PRT-WX-DIN

Using Protege WX

Installation and Programming Manual

ICTProtegeWX®

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited. Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Publication Date: June 2013

Contents

Introduction

Protege WX is an all-in-one, web-based, cross-platform system that gives you a fully functional access control and intrusion detection solution in a fraction of the time of conventional software. With no software to install, setup is quick and simple. Connect the Controller and system components, then open a web browser to launch the intuitive wizard-driven interface which guides you through the process of configuring your system.

Operation Mode

Protege WX launches in basic mode with full access control and intrusion detection ready to go. This hides the more complicated features making the system more intuitive and simple to use. Undertake an optional training course to become a 'WXpert' and unlock the advanced features including building automation, programmable functions, and elevator control.

This manual covers basic mode only. Documentation on the advanced features is available upon enrolment on the Protege WX training course. To find out more about training and unlocking advanced mode, please contact ICT.

What This Manual Covers

This manual is broken into the following sections:

- System Installation and Setup: Connecting the components that make up your system
- Getting Started: Logging in and using the initial configuration Wizards to setup your site
- Monitoring Your System: Using the Events page, Status Lists, and LED Indicators to show what is happening
- Property Reference Guide: An explanation of the available programming options and what they do
- Maintaining Your System: Basic system maintenance, including how to backup and restore Controller programming, and update firmware
- Troubleshooting: Helpful troubleshooting information, including how to resolve health status messages

System Expansion and Capacities

The modular-based hardware design provides the flexibility to accommodate any installation whether it’s small, large, residential or commercial. Optional expandable modules allow you to scale your system as your requirements change. Need more PIRs? Add a Protege Input Expander. Want more doors? Add a Protege Reader Expander.

If you reach capacity, you can easily upgrade to the enterprise level Protege GX. (Note that Protege GX can only be purchased and installed by current members of the ICT Dealer Network)

System Capacities	Protege WX System	Protege GX System
Users	10,000	Unlimited
Events	50,000	Unlimited
Schedules	512	Unlimited
Doors	32	Unlimited
Areas	32	Unlimited
Inputs	512	Unlimited
Outputs	512	Unlimited
Keypad and Expander Modules	32	Unlimited

Technical Specifications

The following specifications are important and vital to the correct operation of the Controller. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void. Integrated Control Technology continually strives to increase the performance of its products. As a result these specifications may change without notice. We recommend consulting the ICT website (http://www.incontrol.co.nz) for the latest documentation and product information.

Operating Voltage	11-14V DC
Operating Current	120mA (Typical)
DC Output (Auxiliary)	0.7A (Typical) Electronic Shutdown at 1.1A
Bell DC Output (Continuous)	8 Ohm 30W Siren or 1.1A (Typical) Electronic Shutdown at 1.6A
Bell DC Output (Inrush)	1500mA
Total Combined Current*	3.4A (Max)
Electronic Disconnection	9.0VDC
Communication (Ethernet)	1 10/100Mbps Ethernet Communication Link
Communication (Serial)	1 RS-485 Communication Interface Port
Communication (Modem)	1 2400bps Modem Communication
Readers (Standard Mode)	2 Wiegand or Clock Data Readers providing one entry/exit Door or two entry/exit only doors
Readers (Multiplex-reader Mode)	4 Wiegand Readers (connected in multiplex reader mode) providing any combination of entry or exit for two doors
Inputs (System Inputs)	8 High Security Monitored Inputs
Outputs	4 50mA (Max) Open Collector Outputs for reader LED and beeper or general functions
Relay Outputs	2 FORM C Relays - 7A 250V max
Operating Temperature	0°-49°C (32° - 122°F)
Storage Temperature	-10°- 85°C (14° - 185°F)
Humidity	0%-93% non condensing, indoor use only (relative humidity)
Dimensions (L x W x H)	156 x 90 x 60mm (6.14 x 3.54 x 2.36")
Weight	376g (13.26oz)

* The **Total Combined Current** refers to the current that will be drawn from the external power supply to supply the Controller itself as well as any devices connected to the outputs of the Controller. The Auxiliary outputs and Bell output are directly connected via electronic fuses to the N+ N- input terminals, and the maximum current is governed by the trip level of these fuses.

System Installation and Setup

The following section outlines what you need to do to install your Protege WX system. The process is broken into the following steps.

1. Mount the Controller (see page 8)
2. Connect the Power Supply (see page 9)
3. Connect any networked modules (see page 12) (such as Reader Expanders and Keypad units)
4. Connect Card Readers (see page 13)
5. Connect Door Contacts (see page 15)
6. Connect Lock Outputs (see page 16)
7. Connect the Ethernet 10/100 Network Interface (see page 16)
8. Connect the Telephone Dialer (see page 17) (only required if using Contact ID for Offsite Monitoring)
9. Connect Inputs (see page 17)
10. Connect Outputs (see page 19)

> When installing hardware, it is important you ensure there is adequate clearance around all sides of the unit and that air flow to the vents is not restricted. We recommend installing the Controller and any expansion devices in a location that allows easy access for wiring such as electrical rooms, communication equipment rooms, closets, or in an accessible area of the ceiling.

Mount the Controller

The Controller is designed to be mounted on standard DIN Rail either in dedicated DIN cabinets or on generic DIN Rail mounting strip. A section of DIN Rail strip is provided as a mounting option.

To mount the Controller:

1. Hook the lower tabs under the bottom edge of the DIN Rail.
2. Push the Controller against the DIN Rail mount until the upper tab clips over the upper rail.

To remove the Controller:

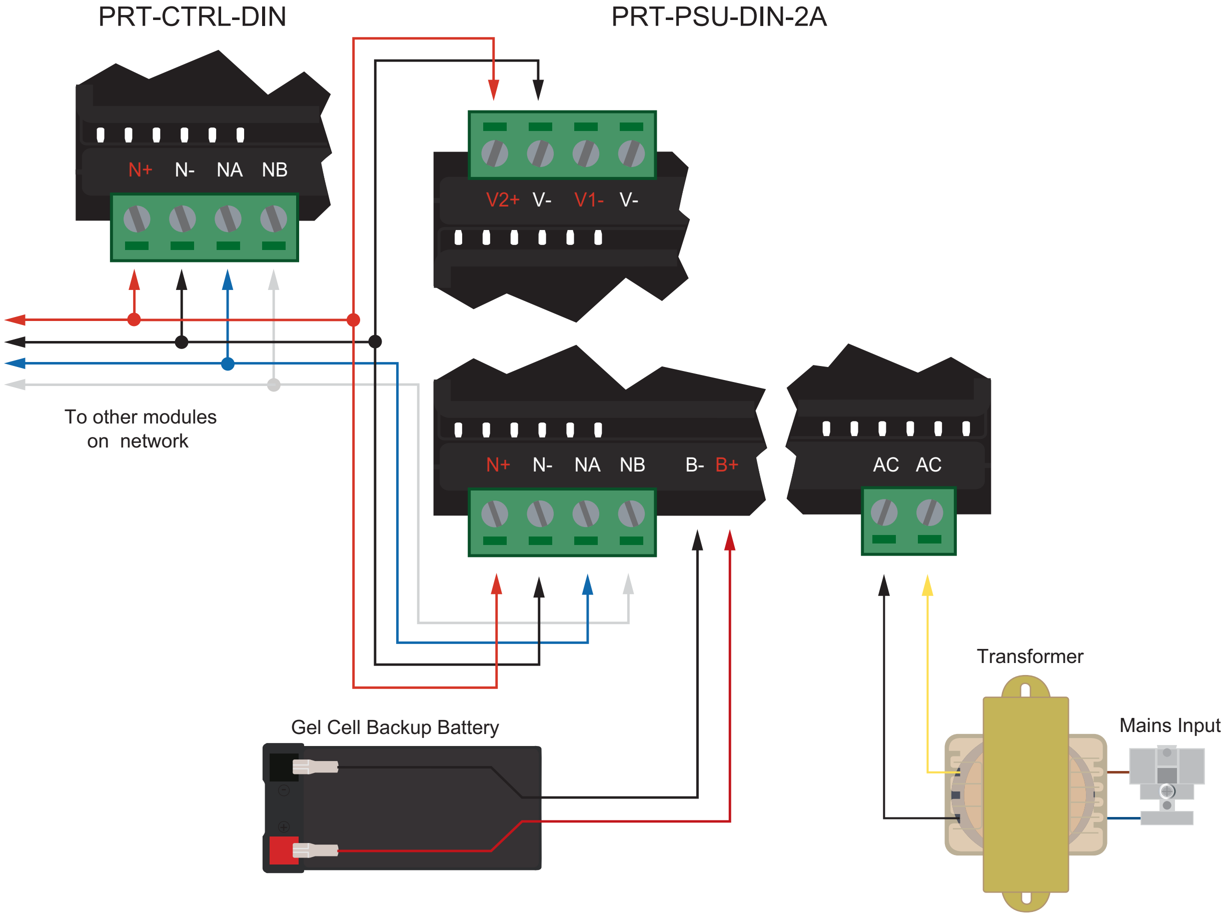
1. Insert a flat blade screwdriver into the hole in the tab at the top of the Controller.
2. Lever the tab up and rotate the unit off the DIN Rail mount.

Connect the Power Supply

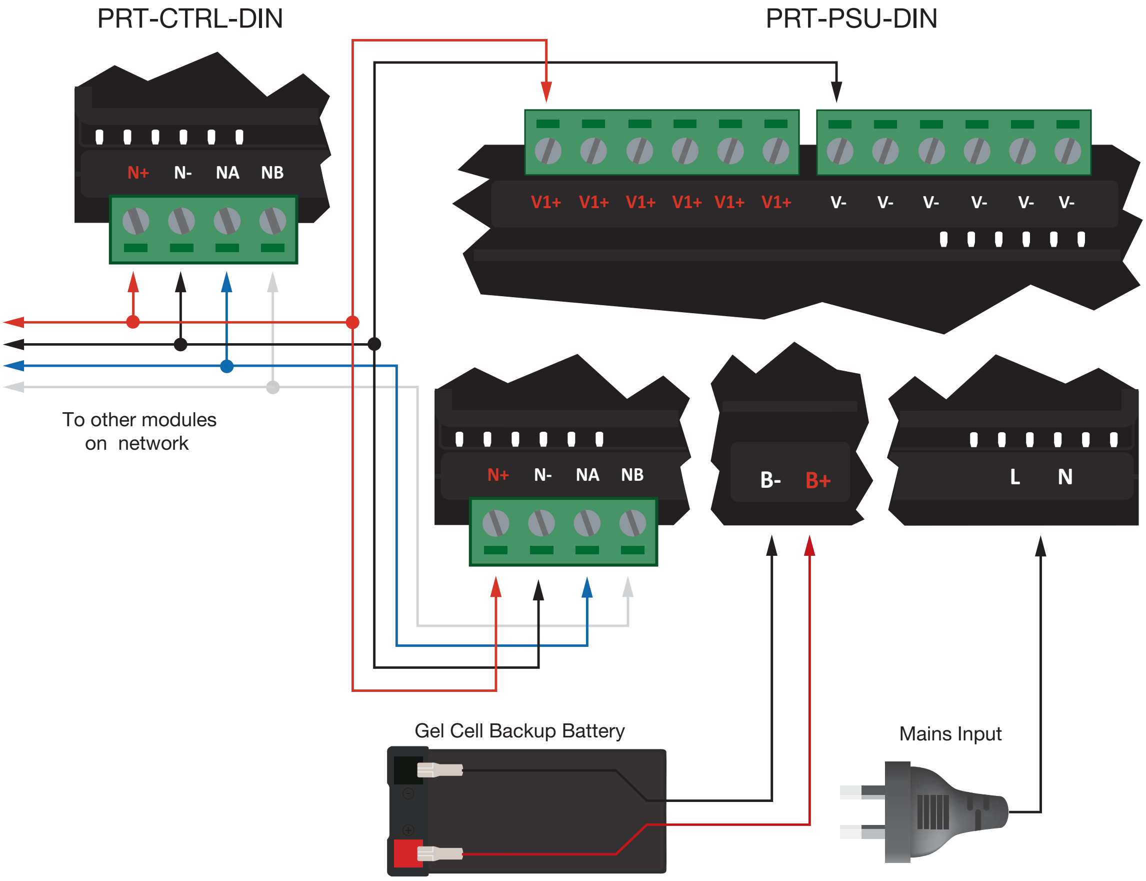
Power is supplied to the Controller by a 12V DC power supply connected to the N+ and N- terminals. The Controller does not contain internal regulation or isolation and we recommend using an ICT PRT-PSU-DIN for this purpose, although any clean 12V DC supply is suitable.

Warning: Termination of wiring to the Controller while power is applied or the battery is connected may cause serious damage to the unit and will VOID ALL WARRANTIES OR GUARANTEES. **Power the unit only after all wiring, configuration and jumper settings are completed.**

If using a PRT-PSU-DIN module, a battery backup must be connected to the module network to provide a monitored supply. The battery plays an important role in power conditioning and provides a continuous source of power in the event of a power outage.

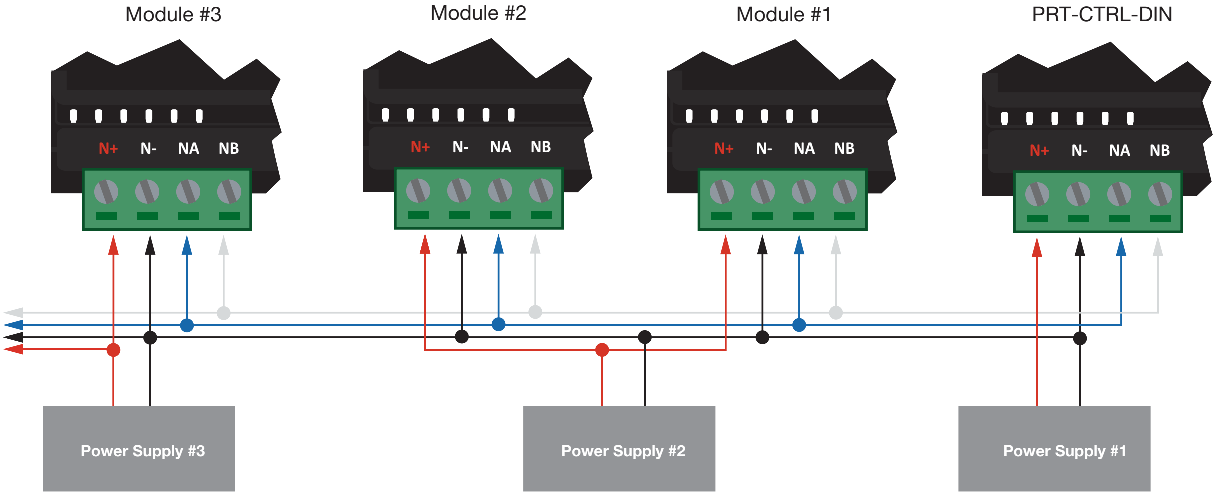


Example Power Supply Connection - PRT-PSU-DIN-2A



Example Power Supply Connection - PRT-PSU-DIN-4A

In a small installation this same power supply can be used to supply the module network as well, so long as the maximum load of the power supply is not exceeded. In larger installations, the power supply may need to be split to allow for load sharing between several supplies.



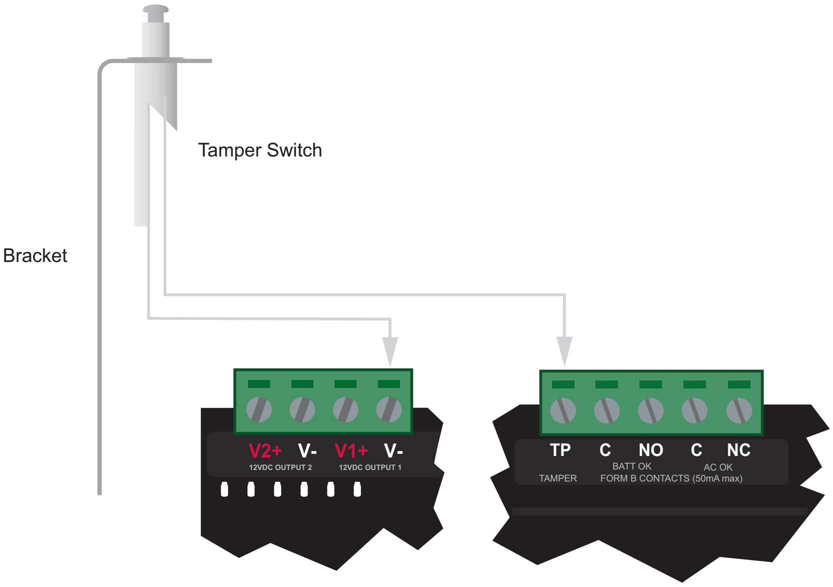
Example Multiple PSU Connection

Warning: When using multiple power supplies it is important to ensure that all ground connections (V-) are connected between all power supplies and that no power connections (V+) are connected between any power supplies.

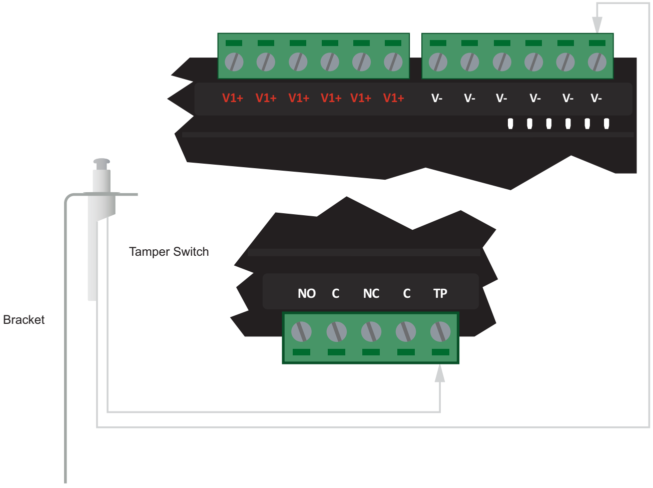
The auxiliary outputs (V- V+) of the PRT-CTRL-DIN can be used to supply other equipment. Note that there is no onboard regulation or isolation for these outputs and they are a fused feed-through from the N+ N- input terminals. When using these outputs to supply other devices, you need to ensure you do not exceed the rating of the internal fuses as described in the Technical Specifications (see page 7).

Cabinet Tamper Switch

The enclosure tamper input signals to the monitoring station or remote computer that the enclosure has been opened. The tamper input switch should be mounted into the steel bracket provided and connected to the tamper connection terminal and the V- terminal as shown below. The tamper input opens and closes trouble input AExxx:01 on the Power Supply.



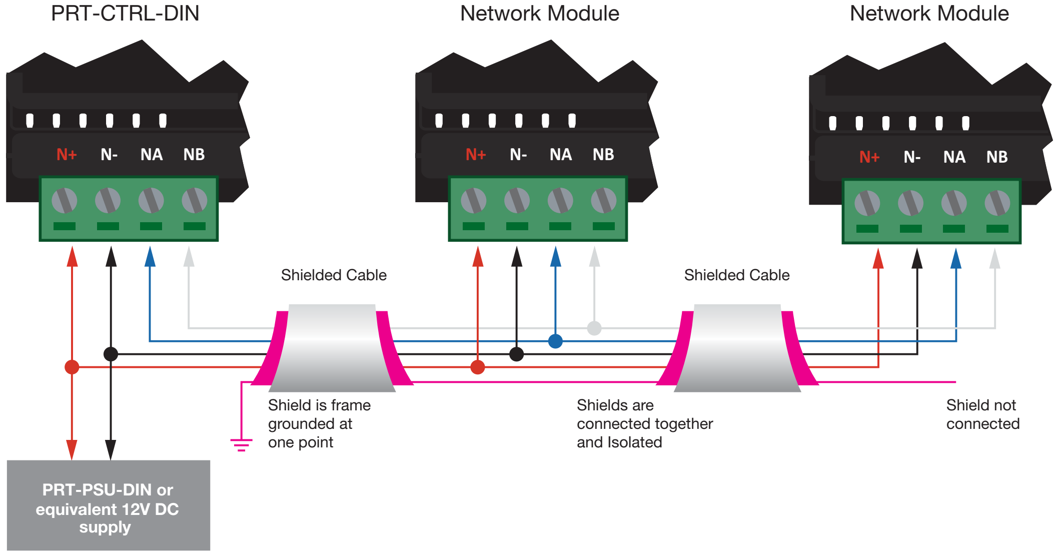
Tamper Input Connection - PRT-PSU-DIN-2A



Tamper Input Connection - PRT-PSU-DIN-4A

Connect Networked Modules

The Controller incorporates encrypted RS-485 communications technology for connecting networked modules.



PRT-CTRL-DIN
Network Module
Network Module
N+
N-
NA
NB
Shielded Cable
Shielded Cable
Shield is frame grounded at one point
Shields are connected together and Isolated
Shield not connected
PRT-PSU-DIN or equivalent 12V DC supply

Standard Network Communication Connection

Always connect the Controller's NA and NB terminals to the NA and NB terminals of the expansion devices and keypads. The N+ and N- must connect to a 12V power supply source capable of supplying the peak current drawn by all modules. If a shielded cable is used, the shield must be connected at only one end of the cable. DO NOT connect a shield at both ends.

Warning:

- The 12V N+ and N- communication input must be supplied from only one point. Connections from more than one 12V supply may cause failure or damage to the units supplying power.
- Make sure that the power supply can provide enough current for the peak load drawn by all modules connected to the 12V supply, including the Controller itself.

Module Wiring

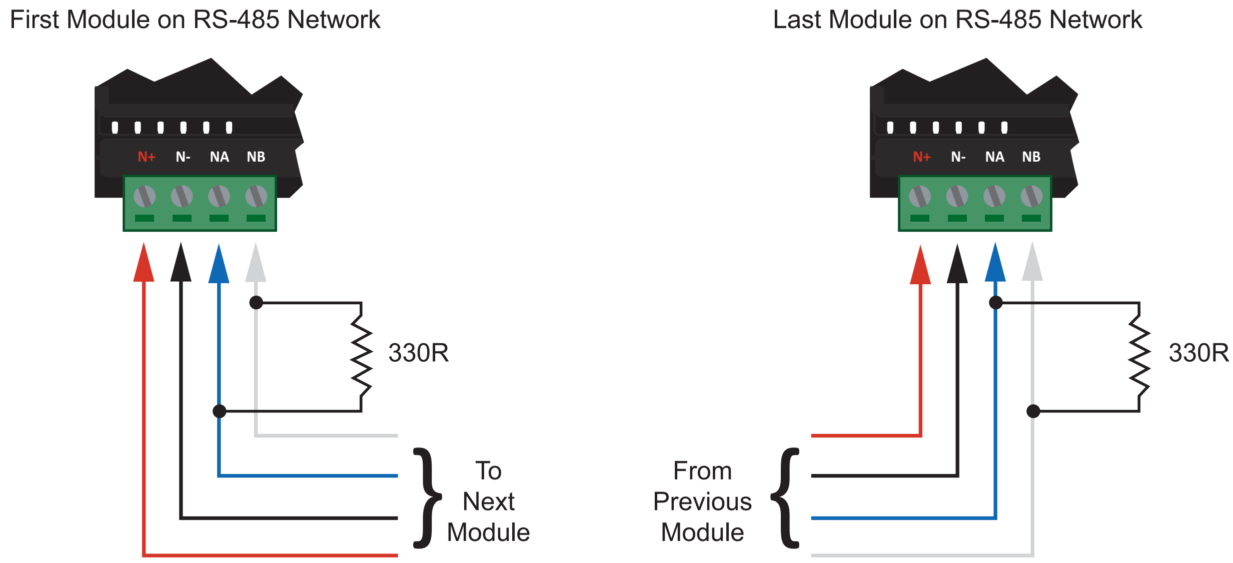
The recommended module network wiring specifications are:

- Belden 9842 or equivalent
- 24AWG twisted pair with characteristic impedance of 120ohm
- Maximum total length of cable is max 900m (3000ft)
- CAT5e / CAT6 are also supported for data transmission when using ground in the same cable (to a maximum length 100m (328ft))

Warning: Unused wires in the cable must not be used to carry power to other devices.

End of Line (EOL) Resistors

The 330 Ohm EOL (End of Line) resistor provided in the accessory bag must be inserted between the NA and NB terminals of the first and last modules on the RS-485 network. These are the modules physically located at the ends of the RS-485 network cabling.



End of Line Resistors

Connect Card Readers

The Controller provides onboard access control. This enables you to connect two Wiegand devices to control two doors (entry or exit only), or - if the Controller is configured for multiplex mode - enables you to connect four Wiegand devices to control two doors giving the flexibility of entry and exit readers, without the need for additional hardware.

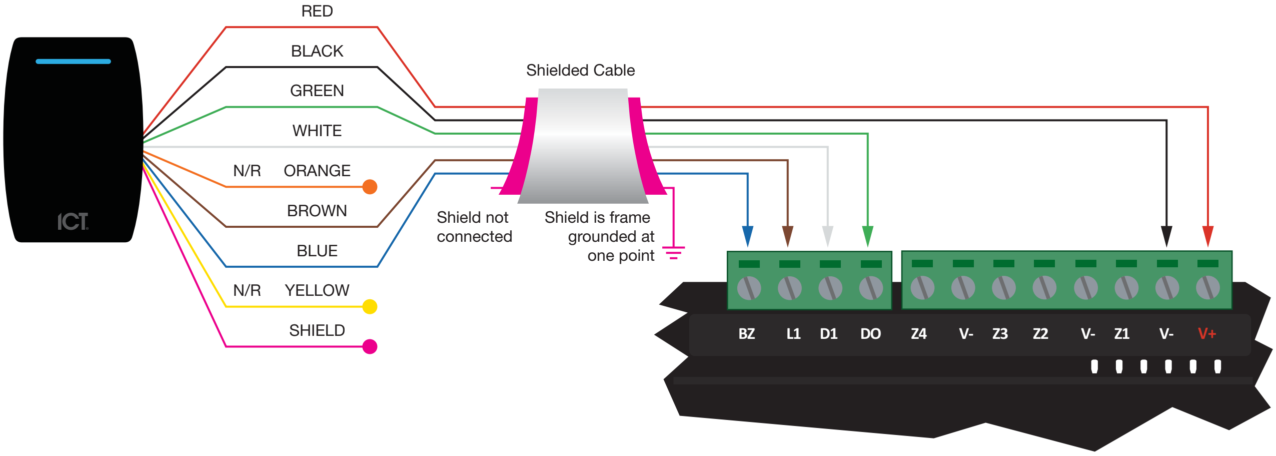
Important:

- Card readers must be connected to the Controller port using a shielded cable.
- The shield connection must only be connected at one end of the cable in the metallic enclosure (frame grounded).
- Do not connect the shield to a V- connection on the Controller.
- Do not join the shield and black wires at the reading device.
- Do not connect the shield to any shield used for isolated communication.
- Always refer to the card reader manufacturer for detailed installation guidelines.

All Protege Readers are shipped with single LED mode set as default.

Standard Card Reader Connection

The following diagram shows the connection of a standard Wiegand Reader with the Controller controlling an access door in entry or exit mode (2 doors, 2 readers).

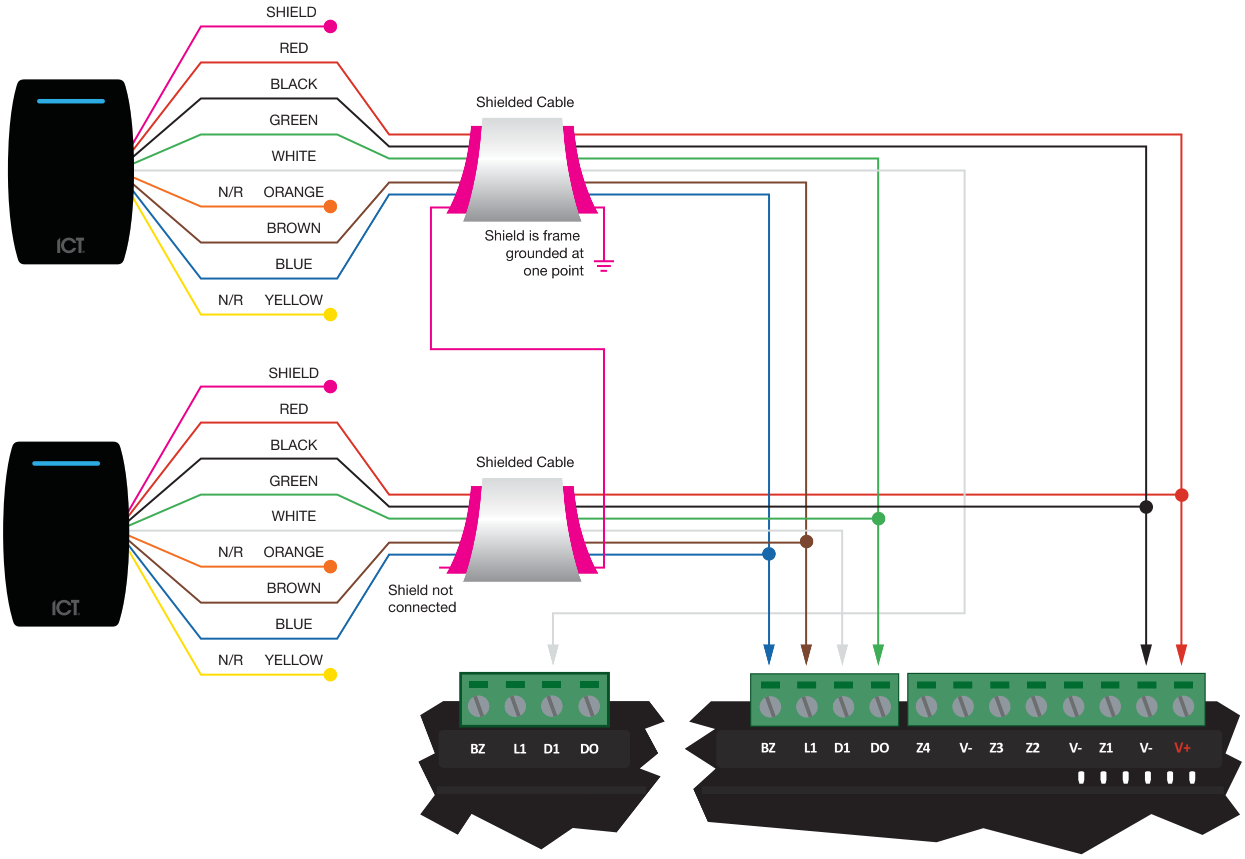


Card Reader Connection

Multiplex Card Reader Connection

Multiplex reader mode allows the connection of 4 Wiegand reading devices controlling two doors each with entry/exit readers.

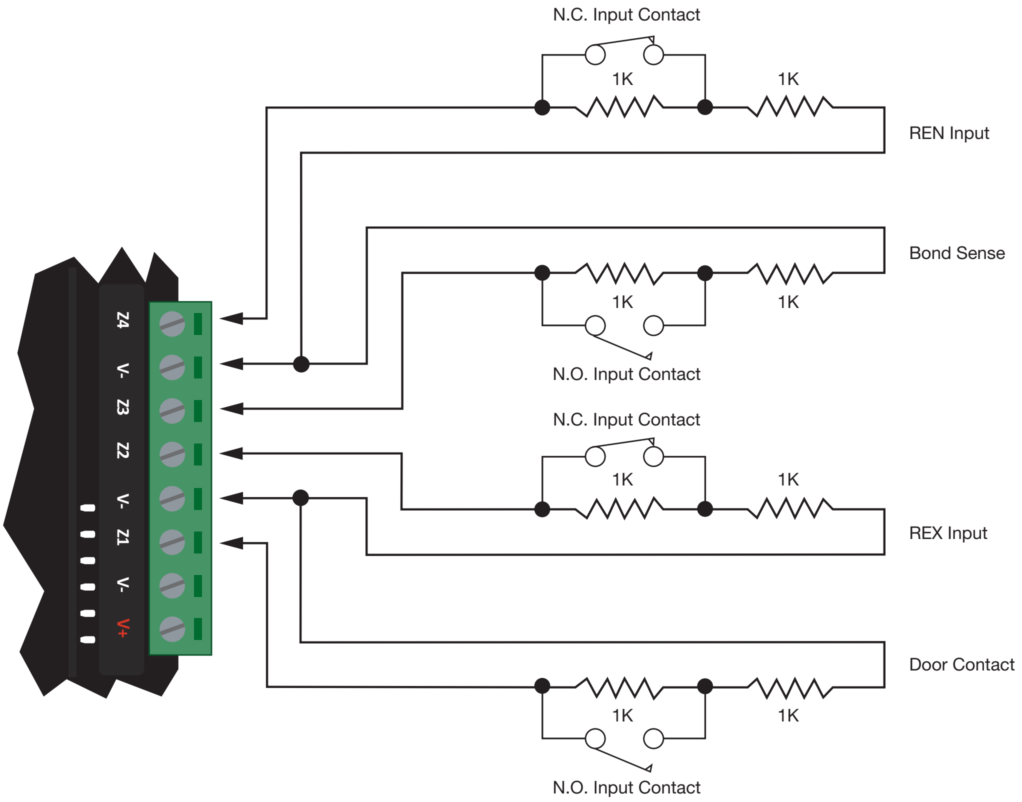
In multiplex mode, the secondary reader has all connections wired to the same port as the primary card reader with the DATA 1 connection wired to the opposite reader connection DATA 1 input.



Multiplex Card Reader Connection

Connect Door Contacts

The Controller allows the connection of up to 4 contacts for monitoring and controlling access control doors. Each input on the Controller can be used for either the door function that is automatically assigned or as a normal input on the system.



Typical Configuration of Door Monitoring Contacts

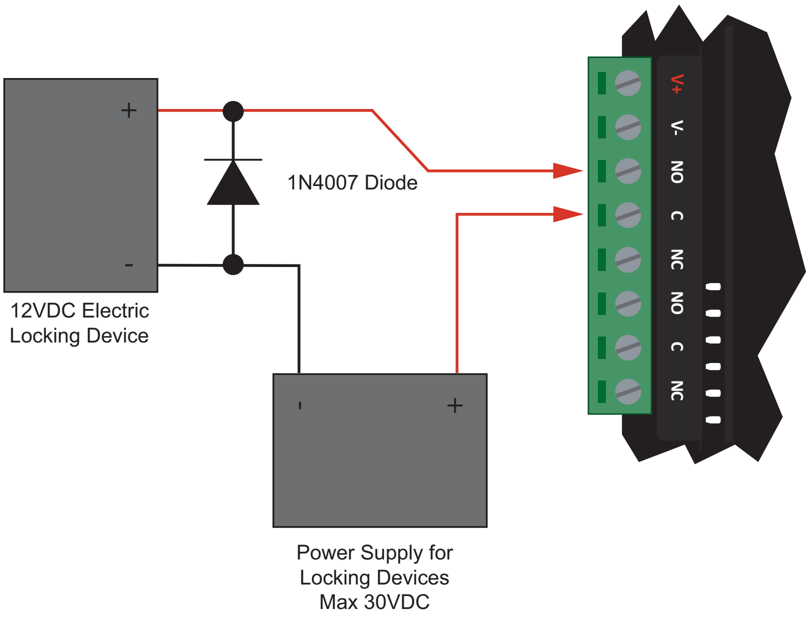
Inputs 1-4 (Door 1) and 5-8 (Door 2) can operate as either general purpose inputs or as onboard reader inputs. If used as general purpose inputs, make sure that these inputs are not defined in the onboard reader set up.

Input	Access Control Function	Default Setting
Input 1	Door Contact, Port 1	Door Contact, Port 1
Input 2	REX Input, Port 1	REX Input, Port 1
Input 3	Bond Sense, Port 1	General Purpose Input
Input 4	REN Input, Port 1	General Purpose Input
Input 5	Door Contact, Port 2	Door Contact, Port 2
Input 6	REX Input, Port 2	REX Input, Port 2
Input 7	Bond Sense, Port 2	General Purpose Input
Input 8	REN Input, Port 2	General Purpose Input

When connected, the REX Input can be programmed to operate regardless of the door contact state. The REX input can also be programmed to recycle the door alarm time to prevent nuisance alarms when the door is held open to permit longer entry.

Connect Lock Outputs

The Controller provides a connection for an electric strike lock with full monitoring of the lock circuit for tamper and over current/fuse blown conditions.



+
-
1N4007 Diode
12VDC Electric Locking Device
-
+
Power Supply for Locking Devices Max 30VDC
V+
V-
NO
C
NC
NO
C
NC

Typical Lock Output Connection

The Bell output current must not exceed 1.1A or electronic shutdown will be engaged. Ensure the devices connected to the outputs are within the limits as described in the Technical Specifications (see page 7).

Connect the Ethernet 10/100 Network Interface

The Controller comes with an onboard 10/100 Ethernet network interface that is used for IP monitoring and to connect to the Controller to carry out configuration and monitoring.

When installing, the Controller should be interfaced using a standard segment (<100m in length) and should be connected to a suitable Ethernet hub or switch.

Ethernet 10/100 Switch hub Connection

Temporary direct connections can be used for onsite programming by connecting directly to the computer Ethernet port.

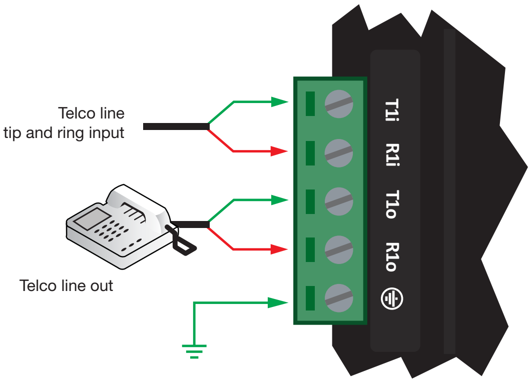
Ethernet 10/100 Direct Connection

The default IP address is set to a static IP address of 192.168.1.2 with a subnet mask of 255.255.255.0. These IP address settings are commonly used for internal networks. The IP address of the Controller can be configured using the LCD Keypad terminal or via the built in web interface.

Installing the Controller on an active network requires knowledge of the configuration and structure for the network. Always consult the network or system administrator and ask them to provide you with a fixed IP address that can be assigned to the Controller.

Connect the Telephone Dialer

If using Contact ID to provide offsite alarm monitoring, connect the telephone line directly to the Controller using the onboard telephone connection terminals.



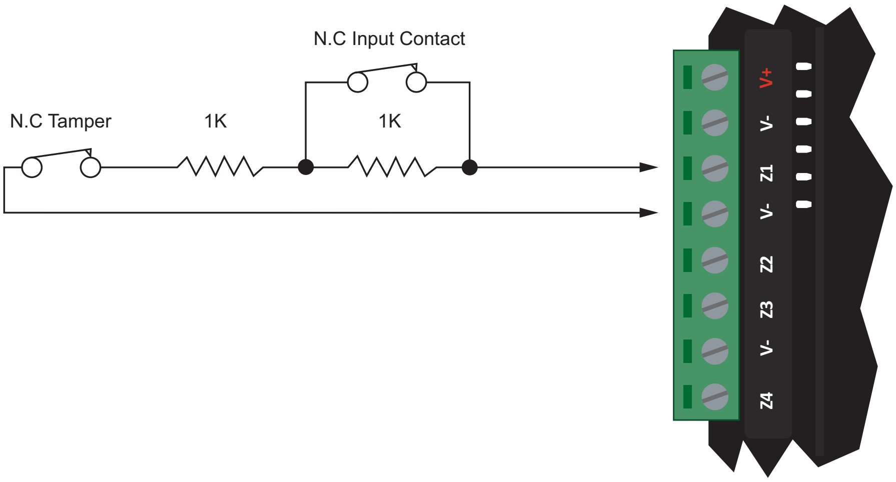
Telephone Line Connection

Connect Inputs

The Controller has 8 onboard inputs for monitoring the state of devices such as magnetic contacts, motion detectors and temperature sensors. Devices connected to these inputs can be installed to a maximum distance of 300m (1000ft) from the Controller when using 22 AWG. The Controller supports normally opened and normally closed configurations with or without EOL resistors.

When using an input with the EOL resistor configuration, the Controller generates an alarm condition when the state of an input is toggled and generates a tamper alarm condition when a wire fault (short circuit) or a cut (tampered) in the line occurs.

Inputs default to require the EOL resistor configuration.

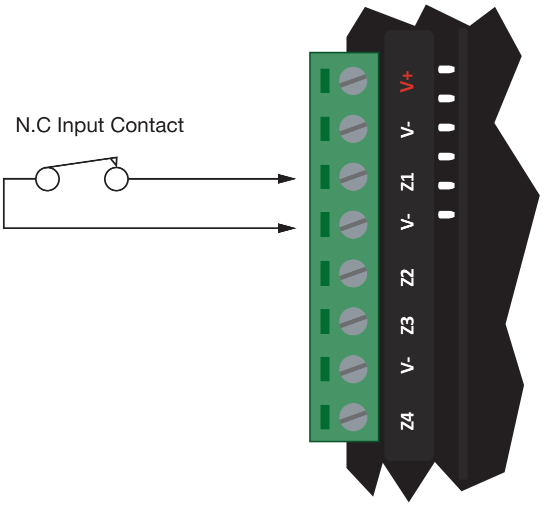


EOL Resistor Input Configuration

Inputs 1-4 (Door 1) and 5-8 (Door 2) can operate as either general purpose inputs or as onboard reader inputs. If used as general purpose inputs you must ensure that they are not defined in the onboard reader set up.

Each input can use a different configuration.

When using the No Resistor configuration, the Controller only monitors the opened and closed state of the connected input device generating the alarm and seal conditions.



No EOL Resistor Input Configuration

Resistor Value Options

When using the EOL resistor configuration, the EOL resistor option must be configured based on the site requirements.

Value 1	Value 2	Monitored Status
1k	1k	Open, Closed, Tamper, Short
1k	No Resistor	Open, Closed
<5K7	No Resistor	Open, Closed
No Resistor	No Resistor	Open, Closed
2k2	6k8	Open, Closed, Tamper, Short
10k	10k	Open, Closed, Tamper, Short
2k2	2k2	Open, Closed, Tamper, Short
4k7	2k2	Open, Closed, Tamper, Short
4k7	4k7	Open, Closed, Tamper, Short

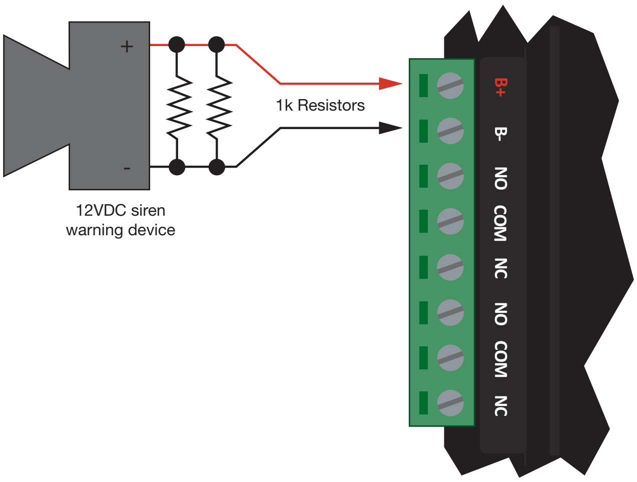
Outputs

The Controller has 7 onboard outputs which can be used to activate sirens, bells, warning devices, control lighting and doors. The first output on the Controller has a special hardware design that allows it to monitor for fault conditions and is ideally suited to driving sirens or warning devices.

Bell/Siren Output

The + and - terminals of the Bell output (CP001:01) are used to power bells, sirens or any devices that require a steady voltage output. The bell output supplies 12VDC upon alarm and supports one 30-watt siren. The bell output uses an electronically fused circuit and automatically shuts down under fault conditions.

Connecting a Piezo siren may result in a dull noise being emitted. This is caused by residual current from the monitoring circuit. To prevent this occurring, connect two 1K resistors in parallel.



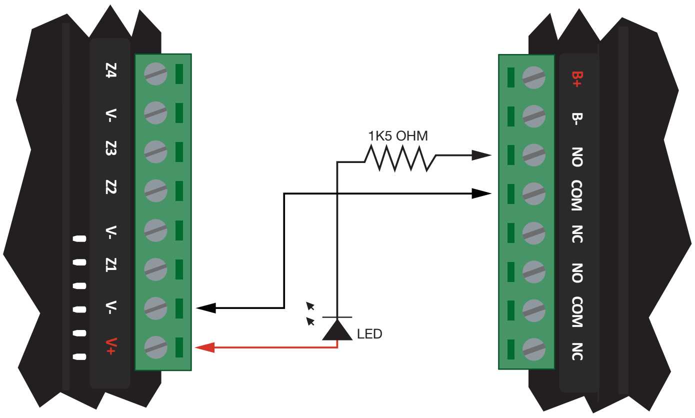
Bell Siren Connection

If the load on the bell terminals returns to normal, the Controller reinstates power to the bell terminals on the next transition of the output.

When the bell output is not used, the appropriate trouble input (see page 43) will be activated. This can be avoided by connecting a 1K resistor across the bell output. If the bell is not being used for another function, and the trouble input is not programmed in the system, a resistor is not required.

Relay Outputs

The Relay Outputs (CP001:03 and CP001:04) on the Controller are Form C relays having normally open and normally closed contacts. These outputs can be used to activate larger relays, sounders, lights, or locks etc.

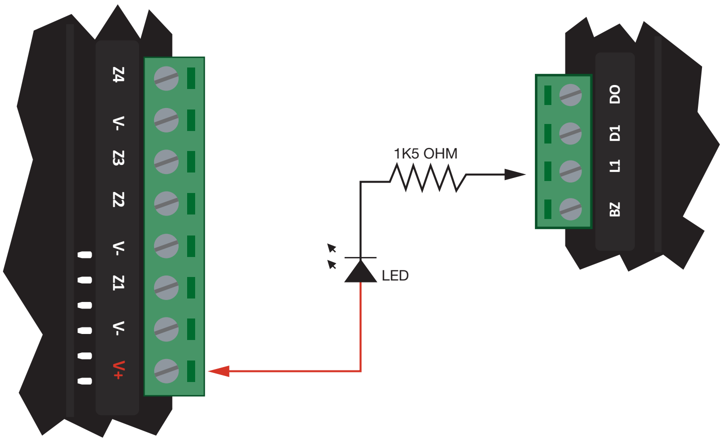


Example Relay Connection

Warning: The Relay outputs can switch to a maximum capacity of 7A. Exceeding this amount will damage the output.

Reader Outputs

If readers are not attached to the reader ports, then the Reader 1 L1 and BZ, and the Reader 2 L1 and BZ outputs can be used as general purpose outputs. These can be controlled by assigning the RDxxxGreen R1, RDxxx Beeper R1, RDxxxGreen R2 and RDxxx Beeper R2 outputs of whichever reader module has been configured as the onboard reader module. These are open drain outputs which switch to the V- reference.



Open Drain Reader Outputs

Warning: The reader outputs can switch to a maximum capacity of 50mA. Exceeding this amount will damage the output.

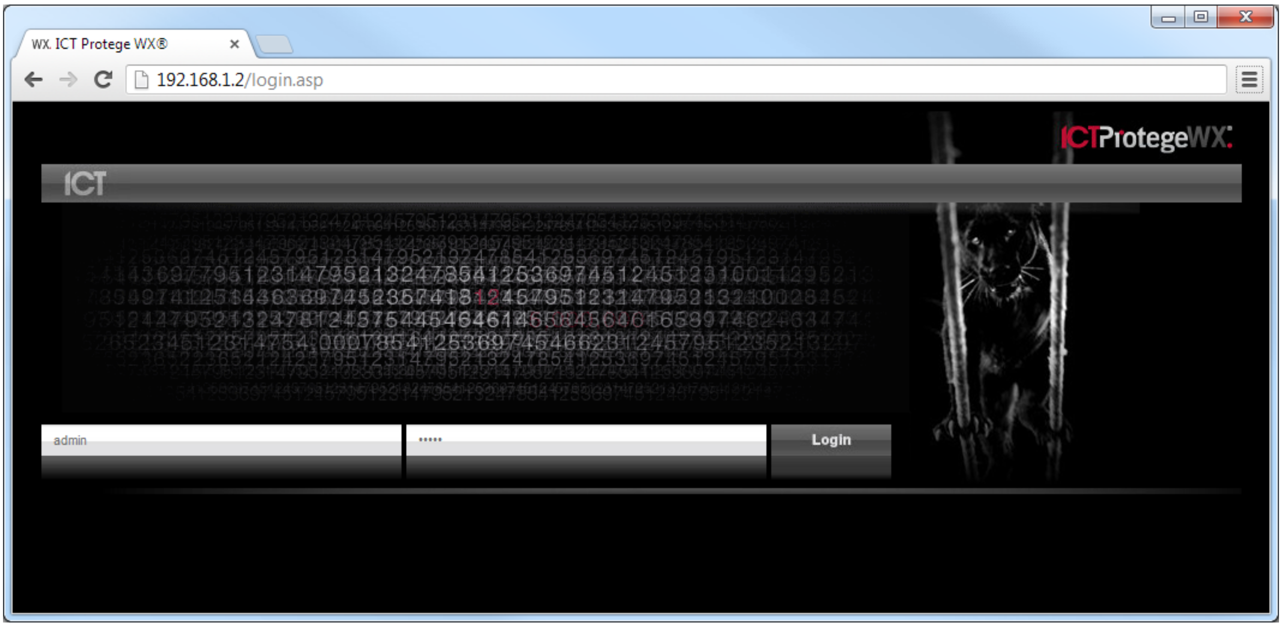
Getting Started

This section outlines the process for logging in for the first time and walks you through the Protege WX Configuration Wizard.

Logging In for the First Time

1. Open a web browser and enter the IP address **192.168.1.2**

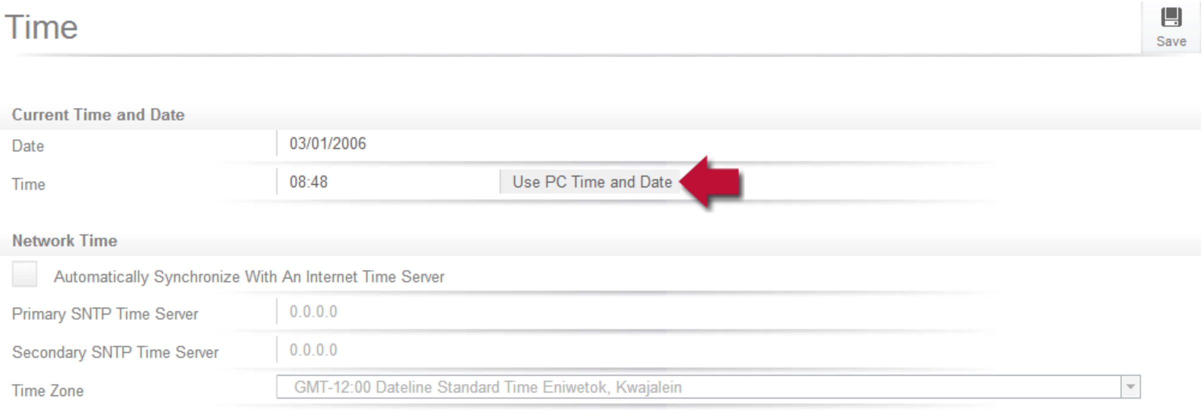
   The Login window is displayed.



2. Enter the default operator login of admin with the password admin. For security reasons, this password should be changed (see page 104) before deployment.
3. Click **Login**.

Set the Controller Time

1. Navigate to **Scheduling | Time**



Time

Save

Current Time and Date

Date	03/01/2006
Time	08:48 Use PC Time and Date

Network Time

□ Automatically Synchronize With An Internet Time Server

Primary SNTP Time Server	0.0.0.0
Secondary SNTP Time Server	0.0.0.0
Time Zone	GMT-12:00 Dateline Standard Time Eniwetok, Kwajalein

2. Click **Use PC Time and Date** to set the current date and time to that of your PC then click **Save**.

   The time is reset and you'll be prompted to login again before you can continue.

Understanding the Defaults

To simplify things and make programming your site as easy as possible, Protege WX includes a number of default settings. These can be used 'as is' for quick and simple deployment, or adapted to suit your needs. Either way, it helps if you understand what the defaults are and what they do. You'll find the names describe them pretty well.

Users:

You'll find three users by default - Installer, Master, and User (Demo). There are also three access levels that determine what users can do in the system, and three menu groups each providing a different level of control:

User	PIN Code	Description/Purpose
Installer	000000	Assigned the Installer access level and Installer menu group, this user has full access to program the system via a keypad, but no area control or door access.
Master	123456	Assigned the Master access level and All Menus menu group, this is a power user with access to all areas and doors. They have complete control from a keypad with the exception of the Installer menus.
User (Demo)	111111	Assigned the Users access level and User menu group, this is a typical staff member/end user, with access to all areas, but with no doors or door groups configured yet. Keypad control (via the menu group), allows basic control over the system for arming/disarming.

Schedules:

There are schedules for Work Hours, After Hours, and Break Hours. These can be edited as required, and used to enable a function or access level to operate only within certain scheduled periods. They can be used to control when a user can gain access to things, to unlock doors automatically, to arm or disarm areas at certain times or days, and to turn thing on and off or change the way they behave at certain times of day.

Inputs, Outputs, and Trouble Inputs

Inputs, Outputs, and Trouble Inputs for the Controller are included by default. Others are added automatically when you add an Expander module using the wizard. For example, adding a Reader Expander will add the inputs, outputs and trouble inputs for that module. Theses are then configured using the wizard.

Door Types and Input Types

The Door types - Card Only, Card and Pin, Card or Pin, Pin Only - are used to define how a door will operate and when the entry mode is valid. Use these as they are or create your own door types to allow different modes of control over the method a user has to access a door. For example, you can create a door type that allows card only access between standard office hours of 8am and 5pm, but requires both card and pin outside these hours for added security.

Input Types define how an input will operate in an area. For example, Delay will go into entry delay when triggered, whereas Instant will activate immediately. There are a range of predefined input types included by default. In most cases these will be enough, but you can modify them as needed or create your own to suit your requirements. The four most commonly used input types are:

- Instant: Activates an armed area immediately when input opens
- Delay: Activates entry delay when input opens
- Trouble Silent: Used for system trouble inputs. Generates an alarm without the Bell
- 24 Hour Alarm: Used for panic inputs. Generates an alarm even when area is disarmed

Using the Protege WX Wizards

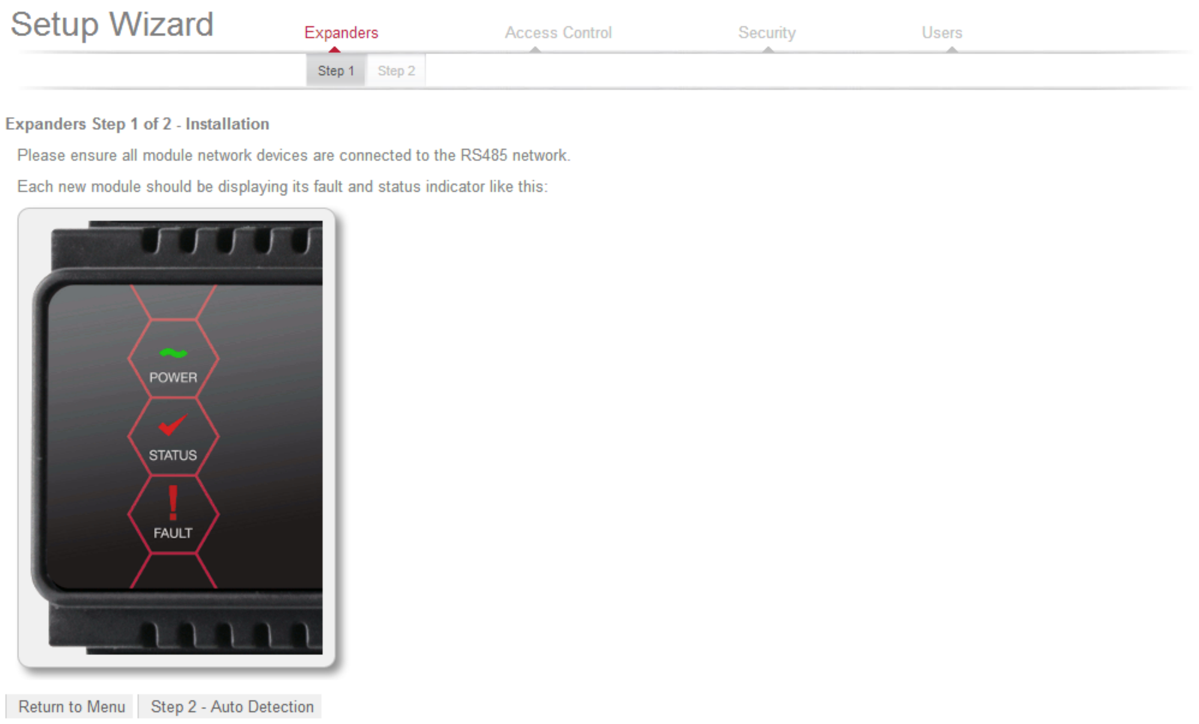
Once logged in, the Home Page is displayed. Select the **Wizards** menu at the top of the page to run through each of the wizards that will guide you through the initial setup, giving you a fully functional access control and intrusion detection solution in no time.

1. Expanders Wizard
2. Access Control Wizard
3. Security Wizard
4. Users Wizard

Expanders

The Expander Wizard is used to detect and add the connected expander modules to the system, and add their corresponding inputs, outputs, and trouble inputs.

1. Ensure the modules are connected to the network (see page 12) and that the LED indicators show the module address is too high. The Fault light should be constantly on and Status light should be flashing three times in quick succession.

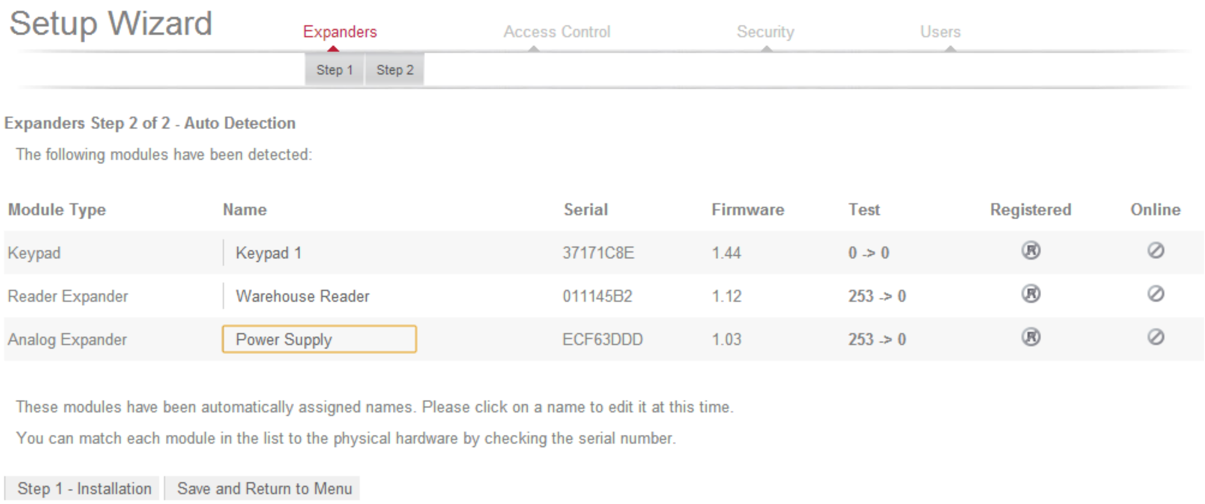


Expanders Step 1 of 2 - Installation

Please ensure all module network devices are connected to the RS485 network.

Each new module should be displaying its fault and status indicator like this:

2. Click Step 2- Auto Detection to continue. The wizard automatically detects the modules and displays them here:



Expanders Step 2 of 2 - Auto Detection

The following modules have been detected:

Module Type	Name	Serial	Firmware	Test	Registered	Online
Keypad	Keypad 1	37171C8E	1.44	0 -> 0	®	⊘
Reader Expander	Warehouse Reader	011145B2	1.12	253 -> 0	®	⊘
Analog Expander	Power Supply	ECF63DDD	1.03	253 -> 0	®	⊘

These modules have been automatically assigned names. Please click on a name to edit it at this time.

You can match each module in the list to the physical hardware by checking the serial number.

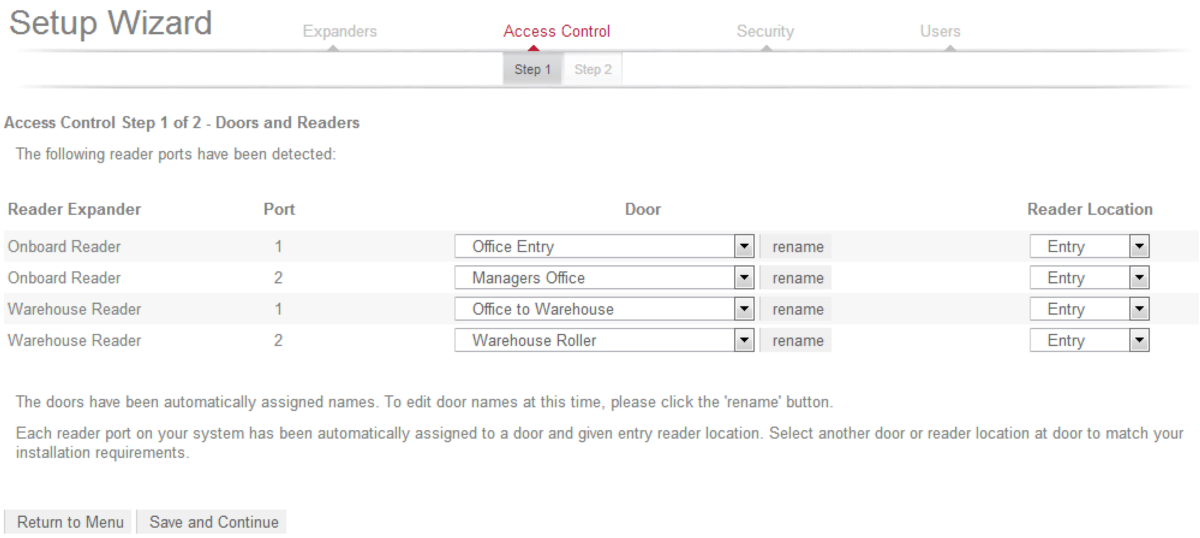
3. Each module is assigned a name automatically. These can be renamed as required to provide a more meaningful name for easier identification.
4. Click Save and Return to Menu to finish.

Progress is shown as the Controller is programmed and the corresponding inputs, outputs, and trouble inputs are created. Once complete, you are returned to the Home page.

Access Control

The Access Control Wizard detects the available reader ports and creates the doors. It also enables you to assign an unlock schedule to each door which will determine when the door will unlocked. For example, a typical staff entry door may need to unlock at 8am and be locked again at 5pm. Use the Schedule Operates Late to Open (see page 51) option to prevent the door unlocking on schedule until the first user accesses the door. You can use the default Work Hours schedule which you can adapt to suit you needs later, or create your own schedules (see page 32) first.

1. The wizard automatically detects the reader ports:



Access Control Step 1 of 2 - Doors and Readers

The following reader ports have been detected:

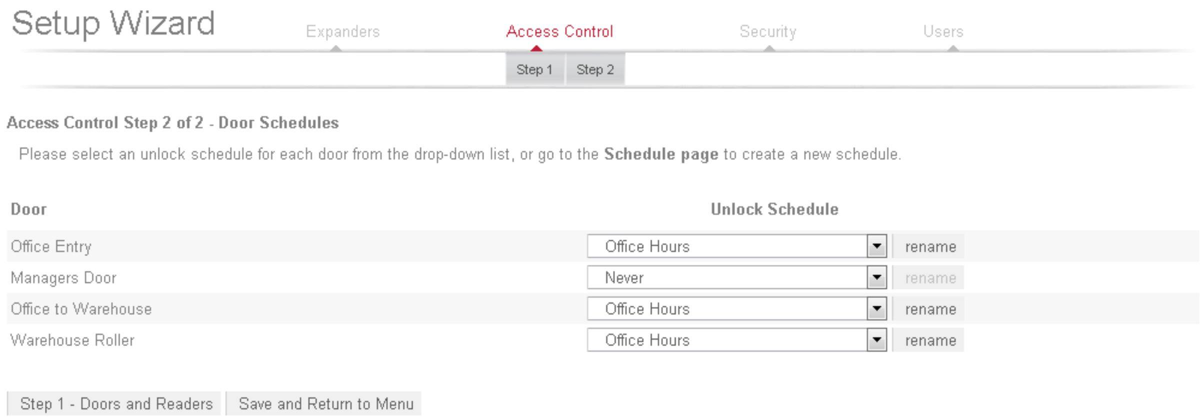
Reader Expander	Port	Door		Reader Location
Onboard Reader	1	Office Entry	rename	Entry
Onboard Reader	2	Managers Office	rename	Entry
Warehouse Reader	1	Office to Warehouse	rename	Entry
Warehouse Reader	2	Warehouse Roller	rename	Entry

The doors have been automatically assigned names. To edit door names at this time, please click the 'rename' button.

Each reader port on your system has been automatically assigned to a door and given entry reader location. Select another door or reader location at door to match your installation requirements.

2. Use the Rename button to assign your own door names and adjust the Reader Location as required.

3. Click **Save and Continue** to proceed to step 2.



Access Control Step 2 of 2 - Door Schedules

Please select an unlock schedule for each door from the drop-down list, or go to the **Schedule page** to create a new schedule.

Door	Unlock Schedule	
Office Entry	Office Hours	rename
Managers Door	Never	rename
Office to Warehouse	Office Hours	rename
Warehouse Roller	Office Hours	rename

4. Select the Unlock Schedule if required then click **Save and Return to Menu**.

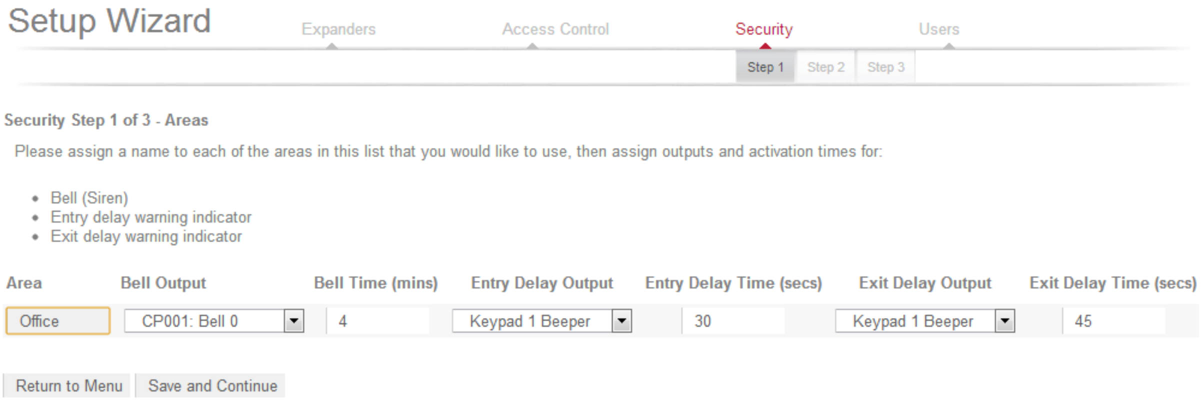
Progress is shown as the Doors are created. Once finished, you are returned to the Home page.

Security

The Security Wizard allows you to configure the Areas in your system, the Inputs that are used to trigger events, and setup basic offsite monitoring services.

This step disarms any areas that are currently armed, and will prompt you to confirm the action.

1. The wizard lists the placeholder Area that is created by default which you can now edit to fit your needs. If you require additional areas, you can create these first, or create and configure them later.



Security Step 1 of 3 - Areas

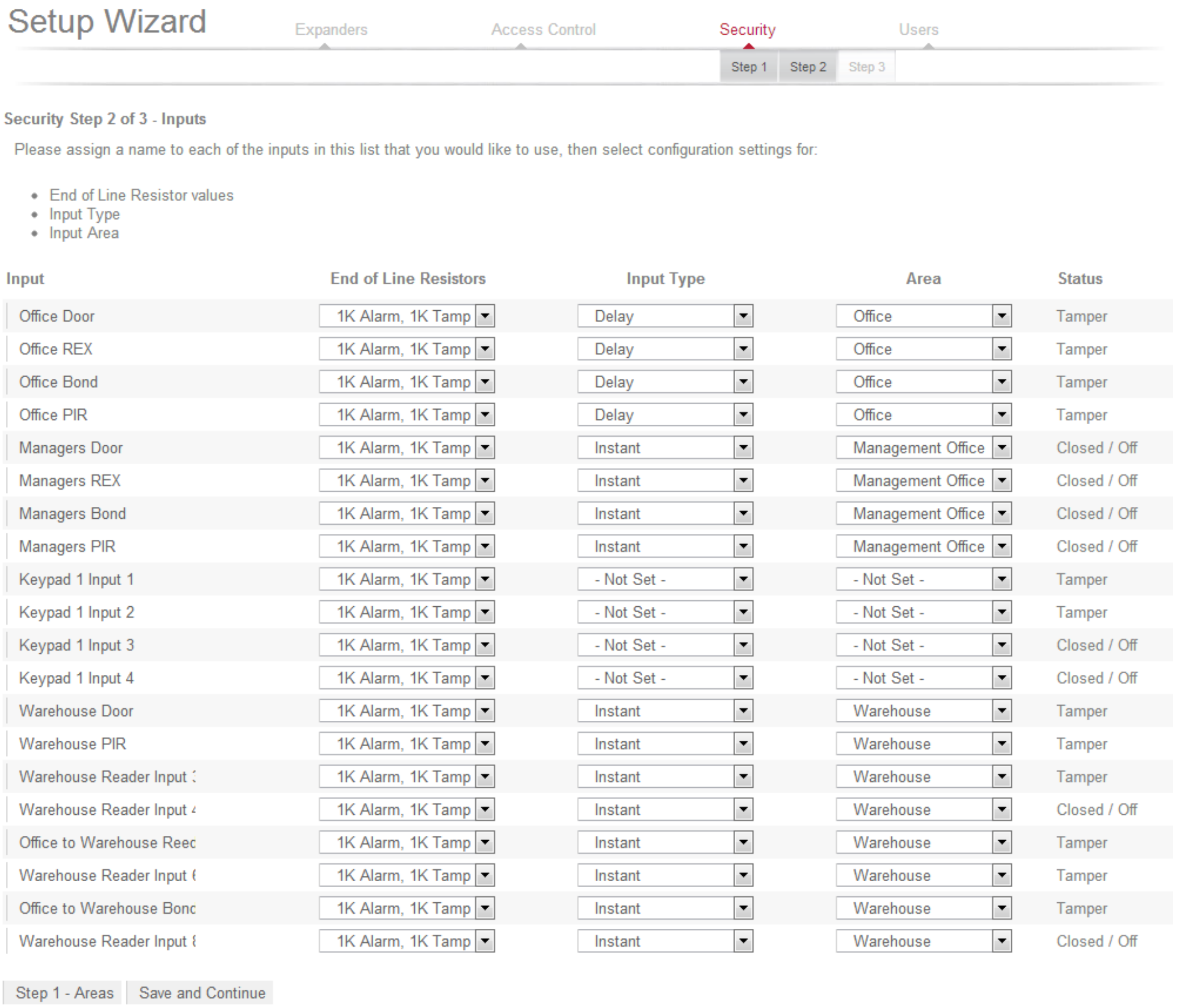
Please assign a name to each of the areas in this list that you would like to use, then assign outputs and activation times for:

- Bell (Siren)
- Entry delay warning indicator
- Exit delay warning indicator

Area	Bell Output	Bell Time (mins)	Entry Delay Output	Entry Delay Time (secs)	Exit Delay Output	Exit Delay Time (secs)
Office	CP001: Bell 0	4	Keypad 1 Beeper	30	Keypad 1 Beeper	45

- Select the **Bell Output** and the **Bell Time**. This is the output that will be triggered when the area alarm is activated and the time it will be activated for. In most cases, this will be used to connect a siren.
- Select the **Entry Delay Output** and the **Entry Delay Time**. This is the output that will be activated whenever the area goes into entry delay and the time users will be given to disarm the area before an alarm is triggered.
- Select the **Exit Delay Output** and the **Exit Delay Time**. This is the output that will be activated whenever the area goes into exit delay and the time users will be given to exit the area before an alarm is triggered.

2. Click **Save and Continue** to proceed to the next step. The wizard lists each of the Inputs in your system.



Security Step 2 of 3 - Inputs

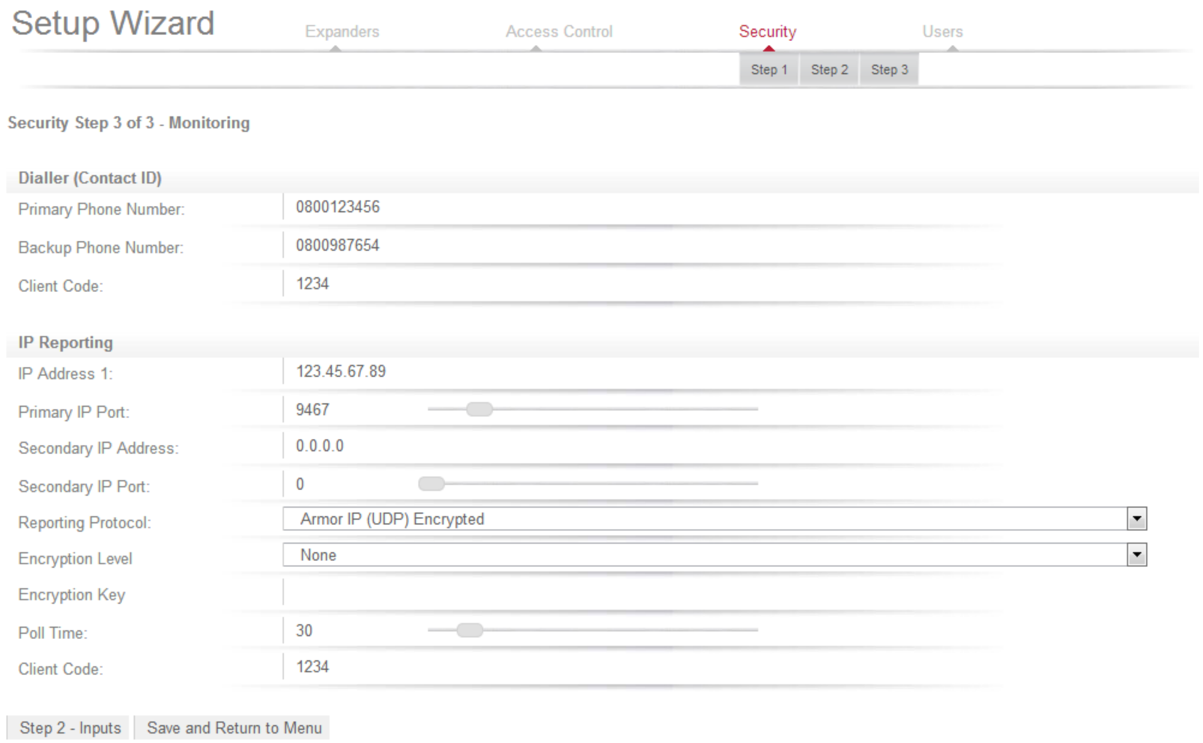
Please assign a name to each of the inputs in this list that you would like to use, then select configuration settings for:

- End of Line Resistor values
- Input Type
- Input Area

Input	End of Line Resistors	Input Type	Area	Status
Office Door	1K Alarm, 1K Tamp	Delay	Office	Tamper
Office REX	1K Alarm, 1K Tamp	Delay	Office	Tamper
Office Bond	1K Alarm, 1K Tamp	Delay	Office	Tamper
Office PIR	1K Alarm, 1K Tamp	Delay	Office	Tamper
Managers Door	1K Alarm, 1K Tamp	Instant	Management Office	Closed / Off
Managers REX	1K Alarm, 1K Tamp	Instant	Management Office	Closed / Off
Managers Bond	1K Alarm, 1K Tamp	Instant	Management Office	Closed / Off
Managers PIR	1K Alarm, 1K Tamp	Instant	Management Office	Closed / Off
Keypad 1 Input 1	1K Alarm, 1K Tamp	- Not Set -	- Not Set -	Tamper
Keypad 1 Input 2	1K Alarm, 1K Tamp	- Not Set -	- Not Set -	Tamper
Keypad 1 Input 3	1K Alarm, 1K Tamp	- Not Set -	- Not Set -	Closed / Off
Keypad 1 Input 4	1K Alarm, 1K Tamp	- Not Set -	- Not Set -	Closed / Off
Warehouse Door	1K Alarm, 1K Tamp	Instant	Warehouse	Tamper
Warehouse PIR	1K Alarm, 1K Tamp	Instant	Warehouse	Tamper
Warehouse Reader Input 3	1K Alarm, 1K Tamp	Instant	Warehouse	Tamper
Warehouse Reader Input 4	1K Alarm, 1K Tamp	Instant	Warehouse	Closed / Off
Office to Warehouse Reed	1K Alarm, 1K Tamp	Instant	Warehouse	Tamper
Warehouse Reader Input 6	1K Alarm, 1K Tamp	Instant	Warehouse	Tamper
Office to Warehouse Bond	1K Alarm, 1K Tamp	Instant	Warehouse	Tamper
Warehouse Reader Input 8	1K Alarm, 1K Tamp	Instant	Warehouse	Closed / Off

- Rename each Input to provide a more meaningful description for easier identification.
- Select the **End of Line Resistors** according to those used when wiring the EOL configuration.
- Select the **Input Type** to defines how an input will operate in an area. For example, Delay will go into entry delay when triggered, whereas Instant will activate immediately.
- Select the **Area** the input is assigned to.

3. Click **Save and Continue** to proceed and configure Offsite Monitoring. All modules will be restarted automatically.



Security Step 3 of 3 - Monitoring

Dialler (Contact ID)

Primary Phone Number:	0800123456
Backup Phone Number:	0800987654
Client Code:	1234

IP Reporting

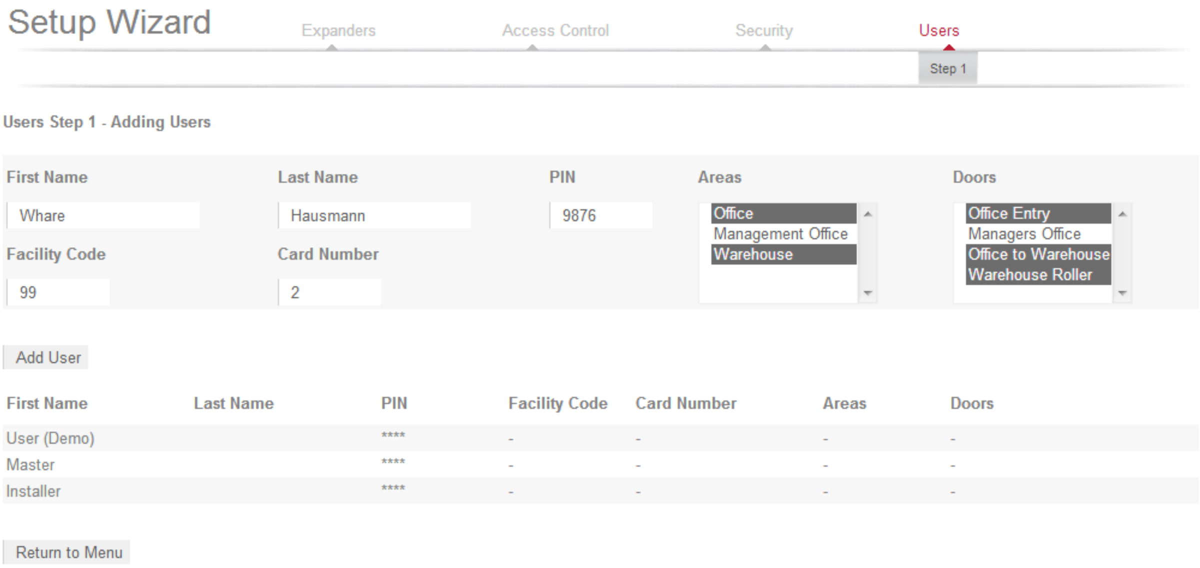
IP Address 1:	123.45.67.89
Primary IP Port:	9467
Secondary IP Address:	0.0.0.0
Secondary IP Port:	0
Reporting Protocol:	Armor IP (UDP) Encrypted
Encryption Level	None
Encryption Key	
Poll Time:	30
Client Code:	1234

4. If using PSTN Monitoring, enter the Dialler information:
   - Set the **Primary Phone Number** of the monitoring station
   - Set the **Backup Phone Number** of the monitoring station. This number will be dialed if a connection with the station cannot be made on the primary phone number.
   - Enter the **Client Code** (or account number). This is the code used to identify the system at the monitoring station and will usually be issued by the monitoring company.
5. If using IP Reporting:
   - Enter the **IP Address** and **IP Port Number** as supplied by your monitoring station.
   - If the monitoring station has a backup path, enter the secondary **IP Address 2** and the Secondary **IP Port 2 Number** to be used if the first IP address fails.
   - Select the **Reporting Protocol** to be used This will usually be supplied by your monitoring station.
   - If using an encrypted protocol, select the **Encryption Level** and the **Encryption Key** to be used
   - If required, adjust the **Poll Time**. One of the advantages of IP reporting is that essentially it is always 'on'. This is achieved by sending regular poll messages at the frequency set here. This defaults to 30 seconds, however your monitoring station may request a different setting.
   - Enter the **Client Code** (or account number). This is the code used to identify the system at the monitoring station and will usually be issued by the monitoring company.
6. Click **Save and Return to Menu** to complete configuration and return to the setup menu

Users

The Users Wizard enables you to quickly create new Users, and define which Areas and Doors they are able to access.

1. For each user, enter the name, PIN, and card details. Select the Area(s) and Door(s) you wish to grant them access to, then click **Add User**.



Users Step 1 - Adding Users

First Name	Last Name	PIN	Areas	Doors
Whare	Hausmann	9876	Office Management Office Warehouse	Office Entry Managers Office Office to Warehouse Warehouse Roller
Facility Code	Card Number			
99	2			

First Name	Last Name	PIN	Facility Code	Card Number	Areas	Doors
User (Demo)		****	-	-	-	-
Master		****	-	-	-	-
Installer		****	-	-	-	-

2. Repeat until you have added all the users you need.

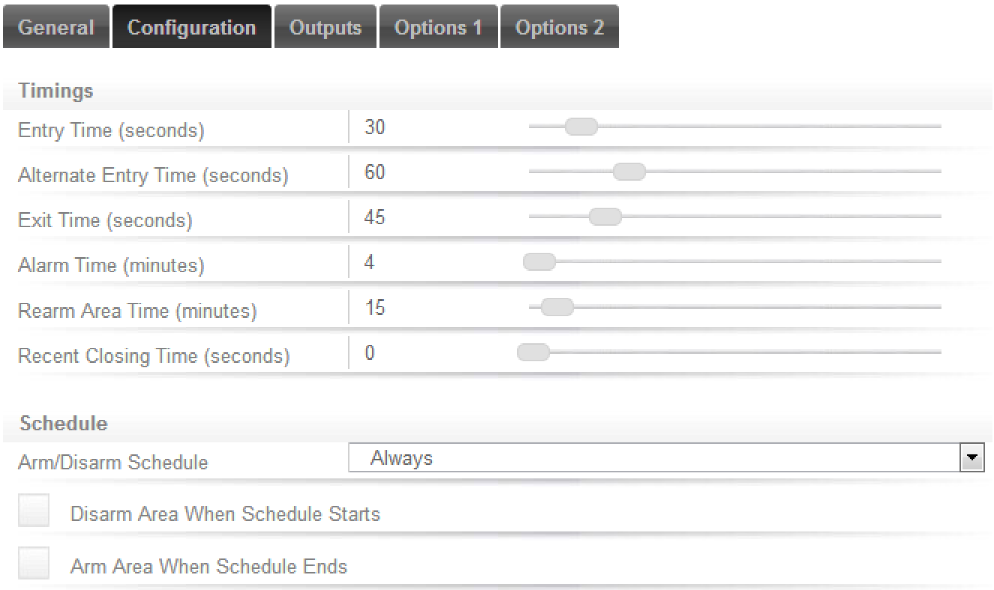
Configuring Additional Areas

Areas allow for the Protege system to be divided up into separate sections (alarm areas or partitions) that will be monitored for intrusion or other purposes.

There is one placeholder Area that is created by default which you can configure using the Security wizard to fit your needs. If you require additional areas, you can either create these before running the wizard then use the wizard to configure them, or create and configure them later.

Creating an Area

1. Navigate to Programming | Areas and click Add
2. Enter a Name for the area then select the Configuration tab to set the timings including entry and exit delays:
   - The Entry Time defines a delay period allowing any users that enter the area time to disarm it before the area generates an alarm
   - The Exit Time defines a delay period allowing users to exit the area once the arming of the area has begun before an alarm is triggered.
   - The Alarm 1 Time determines how long the bell/siren output for the area will remain activated before timing out.



Timings

Entry Time (seconds)	30
Alternate Entry Time (seconds)	60
Exit Time (seconds)	45
Alarm Time (minutes)	4
Rearm Area Time (minutes)	15
Recent Closing Time (seconds)	0

Schedule

Arm/Disarm Schedule: Always

□ Disarm Area When Schedule Starts

□ Arm Area When Schedule Ends

   - If required, adjust the schedule and set the Disarm Area When Schedule Starts and Arm Area When Schedule Ends options to automatically disarm/arm the area when the schedule starts/ends.
3. Select the Outputs tab to define the outputs used by the area and how they behave when triggered:
   - The Bell Output determines the output that will be triggered when the area alarm is activated. In most cases, this will be used to connect a siren.

     The Exit Delay Output and Entry Delay Output are activated whenever the area starts the exit or entry delay cycle. Using an audible output like a keypad beeper provides a distinctive warning to users to let them know the area has begun arming and they need to get out, or that the entry delay period has been triggered and they need to disarm the area before it generates an alarm.
   - The Disarmed Output and Armed Output are activated whenever the area completes the disarming or the arming cycle. Using an output such as a keypad LED provides a visual indication of the status of an area.
   - The Pulse On Time and Pulse Off Time allow you to configure the output to beep or flash when triggered. For example, you may set a keypad beeper to make short beeps for an exit delay, and a long continuous beep for entry delay.
4. Click Save to finish creating the area.

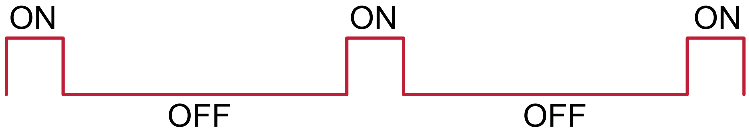
For a full list of the available properties and a description of what they do, refer to the Property Reference Guide (see page 62).

Pulse Times

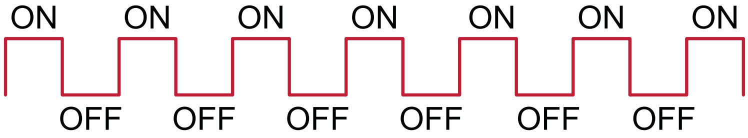
Pulse times allow an output or group of outputs to be pulsed for the duration of an area state. For example, the keypad beeper can be used to make short beeps for an exit delay, then a long continuous beep for entry delay.

Pulse times are measured in tenths of a second or 100ms. A pulse time of 10 equates to 1 second.

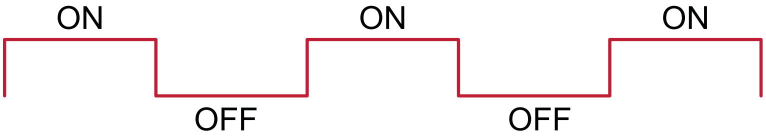
Setting the Pulse On to 1 and the Pulse Off to 9 provides a short pulse (such as a short beep or flash) every second.



Setting both the Pulse On and Pulse Off values to 1 will provide a rapid pulse on/pulse off:



Setting both values to 5 provides a slow steady pulse on/pulse off:



If the Pulse On and Pulse off values are both set to zero (the default setting) the pulse is disabled and the output will remain on for the duration of the cycle time.

If Pulse On is given a value but Pulse Off is set to zero, the output will pulse (flash or beep) once only then remain off.

Configuring Schedules and Holidays

Schedules are defined timeframes that enable a function or access level to operate only within certain scheduled periods. They can be used to control when a user can gain access to things, to unlock doors automatically, to arm or disarm areas at certain times or days, and turn thing on and off or change the way they behave at certain times of day.

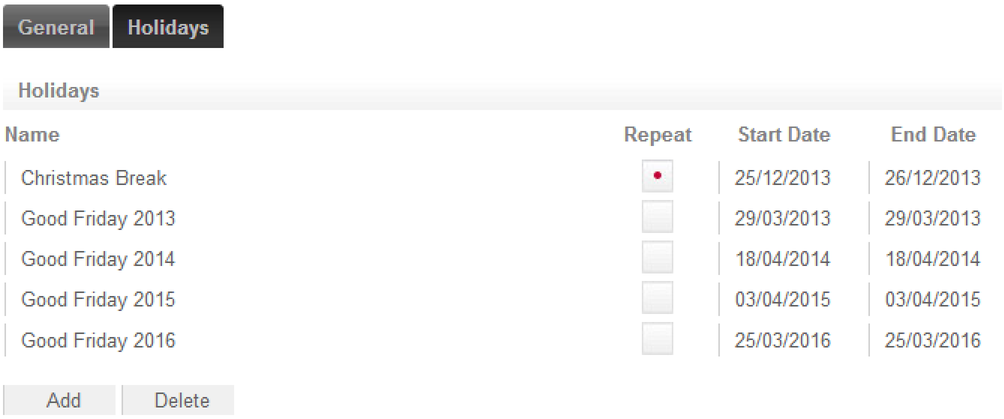
As schedules are commonly used to control access or to secure areas, it's a common requirement to have the schedule behave differently on a holiday. This is achieved by adding **Holiday Groups** which are then used to prevent (or allow) periods within a schedule to function during the holiday duration.

Once a schedule is programmed it will always be either valid or invalid. When it becomes valid, items that are programmed to depend on that schedule become active. For example:

- An Access Level will only grant access when its **operating schedule** is valid
- A door will unlock when its **unlock schedule** becomes valid
- An output will turn on when its **activation schedule** becomes valid

Creating Holiday Groups

1. Navigate to **Scheduling | Holiday Groups** and click **Add**
2. Enter a name for the holiday group then select the **Holidays** tab to add holidays to the group



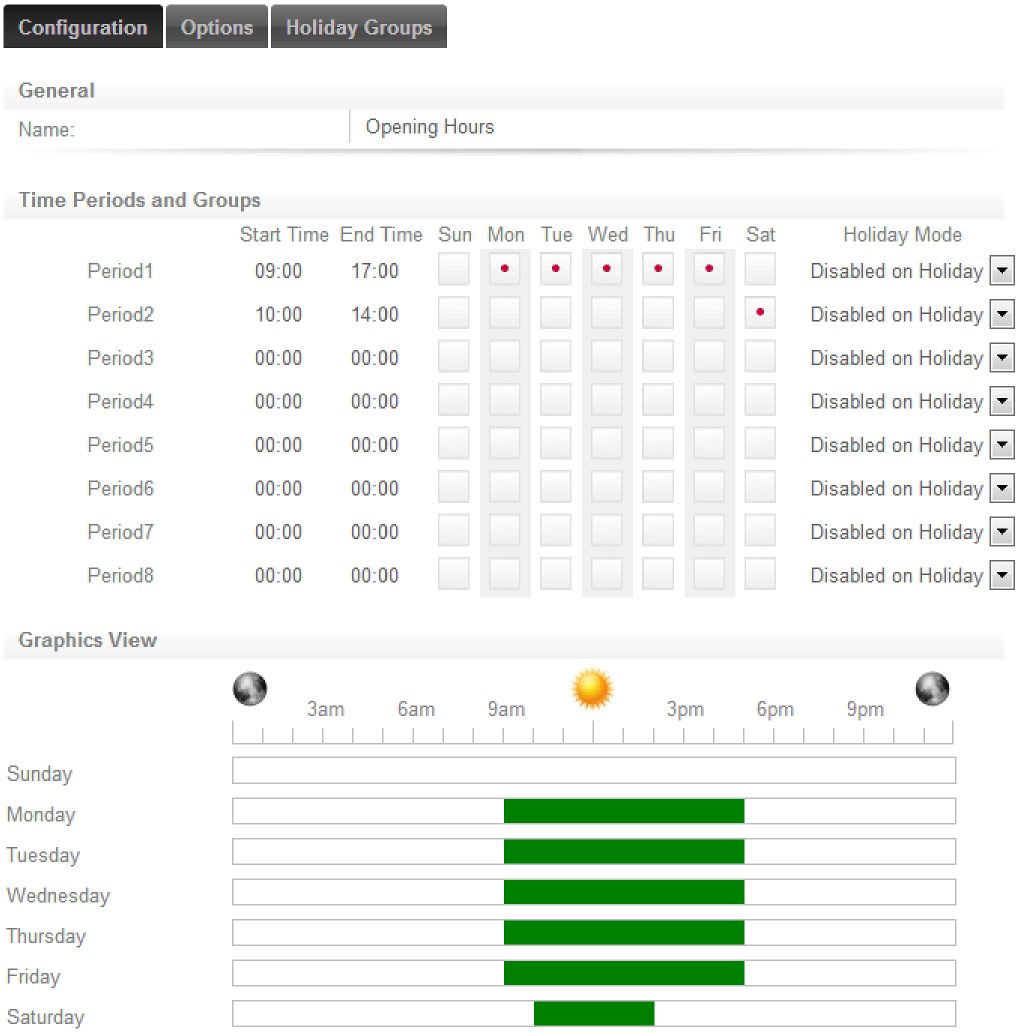
Name	Repeat	Start Date	End Date
Christmas Break	☑	25/12/2013	26/12/2013
Good Friday 2013	☐	29/03/2013	29/03/2013
Good Friday 2014	☐	18/04/2014	18/04/2014
Good Friday 2015	☐	03/04/2015	03/04/2015
Good Friday 2016	☐	25/03/2016	25/03/2016

   - Enable the **Repeat** option for holidays that occur on the same day every year.
   - For holiday periods that span multiple days (such as Christmas and Boxing Day), set a different start and end date.
   - For holidays that fall on a different day each year (such as Easter), these need to be programmed for each occurrence, but adding multiple entries allows you to program many years in advance.

3. Click **Save**. Once you have programmed your holiday group(s), they can be applied to your schedules.

Creating Schedules

1. Navigate to **Scheduling | Schedules** and click **Add**
2. Enter a **Name** for the schedule
3. Enter the start and end time for each period and select the days you wish the schedule to operate on by enabling the appropriate boxes.



General

Name: Opening Hours

Time Periods and Groups

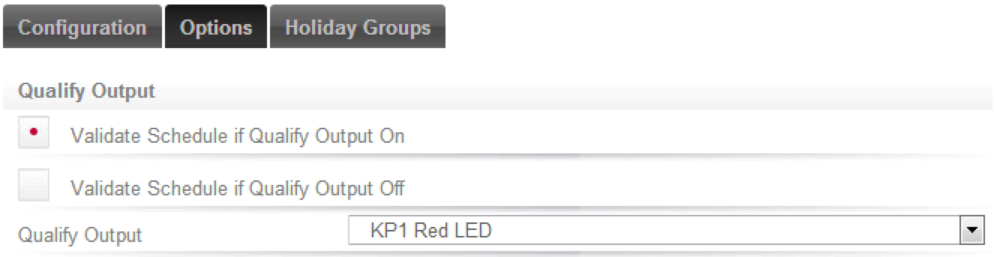
	Start Time	End Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holiday Mode
Period1	09:00	17:00	□	●	●	●	●	●	□	Disabled on Holiday
Period2	10:00	14:00	□	□	□	□	□	□	●	Disabled on Holiday
Period3	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday
Period4	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday
Period5	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday
Period6	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday
Period7	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday
Period8	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday

Graphics View

Notice how the **Graphics View** updates to show when the schedule will be valid.

4. For each period, choose the **Holiday Mode** to define how the schedule will operate during a holiday period. Choose from:
   - **Disabled on Holiday**: When selected, the period will **not** make the schedule valid on a holiday. In other words, if a door is programmed to unlock by this schedule, it will not unlock on a holiday when this option is selected. This is the default mode of operation for schedules.
   - **Enabled on Holiday:** When selected, the period will only ever make the schedule valid **on** a holiday.
   - **Ignore Holiday:** When selected, the period will make the schedule valid **regardless** of whether the day is a holiday or not.

5. If required, select the **Options** tab to set the **Qualify Output**. This allows you to qualify the schedule based on the state of an output.



Qualify Output

● Validate Schedule if Qualify Output On

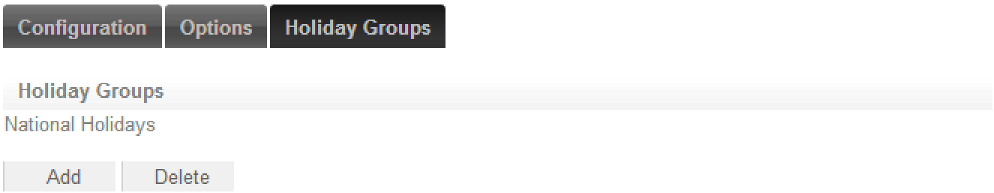
□ Validate Schedule if Qualify Output Off

Qualify Output: KP1 Red LED

In this example, this schedule will only ever become valid if all the other conditions of the schedule are met, and the KP1 Red LED output is **off**. Consider a schedule that has been programmed to unlock the front door of a retail shop. By configuring a qualify output, the front door would unlock at opening time only if the alarm has been unset. If nobody shows up for work, the door doesn't unlock.

6. Select the **Holiday Groups** tab to choose the holidays that apply to the schedule.

7. Click **Add** and select the group or groups of holidays that you wish to apply to this schedule.



Holiday Groups

National Holidays

This tells the schedule **which days** are holidays, but it does not tell the schedule **what to do** if it is a holiday. That is defined by the **Holiday Mode**.

8. Click **Save** to finish creating your schedule.

Schedules and Multiple Time Spans

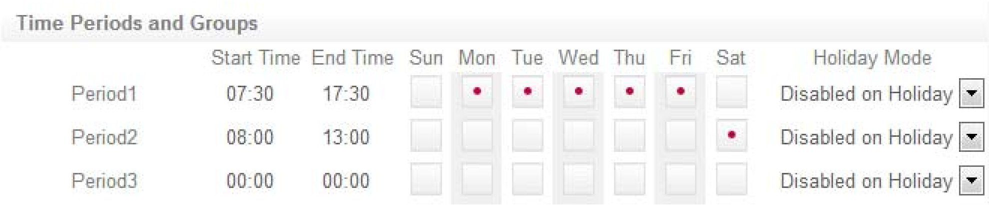
There may be times when schedules need to turn on and off more than once, or at different times on different days. Each schedule has 8 periods to allow for these scenarios.

Let's look at some examples of when you might use this.

Different Hours for Weekends

Premises may need to open for shorter hours on a weekend.

To set this up, you simply add the second period of shorter hours and select the relevant day (in this example Saturday):



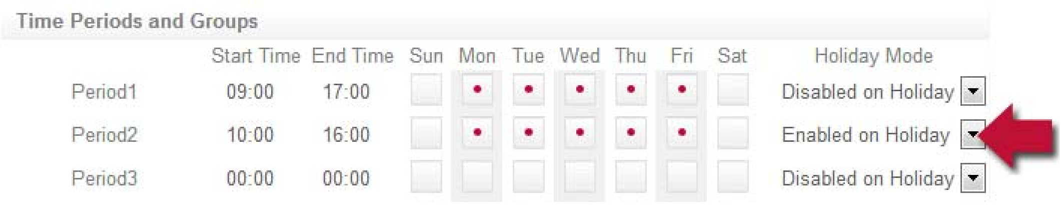
Time Periods and Groups

	Start Time	End Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holiday Mode
Period1	07:30	17:30	□	●	●	●	●	●	□	Disabled on Holiday
Period2	08:00	13:00	□	□	□	□	□	□	●	Disabled on Holiday
Period3	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday

Shorter Hours on a Holiday

In some installations, especially retail, a schedule must still operate on a holiday, but may do so for shorter hours.

In this example, the schedule will be valid from 9am to 5pm, Monday to Friday on normal days. If the day is a holiday, the schedule will only be valid from 10am to 4pm.



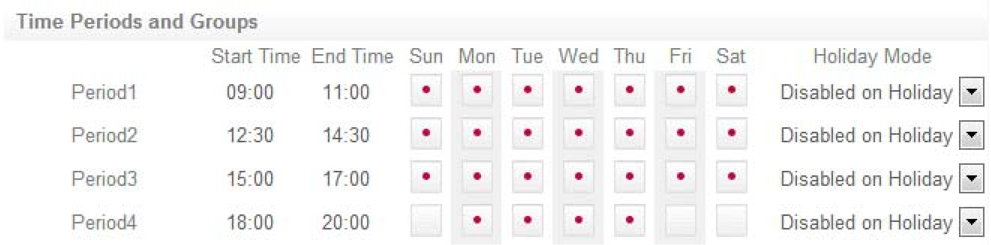
Time Periods and Groups

	Start Time	End Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holiday Mode
Period1	09:00	17:00	□	●	●	●	●	●	□	Disabled on Holiday
Period2	10:00	16:00	□	●	●	●	●	●	□	Enabled on Holiday
Period3	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday

Multiple Periods in a Single Day

Another example would be where there are multiple periods required in a single day.

Consider a movie theater where there are multiple session times and the doors are to be unlocked during these times:



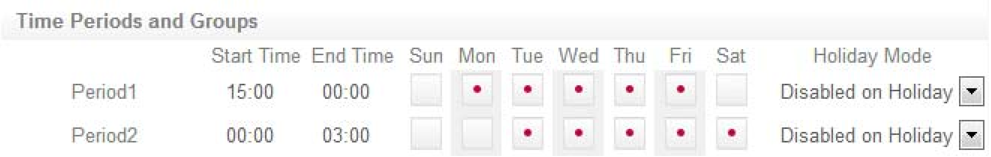
Time Periods and Groups

	Start Time	End Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holiday Mode
Period1	09:00	11:00	●	●	●	●	●	●	●	Disabled on Holiday
Period2	12:30	14:30	●	●	●	●	●	●	●	Disabled on Holiday
Period3	15:00	17:00	●	●	●	●	●	●	●	Disabled on Holiday
Period4	18:00	20:00	□	●	●	●	●	□	□	Disabled on Holiday

Overnight Schedules

Where a schedule is required to operate overnight, enter a start time, but leave the end time as 00:00. This results in the period being valid from the start time until midnight:

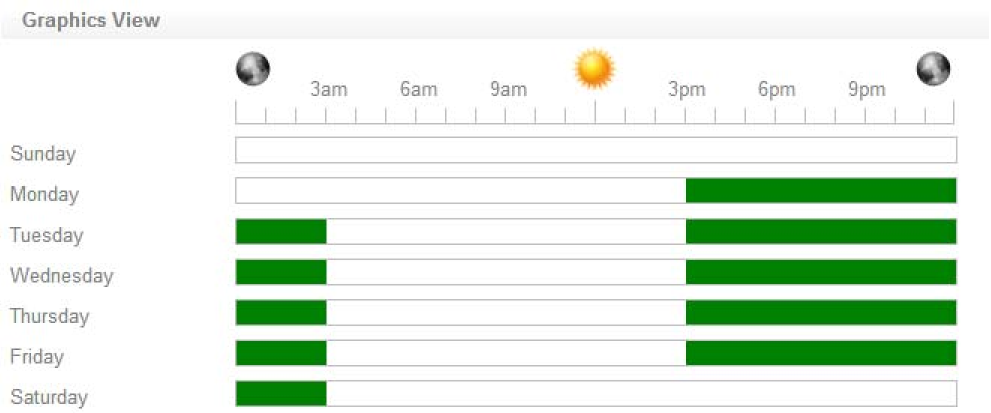
Now program a second period to start at midnight and continue until the end of the shift. In this example, the schedule will become valid at 3pm on Monday, and stay valid until 3am the following morning. By extending the days the period is valid, we can create an overnight Monday to Friday shift:



Time Periods and Groups

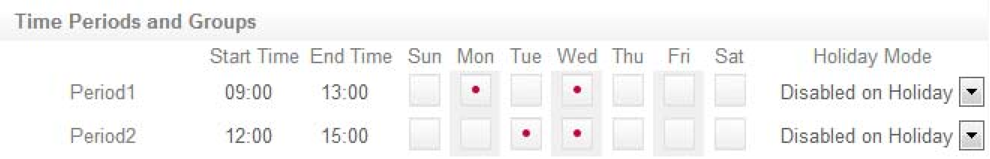
	Start Time	End Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holiday Mode
Period1	15:00	00:00	□	●	●	●	●	●	□	Disabled on Holiday
Period2	00:00	03:00	□	□	●	●	●	●	●	Disabled on Holiday

The Graphics View is used to show when the schedule will be valid:



Overlapping Periods

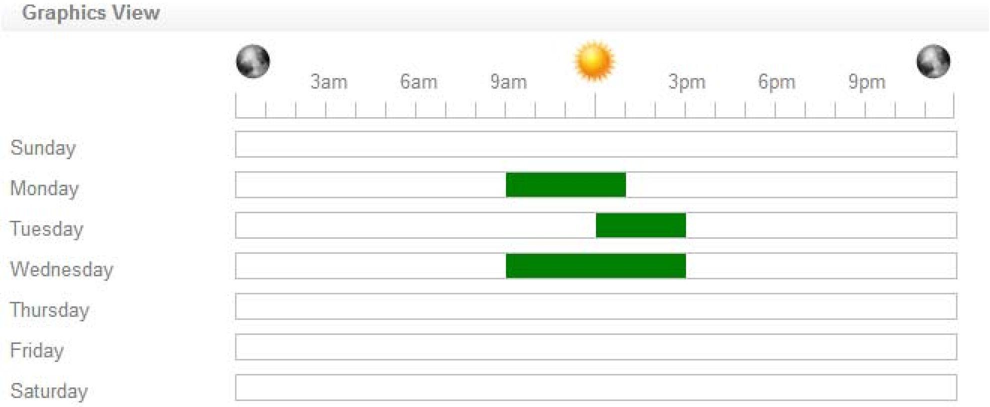
Where overlapping periods are present, the schedule will take the sum of all periods.



Time Periods and Groups

	Start Time	End Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holiday Mode
Period1	09:00	13:00	□	●	□	●	□	□	□	Disabled on Holiday ▾
Period2	12:00	15:00	□	□	●	●	□	□	□	Disabled on Holiday ▾

In this example, Wednesday has two periods that overlap. The two periods are combined, and as a result, the schedule will be valid from 9am to 3pm on Wednesday.



Rules for Schedules and Holidays

If you program times and days in to a schedule, but don't do anything else, then the schedule will always operate.

For a holiday to prevent the schedule from becoming valid, the following must have been programmed:

1. The holiday must be programmed in a holiday group
2. That holiday group must be applied to the schedule
3. The holiday mode must be programmed as Disabled on Holiday

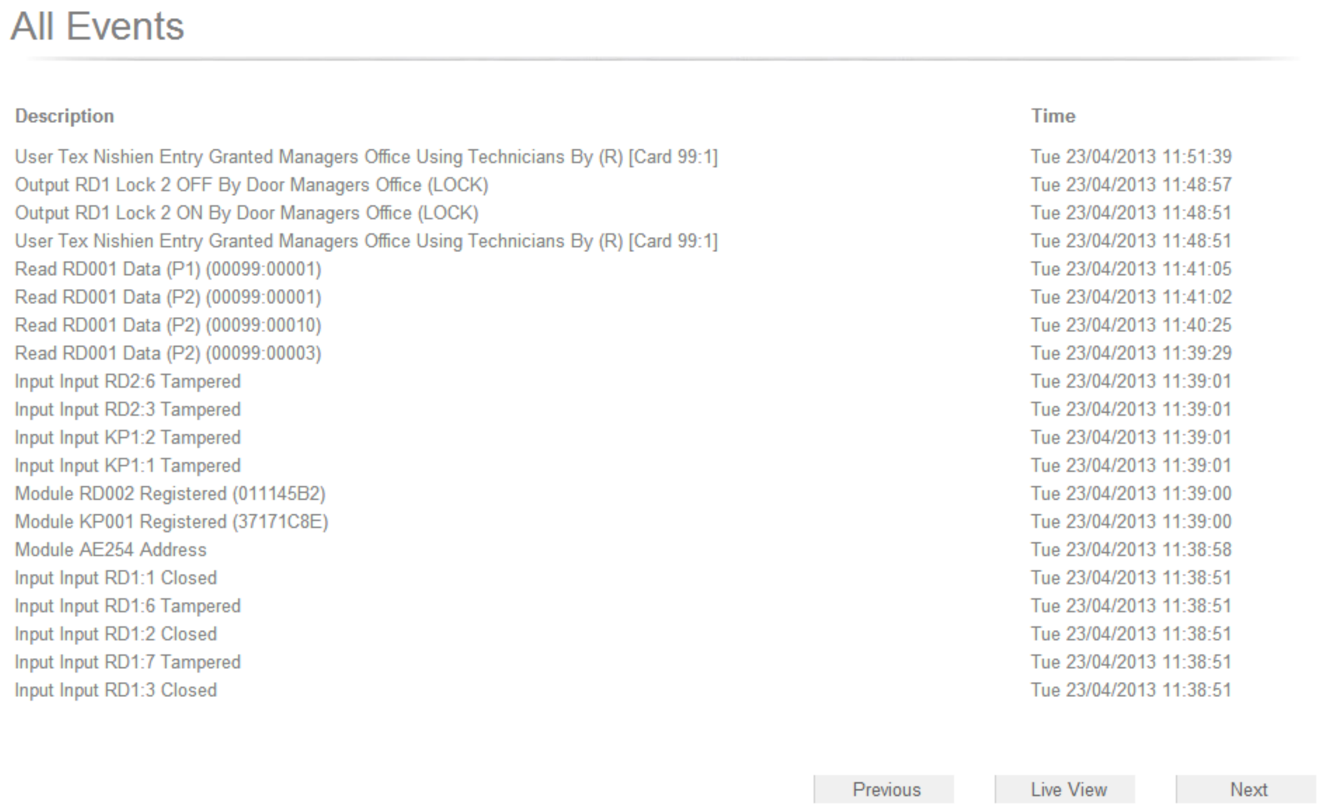
Monitoring Your System

The All Events page and Status Lists provide functions for monitoring your site.

The LED indicators on the Controller and Power Supply are useful for diagnosing faults and conditions.

Viewing Events

The All Events window provides a live and historic view of all events.



All Events

Description	Time
User Tex Nishien Entry Granted Managers Office Using Technicians By (R) [Card 99:1]	Tue 23/04/2013 11:51:39
Output RD1 Lock 2 OFF By Door Managers Office (LOCK)	Tue 23/04/2013 11:48:57
Output RD1 Lock 2 ON By Door Managers Office (LOCK)	Tue 23/04/2013 11:48:51
User Tex Nishien Entry Granted Managers Office Using Technicians By (R) [Card 99:1]	Tue 23/04/2013 11:48:51
Read RD001 Data (P1) (00099:00001)	Tue 23/04/2013 11:41:05
Read RD001 Data (P2) (00099:00001)	Tue 23/04/2013 11:41:02
Read RD001 Data (P2) (00099:00010)	Tue 23/04/2013 11:40:25
Read RD001 Data (P2) (00099:00003)	Tue 23/04/2013 11:39:29
Input Input RD2:6 Tampered	Tue 23/04/2013 11:39:01
Input Input RD2:3 Tampered	Tue 23/04/2013 11:39:01
Input Input KP1:2 Tampered	Tue 23/04/2013 11:39:01
Input Input KP1:1 Tampered	Tue 23/04/2013 11:39:01
Module RD002 Registered (011145B2)	Tue 23/04/2013 11:39:00
Module KP001 Registered (37171C8E)	Tue 23/04/2013 11:39:00
Module AE254 Address	Tue 23/04/2013 11:38:58
Input Input RD1:1 Closed	Tue 23/04/2013 11:38:51
Input Input RD1:6 Tampered	Tue 23/04/2013 11:38:51
Input Input RD1:2 Closed	Tue 23/04/2013 11:38:51
Input Input RD1:7 Tampered	Tue 23/04/2013 11:38:51
Input Input RD1:3 Closed	Tue 23/04/2013 11:38:51

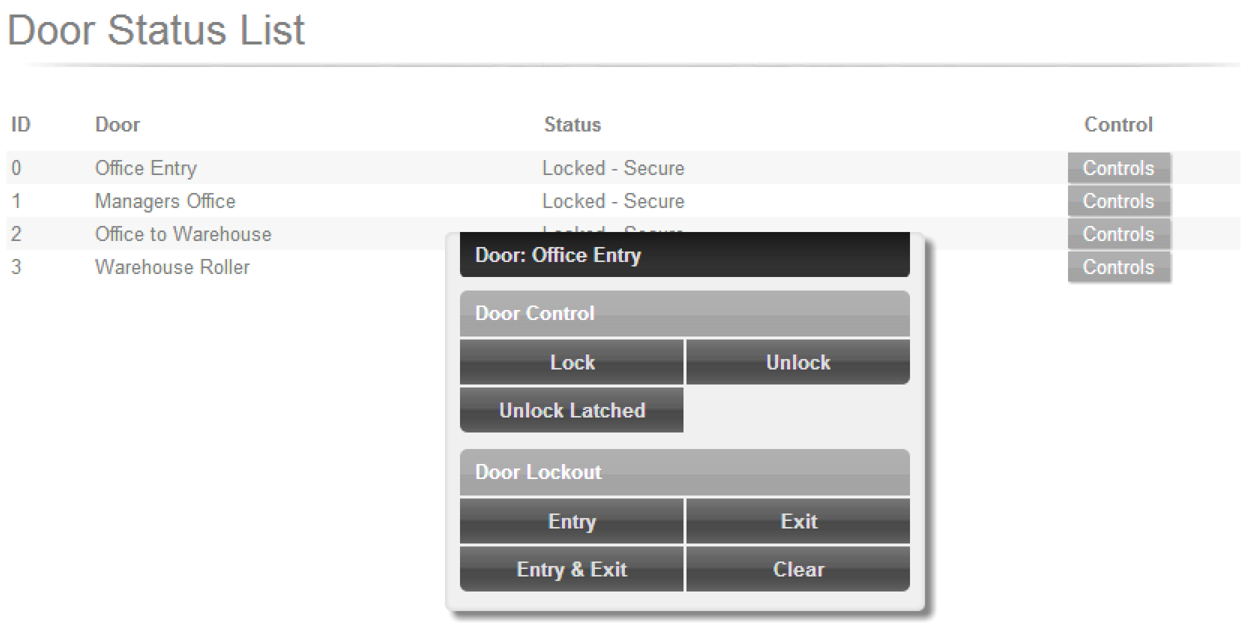
- Use the **Previous** and **Next** buttons to navigate through the pages.
- Click **Live View** to return to the real time display.

Status Lists

Status lists are accessed from the Monitoring menu and provide a real time display of the devices configured within the system.

This Menu Option:	Is Used To:
Doors	Display a list of all doors and their current status
Inputs	Display a list of all inputs and their current status
Areas	Display a list of all areas and their current status
Outputs	Display a list of all outputs and their current status
Trouble Inputs	Display a list of all trouble inputs and their current status
Services	Display a list of all services and their current status

Each status list also enable you to manually control the items from the web interface. For example, you can use the Door Status List to lock and unlock doors, or use the Area Status List to arm and disarm areas.



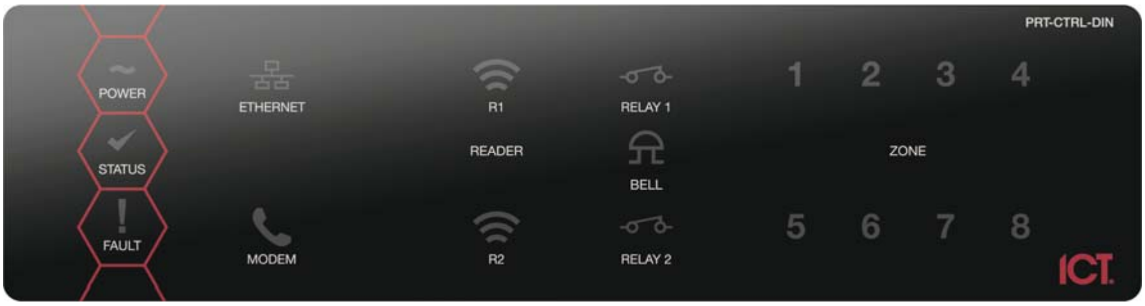
Door Status List

ID	Door	Status	Control
0	Office Entry	Locked - Secure	Controls
1	Managers Office	Locked - Secure	Controls
2	Office to Warehouse	Locked - Secure	Controls
3	Warehouse Roller		Controls

LED Indicators

All DIN Rail modules included comprehensive front panel diagnostic indicators that can assist in diagnosing faults and conditions. In some cases an indicator may have multiple meanings depending on the status indicator display at the time.

Controller (PRT-CTRL-DIN)



Power Indicator

The Power indicator is lit when the correct input voltage is applied to the Controller.

Note that this indicator may take several seconds to light up after power has been applied.

State		Description
~	On (green)	Correct input voltage applied
~	Off	Incorrect input voltage applied

Status Indicator

The Status indicator displays the status of the Controller.

State		Description
✓ ✓ ✓	Flashing (green) at 1 second intervals	The Controller is operating normally

Fault Indicator

The Fault indicator is lit any time the Controller is operating in a non-standard mode. During normal operation the fault indicator is off.

State		Description
!	Off	Controller is operating normally
!	On (red)	Controller is operating in a non-standard mode

Ethernet Link Indicator

The Ethernet indicator shows the status of the Ethernet connection.

State		Description
🖧	On (green)	Valid link with a hub, switch or direct connection to a personal computer detected
🖧 🖧 🖧	Flashing (green)	Data is being received or transmitted
🖧	Off	Ethernet cable not connected, no link detected

Modem Indicator

The Modem indicator shows the status of the onboard modem.

State		Description
☎	On (green)	Modem has control of telephone line
☎	Off	Modem is not active

Reader Data Indicators

The R1 and R2 indicators display the status of the data being received by the onboard readers.

State		Description
📶	Short (red) flash	A SHORT flash (<250 Milliseconds) will show that data was received but was not in the correct format.
📶	Long (red) flash	A LONG flash (>1 Second) indicates that the unit has read the data and the format was correct.

Bell Indicator

The Bell indicator shows the status of the bell output and the over current or circuit fault conditions.

State		Description
🔔	Off	Bell is connected, output is OFF
🔔	On (green)	Bell is ON
🔔	Single (green) flash	Bell is ON, the circuit is in over current protection
🔔 🔔	Two (green) flashes	Bell is OFF, the circuit to the siren/bell is cut, damaged or tampered

Relay Indicators

The Relay 1 and Relay 2 indicators show the status of the lock output relay.

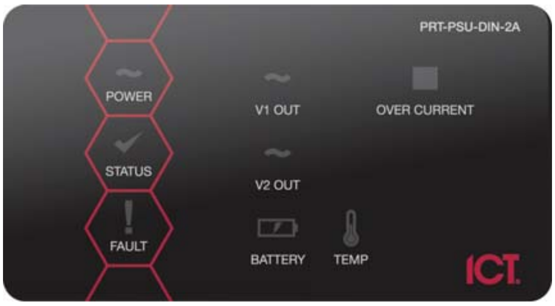
State		Description
	On (red)	Relay output is ON
	Off	Relay output is OFF

Zone (Input) Indicators

Whenever an input on the Controller is programmed with an input type and area, the input status is displayed on the front panel (indicators 1-8) corresponding to the physical input number (Z1-Z8). This allows easy walk test verification of inputs without the need to view the inputs from the keypad or Protege interface.

State		Description
1	Off	Input is not programmed
1	On (red)	Input is in an OPEN state
1	On (green)	Input is in a CLOSED state
1 1 1	Flashing (red)	Input is in a TAMPER state
1 1 1	Flashing (green)	Input is in a SHORT state

Power Supply (PRT-PSU-DIN-2A)



Power Indicator

The Power indicator is lit whenever the correct module input voltage is applied across the AC input terminals.

State		Description
~	Constantly on	Correct module input voltage applied
~	Constantly off	Incorrect module input voltage applied

Status Indicator

The Status indicator displays module status of the Power Supply.

State		Description
✓ ✓ ✓	Continuous fast flash (green)	Module attempting registration with controller
✓ ✓ ✓	Continuous slow flash (green)	Module successfully registered with controller
✓	Single flash (red)	Module communications activity

When the fault and status indicators are flashing alternately, the module is in the identification mode, enabling the installer to easily identify the module in question. Upon either a module update or the identification time period set expiring, the module will return to normal operation.

Fault Indicator

The Fault indicator is lit any time the module is operating in a non-standard mode.

State		Description
! ! !	Continuous slow flash (red)	Module is in boot mode awaiting firmware update
!	Constantly on (red)	Module is in error state

When the module is in an error state and the fault indicator is on, the status indicator will flash to indicate an error code. Refer to the Error Code Display section to determine the error.

V1 Output/V2 Output Indicators

The V1 Output and V2 Output indicators will show the status of the 12VDC output.

State		Description
~	Constantly on	12VDC output operating OK
~	Constantly off	12VDC output failure

Battery Indicator

The Battery indicator will show the status of the backup battery.

State		Description
🔋	Continuous flash (red)	Backup battery is disconnected
🔋	Constantly on (red)	Backup battery failed its dynamic battery test
🔋	Constantly on (green)	Last backup battery dynamic test successful

Temp Indicator

The Temp indicator will show the status of the unit's core temperature.

State		Description
🌡	Constantly on (red)	Core temperature exceeded. Over Temp Shutdown Activated
🌡	Continuous flash (red)	Core temperature within 15˚C of Over Temp Shutdown
🌡	Constantly on (green)	Core temperature OK

Over Current Indicator

The Over Current indicator will show the status of the output current for both V1+ and V2+.

State		Description
🟥	Constantly on	Output current exceeded. Over Current Shutdown Activated
⬛	Constantly off	Maximum output current not exceeded

Error Code Display

The following table is only valid if the FAULT indicator is CONSTANTLY ON and the STATUS indicator is FLASHING RED.

If the fault indicator is FLASHING the module requires a firmware update or is currently in firmware update mode.

The status indicator will FLASH RED with the error code number. The error code number is shown with a 250ms ON and OFF period (duty cycle) with a delay of 1.5 seconds between each display cycle.

Flash	Error Description
1	Unknown Error Code The error code returned by the system controller could not be understood by the module. Contact Integrated Control Technology.
2	Firmware Version The firmware version on the module is not compatible with the system controller. To clear this error, update the module using the module update application.
3	Address Too High The module address is above the maximum number available on the system controller. To clear this error change the address to one within the range set on the system controller, restart the module by disconnecting the power.
4	Address In Use The Address is already in use by another module. To clear this error set the address to one that is not currently occupied. Use the view network status command to list the attached devices, or the network update command to refresh the registered device list.
5	Controller Secured Registration Not Allowed Controller is not accepting any module registrations. To allow module registrations use the network secure command to change the secure setting to not secured.
6	Serial Number Fault The serial number in the device is not valid. Return the unit to the distributor for replacement.
7	Locked Device The module or system controller is a locked device and cannot communicate on the network. Return the unit to the distributor for replacement.

Trouble Inputs

Trouble inputs are used to monitor the status of the Controller and in most cases are not physically connected to an external input. These can then be used to report a message to a monitoring station, remote computer, keypad or siren.

The following lists the trouble inputs that are configured in the Controller:

Input Number	Description
CP001:02	12V Supply Failure
CP001:04	Real Time Clock Not Set
CP001:05	Service Test Report
CP001:06	ContactID Reporting Failure
CP001:07	Phone Line Fault
CP001:08	Auxiliary Fuse / Supply Fault
CP001:09	Bell Siren Tamper / Cut
CP001:11	Bell Siren Current Overload
CP001:13	Module Communication Fault
CP001:14	Module Security Violation
CP001:20	ReportIP Reporting Failure
CP001:24	Installer Logged In
CP001:29	System Restarted

Property Reference Guide

This section describes each of the properties available when programming your system, and what they do.

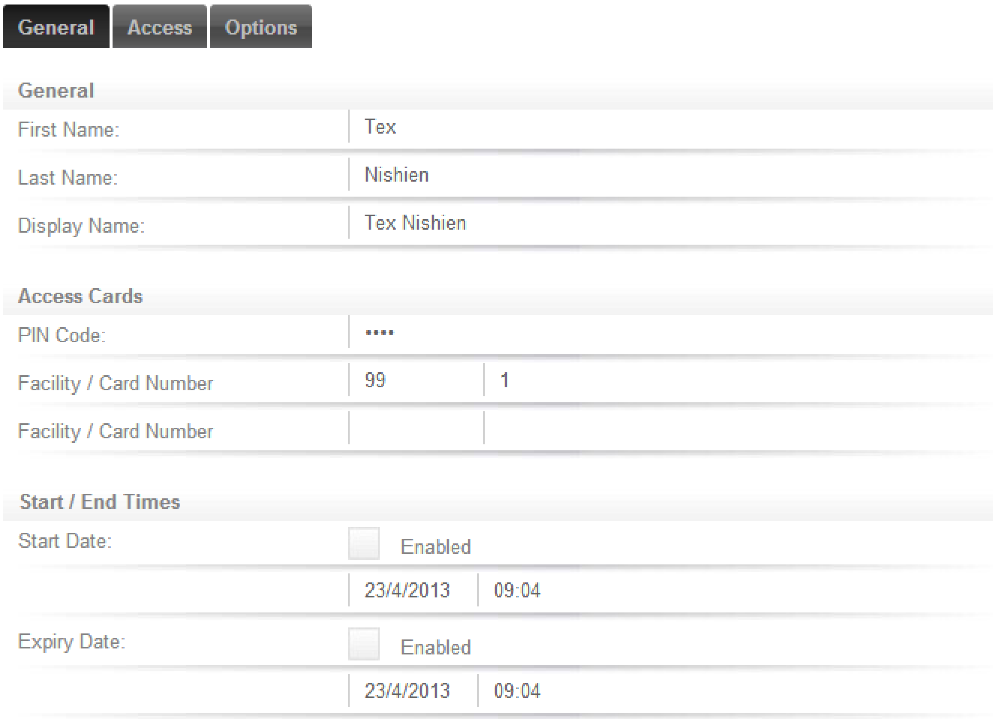
Users

The Users menu contains the various functions for working with and configuring users (sometimes referred to as cardholders), and defining the access they have within a site.

This Option:	Is Used To:
Users	Add and manage users into the system with access credentials
Access Levels	Configure the access levels that will be assigned to users and determine what they can do within the system

Users

A user is a person that is programmed into the system with access control and alarm credentials. The user can then be assigned access to programmed doors and functions of the system.



General

First Name:	Tex	
Last Name:	Nishien	
Display Name:	Tex Nishien	

Access Cards

PIN Code:	••••	
Facility / Card Number	99	1
Facility / Card Number		

Start / End Times

Start Date:	□ Enabled	
	23/4/2013	09:04
Expiry Date:	□ Enabled	
	23/4/2013	09:04

General

- **First Name:** The first name of the user.
- **Last Name:** The last name of the user.
- **Display Name:** The display name of the user as it appears on LCD and Touchscreen keypads. This field prefills automatically based on the first/last names entered, but is limited to 16 characters and can be edited as required.

Access Cards

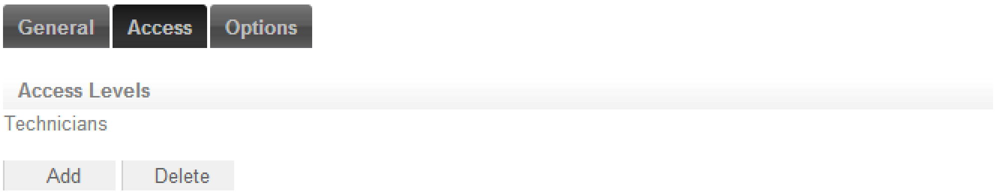
- **Pin Code:** Security pin code for the user to log on with.
- **Facility/Card Number:** The security card and facility number for the user. Each user can have up to 8 facility/card codes.

Start / End Times

- **Start Date:** Optional setting enabling you to set a start date for the user. For example, an employee that will start work on a specific date.
- **Expiry Date:** Optional setting enabling you to set an expiry date for the user. For example, a contractor who will finish on a specific date.

Users | Access

Defines the access level(s) for the user. When the user performs an action, the system checks the access level(s) to ensure the user has the relevant permissions to perform the requested action.

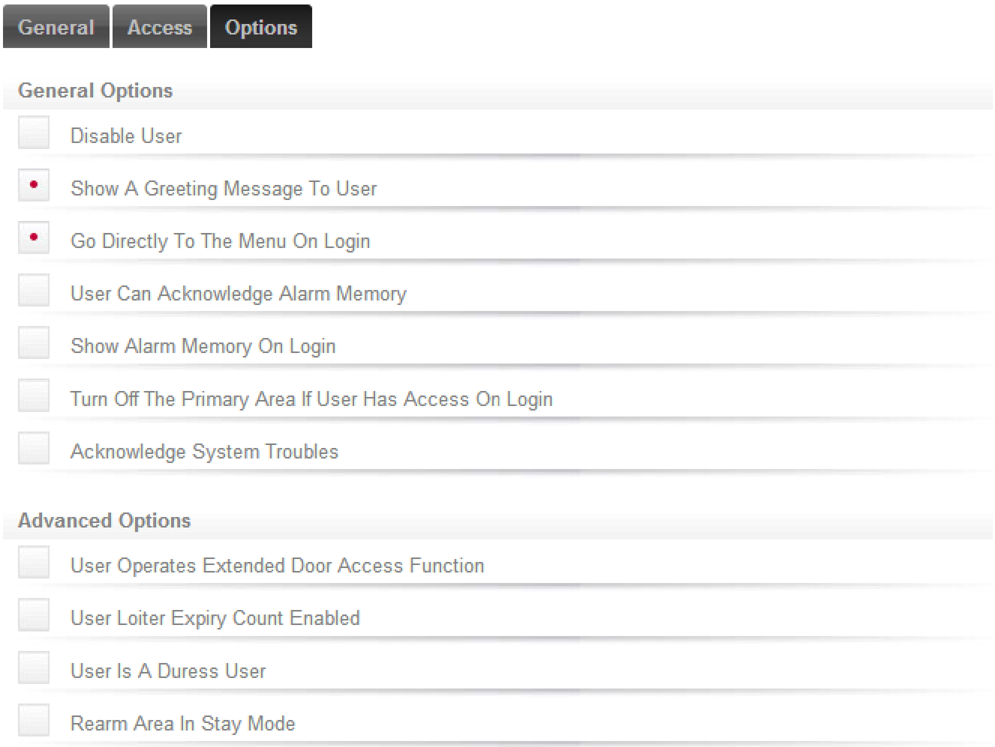


Access Levels

Technicians

1. Click **Add** to open the Select Record window
2. Select the relevant Access Level(s) and click **OK**.

Users | Options



General Options

□ Disable User

☑ Show A Greeting Message To User

☑ Go Directly To The Menu On Login

□ User Can Acknowledge Alarm Memory

□ Show Alarm Memory On Login

□ Turn Off The Primary Area If User Has Access On Login

□ Acknowledge System Troubles

Advanced Options

□ User Operates Extended Door Access Function

□ User Loiter Expiry Count Enabled

□ User Is A Duress User

□ Rearm Area In Stay Mode

General Options

- **Disable User**: When selected, the user record is disabled preventing access via keypad or card reader.
- **Show A Greeting Message To User:** When enabled the user is shown a greeting upon entering their code on a LCD User Station (for example: Good Morning John Smith). Disabling this option takes the user to the area control menu or directly to the main menu. This setting can be overridden by the same option in the users menu group that is assigned to the access level of the user.
- **Go Directly To The Menu On Login (no Area Control):** When enabled the user is taken directly to the main menu and not shown the area control functions. Display of the area control is by default. Enable this option for users that won't normally perform area operations on the keypad.

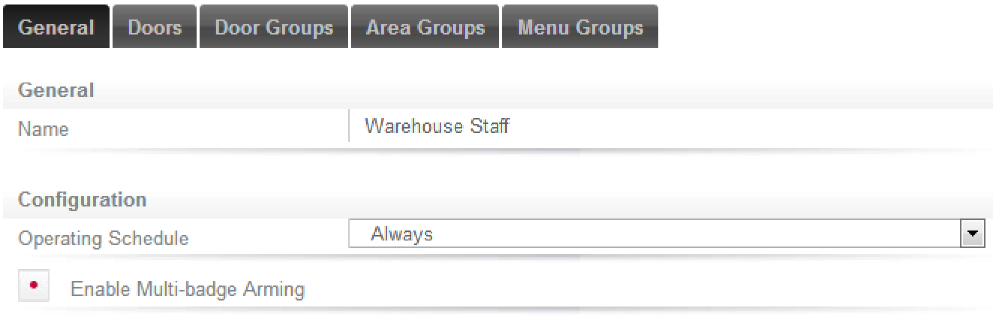
- User Can Acknowledge Alarm Memory: When enabled the user is able to acknowledge alarm memory. Alarm memory is stored for each area and will record the last 4 activations. The alarm memory can be viewed from MENU 5 on the keypad and must be enabled to allow acknowledgment to occur. This setting can be overridden by the same option in the menu group.
- Show Alarm Memory On Login: When enabled if any alarms have occurred on the primary area that the keypad is assigned the memory will be shown to the user. This option can be overridden by the same option in the menu group.
- Turn Off The Primary Area If User Has Access On Login: When enabled the primary area for the keypad that the user logs into will be disarmed automatically.
- Turn Off The User Area On Login If User Has Access: When enabled the area that is programmed as the user area will be turned off when they login to a keypad.
- Acknowledge System Troubles: When enabled the user is able to acknowledge system trouble conditions from the view menu (MENU 5) on the LCD keypad.

Advanced Options

- User Operates Extended Door Access Function: When enabled, extends door access time for people with disabilities.
- User Loiter Expiry Count Enabled: When enabled the user is included in the loiter area timing calculations. This means the user will be allowed access for the period of loiter time set for the area that they have entered. The areas used for the loiter time must be configured as loiter areas and used as the inside and outside areas for the door. This is an administrative setting and should only be edited by the system administrator.
- User Is A Duress User: When enabled the user is a duress user and will activate the duress trouble input on a keypad and monitoring console. The duress trouble input must be enabled and programmed for the keypad.
- Rearm Area In Stay Mode: This option is used in conjunction with the User Rearm in Stay Mode option under the Area programming. If both User and Area options are enabled, when the user disarms the Area, once the rearm period has elapsed the area will automatically rearm in Stay mode.

Access Levels

Access levels are assigned to users. When a user is assigned an access level that user is able to access the programmed options within the access level. The access level determines what they can do in the system and contains Alarm Areas, Doors, and Keypad Menus.



General

Name: Warehouse Staff

Configuration

Operating Schedule: Always

● Enable Multi-badge Arming

General

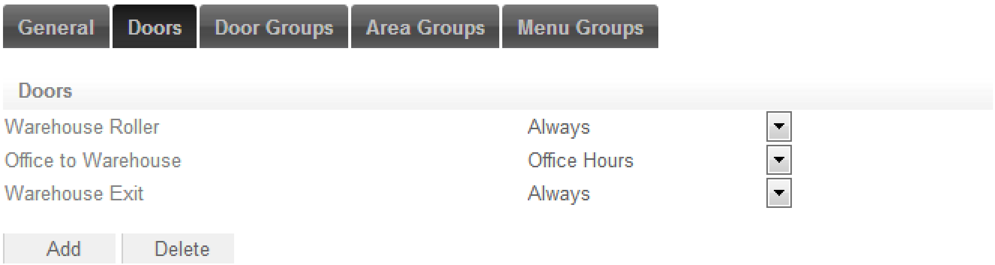
- Name: The name of the access level.

Configuration

- Operating Schedule: Determines when the access level is valid.
- Enable Multi-badge Arming: Used in conjunction with the Reader Arming Mode (defined by the Reader Expander settings) to enable a user to perform various operations when badging their card multiple times.

Access Levels | Doors

Defines the doors that the user has access to, and the schedule that is used.

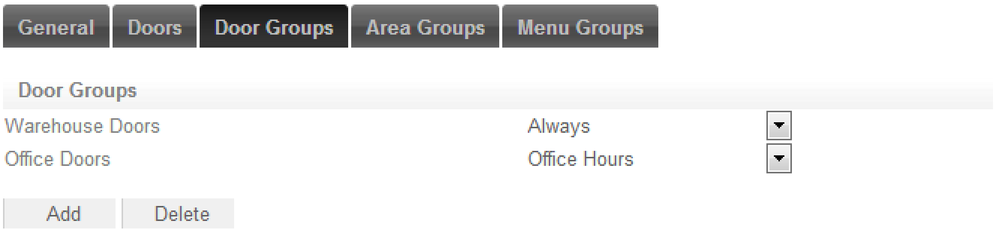


Doors	
Warehouse Roller	Always
Office to Warehouse	Office Hours
Warehouse Exit	Always

By default, the schedule is set to Always, meaning access to the defined doors is permitted at all times. Assigning another schedule will restrict access to the door for the period set in the schedule. For example, limiting access to an office so it may only be entered during office hours.

Access Levels | Door Groups

Defines the Door Groups that the user has access to, and the schedule that is used.

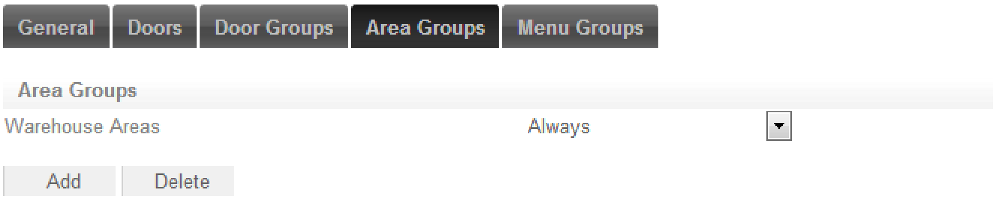


Door Groups	
Warehouse Doors	Always
Office Doors	Office Hours

By default, the schedule is set to Always, meaning access to the defined doors is permitted at all times. Assigning another schedule will restrict access to doors within that group for the period set in the schedule. For example, limiting access to an office so it may only be entered during office hours.

Access Levels | Area Groups

Defines the Area Groups that the user is allowed to arm and disarm, and the schedule that is used.

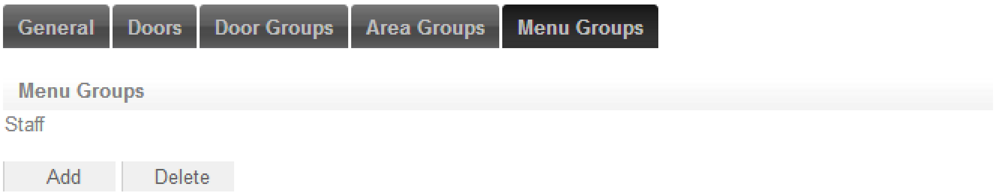


Area Groups	
Warehouse Areas	Always

By default, the schedule is set to Always, meaning they can arm/disarm areas within that group at all times. Assigning another schedule will restrict arming and disarming to the period set in the schedule.

Access Levels | Menu Groups

Defines the Menu Groups that the user has access to. These determine what a user can do at a keypad.



Menu Groups

Staff

Monitoring

Functions for monitoring your site are contained under the Monitoring menu.

This Option:	Is Used To:
Events	Display a live view of all events as they occur
Doors	Display a list of all doors and their current status
Inputs	Display a list of all inputs and their current status
Areas	Display a list of all areas and their current status
Outputs	Display a list of all outputs and their current status
Trouble Inputs	Display a list of all trouble inputs and their current status
Services	Display a list of all services and their current status

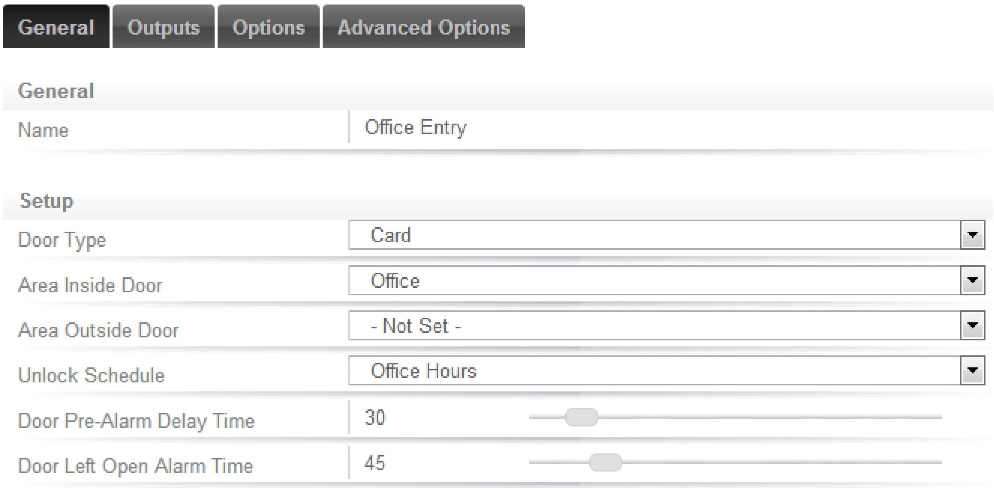
Programming

Functions for programming a site, such as configuring doors, areas, inputs, outputs, and such, are all found under the Programming menu.

This Option:	Is Used To:
Doors	Configure doors to control user access or to monitor and control the flow of people into an area
Door Groups	Create and manage door groups that define which doors a user will be able to access and/or control
Inputs	Configure inputs such as motion detectors, door contacts and other protection devices
Door Types	Create and manage door types to define how a door will operate
Input Types	Create and manage input types to define how an input will operate in an area
Areas	Configure areas enabling the Protege system to be divided up into separate sections (alarm areas or partitions)
Area Groups	Create area groups that are used to control the areas that a user can arm and disarm
Outputs	Create and manage outputs to control devices from the Protege System, such as those that activate lighting, activate a siren, turn on an indicator or unlock a door
Output Groups	Create output groups that group a number of outputs together and are used to control the outputs that a user can activate and deactivate
Menu Groups	Create menu groups that determine which keypad functions those users have access to
Trouble Inputs	Configure the trouble inputs used to monitor the status and condition of the system
Phone Numbers	Configure the phone numbers assigned to a service that communicate using a modem or telephone connection
Services	Create and manage services to provide interaction between Protege and external systems

Doors

Doors are used for the control of access by users or to monitor and control the flow of people in to an area.



General

Name	Office Entry

Setup

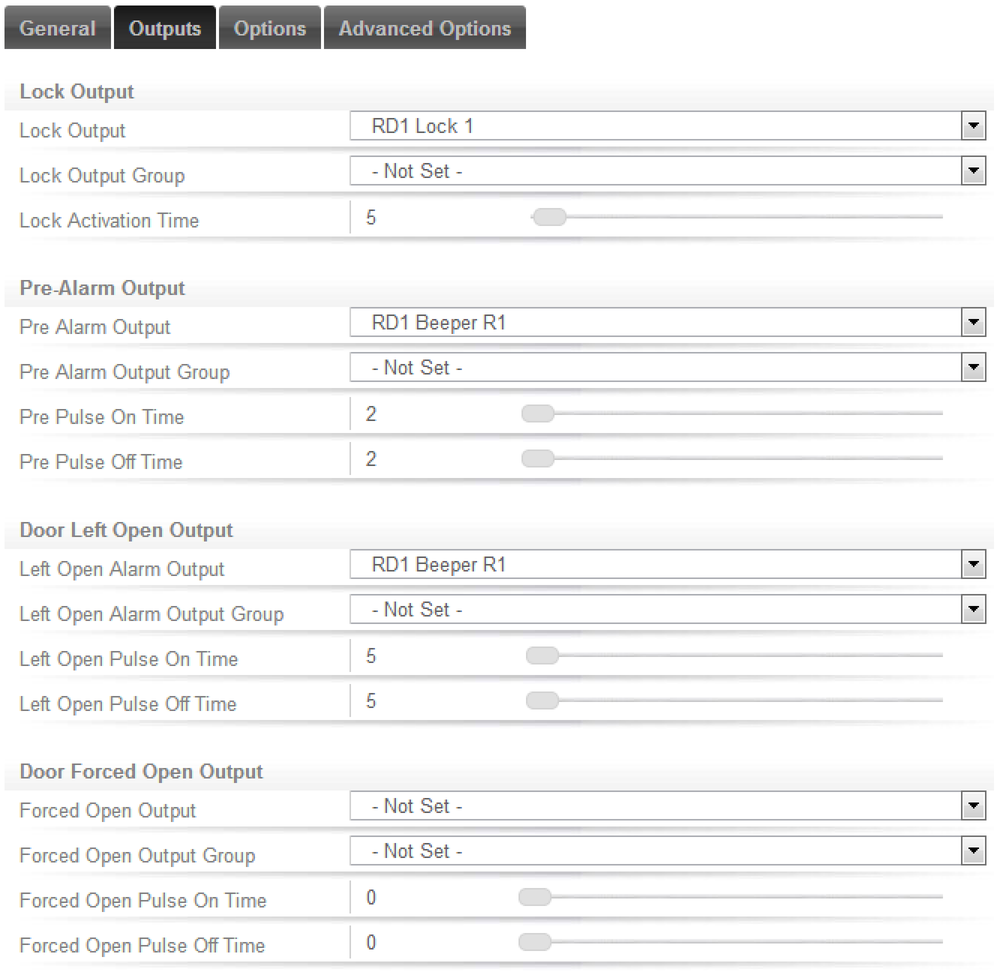
Door Type	Card
Area Inside Door	Office
Area Outside Door	- Not Set -
Unlock Schedule	Office Hours
Door Pre-Alarm Delay Time	30
Door Left Open Alarm Time	45

- Name: The name of the door.

Setup

- Door Type: The door type selection allows the door to function in different modes. These modes require the user to present specific credentials for example a card, card and pin, card or pin and pin only. By using a door type these can be scheduled dependent on the time of day allowing different security credentials to be used.
- Area Inside Door: The inside area defines which area is on the inside of this door. This is used to prevent a user from gaining access to a door when the area is armed and they cannot disarm it as well as automatically disarming the area when the door is accessed. Using the door and area control integrates the two systems and is an ideal solution to false alarm prevention.
- Area Outside Door: The outside area defines which area is on the outside of this door. This is used to prevent a user from gaining access to a door when the area is armed and they cannot disarm it as well as automatically disarming the area when the door is accessed. Using an inside and an outside area usually requires that the door is programmed with both an entry and exit reader.
- Unlock Schedule: The unlock schedule determines when this door will unlocked. For example an employee entry door may require to be unlocked at 7am and locked at 5pm you would assign a suitable schedule here. Using the unlock on late control option prevents the door unlocking on schedule until the first user access the door.
- Door Pre-Alarm Delay Time: The pre-alarm time is programmed to allow the door to be left open for a certain period before it will generate a pre-alarm condition. When the pre-alarm condition is reached this will typically activate an output on the Reader Expander that is controlling the door.
- Door Left Open Alarm Time: The maximum door open time when it is reached will generate a door left open alarm activating the appropriate trouble input and output on the Reader Expander that is controlling the door. The default configuration will mean that the door will generate a left open alarm 15 seconds after the pre-alarm condition. For the trouble inputs to activate they must be set in the reader expander.

Doors | Outputs



Lock Output	
Lock Output	RD1 Lock 1
Lock Output Group	- Not Set -
Lock Activation Time	5

Pre-Alarm Output	
Pre Alarm Output	RD1 Beeper R1
Pre Alarm Output Group	- Not Set -
Pre Pulse On Time	2
Pre Pulse Off Time	2

Door Left Open Output	
Left Open Alarm Output	RD1 Beeper R1
Left Open Alarm Output Group	- Not Set -
Left Open Pulse On Time	5
Left Open Pulse Off Time	5

Door Forced Open Output	
Forced Open Output	- Not Set -
Forced Open Output Group	- Not Set -
Forced Open Pulse On Time	0
Forced Open Pulse Off Time	0

Lock Output:

- Lock Output/Output Group: You can assign an output or output group that controls the physical electric lock for the door. This is typically the lock control output on the reader expander that is being used to control the door.
- Lock Activation Time: The unlock time determines how long the lock that controls the door will remain unlocked for when a user accesses the door.

Pre-alarm Output:

- Pre Alarm Output/Output Group: You can assign an output or output group that will activate when the pre-alarm time that is programmed is reached. Use this to warn users that the door will generate an alarm if it is left open any longer.
- Pre Alarm Pulse On Time: The pre alarm pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
- Pre Alarm Pulse Off Time: The pre alarm pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

Door Left Open Output:

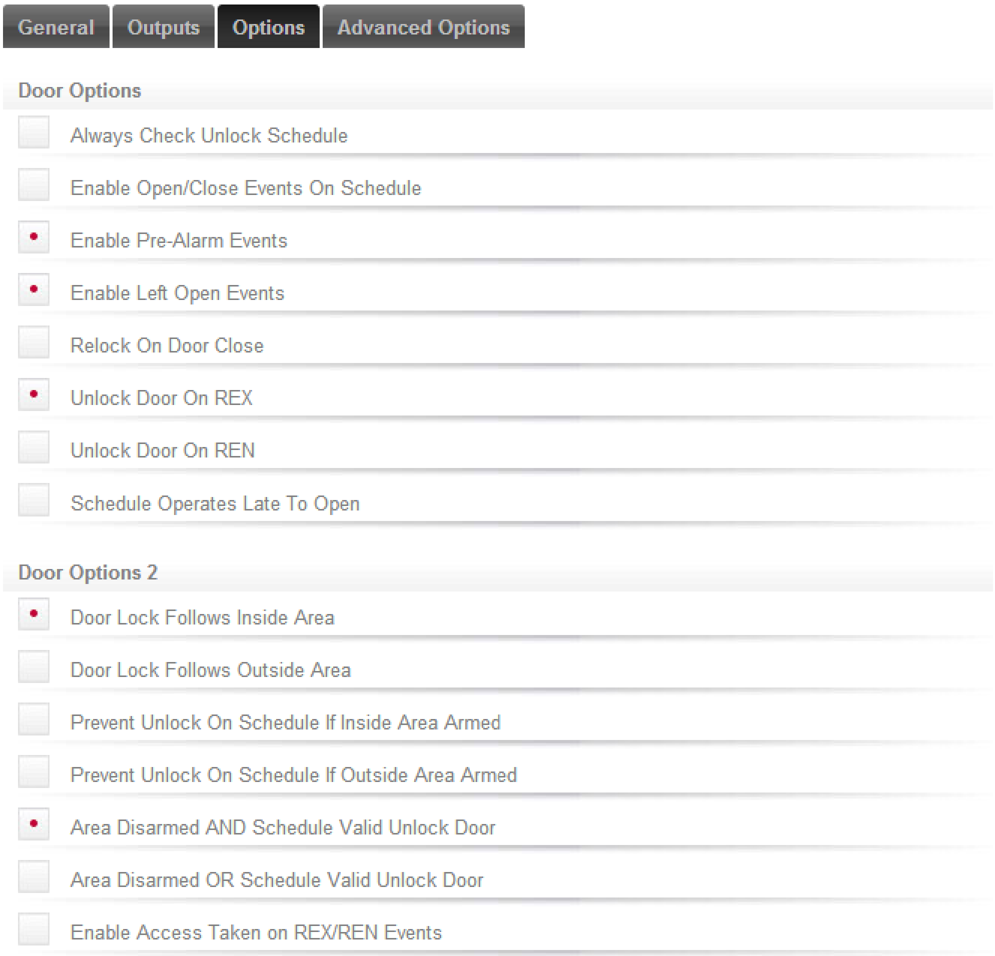
- Left Open Alarm Output/Output Group: You can assign an output or output group that will activate when the maximum open time that is programmed is reached indicating that the door has been left open. Use this to tell users that the door must be closed immediately and that the system has generated an alarm.

- Left Open Alarm Pulse On Time: The left open alarm pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
- Left Open Alarm Pulse Off Time: The left open alarm pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

Door Forced Open Output:

- Force Open Output/Output Group: You can assign an output or output group that will activate when the door is forced open without any access. Use this feature to activate a local output at the door indicating it has been forced. To generate an alarm on a forced door use the forced door trouble input and assign this to an area so that a report can be sent to a monitoring station or locally control computer.
- Force Open Pulse On Time: The forced open pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
- Force Open Pulse Off Time: The forced open pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.

Doors | Options



Door Options

□ Always Check Unlock Schedule

□ Enable Open/Close Events On Schedule

● Enable Pre-Alarm Events

● Enable Left Open Events

□ Relock On Door Close

● Unlock Door On REX

□ Unlock Door On REN

□ Schedule Operates Late To Open

Door Options 2

● Door Lock Follows Inside Area

□ Door Lock Follows Outside Area

□ Prevent Unlock On Schedule If Inside Area Armed

□ Prevent Unlock On Schedule If Outside Area Armed

● Area Disarmed AND Schedule Valid Unlock Door

□ Area Disarmed OR Schedule Valid Unlock Door

□ Enable Access Taken on REX/REN Events

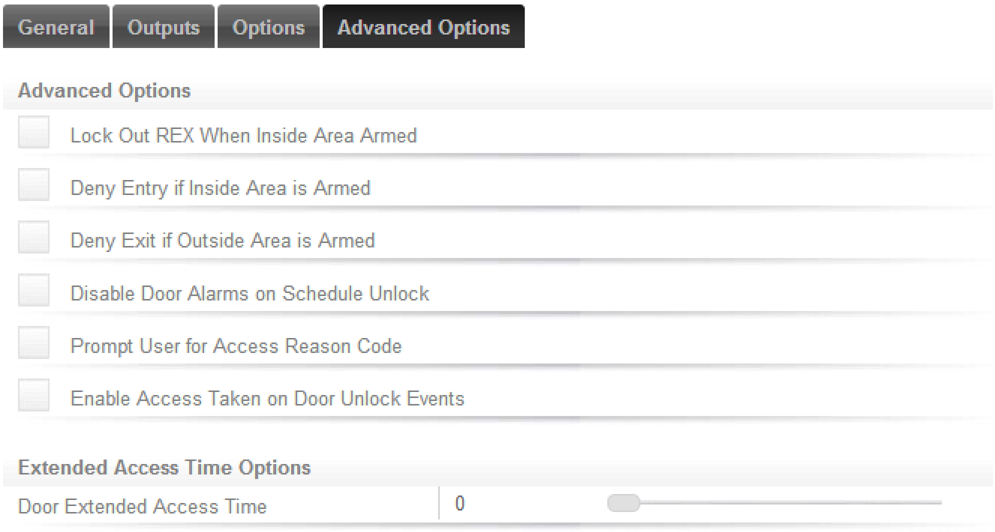
Door Options

- Always Check Unlock Schedule: When enabled the door will revalidate the unlock schedule that it is assigned each minute. This will prevent the door from being controlled and locked when it should be unlocked. This option also prevents schedule and area control from operating correctly and if enabled will prevent the follow inside and follow outside area status from operating. Setting this option will allow the prevent unlock on arming and normal scheduling operations to occur.
- Enable Open/Close Events On Schedule: When enabled the door will not log a door opened event when it is unlocked on schedule. This will prevent the door from filling the event buffer with events that are not needed.
- Enable Pre-Alarm Events: When enabled the door will generate a pre-alarm event when the pre-alarm timer for the door is reached.
- Enable Left Open Events: When enabled the door will generate a door left open event when the door maximum open time is reached.
- Relock On Door Close: When enabled the door will lock when it detects a door close event and the lock output is activated.
- Unlock Door On REX: When enabled the door will activate the lock output when a request to exit occurs.
- Unlock Door On REN: When enabled the door will activate the lock when a request to enter occurs.
- Schedule Operates Late To Open: When enabled the Door will not unlock on schedule until the first access has been accepted at the door.

Door Options 2

- Door Lock Follows Inside Area: When enabled the door will unlock if the inside area is disarmed. If no arm/disarm schedule is set, the Area Disarmed AND Schedule Valid Unlock Door option MUST be enabled for this function to operate.
- Door Lock Follows Outside Area: When enabled the door will unlock if the outside area is disarmed. If no arm/disarm schedule is set, Area Disarmed AND Schedule Valid Unlock Door option MUST be enabled for this function to operate.
- Prevent Unlock On Schedule If Inside Area Armed: When enabled the door will not unlock when the schedule is valid if the inside area is armed. Use this option with the late open option to prevent false alarms by entry of personal before an area is disarmed. This option only operates if the Door Lock Follows Inside Area and Door Lock Follows Outside Area options are not enabled. To prevent unlocking and locking based on schedule and area status set the Area Disarmed AND Schedule Valid Unlock Door and Area Disarmed OR Schedule Valid Unlock Door options to the required values.
- Prevent Unlock On Schedule If Outside Area Armed: When enabled the door will not unlock when the schedule is valid if the outside area is armed. Use this option with the late open option to prevent false alarms by entry of personal before an area is disarmed.
- Area Disarmed AND Schedule Valid Unlock Door: When enabled the door will unlock if the door unlock schedule is valid AND the inside or outside area is disarmed dependent on the options set for Prevent Unlock On Schedule If Inside Area Armed and Prevent Unlock On Schedule If Outside Area Armed.
- Area Disarmed OR Schedule Valid Unlock Door: When enabled the door will unlock if the door unlock schedule is valid OR the inside or outside area is disarmed dependent on the options set for Prevent Unlock On Schedule If Inside Area Armed and Prevent Unlock On Schedule If Outside Area Armed.
- Enable Access Taken On REX/REN Events: When enabled the door will generate a Request to Exit (or Enter) event if the door opens while the door is unlocked from a request to exit. If the door remains closed an Access Not Taken event will be generated

Doors | Advanced Options



Advanced Options

□ Lock Out REX When Inside Area Armed

□ Deny Entry if Inside Area is Armed

□ Deny Exit if Outside Area is Armed

□ Disable Door Alarms on Schedule Unlock

□ Prompt User for Access Reason Code

□ Enable Access Taken on Door Unlock Events

Extended Access Time Options

Door Extended Access Time	0

Advanced Options

- Lock out REX When Inside Area Armed: When enabled the door will deny a request to exit when the inside area has been armed to prevent egress from an armed area.
- Deny Entry if Inside Area is Armed: When enabled the door will deny any entry if the inside area is armed.
- Deny Exit if Outside Area is Armed: When enabled the door will prevent any exit if the outside area is armed.
- Disable Door Alarms on Schedule Unlock: When enabled the door will not generate the door left open alarm events to the reader expanders beeper and led ports if they are programmed. This allows a door to be "propped" open during normal opening times however a pre-alarm warning will still be generated. This option DOES NOT prevent the door left open trouble input from being sent to the monitoring station if reporting on the trouble input is programmed to be generated. To prevent the door open alarms from being sent schedule the input type for the door open alarm events to operate without reporting during the day.
- Prompt User For Access Reason Code: When enabled the user will be prompted on the reader expanders associated keypad to enter their reason for access. The user must enter the reason before access will be granted.
- Enable Access Taken on Door Unlock Events: When enabled the door will generate a User Access Taken event if the door opens while the door is unlocked after entry has been granted. If the door remains closed an Access Not Taken event will be generated.

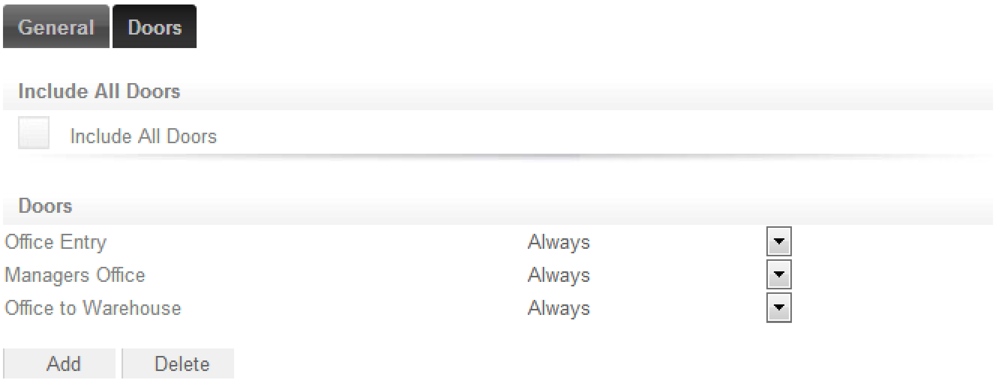
Extended Access Time Options

- Door Extended Access Time: The duration (in seconds) that the door remains opens for users tagged as requiring extended access.

Door Groups

Door groups are used to define which doors a user will be able to access and/or control. A door group is assigned to an access level to restrict the ability for a user to gain entry or exit to certain doors.

Select the **Doors** tab to add doors to the group.



Include All Doors

□ Include All Doors

Doors

Office Entry	Always
Managers Office	Always
Office to Warehouse	Always

Include All Doors

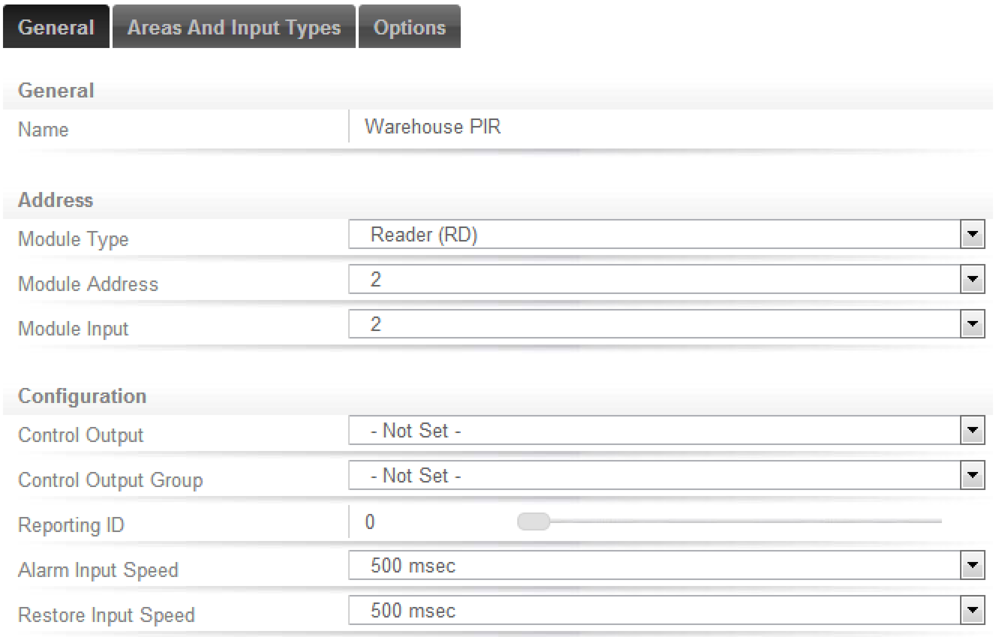
- **Include All Doors**: Select this option to include ALL doors in the group.

Doors

- The doors that belong to the door group. Select doors by clicking **Add** and dragging them to the window from the list that is displayed.

Inputs

Motion detectors, door contacts and other protection devices are connected to the system on inputs. An input belongs to an area to protect the area and system from unauthorized entry. For example, a motion sensor input in reception may be assigned to an Administration Area.



General

Name	Warehouse PIR

Address

Module Type	Reader (RD)
Module Address	2
Module Input	2

Configuration

Control Output	- Not Set -
Control Output Group	- Not Set -
Reporting ID	0
Alarm Input Speed	500 msec
Restore Input Speed	500 msec

General

- **Name**: The name of the input.

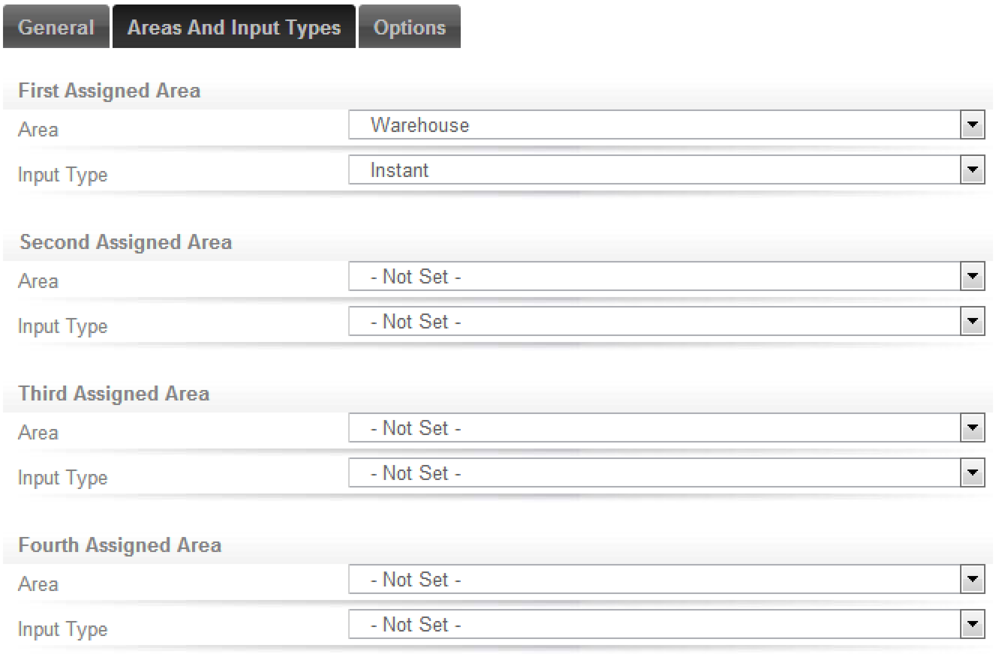
Address

- Module Type: The type of module that the input is attached to.
- Module Address Input: The address of the module that the input is attached to.
- Module Input: The index of the specified input on that module.

Configuration

- Control Output/Output Group: The output that is assigned to the input. This will activate whenever an input type process's the input with the activate input output options enabled. The input type must have the appropriate input control output options set in the output options. An output can be assigned to the input type and to the input allowing many to one and one to many configurations.
- Reporting ID: The Input Reporting ID allows the installer to program any reporting number to any input. This provides an extremely high level of flexibility to assign true reporting numbers to the inputs. An input that is assigned the same reporting ID as another input will result in both the inputs reporting that ID. If an input is assigned an ID number that is higher than the maximum number that can be reported by a particular service, the service will use the maximum number that can be assigned for the format.
- Alarm Input Speed: The alarm input speed determines how long an input must be open for before an alarm event will be generated. This can be set from 0 seconds up to 1 hour. If the Alarm Input Speed is set at 0 seconds, the Restore Input Speed cannot be set below 100ms.
- Restore Input Speed: The restore input speed determines how long an input must be closed for before an restore event will be generated. This can be set from 0 seconds up to 1 hour. If the Alarm Input Speed is set at 0 seconds, the Restore Input Speed cannot be set below 100ms.

Inputs | Areas and Input Types



First Assigned Area

Area	Warehouse
Input Type	Instant

Second Assigned Area

Area	- Not Set -
Input Type	- Not Set -

Third Assigned Area

Area	- Not Set -
Input Type	- Not Set -

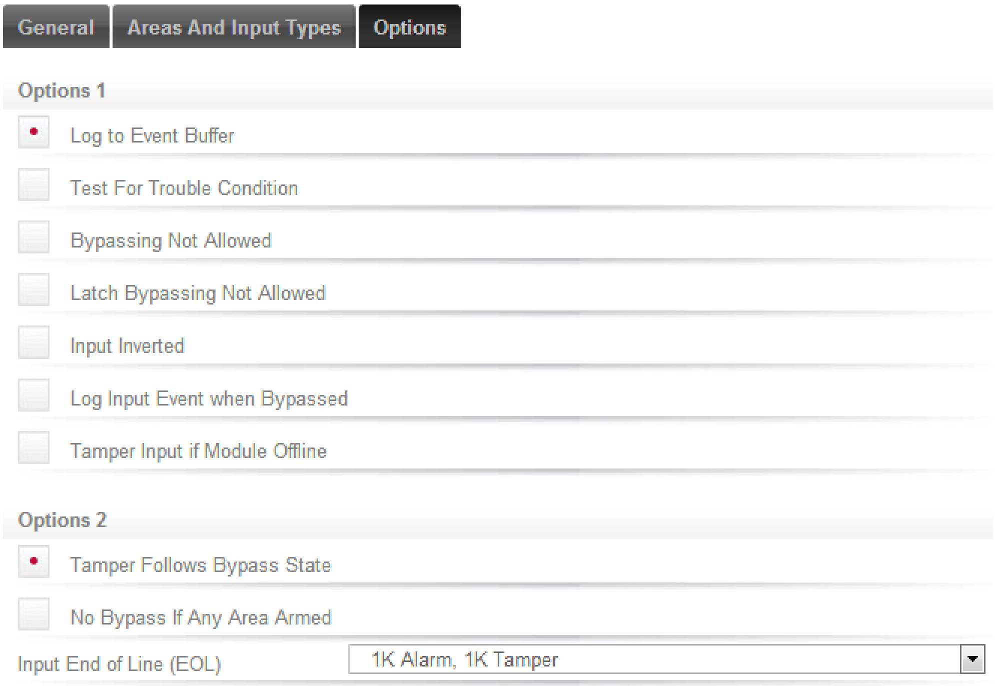
Fourth Assigned Area

Area	- Not Set -
Input Type	- Not Set -

Assigned Areas

- Area: The input must be assigned to at least one area for it to perform any function in the system and an input can be assigned in up to 4 different areas. An input can perform a different function in each area which is defined by the input type. For example an input can be a delay input in one area and an instant input in another.
- Input Type: When an input is assigned to an area the input must be programmed with the type of input (24 Hour Panic, Burglary Delay etc) in order to function.

Inputs | Options



Options 1

☑ Log to Event Buffer

☐ Test For Trouble Condition

☐ Bypassing Not Allowed

☐ Latch Bypassing Not Allowed

☐ Input Inverted

☐ Log Input Event when Bypassed

☐ Tamper Input if Module Offline

Options 2

☑ Tamper Follows Bypass State

☐ No Bypass If Any Area Armed

Input End of Line (EOL) 1K Alarm, 1K Tamper

Options 1

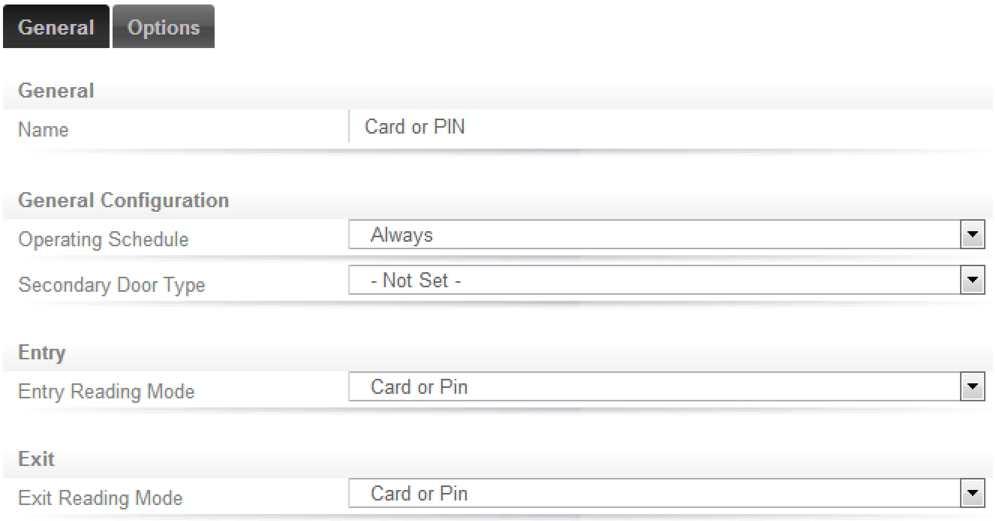
- Log to Event Buffer: When enabled, the input will generate an event whenever it is opened, closed, tampered or shorted. The input will still perform all functions that are programmed if this is not enabled. When using inputs as automation inputs it is recommended to disable the event logging option to reduce the impact on the event log buffer.
- Test For Trouble Condition: When enabled the input will be monitored for a trouble condition and cause a trouble alarm to be generated. The trouble will be generated only if the input is either shorted or tampered.
- Bypassing Not Allowed: When enabled, the input is a high security input and cannot be bypassed. However, the input can still be force armed if the Force Arming option is turned on. In order to avoid this, and to insure that the input is not ignored when force arming, the Input Force Arming option should be turned off in the input type that is assigned to the input.
- Latch Bypassing Not Allowed: When enabled the input is a high security input and cannot be latch bypassed. However, the input can still be force armed if the Force Arming option is turned on. In order to avoid this, and to insure that the input is not ignored when force arming, the Input Force Arming option should be turned off.
- Input Inverted: When enabled, the input will operate in an inverted mode. By default all inputs are normally closed, setting this option will change the input to normally open. At least one input open and close is needed to correctly update the input state.
- Log Input Event when Bypassed: When enabled, the input will generate an event whenever it is bypassed.
- Tamper Input if Module Offline: When enabled, the input will operate as a tamper input when the module is offline.

Options 2

- Tamper Follows Bypass State: When enabled the input will bypass the tamper monitoring of the input at the time the input is bypassed.
- No Bypass If Any Area Armed: When enabled the input will be prevented from being bypassed if it is already assigned to an area that has either the 24HR processing enabled or the area is armed.
- Input End of Line (EOL): Defines the resistors used for EOL configuration.

Door Types

Door types define how a door will operate, and when the door type is valid.



General

Name	Card or PIN

General Configuration

Operating Schedule	Always
Secondary Door Type	- Not Set -

Entry

Entry Reading Mode	Card or Pin

Exit

Exit Reading Mode	Card or Pin

General

- Name: The name of the door type.

General Configuration

- Operating Schedule: The door type schedule allows a door type to be scheduled for use during a certain time period. For example setting a door type schedule for card only from between 9am and 5pm and then a secondary door type of Card and Pin will mean during the hours of 9am and 5pm any door assigned the door type will require card only access during 9am and 5pm however outside this time will require a card access and pin number. Use this option to increase the security of the main entry doors after hours while maintaining a faster traffic flow during working hours.
- Secondary Door Type: Used in conjunction with the Operating Schedule an allows a door to have a secondary configuration when that schedule is invalid. This allows different modes of control over the method a user has to access a door. For example between 9am and 5pm the user may be required to access the door with only a card, however outside these hours a card and pin is required.

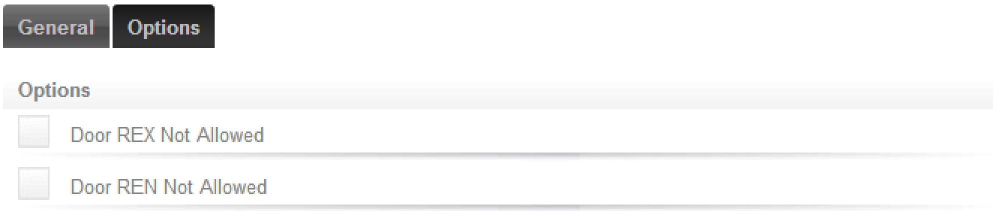
Entry

- Entry Reading Mode: The reader entry operation mode determines how an entry reader that is associated with the door that has this door type assigned will operate. Choose from:
  - Card only
  - Pin only
  - Card and Pin
  - Card or Pin

Exit

- Exit Reading Mode: The reader in operation mode determines how an exit reader that is associated with the door that has this door type assigned will operate. Choose from:
  - Card only
  - Pin only
  - Card and Pin
  - Card or Pin

Door Types | Options



Options

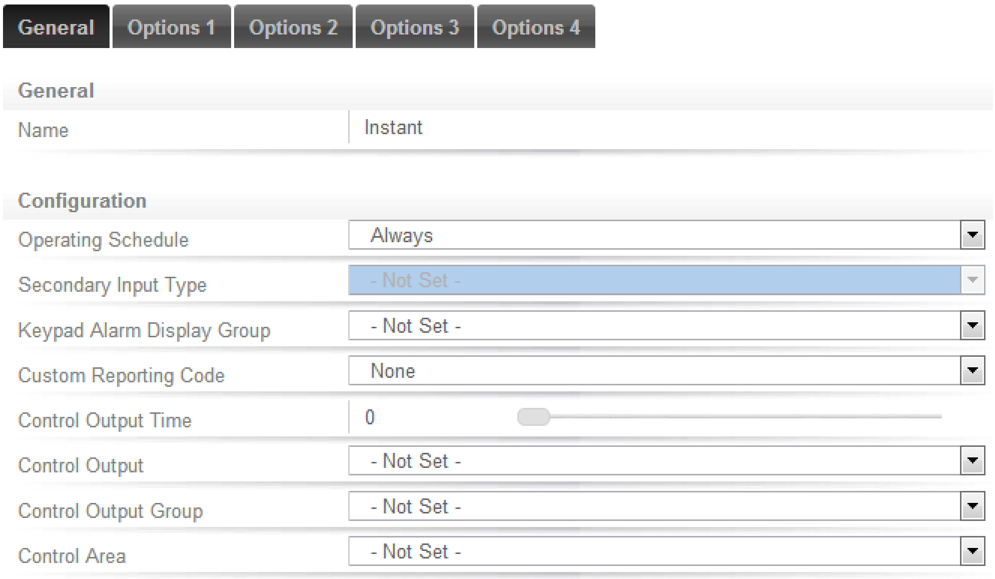
□ Door REX Not Allowed

□ Door REN Not Allowed

- **Door REX Not Allowed:** When enabled the door will disable the REX (request to exit) operation.
- **Door REN Not Allowed:** When enabled the door will disable the REN (request to enter) operation.

Input Types

Input types define how an input will operate in an area.



General

Name	Instant

Configuration

Operating Schedule	Always
Secondary Input Type	- Not Set -
Keypad Alarm Display Group	- Not Set -
Custom Reporting Code	None
Control Output Time	0
Control Output	- Not Set -
Control Output Group	- Not Set -
Control Area	- Not Set -

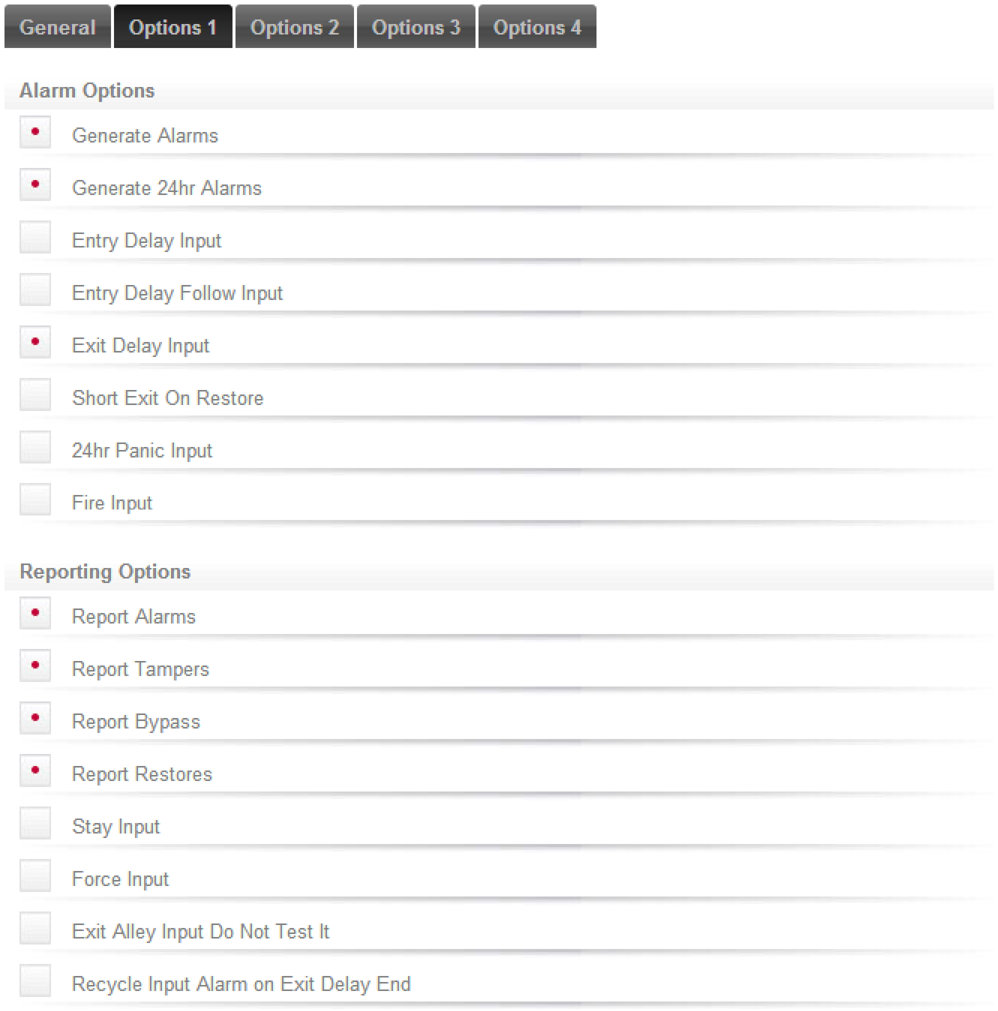
General

- **Name:** The name of the input type.

Configuration

- **Operating Schedule:** Determines when the input type is valid and if it will use a secondary input type when the schedule is not valid.
- **Secondary Input Type:** Allows an input to have a secondary configuration when that Operating Schedule is invalid. This option is only enabled when the Operating Schedule is not set to Always.
- **Keypad Alarm Display Group:** Determines which keypads will be presented with alarm information when the input that the input type is assigned generates an alarm.
- **Custom Reporting Code:** Each input type has a default reporting code already assigned which determines the code that is sent to the central station when an alarm is generated. This option enables you to change the reporting code of the inputs to which this input type is assigned.
- **Control Output Time:** You can override the programmed activation time for an output by setting an activation time in the input type.
- **Control Output / Output Group:** You can assign an output or output group to activate whenever an input type process's an alarm or restore for an input. The input type must have the control output options set in the Output options.
- **Control Area:** An input type can be programmed to control the arming and disarming state of an area from an input (key switch control). The area to be controlled by the input type must be programmed with the force arming option. Arming using an input type is deemed to be an unattended arming condition and therefore the system will attempt to arm the area in the force mode.

Input Types | Options 1



Alarm Options

☑ Generate Alarms

☑ Generate 24hr Alarms

□ Entry Delay Input

□ Entry Delay Follow Input

☑ Exit Delay Input

□ Short Exit On Restore

□ 24hr Panic Input

□ Fire Input

Reporting Options

☑ Report Alarms

☑ Report Tampers

☑ Report Bypass

☑ Report Restores

□ Stay Input

□ Force Input

□ Exit Alley Input Do Not Test It

□ Recycle Input Alarm on Exit Delay End

Alarm Options

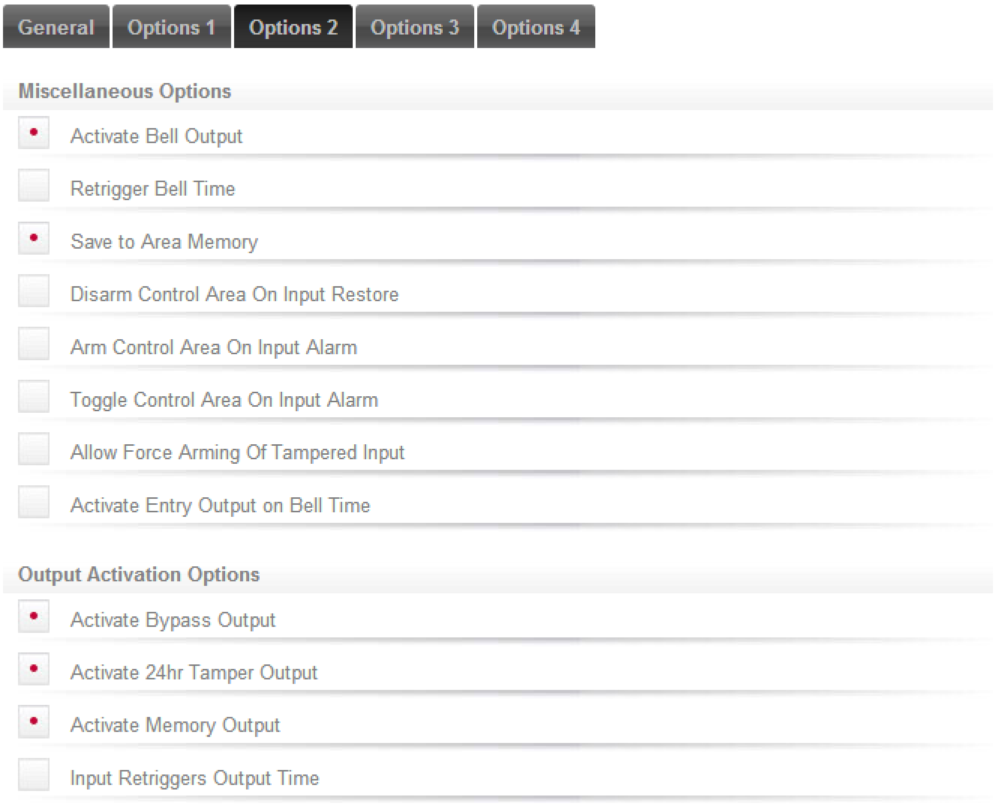
- Generate Alarms: When enabled the input type will process alarms from the input that it is assigned.
- Generate 24HR Alarms: When enabled the input type will process tamper alarms from the input that it is assigned.
- Entry Delay Input: When enabled the input type will start the entry delay timer for the assigned area when the input generates an alarm.
- Entry Delay Follow Input: When enabled the input type will allow this input to generate alarms during the entry delay however it will generate an alarm if the alarm condition occurs outside the entry delay period.
- Exit Delay Input: When enabled the input type will allow this input to generate alarms during the exit delay however it will generate an alarm if the alarm condition occurs outside the exit delay period. Use this feature to prevent 'Sitters' from re-entering a building that is assumed to be secure during a long arming process.
- Short Exit On Restore: When enabled the input type will shorten the exit delay timer on an area to five seconds when the input restores. Use this feature to reduce the arming time of an area.
- 24hr Panic Input: When enabled the input type will generate a 24HR alarm if the input generates an alarm. The area state will not affect the generation of this alarm.
- Fire Input: When enabled the input type will generate a fire alarm when it is activated. This input type will also operate similar to the 24HR Alarm option. Most smoke detectors use a normally open contact so any input that is assigned this option must have the inverted state option selected and the EOL resistors option enabled.

Reporting Options

- Report Alarms: When enabled the input type will generate a reportable alarm message.
- Report Tampers: When enabled the input type will generate a reportable tamper message.

- Report Bypass: When enabled the input type will generate a reportable bypass message.
- Report Restores: When enabled the input type will generate a reportable restore message.
- Stay Input: When enabled the input type will generate an alarm if the area is armed in stay mode. The input will stay armed. For inputs that will be active when an area is armed in stay mode it is recommended to disable the event log for the input.
- Force Input: When enabled the input type will allow the inputs it is assigned to be force armed.
- Exit Alley Input Do Not Test It: When enabled the input type will not verify the status of an input prior to the area starting to arm. Use this feature to assign inputs in exit locations to prevent the area from generating an input open warning when being armed.
- Recycle Input Alarm on Exit Delay End: When enabled the input type will recheck the inputs it is assigned when the area completes the exit delay cycle and if an input is open recycle the input to force it in to generating an alarm. Use this feature for an input type used on an input that may be breached during the exit delay such as a window or door contact.

Input Types | Options 2



Miscellaneous Options

☑ Activate Bell Output

☐ Retrigger Bell Time

☑ Save to Area Memory

☐ Disarm Control Area On Input Restore

☐ Arm Control Area On Input Alarm

☐ Toggle Control Area On Input Alarm

☐ Allow Force Arming Of Tampered Input

☐ Activate Entry Output on Bell Time

Output Activation Options

☑ Activate Bypass Output

☑ Activate 24hr Tamper Output

☑ Activate Memory Output

☐ Input Retriggers Output Time

Miscellaneous Options

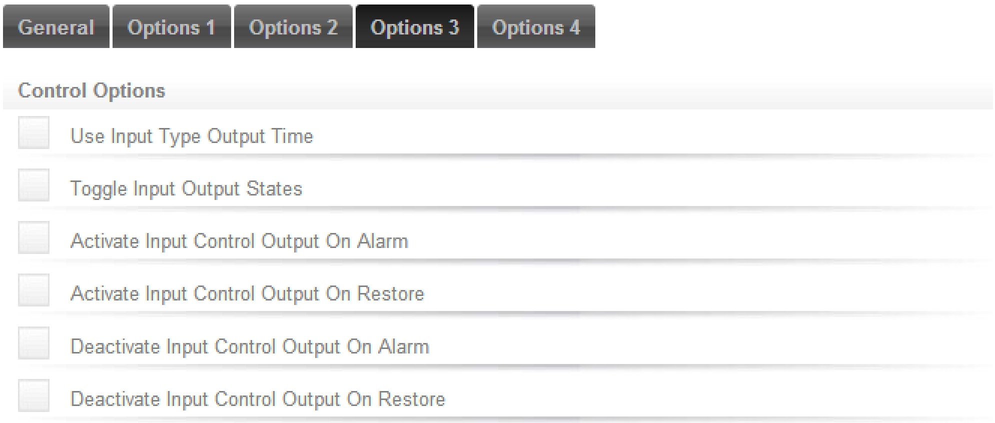
- Activate Bell Output: When enabled the input type will activate the siren bell output programmed for the area.
- Retrigger Bell Time: When enabled the input type will restart the bell timer on each subsequent alarm
- Save To Area Memory: When enabled the input type will save an alarm message to the area's alarm memory storage area.
- Disarm Control Area On Input Restore: When enabled the input type will disarm the control area when an input assigned the input type restores from an alarm condition. Use this feature and the arming control area feature as a on and off key switch arming input.
- Arm Control Area On Input Alarm: When enabled the input type will start arming the control area when an input assigned the input type generates an alarm condition.
- Toggle Control Area On Input Alarm: When enabled the input type will toggle the state of the control area when the input that is assigned this input type generates an alarm.
- Allow Force Arming Of Tampered Input: When enabled the input type will allow the input to be force armed if the input assigned the input type is tampered.

- Activate Entry Output on Bell Time: When enabled the input type will activate the entry output programmed for the area for the duration of the bell siren time. Use this feature for an input that you want to only generate a beeper alarm and assign the entry output a keypad beeper output. This option will not function if the bell option is enabled.

Output Activation Options

- Activate Bypass Output: When enabled the input type will activate bypass output for the area if an input is bypassed.
- Activate 24hr Tamper Output: When enabled the input type will activate the tamper output for the area if a tamper alarm occurs.
- Activate Memory Output: When enabled the input type will activate the memory output for the area if an alarm occurs. This option can be used to indicate that an alarm has occurred in the system. Use this feature to display an indication to the users of the system to prevent possible "Sitter and Hostage" situations.
- Input Retriggers Output Time: When enabled, reinitiates the activation time of an output when the input is triggered, for example reactivating lights when a motion sensor is triggered.

Input Types | Options 3



Control Options

□ Use Input Type Output Time

□ Toggle Input Output States

□ Activate Input Control Output On Alarm

□ Activate Input Control Output On Restore

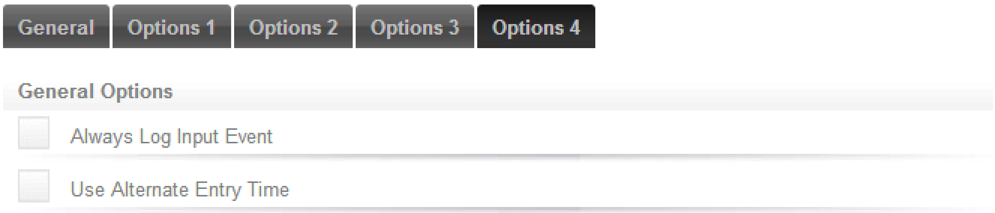
□ Deactivate Input Control Output On Alarm

□ Deactivate Input Control Output On Restore

Control Options

- Use Input Type Output Time: When enabled the input will activate the output timed (if a time is programmed) and use the Output Time Set in the Input Type. If the input type does not have a time programmed no time will be used.
- Toggle Input Output State: When enabled the input control output will be toggled when the input goes in to alarm. You can use this option to activate a output on alarm and deactivate on the next alarm. This is ideal for lighting control and automation applications.
- Activate Input Control Output On Alarm: When enabled the input type will activate the input control output when the input assigned generates an alarm.
- Activate Input Control Output On Restore: When enabled the input type will activate the input control output when the input assigned restores from an alarm.
- Deactivate Input Control Output On Alarm: When enabled the input type will deactivate the input control output when the input assigned generates an alarm.
- Deactivate Input Control Output On Restore: When enabled the input type will deactivate when the input control output assigned restores from an alarm.

Input Types | Options 4



General Options

□ Always Log Input Event

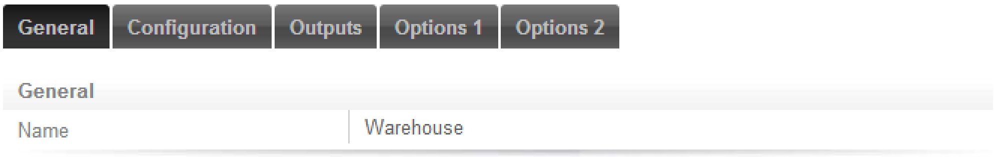
□ Use Alternate Entry Time

- **Always Log Input Event:** When enabled, the input will generate an event whenever it is opened, closed, tampered or shorted.
- **Use Alternate Entry Time:** When enabled the input type will start the alternate entry delay timer for the assigned area when the input generates an alarm.

Areas

Areas allow for the Protege system to be divided up into separate sections (alarm areas or partitions). This allows for areas to be grouped for easy management of multiple areas at a time.

An installation may contain up to 32 areas or partitions depending on the configuration and size of the system needed. Areas can contain inputs and trouble inputs that protect the area. Inputs can be assigned to as many as four areas and perform a different function in each area individually of the other area's status.



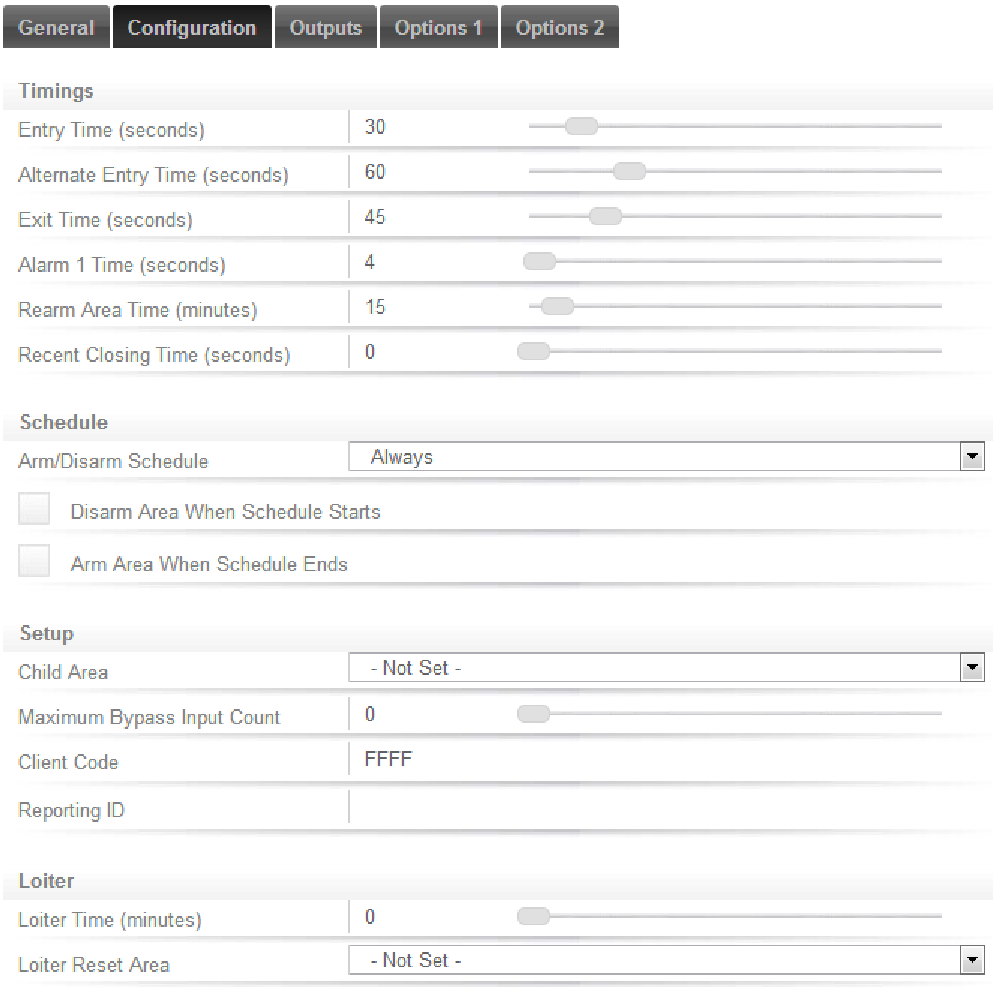
General

Name	Warehouse

General

- **Name:** The name of the area.

Areas | Configuration



Timings

Entry Time (seconds)	30
Alternate Entry Time (seconds)	60
Exit Time (seconds)	45
Alarm 1 Time (seconds)	4
Rearm Area Time (minutes)	15
Recent Closing Time (seconds)	0

Schedule

Arm/Disarm Schedule	Always

□ Disarm Area When Schedule Starts

□ Arm Area When Schedule Ends

Setup

Child Area	- Not Set -
Maximum Bypass Input Count	0
Client Code	FFFF
Reporting ID	

Loiter

Loiter Time (minutes)	0
Loiter Reset Area	- Not Set -

Timings

- Entry Time (seconds): Setting an entry delay time for the area allows users that have entered a secured point to have time to disarm the area before the area generates an alarm. Only inputs that have an input type assigned with an entry delay option set will start the entry delay timer for the area.
- Alternate Entry Time (seconds): Defines the entry delay time when using an alternate entry to the area. For example, if an area can be accessed through a secondary entry point such as a garage door, you can allow users more (or less) time to disarm the area before an alarm is generated.
- Exit Time (seconds): Setting an exit delay time for the area allows users to exit the area once the arming of the area has begun without triggering an alarm. Inputs that are part of the exit route should be programmed with the exit option in the assigned input type.
- Alarm 1 Time (minutes): The bell time determines how long the bell/siren output for the area will remain activated before timing out. If the option to retrigger the bell time is set in the input type assigned to an input that is triggered in the area the siren bell time is reloaded on each subsequent alarm activation. Use the siren bell time and the retrigger bell option from the input type for smart automation of lighting and building control.
- Rearm Area Time (minutes): Setting the rearm delay will result in the area automatically re-arming after the re-arm timer has elapsed. This should be programmed for area's used to monitor and control system functions that should not be disarmed. This is also used to control vault and automatic teller machines when using the banking area functions to prevent an area from being disarmed for longer than the time programmed.
- Recent Closing Time (seconds): The recent closing time defines how long the system considers an armed area recently closed. If, after arming the area, an alarm is generated within the programmed period, the Protege System Controller transmits a recent closed message. For this feature to operate correctly the input must have its report options enabled in the assigned input type.

Schedule

- Arm/Disarm Schedule: Defines a schedule that enables the area to be armed and disarmed automatically.
- Disarm Area When Schedule Starts: When enabled, the area will automatically disarm when the Arm/Disarm Schedule assigned above starts.
- Arm Area When Schedule Ends: When enabled, the area will automatically arm when the Arm/Disarm Schedule assigned above ends.

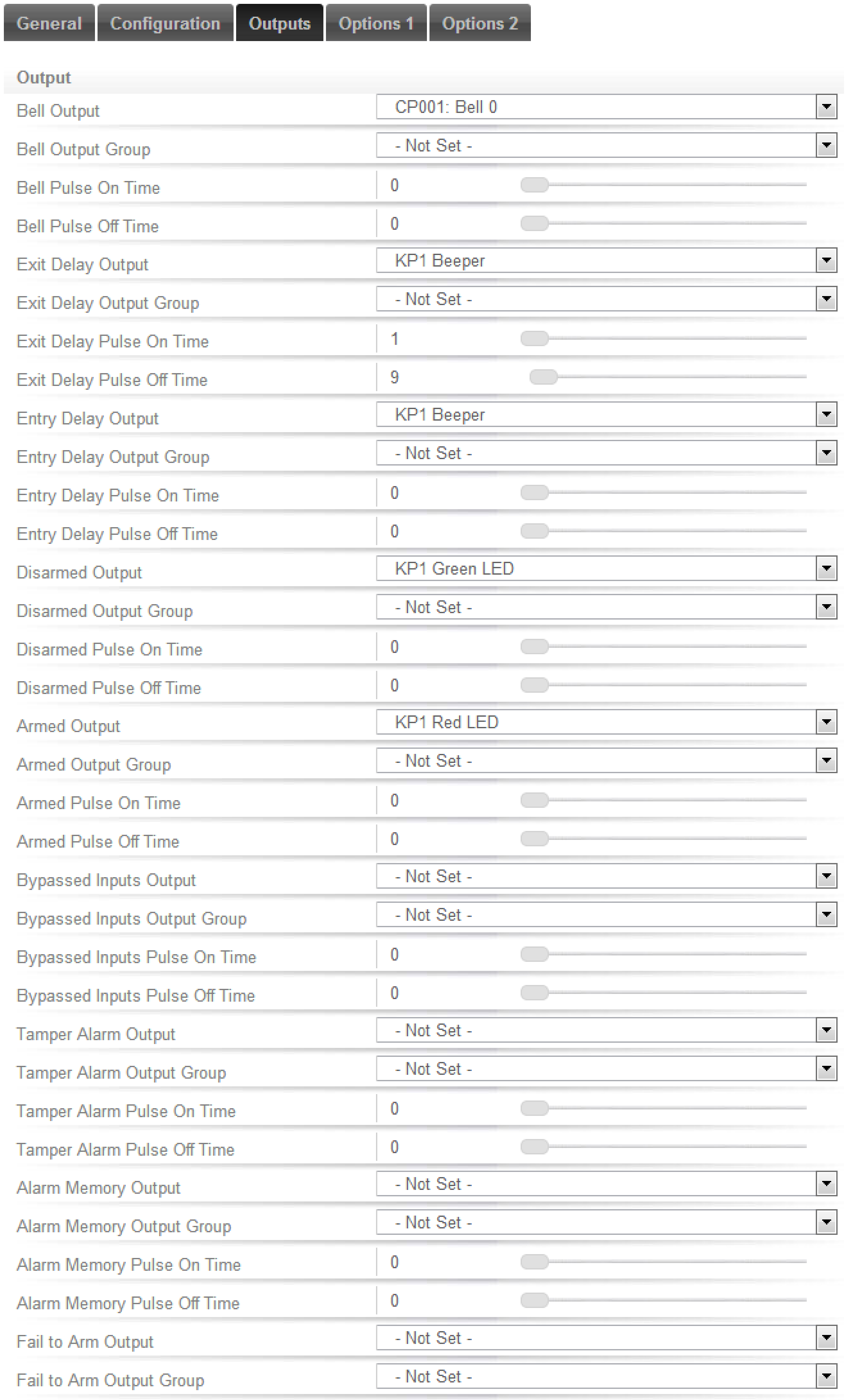
Setup

- Child Area: The child area is an area dependent on another area (the parent area). For example, if an area is armed, then its child area can also be automatically armed. If you select "None", the area will not have a child area assigned. You can use this option to program a common area as there is no limit to the number of areas containing the same child area. A common area is an area that is the child area of more than one parent area. The common area can only be armed once all of its parent areas are armed.
- Maximum Bypass Input Count: The bypass count number sets the maximum number of inputs that can be bypassed within the programmed area.
- Client Code: The client code for the area is the code that will be used to report alarms to the monitoring station. If the client code is left at the default value of FFFF then the client code that will be used is the client code assigned in the service that is being used to report the alarms.
- Reporting ID: The code by which this area will be reported to a monitoring station. Both ContactID and ReportIP use this code.

Loiter

- Loiter Timer (minutes): The loiter time defines how long a user can remain in a specific loiter enabled area. If the loiter time has elapsed and the user is still in the area, the user will be denied access when an attempt is made to exit the area. If the user has not exited the loiter area before the loiter time has elapsed, then the user status must be reset manually from the interface or local keypad. For this option to operate, the Loiter Mode options must be turned on for the user and a loiter area must be programmed. Furthermore, the area requires an entry and exit reader set with the anti-passback feature to control the user traffic.
- Loiter Reset Area: The loiter area violation setting is used when a user has violated the loiter configuration for the installation and must be set to an area that they cannot exit or enter from. The setting here is typically an area that is not used in the system and is defined as being an invalid area.

Areas | Outputs



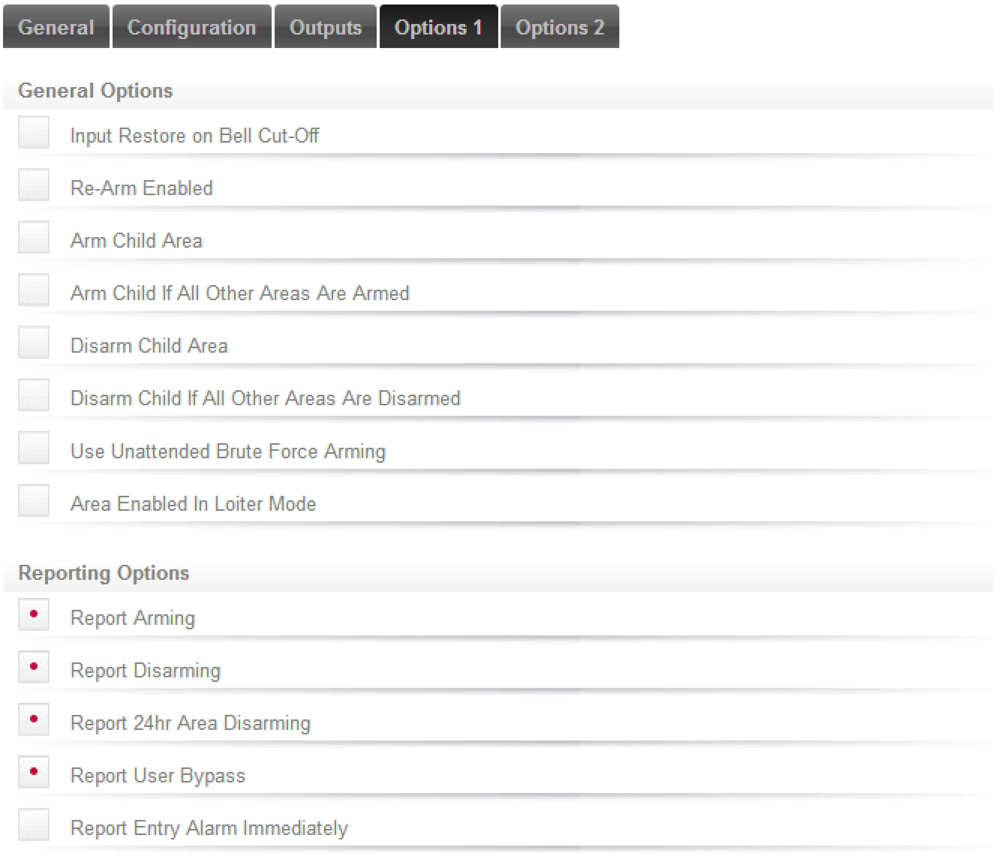
Output

Bell Output	CP001: Bell 0
Bell Output Group	- Not Set -
Bell Pulse On Time	0
Bell Pulse Off Time	0
Exit Delay Output	KP1 Beeper
Exit Delay Output Group	- Not Set -
Exit Delay Pulse On Time	1
Exit Delay Pulse Off Time	9
Entry Delay Output	KP1 Beeper
Entry Delay Output Group	- Not Set -
Entry Delay Pulse On Time	0
Entry Delay Pulse Off Time	0
Disarmed Output	KP1 Green LED
Disarmed Output Group	- Not Set -
Disarmed Pulse On Time	0
Disarmed Pulse Off Time	0
Armed Output	KP1 Red LED
Armed Output Group	- Not Set -
Armed Pulse On Time	0
Armed Pulse Off Time	0
Bypassed Inputs Output	- Not Set -
Bypassed Inputs Output Group	- Not Set -
Bypassed Inputs Pulse On Time	0
Bypassed Inputs Pulse Off Time	0
Tamper Alarm Output	- Not Set -
Tamper Alarm Output Group	- Not Set -
Tamper Alarm Pulse On Time	0
Tamper Alarm Pulse Off Time	0
Alarm Memory Output	- Not Set -
Alarm Memory Output Group	- Not Set -
Alarm Memory Pulse On Time	0
Alarm Memory Pulse Off Time	0
Fail to Arm Output	- Not Set -
Fail to Arm Output Group	- Not Set -

- Bell Output/Output Group: You can assign a bell/siren output or output group to activate whenever the area goes in to alarm. The input that triggers the alarm must have the bell output option enabled for the input type. The bell/siren output and output Group will be deactivated when the bell timer times out or when the area is disarmed, the bell/siren may also be disarmed when the user logs in to the keypad.
  - Bell Pulse On Time: The bell/siren pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
  - Bell Pulse Off Time: The bell/siren pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.
- Exit Delay Output/Output Group: You can assign an exit delay output or output group to activate whenever the area starts an exit delay cycle. The exit delay output or output group will be deactivated when the area completes the arming cycle or if an alarm occurs during the exit delay period. Disarming the area will also result in the exit delay output or output group being deactivated.
  - Exit Delay Pulse On Time: The exit delay output pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
  - Exit Delay Pulse Off Time: The exit delay output pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.
- Entry Delay Output/Output Group: You can assign a entry delay output or output group to activate whenever the area starts an entry delay cycle. The entry delay output or output group will be deactivated when the area is disarmed during the entry delay period or the area activates the alarm due to the entry delay timing out.
  - Entry Delay Pulse On Time: The entry delay output pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
  - Entry Delay Pulse Off Time: The entry delay output pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.
- Disarmed Output/Output Group: You can assign a output or output group to activate whenever the area completes the disarming cycle. The disarmed output or output group will be deactivated when the area completes the arming cycle. Use this to drive local indicators on keypads, card readers and relays for signalling that the system is disarmed and can be entered. This can also be used for interlocking non reader controlled doors to prevent entry to areas if the area is armed. Use this output in conjunction with user area's to control multiple storage lockers or storage facilities.
  - Disarmed Pulse On Time: The disarmed output pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
  - Disarmed Pulse Off Time: The disarmed output pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.
- Armed Output/Output Group: You can assign a output or output group to activate whenever the area completes the arming cycle. The armed output or output group will be deactivated when the area completes the disarming cycle. Use this to drive local indicators on keypads, card readers and relays for signalling that the system is armed.

  - Armed Pulse On Time: The armed output pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
  - Armed Pulse Off Time: The armed output pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.
- Bypassed Inputs Output/Output Group: You can assign a output or output group to activate whenever the area has a bypassed input. The bypass output or output group will be deactivated when the area completes the disarming cycle.
  - Bypassed Inputs Pulse On Time: The bypass output pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
  - Bypassed Inputs Pulse Off Time: The bypass output pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.
- Tamper Alarm Output/Output Group: You can assign an output or output group to activate whenever the area has a tamper alarm. The tamper output or output group will be deactivated when the area completes the disarming cycle on the 24HR portion of the area.
  - Tamper Alarm Pulse On Time: The tamper output pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
  - Tamper Alarm Pulse Off Time: The tamper output pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.
- Alarm Memory Output/Output Group: You can assign an output or output group to activate whenever the area has an alarm and the output or output group will remain activated. The memory output or output group will be deactivated when the area completes the disarming cycle. Use this to drive local indicators on keypads, card readers and relays for signaling that the system has had an alarm activation.
  - Alarm Memory Pulse On Time: The memory output pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
  - Alarm Memory Pulse Off Time: The memory output pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.
- Area Defer Arming Started Output: You can assign a output or output group to activate whenever the area begins the defer warning cycle and is about to arm. The defer warning time is programmed in the defer time setting. The defer output or output group will be deactivated when the area begins the arming cycle or when the defer time is canceled by a user.
  - Defer Arming Started Pulse On Time: The defer output pulse on time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit on for 1 second and then off for the programmed time set in the pulse off section.
  - Defer Arming Started Pulse Off Time: The defer output pulse off time is used to make the output pulse on and off when activated. The value entered here must be greater than 0 and is in increments of 100ms. For example setting 10 will pulse the unit off for 1 second and then on for the programmed time set in the pulse on section.
- Fail to Arm Output/Output Group: You can assign an output or output group to activate whenever the area fails to arm.

Areas | Options 1



General Options

☐ Input Restore on Bell Cut-Off

☐ Re-Arm Enabled

☐ Arm Child Area

☐ Arm Child If All Other Areas Are Armed

☐ Disarm Child Area

☐ Disarm Child If All Other Areas Are Disarmed

☐ Use Unattended Brute Force Arming

☐ Area Enabled In Loiter Mode

Reporting Options

☑ Report Arming

☑ Report Disarming

☑ Report 24hr Area Disarming

☑ Report User Bypass

☐ Report Entry Alarm Immediately

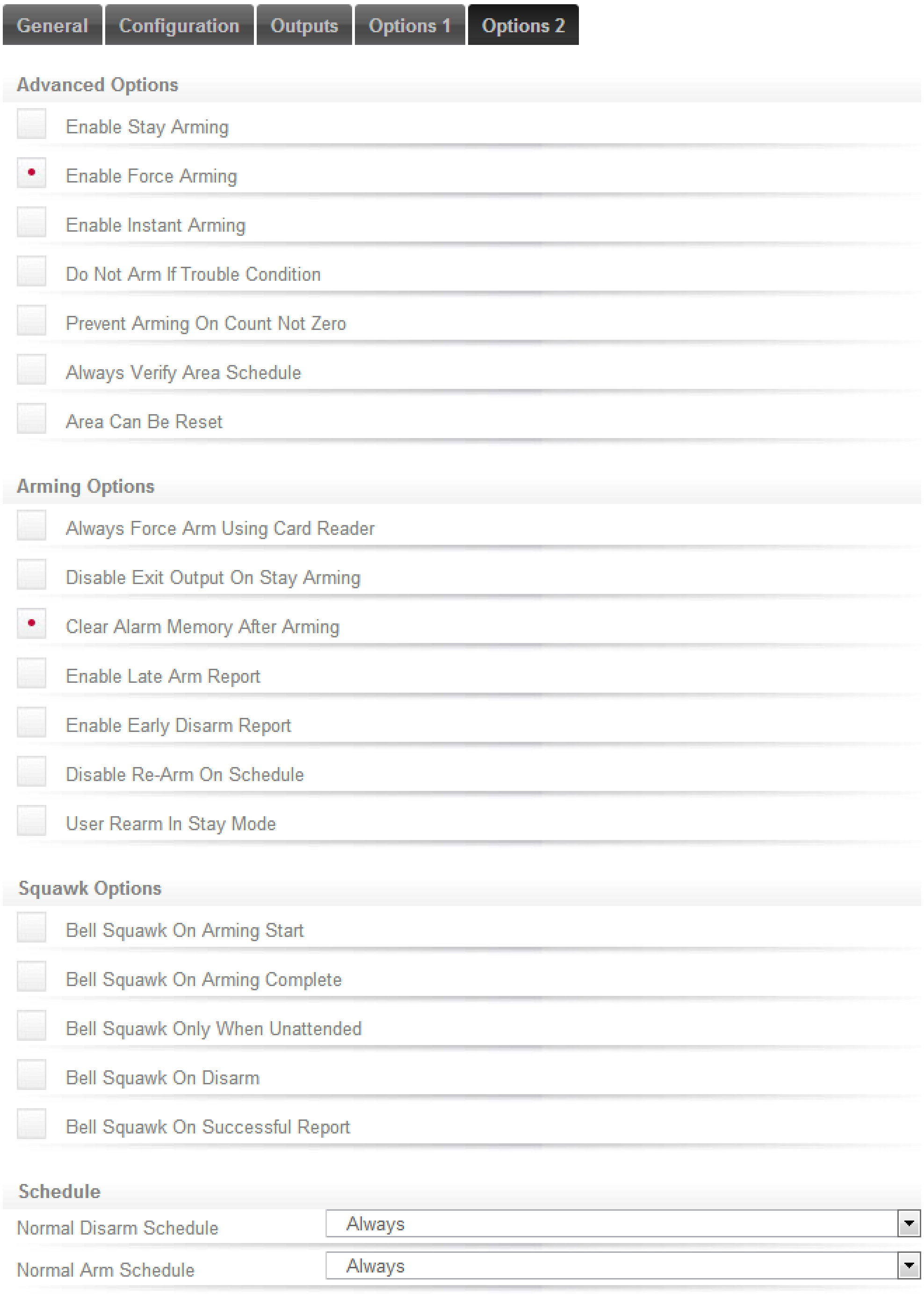
General Options

- Input Restore on Bell Cut-Off: When enabled the inputs that are assigned to this area will restore when the bell time completes. This does not prevent the input from generating multiple alarms for another area when this setting is specific to the area assigned. The inputs in the area will still log an event regardless of the bell time to prevent an input from triggering an event remove the event log option in the input configuration. Setting this option will prevent the retrigger bell timer from operating in the input type. Do not use this option for an area that is used for automation control or motion controlled lighting.
- Re-Arm Enabled: When enabled the area will re-arm if the area is disarmed. This feature is used for dead man timers and areas that should not remain disarmed for a longer than a predefined time. For this option to operate the re-arm time must be set to a value greater than 0.
- Arm Child Area: When enabled the child area will be armed when the parent (this) area is armed. Can be used in conjunction with the option below.
- Arm Child If All Other Areas Are Armed: When enabled the child area will only be armed if ALL the areas that the child area are assigned are armed. Use this option when multiple areas are assigned the same child area that needs to be controlled with a specific disarming and arming order. This effectively allows an OR and AND operation to be done on the child area.
- Disarm Child Area: When enabled the child area will only be disarmed when the parent (this) area disarms.
- Disarm Child If All Other Areas Are Disarmed: When enabled the child area will only be disarmed if ALL the areas that the child area are assigned are disarmed. Use this option when multiple areas are assigned the same child area that needs to be controlled with a specific disarming and arming order. This effectively allows an OR and AND operation to be done on the child area.
- Use Unattended Brute Force Arming: When enabled the area will be prevented from arming if an input that is not a force enabled input is open when the area is armed in an unattended mode.
- Area Enabled In Loiter Mode: When enabled the area will control the users that access the area for a period of time assigned to the loiter control time. If a user breaches the allocated time the user will be set to the area programmed in the loiter area setting.

Reporting Options

- Report Arming: When enabled the area will generate a reportable event that can be directed to a monitoring station.
- Report Disarming: When enabled the area will generate a reportable event that can be sent to a monitoring station.
- Report 24HR Area Disarming: When enabled the area will report both an opening (Disabled) or closing (Enabling) of the 24HR section of this area.
- Report User Bypass: When enabled the area will report all inputs that are bypassed once it completes the arming process.
- Report Entry Alarm Immediately: When enabled the area will report the activation of an entry input immediately event though the alarm may be in an entry delay operation.

Areas | Options 2



Advanced Options

☐ Enable Stay Arming
☑ Enable Force Arming
☐ Enable Instant Arming
☐ Do Not Arm If Trouble Condition
☐ Prevent Arming On Count Not Zero
☐ Always Verify Area Schedule
☐ Area Can Be Reset

Arming Options

☐ Always Force Arm Using Card Reader
☐ Disable Exit Output On Stay Arming
☑ Clear Alarm Memory After Arming
☐ Enable Late Arm Report
☐ Enable Early Disarm Report
☐ Disable Re-Arm On Schedule
☐ User Rearm In Stay Mode

Squawk Options

☐ Bell Squawk On Arming Start
☐ Bell Squawk On Arming Complete
☐ Bell Squawk Only When Unattended
☐ Bell Squawk On Disarm
☐ Bell Squawk On Successful Report

Schedule

Normal Disarm Schedule: Always
Normal Arm Schedule: Always

Advanced Options

- Enable Stay Arming: When enabled the area can be stay armed.
- Enable Force Arming: When enabled the area can be force armed.
- Enable Instant Arming: When enabled the area can be instant armed.
- Do Not Arm if Trouble Condition: When enabled the area will be prevented from arming if a trouble condition is present in the system.
- Prevent Arming On Count Not Zero: When enabled the area will be prevented from arming if the count value for the area is greater than 0.
- Always Verify Area Schedule: When enabled the area will verify that the programmed schedule has not changed or the area has not been disarmed when it should have been armed. This will occur every one minute period.
- Area can be Reset: When enabled, allows the area to armed while it is already armed. This means that an area that goes into alarm can be reset to the armed state, turning sirens and such off, without having to be disarmed first. Use this option for areas that should never be disarmed.

Arming Options

- Always Force Arm Using Card Reader: When enabled the area will force arm the area when the arming process is started by a card reader.
- Disable Exit Output on Stay Arming: When enabled the area will not activate the Exit Output when the area is stay armed.
- Clear Alarm Memory after Arming: When enabled the area clear all alarm memory when the area is armed.
- Enable Late Arm Report: When enabled the area will generate Early to Arm and Late to Arm reportable events according to the normal operating schedule (see above).
- Enable Early Disarm Report: When enabled the area will generate Early to Disarm and Late to Disarm reportable events according to the normal operating schedule (see above).
- Disable Rearm on Schedule: When enabled the area will rearm as per the associated schedule.
- User Rearm in Stay Mode: When enabled, a user that has the Rearm Area in Stay Mode option enabled disarms the Area, the area will automatically rearm in Stay mode. Prior to rearming, the area will remain disarmed for the length of time specified by the Rearm Area time setting.

Squawk Options

- Bell Squawk on Arming Start: When enabled the area will squawk the Bell Output when the arming process starts.
- Bell Squawk on Arming Complete: When enabled the area will squawk the Bell Output when the arming process is complete and the exit delay has ended.
- Bell Squawk Only When Unattended: When enabled the area will only squawk the Bell Output when the area is armed by an unattended arming, e.g. Card Reader, Remote Service, Key Switch, Door, another Area etc.
- Bell Squawk on Disarm: When enabled the area will squawk the Bell Output when the area is disarmed.
- Bell Squawk on Successful Report: When enabled the area will squawk the Bell Output when the a successful Area Armed report has been sent and acknowledge by a reporting service.

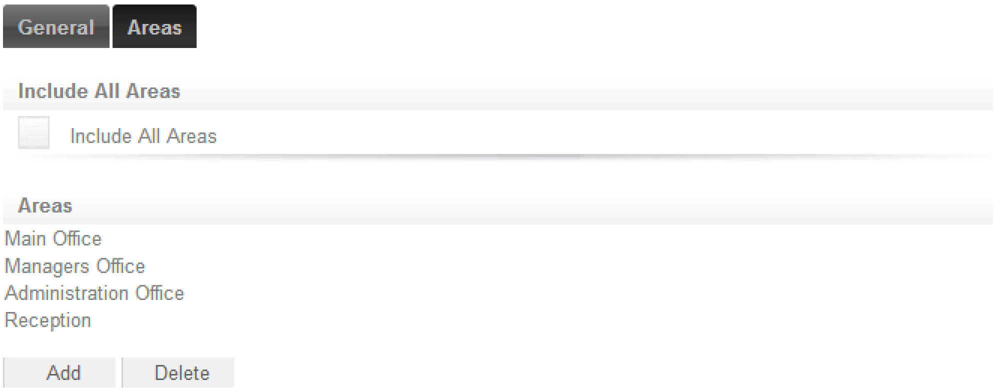
Schedule

- Normal Disarm Schedule: Period 1 of the schedule defines the time period when the area can be disarmed. If the area is disarmed before the start of Period 1 an Early to Disarm event will be generated. If the area is still armed when Period 1 ends the System will generate a Late to Disarm event. No event is generated if the area is disarmed while Period 1 of the schedule is valid.
- Normal Arm Schedule: Period 2 defines the time period when the area can be armed. If the area is armed before the start of Period 2 an Early to Arm event will be generated. If the area is still disarmed when Period 2 ends the System will generate a Late to Arm event. No event is generated if the area is armed while Period 2 of the schedule is valid.

Area Groups

Area groups are assigned to an access level and are used to control the areas that a user can arm and disarm. An area group can be assigned for arming and disarming. Areas assigned in the disarm area group can also be armed by the user.

Select the **Areas** tab to add areas to the group.



Include All Areas

□ Include All Areas

Areas

Main Office
Managers Office
Administration Office
Reception

Include All Areas

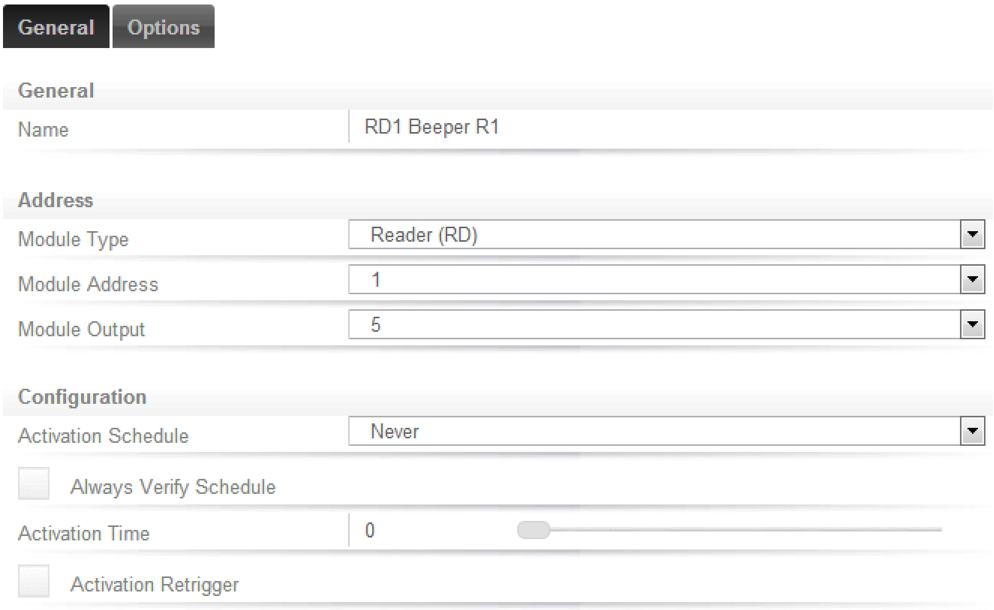
- **Include All Areas**: Select this option to include ALL areas in the group.

Areas

- The areas that belong to the area group. Select areas by clicking **Add** and dragging them to the window from the list that is displayed.

Outputs

Outputs are used to control devices from the Protege System. An output can be used to activate lighting, activate a siren, turn on an indicator or unlock a door.



General

Name	RD1 Beeper R1

Address

Module Type	Reader (RD)
Module Address	1
Module Output	5

Configuration

Activation Schedule	Never

□ Always Verify Schedule

Activation Time	0

□ Activation Retrigger

General

- **Name**: The name of the output.

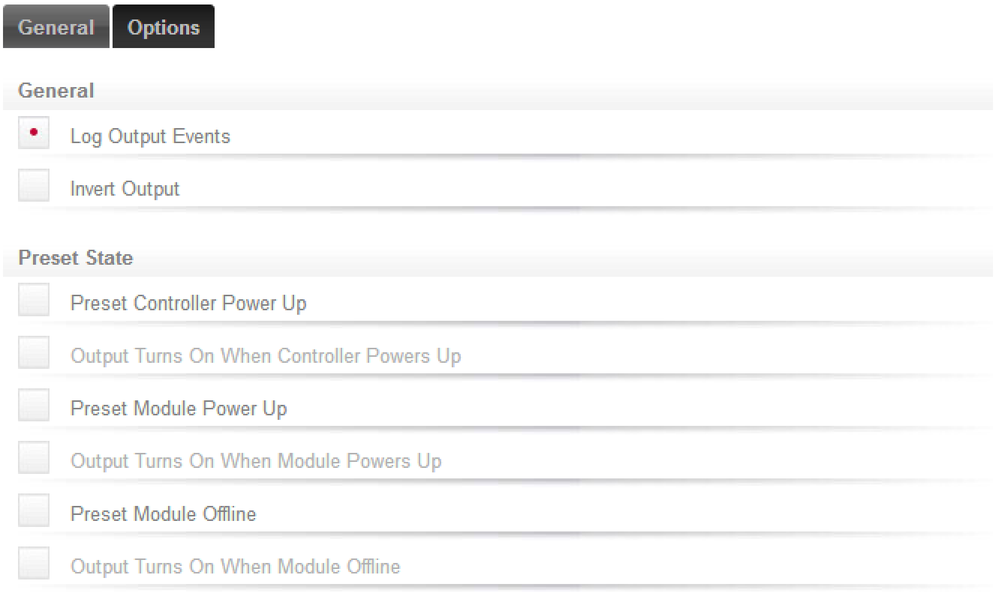
Address:

- **Module Type:** The type of module that the output is attached to.
- **Module Address:** The address of the module that the output is attached to.
- **Module Output**: The index of the specified output on that module.

Configuration:

- **Activation Schedule:** The activation schedule is programmed to activate the output at a certain time of the day or to activate the output between certain hours. The schedule will be checked at the start and end times and if the start is valid the output will be activated, if the end time of the schedule is valid the output will be deactivated. If an output is controlled by an operator, user or other function during this activation time and is deactivated it will remain in the deactivated state. Setting the recheck schedule option for the output will force the output to have the schedule verified every 60 second period. This will prevent the output from being controlled manually as the schedule will override the manual operation.
- **Always Verify Schedule:** When enabled the output will re-verify the schedule that is programmed every 60 seconds. If the output is meant to be activated but is in a deactivated state the system will activate the output.
- **Activation Time:** Setting an activation time for an output will mean that any device controlling the output will only activate the output for the programmed time.
- **Activation Retrigger**: When enabled, if an output receives a command to activate for a defined period, and during that time it receives a second command to activate, this option retriggers the output for the second period. If this option is disabled, the second command is ignored.

Outputs | Options



General

☑ Log Output Events

□ Invert Output

Preset State

□ Preset Controller Power Up

□ Output Turns On When Controller Powers Up

□ Preset Module Power Up

□ Output Turns On When Module Powers Up

□ Preset Module Offline

□ Output Turns On When Module Offline

General

- **Log Output Events:** When enabled the output will generate an event whenever it is activate or deactivated. The output will still perform all functions that are programmed if this is not enabled. When using output's as automation control outputs it is recommended to disable the event logging option to reduce the impact on the event log buffer.
- **Invert Output:** When enabled the output will operate inverted. Deactivation will result in the output being activated and activation will result in the output being deactivated.

Preset State

- **Preset Controller Power Up:** When enabled, the state of the output will be set when the controller is reset or powered up for the first time.
- **Output Turns On When Controller Powers Up:** Defines the state of the state of the output when the Preset Controller Power Up option is enabled. If enabled, the output will be activated. If disabled, the output

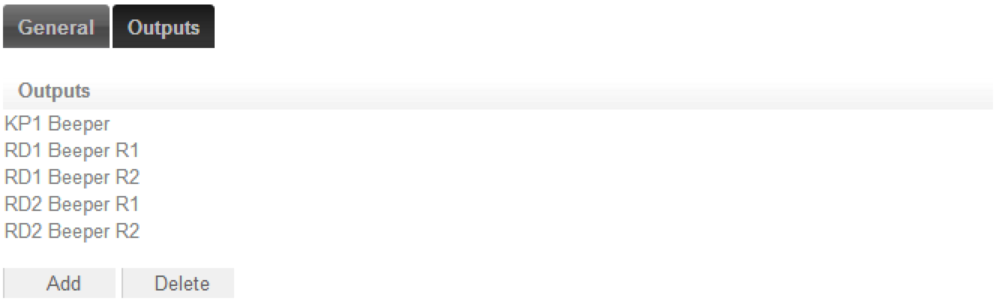
will be deactivated.

- Preset Module Power Up: When enabled, the state of the output will be set when the module powers up and will override the current state that is held in the controller.
- Output Turns On When Module Powers Up: Defines the state of the state of the output when the Preset Module Power Up option is enabled. If enabled, the output will be activated. If disabled, the output will be deactivated.
- Preset Module Offline: When enabled, the state of the output will be set when the module goes offline.
- Output Turns on When Module Offline: Defines the state of the state of the output when the Preset Module Offline option is enabled. If enabled, the output will be activated. If disabled, the output will be deactivated.

Output Groups

Output groups are used to group a number of outputs together and are assigned to an access level and are used to control the outputs that a user can activate and deactivate.

Select the **Outputs** tab to add outputs to the group.



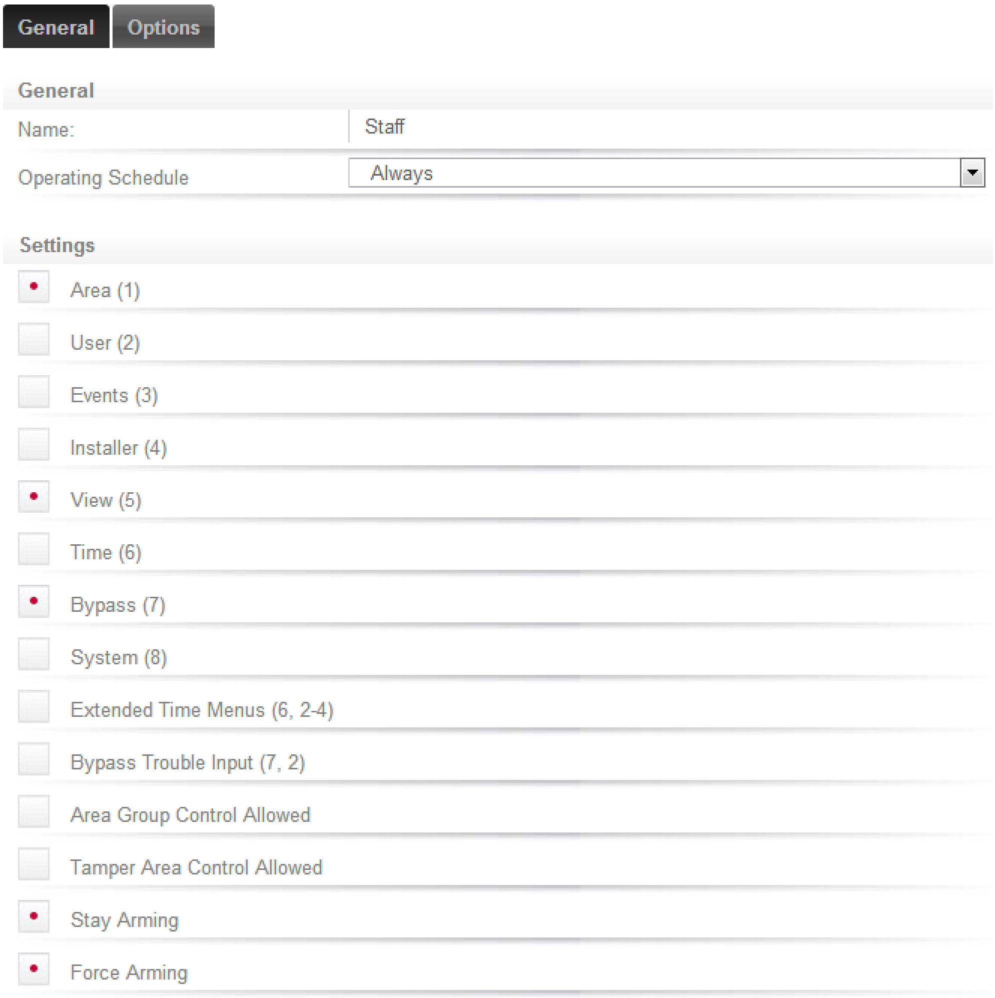
Outputs
KP1 Beeper
RD1 Beeper R1
RD1 Beeper R2
RD2 Beeper R1
RD2 Beeper R2

Outputs

- The outputs that belong to the output group.

Menu Groups

Menu groups provide a way of grouping together the various keypad menus that are programmed in the system. Menu groups can be assigned to an access level, determining which keypad functions those users have access to.



General

Name:	Staff
Operating Schedule	Always

Settings

- ☑ Area (1)
- □ User (2)
- □ Events (3)
- □ Installer (4)
- ☑ View (5)
- □ Time (6)
- ☑ Bypass (7)
- □ System (8)
- □ Extended Time Menus (6, 2-4)
- □ Bypass Trouble Input (7, 2)
- □ Area Group Control Allowed
- □ Tamper Area Control Allowed
- ☑ Stay Arming
- ☑ Force Arming

General

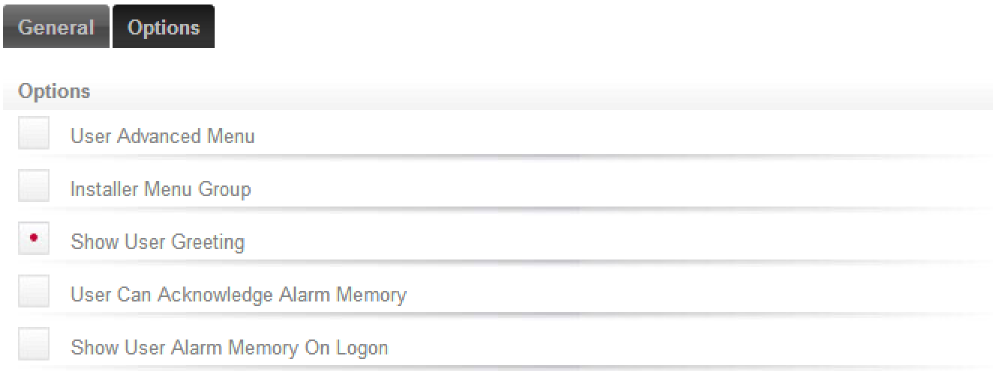
- Name: The name of the menu group.
- Operating Schedule: The operating schedule for the menu group determines when the menu group is valid and if it will use a secondary menu group if the schedule is not valid.

Settings

- Area (1): When enabled, the menu group will allow the user to access the Area menu.
- User (2): When enabled, the menu group will allow the user to access the User menu.
- Events (3): When enabled, the menu group will allow the user to access the Events menu.
- Installer (4): When enabled, the menu group will allow the user to access the Installer menu.
- View (5): When enabled, the menu group will allow the user to access the View menu.
- Time (6): When enabled, the menu group will allow the user to access the Time menu.
- Bypass (7): When enabled, the menu group will allow the user to access the Bypass menu.
- System (8): When enabled, the menu group will allow the user to access the System menu.
- Extended Time Menus (6, 2-4): When enabled, the menu group will allow the user to access the Extended Time menus.
- Bypass Trouble Input (7, 2): When enabled, the menu group will allow the user to access the Bypass Trouble Input menu.

- **Area Group Control Allowed:** When enabled, will allow the user to access the area group control screen from the area status display screen.
- **Tamper Area Control Allowed:** When enabled, will allow the user to access the tamper area control screen.
- **Stay Arming:** When enabled, will allow the user to stay arm an area. The area must also have the stay arming option enabled.
- **Force Arming:** When enabled, will allow the user to force arm an area. The area must also have the force arming option enabled.

Menu Groups | Options



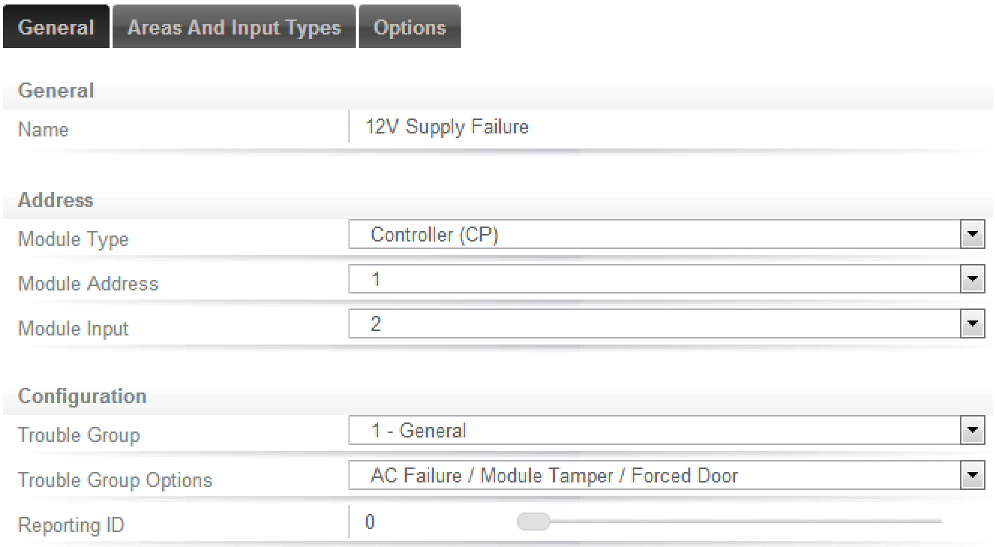
Options

- □ User Advanced Menu
- □ Installer Menu Group
- ☑ Show User Greeting
- □ User Can Acknowledge Alarm Memory
- □ Show User Alarm Memory On Logon

- **User Advanced Menu:** When enabled, the current menu group will be acknowledged as a user advanced menu.
- **Installer Menu Group:** When enabled, the current menu group will be acknowledged as an installer menu group.
- **Show User Greeting:** When enabled, the menu group will display the time of day greeting to the user once they have entered their user code.
- **User Can Acknowledge Alarm Memory:** When enabled, the user will be able to acknowledge alarm memory that is displayed when they first login.
- **Show User Alarm Memory On Logon:** When enabled, the user will be shown any alarms that are in the memory when they log in to the keypad.

Trouble Inputs

Trouble inputs operate similar to regular inputs however they are used to monitor the status and condition of the system. For example, if the enclosure door on the main control device is opened it will open the Enclosure Tamper trouble input.



General	
Name	12V Supply Failure
Address	
Module Type	Controller (CP)
Module Address	1
Module Input	2
Configuration	
Trouble Group	1 - General
Trouble Group Options	AC Failure / Module Tamper / Forced Door
Reporting ID	0

General

- Name: The name of the trouble input.

Address

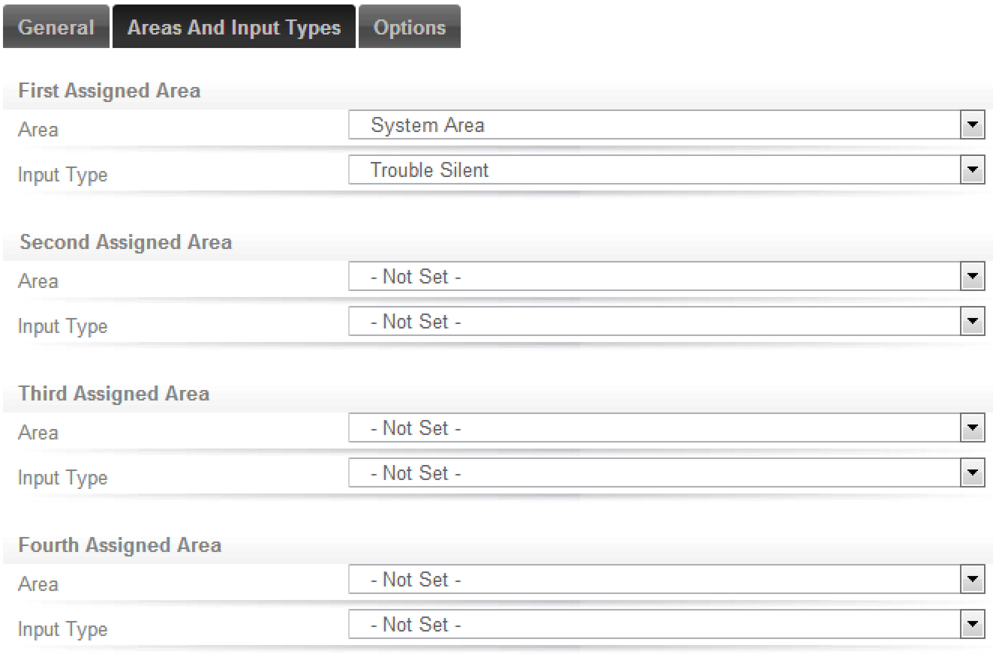
- Module Type: The type of module that the input is attached to.
- Module Address Input: The address of the module that the trouble input is attached to.
- Module Input: The index of the specified input on that module.

Configuration

- Trouble Group: The high level of flexibility that is provided with the Protege System allows the definition of the trouble type and group that is generated by a trouble input. Troubles are grouped by a trouble group and then a trouble type within the group. When the trouble input generates an alarm it will also generate the appropriate trouble condition that is configured. The trouble group and type are used to generate trouble conditions on the keypad and to prevent an area from Arming based on the trouble condition.
  - 1- General: The General Trouble group consists of the trouble types that are part of the main system operation. Trouble conditions such as AC Failure, Real Time Clock and Bell Output Troubles belong to this group and are assigned the General Trouble Group and the appropriate trouble type from the group by default.
  - 2- System: The System Trouble group is used for module related system messages, hardware faults and other system conditions that do not belong in the general trouble group.
  - 3 - Access: The Access Control trouble group consists of the trouble conditions that are related to access control and door operation these include door forced open, door left open and number of attempts are some of the trouble types.
- Trouble Group Options: When a trouble input is assigned to a trouble group it can then have a trouble type within the group assigned. The trouble input types belong to the trouble groups, selecting a trouble group will allow the appropriate trouble type from that group to be selected. The following trouble types are shown for each of the three groups below.
  - AC Failure: AC Failure has occurred on one or more devices in the system.
  - Module Tamper: A module in the system has been tampered.
  - Forced Door: A door in the system has been forced open or opened without being accessed correctly.
  - Battery: A Low Battery or Missing Battery on one or more devices in the system.
  - Module Loss: A module has failed to communicate with the system controller.
  - Door Left Open: A door has been left open past the left open time.
  - Clock Loss: The Real Time Clock has not been set since the System Controller has powered up. To reset the associated trouble set the time from the time menu.
  - Module Security: A module has attempted to register with the system controller however the system controller is secured.
  - Number Attempts: The number of attempts to gain entry in to a door or keypad devices has been exceeded. The next valid access will reset this trouble condition.
  - Reporting: The System Controller has failed to get a report through to the monitoring station in the programmed number of attempts. This will restore when the next reporting event is successful.
  - Hardware Fault: The system controller cannot communicate with an accessory interface board or a device that is connected to the system controller has a hardware failure.
  - User Denied: A user has been denied entry to a keypad or door.
  - Phone Line: The phone line is either cut or damaged on the system controller.
  - Unknown Card: An unknown card has been received by the system on a card reader input.
  - Zone (Input) Fault: An input in the system is tampered or short circuited.
  - Fire Loop: A fire input has a loop fault.
  - Power: A power problem (auxiliary, fuse or analog) has occurred on the Controller or a device in the system.
  - Bell: The Bell/Output on the system controller or a device in the system has either been disconnected or it has shut down due to excessive current consumption.

- Reporting ID: The Trouble Input Reporting ID allows the installer to program any reporting number to any trouble input. This provides an extremely high level of flexibility to assign true reporting numbers to the trouble inputs. A trouble input that is assigned the same reporting ID as another trouble input will result in both the trouble inputs reporting that ID. If a trouble input is assigned an ID number that is higher than the maximum number that can be reported by a particular service, the service will use the maximum number that can be assigned for the format.

Trouble Inputs | Areas and Input Types



First Assigned Area

Area	System Area
Input Type	Trouble Silent

Second Assigned Area

Area	- Not Set -
Input Type	- Not Set -

Third Assigned Area

Area	- Not Set -
Input Type	- Not Set -

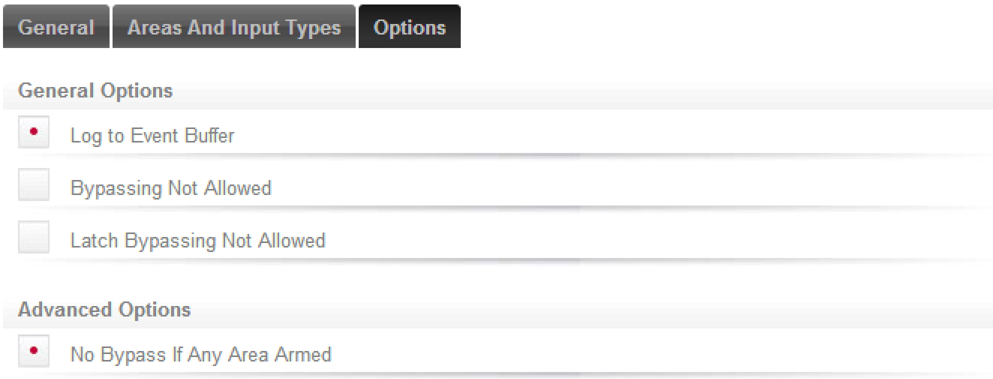
Fourth Assigned Area

Area	- Not Set -
Input Type	- Not Set -

Assigned Areas

- Area: The trouble input must be assigned to an area for it to perform any function in the system. By default ALL trouble inputs are assigned to the predefined trouble area which is the last programmable area in the system. A trouble input can be assigned in up to 4 different areas. A trouble input can perform a different function in each area which is defined by the trouble input type.
- Input Type: When a trouble input is assigned to an area the input must be programmed with the type of trouble input (24 Hour Panic, Burglary Delay, etc).

Trouble Inputs | Options



General Options

☑ Log to Event Buffer

□ Bypassing Not Allowed

□ Latch Bypassing Not Allowed

Advanced Options

☑ No Bypass If Any Area Armed

General Options

- Log to Event Buffer: When enabled, the trouble input will generate an event whenever it is opened or closed.
- Bypassing Not Allowed: When enabled, the trouble input is a high security trouble input and cannot be bypassed.

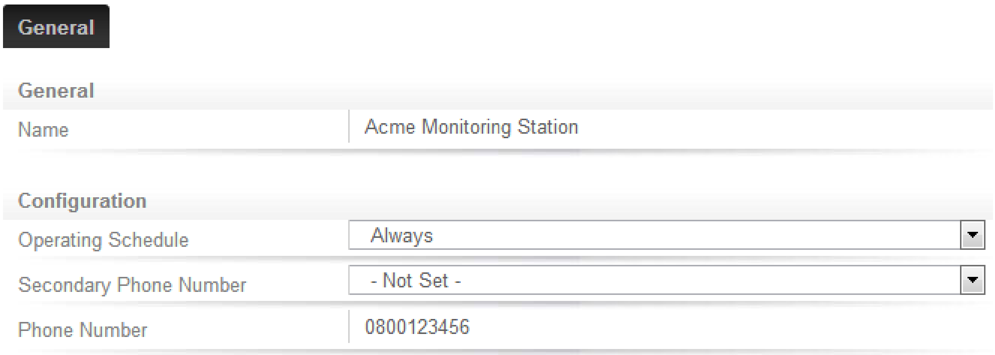
- **Latch Bypassing Not Allowed:** When enabled the trouble input is a high security trouble input and cannot be latch bypassed.

Advanced Options

- **No Bypass If Any Area Armed:** When enabled, the input will be prevented from being bypassed if it is already assigned to an area that has either the 24HR processing enabled or the area is armed.

Phone Numbers

Phone numbers are defined so that a telephone number can be assigned to a Contact ID service that communicates using a modem or telephone connection.



General

Name	Acme Monitoring Station

Configuration

Operating Schedule	Always
Secondary Phone Number	- Not Set -
Phone Number	0800123456

General

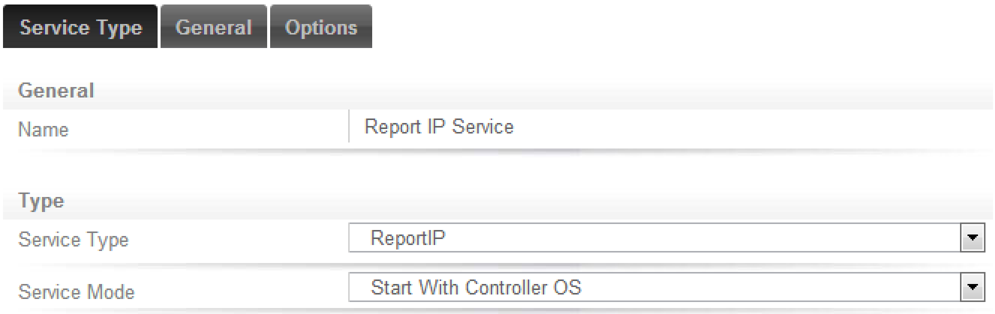
- **Name**: The name of the phone number.

Configuration

- **Operating Schedule:** The operating schedule for the telephone number determines when the telephone number is valid to be dialed and if it will use a secondary telephone if the schedule is not valid. A schedule is a series of times and days that can be programmed to prevent the operation of functions based on a 7 day week and 24 hour clock. For example, the schedule may allow you to report messages during a normal day (8am to 5pm) to one telephone number or monitoring station, and to report them to another location outside of these hours.
- **Secondary Phone Number:** A secondary telephone number when programmed will be used when the schedule of the telephone number that is being programmed is not valid. The schedule of the secondary telephone number must be valid or set to none.
- **Phone Number:** Program the telephone number that you want to assign to this telephone number entry.

Services

Services are used to provide interaction between Protege and external systems.



General

Name	Report IP Service

Type

Service Type	ReportIP
Service Mode	Start With Controller OS

General

- **Name**: The name of the service.

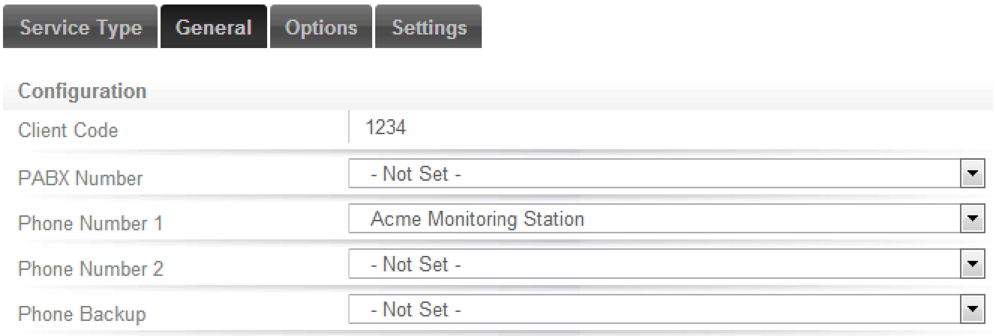
Type

- Service Type: The type of service that is programmed determines the operation that this service performs. This also determines the programming screens that follow in each of the sub sections as the programming of services can contain many features and options dependent on this selection. The following section provides an explanation of each service type. Services require the use of onboard hardware devices or expansion devices.
  - Contact ID: Sends alarms, tests and events using the Contact ID reporting format to a monitoring station capable of receiving the Contact ID format. This service will share the modem with the SIA, Monitor Phone and ModBUS remote services if they are running.
  - Report IP: Allows the Protege System controller to send alarm and activation information over an IP connected network. The Report IP Service supports multiple formats and allows the connection to third party reporting if required.
- Service Mode: The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to Start With The Operating System (Start With O/S) allows the service to operate automatically, if the system controller is reset or restarts the service will automatically restart with the operating system. To only start and stop the service manually select the manual option.

Contact ID

The Contact ID Service is used to sends alarms, tests and events using the Contact ID reporting format to a monitoring station capable of receiving the Contact ID format.

Contact ID | General

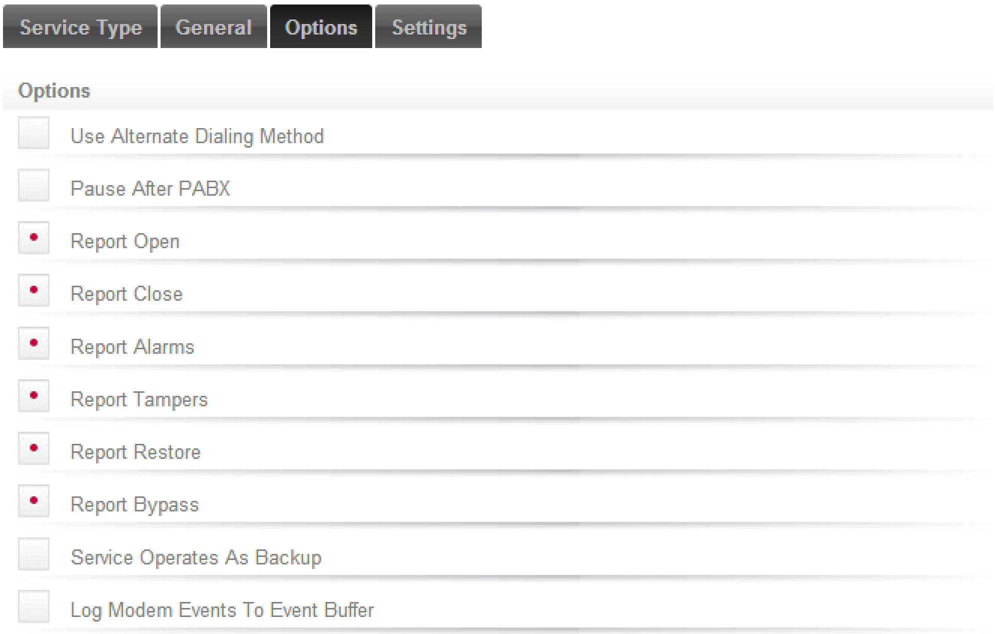


Configuration

Client Code	1234
PABX Number	- Not Set -
Phone Number 1	Acme Monitoring Station
Phone Number 2	- Not Set -
Phone Backup	- Not Set -

- Client Code: The client code is used to identify the system to the remote monitoring company when a report is generated. The client code will accept hexadecimal numbers however this will be dependent on the ability of the receiver and should be verified before configuration.
- PABX Number: The PABX phone number is dialed to gain an outside line if the system is connected to a internal phone extension. The PABX phone number can also be programmed with a schedule in the case that between certain times the phone line is directly connected with an outside line.
- Phone Number 1: The primary phone number will be dialed by the contact ID service when it first is initiated to report an event. The sequence of telephone number dialing is limited by the number of dialing attempts and the method of dialing that is configured (alternate or sequential).
- Phone Number 2: The secondary phone number will be dialed by the contact ID service if a connection with the central station cannot be made on the primary phone number. This may be dialed after the total number of attempts is reached on the primary or sequential until the total number of attempts is reached for the primary and secondary numbers. The sequence of telephone number dialing is limited by the number of dialing attempts and the method of dialing that is configured (alternate or sequential).
- Phone Backup: The backup phone number will be dialed by the contact ID service if a connection with the central station cannot be made on either the primary or secondary phone number. This will be dialed after the total number of attempts is reached on the primary and secondary numbers. The backup number will be dialed for the configured number of dialing attempts programmed for the service.

Contact ID | Options

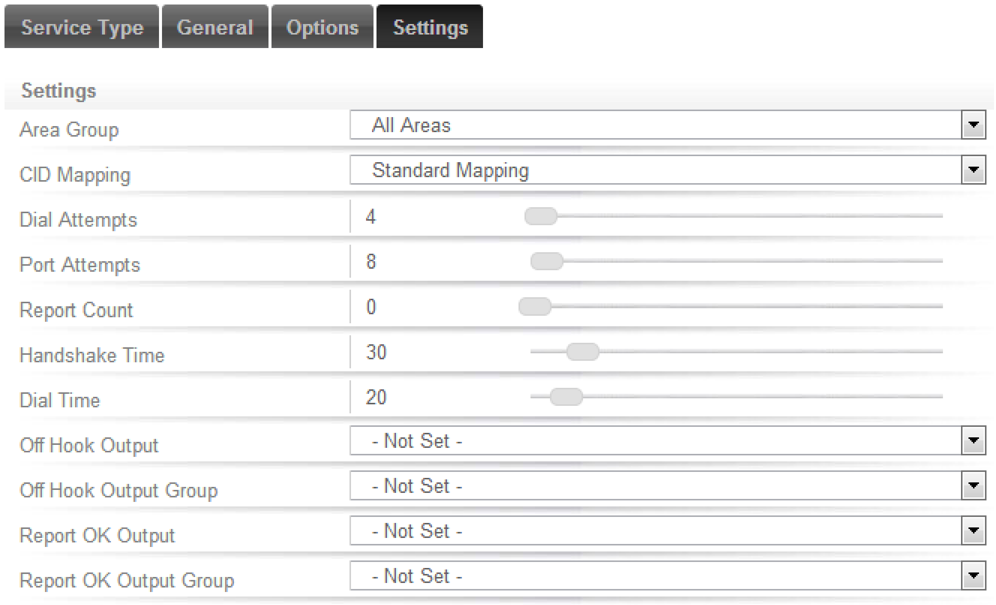


Options

- ☐ Use Alternate Dialing Method
- ☐ Pause After PABX
- ☑ Report Open
- ☑ Report Close
- ☑ Report Alarms
- ☑ Report Tampers
- ☑ Report Restore
- ☑ Report Bypass
- ☐ Service Operates As Backup
- ☐ Log Modem Events To Event Buffer

- Use Alternate Dialing Method: When enabled the service will switch between phone numbers 1 and 2 if a connection cannot be made. If the first phone number fails, the service will switch to the second phone number and vice versa until the max number of attempts is reached.
- Pause After PABX: When enabled the dialer will insert a pause of 2.5 seconds after the PABX telephone number is dialed.
- Report Open: When enabled the service will report opens (Disarming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Report Close: When enabled the service will report closes (Arming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Report Alarms: When enabled the service will report alarms for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Report Tampers: When enabled the service will report tampers for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Report Restore: When enabled the service will report restores for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Report Bypass: When enabled the service will report bypasses for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Service Operates as Backup: When enabled the service will NOT report messages and alarms unless it is started by another service that has failed. It will then start reporting messages immediately from the point that the service that started it failed to report and then return operation to the service that started. This cycle will continue until the service that failed operates normally.
- Log Modem Events to Event Buffer: When enabled the service will provide step by step event information showing the call progression and detailed logging information. This option can be turned on for diagnostic purposes but should not be enabled permanently as large volumes of events are stored.

Contact ID | Settings



Settings

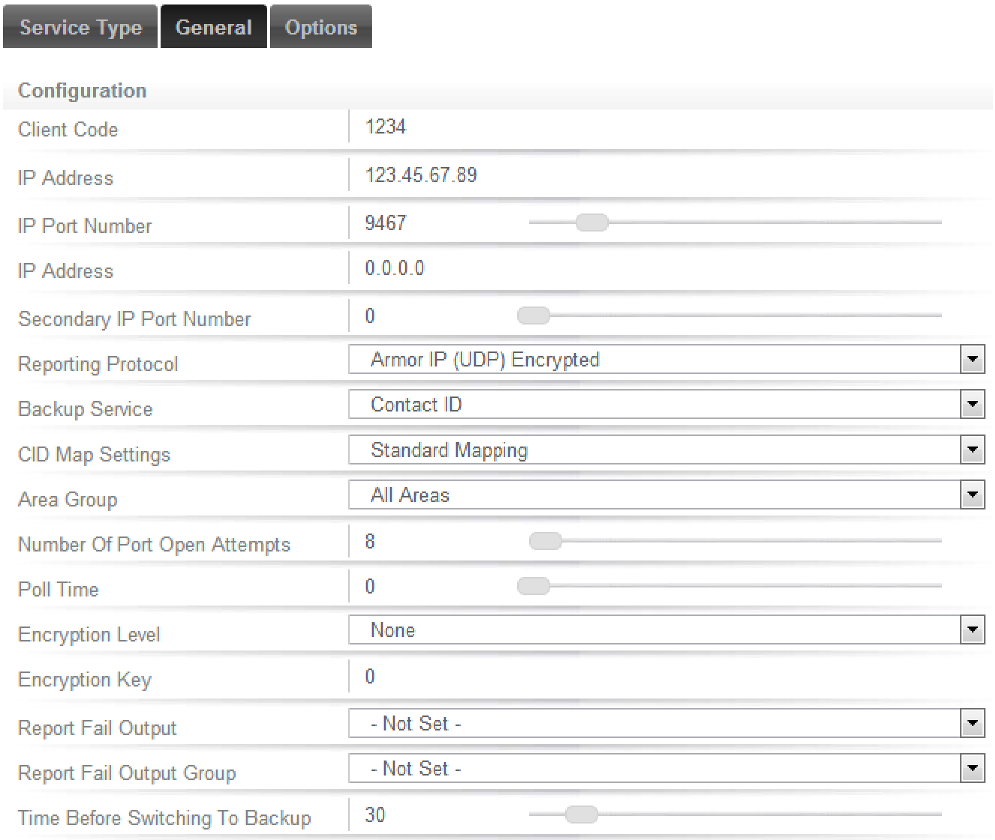
Area Group	All Areas
CID Mapping	Standard Mapping
Dial Attempts	4
Port Attempts	8
Report Count	0
Handshake Time	30
Dial Time	20
Off Hook Output	- Not Set -
Off Hook Output Group	- Not Set -
Report OK Output	- Not Set -
Report OK Output Group	- Not Set -

- Area Group: Defines which areas the service will process when a reportable event is generated. If an area group is not set (default), all areas are processed.
- CID Mapping: With the size of the Protege system the maximum reporting points available in the Contact ID format is easily exceeded, to allow flexibility a reporting table has been created to allow information to be sent using predefined input numbers or values. There are 2 predefined configurations for the reporting tables and 8 custom tables that can be configured for use by any of the services.
- Dial Attempts: Determines how many times the dialer will attempt to dial a number before failure. This setting will be overridden by the modem configuration dependent on the country of installation. For UL and ULC installations this value cannot be set above 8 and will be internally restricted if a value is programmed above this value. The dialing attempts operates in conjunction with the dialing delay setting.
- Port Attempts: The port open attempts determine how many times the service will wait for the modem to become available if another service is already using modem for communication. This operates in conjunction with the port open time settings.
- Report Count: The report count if set to a value other than 000 will restrict the service from sending more than the programmed number of reports to the monitoring station. When using multiple reporting paths that potentially can report the same event to 2 or more locations the report count should be programmed with an acceptable limit (Between 8 and 16 is recommended).
- Handshake Time: The handshake time determines the time it takes for the remote receiving unit to answer and provide a handshake message for the contact ID format. By default this is set to 030 seconds and should only be adjusted if a longer than normal call completion is required.
- Dial Time: The redial time determines inter phone number dialing timeout. A value of 20 seconds is programmed by default meaning each phone number will be dialed with 20 second intervals from the time the previous call was terminated.
- Off Hook Output/Output Group: The Off Hook output or output group is activated when the service takes the telephone line, and is deactivated when the service completes communication. This output setting can be used with remote exchange systems that require ground start communication connections.
- Report OK Output/Output Group: The Report OK output or output group is activated when the service completes the reporting and the messages have been successfully acknowledged. The output is activated when the service returns a reporting complete result OK message. The output is not deactivated and should be programmed with a timer, this can be connected to an external audible device to signal that the report was completed. Using this feature with the shorten exit delay for an area allows an end user to verify the communication path on arming of the building

Report IP

This service allows the Controller to send alarm and activation information over an IP connected network. The Report IP Service supports multiple formats and allows the connection to third party reporting if required.

Report IP | General

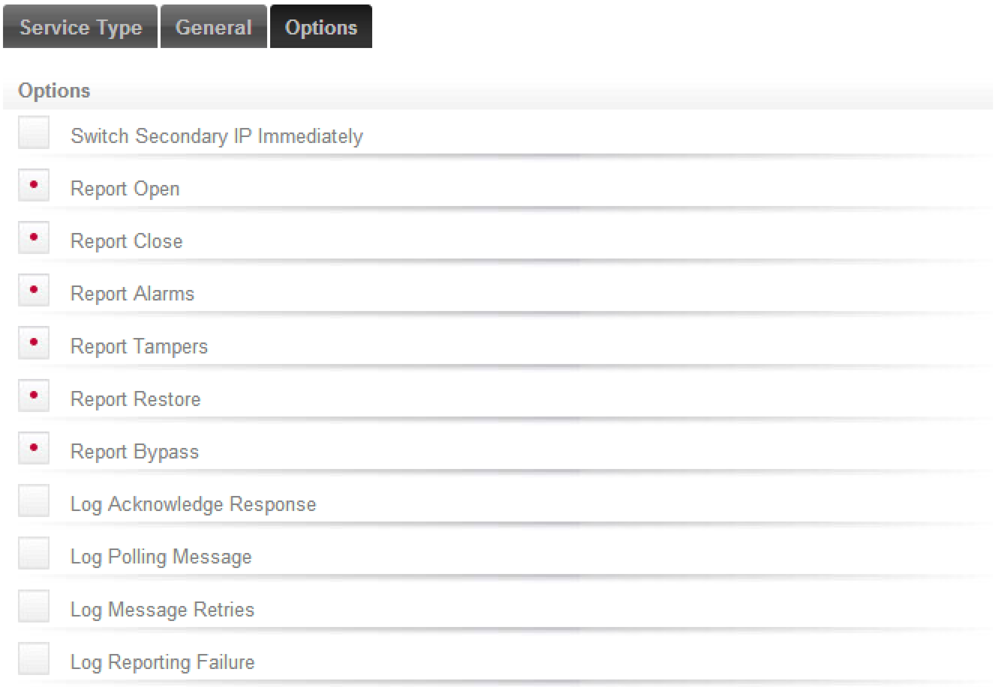


Configuration	
Client Code	1234
IP Address	123.45.67.89
IP Port Number	9467
IP Address	0.0.0.0
Secondary IP Port Number	0
Reporting Protocol	Armor IP (UDP) Encrypted
Backup Service	Contact ID
CID Map Settings	Standard Mapping
Area Group	All Areas
Number Of Port Open Attempts	8
Poll Time	0
Encryption Level	None
Encryption Key	0
Report Fail Output	- Not Set -
Report Fail Output Group	- Not Set -
Time Before Switching To Backup	30

- Client Code: The account number for the Report IP Service can be up to 8 digits. An account code with leading zeros will be truncated to send the minimum number of digits, for example the account code 004311 will be sent as 4311. Where there are more digits set in the account code than the format that is selected allows, the account number will be truncated.
- IP Address: The primary IP address is the IP of the server that has the receiver attached, the receiver can be the ArmorIP Server or an IP receiving device.
- IP Port Number: The primary port configures the reporting service with the remote port number to communicate on. Consult the documentation provided with the Receiver software or hardware to find this information. This information may also be different based on how the device is connected to the internet or intranet that you are communicating on.
- Secondary IP Address: The secondary IP address is the IP of the server that has the receiver attached and can be set so that it will be routed through a separate connection. For example an ADSL modem maybe used for primary and a wireless connection for the secondary communications. For higher security it may also be desirable to have two service providers of internet.
- Secondary IP Port Number: The secondary port configures the reporting service with the remote port number to communicate on for the secondary IP. By using this information in association with the secondary IP, a specific route can be set for this connection.
- Reporting Protocol: The reporting protocol defines how the IP communication data will be sent to the monitoring station. Various protocols are supported to allow the most comprehensive solution.
  - ArmorIP: ArmorIP will communicate to the ArmorIP server software running on a remotely connected server. The ArmorIP Server provides a standard Ademco 685 output and allows routing and redirection of signals to other reception devices such as E-Mail, SMS Messaging and Websites. The ArmorIP software is designed to be used with a Concentrator operating in the central station control room.

  - SIA Over IP: SIA Over IP communicates a SIA Level 2 message using the SIA DC09 specification format to any receiver that supports the SIA DC09 specification. SIA DC09 Specification is currently not released as a formal specification and is subject to change.
  - CID Over IP: CID Over IP communicates a Contact ID message using the SIA DC09 specification format to any receiver that supports the SIA DC09 specification. SIA DC09 Specification is currently not released as a formal specification and is subject to change.
  - AlarmNZ IP: AlarmNZ IP is the IP Communication format used by Alarm New Zealand Limited. By default the AlarmNZ IP service will use the Contact ID reporting format. Information is sent using a login and password and then event information in a ASCII comma separated data format.
  - Patriot LS30: Patriot LS30 Protocol is the IP Communication format used by Patriot Systems central station automation application. By default the Patriot LS30 service will use a form of Contact ID reporting. Information is sent using a proprietary format and to obtain details the user should contact Patriot Systems directly.
- Back Up Service: A back up service can be programmed to allow the IP reporting functions to be backed up by a telephone dialer or similar. Using a back up service can be beneficial to allow link failures and internet access to be reported over an alternate connection.
- CID Map Settings: The CID map settings for the service to use.
- Area Group: An area group will define which areas this service will process when a reportable event is generated. An area group of None (default) will result in all areas being sent with the service.
- Number of Port Open Attempts: The number of times the service should try and attempt to open the communications port.
- Poll Time: The polling time is set to schedule periodic connections with the server. The polling messages sent to the receiver will depend on the format. Some formats require that the polling time be set at both the controller and receivers, in this case ensure that this setting matches the setting provided by the central monitoring station company.
- Encryption Level: The level of encryption for the service.
- Encryption Key: The encryption key for the service.
- Report Fail Output: The output to activate when the service's communications fail.
- Report Fail Output Group: The output group to activate when the service's communications fail.
- Time Before Switching to Backup: If a back up service has been programmed, this field defines the length of time (in seconds) before the service will switch over to backup if it cannot establish a connection through the specified IP channels. If no backup service is specified, then this field is ignored.

Report IP | Options



Options

☐ Switch Secondary IP Immediately

☑ Report Open

☑ Report Close

☑ Report Alarms

☑ Report Tampers

☑ Report Restore

☑ Report Bypass

☐ Log Acknowledge Response

☐ Log Polling Message

☐ Log Message Retries

☐ Log Reporting Failure

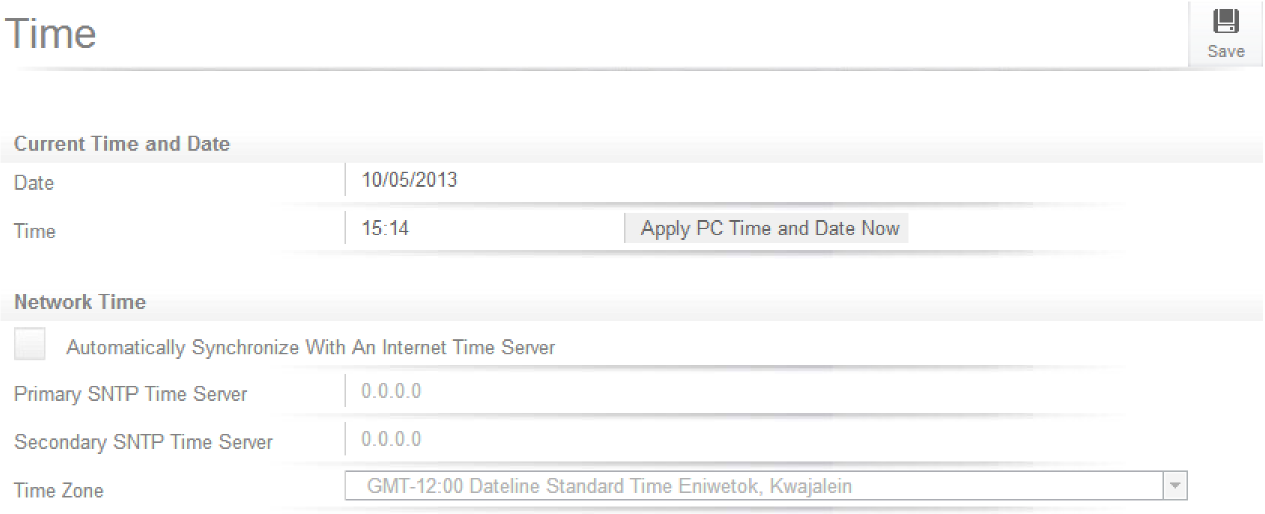
- Switch Secondary IP Immediately: When enabled the service will immediately use the secondary IP settings.
- Report Open: When enabled the service will report opens (Disarming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Report Close: When enabled the service will report closes (Arming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Report Alarms: When enabled the service will report alarms for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Report Tampers: When enabled the service will report tampers for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Report Restore: When enabled the service will report restores for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Report Bypass: When enabled the service will report bypass's for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- Log Acknowledge Response: When enabled the service will log acknowledge communication events.
- Log Polling Message: When enabled the service will log and event when the polling has been accepted by the remote host receiver.
- Log Message Retires: When enabled the service will log a communications retry that occurs because of a network failure or loss of service.
- Log Reporting Failure: When enabled the service will log an event when communications have failed completely and the service is waiting on another attempt.

Scheduling

The Scheduling menu contains the functions relating to date and time information, including schedules and holiday groups.

This Option:	Is Used To:
Time	Set the current date and time
Holiday Groups	Configure holiday periods for use in schedules to prevent (or allow) periods within a schedule to function during the holiday duration
Daylight Savings	Define the daylight savings period associated with a controller
Schedules	Configure schedules for use by system controllers that enable a function or access level to operate only within certain scheduled periods

Time



Current Time and Date

Date: 10/05/2013

Time: 15:14 Apply PC Time and Date Now

Network Time

□ Automatically Synchronize With An Internet Time Server

Primary SNTP Time Server: 0.0.0.0

Secondary SNTP Time Server: 0.0.0.0

Time Zone: GMT-12:00 Dateline Standard Time Eniwetok, Kwajalein

Current Time and Date

- Date: The current date.
- Time: The current time.
- Apply PC Time and Date Now: When selected, sets the current date and time to that of the PC being used.

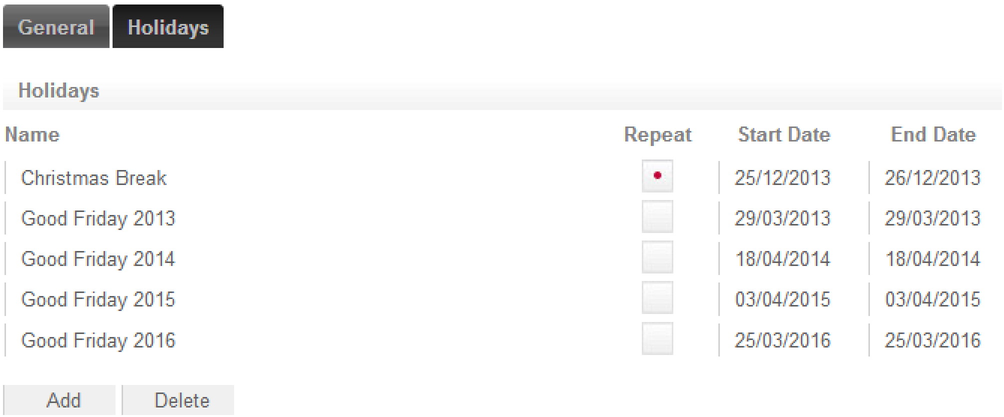
Network Time

- Automatically Synchronize with an Internet Time Server: Select this option to automatically synchronize the controller with an internet time server.
- Primary SNTP Time Server: IP address of the primary SNTP time server for the controller to update its time from.
- Secondary SNTP Time Server: IP address of the secondary SNTP time server for the controller to update its time from should it not be able to connect to the primary SNTP server.
- Time Zone: The current time zone that should be assigned to the controller. Offset from GMT.

Holiday Groups

Holiday Groups are used to prevent (or allow) periods within a schedule from functioning during the holiday duration.

Select the **Holidays** tab to add holidays to the group.



General | Holidays

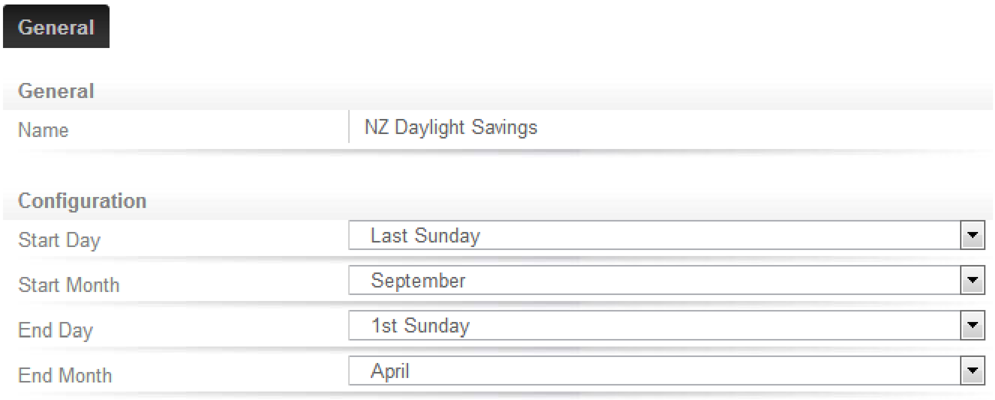
Holidays

Name	Repeat	Start Date	End Date
Christmas Break	☑	25/12/2013	26/12/2013
Good Friday 2013	□	29/03/2013	29/03/2013
Good Friday 2014	□	18/04/2014	18/04/2014
Good Friday 2015	□	03/04/2015	03/04/2015
Good Friday 2016	□	25/03/2016	25/03/2016

- **Name:** The name of the holiday.
- **Repeat:** When enabled, the holiday will recur on an annual basis.
- **Start Date:** The start date of the holiday.
- **End Date:** The end date of the holiday.

Daylight Savings

Daylight savings periods are associated with a controller. The number of daylight savings periods available will depend on the number of controllers connected to the system. Programming the daylight saving settings in the Protege System allows the system to accurately compensate for daylight savings adjustments for the time zone the system controller is located in.



General

General

Name: NZ Daylight Savings

Configuration

Start Day: Last Sunday

Start Month: September

End Day: 1st Sunday

End Month: April

General

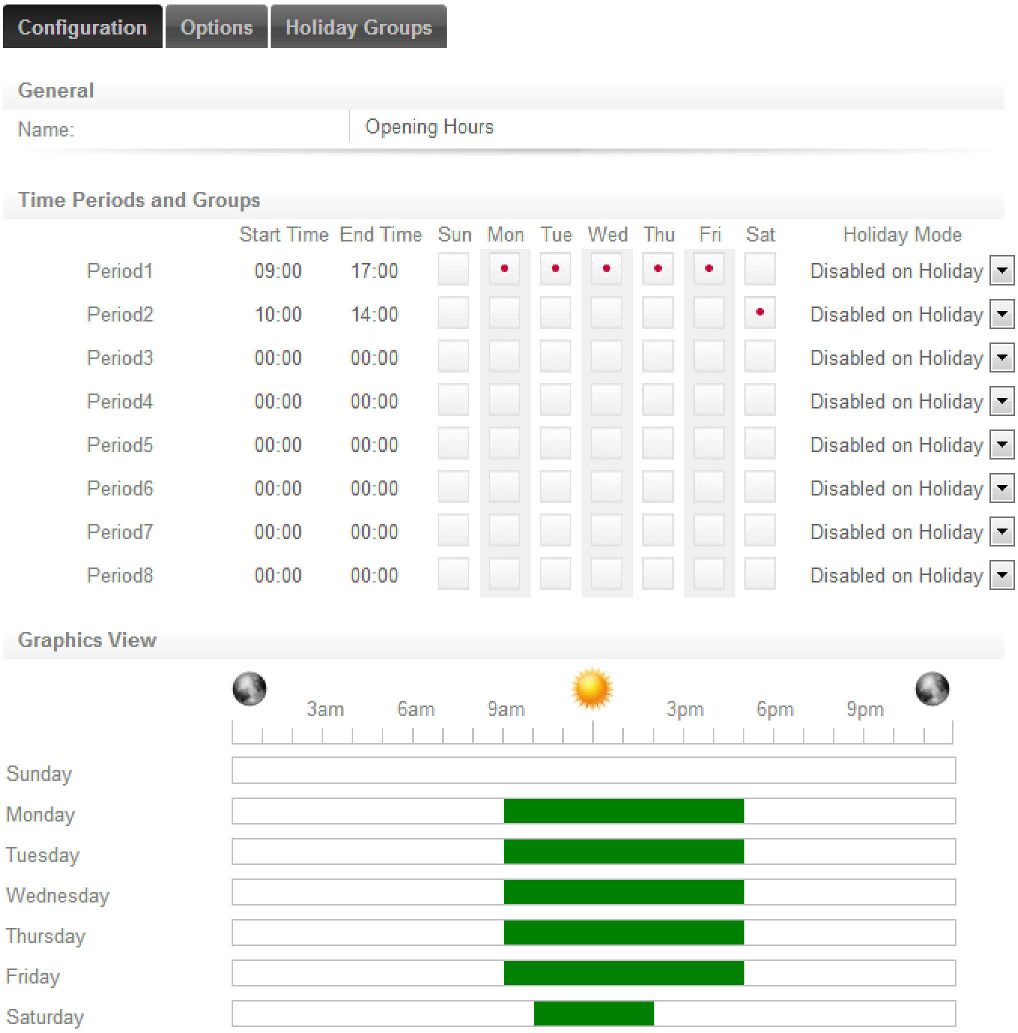
- **Name:** The name of the Daylight Savings period.

Configuration

- **Start Day:** Determines the date that daylight savings will start on.
- **Start Month:** Determines the month that daylight savings will start on.
- **End Day:** Determines the date that daylight savings will end on.
- **End Month:** Determines the month that daylight savings will end on.

Schedules

Schedules enable a function or access level to operate only within certain scheduled periods. Each schedule contains up to 8 periods that can have various times and days programmed. Holiday groups can also be selected to allow a schedule to function when a holiday is active.



Configuration | Options | Holiday Groups

General

Name: Opening Hours

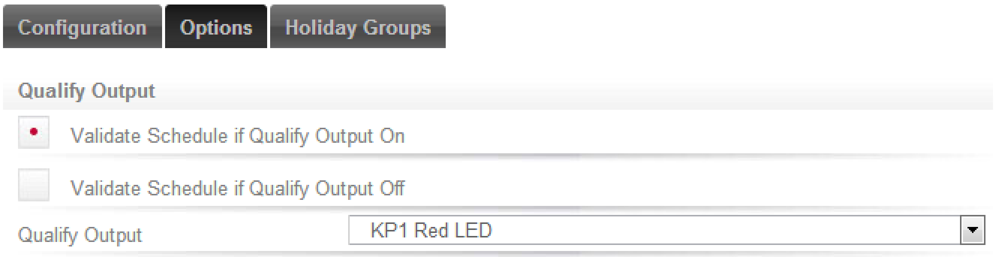
Time Periods and Groups

	Start Time	End Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holiday Mode
Period1	09:00	17:00	□	☑	☑	☑	☑	☑	□	Disabled on Holiday
Period2	10:00	14:00	□	□	□	□	□	□	☑	Disabled on Holiday
Period3	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday
Period4	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday
Period5	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday
Period6	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday
Period7	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday
Period8	00:00	00:00	□	□	□	□	□	□	□	Disabled on Holiday

Graphics View

- Name: The name of the schedule.
- Period 1-8: Time periods for the schedule. Enter a start and finish time for each period and select which days you wish the schedule to operate on by checking the appropriate boxes.
- Holiday Mode: Defines how the schedule will operate during a holiday period. Choose from:
  - Disabled on Holiday: When selected, the period will not make the schedule valid on a holiday. In other words, if a door is programmed to unlock by this schedule, it will not unlock on a holiday if Disabled on Holiday is selected. This is the default mode of operation for schedules.
  - Enabled on Holiday: When selected, the period will only ever make the schedule valid on a holiday.
  - Ignore Holiday: When selected, the period will make the schedule valid regardless of whether the day is a holiday or not.
- Graphics View: The Graphics View provides a visual representation of the schedules periods. Each day of the week is represented by a 24 hour time line where times when the schedule is active are indicated by blue sections. The Graphics View is read-only and as such period times cannot be adjusted from this section of the screen.

Schedules | Options



Qualify Output

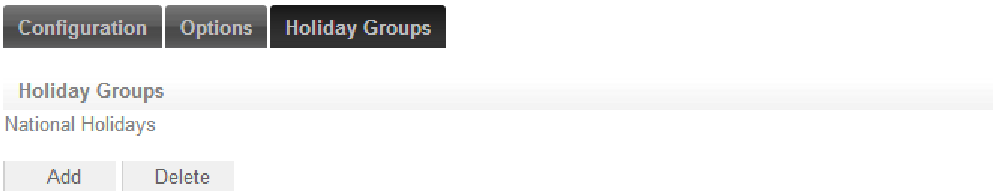
☑ Validate Schedule if Qualify Output On

□ Validate Schedule if Qualify Output Off

Qualify Output: KP1 Red LED

- Invalidate Schedule if Qualify Output On: When enabled the schedule will only operate if the qualify output is on and will be invalidated when the output turns on if it was valid.
- Invalidate Schedule if Qualify Output Off: When enabled the schedule will only operate if the qualify output is off and will be invalidated when the output turns off if it was valid.
- Qualify Output: The schedule can be qualified using an output. This means even if the schedule is valid the schedule will be considered invalid if the output turns on or off. This can be used to change the way a reader functions when the area arms. The qualify schedule output can be used to prevent access to a door if a specific output has been activated.

Schedules | Holiday Groups



Holiday Groups

National Holidays

Holiday Groups: The holiday groups for which the schedule is to apply. Select which holidays groups are required by clicking Add and selecting them from the list.

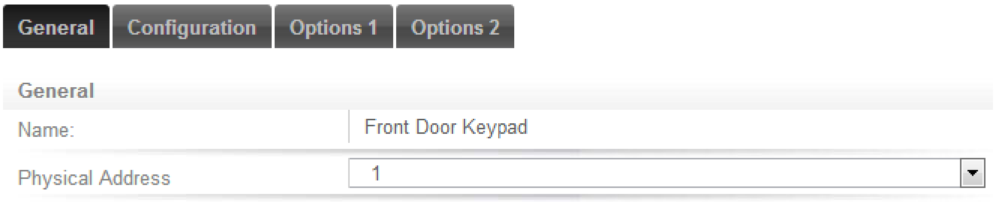
Expanders

The Expanders menu contains the settings required to connect and configure the various expander modules available that extend your Protege WX system.

This Option:	Is Used To:
Keypads	Configure the keypads attached to your system
Analog Expanders	Configure the analog expanders used to connect industrial automation devices to your Protege WX system
Input Expanders	Configure the input expanders used to extend the number of inputs available within the system
Output Expanders	Configure the output expanders used to extend the number of outputs available within the system
Reader Expanders	Configure the reader expanders used to extend the number of reading devices and locking inputs available within the system
Expander Addressing	View the hardware that is connected to the system network, and set the addresses of the modules that have auto-addressing capability

Keypads

Keypads are used for all functions within the Protege System and are typically located near an entrance or door to allow areas within the system to be armed and disarmed.



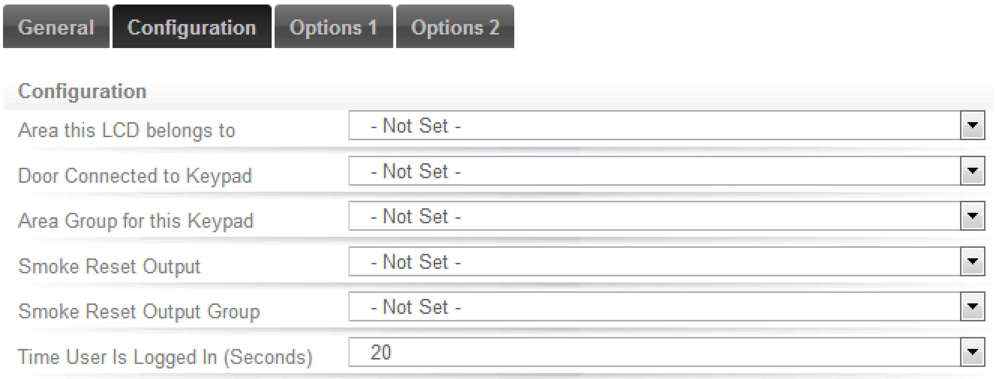
General

Name:	Front Door Keypad
Physical Address	1

General

- **Name**: The name of the keypad
- **Physical Address**: The network address of the keypad.

Keypads | Configuration



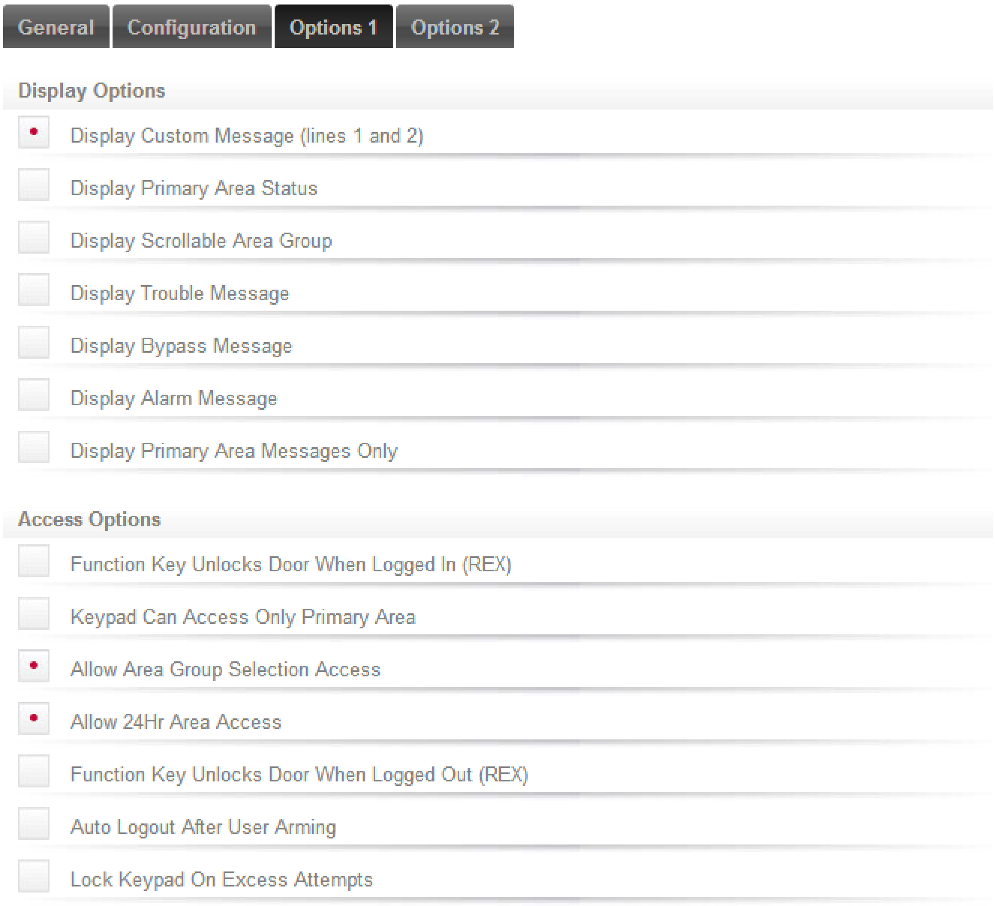
Configuration

Area this LCD belongs to	- Not Set -
Door Connected to Keypad	- Not Set -
Area Group for this Keypad	- Not Set -
Smoke Reset Output	- Not Set -
Smoke Reset Output Group	- Not Set -
Time User Is Logged In (Seconds)	20

- **Area this LCD belongs to:** The primary area for the keypad is the area that the keypad will display first on all area display modes. The primary area should be belong to the keypad's area group, if any area actions are to be performed on the keypad.
- **Door Connected to Keypad:** The door which is connected to the keypad.
- **Area Group for this Keypad:** Users can only access an area assigned to the keypad if the same area is also assigned to the user's arm and/or disarm area group.

- **Smoke Reset Output/Output Group:** The output (or output group) that is programmed as the keypad smoke detector reset output will be activated when a user presses the CLEAR + ENTER keys together.
- **Time User Is Logged In (Seconds):** When the user does not perform any action on the keypad for the programmed time, the keypad will automatically log the user out. Programming the option 'Never Logout' should be avoided unless for training or demonstration purposes.

Keypads | Options 1



Display Options

- ☑ Display Custom Message (lines 1 and 2)
- □ Display Primary Area Status
- □ Display Scrollable Area Group
- □ Display Trouble Message
- □ Display Bypass Message
- □ Display Alarm Message
- □ Display Primary Area Messages Only

Access Options

- □ Function Key Unlocks Door When Logged In (REX)
- □ Keypad Can Access Only Primary Area
- ☑ Allow Area Group Selection Access
- ☑ Allow 24Hr Area Access
- □ Function Key Unlocks Door When Logged Out (REX)
- □ Auto Logout After User Arming
- □ Lock Keypad On Excess Attempts

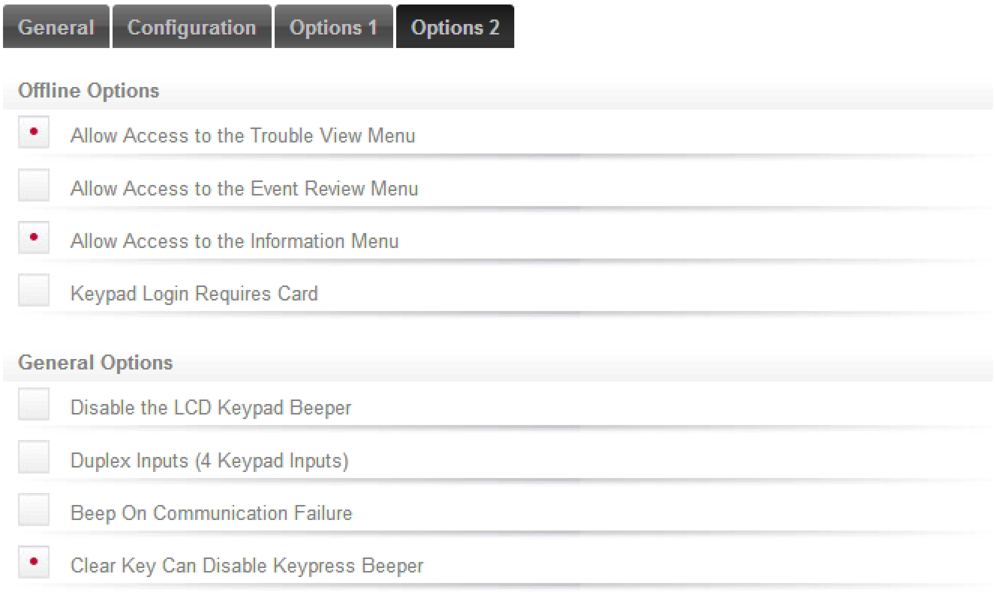
Display Options

- **Display Custom Message (lines 1 and 2):** When enabled, the keypad will display the text programmed in the Controller settings.
- **Display Primary Area Status:** When enabled, the keypad will display the status of the primary area that is assigned to the keypad.
- **Display Scrollable Area Group:** When enabled, the keypad will display the status of the area's that are assigned in the area group.
- **Display Trouble Message:** When enabled, the keypad will display the trouble input(s) when a failure has occurred.
- **Display Bypass Message:** When enabled, the keypad will display the message input(s) bypassed when an input has been bypassed in the system or primary area if the Display Primary Area Messages Only option is also enabled.
- **Display Alarm Message:** When enabled, the keypad will display the message alarm(s) in memory.
- **Display Primary Area Messages Only:** When enabled in conjunction with the Display Alarm Message option, the keypad will only display the bypassed input status and alarm memory for the primary area of the keypad. Setting this option means that only the primary area's alarms are shown, in which case, the alarm message is cleared only if the primary area's memory is acknowledged. If this option is not enabled, then any area that has an alarm stored in memory is shown and all the area's memory must be acknowledged before this message is cleared.

Access Options

- **Function Key Unlocks Door When Logged In (REX):** When enabled, allows the user to unlock the controlled door by pressing the FUNCTION key when they are logged in.
- **Keypad Can Access Only Primary Area:** When enabled, the keypad will only allow the user to access the keypad's primary area.
- **Allow Area Group Selection Access:** When enabled, the keypad will allow the area group access screen to be accessed by the user.
- **Allow 24Hr Area Access:** When enabled, the keypad will allow the 24Hr status screen of an area to be accessed by the user. The user must have the 24Hr menu option set.
- **Function Key Unlocks Door When Logged Out (REX):** When enabled, allows the user to unlock the controlled door by pressing the FUNCTION key when they are logged out.
- **Auto Logout After User Arming:** When enabled, the keypad will automatically log the user out once they have armed an area.
- **Lock Keypad On Excess Attempts:** When enabled, the keypad will lock if a user makes 3 invalid attempts to log on.

Keypads | Options 2



Offline Options

☑ Allow Access to the Trouble View Menu

□ Allow Access to the Event Review Menu

☑ Allow Access to the Information Menu

□ Keypad Login Requires Card

General Options

□ Disable the LCD Keypad Beeper

□ Duplex Inputs (4 Keypad Inputs)

□ Beep On Communication Failure

☑ Clear Key Can Disable Keypress Beeper

Offline Options

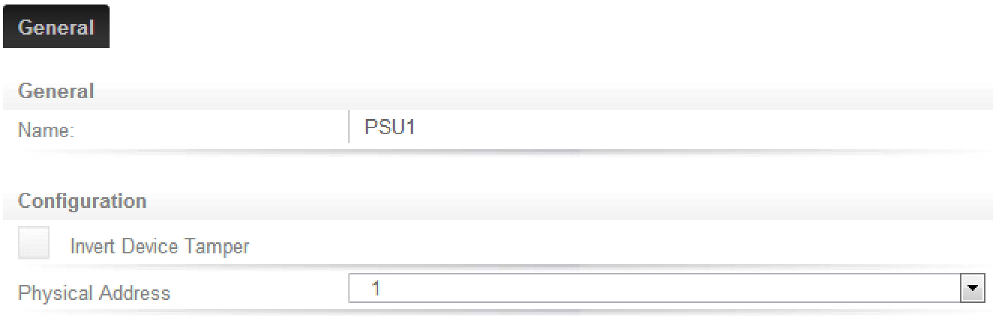
- **Allow Access to the Trouble View Menu:** When enabled, the keypad will allow access to the View Trouble Menu if no user is logged in.
- **Allow Access to the Event Review Menu:** When enabled, the keypad will allow access to the Event Review Menu if no user is logged in.
- **Allow Access to the Information Menu:** When enabled, the keypad will allow access to the Keypad Information menu is no user is logged in.
- **Keypad Login Requires Card:** When enabled, the keypad will require access card verification along with a user code before the user login can succeed.

General Options

- **Disable the LCD Keypad Beeper:** When enabled, the keypad will not beep when a key is pressed.
- **Duplex Inputs (4 Keypad Inputs):** When enabled, the keypad will enable the Duplex Input option making it possible to connect four inputs to the keypad.
- **Beep On Communication Failure:** When enabled, the keypad will beep on a communication failure.
- **Clear Key Can Disable Keypress Beeper:** When enabled, the CLEAR key can disable the keypad beeper.

Analog Expanders

Analog Expanders are used to connect industrial automation devices to your Protege system.



General

Name: PSU1

Configuration

□ Invert Device Tamper

Physical Address: 1

General

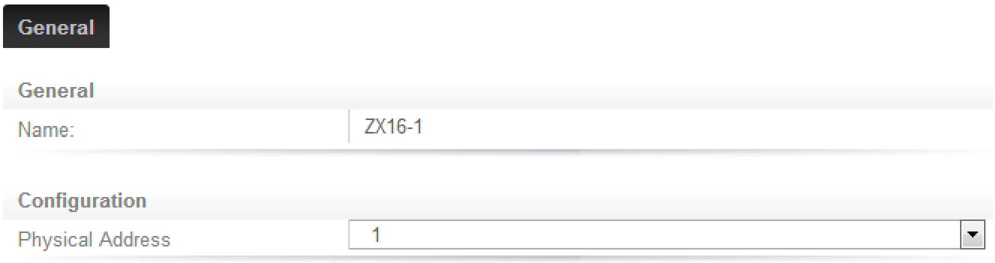
- **Name:** The name of the analog expander.

Configuration

- **Invert Device Tamper**: When enabled, the analog expander will invert the module tamper input allowing a normally open tamper switch to be used. When disabled the analog expander will use the standard normally closed tamper switch.
- **Physical Address**: The device address of the Analog Expander.

Input Expanders

Input Expanders extend the number of inputs available within the system.



General

Name: ZX16-1

Configuration

Physical Address: 1

General

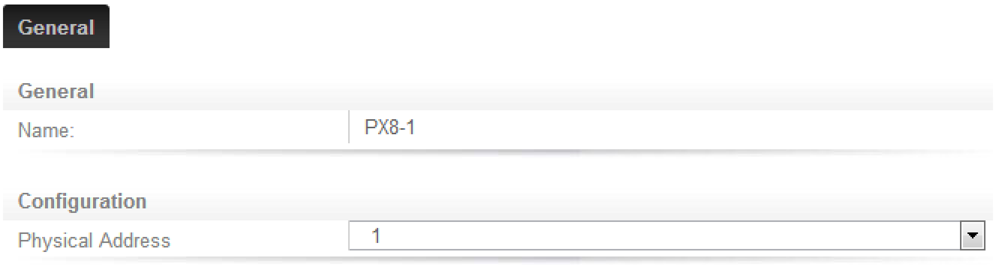
- **Name:** The name of the input expander.

Configuration

- **Physical Address**: The device address of the Input Expander.

Output Expanders

Output Expanders extend the number of outputs available within the system.



General

Name: PX8-1

Configuration

Physical Address: 1

General

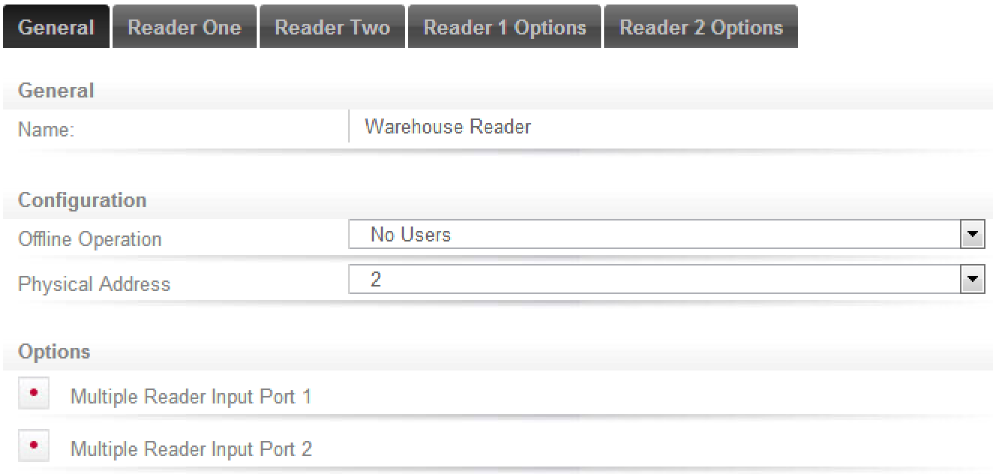
- Name: The name of the output expander.

Configuration

- Physical Address: The device address of the Analog Expander.

Reader Expanders

Reader Expanders extend the number of reading devices and locking inputs available within the system.



General

Name: Warehouse Reader

Configuration

Offline Operation: No Users

Physical Address: 2

Options

☑ Multiple Reader Input Port 1

☑ Multiple Reader Input Port 2

General

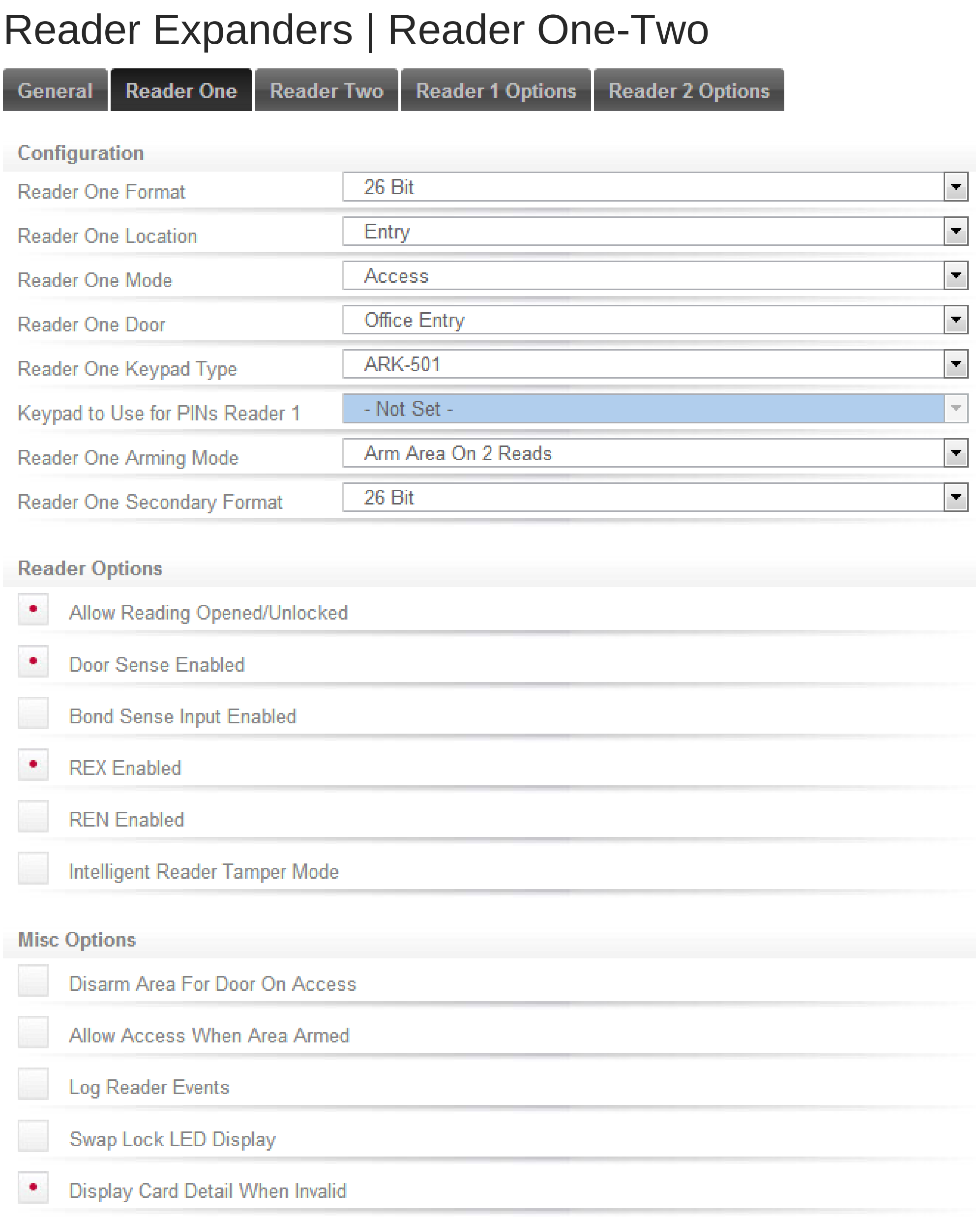
- Name: The name of the reader expander.

Configuration

- Offline Operation: Defines the mode of offline operation allowed, enabling the reader to operate autonomously if communications with the controller fail.
- Physical Address: The device address of the Reader Expander.

Options

- Multiple Reader Input Port 1: When enabled, the reader will process the multiplexed reader inputs on Port 1 so that dual readers can be connected for entry and exit processing. The duplex reader that is connected will always operate as the exit reader. When disabled the reader port 1 interface will operate as a single reader input.
- Multiple Reader Input Port 2: When enabled, the reader will process the multiplexed reader inputs on Port 2 so that dual readers can be connected for entry and exit processing. The duplex reader that is connected will always operate as the exit reader. When disabled the reader port 2 interface will operate as a single reader input.



Reader Expanders | Reader One-Two

Configuration

Reader One Format	26 Bit
Reader One Location	Entry
Reader One Mode	Access
Reader One Door	Office Entry
Reader One Keypad Type	ARK-501
Keypad to Use for PINs Reader 1	- Not Set -
Reader One Arming Mode	Arm Area On 2 Reads
Reader One Secondary Format	26 Bit

Reader Options

- ☑ Allow Reading Opened/Unlocked
- ☑ Door Sense Enabled
- ☐ Bond Sense Input Enabled
- ☑ REX Enabled
- ☐ REN Enabled
- ☐ Intelligent Reader Tamper Mode

Misc Options

- ☐ Disarm Area For Door On Access
- ☐ Allow Access When Area Armed
- ☐ Log Reader Events
- ☐ Swap Lock LED Display
- ☑ Display Card Detail When Invalid

Configuration

- Reader Format: The reading format used to inform the reader expander what type of card readers are connected to the reader port. The reader expander supports nearly all publicly available protocols and some special protocols. Any 26 or 37 bit card reader that conforms to the standard format specification will work on the Reader Expander.
  - 26 Bit: The industry standard 26 bit format consisting of 8 site code/facility bits and 16 bits of card information. The most common format used in the access control industry.
  - ICT 37 Bit
  - Keyscan 36: A proprietary format used by HID® Readers that are re-branded for with the Keyscan Corporation of Canada and implemented through out North America.
  - NCS 25/29 Bit: An older format that allows dual card technology. Northern Control Systems 25 Bit Swipe and 29 Bit Swipe cards.
  - Northern 34 Bit: Northern Computers® proprietary 34 Bit Format.
  - Kantech 32 Bit: Kantech Systems from Canada. A 32 Bit format sometimes referred to as KSF 32 or Kantech Secure Format.
  - STID ISO T2: STID of Europe ISO compliant track 2 magnetic card format used for hotels and various other hospitality establishments. Uses the first 8 digits on the card.

- Sentrax 9000 T2: A track 2 magnetic card format utilized in New Zealand by the Sentrax T2 Access Control System. Uses an 8 digit site code and 10 digit card number encoded with expiration and utility codes. This format ONLY decodes the Facility and Card numbers.
- Propel Track 2: A track 2 format used through out Asia proprietary based for Propel Systems Sdn Bhd of Kuala Lumpur. Uses a 4 digit site code and 5 digit card number on a track 2 magnetic format card.
- 40 Bit: A 40 Bit Wiegand format used in some older model readers which implements a 12 bit site code and 16 bit card number.
- Mirage 33 Bit: A 33 Bit format implemented in the Mirage readers, has a 8 bit site code and 16 bit card number.
- Motorola 27 Bit: A 27 Bit format that has 9 site code bits and 16 card number bits.
- ABA T2: American Banking Association Track 2 magnetic format that uses the data encoded on a standard 16 digit bank card. The data is hashed and then sent to the controller. This prevents the data from being reversed to establish the card number. This format does NOT require a full 16 digits to create the hash.
- Multi 26/34 Bit: A multi bit format to allow the operation of both 26 and 34 Bit Cards on the same port. This can also be achieved by using the secondary reader format.
- First 4 T2: The first 4 digits of a track 2 card will be used as the card number and a site code of 0 will be generated.
- Kantech 39 Bit: A Kantech Systems of Canada format that uses 39 bits of information with a 8 bit facility code and 24 bit card number.
- Setec 37 Bit: A Setec Card Reader format that is similar to the 37 Bit format however overall parity is used in place of the individual 4 parity bits.
- Motorola ABA T2: Motorola Indala® produced card readers that were capable of outputting a multiple format. These generated a format similar to the Track 2 format however the number of digits generated was based on the card programming data.
- Hotel T2: An encrypted format used for the hotel industry and prevents the creation of cards. The hotel format can be used with MANY key and lock manufactures. The Hotel Format is not widely used and now slowly being replaced by Smart Card technology. We recommend that this format is not used and is included for legacy implementations.
- 32 Bit: A straight 32 bit format consisting of a single card serial number and is typically used by Mifare® reading devices when outputting data. This can also be sent using the 34 Bit formats.
- 32 Bit (Rev): Identical to the 32 Bit format above however the data is sent in reverse order from Bit 32 to Bit 0.
- WSE 34 Bit: Westinghouse® Security Electronics format. A 34 bit format based on 16 Digit Family number and 16 Digit Card Number.
- HID 32 Bit: HID® 32 Bit format has no parity and data is generated as a complete 32 Bit data block.
- First 6 Track 2: The first 6 digits of a track 2 card will be used as the card number and a site code of 0 will be generated.
- 30 Bit: The 30 Bit format consists of 2 14 bit blocks with parity and a 8 digit facility code and 20 digit card number. Not a common format and is typically found on older Smart Card readers.
- 37 Bit: The 37 bit format is different to the first format and of 1 block of 35 bits of data which is broken in to a 20 bit card number and 15 bit site code. This is commonly used with older HID® readers.
- 36 Bit: A standard 36 Bit format which consists of 4 8 bit blocks each with a parity bit. This is commonly used with the Dallas one wire and Kwik Key products.
- Rusco 40 Bit: A Casi Rusco 40 Bit format used on the smart card readers produced by Casi Rusco and WSE. The format will output a 24 bit card number and 10 bit site code.
- ABA BIN T2:American Banking Association Track 2 magnetic format that uses the BIN (Bank Identification Number) stored in the first 4 digits as the card number. This format can be used to allow entry in to Bank ATM Foyers. By putting an access level on the cards they can also be used to prevent access at certain times and can be used to activate the lighting in the ATM area when presented.
- ABA Card T2: American Banking Association Track 2 magnetic format that uses the data encoded on a standard 16 digit bank card. The data is hashed and then sent to the controller. This prevents the data from being reversed to establish the card number. This format is the same as the ABA T2 format however it strictly requires a 16 Digit Card to be presented for the format to operate.

  - NCS 29 Bit: An older format that is used by Northern Control Systems and is a 29 Bit Format.
  - HID 34 Bit: A standard HID format consisting of a 16 digit site code and a 16 digit card number with parity calculated on the end two bits.
  - HID 26/34 Bit: A dual format consisting of the standard 26 Bit and Standard 34 Bit formats.
  - Auto - Wiegand: Automatically selects the best available Wiegand format from the formats to decode the card.
  - Auto - Magnetic: Automatically selects the best available Magnetic Card format from the formats to decode the card data.
  - 36 Bit (IEI): A standard 36 Bit Output format that is compatible with the IEI keypads, this allows wiegand data to be received from the keypad as a card number. This format can also be used with compatible card reading devices.
  - 34 Bit (Pass): Decodes the Pass Point 34 Bit Cards used on the HID Card Readers in to the correct large card number 32 bits and standard site code.
  - 34 Bit (Pass NP): Decodes the Pass Point 34 Bit Cards used on the HID Card Readers however skips the parity validation on the data stream to allow the Nano Prox card readers to be retrofitted to new or existing doors that use the Pass Point cards.
  - Any Bit (Raw): Any Bit format decodes ANY wiegand data stream up to 64 bits and then presents this to the system using the multiple decoding display. The display contains encoded data based on the raw data stream sent by the card reader. This allows ANY wiegand reader to operate on the Protege System in a native data format. This format will decode the data explicitly and can be used to verify wiegand data streams.
  - 26 Bit (NP): Decodes a standard 26 bit wiegand data stream however skips the parity validation portion of the wiegand data. This format can be used when certain card formats have parity detection reversed or if the parity calculation deviates from the standard.
  - 34 Bit (NP): Decodes a standard 34 bit wiegand data stream however skips the parity validation portion of the wiegand data. This format can be used when certain card formats have parity detection reversed or if the parity calculation deviates from the standard.
  - First 5 Track 2: The first 5 digits of a track 2 card will be used as the card number and a site code of 0 will be generated for the card swipe.
  - Apollo 44 Bit: Decodes an encrypted 44 bit wiegand data stream from the AMDI Apollo format card readers. The card number received will match the hot stamp card number. Site codes may vary but will typically be the preceding 3 digits.
  - CANSEC 37 Bit
  - Tecom 27 Bit
  - HID Corp 1000: A 35 bit format with a unique Company ID Code and over 1,000,000 card numbers available for use.
- Reader Location: The reader location informs the reader expander which location of the door the reader is installed at, which is connected to the reader expander port. The reader expander uses this information to pass the correct direction of travel to the door control functions. For an access door this should be set to 'Entry' reader.

  When using the reader with a door that controls an inside or outside area for arming or disarmed or for global anti-passback the ENTRY and EXIT configuration must be set correctly to ensure the correct action is taken by the reader expander.

  - Exit: The reader is located on the inside of the door and is used to exit out of the area that is being protected by the door.
  - Entry: The reader is located on the outside of the door and is used to enter in to the area that is being protected by the door. This is the default setting and should be set for all general access doors (single reader)

    If the reader expander is configured for multiplex reader mode the multiplexed reader is ALWAYS the EXIT reader.
- Reader Mode: The reader expander port mode.
  - Access: The reader expander port is used to control access through doors. You must configure the door that is controlled by this reader expander.

- Reader Door: The reader controlled door setting sets the door that the reader on port one will provide card and control information to. It is possible that more than one reader has the same controlled door (Entry and Exit reading configuration).
- Reader Keypad Type: The keypad operation mode programmed for the reader on a port determines if the reader port has a pin entry device attached or uses a local LCD keypad.
  - LCD Keypad: An LCD keypad is used for PIN entry. PIN entry is only possible with the Card and PIN configuration when using an LCD Keypad. To unlock in the PIN Only or Card or PIN modes the unlock shortcut key can be used. The LCD Keypad Address is configured in the next screen.
  - 26 Bit (Site 0): A 26 Bit Wiegand Keypad is connected in parallel with the Reader Device and has a site code of 0 set for the unit.
  - ARK-501: A Motorola® Format the ARK-501 outputs 8 bits of data for each key that is pressed consisting of the first 4 bits being inverted from the remaining 4. This format requires the user to press the '#' key on completion of the PIN entry.
  - 4 Bit: 4 Bits of data is output for each pressed key.
  - 4 Bit Parity: 5 Bits of data is output for each pressed key with the last bit being ODD parity on the first 4 bits.
  - 4 Bit Buf: The number of bits that are sent relate to the key press's multiplied by 4. The data is buffered and only sent when the user of the keypad press's the Enter key on the keypad.
  - 4 Bit Buf and Par: The number of bits that are sent relate to the key press's multiplied by 5, each key press is 4 bits followed by a last parity bit. The data is buffered and only sent when the user of the keypad press's the Enter key on the keypad.
  - 36 Bit (IEI Site 0): A 36 Bit Wiegand Keypad format typical of an IEI keypad which can be set to decode PIN numbers from 0-999999
  - None: There is no keypad device connected to or associated with this reader input device.

  When a Wiegand 26 Bit or 36 Bit Keypad is used PIN numbers that are prefixed with a 0 cannot be used and a maximum pin number of 65533 can be used for 26 Bit and 999999 for 36 Bit. This is a limitation of the 26 Bit and 36 Bit Format and not the Reader Expander. To utilize the full 8 digit capacity for the PIN number of a user and allow prefixed PIN numbers select a PIN device that supports the ARK-501 or Bit Buffered Outputs.
- Keypad to use for PINs reader: If the keypad operation mode is set to use one of the selected LCD keypads you can program the address of the keypad to use for pin entry. When using this mode of operation the LCD keypad will present a login message when a valid card is presented that requires pin entry.
- Reader Arming Mode: The reader port can perform various operations when a user badges their card multiple times. The list below details the modes this can operate in.

  When a multi badge operation has taken place the reader expander will beep the buzzer output four times. In area control, if the area is already armed the reader will only beep twice.
  - Do Nothing: No action will be taken by the system for arming an area associated with the door.
  - Arm Area on 2 Reads: Two successive reads from the same user will result in the inside or outside area (depending on the card reader type configuration) starting the arming process.
  - Read and Input 4 of Expander: Pressing and holding Input 4 (RDXXX:04) while presenting a card will begin arming. Input 4 must be in an area that is armed to ensure the input information is transmitted to the system controller. The area armed will depend on the card reader type setting. This option cannot be used with the PRT-RDM2, Input 4 is not available on the module. Use another arming method or use the PRT-RDS2 or PRT-RDI2.
  - Arm Area on 3 Reads: Three successive reads from the same user will result in the inside or outside area (depending on the card reader type configuration) starting the arming process.
  - Toggle Function Output on 3 Reads: Three successive reads from the same user will result in the function output state being toggled. If the output is currently on it will be turned off and if it is off it will be turned on.
  - Activate Function Output on 3 Reads: Three successive reads from the same user will result in the function output state being turned on.
- Reader Secondary Format: The secondary reading format is used to program an alternate format for the reader expander and has the same options as the standard reader selection. The secondary format will only be used if the first format cannot decode the card information that is received by the reader interface.

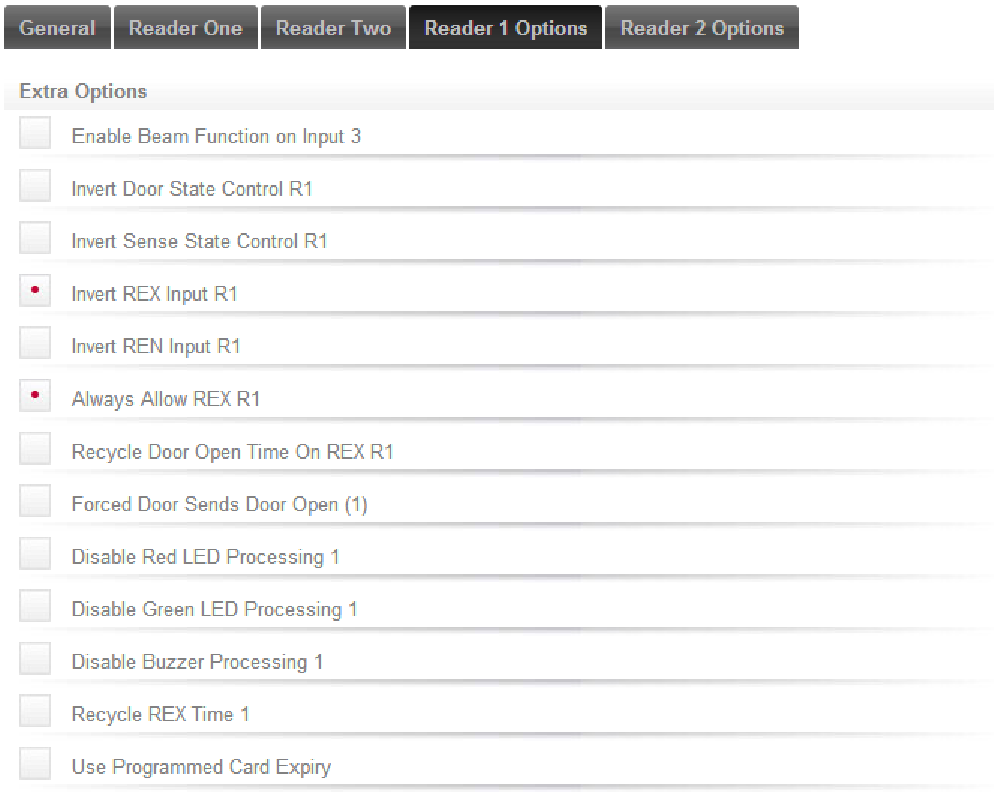
Reader Options

- Allow Reading Opened/Unlocked: When enabled, the reader expander will send card information to the system controller when a door is unlocked or opened. This option is set by default and should be left set if the door control areas or time and attendance events are required from the reader port. When disabled the reader performs no action when a card is presented and the door is unlocked or open.
- Door Sense Enabled: When enabled the reader will send door events when the door input is opened or closed. This is enabled by default but should be disabled on at least one reader port if both reader ports are controlling the same door (ENTRY and EXIT access control).
- Bond Sense Input Enabled: Enables the magnetic bond sense functions. The magnetic bond sense is a contact that indicates if the magnetic bond between the electromagnet and the clamp is complete. It is used when a separate door contact and bond sense input are to be used however the generation of door events should be processed using both inputs.
- REX Enabled: When enabled, the reader expander will generate request to exit events from the REX input on the reader expander. When disabled the keypad will not generate any REX events.
- REN Enabled: When enabled, the reader expander will generate request to enter events from the REN input on the reader expander. When disabled no action will be taken for the Request To Enter function.
- Intelligent Reader Tamper Mode: When enabled, the reader expander will assume that the external device has smart messaging that allows a communication path to be formed from the reading devices (Card reader) to the reader expander. When disabled the intelligent reader mode is disabled.

Misc Options

- Disarm Area For Door On Access: When enabled, the reader process will disarm the area designated by the reader type (Entry or Exit) and the door configuration programmed (if it has an area on the inside or outside assigned). When disabled the reader will not perform any disarm functions.
- Allow Access When Area Armed: When enabled, the user will be granted access based on the access control configuration only and the area status will not be checked against the user's ability to disarm the area. When the option is disabled and the user who is attempting access to a door that has an area assigned that is armed and the user cannot disarm the area the user will be denied entry to the door even though they may have the correct door and schedule settings.
- Log Reader Events: When enabled, the reader events will be logged to the event review log. When disabled the reader will not log the events to the event review log.
- Swap Lock LED Display: When enabled, the LED display associated with the lock status will follow lock output two. Use this option when a reader expander is used in an Entry and Exit configuration and only one lock output is controlling the door. When disabled the lock and LED display is processed normally.
- Display Card Detail When Invalid: When enabled, the reader expander will display the actual card data received from the reader when the card number is not known. This option is enabled by default and can be used to identify facility and card number details before adding card data to a user. When disabled, the reader will display the card number not found message.

Reader Expanders | Reader 1-2 Options



Extra Options

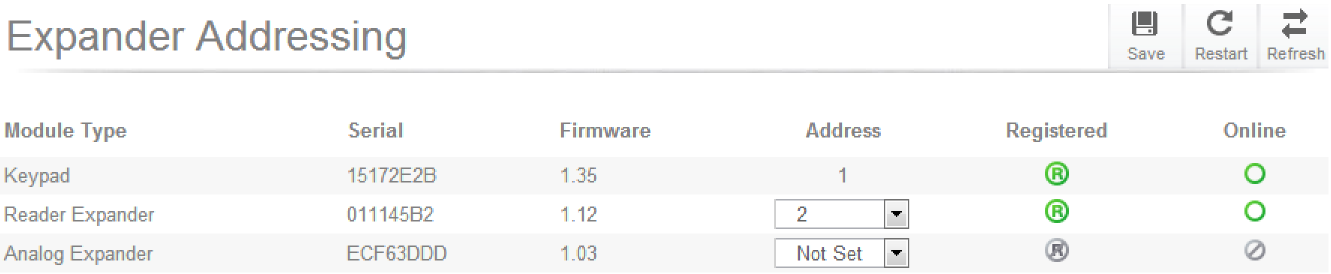
- □ Enable Beam Function on Input 3
- □ Invert Door State Control R1
- □ Invert Sense State Control R1
- ☑ Invert REX Input R1
- □ Invert REN Input R1
- ☑ Always Allow REX R1
- □ Recycle Door Open Time On REX R1
- □ Forced Door Sends Door Open (1)
- □ Disable Red LED Processing 1
- □ Disable Green LED Processing 1
- □ Disable Buzzer Processing 1
- □ Recycle REX Time 1
- □ Use Programmed Card Expiry

- Enable Beam Function On Input: When enabled, the reader expander will process the sense input for beam control. Beam control allows the reader expander to control an automatic gate which must have its contacts held open even if the pathway is blocked. When disabled the reader will not perform beam processing.
- Invert Door State Control: When enabled, the door contact input is inverted. This does not affect the input functionality if it is being used. When disabled door contact functions normally.
- Invert Sense State Control: When enabled, the reader will invert the bond sensing input. When disabled bond sensing will operate normally.
- Invert REX Input: When enabled, the reader will invert the request to exit input. When disabled REX input will operate normally.
- Invert REN Input: When enabled, the reader will invert the request to enter input. When disabled REN input will operate normally.
- Always Allow REX: When enabled, the reader will always allow a request to exit event even if the door is forced open. This will not restart the forced door or the door alarm operation. When disabled REX input will operate only when the door is closed.
- Recycle Door Open Time on REX: When enabled, the reader will extend the door open time when the REX is received. The REX must be received during the normal open time or during the pre-alarm time for the timer to be recycled. Pressing the request to exit once the door has been open too long will require that the door be closed. This option will not affect the ability for the request to exit action to unlock the door. When disabled REX input will not alter the door open time once the door as been opened.
- Forced Door Sends Door Open: When enabled, the reader expander will process door forced open events as door open events. When disabled the reader will process forced door events as normal.
- Disable Red LED Processing: When enabled, the reader expander will not control the Red LED (L2) and the output can be used for another function, this is particularly useful if the attached proximity reader LED's is controlled with one wire. When disabled the reader will turn on the Red LED when the door is locked.
- Disable Green LED Processing: When enabled, the reader expander will not control the Green LED (L1) and the output can be used for another function, this is particularly useful if the attached proximity reader LED's is controlled with one wire. When disabled the reader will turn on the Green LED when the door is unlocked.
- Disable Buzzer Processing: When enabled, the reader expander will not control the Buzzer Output (BZ) and the output can be used for another function. When disabled the reader will control the buzzer output.

- Recycle REX Time: When enabled, will restart the door open time allowing the door to be held open and the REX pressed at each point the pre-alarm starts silencing the pre-alarm and restarting the open timer. This allows a door to be held while furniture is being moved or to provide extended access for mobility users.
- Use Programmed Card Expiry: Used for short term users (such as visitors or hotel guests) that will be configured with a start (check in) and end (check out) time, these options are designed to work with Hotel card readers and allow the reader port to alter the access control decision of a user based on the data sent from the guest card.

Expander Addressing

The Expander Addressing option is used to view the hardware that is connected to the system network, and to set the addresses (see page 108) of the modules that have auto-addressing capability. This page displays the details of all modules currently connected or that have registered previously but may currently be offline.



Module Type	Serial	Firmware	Address	Registered	Online
Keypad	15172E2B	1.35	1	®	○
Reader Expander	011145B2	1.12	2 ▾	®	○
Analog Expander	ECF63DDD	1.03	Not Set ▾	®	⊘

Listed for each module is:

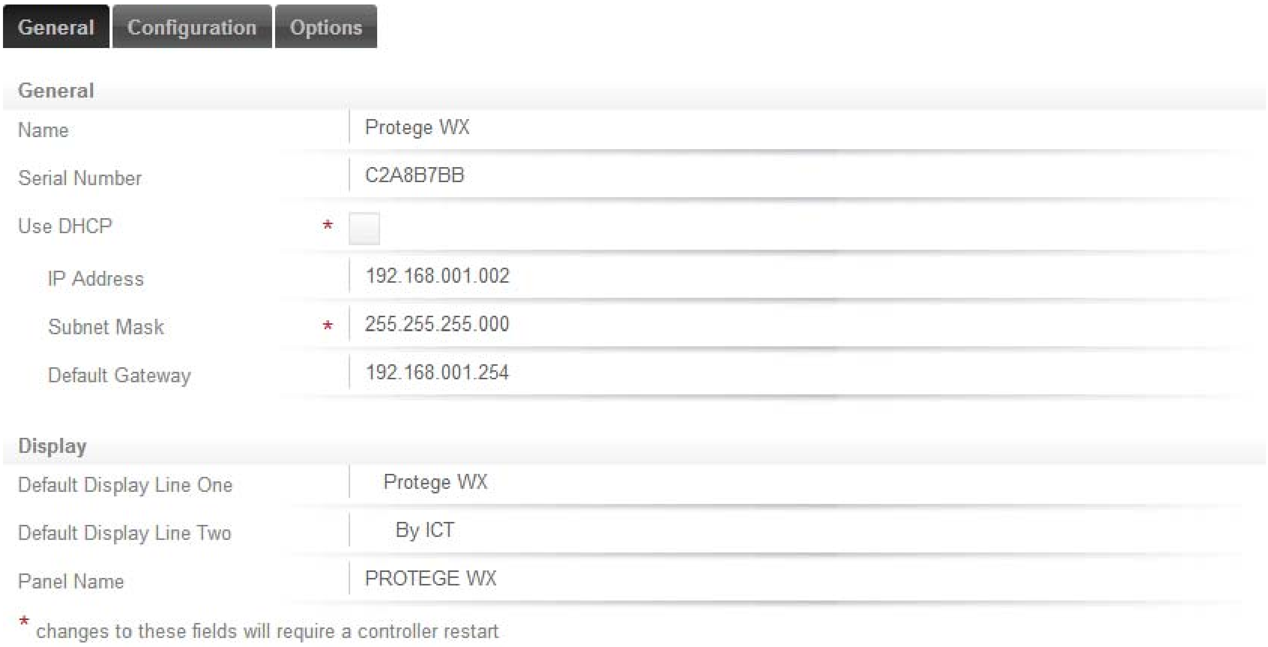
- The module type
- The serial number
- Current firmware version
- The current address of the module
- Whether the module is registered with the Controller
- Whether the module is currently online

System

The System menu is used to configure system settings, backup programming and update firmware.

This Option	Is Used To:
Settings	Configure the Controller settings including the IP address
Operators	Create and manage the operators that can access Protege WX to maintain and monitor the system
Roles	Configure the operator roles and the access they have
Backup	Backup and restore Controller programming
Firmware	View current version information and update firmware

Settings



General

Name		Protege WX
Serial Number		C2A8B7BB
Use DHCP	*	□
IP Address		192.168.001.002
Subnet Mask	*	255.255.255.000
Default Gateway		192.168.001.254

Display

Default Display Line One	Protege WX
Default Display Line Two	By ICT
Panel Name	PROTEGE WX

* changes to these fields will require a controller restart

General

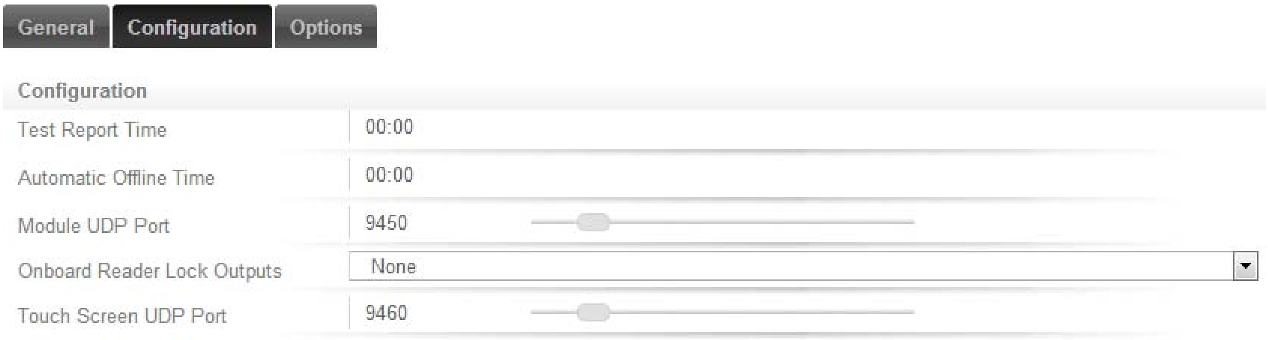
- Name: The Controller name is programmed to identify the panel to the operator or system user. Ideally the name should describe the premises or the building where the panel is installed. The name is also used within the IP and SMTP Mail Services to identify the panel to the e-mail recipient.
- Serial Number: The serial number of the Controller. This can be obtained from the label on the side of the Controller or from the configuration page of the built in web interface.
- Use DHCP: When enabled, the Controller will use DHCP to dynamically allocate an IP address instead of using a static IP address. To use this, there must be a DHCP server on the network you are attempting to connect to.
- IP Address: The Controller has a built in TCP/IP Ethernet Device and it must be programmed with a valid TCP/IP Address to allow communication. By default the IP address is set to 192.168.1.2.
- Subnet Mask: Used in conjunction with the IP Address a netmask must be configured to allow access to the appropriate node on the subnet. By default this is set to a value of 255.255.255.0.
- Default Gateway: Used in conjunction with the IP Address, the gateway can be configured to allow access to a router for external communications beyond the subnet to which the Controller is connected. By default this is set to a value of 0.0.0.0 to prevent any external communication.

> Programming the IP Address, Subnet Mask, and Default Gateway requires knowledge of the network and subnet that the system will be connected to. You should always consult the network or system administrator before programming these values.

Display

- **Default Display Line One:** The default LCD text for line one is shown on LCD keypads when they are first connected to the system. This text should be changed to the name of the building, installation or owners details.
- **Default Display Line Two:** The default LCD text for line two is shown on LCD keypads when they are first connected to the system. This text should be changed to the name of the building, installation or owners details.
- **Panel Name:** The default LCD panel name that is shown on LCD keypads when they are first connected to the system. This name will also be used to identify the Controller in the IP reporting services.

Settings | Configuration



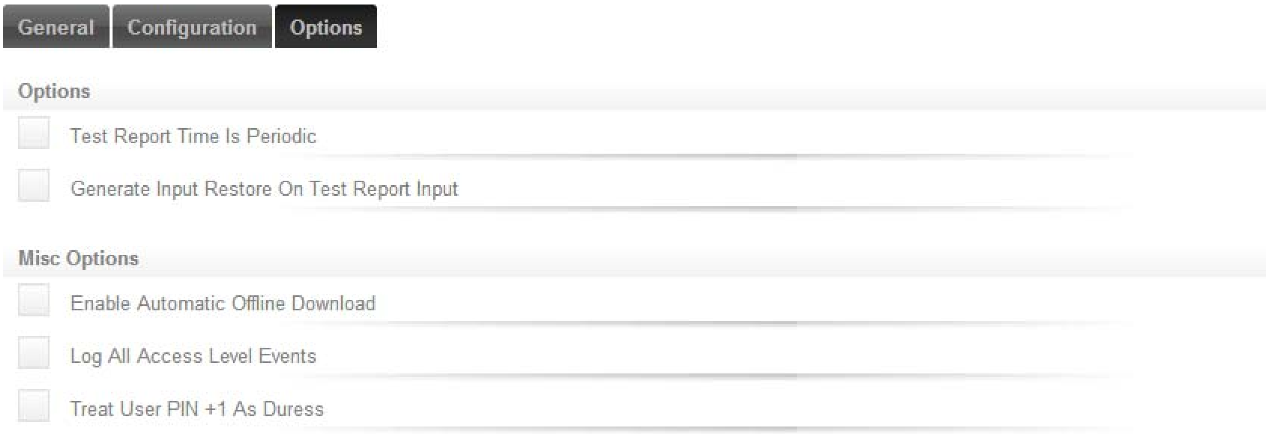
Configuration

Test Report Time	00:00
Automatic Offline Time	00:00
Module UDP Port	9450
Onboard Reader Lock Outputs	None
Touch Screen UDP Port	9460

Configuration

- **Test Report Time (HH:MM):** Used in conjunction with the Test Report Time is Periodic option (defined under Settings | Options (see page 101)) to set the time of the day or the period that the test report trouble input activates. When the Test Report Time is Periodic option is enabled, the time programmed will be used as a period between reports in hours and minutes. Otherwise it is treated as a time of day.
- **Automatic Offline Time:** Allows the panel to update the users and other offline parameters on all intelligent modules at a set time of the day.
- **Module UDP Port:** This is the UDP port that all Ethernet enabled modules will communicate with the Protege Controller over. If this port is changed all modules will also need to be changed.
- **Onboard Reader Lock Outputs:** Defines the output that will be activated upon successful door access. If set to none, the lock output (if any) programmed under the associated Reader Expander is used.
- **Touchscreen UDP Port:** The UDP port that a touchscreen will communicate over.

Settings | Options



Options

□ Test Report Time Is Periodic

□ Generate Input Restore On Test Report Input

Misc Options

□ Enable Automatic Offline Download

□ Log All Access Level Events

□ Treat User PIN +1 As Duress

Options

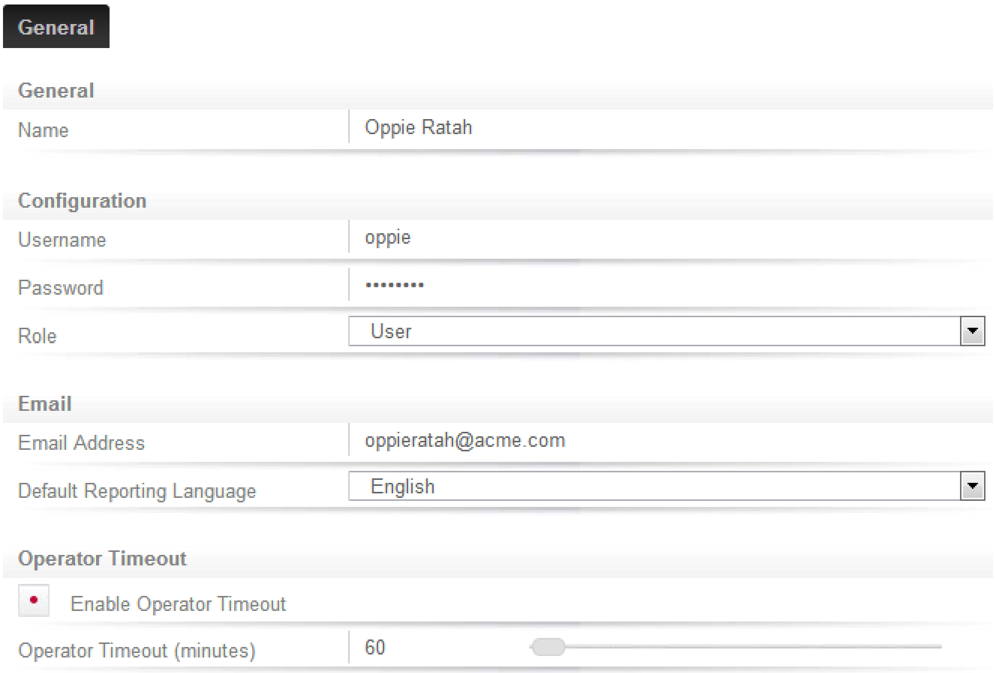
- Test Report Time is Periodic: When enabled, the test report trouble input will be activated at the frequency defined by the Test Report Time. When disabled the test report trouble input will be activated at the specified time of day.
- Generate Input Restore On Test Report Input: When enabled the Controller will generate a restore event for the trouble input test report input restoring. This occurs one minute after the trouble input has been activated.

Misc Options

- Enable Automatic Offline Download: When enabled the Controller will automatically update offline configuration parameters to all intelligent (RDI2, RDE2) modules at the time programmed in the Automatic Offline Time.
- Log All Access Level Events: When enabled the Controller will generate events including the reason a user was denied access if they do not have the required access rights.
- Treat User PIN +1 as Duress: When enabled, treats the last digit of a user's pin plus 1 as a duress code. For example, if the user pin is 1234 but the pin is entered as 1235, it will be processed as a duress code. Note that the plus 1 counter applies to the last digit only. This means if the user pin is 1239, the pin to trigger a duress code would be entered as 1230.

Operators

An operator is a person that uses Protege WX for maintaining the system and monitoring the site.



General

Name	Oppie Ratah

Configuration

Username	oppie
Password	••••••••
Role	User

Email

Email Address	oppieratah@acme.com
Default Reporting Language	English

Operator Timeout

☑ Enable Operator Timeout

Operator Timeout (minutes)	60

General

- Name: The name of the operator. This is the name that is displayed in the status bar at the top of the page.

Configuration

- Username: The username of the operator. This is the name used when logging in.
- Password: The password of the operator.
- Role: Select the appropriate role to determine what access the operator has once logged in.

E-mail

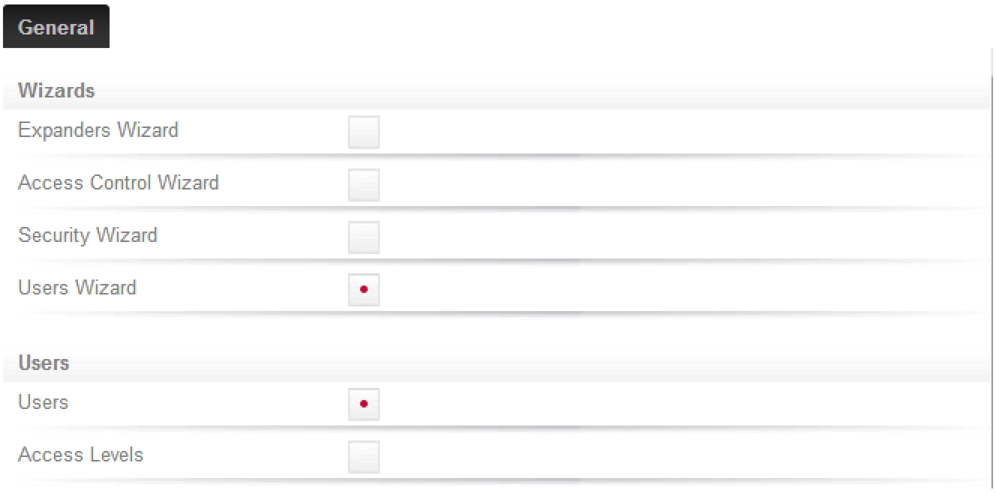
- **Email**: The email address of the operator. Currently only used for information purposes.
- **Default Reporting Language**: Reserved for future use.

Operator Timeout

- **Enable Operator Timeout:** Select this option to automatically log the operator out after a period of inactivity as defined in the Operator Timeout setting below.
- **Operator Timeout**: Defines the inactivity period at which point Protege WX will timeout and the operator will be prompted to login again to continue.

Roles

To control the access an operator has to the Protege WX system, they must be assigned a role. The role determines which pages are visible to the operator when they are logged in. If an option is enabled, that page will be visible. If it is disabled, the page is hidden.



General

Wizards

Expanders Wizard □

Access Control Wizard □

Security Wizard □

Users Wizard ●

Users

Users ●

Access Levels □

The system comes programmed with three preset roles. These roles can be customized to meet your specific requirements however caution should be taken when making changes, particularly to the Installer role, as removing permissions can prevent an operator from accessing the system.

Operator Role	Function
User	Can monitor the system and perform basic user configuration
Master	Can perform actions required to program and configure the system
Installer	Can perform all actions without any restrictions

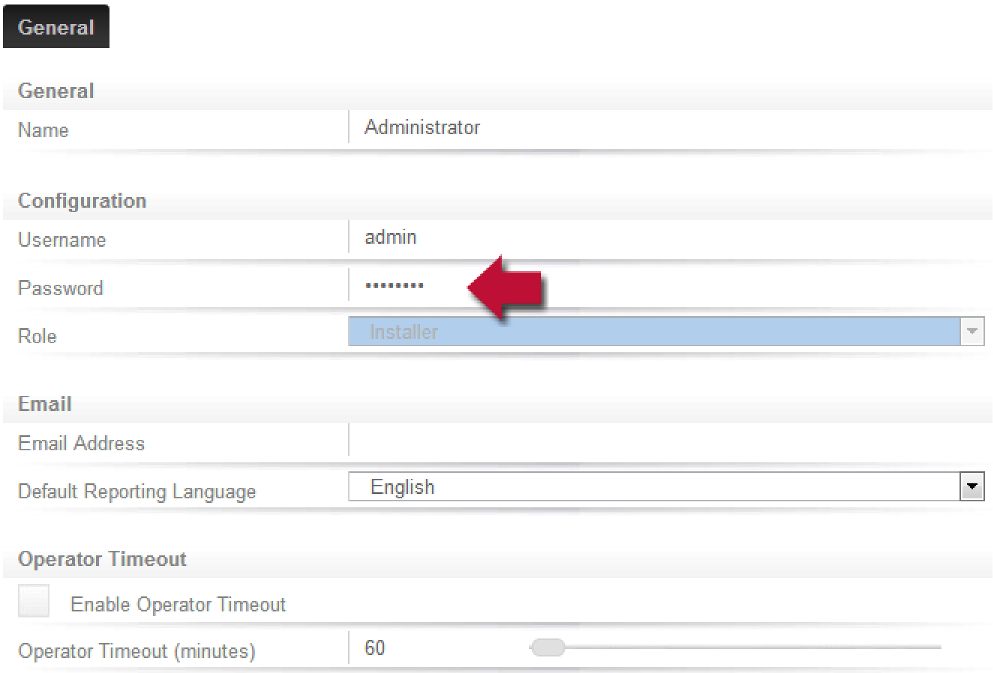
Maintaining Your System

This section covers system maintenance, including how to backup and restore Controller programming, update firmware, and addressing additional expanders that are added to the network.

Changing the Admin Password

For security reasons, it is important that you change the default admin password when Protege WX is first installed. You can also change this later.

1. To change the admin password, navigate to **System | Operators** and select **Administrator**



General

General

Name	Administrator

Configuration

Username	admin
Password	••••••••
Role	Installer

Email

Email Address	
Default Reporting Language	English

Operator Timeout

□ Enable Operator Timeout

Operator Timeout (minutes)	60

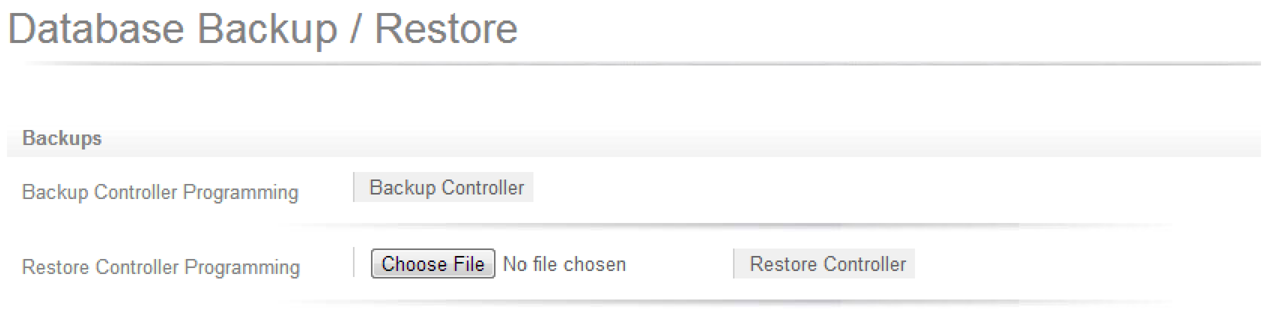
2. Enter your new password, then press **Save**.

Backing Up and Restoring Controller Programming

Creating backups of your Controller programming is good practice to ensure you are protected against damage in the event of hardware failure or malfunction.

The Protege WX interface provides a simple export tool for backing up the system to a SQL backup file (*.BAK). This file works as a snapshot of your current system, enabling you to later restore and retain the programming at the same point as you exported it. You can even backup programming from one Controller and restore it to another. This can be useful when running a test environment, or for pre-programming a system prior to deployment at a client site.

1. Navigate to System | Backup



Database Backup / Restore

Backups

Backup Controller Programming

Restore Controller Programming

No file chosen

2. To create a backup, select **Backup Controller Programming.** This creates a copy of the controllers programming which may then be restored at a later date.

   Depending on your browser settings, you may be prompted to save the file otherwise it is downloaded automatically to your Downloads folder.

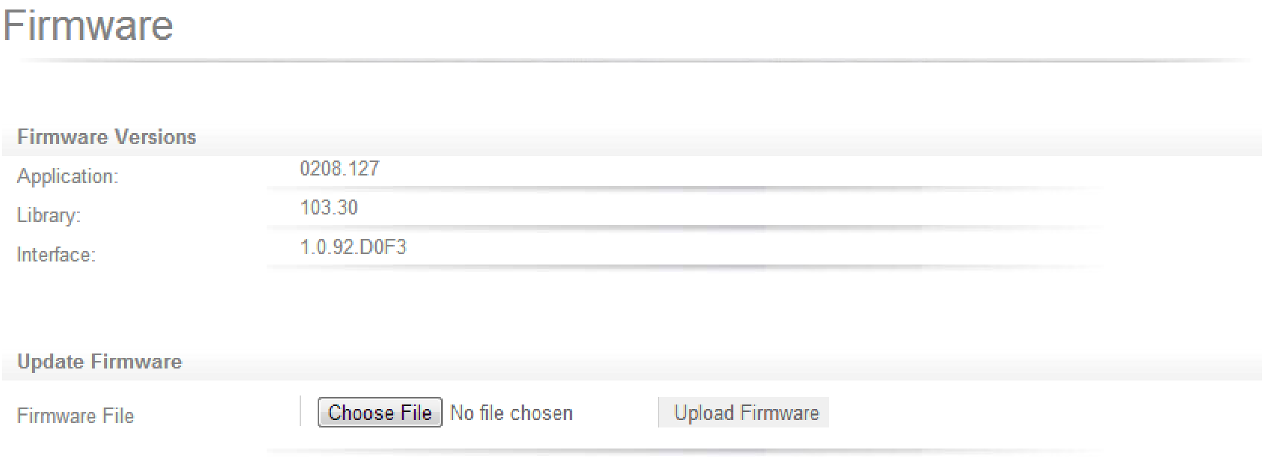
3. To restore programming, select **Restore Controller Programming.** This Imports a copy of the programming from a BAK file created using the backup option.
4. Browse to the BAK file then press **Import.**

Upgrading Firmware

From time to time, ICT release new firmware with updates and enhancements to the features included. To ensure your installation is running at the optimal performance, we recommend that all installed modules utilize the latest firmware releases.

1. From the main menu, select **System | Firmware**.

   The Firmware page opens containing details about the current firmware version that is installed.



Firmware

Firmware Versions

Application:	0208.127
Library:	103.30
Interface:	1.0.92.D0F3

Update Firmware

Firmware File

2. Click the **Choose File** button and browse to the supplied update file.
3. Click **Upload Firmware** to commence the firmware update procedure.

Progress is shown as the new firmware is installed. Once finished, you will be prompted to cycle power to the controller. The Controller is then restarted and normal operation is resumed.

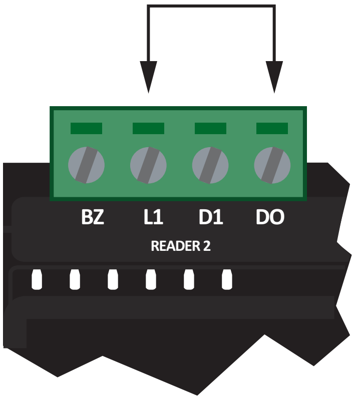
> Note that this process can take up to 5 minutes to complete so we recommend that firmware updates are performed when the site is closed for maintenance or at times of low activity. The Controller will not be able to perform it's normal function while firmware is being updated.

Defaulting a Controller

The Controller can be set back to the factory default which resets all internal data and event information. This allows you to remove all programming and start afresh.

1. Remove power to the Controller by disconnecting the 12V DC input.
2. Connect a wire link between the **Reader 2** D0 input and the **Reader 2** L1 output.
3. Power up the Controller.
4. Once the Controller has started and the Status light is flashing, remove the wire link from the Reader 2 connector.

The system will now be defaulted with all programming and settings returned to factory configuration.



> Defaulting the Controller does not reset the IP address. Refer to Configuring the IP Address (see page 107) for instructions on how to reset the address.

Configuring the IP Address

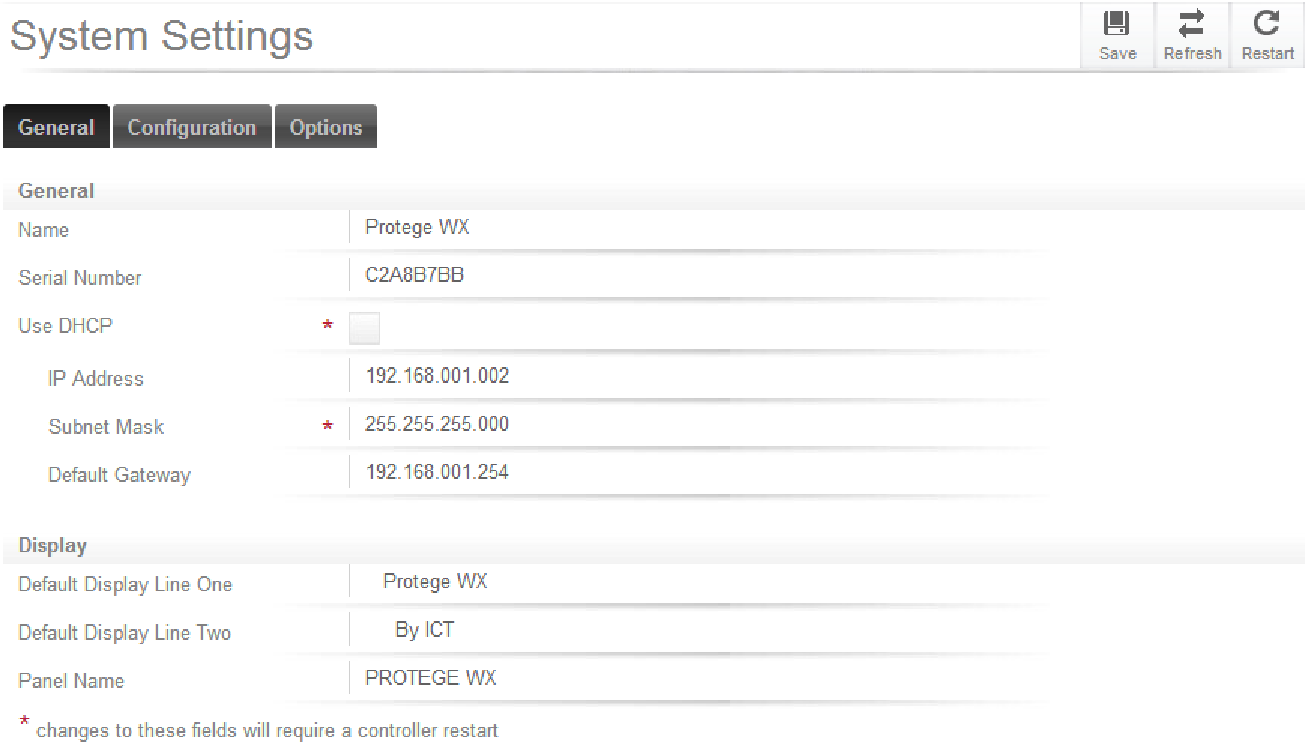
The Controller must be programmed with a valid IP Address to allow communication. By default this is set to 192.168.1.2 but can be adapted to suit your network requirements and addressing scheme.

> Programming the IP Address, Subnet Mask, and Default Gateway requires knowledge of the network and subnet that the system will be connected to. You should always consult the network or system administrator before programming these values.

1. With the Controller connected to your network, type the IP address into your browser. The default IP address is 192.168.1.2

   If the IP address has been configured previously and you are not sure what it is, you can temporarily default it (see page 108).

2. Login and navigate to System | Settings



System Settings

General	
Name	Protege WX
Serial Number	C2A8B7BB
Use DHCP *	□
IP Address	192.168.001.002
Subnet Mask *	255.255.255.000
Default Gateway	192.168.001.254
Display	
Default Display Line One	Protege WX
Default Display Line Two	By ICT
Panel Name	PROTEGE WX

* changes to these fields will require a controller restart

3. Enter the required settings, and click Save.

   - Use DHCP: When enabled, the Controller will use DHCP to dynamically allocate an IP address instead of using a static IP address. To use this, there must be a DHCP server on the network you are attempting to connect to.
   - IP Address: The IP address to use. By default this is set to 192.168.1.2.
   - Subnet Mask: Used in conjunction with the IP Address, a netmask must be configured to allow access to the appropriate node on the subnet. By default this is set to 255.255.255.0.
   - Default Gateway: Used in conjunction with the IP Address, the gateway can be configured to allow access to a router for external communications beyond the subnet to which the Controller is connected. By default this is set to 0.0.0.0 to prevent any external communication.

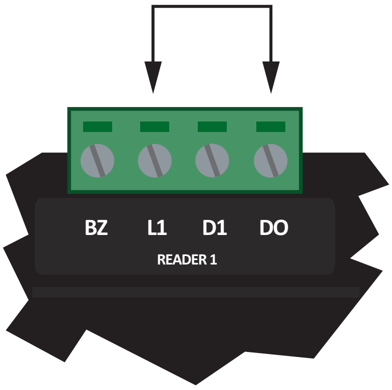
4. You must then Restart the controller for the new configuration to take effect.

Temporarily Defaulting the IP Address

If you don't know the currently configured IP address, you can temporarily set to 192.168.111.222, then connect to the web interface to view and/or change it.

This resets the IP address for as long as power is applied but **does not** save the change permanently. Once the link is removed and power is cycled to the unit, the previously configured IP address is used again.

1. Remove power from the Controller by disconnecting the 12V DC input.
2. Connect a wire link between **Reader 1** D0 input and **Reader 1** L1 output.



3. Power up the Controller.
4. When the Controller starts up it will use the following settings:

   IP address : 192.168.111.222

   Subnet Mask : 255.255.255.0

   Gateway : 192.168.111.254

   DHCP : disabled
5. Connect to the Controller by entering 192.168.111.222 into the address bar of your web browser, and view or change the IP address as required.
6. Remove the wire link and cycle power to the Controller again.

   You can now connect to the Controller using the newly configured (or now known) IP address.

Addressing Expanders

The Expander Addressing option is used to view the hardware that is connected to the system network, and to set the addresses of DIN Rail modules which have auto-addressing capability. This page displays the details of all modules currently connected or that have registered previously but may currently be offline.

Listed for each module is:

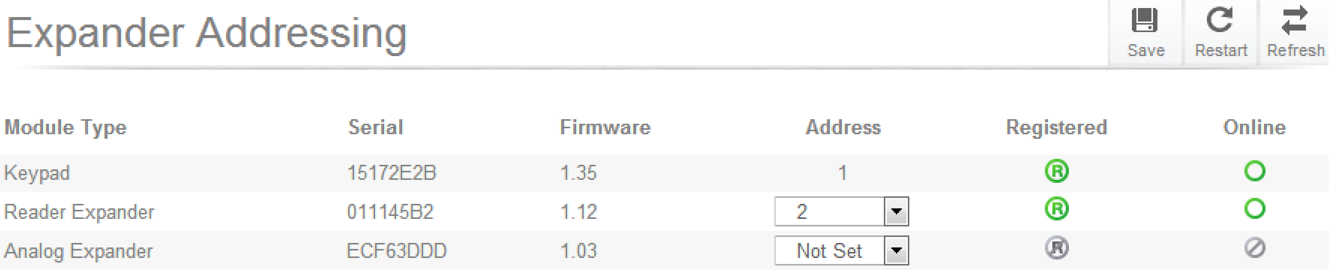
- The module type
- The serial number
- Current firmware version
- The current address of the module
- Whether the module is registered with the Controller
- Whether the module is currently online

When connecting a module to the network, it must be added to Protege WX and allocated a unique physical address. By default all DIN Rail modules are shipped from ICT with the address of 254 and without changing this address, the module will not be able to register with the Controller.

For older legacy PCB modules, the address is configured via DIP switches. Refer to the relevant Installation Manual for instructions on configuring the address of the module.

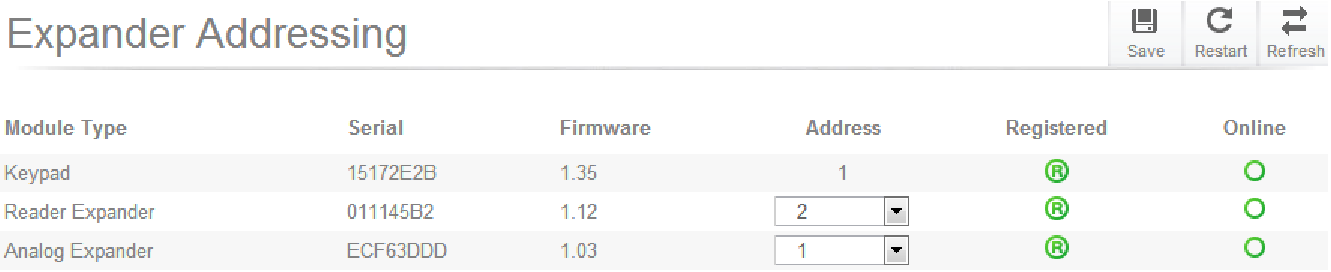
To Set the Network Address of a Module:

1. Ensure the Controller is correctly powered.
2. Connect the module(s) that require addressing to the module network. Make sure that the Power light on each module is on and that the Status light begins flashing rapidly.
3. Allow some time for the module(s) to attempt to register with the Controller.
   - If the module has the default address of 254 or has the same address as another module, the **Fault** light will begin flashing at 1 second intervals.
   - If the module has been previously addressed and is not a duplicate, then it will succeed in registering and the **Status** light will begin flashing at 1 second intervals.
4. Once all modules have completed the registration process (successful or not), open the Module Addressing window by selecting **Expanders | Expander Addressing**



Module Type	Serial	Firmware	Address	Registered	Online
Keypad	15172E2B	1.35	1	®	○
Reader Expander	011145B2	1.12	2	®	○
Analog Expander	ECF63DDD	1.03	Not Set	®	⊘

5. Enter an address for the relevant module(s) by selecting an option under the Address column then click **Save** to save the address and restart the module.
6. Allow around 5 seconds per module for the new address to be sent and registered then click **Refresh** to update the list and display the new addresses.



Module Type	Serial	Firmware	Address	Registered	Online
Keypad	15172E2B	1.35	1	®	○
Reader Expander	011145B2	1.12	2	®	○
Analog Expander	ECF63DDD	1.03	1	®	○

   - If the address has not changed, check the module is online and communicating and that is has finished attempting to register.
   - If the address has changed but the module is not shown as registered, check the address is in the valid address range and that it is not a duplicate of another modules address.

   Once all modules are online and registered with the desired addresses, the addressing process is complete.

Troubleshooting

This section includes helpful troubleshooting information.

Common Health Status Messages

The Health Status is displayed on the Home Page and provides details of the overall status of the system and can be useful in identifying any problem areas that need to be addressed.

It lists any problems that the Controller has with its current configuration. This includes:

- Modules that require a restart
- Modules that are offline
- Areas that require rearming due to input changes
- Areas where the tamper area (24 hour monitoring) is disarmed
- Inputs that have been assigned to an area, but not assigned a type
- Items that can't fit in the internal database

Essentially, anything that has been configured but that is not operating according to that configuration, is shown in this list.

Modules that Require a Restart

Typical Health Status Message

Reader Expander Warehouse Reader requires a module restart

Cause

Modules need to be restarted whenever a programming change is made that requires the hardware to physically function in a different manner.

Solution

1. Navigate to the appropriate Expander menu (for example Expanders | Reader Expander)
2. Select the module that is listed in the health status message, then click the Restart button on the toolbar

Modules that are Offline

Typical Health Status Message

Reader Expander Warehouse Reader is offline

Cause

This can occur when the module has been added, but the address has not been correctly set.

Note that if you have recently cycled power to the Controller, it can take up to 250 seconds for the module to come back online.

Solution

1. If you have cycled power to the Controller, ensure you have allowed enough time for the module to come online.
2. Navigate to the appropriate Expander menu (for example Expanders | Reader Expander)
3. Check that the **Physical Address** allocated on the General tab, matches that allocated under Expanders | Expander Addressing
4. If the problem continues, check that the module is wired correctly.
5. Check the LED indicators of the module. If the fault light is on and the status light is flashing red, the number of sequential flashes will indicate an error code (see page 42).

Areas Requiring Rearming due to Input Changes

Typical Health Status Message

Area Warehouse requires rearming due to Input Warehouse PIR changes

Cause

The 24 hour portion of an area must be rearmed when programming changes result in the input functioning in a different manner. This is to prevent inadvertent changes to a live system that could result in an undetected security breach.

Solution

1. Navigate to Monitoring | Areas and click Controls to open the manual control window.
2. Click Disarm 24 to disarm 24 hour monitoring, then Arm 24 to enable it.

Areas with the Tamper Area Disarmed

Typical Health Status Message

Area Warehouse has its Tamper Area disarmed

Cause

Every Area created in Protege WX is actually made up of two areas: The main area that monitors devices (such as PIRs) only when it is armed, and the 24 hour (or Tamper) area that monitors for a tamper or short condition on devices (such as PIRs) 24/7.

The 24 hour tamper area is armed automatically when the main area is armed.

Solution

1. Navigate to Monitoring | Areas and click Controls to open the manual control window.
2. Click Arm 24 to enable 24 hour monitoring.

Inputs Assigned an Area but no Input Type

Typical Health Status Message

Input Warehouse PIR has an Area but no Input Type assigned

Cause

An input has been assigned to an area, but the system has not been instructed on what to do if the input is activated.

Solution

1. Navigate to Programming | Inputs and select the input listed in the message
2. Click the Areas and Input Types tab, then select an Input Type from the dropdown
3. Save your changes

Items that Can't Fit in the Database

Typical Health Status Message

Input Warehouse PIR will not fit into the internal database

Cause

Each module only has a set number of inputs and outputs. For example, the Controller has 8 inputs and 3 outputs, whereas a Reader Expander has 8 inputs and 8 outputs. If you add a record where the address is higher than the maximum allowed for that Expander, it cannot be added to the system. For example, if an input is added to a Controller with a Module Input of 9 or higher, where the Controller only has 8 physical inputs.

Solution

Ensure the Module Input address physically exists.

Contact

Integrated Control Technology welcomes all feedback.

Please visit our website (http://www.incontrol.co.nz) or use the contact information below.

Integrated Control Technology

P.O. Box 302-340
North Harbour Post Centre
Auckland
New Zealand

11 Canaveral Drive
Albany
North Shore City 0632
Auckland
New Zealand

Phone:	+64-9-476-7124
	Toll Free Numbers:
	0800 ICT 111 (0800 428 111) - New Zealand
	1800 ICT 111 (1800 428 111) - Australia
	1855 ICT 9111 (1855 428 9111) - USA/Canada
Email:	sales@incontrol.co.nz or support@incontrol.co.nz
Web:	www.incontrol.co.nz

Index

Integrated Control Technology Limited

11 Canaveral Drive, Albany, Auckland 0632
P.O. Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: support@incontrol.co.nz Phone: +64 (9) 476 7124 **Fax:** +64 (9) 476 7128
Designers & manufacturers of integrated electronic access control, security & automation products.
Designed & manufactured by Integrated Control Technology Limited.

www.incontrol.co.nz

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees, shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the Integrated Control Technology policy of enhanced development, design and specifications are subject to change without notice.