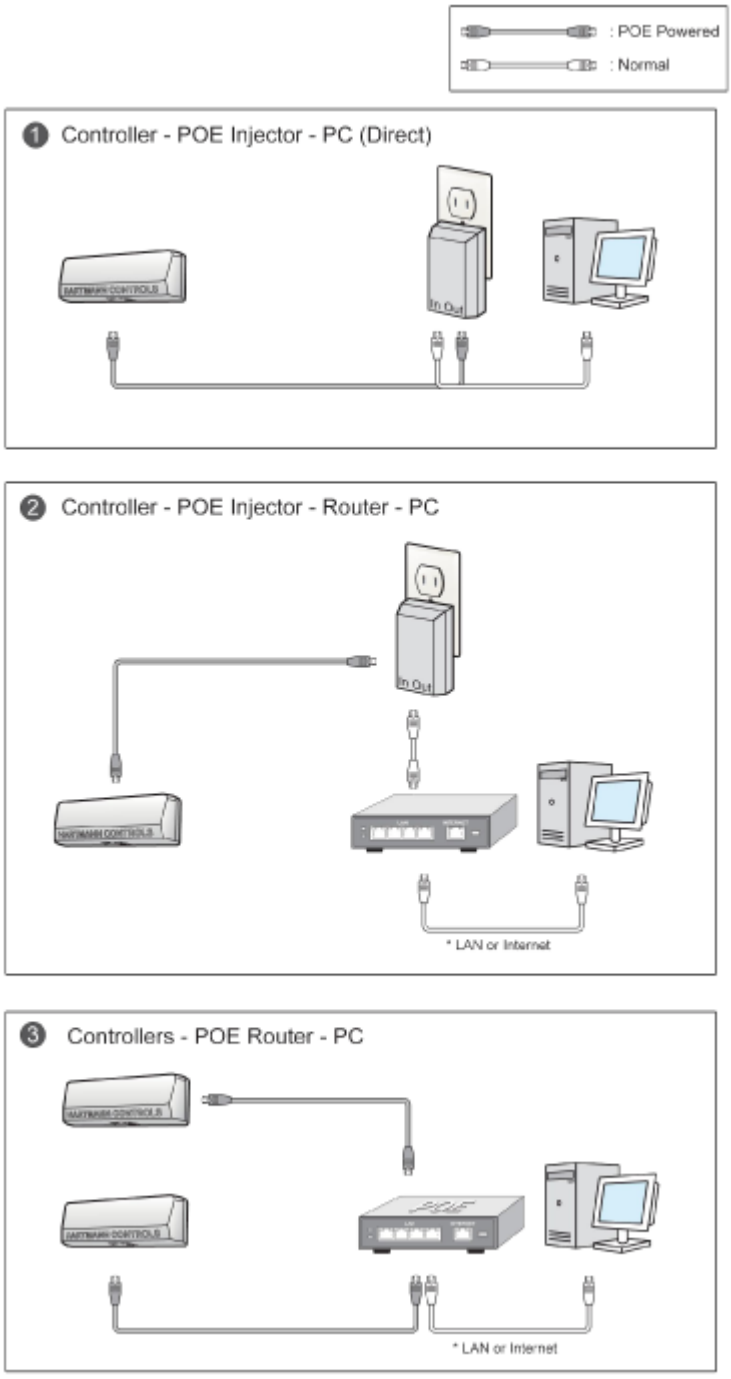


Figure 30.9. Network Examples Continued

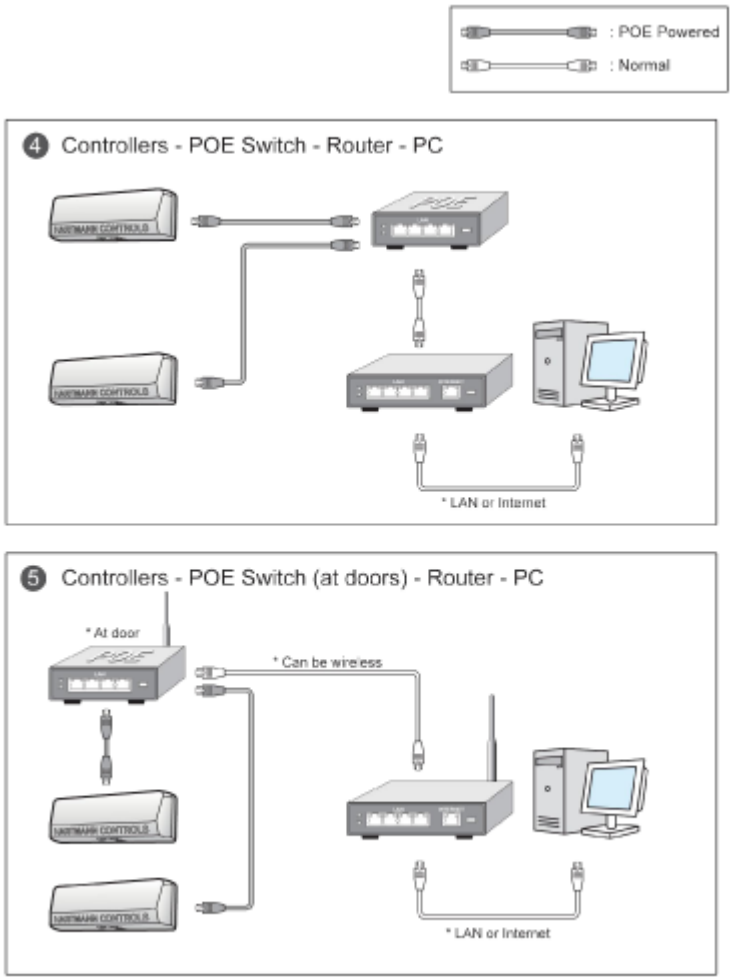
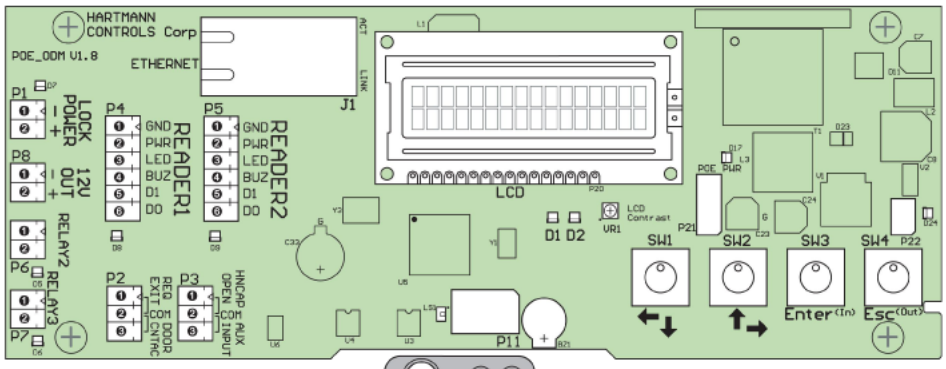


Figure 30.10. Panel Layout



LEDs

D1	System heart beat
D2	Server log on/off state Key pressed
D3	On: Server log off Blink: Server log in
D4	Green: Motion detected Red: Door Opened
D5	Relay2 on
D6	Relay3 on
D7	Relay1 on
D8	Reader1 data flow
D9	Reader2 data flow
D17	POE power
D24	CPU power
LINK	Ethernet linked
ACT	Ethernet Activity

Connectors

P1	Relay1, DC 12V wet contact
P2	Input1, Common, Input2
P3	Input3, Common, Input4
P4	Reader1
P5	Reader2
P6	Relay2
P7	Relay3
P8	DC 12V out
P11	Sensor module
P21	Expansion
P22	Expansion
J1	Ethernet

Keys

SW1	Left(↔), down(↓)
SW2	Right(↔), up(↑)
SW3	Enter, get in
SW4	Esc, exit

Etc

LS1	Tamper sensor
S1	Motion sensor
BZ1	Embedded buzzer
P20	LCD display
VR1	LCD contrast

Tools Menu Mode*

Get in	Up-Down-Down-Up (↑↓↓↑ in order.)
Get out	Esc
Move cursor	Up(Right),Down(Left)
Select menu	Enter
Exit menu	Esc

Setup Menu Edit Mode

Get in	Press and hold Enter (beeps after 2 sec) Enter password**
Toggle cursor	Enter White blink: move Black blink: edit
Get out	Esc
Move cursor	Up(Right),Down(Left)
Select menu	Enter
Exit menu	Esc

Setup Menu View Mode

Get in	Press and hold Esc (beeps after 2 sec)
Get out	Esc
Move cursor	Up(Right),Down(Left)
Select menu	Enter
Exit menu	Esc

Note

* For the first time installation, get in this mode and do following tests.
- Output Test : Toggle relays with Enter
- Input Test : Shows input states
- Reader Test : Shows scaned card info

** Contact us for the installer password
Toll Free: 1-877-411-0101

Figure 30.11. Panel Dimensions

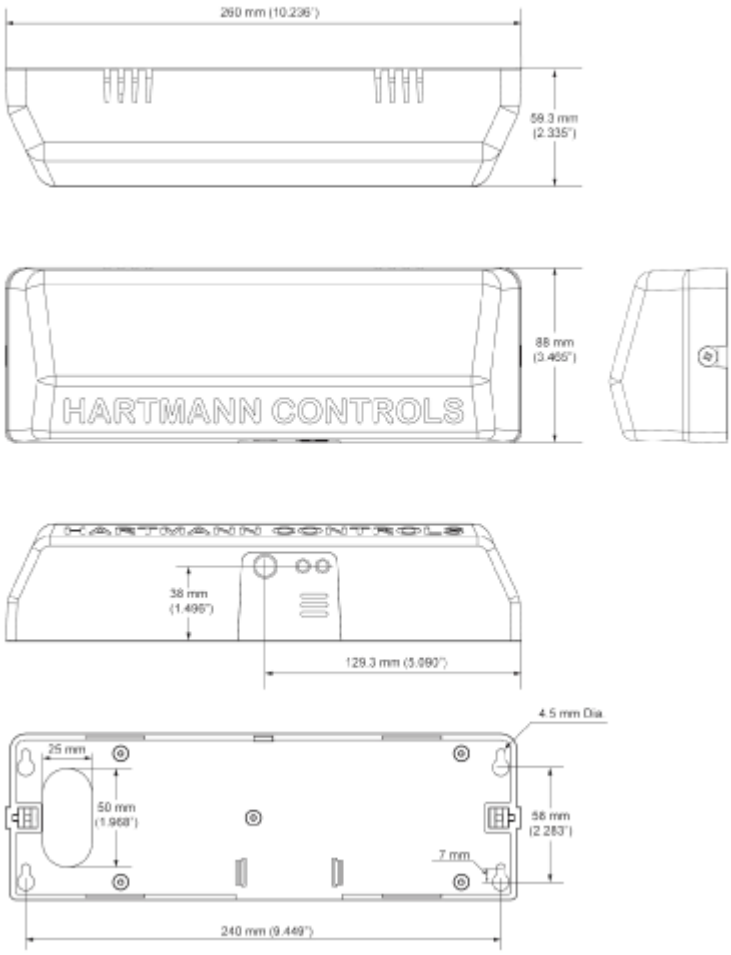


Figure 30.12. Input Types

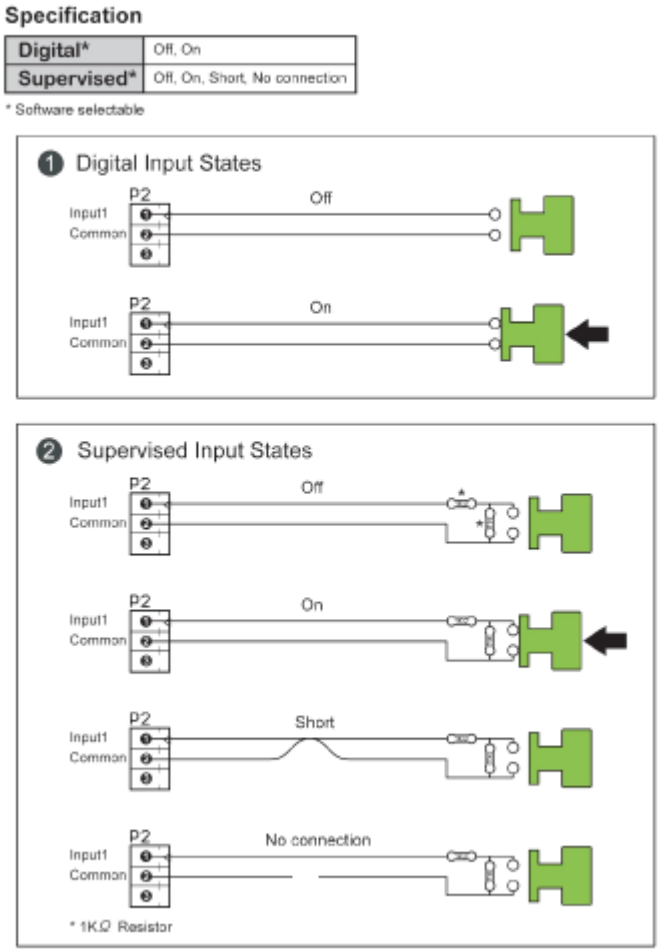


Figure 30.13. Input Example

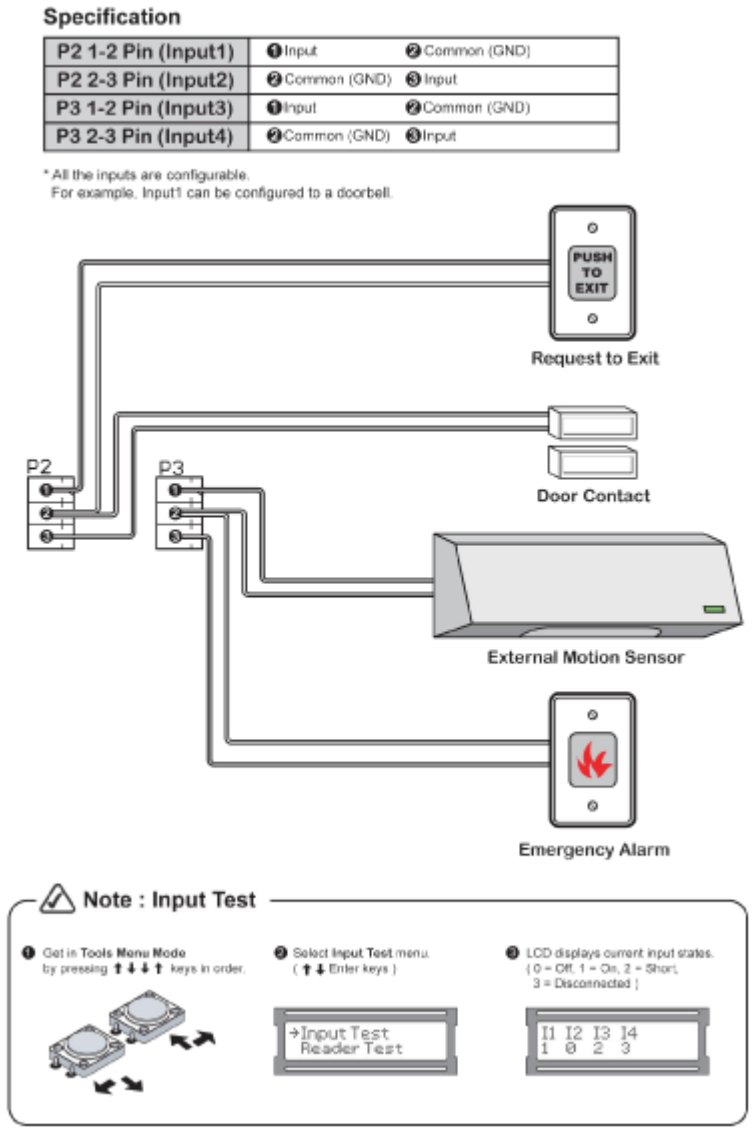
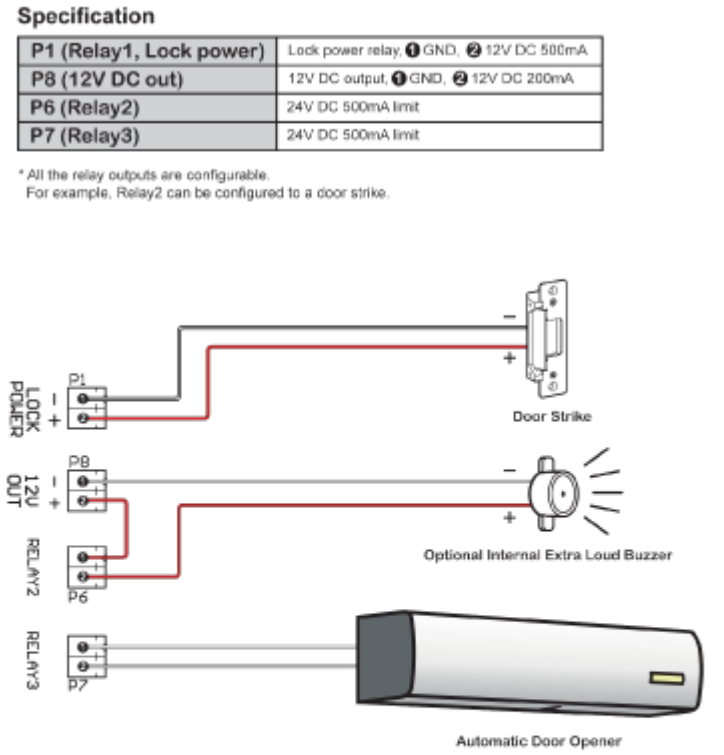


Figure 30.14. Relay Example



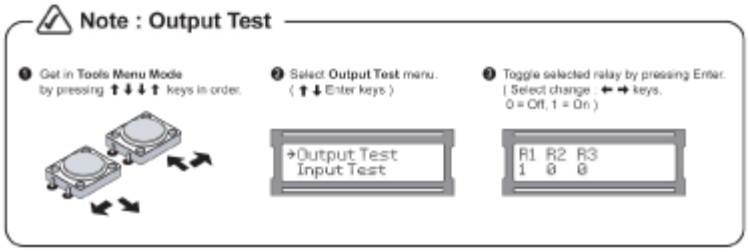


Figure 30.15. Reader Example

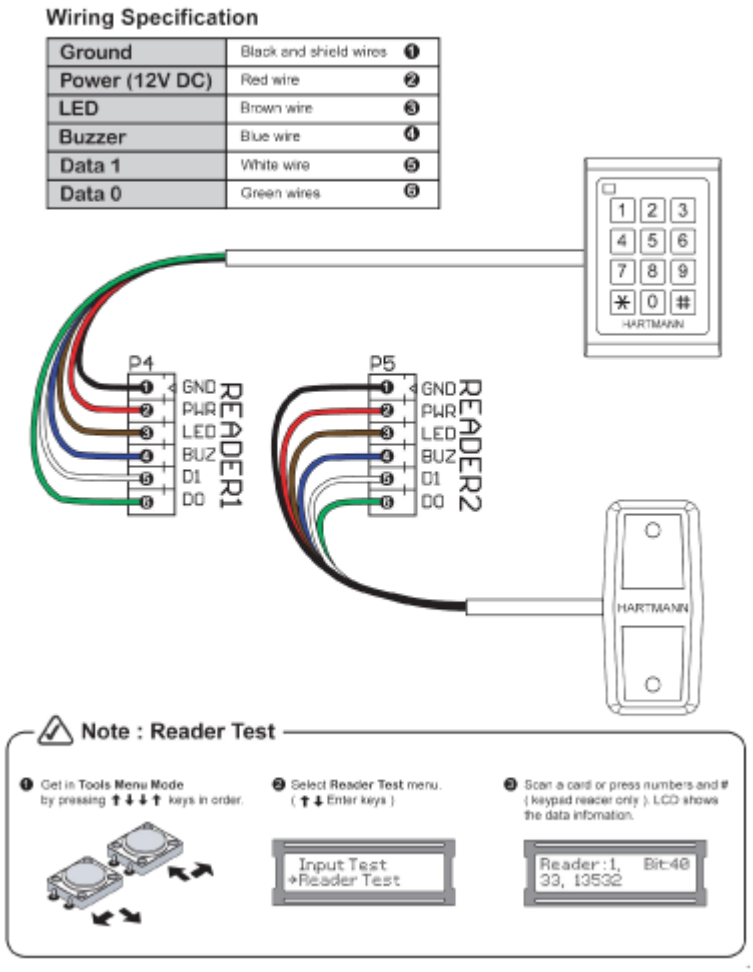
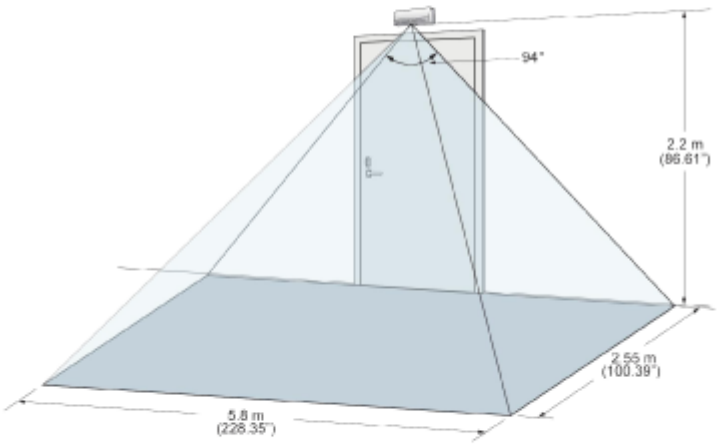


Figure 30.16. Motion Sensor

Specification

Sensor Type	PIR
Detection Range	5 m
Detection Angle	H: 94°, V: 82°
Detection Zone	64 zones



Appendix A. Appendix

Panel Model Reference

Table A.1. Panel Model Reference

Model	Max Doors	Max Readers	Motion REX	Brief Explanation
POE-ODM-X	1	2	No	Over The Door Module with PoE Power
POE-ODM-M	1	1	Yes	Over The Door Module with PoE Power and Integrated Motion
POE-TDM	2	2	No	Two Door Module with PoE Power
POE-TDM-M	2	2	Yes	Two Door Module with PoE Power and Integrated Motion
POE-APERIO-2	2	2	No	ASSA ABLOY Aperio master controller capable of controlling up to 2 Aperio devices via 1 - 2 Aperio Hubs
POE-APERIO-4	4	4	No	ASSA ABLOY Aperio master controller capable of controlling up to 4 Aperio devices via 1 - 4 Aperio Hubs
POE-APERIO-8	8	8	No	ASSA ABLOY Aperio master controller capable of controlling up to 8 Aperio devices via 1 - 8 Aperio Hubs
POE-Elevator-64	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.

WARRANTY AND SPECIAL PROVISIONS

WARRANTY AND SPECIAL PROVISIONS FOR THE UNITED STATES OF AMERICA, CANADA ANY OTHER COUNTRY . LIMITED WARRANTY: Hartmann Controls Corp. 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, Hartmann Controls Corp. 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 Hartmann Controls Corp. 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 Hartmann Controls Corp. has been advised of the possibility of such damages. In any case, Hartmann Controls Corp. 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.

Hartmann Controls Corp.

Phone: 1-877-411-0101 (Toll Free Canada/USA)

Fax: + 705-792-5632

Web site: www.hartmann-controls.com